WatchGuard Endpoint Security

WatchGuard SIEMFeeder Event Guide

For WatchGuard Advanced EPDR, WatchGuard EPDR and WatchGuard EDR

Revision Date: June 2024

Version: 4.40.00

About This Guide

The purpose of this guide is to help you leverage the endpoint security information provided by WatchGuard Endpoint Security and integrate it into the storage infrastructure implemented in your company.

The product name WatchGuard Endpoint Security is used generically in this guide to refer to WatchGuard Advanced EDR, WatchGuard Advanced EPDR and WatchGuard Advanced EPDR.

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 6/28/2024

Copyright, Trademark, and Patent Information

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, providing best-in-class Unified Threat Management, Next Generation Firewall, secure Wi-Fi, and network intelligence products and services to more than 75,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for Distributed Enterprises and SMBs. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter, @WatchGuard on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

Address

WatchGuard Technologies
255 S. King St.
Suite 1100
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

Contents

How to Use This Guide

This document is intended for Companies that have contracted the WatchGuard SIEMFeeder service from WatchGuard for the WatchGuard Advanced EDR, WatchGuard Advanced EPDR and WatchGuard Advanced EPDRproducts.

Within organizations, the information in this guide is intended for:

- IT security specialists who require a detailed description of the data WatchGuard SIEMFeeder sends to the organization's SIEM platform.
- The administrator of the SIEM solution implemented in the company, who must know the format of the information received to incorporate it into the organization's database.

Unless otherwise indicated, all the procedures and instructions in this guide apply equally to:

- Customers with WatchGuard Advanced EDR licenses contracted.
- Customers with WatchGuard Advanced EPDR licenses contracted.
- Customers with WatchGuard Advanced EPDR licenses contracted.
- Customers with the WatchGuard SIEMFeeder service contracted.

Document Conventions

This document uses these formatting conventions to highlight specific types of information:

This is a note. It highlights important or useful information.

This is a caution. Read carefully. There is a risk that you could lose data, compromise system integrity, or impact device performance if you do not follow instructions or recommendations.

Benefits and General Architecture

WatchGuard SIEMFeeder is the WatchGuard service that delivers information and knowledge generated by the WatchGuard Endpoint Security products to customer SIEM platforms.

SIEMFeeder sends security intelligence about the processes run on user computers to customer SIEM platforms. With this information, network administrators have more visibility into what happens in the IT infrastructure they manage.

Network administrators can use this information to uncover unknown threats, advanced malware (Advanced Persistent Threats), and targeted attacks to extract confidential information from companies. To achieve this goal, SIEMFeeder gets information about the activities conducted by running applications from the continuous monitoring in the WatchGuard Endpoint Security software installed on computers and devices. This endpoint information is enriched with the security intelligence generated at WatchGuard and sent to the customer SIEM platform.

Benefits

With the security information provided, security administrators can:

- **View the evolution of the malware detected on the network** — Whether it was run or not, the infection vector, and the actions taken by processes. With this information, administrators can make decisions to take remediation actions and adjust security policies.
- **View the actions run by each process** — This enables administrators to focus their attention on the suspicious activities performed by new, yet-to-be-identified programs, and compile data that can be used to reach conclusions about their potential risk.
- **View attempts to access confidential information** — This prevents data leakage and theft. The service shows the Office files, databases, and other repositories of confidential information accessed by malware.
- **View the network connections made by processes** — This identifies suspicious or potentially risky destinations used to exfiltrate data.
- **Find all executed programs** — This is useful to for programs with known vulnerabilities installed on user computers, to design software update plans and adjust security policies.

Information Flow Generated by SIEMFeeder

WatchGuard Endpoint Security constantly monitors the actions taken by the processes run on user computers. These actions are sent to the WatchGuard cloud platform, where they are analyzed and leveraged to automatically extract advanced security intelligence.

SIEMFeeder gathers information about the events monitored by WatchGuard Endpoint Security and the security data generated, creating a single data flow compatible with the customer SIEM server.

For more information about the data flow generated by SIEMFeeder see the WatchGuard SIEMFeeder online help (https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Endpoint-Security/security-modules/siemfeeder/siemfeeder-about.html).

Requirements

SIEMFeeder does not require any changes on the monitored computers because the service receives data automatically from each workstation and server. It might be necessary to install and configure various items in the company IT infrastructure, depending on the contracted product.

Theses resources are required in the customer's IT infrastructure:

- WatchGuard Importer must be installed and configured, preferably on a server.
- If the event flow received is large, we recommend that you install a queue manager compatible with WatchGuard Importer.
- A SIEM server that supports the CEF and LEEF log formats must be installed.

For more information about how to install and configure WatchGuard Importer, see the WatchGuard SIEMFeeder online help (https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Endpoint-Security/security-modules/siemfeeder/siemfeeder-about.html).

Events and Extended Information

WatchGuard SIEMFeeder transforms the telemetry received from the computers and devices protected by WatchGuard Advanced EPDR and WatchGuard Advanced EDR into text files, which contain formatted events compatible with SIEM servers.

The basic unit of information that customers receive is called an event. Each relevant action performed by processes run on a user computer is transformed into an event which is delivered to the SIEM server. This section describes each event and provides example values.

Event Structure

An event is an action recorded on a customer computer and described through pairs of field-value combinations. There are numerous types of events, and each type includes specific field-value combinations. SIEMFeeder adds a header to this collection of field-value pairs. The header information enables the event to be included in a log file that is compatible with log formats used by SIEM servers: CEF or LEEF.

For more information about the LEEF format, see: https://www.ibm.com/docs/en/dsm?topic=leef-overview.

For more information about the CEF format, see: https://community.microfocus.com/cfs-file/__key/communityserver-wikis-components-files/00-00-00-00-23/3731.CommonEventFormatV25.pdf.

Event groups

A log or log file is a group of events delivered to the customer SIEM server. Log files generated by SIEMFeeder are of different sizes and can contain one or more events in different categories. The events included in a single log file can come from one or more computers on the customer network.

Sequences and Delays

The maximum time that elapses between a process that performs an action on a computer protected by WatchGuard Endpoint Security and when SIEMFeeder formats the corresponding event and adds security intelligence is approximately 20 minutes.

Events received from customer computers are processed on a First In First Out (FIFO) basis.

Log files sent to the SIEM server are not sent in a predefined sequence. However, all events have a time stamp that enables them to be precisely situated on a timeline.

Log Format in WatchGuard SIEMFeeder

WatchGuard SIEMFeeder delivers information in CEF or LEEF format. Contact your assigned sales representative to change the format of the logs received. You can also send an email to panda.AD_SIEMFeeder@watchguard.com.

All log files sent by SIEMFeeder have UTF-8 encoding.

Common Event Format (CEF)

CEF format consists of these data sections:

- **Prefix section or header**: Identifies the event category and defines the file as a CEF log file. Fields in this section are separated by pipes "|" and the meaning of each field is determined by its position.
- **Event extensions section**: Common to both types of log files (CEF and LEEF). This includes field-value pairs separated by spaces.

SIEMFeeder does not include the syslog header in CEF logs.

This is an example of the **registryc** event (**createExekey**) in CEF format:

```
CEF:1|WatchGuard Technologies,
Ltd.|paps|02.45.00.0000|registryc|registryc|1|Date=2018-09-27 02:26:52.200188
MachineName=DESKTOP-PC MachineIP=192.168.0.11 User=NT AUTHORITY\SYSTEM
MUID=713FC2B45B429J291EB53467357AC1B7 Op=CreateExeKey
Hash=C86854DF4F3AEC59D523DBAD1F5031FD DriveType=Fixed
Path=SYSTEMX86|\CompatTelRunner.exe ValidSig=true Company=Microsoft Corporation
Broken=true ImageType=EXE 32 ExeType=Unknown Prevalence=Medium PrevLastDay=Low
Cat=Goodware MWName= TargetPath=3|PROGRAM_FILESX86|\Windows Defender\MsMpeng.exe
RegKey=\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\WicaAvPathsExpiredTemp?0
```

Prefix Section

```
CEF:1|WatchGuard Technologies, Ltd.|paps|02.45.00.0000|registryc|registryc|1|
```

The fields in the prefix section are separated by pipes "|".

Field	Description	Example
Format:version	Log format and version identifier.	CEF:1
Device vendor	Name of the service provider.	WatchGuard Technologies, Ltd.
Device Product	Internal name of the software or device.	paps
Signature	Version of the protection that generated the event.	2.43.00.0000
Name and Name 2	For alert events, the name of the event is in the fields **Name** and **Name 2**. So the fields **Name** and **Name 2** must be combined to get the full name of the alert. For other types of event, **Name 2** contains a copy of the contents of **Name**.	registryc
Severity	Except for alert events, the value of the Severity field is always 1. For alert events, the value of this field is calculated based on the type of alert and the action taken by the security software on the user computer. This action is specified in the second value of the event ExecutionStatus field. For more information about the possible values of the Severity field, see the section on the relevant event.	Numeric value

Event Extensions Section

For more information about the supported events, their fields, and a detailed description of each field, see *Event Structure and Field Syntax*.

Log Event Extended Format (LEEF)

LEEF format consists of these data sections:

- **Header**: Identifies the event category and defines the file as a LEEF log file. Fields in this section are separated by pipes "|" and the meaning of each field is determined by its position.
- **Event attributes section**: Common to both types of log files (CEF and LEEF). This section contains fields that describe the event and its values.

SIEMFeeder does not include the syslog header in LEEF logs.

This is an example of the registryc event (createExekey) in LEEF format:

```
LEEF:1.0|WatchGuard Technologies, Ltd.|paps|02.43.00.0000|registryc|sev=1
devTime=2016-09-22 15:25:11.000628 devTimeFormat=yyyy-MM-dd HH:mm:ss.SSS
usrName=LOCAL SERVICE domain=NT AUTHORITY src=10.219.202.149
identSrc=10.219.202.149 identHostName=PXE68XXX HostName= PXE68XXX
MUID=1F109BA4E0XXXX37F9995D31FXXXX319 Op=CreateExeKey
Hash=C78655BC80301D76ED4FEF1C1EA40A7D DriveType=Fixed Path=SYSTEM|\svchost.exe
ValidSig= Company=Microsoft Corporation Broken=true ImageType=EXE 64
ExeType=Unknown Prevalence=High PrevLastDay=Low HeurFI=67108872 Skeptic=
AVDets=0 JIDFI=3431993 1NFI=116241 JIDMW=11195630 1NMW=4308325 Class=100
Cat=Goodware MWName= TargetPath=0|pune.com RegKey=\ REGISTRY\ MACHINE\ SYSTEM\
ControlSet001\services\Tcpip\Parameters?DhcpDomain
```

Header Section

```
LEEF:1.0|WatchGuard Technologies, Ltd.|paps|02.43.00.0000|registryc|
```

In LEEF log files, the event severity is not indicated by the Severity field in the header. It is specified in the attributes section ('Sev=number' field). For more information about the possible values of the Sev field, see the section on the relevant event.

Field	Description	Example
Format:version	Log format and version identifier.	LEEF:1
Vendor	Name of the service provider.	WatchGuard Technologies, Ltd.
Product	Internal name of the software or device.	paps
Version	Version of the protection that generated the event.	2.43.00.0000
Event ID Description	Full name of the event sent.	registryc

Event Attributes Section

For more information about the supported events, their fields, and a detailed description of each field, see *Event Structure and Field Syntax*.

Event Categories

The type of event received is specified in the Name and Name 2 fields of the Prefix section of CEF files or in the Event ID Description field of the Header section of LEEF files. The type of event is also included in the op field of the Attributes section in LEEF files, or the Extensions section in CEF files, although not all types of events include this field.

This section includes a description of all the events that can appear in the Name/Event ID Description field, grouped by type.

Agent Deployment

Field	Description
install	Installation and removal of the WatchGuard endpoint agent.

Alert Creation

Field	Description
alertmalware Malware Detected	Malware detected.
alertpup PUP Detected	Unwanted program (PUP) detected.
alertrdpattack RDPAttack Detected	Brute-force RDP attack detected.
alertadvpolicy ADVPolicy Detected	Detection made by the advanced security policies. This event is available only in WatchGuard Advanced EPDR.
alertsecappcontrol SecAppControl Detected	Detection by a process name or MD5 defined by the administrator in the advanced security policies. This event is available only in WatchGuard Advanced EPDR.
alertprodappcontrol ProdAppControl Detected	Detection made by the program blocking settings defined by the administrator.
alertexploit Exploit Detected	Exploit detected.

Field	Description
alertdeepinspection DeepInspection Detected	Network attack detected.
Alerteae AccessEnforcement	Detection of connections from a computer with a risk level higher than the level defined by the network administrator.
Alertvulnerabledriver VulnerableDriver Detected	Vulnerable driver load blocked or detected.
thalert	Detections of these types: ■ Indicators generated by the cyberattack radar in Orion. ■ IOCs loaded onto the platform through the Orion API. ■ IOAs detected by WatchGuard Endpoint Security. ■ Advanced IOAs detected by WatchGuard Advanced EPDR.

Changes to User Operating Systems

Field	Description
hostfiles	Modification of the HOSTS file.
monitoredregistry	Access to sensitive registry branches in an attempt to persist on the system after a restart.
registrym	A branch in the registry has been modified to point to an executable file.
registryc	Creation of a branch in the computer registry that points to an executable file.
openlsass	Access to the LSASS process in an attempt to compromise user credentials.
modLinuxCfg	Modification of a Linux operating system configuration file.
modOSXCfg	Modification of a macOS operating system configuration file.
systemops	Modification of the operating system through WMI (Windows Management Interface).

Process Manipulation

Field	Description
createremotethread	Remote execution thread created.
exec	Process executed.
createprocessbyWMI	Creation of a process through the WMI system.
scriptcreation	Script created.
scriptlaunch	Script executed.
createpe	Executable program created.
modifype	Executable file modified.
renamepe	Executable file renamed.
deletepe	Executable program deleted.
loadlib	Library loaded.
heuhooks	Exploit attempt detected.
loaddrvvulnerable	Vulnerable driver loaded.

File Download

Field	Description
urldownload	File downloaded.

Access to Data

Field	Description
createcmp	Compressed file created.
opencmp	Compressed file opened.
monitoredopen	Access to monitored data files.
createdir	Directory created in the file system.
socket	Network communication established.

Other

Field	Description
criticalsoft	Detection of vulnerable applications installed on the device.
processnetbytes	Network data consumed by a process.
dnsops	Process with failed DNS resolution requests.
loginoutsops	Login and logout on the user's computer.
deviceops	Connection or removal of external devices.
notblocked	Event that WatchGuard Endpoint Security has not analyzed due to exceptional circumstances.
svcControl	Attempt to modify files of the security product installed.
block	Blocked the execution of a program because it is not yet classified or is suspected of being malware.

Subscription to Event Categories

SIEMFeeder can generate a significant amount of events, depending on the activity detected in the customer IT infrastructure. This could affect the performance of the customer network and the event storage and processing services. For this reason, customers have the option to subscribe only to the groups of events that are most relevant to them.

The available types of events are grouped into several categories. A customer can subscribe to one or several categories, or receive all events, unfiltered. By default, customers are subscribed to special category 7, which includes all events with no filters.

Change Event Subscription

Send an email to panda.AD_SIEMFeeder@watchguard.com, specifying the numbers of the event categories you want to subscribe to.

Available Event Categories

The createcmp, createdir, criticalsoft, hostfiles, install, opencmp, block, urldownload, and notblocked events do not belong to any specific category. To receive them, the customer must be subscribed to special category 7, which includes all events with no filters.

Field	Category	Description
Threat detections (malware, PUPs, exploits)	1	Alerts about malware/PUPs, exploits, items blocked by advanced policies, and network attacks. ■ alertmalware Malware Detected ■ alertpup PUP Detected ■ alertdeepinspection DeepInspection Detected ■ alertrdpattack RDPAttack Detected ■ alertadvpolicy ADVPolicy Detected (event available in WatchGuard Advanced EPDR) ■ alertsecappcontrol SecAppControl Detected (event available in WatchGuard Advanced EPDR) ■ alertprodappcontrol ProdAppControl Detected ■ alertexploit Exploit Detected ■ alertvulnerabledriver VulnerableDriver Detected
Loading and execution of executable (PE) files and scripts	2	Loading and execution of binary and non-binary (scripts) executable files. ■ createremotethread ■ exec ■ loadlib ■ scriptlaunch ■ createprocessbyWMI
Communications	3	Socket open and use events. ■ sockets ■ processnetbytes ■ dnsops
Data access	4	Access to data contained in files and in the Windows registry. ■ monitoredopen ■ monitoredregistry ■ openlass
Creation and modification of executable (PE)	5	Creation and modification of binary and non-binary (scripts) executable files.

Field	Category	Description
files and scripts		■ createpe ■ modifype ■ renamepe ■ deletepe ■ scriptcreation
Access to the Windows registry	6	Events related to access to the Windows Registry. ■ registryc ■ registrym
No filters	7	All events are sent, including createcmp, createdir, criticalsoft, hostfiles, install, opencmp, block, urldownload, notblocked, loaddrvvulnerable and alerteae.
System events	8	Events related to access to devices, the WMI engine, as well as logins and logouts. ■ deviceops ■ loginoutsops ■ systemops ■ modLinuxCfg ■ modOSXCfg
Malware indicators	9	THAlert event with alerts generated by: ■ The threat hunting rules in Orion ■ The IOCs defined in Orion ■ The IOAs module in WatchGuard Endpoint Security.

Event Structure and Field Syntax

Internal structure of events

SIEMFeeder describes every event by means of a field–value pair. SIEMFeeder events are active events or passive events.

Active Events

Most received events describe situations in which a process performs an action on a sub-process. The type of item that receives the action varies depending on the event category. The sub-process or item can be:

- **Another process**: In events where a process is uploaded or downloaded, a library is loaded, etc.
- **Executable file**: In events where a program is created, deleted, or modified.
- **System file**: In events where the computer HOSTS file or registry is manipulated.
- **Data file**: In events where an Office file, a database, etc. is accessed.
- **Download file**: In events generated when a process downloads data.
- **Compressed file**: In events where a compressed file is created, deleted, or modified.
- **Directory**: In events where a directory is created, deleted, or modified.

Depending on its type, an event includes or excludes fields that describe the characteristics of the process and sub-process or item. For example, in a directory creation-type event, the fields associated with the event describe the characteristics of the process (whether it is malware or not, process path, process metadata, etc.), as well as the characteristics of the sub-process. However, in this case, as it is a directory, some of the fields in the event are blank. For example, the fields that describe the sub-process as malware or the directory metadata are blank, as this information cannot be provided for directories. Other information, such as the directory path, is included in the event.

Passive Events

These are events which, in many cases, do not have a clearly defined process or sub-process, because they describe situations which occur on user computers. Passive events include the generation of alerts when malware is detected, or the installation, upgrade, or modification of the WatchGuard endpoint agent, among others.

Parent and Child Prefixes

Active processes that involve two files or processes usually show a **Parent** and **Child** prefix to differentiate the information that refers to each process:

- **Parent**: Describes an attribute of the parent process.
- **Child**: Describes an attribute of the sub-process or child process.

Other Prefixes and Affixes

Fields and values can use these abbreviations:

- **Sig**: Digital signature
- **Exe and pe**: Executable file
- **Mw**: Malware
- **Sec**: Seconds
- **Op**: Operation
- **Cat**: Category
- **PUP**: Potentially Unwanted Program
- **Ver**: Version
- **SP**: Service Pack
- **Cfg**: Configuration
- **Cmp and comp**: Compressed file
- **Dst**: Destination

Alertadvpolicy ADVPolicy Detected

Passive event that describes the parameters of the alert that WatchGuard Advanced EPDR creates when it detects a threat through the advanced security policies defined by the administrator in the Workstations and Servers settings (Advanced Protection > Advanced Security Policies).

This event is available only in WatchGuard Advanced EPDR.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date on the user computer when the event was generated.	Date
HostIp (CEF)	IP of the workstation or server on which the event was generated.	IP address
sev (LEEF)	Event severity.	9
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string
HostName	Name of the user computer where the event was generated.	Character string
ThreatType	Type of detected malware.	“ADVPolicy” character string
ExecutionStatus	Action taken by the WatchGuard endpoint agent.	Enumeration

Field	Description	Value
	■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands.	

Field	Description	Value
	■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file belonging to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key belonging to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key belonging to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file belonging to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file belonging to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache. ■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
DwellTimeSecs	Time elapsed from the first time the threat was	Seconds

Field	Description	Value
	seen on the customer network.	
MWHash (LEEF) ItemHash (CEF)	Malware hash.	Character string
MWPath (LEEF) ItemPath (CEF)	Malware path.	Character string
MWName (LEEF) ItemName (CEF)	Name of the malware item if it is already cataloged as a threat.	Character string
SourceIP	IP address of the remote computer if the malware came from an external computer.	IP address
SourceMachineName	Name of the remote computer if the malware came from an external computer.	Character string
SourceUserName	User of the remote computer if the malware came from an external computer.	Character string
UrlList	List of accessed URLs if a browser exploit is detected.	Character string
DocList	List of accessed documents if a file exploit is detected.	Character string
Version	Content of the Version attribute of the process metadata.	Character string

Field	Description	Value
Vulnerable	Indicates if the application is vulnerable.	Boolean
MUID	Internal ID of the customer computer.	Character string
DriveType	Type of drive that contains the process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration

Alertdeepinspection DeepInspection Detected

Passive event that describes the parameters of the alert SIEMFeeder creates when it detects an attempt to exploit a vulnerability through the network.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date of the user computer when the event was generated.	Date
HostIp (CEF)	IP address of the workstation or server on which the event was generated.	IP address
sev (LEEF)	Event severity. See *Severity/Sev Field Calculation*.	Numeric value
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string
HostName	Name of the user computer that generated the event.	Character string
ThreatType	Type of malware detected.	“DeepInspection” character string
ExecutionStatus	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block**	Enumeration

Field	Description	Value
	■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands.	

Field	Description	Value
	■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file belonging to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key belonging to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key belonging to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file belonging to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file belonging to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache. ■ **AllowSWAuthorized**:Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	

Field	Description	Value
DwellTimeSecs	Time elapsed from the first time the threat was seen on the customer network.	Seconds
MWHash (LEEF) ItemHash (CEF)	Malware hash.	Character string
MWPath (LEEF) ItemPath (CEF)	Malware path.	Character string
MWName (LEEF) ItemName (CEF)	Name of the malware item if it is already cataloged as a threat.	Character string
SourceIP	IP address of the remote computer if the malware came from an external computer.	IP address
SourceMachineName	Name of the remote computer if the malware came from an external computer.	Character string
SourceUserName	User of the remote computer if the malware came from an external computer.	Character string
UrlList	List of accessed URLs if a browser exploit is detected.	Character string
DocList	List of accessed documents if a file exploit is detected.	Character string
Version	Content of the Version attribute of the process metadata.	Character string

Field	Description	Value
Vulnerable	Indicates if the application is vulnerable.	Boolean
MUID	Internal ID of the customer computer.	Character string
DriveType	Type of drive that contains the process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration

Severity/Sev Field Calculation

Depending on the value of the ExecutionStatus - Action field, the value of the Severity/Sev field varies according to this table:

ExecutionStatus - Action	Severity
■ Allow ■ AllowWL ■ AllowByUser ■ Informed ■ Unquarantine ■ Rename ■ BlockURL ■ BlockExploit ■ RebootNeeded ■ AllowSonGwInstaller ■ InformNewPE ■ SonMSIGW ■ RDPOff	8
■ Block ■ BlockBL ■ BlockTimeout ■ Delete ■ Disinfect ■ Quarantine ■ KillProcess ■ EmbebedBlocked ■ SuspendProcess ■ BlockedIp ■ RenameRegistry ■ AllowSWAutoriced	7
■ ExploitAllowByUser ■ ExploitInformed ■ EmbebedInformed ■ ModifyMarkFile ■ UncertainAction	10

ExecutionStatus - Action	Severity
■ ResponseLast ■ IsolateHost	
■ ModifyRegistry ■ AllowFGW	6
■ ExploitAllowByAdmin	5

Alerteae AccessEnforcement

Passive event that describes the parameters of the alert that WatchGuard Advanced EPDR creates when it detects a connection from a computer whose risk level is higher than the level defined by the network administrator.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date on the user computer when the event was generated.	Date
HostIp (CEF)	IP address of the workstation or server on which the event was generated.	IP address
sev (LEEF)	Indicates the status of the computer that tried to connect to the protected computer: ■ **0 (Unknown)**: Unable to determine status. ■ **1 (ProtectionEnabled)**: The computer protection software is enabled. ■ **2 (NonManaged)**: Unmanaged computer (no protection software installed or the software is from another vendor). ■ **3 (DifferentAccount)**: The computer has protection software installed but it is managed by an account other than the account that manages the protected computer. ■ **4 (ProtectionDisabled)**: The computer protection software is disabled. ■ **5 (RiskMedium)**: Medium risk level. ■ **6 (RiskHigh)**: High risk level. ■ **7 (RiskCritical)**: Extremely high risk level.	Numeric value
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat	Time stamp format.	“yyyy-MM-dd” character string

Field	Description	Value
(LEEF)		
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string
HostName	Name of the user computer where the event was generated.	Character string
ThreatType	Type of detected malware.	“AccEnforment ExecutionStatus” character string
ExecutionStatus	Action taken by the WatchGuard Endpoint Security agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator’s allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded “Allow ”. ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected.	Enumeration

Field	Description	Value
	■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file belonging to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key belonging to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key belonging to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file belonging to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file belonging to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the protection software is configured in Global Audit mode.	
DwellTimeSecs	Empty field.	
MWHash (LEEF) ItemHash (CEF)	Empty field.	
MWName (LEEF) ItemName (CEF)	Empty field.	
MWPath (LEEF) ItemPath (CEF)	Empty field.	
SourceIP	IP address of the protected computer that received the connection from a computer at risk.	IP address
SourceMachineName	Empty field.	
SourceUserName	Empty field.	
UrlList	Empty field.	
DocList	Empty field.	

Field	Description	Value
Version	Empty field.	
Vulnerable	Empty field.	
MUID	Internal ID of the customer computer.	Character string
DriveType	Type of drive that contains the process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration
AttackerDeviceId	Identifier of the computer that tried to connect to the protected computer.	Character string
SourcePort	Local port of the protected computer that received the connection from a computer at risk.	Numeric value
RemoteIp	IP address of the computer that tried to connect to the protected computer.	IP address
RemotePort	Local port of the computer that tried to connect to the protected computer.	Numeric value

Alertexploit Exploit Detected

Passive event that describes the parameters of an alert WatchGuard Endpoint Security created when it detects an attempt to exploit a vulnerability in a program installed on a computer on the network.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date of the user computer when the event was generated.	Date
HostIp (CEF)	IP address of the workstation or server on which the event was generated.	IP address
sev (LEEF)	Event severity.	9
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string
HostName	Name of the user computer that generated the event.	Character string
ThreatType	Type of malware detected.	“Exploit” character string
ExecutionStatus	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block**	Enumeration

Field	Description	Value
	■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands.	

Field	Description	Value
	■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file belonging to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key belonging to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key belonging to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file belonging to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file belonging to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache. ■ **AllowSWAuthorized**:Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	

Field	Description	Value
DwellTimeSecs	Time elapsed from the first time the threat was seen on the customer network.	Seconds
MWHash (LEEF) ItemHash (CEF)	Malware hash.	Character string
MWPath (LEEF) ItemPath (CEF)	Malware path.	Character string
MWName (LEEF) ItemName (CEF)	Name of the malware item if it is already cataloged as a threat.	Character string
SourceIP	IP address of the remote computer if the malware came from an external computer.	IP address
SourceMachineName	Name of the remote computer if the malware came from an external computer.	Character string
SourceUserName	User of the remote computer if the malware came from an external computer.	Character string
UrlList	List of accessed URLs if a browser exploit is detected.	Character string
DocList	List of accessed documents if a file exploit is detected.	Character string
Version	Content of the Version attribute of the process metadata.	Character string

Field	Description	Value
Vulnerable	Indicates if the application is vulnerable.	Boolean
MUID	Internal ID of the customer computer.	Character string
DriveType	Type of drive that contains the process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration

Alertmalware Malware Detected

Passive event that describes the parameters of the alert WatchGuard Endpoint Security creates when it detects an item classified as malware.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date on the user computer when the event was generated.	Date
HostIp (CEF)	IP of the workstation or server on which the event was generated.	IP address
sev (LEEF)	Event severity. See *Severity/Sev Field Calculation*.	Numeric value
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string
HostName	Name of the user computer where the event was generated.	Character string
ThreatType	Type of detected malware.	“Malware” character string
ExecutionStatus	Indicates whether or not the detected threat was run: ■ Executed ■ Not executed Action taken by the WatchGuard endpoint agent.	Enumeration - Enumeration

Field	Description	Value
	■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands.	

Field	Description	Value
	■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file belonging to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key belonging to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key belonging to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file belonging to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file belonging to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache. ■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
DwellTimeSecs	Time elapsed from the first time the threat was	Seconds

Field	Description	Value
	seen on the customer network.	
MWHash (LEEF) ItemHash (CEF)	Malware hash.	Character string
MWPath (LEEF) ItemPath (CEF)	Malware path.	Character string
MWName (LEEF) ItemName (CEF)	Name of the malware item if it is already cataloged as a threat.	Character string
SourceIP	IP address of the remote computer if the malware came from an external computer.	IP address
SourceMachineName	Name of the remote computer if the malware came from an external computer.	Character string
SourceUserName	User of the remote computer if the malware came from an external computer.	Character string
UrlList	List of accessed URLs if a browser exploit is detected.	Character string
DocList	List of accessed documents if a file exploit is detected.	Character string
Version	Content of the Version attribute of the process metadata.	Character string

Field	Description	Value
Vulnerable	Indicates if the application is vulnerable.	Boolean
MUID	Internal ID of the customer computer.	Character string
DriveType	Type of drive that contains the process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration

Severity/Sev Field Calculation

Depending on the value of the ExecutionStatus - Action field, the value of the Severity/Sev field varies according to this table:

ExecutionStatus - Action	Severity
■ Allow ■ AllowWL ■ AllowByUser ■ Informed ■ Unquarantine ■ Rename ■ BlockURL ■ BlockExploit ■ RebootNeeded ■ AllowSonGwInstaller ■ InformNewPE ■ SonMSIGW ■ RDPOff	8
■ Block ■ BlockBL ■ BlockTimeout ■ Delete ■ Disinfect ■ Quarantine ■ KillProcess ■ EmbebedBlocked ■ SuspendProcess ■ BlockedIp ■ RenameRegistry ■ AllowSWAutoriced	7
■ ExploitAllowByUser ■ ExploitInformed ■ EmbebedInformed ■ ModifyMarkFile ■ UncertainAction	10

ExecutionStatus - Action	Severity
■ ResponseLast ■ IsolateHost	
■ ModifyRegistry ■ AllowFGW	6
■ ExploitAllowByAdmin	5

Alertprodappcontrol ProdAppControl Detected

Passive event that describes the parameters of the alert WatchGuard Endpoint Security creates when it blocks items by name or the MD5 defined by the administrator in the **Program Blocking** settings.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date of the user computer when the event was generated.	Date
HostIp (CEF)	IP of the workstation or server on which the event was generated.	IP address
sev (LEEF)	Event severity.	9
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string
HostName	Name of the user computer that generated the event.	Character string
ThreatType	Type of malware detected .	“ProdAppControl” character string
ExecutionStatus	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time.	Enumeration

Field	Description	Value
	■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file belonging to the protection software.	

Field	Description	Value
	■ **ModifyRegistry**: The item attempted to modify a protected registry key belonging to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key belonging to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file belonging to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file belonging to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache. ■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
DwellTimeSecs	Time elapsed from the first time the threat was seen on the customer network.	Seconds
MWHash (LEEF) ItemHash (CEF)	Malware hash.	Character string
MWName (LEEF)	Name of the malware item if it is already cataloged as a threat.	Character string

Field	Description	Value
ItemName (CEF)		
MWPath (LEEF) ItemPath (CEF)	Malware path.	Character string
SourceIP	IP address of the remote computer if the malware came from an external computer.	IP address
SourceMachineName	Name of the remote computer if the malware came from an external computer.	Character string
SourceUserName	User of the remote computer if the malware came from an external computer.	Character string
UrlList	List of accessed URLs if a browser exploit is detected.	Character string
DocList	List of accessed documents if a file exploit is detected.	Character string
Version	Content of the Version attribute of the process metadata.	Character string

Field	Description	Value
Vulnerable	Indicates if the application is vulnerable.	Boolean
MUID	Internal ID of the customer computer.	Character string
DriveType	Type of drive that contains the process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration

Alertpup PUP Detected

Passive event that describes the parameters of the alert WatchGuard Endpoint Security creates when it detects an item classified as a Potentially Unwanted Program (PUP).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date of the user computer when the event was generated.	Date
HostIp (CEF)	IP address of the workstation or server on which the event was generated.	IP address
sev (LEEF)	Event severity. See *Severity/Sev Field Calculation*.	Numeric value
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string
HostName	Name of the user computer that generated the event.	Character string
ThreatType	Type of malware detected.	“PUP” character string
ExecutionStatus	Indicates whether or not the detected threat was run: ■ Executed ■ Not executed Action taken by the WatchGuard endpoint agent.	Enumeration - Enumeration

Field	Description	Value
	■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services.	

Field	Description	Value
	■ **ModifyDiskResource** The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache. ■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
DwellTimeSecs	Time elapsed from the first time the threat was seen on the customer network.	Seconds
MWHash (LEEF)	Malware hash.	Character string

Field	Description	Value
ItemHash (CEF)		
MWPath (LEEF) ItemPath (CEF)	Malware path.	Character string
MWName (LEEF) ItemName (CEF)	Name of the malware item if it is already cataloged as a threat.	Character string
SourceIP	IP address of the remote computer if the malware came from an external computer.	IP address
SourceMachineName	Name of the remote computer if the malware came from an external computer.	Character string
SourceUserName	User of the remote computer if the malware came from an external computer.	Character string
UrlList	List of accessed URLs if a browser exploit is detected.	Character string
DocList	List of accessed documents if a file exploit is detected.	Character string
Version	Content of the Version attribute of the process metadata.	Character string

Field	Description	Value
Vulnerable	Indicates if the application is vulnerable.	Boolean
MUID	Internal ID of the customer computer.	Character string
DriveType	Type of drive that contains the process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration

Severity/Sev Field Calculation

Depending on the value of the ExecutionStatus - Action field, the value of the Severity/Sev field varies according to this table:

ExecutionStatus - Action	Severity
■ Allow ■ AllowWL ■ AllowByUser ■ Informed ■ Unquarantine ■ Rename ■ BlockURL ■ BlockExploit ■ RebootNeeded ■ AllowSonGwInstaller ■ InformNewPE ■ SonMSIGW ■ RDPOff	6
■ Block ■ BlockBL ■ BlockTimeout ■ Delete ■ Disinfect ■ Quarantine ■ KillProcess ■ EmbebedBlocked ■ SuspendProcess ■ BlockedIp ■ RenameRegistry ■ AllowSWAutoriced	5
■ ExploitAllowByUser ■ ExploitInformed ■ EmbebedInformed ■ ModifyMarkFile ■ UncertainAction	8

ExecutionStatus - Action	Severity
■ ResponseLast ■ IsolateHost	
■ ModifyRegistry ■ AllowFGW	4
■ ExploitAllowByAdmin	3

Alertrdpattack RDPAttack Detected

Passive event generated to describe the parameters of the alert WatchGuard Endpoint Security creates when it detects a brute-force attack through RDP (Remote Desktop Protocol).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date of the user computer when the event was generated.	Date
HostIp (CEF)	IP address of the workstation or server on which the event was generated.	IP address
sev (LEEF)	Event severity.	9
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string
HostName	Name of the user computer that generated the event.	Character string
ThreatType	Type of attack detected.	“RDPAttack” character string
ExecutionStatus	Type of action taken.	“Blocked by IP” character string
DwellTimeSecs	Not used.	Seconds
MWHash (LEEF) ItemHash (CEF)	Not used.	

Field	Description	Value
MWName (LEEF) ItemName (CEF)	Name of the logged attack: ■ **Exploit/BruteForce_RDP**: Brute-force intrusion attempt using the RDP protocol. ■ **Exploit/RemoteDesktopIntrusion**: RDP intrusion detected.	Character string
MWPath (LEEF) ItemPath (CEF)	Name of the used attack.	“Malicious Network RDP Attack” character string
SourceIP	IP address of the attacking computer.	IP address
SourceMachineName	Name of the attacking computer.	Character string
SourceUserName	Name of the user account used in the attack.	Character string
UrlList	Not used.	Character string
DocList	Not used.	Character string
Version	Not used.	Character string

Field	Description	Value
Vulnerable	Not used.	Boolean
MUID	Internal ID of the customer computer.	Character string
DriveType	Type of drive that contains the process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration

Alertsecappcontrol SecAppControl Detected

Passive event that describes the parameters of the alert WatchGuard Advanced EPDR creates when it detects an item by the name or MD5 defined by the administrator in the Workstations and Servers settings (Advanced Protection > Advanced Security Policies > Block Programs).

This event is available only in WatchGuard Advanced EPDR.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date on the user computer when the event was generated.	Date
HostIp (CEF)	IP of the workstation or server on which the event was generated.	IP address
sev (LEEF)	Event severity.	9
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string
HostName	Name of the user computer where the event was generated.	Character string
ThreatType	Type of detected malware.	“SecAppControl” character string
ExecutionStatus	Action taken by the WatchGuard endpoint agent.	Enumeration -

Field	Description	Value
	■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands.	Enumeration

Field	Description	Value
	■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file belonging to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key belonging to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key belonging to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file belonging to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file belonging to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache. ■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
DwellTimeSecs	Time elapsed from the first time the threat was	Seconds

Field	Description	Value
	seen on the customer network.	
MWHash (LEEF) ItemHash (CEF)	Malware hash.	Character string
MWPath (LEEF) ItemPath (CEF)	Malware path.	Character string
MWName (LEEF) ItemName (CEF)	Name of the malware item if it is already cataloged as a threat.	Character string
SourceIP	IP address of the remote computer if the malware came from an external computer.	IP address
SourceMachineName	Name of the remote computer if the malware came from an external computer.	Character string
SourceUserName	User of the remote computer if the malware came from an external computer.	Character string
UrlList	List of accessed URLs if a browser exploit is detected.	Character string
DocList	List of accessed documents if a file exploit is detected.	Character string
Version	Content of the Version attribute of the process metadata.	Character string

Field	Description	Value
Vulnerable	Indicates if the application is vulnerable.	Boolean
MUID	Internal ID of the customer computer.	Character string
DriveType	Type of drive that contains the process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration

Alertvulnerabledriver VulnerableDriver Detected

Passive event that describes the parameters of the alert that WatchGuard Advanced EPDR creates when it detects or blocks a vulnerable driver from loading. A driver is considered vulnerable when it is from a legitimate vendor and works correctly, but has flaws that could be exploited by malware. Drivers that load as part of the operating system startup process are not detected.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date on the user computer when the event was generated.	Date
HostIp (CEF)	IP address of the workstation or server on which the event was generated.	IP address
sev (LEEF)	Event severity. ■ **ExecutionStatus = Block**: The driver was blocked from loading and the alert was resolved (sev=1). ■ **ExecutionStatus = AllowByConfig** : The driver was allowed to load and the alert was not resolved (sev 9).	Numeric value
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string
HostName	Name of the user computer where the event was generated.	Character string
ThreatType	Type of detection.	“VulnerableDriver” character string

Field	Description	Value
ExecutionStatus	Action taken by the WatchGuard Endpoint Security agent. ■ **Block**: The security software blocked the driver from loading. ■ **AllowByConfig**: The driver was allowed to load because of the security software configuration.	Enumeration
DwellTimeSecs	Time elapsed from the first time the driver was seen on the customer network.	Seconds
MWHash (LEEF) ItemHash (CEF)	Driver hash.	Character string
MWName (LEEF) ItemName (CEF)	Type of detection.	“BYOVD” character string
MWPath (LEEF) ItemPath (CEF)	Driver path.	Character string
SourceIP	IP address of the remote computer if the driver came from an external computer.	IP address
SourceMachineName	Name of the remote computer if the driver came from an external computer.	Character string
SourceUserName	User of the remote computer if the driver came from an external computer.	Character string
UrlList	List of accessed URLs at the time the driver load attempt was detected.	Character string
DocList	List of accessed documents at the time the driver load attempt was detected.	Character string
Version	Content of the Version attribute of the process metadata.	Character string

Field	Description	Value
Vulnerable	Indicates whether the application is vulnerable.	False
MUID	Internal ID of the customer computer.	Character string
Drivetype	Type of drive that contains the process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration

Block

Active event that describes the pop-up message WatchGuard Endpoint Security shows to the user when it blocks an executable file that has not yet been classified.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	8
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string

Field	Description	Value
HostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
LocalCat	Item category calculated by the WatchGuard endpoint agent: ■ **NotClassified**: File in the process of classification. ■ **Goodware** ■ **Malware** ■ **Suspect**: The file is in the process of classification and there is a high probability that it is malware. ■ **Compromised**: A process compromised by an exploit attack. ■ **GoodwareNotConfirmed**: A file that appears to be goodware but is pending classification. ■ **PUP** ■ **GoodwareUnwanted**: Equivalent to PUP. ■ **GoodwareRanked**: A process classified as goodware.	Enumeration
cloudAcces	Indicates whether the protection can access the cloud.	Boolean
DetId	Detection ID.	Numeric value
FirstSeen	Date when the file was first seen.	Date

Field	Description	Value
LastQueryDate	Date when the WatchGuard endpoint agent last queried the cloud.	Date
ToastBlockReason	Reason why the pop-up message was displayed on the workstation or server. **0**: Blocked because the file was unknown and the protection was in 'Lock' mode. **1**: Blocked by local rules. **2**: Blocked because the file came from an untrusted source. **3**: Blocked by context rule. **4**: Blocked because it is an exploit. **5**: The file was blocked after asking the user for permission to close the process.	Enumeration
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule. ■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy**	List

Field	Description	Value
	■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration
Hash	File hash or digest.	MD5
Path	Path of the item that triggered the logged action.	Character string (path)

Field	Description	Value
MUID	Internal ID of the customer computer.	Character string
DriveType	Type of drive that contains the process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration

Createcmp

Active event generated when a process creates a new compressed file (sub-process).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the user computer that triggered the event.	IP address
MachineName (CEF)	Name of the user computer that triggered the event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that triggered the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that triggered the event.	Character string
identHostName (LEEF)	Name of the user computer that triggered the event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “createcmp”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the logged operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupt or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DDLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the operation. ■ Goodware ■ Malware	Enumeration

Field	Description	Value
	■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process that performed the operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process. ■ Delphi	Enumeration

Field	Description	Value
	■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process that received the operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether or not vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string
OCS_Version	Version of the vulnerable software run.	Character string

Field	Description	Value
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped.	Enumeration - Enumeration

Field	Description	Value
	■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**:The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache. ■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings).	

Field	Description	Value
	■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the endpoint agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: Agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule. ■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files.	Enumeration

Field	Description	Value
	■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Createdir

Active event generated when a process (parent) creates a new directory (sub-process/child).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “Createdir”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean
ParentCompany	Content of the Company attribute of the parent	Character string

Field	Description	Value
	process metadata.	
ParentBroken	The parent process is corrupt or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware ■ PUP	Enumeration

Field	Description	Value
	■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process. ■ Delphi ■ DOTNET	Enumeration

Field	Description	Value
	■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether or not vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string
OCS_Version	Version of the vulnerable software run.	Character string
Params	Command-line execution parameters of the process run.	Character string

Field	Description	Value
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed.	Enumeration

Field	Description	Value
	■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache. ■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source.	

Field	Description	Value
	■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by ip**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule. ■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature.	Enumeration

Field	Description	Value
	■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

CreatePE

Active event generated when a process (parent) creates a new executable file (sub-process/child).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Timestamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “CreatePE”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupt or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware	Enumeration

Field	Description	Value
	■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure/type of the sub-process. ■ Delphi	Enumeration

Field	Description	Value
	■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the child file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string
OCS_Version	Version of the vulnerable software run.	Character string

Field	Description	Value
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped.	Enumeration

Field	Description	Value
	■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by ip**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule.	Enumeration

Field	Description	Value
	■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string

Field	Description	Value
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

CreateprocessbyWMI

Active event generated when a process (parent) creates a new sub-process through WMI.

Description of the Event Field

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “CreateprocessbyWMI”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string

Field	Description	Value
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware ■ PUP	Enumeration

Field	Description	Value
	■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process. ■ Delphi ■ DOTNET	Enumeration

Field	Description	Value
	■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the child file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string
OCS_Version	Version of the vulnerable software run.	Character string
Params	Command-line execution parameters of the process run.	Character string

Field	Description	Value
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped.	Enumeration

Field	Description	Value
	■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud.	Enumeration

Field	Description	Value
	■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule. ■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string

Createremotethread

Active event generated when a process (parent) creates a remote execution thread.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “Createremotethread”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string

Field	Description	Value
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the operation. ■ Goodware ■ Malware ■ PUP	Enumeration

Field	Description	Value
	■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process. ■ Delphi ■ DOTNET	Enumeration

Field	Description	Value
	■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string
OCS_Version	Version of the vulnerable software run.	Character string
Params	Command-line execution parameters of the process run.	Character string

Field	Description	Value
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped.	Enumeration

Field	Description	Value
	■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule.	Enumeration

Field	Description	Value
	■ **ContextMinerva**: Cloud-hosted context rule. ■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string

Field	Description	Value
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Criticalsoft

Passive event generated when a vulnerable application is executed.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
criticalSoftEventType	■ **True**: Vulnerable software ran on the computer. ■ **False**: Vulnerable software was seen on the computer but did not run.	Boolean
ItemHash	Hash or digest value of the threat or vulnerable program found.	Character string
Filename	Name of the vulnerable file.	Character string
filePath	Full path to the vulnerable file.	Character string
Size	Size of the vulnerable file.	Numeric value
InternalName	Content of the Name attribute of the vulnerable file metadata.	Numeric value
CompanyName	Content of the Company attribute of the vulnerable file metadata.	Character string

Field	Description	Value
FileVersion	Content of the Version attribute of the vulnerable file metadata.	Character string
ProductVersion	Content of the ProductVersion attribute of the vulnerable file metadata.	Character string
FilePlatform	Internal architecture of the vulnerable file. ■ Win32NT ■ Win64NT	Enumeration
MUID	Internal ID of the customer computer.	Character string

DeletePE

Active event generated when a process (parent) deletes an executable program (sub-process/child).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “DeletePE”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware	Enumeration

Field	Description	Value
	■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process. ■ Delphi	Enumeration

Field	Description	Value
	■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the child file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string
OCS_Version	Version of the vulnerable software run.	Character string

Field	Description	Value
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped.	Enumeration

Field	Description	Value
	■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule.	Enumeration

Field	Description	Value
	■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string

Field	Description	Value
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Deviceops

Active event generated when an operation is executed on an external device by a process.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date on the user computer when the event was generated.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	String
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string
HostName	Name of the user computer where the event was	Character string

Field	Description	Value
(LEEF)	generated.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the server and obtained by calculation. **2**: Real date provided by the server.
NotificationType	Type of action carried out. ■ **40067**: Device connected. ■ **40068**: Device disconnected correctly. ■ **40070**: Device disconnected without unmounting it first.	Enumeration
DeviceType	Type of drive where the process or file that triggered the operation resides. ■ **0**: Unknown ■ **1**: CD or DVD drive ■ **2**: USB storage device ■ **3**: Image file ■ **4**: Bluetooth device ■ **5**: Modem ■ **6**: USB printer ■ **7**: Smartphone ■ **8**: Keyboard ■ **9**: Keyboard and mouse ■ **10**: Mouse	Enumeration

Field	Description	Value
UniqueId	Unique ID of the device.	Character string
IsDenied	Indicates whether the reported action was denied.	Bolean
IdName	Device name.	Character string
ClassName	Type of device. This corresponds to the class specified in the .INF file associated with the device.	Boolean
FriendlyName	The device's user-readable name.	Character string
Description	Device description.	Character string
Manufacturer	Device manufacturer.	Character string
PhoneDescription	Phone description if the operation involved a device of this type.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Dnsops

Passive event generated with each DNS resolution request sent by a process.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date on the user computer when the event was generated.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	String
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string
HostName	Name of the user computer where the event was	Character string

Field	Description	Value
(LEEF)	generated.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the server and obtained by calculation. **2**: Real date provided by the server.
ProcessCount	Number of processes on the computer with DNS resolution failures in the last hour.	Numeric value
ProcessMD5	MD5 hash of the process with DNS resolution failures.	Numeric value
ProcessPid	ID of the process with DNS resolution failures.	Numeric value
ProcessPath	Path of the process with DNS resolution failures.	Character string
FailedQueries	Number of failed DNS resolution requests sent by the process in the last hour.	Numeric value
QueriedDomainCount	Number of different domains sent by the process for which there was a DNS resolution failure in the last hour.	Numeric value
DomainList	List of domains sent by the process to the DNS server for resolution and number of resolutions per domain.	{domain_ name,number#domain_ name,number}

Field	Description	Value
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Exec

Active event generated when a process (parent) executes a new sub-process (child).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “Exec”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware	Enumeration

Field	Description	Value
	■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process. ■ Delphi	Enumeration

Field	Description	Value
	■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string
OCS_Version	Version of the vulnerable software run.	Character string

Field	Description	Value
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User's response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped.	Enumeration

Field	Description	Value
	■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule.	Enumeration

Field	Description	Value
	■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string

Field	Description	Value
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

HeuHooks

Active event generated when we analyze the function of an intercepted DLL and conclude that it could be involved in the execution of an attack on the computer. Depending on the settings of the anti-exploit module included in the security product installed on the protected computer, the operation is blocked or reported to the user.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName	Name of the workstation that triggered the logged event.	Character string

Field	Description	Value
(LEEF)		
HostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “DeletePE”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value

Field	Description	Value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation.	Enumeration

Field	Description	Value
	■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process.	Enumeration

Field	Description	Value
	■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the child file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string

Field	Description	Value
OCS_Version	Version of the vulnerable software run.	Character string
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped.	Enumeration

Field	Description	Value
	■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule.	Enumeration

Field	Description	Value
	■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string

Hostfiles

Active event generated when a process (parent) detects the modification of the HOSTS file.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
HostName	Name of the workstation that triggered the logged event.	Character string
Hash	File hash or digest.	Character string
Drivetype	Type of drive where the process or file that triggered the operation resides. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
Path	Path of the item that triggered the logged action.	Character string
ValidSig	Digitally signed process.	Boolean
Company	Content of the Company attribute of the process metadata.	Character string

Field	Description	Value
Broken	The file is corrupted or damaged.	Character string
imageType	Internal architecture of the process. ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ExeType	Internal structure or type of process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
Prevalence	Historical prevalence of the process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
PrevLastDay	Previous-day prevalence of the process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
Cat	Category of the file that performed the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown	Enumeration

Field	Description	Value
	■ Monitoring	
MWName	Name of the malware item if it is already cataloged as a threat.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Install

Passive event generated when the WatchGuard Endpoint Security software is installed.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Operation	Type of action carried out: ■ Install ■ Uninstall	Enumeration
Result	Result of the operation: ■ OK ■ Not ok	Enumeration
OSVersion	Version of the operating system installed on the user computer.	Character string
OSServicePack	Service Pack of the operating system installed on the user computer.	Character string
OSPlatform	Platform of the operating system installed on the user computer. ■ WIN32 ■ WIN64	Enumeration
MachineIP0	IP address of the workstation or server that generated the event.	IP address
MUID	Internal ID of the customer computer.	Character string

Loadlib

Active event generated when a process (parent) loads a library (sub-process/child).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “Loadlib”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware	Enumeration

Field	Description	Value
	■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process. ■ Delphi	Enumeration

Field	Description	Value
	■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string
OCS_Version	Version of the vulnerable software run.	Character string

Field	Description	Value
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped.	Enumeration

Field	Description	Value
	■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**:The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule.	Enumeration

Field	Description	Value
	■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string

Field	Description	Value
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

LoadDrvVulnerable

Passive event that is generated when a process (parent) tries to load a driver (child) with known vulnerabilities from a legitimate vendor.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the computer that triggered the logged event.	IP address
MachineName (CEF)	Name of the computer that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the computer that generated the event.	Character string
identSrc (LEEF)	IP address of the computer that generated the event.	Character string
identHostName (LEEF)	Name of the computer that triggered the logged event.	Character string

Field	Description	Value
HostName (LEEF)	Name of the computer that triggered the logged event.	Character string
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “LoadDrvVulnerable”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the logged operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupt or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the operation. ■ Goodware	Enumeration

Field	Description	Value
	■ Malware ■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process.	Enumeration

Field	Description	Value
	■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process that received the operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether or not vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string

Field	Description	Value
OCS_Version	Version of the vulnerable software run.	Character string
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User response to the pop-up message shown by WatchGuard. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard Endpoint Security agent. ■ **Block**: The driver was blocked from loading because of the security software configuration. ■ **AllowByConfig**: The driver was allowed to load because of the security software configuration.	Enumeration
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	Enumeration
WinningTech	Technology that triggered the event.	“VulnerableDriver” character string
DetId	Detection ID.	Character string

Field	Description	Value
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, the security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated event**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Loginoutops

Active event generated when a login attempt is detected on the device.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date on the user computer when the event was generated.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	String
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string
HostName	Name of the user computer where the event was	Character string

Field	Description	Value
(LEEF)	generated.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	0: Real date not supported as it is an old event. 1: Real date not available to the server and obtained by calculation. 2: Real date provided by the server.
ActionType	■ **0**: Login ■ **1**: Logout.	Enumeration
Session Type	Login type: ■ **2**: Session created physically through a keyboard or via KVM over IP. ■ **3**: Session created remotely in shared folders or printers. This login type uses secure authentication. ■ **4**: Session created by the Windows task scheduler. ■ **5**: Session created when a service that needs to run in the user session is launched. The session is deleted when the service stops. ■ **7**: Session created when a user tries to join a previously created session that has been blocked. ■ **8**: Same as type 3 but the password is sent in plain text. ■ **9**: Session created when the “RunAs” command is used under an account other than the account used to log in, and the “/netonly” parameter is specified. If the “/netonly” parameter is not specified, a type 2 session is created.	Numeric value

Field	Description	Value
	■ **10**: Session created when accessing through “Terminal Service”, “Remote Desktop”, or “Remote Assistance”. It identifies a remote user connection. ■ **11**: User session created with domain credentials cached on the machine, but with no connection to the domain controller.	
ErrorCode	■ **0xC0000064**: The user name does not exist. ■ **0XC000005E**: The server required to validate the login is not available. ■ **0xC000006A**: The user name is correct, but the password is incorrect. ■ **0XC000006D**: The user name or the authentication information is wrong. ■ **0XC000006E**: Unknown name or wrong password. ■ **0xC0000234**: Access blocked. ■ **0xC0000072**: Account disabled. ■ **0xC000006F**: Login attempt outside authorized hours. ■ **0xC0000070**: Login attempt from an unauthorized computer. ■ **0xC00000DC**: An error occurred on the validation server. Cannot perform operation. ■ **0xC0000193**: Account expired. ■ **0xC0000071**: Password expired. ■ **0xC0000133**: Connected computer clocks too far out of sync. ■ **0xC0000224**: User must change their password on next boot. ■ **0xC0000225**: A bug in Windows and not a risk. ■ **0xc000018c**: The login request failed because the trust relationship between the primary domain and the trusted domain failed.	Hexadecimal number

Field	Description	Value
	■ **0XC0000192**: An attempt was made to log in, but the Netlogon service was not started. ■ **0XC00002EE**: An error occurred during login. ■ **0XC0000413**: The machine the user is logging in to is protected by an authentication firewall. The specified account is not allowed to authenticate to the machine. ■ **0xc000015b**: The user has not been granted the requested login type.	
User	Domain or user with which the session was created.	Character string
Interactive	Indicates whether the login is an interactive login.	Boolean
RemoteMachineName	If the event is a remote login, it indicates the name of the remote computer.	Character string
RemoteIP	If the event is a remote login, it indicates the IP address of the remote computer.	IP address
RemotePort	If the event is a remote login, it indicates the port of the remote computer.	Numeric value

Field	Description	Value
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Modifype

Active event generated when a process (parent) modifies an executable program (child).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “Modifype”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware	Enumeration

Field	Description	Value
	■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process. ■ Delphi	Enumeration

Field	Description	Value
	■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string
OCS_Version	Version of the vulnerable software run.	Character string

Field	Description	Value
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped.	Enumeration

Field	Description	Value
	■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule.	Enumeration

Field	Description	Value
	■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string

Field	Description	Value
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

ModLinuxCfg

Active event generated when a modification of a Linux OS configuration file is detected.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “ModLinuxCfg”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware	Enumeration

Field	Description	Value
	■ Malware ■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process.	Enumeration

Field	Description	Value
	■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string

Field	Description	Value
OCS_Version	Version of the vulnerable software run.	Character string
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The file was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked.	Enumeration

Field	Description	Value
	■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule.	Enumeration

Field	Description	Value
	■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string

ModOSXCfg

Active event generated when a modification of a macOS configuration file is detected.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “ModOSXCfg”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware	Enumeration

Field	Description	Value
	■ Malware ■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process.	Enumeration

Field	Description	Value
	■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string

Field	Description	Value
OCS_Version	Version of the vulnerable software run.	Character string
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The useraccepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked.	Enumeration

Field	Description	Value
	■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**:Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule.	Enumeration

Field	Description	Value
	■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack that uses the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string

Monitoredopen

Active event generated when a process (parent) accesses a data file (sub-process/child).

In order to preserve the privacy of customer data, the Childpath field contains only the extension of accessed files. To display the path and full name of those files, see the WatchGuard Endpoint Security online help (https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Endpoint-Security/_intro/wes_front.html).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src	IP address of the workstation or server that generated the event.	Character string

Field	Description	Value
(LEEF)		
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
ParentPid	Identifier of the parent process.	Numeric value
ParentHash	Hash of the parent process.	Character string
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64	Enumeration

Field	Description	Value
	■ DLLx32 ■ DLLx64	
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildPath	Path of the child file that received the logged	Character string

Field	Description	Value
	operation.	
LoggedUser	Logged-in user at the time the event was generated.	Character string
ConfigString	This indicates the version of the set of rules active when the event was logged. It is used for diagnostic tasks by WatchGuard technical support.	“Mx” (M0, M1, M2, etc.) character string.
ParentAttibutes	Parent process attribute flags. ■ **0x0000**: Integrity level of the process: Untrusted. ■ **0x1000**: Integrity level of the process: Low integrity. ■ **0x2000**: Integrity level of the process: Medium integrity. ■ **0x3000**: Integrity level of the process: High integrity. ■ **0x4000**: Integrity level of the process: System integrity. ■ **0x5000**: Integrity level of the process: Protected. ■ **0x00000100**: Cumulative event. ■ **0x00000200**: Indicates if the process was created locally or remotely. ■ **0x00000400**: Indicates that the operation occurred before the service started.	Numeric value
ChildAttributes	Sub-process attribute flags. ■ **0x0000**: Integrity level of the process: Untrusted. ■ **0x1000**: Integrity level of the process: Low integrity. ■ **0x2000**: Integrity level of the process: Medium integrity. ■ **0x3000**: Integrity level of the process: High integrity. ■ **0x4000**: Integrity level of the process: System integrity.	Numeric value

Field	Description	Value
	■ **0x5000**: Integrity level of the process: Protected. ■ **0x00000100**: Cumulative event. ■ **0x00000200**: Indicates if the process was created locally or remotely. ■ **0x00000400**: Indicates that the operation occurred before the service started.	
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Monitoredregistry

Active event generated when a process (parent) accesses the registry of a user computer to read a branch.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
ParentPid	Identifier of the parent process.	Numeric value
ParentHash	Hash of the parent process.	Character string
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC	Enumeration

Field	Description	Value
	■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
RegAction	Type of operation performed on the computer registry. ■ CreateKey ■ CreateValue ■ ModifyValue	Enumeration
Key	Affected registry branch or key.	Character string

Field	Description	Value
Value	Name of the affected value under the registry key.	Character string
ValueData	Content of the registry key value.	Character string
LoggedUser	Logged-in user at the time the event was generated.	Character string
ConfigString	This indicates the version of the set of rules active when the event was logged. It is used for diagnostic tasks by WatchGuard technical support.	“Mx” (M0, M1, M2, etc.) character string.
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	▪ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ▪ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ▪ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Notblocked

Active event generated for each action that WatchGuard Endpoint Security does not scan because of an exceptional situation (while the service is starting, settings changes, etc.).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName	Name of the workstation that	Character string

Field	Description	Value
(LEEF)	triggered the logged event.	
HostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
ParentHash	Parent file digest or hash.	Character string
ParentPath	Parent process path.	Character string
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi	Enumeration

Field	Description	Value
	■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)

Field	Description	Value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium	Enumeration

Field	Description	Value
	■ Low	
ChildCat	Category of the child file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ResponseCat	File category assigned by the local technologies implemented in the protection software. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
NumCacheClassifiedElements	Number of identifiers cached on the user's computer at the time the event was generated.	Numeric value
MUID	Internal ID of the customer computer.	Character string

Opencmp

Active event generated when a process (parent) opens a compressed file (sub-process or child).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “Opencmp”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process: ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware	Enumeration

Field	Description	Value
	■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process. ■ Delphi	Enumeration

Field	Description	Value
	■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the child file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string
OCS_Version	Version of the vulnerable software run.	Character string

Field	Description	Value
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped.	Enumeration

Field	Description	Value
	■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule.	Enumeration

Field	Description	Value
	■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string

Field	Description	Value
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Openlsass

Active event generated when a process (parent) accesses the LSASS process to compromise user credentials.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “OpenIsass”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware	Enumeration

Field	Description	Value
	■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether or not the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process. ■ Delphi	Enumeration

Field	Description	Value
	■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether or not vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string
OCS_Version	Version of the vulnerable software run.	Character string

Field	Description	Value
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow ". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped.	Enumeration

Field	Description	Value
	■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule.	Enumeration

Field	Description	Value
	■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack that uses the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string

Field	Description	Value
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

ProcessNetBytes

Active event generated when a process consumes network data. An event is sent for each process approximately every four hours with the amount of data transferred since the last time the event was sent. The total amount of bytes sent and received for each process is the sum of all data logged.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName	Name of the workstation that triggered the logged event.	Character string

Field	Description	Value
(LEEF)		
HostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Hash	File hash or digest.	Character string
Path	Path of the item that triggered the logged action.	Character string
PID	Process ID.	Numeric value
BytesSent	Number of bytes sent by the process since the last ProcessNetBytes event was generated.	Numeric value
BytesReceived	Number of bytes received by the process since the last ProcessNetBytes event was generated.	Numeric value
MUID	Internal ID of the customer computer.	Character string

Registryc

Active event generated when a process (parent) creates a registry branch that points to an executable file (sub-process/child).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string

Field	Description	Value
HostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
op	Logged operation.	CreateExeKey
Hash	Hash of the parent process.	Character string
Drivetype	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
Path	Path of the parent file that performed the logged operation.	Character string
ValidSig	Indicates whether the parent process is digitally signed.	Boolean
Company	Content of the Company attribute of the parent process metadata.	Character string

Field	Description	Value
Broken	The parent process is corrupted or damaged.	Boolean
ImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
Prevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
PrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
Cat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown	Enumeration

Field	Description	Value
	■ Monitoring	
MWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
TargetPath	Path of the executable that the registry key points to.	Character string
Regkey	Registry key.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Registrym

Active event generated when a process (parent) modifies a registry branch that points to an executable file (sub-process child).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string

Field	Description	Value
HostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “ModifyExeKey”
Hash	Hash of the parent process.	Character string
Drivetype	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
Path	Path of the parent file that performed the logged operation.	Character string
ValidSig	Indicates whether the parent process is digitally signed.	Boolean
Company	Content of the Company attribute of the parent	Character string

Field	Description	Value
	process metadata.	
Broken	The parent process is corrupted or damaged.	Boolean
imageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
Prevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
PrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
Cat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware ■ PUP	Enumeration

Field	Description	Value
	■ Unknown ■ Monitoring	
MWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	*Character string*
TargetPath	Path of the executable that the registry key points to.	Character string
Regkey	Registry key.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Renamepe

Active event generated when a process (parent) changes the name of an executable program (sub-process/child).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “Renamepe”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware	Enumeration

Field	Description	Value
	■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process. ■ Delphi	Enumeration

Field	Description	Value
	■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string
OCS_Version	Version of the vulnerable software run.	Character string

Field	Description	Value
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked. ■ **KillProcess**: The process was stopped.	Enumeration

Field	Description	Value
	■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule.	Enumeration

Field	Description	Value
	■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack that uses the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string

Field	Description	Value
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Scriptcreation

Active event generated when a process (parent) creates a script-type process (sub-process/child).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “scriptcreation”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentFlags	Flags used internally by the service.	Character string
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware	Enumeration

Field	Description	Value
	■ Malware ■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string
ChildFlags	Flags used internally by the service.	Character string
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process.	Enumeration

Field	Description	Value
	■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware.	Enumeration

Field	Description	Value
	■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Scriptlaunch

Active event generated when a process (parent) launches a script-type process (sub-process/child).

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Op	Logged operation.	Character string: “scriptlaunch”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentFlags	Flags used internally by the service.	Character string
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean

Field	Description	Value
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware	Enumeration

Field	Description	Value
	■ Malware ■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string
ChildFlags	Flags used internally by the service.	Character string
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process.	Enumeration

Field	Description	Value
	■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on the WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware.	Enumeration

Field	Description	Value
	■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all running processes.	
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Socket

Active event generated when a process (parent) opens a socket.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
Protocol	Communications protocol used by the process. ■ TCP ■ UDP ■ RDP	Enumeration
Localport	Local port of the process.	Numeric value
Direction	Network connection direction. ■ Up ■ Down ■ Both	Enumeration
LocalIP	Local IP address of the process.	IP address
Hash	File hash or digest.	Character string
DriveType	Type of drive where the process or file that triggered the operation resides. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device.	Enumeration

Field	Description	Value
	■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	
Path	Path of the item that triggered the logged action.	Character string
Hostname	Name of the remote computer that started the connection.	Character string
IP	Destination IP address of the communication.	IP address
Port	Communications port used by the process.	Numeric value
Times	Number of times the same communication event occurred in the last hour. For two communication events to be considered the same, these parameters and the communication direction must be the same: ■ The process name. ■ The local IP address of the process. ■ The process path. ■ The target IP address of the communication. ■ The target port of the communication. The first time a communication is detected, an event is sent with the times field set to 1. For each hour that passes after the first event, the times field indicates the number of equal communication events that have occurred in the time span minus 1, along with the date of the last event logged.	Numeric value
Pid	Process ID.	Numeric value
ValidSig	Indicates whether the parent process is digitally signed.	Boolean
Company	Content of the Company attribute of the parent process metadata.	Character string
Broken	The parent process is corrupted or damaged.	Character string
imageType	Internal architecture of the process.	Enumeration

Field	Description	Value
	■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	
ExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
Prevalence	Historical prevalence of the process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
PrevLastDay	Previous-day prevalence of the process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
Cat	Category of the file that performed the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
MWName	Name of the malware item if it is already cataloged as a threat.	Character string

Field	Description	Value
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	▪ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ▪ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ▪ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

SvcControl

Event that corresponds to an attempt to modify files of the security product installed.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
HostName	Name of the workstation that triggered the logged event.	Character string
Op	Logged operation.	Character string: “Loadlib”
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentPID	Parent process ID.	Numeric value

Field	Description	Value
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation.	Enumeration

Field	Description	Value
	■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)
ChildPID	Sub-process ID.	Numeric value
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process.	Enumeration

Field	Description	Value
	■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
OCS_Exec	Indicates whether vulnerable software was run on the computer.	Boolean
OCS_Name	Name of the vulnerable software run.	Character string

Field	Description	Value
OCS_Version	Version of the vulnerable software run.	Character string
Params	Command-line execution parameters of the process run.	Character string
ToastResult	User response to the pop-up message shown by WatchGuard Endpoint Security. ■ **OK**: The user accepted the message. ■ **Timeout**: The pop-up message closed as the user did not respond. ■ **Angry**: The user chose not to block the item from the pop-up message. ■ **Block** ■ **Allow**	Enumeration
Action	Action taken by the WatchGuard endpoint agent. ■ **Allow** ■ **Block** ■ **BlockTimeout**: A pop-up message was shown to the user but they did not respond in time. ■ **AllowWL**: The item was allowed because it was on the administrator's allowlist. ■ **Disinfect** ■ **Delete** ■ **Quarantine** ■ **AllowByUser**: A pop-up message was shown to the user and they responded "Allow". ■ **Informed**: A pop-up message was shown to the user. ■ **Unquarantine**: The item was removed from quarantine. ■ **Rename**: The item was renamed because it could not be moved to quarantine, deleted, or disinfected. ■ **BlockURL**: Access to a URL was blocked.	Enumeration

Field	Description	Value
	■ **KillProcess**: The process was stopped. ■ **BlockExploit**: An attempt to exploit a vulnerable process was stopped. ■ **ExploitAllowByUser**: The user prevented the exploited process from being closed. ■ **RebootNeeded**: The computer must be rebooted to block the exploit attempt. ■ **ExploitInformed**: A pop-up message was shown to the user to inform them of an attempt to exploit a vulnerable process. ■ **AllowSonGWInstaller**: The program is part of an installation package classified as goodware. ■ **EmbebedInformed**: The item is a PowerShell script that executes commands. ■ **SuspedProcess**: The item attempted to suspend one of the protection software services. ■ **ModifyDiskResource**: The item attempted to modify a protected file that belongs to the protection software. ■ **ModifyRegistry**: The item attempted to modify a protected registry key that belongs to the protection software. ■ **RenameRegistry**: The item attempted to rename a protected registry key that belongs to the protection software. ■ **ModifyMarkFile**: The item attempted to rename a protected file that belongs to the protection software. ■ **UncertainAction**: The item attempted to launch an undefined action on a file that belongs to the protection software. ■ **AllowGWFilter**: Execution of the item is allowed because it is in the goodware cache.	

Field	Description	Value
	■ **AllowSWAuthoriced**: Execution of the item is allowed because it is authorized by the administrator (Authorized software settings). ■ **NewPE**: Appearance of a new executable program on the computer from an external source. ■ **AllowedByAdmin**: Execution of the item is allowed because the exploit technique has been excluded by the administrator. ■ **Blocked by IP**: The source IP address was blocked because a brute-force RDP attack was detected. ■ **AllowSonMsiGW**: Execution of the item is allowed because it is an executable from a trusted installation package. ■ **Allowed by Global Audit**: The item is allowed because the security software is configured in Global Audit mode.	
ServiceLevel	Execution mode of the agent. ■ **Blocking**: Agent blocks all unclassified executables and items classified as malware. ■ **Hardening**: Agent blocks all unclassified programs coming from an untrusted source, and items classified as malware. ■ **Learning**: Agent does not block any items but monitors all run processes.	Enumeration
WinningTech	Technology that triggered the event. ■ **Blockmode**: The agent was in Lock mode when the item was blocked. ■ **Cache**: Locally cached classification. ■ **Cloud**: Classification downloaded from the cloud. ■ **Context**: Local context rule. ■ **ContextMinerva**: Cloud-hosted context rule.	Enumeration

Field	Description	Value
	■ **Digital Signature**: Digitally signed file. ■ **Exploit**: Technology that identifies attempts to exploit vulnerable processes. ■ **ExploitLegacy** ■ **GWFilter**: Technology that identifies unknown goodware files. ■ **LegacyUser**: The user was asked about the action to take. ■ **Local Signature**: Local signature. ■ **MetaEsploit**: Attack created with the Metasploit framework. ■ **NetNative**: Binary type. ■ **Serializer**: Binary type. ■ **User**: The user was asked about the action to take. ■ **RDP**: Brute-force attack using the RDP protocol. ■ **AMSI**: Detection made by the Antimalware Scan Interface.	
DetId	Detection ID.	Character string
MUID	Internal ID of the customer computer.	Character string

Systemops

Active event generated on detecting the execution of actions that affect or modify operating system processes or files through the WMI (Windows Management Interface) system.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Date on the user computer when the event was generated.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	String
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the user computer that generated the event.	Character string

Field	Description	Value
HostName (LEEF)	Name of the user computer where the event was generated.	Character string
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the server and obtained by calculation. **2**: Real date provided by the server.
Client	Identifier used to differentiate the events received from each of the partner's customers. This field is only used in the product Panda SIEMFeeder for Partners.	Numeric value
HostName	Name of the workstation that triggered the logged event.	Character string
Type	■ **0 (WMI_COMMAND_LINE_EVENT_ CREATION)**: Event generated every time a "CommandLineEventConsumer" is created. This is a command line ran by WMI when an event is logged in the database. ■ **1 (WMI_ACTIVE_SCRIPT_EVENT_ CREATION)**: A query was created to run a script. ■ **2 (CREATE_WMI_EVENT_ CONSUMER_TO_FILTER_ CONSUMER)**: A query will be run to run a process, a JS/VBS file, or a JS/VBS script embedded in the database (with no file on disk). ■ **3 (CREATE_WMI_EVENT_ CONSUMER_TO_FILTER_QUERY)**: A filter was logged which is a query.	Enumeration

Field	Description	Value
	■ **4 (WMI_EVENT_CREATE_USER)**: A user account was created. ■ **5 (WMI_EVENT_DELETE_USER)**: A user account was deleted. ■ **6 (WMI_EVENT_ADD_USER_GROUP)**: A user account was added to a user group. ■ **7 (WMI_EVENT_DELETE_USER_ GROUP)**: A user account was deleted from a user group. ■ **8 (WMI_EVENT_USER_GROUP_ ADMIN)**: A user was added to an administrator group. ■ **9 (WMI_EVENT_USER_GROUP_RDP)**: A user was added to a group of users with RDP access to the device. ■ **10 (WMI_EVENT_CREATE_SERVICE)**: A new service was installed on the system. ■ **11 (WMI_EVENT_USER_ACCOUNT_ CHANGED**: A user account was modified. ■ **12 (WMI_EVENT_USER_PASSWORD_ RESET_ATTEMPT)**: An attempt was made to delete a user account password. ■ **13 WMI_QUERY**: A query was made to the computer WMI system. The **CommandLine** field shows the query. ■ **14 WMI_LOGIN_ATTEMP**: The computer tried to log in to another computer. ■ **15 WMI_SCHEDULER_TASKS**: The computer performed an operation with the Task Scheduler. ■ **16 WMI_LOGIN_SPECIAL_ PRIVILEGES**: A process escalated privileges. ■ **17 NOTIFICATION_ID_ INTERCEPTION_AMSI_BUFFER_ SCAN_REQUEST**: A command tried to run a script. The solution logs the command as well as whether malware was detected or not.	

Field	Description	Value
ObjectName	Unique name of the object within the WMI hierarchy.	Character string
CommandLine	Command line configured as a task to be run through WMI.	Character string
MachineName	Name of the computer that ran the process.	Character string
User	User under which the task was launched.	Character string
IsLocal	Indicates if the task was created locally or remotely.	Boolean
ExtendedInfo	Extended information, dependent on the operation.	Character string
ChildMD5	File hash (when applicable).	Character string
ParentPid	Parent process PID.	Numeric value
RemoteMachineName	Name of the remote computer that generated the event.	Character string
RemoteIP	Remote IP address that generated the event.	Character string
SessionInteractive	Indicates whether the session is interactive.	Boolean

Field	Description	Value
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration

Thalert

Passive event. It describes the indicators generated by these detection technologies:

- **IOCs (Indicators of Compromise)**: Implemented in Orion. These are rules created by customers to find indicators of compromised computers on the managed network.
- **IOAs (Indicators of Attack)**: Implemented in WatchGuard Endpoint Security and mapped to the MITRE ATT&CK Framework. These are rules to find indicators of attacks received on the managed network.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Timestamp indicating when the event was generated on the user's computer.	Date
MachineIP (CEF)	IP of the workstation or server on which the event was generated.	IP address
MachineName (CEF)	Name of the user computer that triggered the event	Character string
sev (LEEF)	Event severity. See *Severity/Sev Field Calculation*.	Numeric value
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	"yyyy-MM-dd" character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	IP address
identSrc (LEEF)	IP address of the workstation or server that generated the event.	IP address
identHostName (LEEF)	Name of the user computer that generated the event.	Character string

Field	Description	Value
AlertDate	Date the indicator was created on the platform.	Date
THRuleName	Name of the hunting rule that generated the indicator.	Character string
Mitre	MITRE technique and tactic associated with the hunting rule that generated the indicator.	List of Technique/Tactic pairs
Severity	Indicator severity. The lower the number, the more severe the indicator.	Numeric value
TimeStamp	Timestamp of the action detected on the customer's computer that generated the indicator.	Date
EvidenceData	Relevant data related to the indicator and dependent on the enabled hunting rule. Contains multiple space-separated fields in the format "FieldName: value".	Character string
LastHourEvidenceCount	Number of times the same indicator has occurred on the customer's computer in the last hour.	Numeric value
MUID	Internal ID of the customer's computer.	Character string
Times	Number of occurrences of the IOA. See *Grouping of Alerts*.	Numérico

Severity/Sev Field Calculation

Depending on the value of the ExecutionStatus - Action field, the value of the Severity/Sev field varies according to this table:

ExecutionStatus - Action	Severity
■ Allow ■ AllowWL ■ AllowByUser ■ Informed ■ Unquarantine ■ Rename ■ BlockURL ■ BlockExploit ■ RebootNeeded ■ AllowSonGwInstaller ■ InformNewPE ■ SonMSIGW ■ RDPOff	8
■ Block ■ BlockBL ■ BlockTimeout ■ Delete ■ Disinfect ■ Quarantine ■ KillProcess ■ EmbebedBlocked ■ SuspendProcess ■ BlockedIp ■ RenameRegistry ■ AllowSWAutoriced	7
■ ExploitAllowByUser ■ ExploitInformed ■ EmbebedInformed ■ ModifyMarkFile ■ UncertainAction	10

ExecutionStatus - Action	Severity
■ ResponseLast ■ IsolateHost	
■ ModifyRegistry ■ AllowFGW	6
■ ExploitAllowByAdmin	5

Grouping of Alerts

To minimize bandwidth usage and prevent saturation of the IT infrastructure that manages and stores events on the customer network, SIEMFeeder implements an algorithm that groups together alerts with similar characteristics.

For two or more alerts to be considered the same, they must meet all these conditions:

- They must be of the same type.
- They must have been logged close to each other in time.
- They must have been logged on the same workstation or server.

Grouping of WatchGuard Endpoint Security advanced IOAs

Advanced IOAs are not grouped if the computer is in Audit mode. Each IOA received from a computer in Audit mode has the Times field set to 1. For more information, see the guide of your WatchGuard Endpoint Security security product.

- The first IOA logged generates a THAlert alert with the Times field set to 1.
- All equal IOAs detected every 6 hours since the first IOA was logged are grouped together. A THAlert alert is sent at the end of each 6-hour interval. The Times field specifies the total number of IOAs logged so far.
- If no equal IOAs are logged within a 6-hour interval, no THAlert alert is sent for the interval.
- After 4 intervals (24 hours), the process starts again.

Grouping of WatchGuard Endpoint Security IOAs

- The first IOA logged generates a THAlert alert with the Times field set to 1.
- All equal IOAs detected every hour since the first IOA was logged are grouped together. A THAlert alert is sent at the end of each 1-hour interval. The Times field specifies the total number of IOAs logged so far.

- If no equal IOAs are logged within a 1-hour interval, no THAlert alert is sent for the interval.
- After 24 hours, the process starts again.

Grouping of IOCs in Orion retrospective searches

IOCs are loaded onto the platform through the Orion API. For more information, see the product guide.

These searches examine, only once, the flow of events generated by the customer computers over the last year since an IOC is imported. A single alert is generated for each computer/IOC pair found.

Grouping of IOCs in Orion real-time searches

IOCs are loaded onto the platform through the Orion API. For more information, see the product guide.

These searches examine, in real time, the information generated by processes running on the customer computers. A single alert is generated for each computer/IOC pair every hour.

Grouping of Orion indicators

- The first indicator logged generates a THAlert alert with the Times field set to 1.
- All equal indicators detected every hour since the first indicator was logged are grouped together. A THAlert alert is sent at the end of each 1-hour interval. The Times field specifies the total number of indicators logged so far.
- If no equal indicators are logged within a 1-hour interval, no THAlert alert is sent for the interval.
- After 24 hours, the process starts again.

Urldownload

Active event generated when a process downloads or requests the download of a data file via HTTP.

Description of the Event Fields

Field	Description	Value
Date (CEF)	Time stamp that indicates when the event was generated on the user computer.	Date
User (CEF)	Name and domain of the user account used to run the process that generated the event.	Character string
MachineIP (CEF)	IP address of the workstation that triggered the logged event.	IP address
MachineName (CEF)	Name of the workstation that triggered the logged event.	Character string
sev (LEEF)	Event severity.	1
devTime (LEEF)	Time stamp that indicates when the event was generated on the user computer.	Date
devTimeFormat (LEEF)	Time stamp format.	“yyyy-MM-dd” character string
usrName (LEEF)	User account used by the process that performed the operation.	Character string
domain (LEEF)	Domain of the user account used by the process that performed the operation.	Character string
src (LEEF)	IP address of the workstation or server that generated the event.	Character string
identSrc (LEEF)	IP address of the workstation or server that generated the event.	Character string
identHostName (LEEF)	Name of the workstation that triggered the logged event.	Character string
HostName	Name of the workstation that triggered the	Character string

Field	Description	Value
(LEEF)	logged event.	
LocalDateTime	The computer date (in UTC format) at the time the event occurred. This date depends on the computer settings and, consequently, it could be incorrect.	Date
PandaTimeStatus	Contents of the DateTime, Date, and LocalDateTime fields.	**0**: Real date not supported as it is an old event. **1**: Real date not available to the WatchGuard server and obtained by calculation. **2**: Real date provided by the WatchGuard server.
ParentHash	Hash of the parent process.	Character string
ParentDriveType	Type of drive that contains the parent process or file that triggered the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ParentPath	Path of the parent file that performed the logged operation.	Character string
ParentValidSig	Indicates whether the parent process is digitally signed.	Boolean
ParentCompany	Content of the Company attribute of the parent process metadata.	Character string
ParentBroken	The parent process is corrupted or damaged.	Boolean

Field	Description	Value
ParentImageType	Internal architecture of the parent process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ParentExeType	Internal structure or type of the parent process. ■ Delphi ■ DOTNET ■ VisualC ■ VB ■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	Enumeration
ParentPrevalence	Historical prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentPrevLastDay	Previous-day prevalence of the parent process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ParentCat	Category of the parent file that performed the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration

Field	Description	Value
ParentMWName	Name of the malware detected in the parent process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
URL	Download URL launched by the process that generated the logged event.	Character string
ChildHash	Hash of the sub-process.	Character string
ChildDriveType	Type of drive that contains the sub-process or file that received the operation. ■ **Fixed**: Non-removable drive such as an internal hard disk. ■ **Remote**: Network drive. ■ **Removable**: Removable drive such as a pen drive or floppy disk. ■ **Unknown**: Unknown type of device. ■ **NoRootDir**: A device that is not available in the path displayed. ■ **Cdrom**: CD-ROM drive. ■ **Ramdisk**: RAM disk drive.	Enumeration
ChildPath	Path of the sub-process file that received the logged operation.	Character string (path)
ChildValidSig	Indicates whether the sub-process is digitally signed.	Boolean
ChildCompany	Content of the Company attribute of the sub-process metadata.	Character string
ChildBroken	The sub-process is corrupt or damaged.	Boolean
ChildImageType	Internal architecture of the sub-process: ■ EXEx32 ■ EXEx64 ■ DLLx32 ■ DLLx64	Enumeration
ChildExeType	Internal structure or type of the sub-process. ■ Delphi ■ DOTNET ■ VisualC ■ VB	Enumeration

Field	Description	Value
	■ CBuilder ■ Mingw ■ Mssetup ■ Setupfactory ■ Lcc32 ■ Vc7setupproject ■ Unknown	
ChildPrevalence	Historical prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildPrevLastDay	Previous-day prevalence of the sub-process on WatchGuard systems. ■ High ■ Medium ■ Low	Enumeration
ChildCat	Category of the sub-process file that received the logged operation. ■ Goodware ■ Malware ■ PUP ■ Unknown ■ Monitoring	Enumeration
ChildMWName	Name of the malware detected in the sub-process if it is already classified as a threat. If the value is Null, the item is not malware.	Character string
ParentPid	PID of the parent process that downloaded the file.	Numeric value

Field	Description	Value
MUID	Internal ID of the customer computer.	Character string
TTPs	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
IOAIds	When a sequence of events follows a pattern described in the MITRE matrix, The security software creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
TelemetryType	■ **0: Normal telemetry**. The event does not belong to an indicator that follows a pattern described in the MITRE matrix. ■ **1: Resent event**. The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and TTPs fields completed. ■ **2: Accumulated events**. To save resources, part of the telemetry generated for the user computer is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.	Enumeration