# Threat Detection and Response Exam Guide

The Threat Detection and Response exam tests your knowledge of how to configure and manage the Threat Detection and Response (TDR) subscription service.

## Exam Overview

### Key Concepts

To successfully complete the Threat Detection and Response Exam, you must understand these key TDR concepts:

- TDR initial account creation and user roles
- Cybercon levels
- Indicators and Incidents
- Threat scores
- Signature overrides
- TDR Policies
- Host Sensor settings
- Host Sensor installation and licensing
- Host Sensor events and actions
- Configure TDR on a Firebox

## Exam Description

***Content***

40 multiple choice (select one option), multiple selection (select more than one option), and true or false questions

***Passing score***

75% correct

***Time limit***

Two hours

***Reference material***

You cannot reference printed or online materials during the exam.

***Test environment***

This is a proctored exam, with two location testing options:

- Kryterion testing center
- Online, with virtual proctoring through an approved webcam

***Prerequisites***

None

# Prepare for the Exam

WatchGuard provides reference materials to help you prepare for the Threat Detection and Response exam. In addition to the reference materials described in the subsequent sections, before you take this exam, we strongly recommend that you set up Threat Detection and Response with a Firebox and at least one Host Sensor.

## Self-Study Materials

WatchGuard offers courseware that you can use for self-study. We recommend that you review all available courseware before you take the exam. Courseware is available on the **Technical Training** tab in the WatchGuard Portal (login required).

***Threat Detection and Response Courseware***

The *Threat Detection and Response* courseware (.PPT file) is available online for self-study and review.

## Other Resources

***Online Help***

*Fireware Help* is available online and includes detailed information that expands on the principles presented in the *Threat Detection and Response* courseware.

For detailed information about the knowledge categories included in the *Assessment Objectives* section, we recommend that you review the related content in the Threat Detection and Response section of Fireware Help on the WatchGuard website.

***Video Tutorials***

Fireware Video Tutorials include information about specific subjects to help you learn more about some areas of Threat Detection and Response and Fireware OS. You can use these videos to help you expand your understanding of Fireware, as it relates to the knowledge categories specified in the *Assessment Objectives* section.

You can find the Video Tutorials on the WatchGuard website documentation pages:

- Recommended Video Tutorial — Getting Started with TDR
- All Video Tutorials — Video Tutorials

# Assessment Objectives

The Threat Detection and Response Exam evaluates your knowledge of the categories in the subsequent list. For each knowledge category assessed in this exam, the *Weight* column includes the approximate percentage of exam questions from that knowledge category. Because some exam questions require skills or knowledge from more than one category, the weights do not exactly correspond to the percentage of exam questions.

| Category | Skills / Knowledge | Weight |
|---|---|---|
| TDR Initial Setup / General | | 20 |
| | TDR account setup | |
| | TDR user roles | |
| | CYBERCON level | |
| | Backup and Import | |
| Incidents, Indicators, and Actions | | 25 |
| | Incidents and indicators | |
| | Threat scores | |
| | Signature overrides | |
| | Machine guided actions | |
| | Quarantine action | |
| TDR Policies | | 15 |
| | Policy thresholds | |
| | Policy actions | |
| | Policy rank | |
| TDR Host Sensor | | 20 |
| | Host Sensor event reporting | |
| | Host Sensor actions | |
| | Host Ransomware Prevention (HRP) | |
| | Host Sensor installation and removal | |
| | Host Sensor settings | |
| TDR on a Firebox | | 15 |
| | Enable TDR on a Firebox | |
| | Network events and correlation | |
| | Configure security services to send TDR events | |
| | Firewall policies for TDR | |

# Example Exam Questions

The exam includes multiple choice, multiple selection, and true or false questions. The subsequent examples show the types of questions to expect on the exam. Answers to each question appear on the last page of this guide.

## Questions

1. Indicators are rescored if they are successfully remediated or added to the Whitelist. (Select one.)
    a. True
    b. False
2. What happens when a Host Sensor license expires? (Select three.)
    a. Host Sensors that were installed earliest expire first
    b. Expired Host Sensors cannot take action on an endpoint
    c. Expired Host Sensors cannot report threats after the expiration date
    d. The Host Sensor is automatically uninstalled 7 days after expiration
3. For what amount of time do indicators remain in your TDR account? (Select one.)
    a. 30 days
    b. 60 days
    c. 90 days
    d. Forever
4. How does the behavior of a Host Sensor change after you add an exclusion for files in a specific path? (Select one.)
    a. The Host Sensor continues to monitor files in the specified path, but excludes those files from any action configured in a policy.
    b. The Host Sensor automatically assigns any events for files in the specified path a Threat Score of 1.
    c. The Host Sensor does not monitor the files in the specified path.
    d. The Host Sensor does not warn the end-user of changes to files in the specified path.
5. All network events sent by a Firebox to TDR are scored as network incidents. (Select one.)
    a. True
    b. False

## Answers

1. a (True). The score for a remediated indicator is 1.
2. a, b, d. Expired host sensors continue to report threats for 7 days after expiration.
3. b. TDR indicators remain in your account for 60 days.
4. c. An exclusion causes the Host Sensor to completely ignore the specified path
5. b (False). Network events are not scored as incidents unless a Host Sensor is installed on the endpoint.

# Register for the Exam

To schedule an exam, you must create a Kryterion user account.

1. Log in to the WatchGuard website with your WatchGuard account credentials.
2. Select the **Technical Training** tab.
3. At the right side of the page, click **Register for an exam**.
   *This opens a WatchGuard-branded Kryterion web page*.
4. At the top-right corner of the page, click the link to create a new Kryterion user account, or log in with an existing Kryterion user account for WatchGuard exams.
5. Click **Schedule an Exam**.

For more information about the certification process, see this FAQ.