

□

IBM Security QRadar Incident Forensics Configuration and Usage Information

<b>Length:</b>	2.0 Days
<b>Ref:</b>	BQ161G-X
<b>Delivery method:</b>	ClassroomInstructor Led OnlineSelf-paced Virtual Training
<b>Price:</b>	EUR

Overview

In this course, QRadar SIEM administrators learn how to integrate and configure QRadar Incident Forensics in an existing QRadar SIEM deployment. End users such as Security Analysts learn how to use the QRadar Incident Forensics tools to effectively perform network forensics.

If you are enrolling in a Self Paced Virtual Classroom or Web Based Training course, before you enroll, please review the Self-Paced Virtual Classes and Web-Based Training Classes on our Terms and Conditions page, as well as the system requirements, to ensure that your system meets the minimum requirements for this course. <http://www.ibm.com/training/terms>

Public

This intermediate course is for:

- QRadar SIEM administrators
- QRadar SIEM Security Analysts

Prerequisites

You should have:

- Working experience with QRadar SIEM.
- Knowledge of how to navigate through the QRadar SIEM pagesand using the mouse click options is mandatory.

Objective

- Learn how to integrate and configure QRadar Incident Forensics
- Learn how to use the QRadar Incident Forensics tools

## Topics

- Explanation of network forensics and the functions and aspects of IBM Security QRadar Incident Forensics 7.2.4
- Integration of IBM Security QRadar Incident Forensics 7.2.4 in IBM Security QRadar SIEM 7.2.4
- Administration of IBM Security QRadar Incident Forensics 7.2.4; creating cases, managing users, and configuring the Incident Forensics server.
- Using the concepts and terminology of IBM Security QRadar Incident Forensics 7.2.4
- Using IBM Security QRadar Incident Forensics 7.2.4 to analyze a network forensic case using the IBM Security QRadar Incident Forensics 7.2.4 Forensic search page and tools.

□