IBM QRADAR SIEM FOUNDATIONS

Course Code: 7021

Learn how QRadar collects data to detect suspicious activities and how to perform many QRadar SIEM tasks.

IBM QRadar SIEM provides deep visibility into network, user, and application activity. It provides collection, normalization, correlation, and secure storage of events, flows, asset profiles, and vulnerabilities. QRadar SIEM classifies suspected attacks and policy violations as offenses.

What You'll Learn

After completing this course, you should be able to perform the following tasks:

• Describe how QRadar SIEM collects data to detect suspicious activities
• Describe the QRadar SIEM component architecture and data flows
• Navigate the user interface
• Investigate suspected attacks and policy violations
• Search, filter, group, and analyze security data
• Investigate events and flows
• Investigate asset profiles
• Describe the purpose of the network hierarchy
• Determine how rules test incoming data and create offenses
• Use index and aggregated data management
• Navigate and customize dashboards and dashboard items
• Create customized reports
• Use filters
• Use AQL for advanced searches
• Analyze a real world scenario

Who Needs to Attend

This course is designed for security analysts, security technical architects, offense managers, network administrators, and system administrators using QRadar SIEM.

Prerequisites

Before taking this course, make sure that you have the following skills:

• IT infrastructure
• IT security fundamentals
• Linux
• Windows
• TCP/IP networking
• Syslog
IBM QRADAR SIEM FOUNDATIONS
Course Code: 7021

| CLASSROOM LIVE | $2,385 USD | 3 days |
IBM QRADAR SIEM FOUNDATIONS
Course Code: 7021

VIRTUAL CLASSROOM LIVE $2,385 USD 3 days

Virtual Classroom Live Outline
- Unit 1: Introduction to IBM QRadar
- Unit 2: IBM QRadar SIEM component architecture and data flows
- Unit 3: Using the QRadar SIEM User Interface
- Unit 4: Investigating an Offense Triggered by Events
- Unit 5: Investigating the Events of an Offense
- Unit 6: Using Asset Profiles to Investigate Offenses
- Unit 7: Investigating an Offense Triggered by Flows
- Unit 8: Using Rules
- Unit 9: Using the Network Hierarchy
- Unit 10: Index and Aggregated Data Management
- Unit 11: Using the QRadar SIEM Dashboard
- Unit 12: Creating Reports
- Unit 13: Using Filters
- Unit 14: Using the Ariel Query Language (AQL) for Advanced Searches
- Unit 15: Analyzing a Real-World Large-Scale Attack
- Appendix A: A real-world scenario introduction to IBM QRadar SIEM
- Appendix B: IBM QRadar architecture

Virtual Classroom Live Labs
Extensive lab exercises are provided to allow students an insight into the routine work of an IT Security Analyst operating the IBM QRadar SIEM platform. Extensive lab exercises are provided to allow students an insight into the routine work of an IT Security Analyst operating the IBM QRadar SIEM platform.

Mar 23 - 25, 2020 | 9:00 AM - 5:00 PM EST
Apr 13 - 15, 2020 | 9:00 AM - 5:00 PM EST
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 4 - 6, 2020</td>
<td>9:00 AM - 5:00 PM EST</td>
<td></td>
</tr>
<tr>
<td>Jun 15 - 17, 2020</td>
<td>9:00 AM - 5:00 PM EST</td>
<td></td>
</tr>
<tr>
<td>Jul 6 - 8, 2020</td>
<td>9:00 AM - 5:00 PM EST</td>
<td></td>
</tr>
<tr>
<td>Jul 27 - 29, 2020</td>
<td>9:00 AM - 5:00 PM EST</td>
<td></td>
</tr>
<tr>
<td>Aug 17 - 19, 2020</td>
<td>9:00 AM - 5:00 PM EST</td>
<td></td>
</tr>
<tr>
<td>Sep 28 - 30, 2020</td>
<td>9:00 AM - 5:00 PM EST</td>
<td></td>
</tr>
<tr>
<td>Oct 19 - 21, 2020</td>
<td>9:00 AM - 5:00 PM EST</td>
<td></td>
</tr>
</tbody>
</table>
IBM QRADAR SIEM FOUNDATIONS
Course Code: 7021

PRIVATE GROUP TRAINING  3 days

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 2/26/2020 2:40:06 PM
Copyright © 2020 Global Knowledge Training LLC. All Rights Reserved.