IBM Skills Academy

Security Intelligence Engineer

(Classroom)

Career path description

The Security Intelligence Engineer career path prepares students to consolidate event logs from device endpoints within a network to identify threats. This will require skills in security intelligence such as data security, event offenses, asset profile offenses and event rules. The Security Intelligence Engineer will use tools to investigate offenses that are generated from network logs and create rules that will prevent them from happening further.

ibm.com/training

General information

Delivery method

100% Instructor-led training

Version

2018

Product

IBM QRadar SIEM

Audience

Undergraduate senior students from IT related academic programs i.e. computer science, software engineering, information systems and similar others

Learning objectives

After completing this course, you should be able to:

- Identify enterprise business and IT drivers that influence the overall IT Security Architecture
- Define the role of a centralized Security Intelligence solution and how it integrates with other IT enterprise security components
- Explain how a Security Intelligence solution can be used to investigate and stop advanced threats and address IT governance and regulatory compliance
- Describe how QRadar SIEM collects data to detect suspicious activities
- Navigate and customize the QRadar SIEM dashboard
- Investigate suspected attacks and policy breaches
- Search, filter, group, and analyze security data
- Investigate the vulnerabilities and services of assets
- Locate custom rules and inspect actions and responses of rules
- Use QRadar SIEM to create customized reports
- Use charts and apply advanced filters to examine specific activities in your environment

Prerequisites Skills

- Basic understanding of the security fundamentals
- Basic understanding of the IT infrastructure and IT security fundamentals
- Basic understanding of Linux, Windows, TCP/IP networking and Syslog
- Exposure to the IBM Skills Academy Portal learning environment
- Exposure to the IBM Skills Academy Cloud hands-on labs platform

Duration

31 hours

Skill level

Basic – Intermediate

Hardware requirements

Classroom (ILT) setup requirements	
Processor	5 processor core
GB RAM	13 GB
GB free disk space	60 GB
Network requirements	Yes
Other requirements	IBM ID

Notes

The following unit and exercise durations are estimates, and might not reflect every class experience. If the course is customized or abbreviated, the duration of unchanged units will probably increase.

Course Agenda

MODULE I – Cyber Security Overview

Course I – Security Intelligence Fundamentals

Duration: 5.2 hours

Course introduction Duration: 10 minutes

Unit 1. The status quo of IT Security Duration: 2 hours

Overview	This unit introduces current technology trends and explains what to IT security landscape is.
Learning objectives	After completing this unit, you should be able to: • Identify latest technology trends and the IT security landscape • Explain the business and IT drivers that influence security-related business decisions • Define a comprehensive security solution portfolio to address the holistic IT security requirements in an organization

Unit 2. Security intelligence and operations
Duration: 3 hours

Overview	This unit describes how an organization can use a centralized security intelligence solution to improve their overall security maturity by integrating capabilities from all security domains.
Learning objectives	After completing this unit, you should be able to: • Illustrate the integration between security intelligence and other IT security domains • Describe how security intelligence can help detect and stop threats • Describe how security intelligence can help address organizational and regulatory compliance • Describe how a security intelligence solution can be integrated into an overall enterprise security architecture

MODULE II – Cyber Security Foundations

Course I – Security Intelligence Fundamentals

Duration: 6 hours

Unit 3. Designing a security intelligence solution
Duration: 2 hours and 15 minutes

Overview	This unit introduces a design methodology that covers all steps from information gathering to specifying the required maintenance on the solution
Learning objectives	After completing this unit, you should be able to: • Explain and discuss the high level steps needed to design and implement a security intelligence solution • Describe the detailed activities needed to design and implement a security intelligence solution

Unit 4. Security intelligence functional components
Duration: 2 hours and 15 minutes

Overview	This unit will explain the security intelligence solution and its functional architecture.
Learning objectives	After completing this unit, you should be able to: • Explain how to build a foundation through centralized security intelligence management • Explain the principles of designing and deploying a centralized and well-integrated security intelligence solution • Examine how data and information is exchanged within the system • Explain external threat intelligence feeds

Exercise 1. Obtain the necessary documents to create a micro design for Windows Duration: 30 minutes	
Overview	In this exercise, you will learn how to start a micro design for Windows
Learning objectives	After completing this exercise, you should be able to: • Start a micro design for Windows

Exercise 2. Create re-useable list of audit controls Duration: 30 minutes	
Overview	In this exercise, you will create a re-useable list of audit controls.
Learning objectives	After completing this unit, you should be able to: • Create a re-useable list of audit controls

Exercise 3. Use the common criteria security target document Duration: 30 minutes	
Overview	In this exercise, you will use the common criteria security target document
Learning objectives	After completing this exercise, you should be able to: • Use the common criteria security target document

MODULE III – SECURITY INTELLIGENCE ENGINEER

Course I– IBM QRadar SIEM Foundations

Duration: 19.7 hours

Course introduction Duration: 10 minutes

Unit 1. Introduction to IBM QRadar Duration: 30 minutes	
Overview	In this unit, you will learn about QRadar, and its ecosystem.
Learning objectives	• Describe why we need Security Intelligence and a security immune • system • Describe the QRadar ecosystem

Unit 2. IBM QRadar SIEM component architecture and data flows
Duration: 30 minutes

Overview	In this unit, you will learn about QRadar, and the EM component architecture.
Learning objectives	After completing this unit, you should be able to: • Describe QRadar functional architecture and deployment models • Describe QRadar SI • EM component architecture

Unit 3. Using the QRadar SIEM User Interface
Duration: 30 minutes

Overview	In this unit you will learn about the QRadar SIEM User Interface
Learning objectives	After completing this unit, you should be able to: • Leverage the QRadar SIEM user interface

Exercise 1. Sending sample data to QRadar
Duration: 30 minutes

Overview	The exercise you will learn how to send sample data to QRadar
Learning objectives	After completing this exercise, you should be able to: • Send sample data to QRadar

Exercise 2. Discover the User Interface
Duration: 30 minutes

Overview	In this exercise, you will discover the User Interface.
Learning objectives	After completing this exercise, you should be able to: • Understand the QRadar user interface

Unit 4. Investigating an offense that is triggered by events
Duration: 1 hour and 5 minutes

Overview	This unit teaches you how to investigate the information that is contained in an offense and response to an offense

Learning objectives	After completing this unit, you should be able to:
	• Explain the concept of offenses
	• Investigate an offense, which includes this information
	  ○ Summary information
	  ○ The details of an offense
	• Respond to an offense

Exercise 1. Investigating the local DNS scanner offense
Duration: 30 minutes

Overview	To investigate an offense triggered by events, this exercise looks at the offense named Local DNS Scanner containing invalid DNS
Learning objectives	After completing this exercise, you should be able to: • Identify the Offenses tab in Security Intelligence Solution SIEM • Identify the offense type and offense source and magnitude • Identify the number of events associated with the offense • List the event categories that contributed to this offense • Protect the offense and explain why

Unit 5. Investigating the events of an offense
Duration: 1 hour and 20 minutes

Overview	This unit teaches you how to find, filter, and group events in order to gain critical insights about the offense.
Learning objectives	After completing this unit, you should be able to: • Use the list of events to navigate event details • Filter events included in an offense • Group events to gain different perspectives • Save a search that monitors a suspicious host • Modify a saved search

Exercise 1. Looking for events that contribute to an offense
Duration: 30 minutes

Overview	In this exercise, you use the log events that are viewed in the Log Activity tab to further analyze the offense.
Learning objectives	After completing this exercise, you should be able to: • Find the Local DNS Scanner containing invalid DNS offense • Show the low-level categories of the offense's events • Investigate the events associated with the offense • Create a filter to exclude the source IP that contributed to the Local DNS Scanner offense • Explain what do the results indicate • Look for similar DNS requests unrelated to the offense

Exercise 2. Saving search criteria and search results
Duration: 30 minutes

Overview	In this exercise you will learn to create and edit a search that monitors the events of suspicious hosts.
Learning objectives	After completing this exercise, you should be able to: • Configure and verify the Save Criteria window and settings • Save the current search criteria • Revisit or delete your saved search results

Exercise 3. Investigating event details
Duration: 20 minutes

Overview	In this exercise you will learn to investigate the details of an event. The details of an event, particularly its payload, can provide further insights.
Learning objectives	After completing this exercise, you should be able to: • Find and run your saved search • Verify whether the log message that is displayed in the payload is a concern

Unit 6. Using asset profiles to investigate offenses
Duration: 30 minutes

Overview	This unit teaches you how asset profiles are created and updated, and how to use them as a part of an offense investigation
Learning objectives	After completing this unit, you should be able to: • Describe the purpose of an asset profile • Investigate asset profile details • Navigate the assets tab

Unit 7. Investigating an offense that is triggered by flows
Duration: 1 hour

Overview	This unit teaches you how to investigate the flows that contribute to an offense. You also learn how to create and tune false positives and investigate superflows.
Learning objectives	After completing this unit, you should be able to: • Find and group flows on the Network Activity tab • Investigate the summary of an offense that is triggered by flows • Investigate flow details • Tune false positives • Investigate superflows

Exercise 1. Investigating an offense that is triggered by flows
Duration: 1 hour

Overview	In this exercise you will learn to investigate an offense that is triggered by flows
Learning objectives	After completing this exercise, you should be able to: • Generate network traffic • Observe the network events and verify that a network event triggers an offense • Identify the offense name, type and source • Investigate flows related to the offense

Unit 8. Using rules
Duration: 35 minutes

Overview	This unit teaches you the significance of rules and building blocks, and how to locate and understand their tests, actions and responses.
Learning objectives	After completing this unit, you should be able to: • Navigate rules and rule groups • Locate the rules that fired for an event or flow, and triggered an offense • Investigate which test conditions caused a rule to fire • Investigate building blocks and function tests • Examine rule actions and responses • Use rules in searches • Examine for which indicators anomaly detection rules can fire

Exercise 1. Creating an event rule
Duration: 10 minutes

Overview	In this exercise you will learn how to configure Security Intelligence Solution SIEM
Learning objectives	After completing this exercise, you should be able to: • Create an event rule to create offenses for login activity • Use a reference set to identify a class of objects

Exercise 2. Analyzing the rule that contributed to the Local DNS Scanner offense
Duration: 10 minutes

Overview	In this exercise you will analyze the rule that contributed to the Local DNS Scanner offense
Learning objectives	After completing this exercise, you should be able to: • Review the Local DNS Scanner containing Invalid DNS • Describe the behavior that caused this rule to trigger • Explain how to change the rule behavior so that this source IP does not create an offense

Exercise 3. Working with rule parameters
Duration: 10 minutes

Overview	In this exercise you will learn to work with rule parameters
Learning objectives	After completing this exercise, you should be able to: • Sort the Offense Count parameter is descending order • Identify what rule created most offenses • Identify how many events or flows are associated with a rule

Exercise 4. Deleting changes that are made to a rule
Duration: 10 minutes

Overview	In this exercise you will learn two different methods to delete changes that are made to a rule
Learning objectives	After completing this exercise, you should be able to: • Tune the Firewall Deny event as a false positive • Remove a testable object • Remove a limited number of rule changes • Revert a rule to the system default

Exercise 5. Searching for a rule
Duration: 10 minutes

Overview	In this exercise, you will learn to find a rule or building block that included in other rules.
Learning objectives	After completing this exercise, you should be able to: • Select Rules from the display list • Clear the Group filter • Search Rules

Unit 9. Using the Network Hierarchy
Duration: 1 hour

Overview	This unit teaches you the significance of the Network Hierarchy and the many ways that QRadar SIEM uses and displays its information.
Learning objectives	After completing this unit, you should be able to: • Locate and explain the structure of the Network Hierarchy • Use networks in investigations • Use Flow Bias and Direction in investigations • Use the Network Hierarchy in rules

Exercise 1. Create a network object
Duration: 15 minutes

Overview	In this exercise you will create a network object.
Learning objectives	After completing this exercise, you should be able to: • Create a network object

Exercise 2. View network object in flows
Duration: 15 minutes

Overview	In this exercise you will learn how to view network object in flows.
Learning objectives	After completing this exercise, you should be able to: • View network object in flows

Unit 10. Index and Aggregated Data Management
Duration: 30 minutes

Overview	This unit teaches you about indexes and aggregated data.
Learning objectives	After completing this unit, you should be able to: • Use the Index Management administration tool to enable, disable, and configure an index • Use the Aggregated Data Management administration tool to see Aggregated Data View statistics and manage the data that QRadar SIEM accumulates • Use the information provided by the Aggregated Data Management tool in combination with Index Management to optimize search and rule performance

Exercise 1. Manage indexes
Duration: 15 minutes

Overview	In this exercise you will create a network object.
Learning objectives	After completing this exercise, you should be able to: • Manage indexes

Unit 11. Using Dashboards
Duration: 30 minutes

Overview	This unit teaches you how to navigate and customize the Dashboard tab.
Learning objectives	After completing this unit, you should be able to: • Navigate the Dashboard tab • Customize dashboard items • Utilize time-series charts

Exercise 1. Create a new dashboard
Duration: 15 minutes

Overview	In this exercise you will create a new dashboard.
Learning objectives	After completing this exercise, you should be able to: • Create a dashboard

Unit 12. Creating Reports
Duration: 30 minutes

Overview	This unit teaches you how to generate a report using a predefined template and create a report template.
Learning objectives	After completing this unit, you should be able to: • Navigate and use the Reports tab • Generate and view a report • Use the Report Wizard to create a custom report template

Exercise 1. Viewing an existing report
Duration: 15 minutes

Overview	In this exercise you will create an existing report.
Learning objectives	After completing this exercise, you should be able to: • Create an existing report

Exercise 2. Creating a new event report
Duration: 15 minutes

Overview	In this exercise you will create a new event report.
Learning objectives	After completing this exercise, you should be able to: • Create a new event report

Exercise 3. Creating a new search and report
Duration: 15 minutes

Overview	In this exercise you will create a new search and report.
Learning objectives	After completing this exercise, you should be able to: • Create a new search and report

Unit 13. Using Filters
Duration: 30 minutes

Overview	Filters limit a search result to the data that meets the conditions of the applied filters. Use filters to look for specific activities or to view your environment from various angles. This unit teaches you about some of the many available filters.
Learning objectives	After completing this unit, you should be able to: • Apply filters that include or exclude specific events and flows

Unit 14. Using the Ariel Query Language (AQL) for Advanced Searches
Duration: 30 minutes

Overview	Ariel Query Language (AQL) queries can retrieve stored data more flexibly than interactively built searches. This unit teaches you how to build use AQL.
Learning objectives	After completing this unit, you should be able to: • Describe the basics of AQL • Build AQL queries in advanced searches

Exercise 1. Sending Windows events to QRadar SIEM
Duration: 15 minutes

Overview	In this exercise you will send windows events to QRadar SIEM.
Learning objectives	After completing this exercise, you should be able to: • Send Windows events to QRadar SIEM

Exercise 2. Using the Select statement
Duration: 15 minutes

Overview	In this exercise you will use the Select statement
Learning objectives	After completing this exercise, you should be able to: • Use the select statement

Exercise 3. Using clauses to narrow a search
Duration: 15 minutes

Overview	In this exercise you will use clauses to narrow a search
Learning objectives	After completing this exercise, you should be able to: • Use clauses to narrow a search

Exercise 4. Use functions and operators
Duration: 15 minutes

Overview	In this exercise you will use functions and operators
Learning objectives	After completing this exercise, you should be able to: • Use functions and operators

Exercise 5. Ready for a challenge?
Duration: 15 minutes

Overview	In this exercise you will write some AQL queries to solve problems.
Learning objectives	After completing this exercise, you should be able to: • Write some AQL queries to solve problems

Unit 15. Analyzing a Real-World Large-Scale Attack
Duration: 30 minutes

Overview	This unit evaluates a large-scale advanced persistent attack against a US retailer. You will evaluate how a properly implemented Security Intelligence solution could have helped to fend off the attackers.
Learning objectives	After completing this unit, you should be able to: • Analyze the provided attack scenario • Discuss in your team how a proper centralized Security Intelligence approach could have avoided this nightmare scenario

Exercise 1. Investigate the Target kill chain timeline
Duration: 30 minutes

Overview	In this exercise, you investigate the Target breach to find potential improvements that could have avoided the nightmare scenario.
Learning objectives	After completing this exercise, you should be able to: • Investigate target breach properly

Exercise 2. Suggest improvements
Duration: 30 minutes

Overview	In this exercise, you will need to suggest improvements for the scenarios presented.
Learning objectives	After completing this exercise, you should be able to: • Analyze situations and suggest solutions to improve them

Appendix A. A real-world scenario introduction to IBM QRadar SIEM Duration: 30 minutes	
Overview	In this appendix you can study a real world attack scenario to explain how to instigate a successful attack, how an infected computer spreads a malicious code, how the overall timeline works for bad guys, and how this type of an attack can only be mitigated by correlation and collaboration inside an organization.
Learning objectives	After completing this unit, you should be able to: • Investigate the anatomy of an attack

Appendix B. A real-world scenario introduction to IBM QRadar SIEM Duration: 30 minutes	
Overview	In this appendix, we start at the functional architecture level and explain how IBM QRadar was designed as a modular Security Intelligence solution from the ground up. After taking a look at this modular design, its extensibility and deployment pattern, we closely examine the component architecture so that the analyst understands how data is ingested and processed. When the analysts later examine bits and pieces of a larger security incident investigation, this architectural understanding can substantially enhance their capability for detailed and fast analysis.
Learning objectives	After completing this unit, you should be able to: • Describe QRadar functional architecture and deployment models • Describe QRadar SIEM component architecture

IBM Official Badges and Associated Job Roles	
IBM Official Badges	Security Intelligence Engineer 2018: Explorer I Mastery Award
Associated Job Roles	• Application Security Engineer • Cloud Solution Administrator • Predictive Analytics Modeler • Watson Cognitive Specialist

For more information

To learn more about this career path and others, see ibm.biz/ibmskillsacademy

To learn more about validating your technical skills with IBM Open Badges, see www.youracclaim.com

To stay informed about the IBM Skills Academy, see the following sites:

Facebook: www.facebook.com/ibmskillsacademy