ServiceNow Security Incident Response (SIR) Implementation

16 Hours

Course Description

This interactive course provides comprehensive coverage of Security Incident Response (SIR) implementation, offering participants domain knowledge, practical skills, and strategic insights necessary for effective security incident management. Through a combination of lectures, group discussions, and hands-on labs, attendees will explore common implementation scenarios, technical aspects, and various processes required for successful SIR implementation.

Audience

This course is ideal for security professionals, IT administrators, and ServiceNow platform users responsible for implementing and managing Security Incident Response. Participants should have a foundational understanding of ServiceNow fundamentals and security operations.

Pre-requisite Knowledge/Skills

Mandatory

- Welcome to ServiceNow
- ServiceNow Administration Fundamentals
- Security Operations Fundamentals or Security Operations Fundamentals
- ServiceNow Platform Implementation

Optional

- Automated Test Framework (ATF) Fundamentals
- Common Service Data Model (CSDM) Fundamentals
- Configuration Management Database (CMDB) Fundamentals
- Flow Designer Fundamentals
- Get Started with Now Create
- IntegrationHub Fundamentals
- Mobile Development Fundamentals
- Service Portal Fundamentals
- Introduction to Playbooks and Process Automation Designer
- Playbooks and Process Automation Designer Fundamentals

Course Objectives

Upon completion of the course, participants will be able to:

- Identify the goals of Security Incident Response (SIR)
- Understand and meet customer goals in a SIR Implementation
- Create Security Incidents and use dashboards and reports
- Utilize the MITRE-ATT&CK framework in SIR
- Explore SIR Integrations and Capabilities
- Use the Security Incident Response Workspace
- Create and apply Security Tags
- Identify Calculators and apply Risk Scores
- Enhance Process Definitions and Selection
- Conduct Post-Incident Reviews
- Configure SIR Workspace Playbooks
- Leverage the User Reported Phishing v2 Feature

Course Outline

Module 1 - Introduction to Security Incident Response Implementation Course

- Overview

Module 2 - Security Incident Response Overview and Data Visualization

- Introducing Security Incident Response
- Lab - Initial Application Setup
- Data Visualization and SIR Components

Module 3 - Security Incident Creation and Threat Intelligence

- Explore How to Create Security Incidents
- Lab - Manual Creation of Security Incidents
- Major Security Incident Response
- Lab - Major Security Incident Response
- Understanding Threat Intelligence and MITRE-ATT&CK Framework
- Lab - Leverage the MITRE-ATT&CK Framework

Module 4 - Security Incident and Threat Intelligence Integrations

- ServiceNow Store and Managing Pre-Built Integrations

- Managing Pre-Built Integrations, Supporting Applications, and Custom Integration
- Lab - Custom Security Incident Integration

Module 5 - Security Incident Response Management

- Security Incident Response Workspace
- Lab - Security Incident Response Workspace
- Standard Automated Assignment Options, Escalation Paths, and Security Tags
- Lab - Configure Security Tags
- Process Definitions and Selection
- Lab - Security Incident Process Selection

Module 6 - Risk Calculations and Post-Incident Response

- Security Incident Calculator Groups and Risks Scores
- Lab - Security Incident Calculator Groups
- Post-Incident Reviews
- Lab - Post-Incident Reviews

Module 7 - Automation and Standard Processes

- Automate Security Incident Response Overview and Automation using Playbooks
- Lab - Configure Security Incident Playbooks
- Security Incident Automation using Runbooks and Use Case: User Reported Phishing V2
- Lab - Use Case URP v2

Module 8 - Conclusion and Capstone Project

- Capstone Project Overview
- Capstone Challenge Format, Simulator, and Conclusion

Module 9 - Certified Implementation Specialist – Security Incident Response Voucher Info