ServiceNow Security Incident Response (SIR) Implementation

Course Description:

This interactive, self-paced course provides domain knowledge, common implementation practices, technical aspects, and processes essential for effectively managing a Security Incident Response (SIR) implementation aligned with the NIST Framework. Through lectures, group discussions, and hands-on labs, participants develop tactical skills and strategies to implement SIR best practices confidently.

Audience Profile:

The course is ideal for ServiceNow implementers, security operations professionals, and IT practitioners responsible for security incident response and interested in mastering ServiceNow Security Incident Response capabilities.

Prerequisite:

Mandatory:

- Welcome to ServiceNow
- ServiceNow Administration Fundamentals (Instructor-Led or On Demand)
- Security Operations Fundamentals or Security Operations Fundamentals On Demand
- ServiceNow Platform Implementation or ServiceNow Platform Implementation On Demand

Optional (recommended for enhanced knowledge):

- 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 Objective:
Participants completing this course will be able to:

- Identify the goals of Security Incident Response (SIR)
- Understand and meet customer goals in a SIR implementation
- Create and manage Security Incidents
- Use and configure dashboards and reports in SIR
- Apply the MITRE ATT&CK framework within SIR
- Explore and use SIR integrations and capabilities
- Utilize the Security Incident Response Workspace effectively
- Create and apply Security Tags
- Identify and apply Calculators and Risk Scores
- Enhance process definitions and selections
- Complete Post Incident Reviews
- Configure SIR Workspace Playbooks
- Leverage the User Reported Phishing v2 feature

Table of Contents (TOC):

1. Welcome to Security Incident Response Implementation
2. Domain Knowledge for SIR
3. Common SIR Implementation Practices
4. Technical Aspects of SIR Implementation
5. Managing Security Incidents
6. Configuring Dashboards and Reports
7. Using the MITRE ATT&CK Framework in SIR
8. Exploring SIR Integrations and Capabilities

9. Navigating the Security Incident Response Workspace
10. Creating and Applying Security Tags
11. Risk Scoring and Calculators
12. Enhancing Process Definitions and Selection
13. Conducting Post Incident Reviews
14. Configuring SIR Workspace Playbooks
15. Leveraging User Reported Phishing v2 Feature