Security Incident Response Implementation

1: Security Incident Response Overview: Identify the goals of Security Incident Response (SIR), Discuss the importance of understanding customers and their goals, and discuss how Security Incident Response meets customer expectations.

2: Create Security Incidents: Determine how to create Security Incident Response incidents: Setup Assistant, Using the Service Catalog, Manual Creation, and Via Email Parsing.

3: Security Incident and Threat Intelligence Integrations: Discuss different integration capabilities, Describe the Three Key Security Incident Response Integrations: Custom, Platform, Store & Share.

4: Security Incident Response Management: Describe the Security Incident Response Management process and components: Assignment Options, Escalation Paths, Security Tags, Process Definitions and Selection.

5: Risk Calculations Post Incident Response: Identify Calculators and Risk Scores, Be able to post Incident Reviews.

6: Security Incident Automation: Discuss the Security Incident Response Automation processes available on the ServiceNow Platform: Workflows, Flow Designer, and Playbooks.

7: Data Visualization: Explain the different Security Incident Response Dashboards and Reports available in the ServiceNow platform: Data Visualization, Dashboards and Reporting, Performance Analytics.

8 Security Incident Response Family Release DELTA: Learn about the new, enhanced, and/or deprecated features of the current Security Incident Response family release.

9 Capstone Project: There is a final take-home Capstone project where participants provision a Developer instance and complete directed tasks to reinforce the concepts learned in class.