List of SOC with IBM QRadar & Splunk Topics

Introduction to SOC

- - SOC Overview
- - Importance of SOC
- - Benefits of SOC

Insights into CyberThreats
- - Network Level Threats
- - Web App Level Threats
- - Host Level Threats

Understanding Events and Logging Mechanisms
- - What Are Logs
- - Local Vs Centralized Logging
- - Exploration of Various Logs

SOC Analysis Using IBM QRadar:
- - Investigating Logs
- - Investigating Flows
- - Dashboard Creation
- - Asset Management
- - Report Generation
- - Exploring Rules and Building Blocks

IBM QRadar Advanced Concepts:
- - Offense Management
- - Customizing/Optimizing Rules and Building Blocks
- - Device Support Modules

Splunk Fundamentals
- - Data Ingestion
- - Splunk Apps and Addons
- - Splunk Data Models
- - Basic Searching

SOC Analysis Using Splunk
- - Data Visualization with Pivots and Databases
- - Search Processing Language Basics
- - Splunk Knowledge Objects
- - Generating Alerts

Incident Response Activities:
- - Incident Response Fundamentals

- - Incident Response and Security Operations Integration