CYBER SECURITY SOC ANALYST TRAINING – SIEM (SPLUNK)

1. Course Introduction
2. Networking Concepts
3. Cyber Security Concepts
4. Understanding Splunk, SIEM and SOC Process
5. Understanding Various Logs, Dashboard and Alert creations
6. Walkthrough SIEM use cases and Incident Handling Stages
7. Introduction to threat Hunting
8. Networking and Security Interview Questions
9. SIEM Interview Questions
10. SOC Process Interview Questions and Day to Day Activities
11. SIEM Alert Analysis Interview Questions
12. Discussion on Real Time Activities
13. Course wrap up

Section 1: Course Introduction – 1Hrs

1. Cyber Security Analyst – Intro to Course Content

Section 2: Networking Concepts – 15Hrs

1. Introduction to Organization Network-1
2. Introduction to Organization Network-2
3. ISO Model - Application and Presentation Layer Basics
4. ISO Model - Session, Transport, Network and Data Link Layer Basics
5. ISO Model Recap AND Public/Private Address Range
6. Introduction to web technology
7. Understanding HTTP protocol Part 1
8. Understanding HTTP Part 2 and Understanding Service Ports Part1
9. Understanding SMB, Telnet, FTP, NFS, SMTP, MySQL Services.
10. Introduction to Windows - Types of Windows OS and Permissions
11. Windows OS - Computer Management, Utilities
12. Port Numbers - Part 1
13. Port Numbers - Part 2

CYBER SECURITY SOC ANALYST TRAINING

Section 3: Cyber Security Concepts – 11Hrs

1. Introduction to Security CIA Encryption and Hashing
2. Defense in Depth Approach
3. Cyber Kill chain OR Phases of Attack
4. Brute Force Attack and Types
5. Phishing and Spoofing Attacks
6. DNS Tunneling Attack
7. Malware and its Types
8. OWASP Top 10

Section 4: Understanding Splunk, SIEM and SOC Process– 10Hrs

1. SOC Introduction and Process
2. SOC Roles and Responsibilities
3. SIEM Architecture
4. Splunk Introduction
5. Splunk Installation
6. Splunk Universal Forward Installation

Section 5: Understanding Various Logs, Dashboard and Alert creations – 24Hrs

1. Uploading Demo Logs to Splunk and firewall Log analysis
2. Understanding Firewall Logs
3. Splunk Dashboard creation - Firewall Part 1
4. Splunk Dashboard creation - Firewall Part 2
5. IDS Log Analysis
6. DNS Profiling Scenarios Part 1
7. DNS Profiling Scenarios Part 2
8. Understanding DNS Logs
9. Understanding HTTP Logs Part 1
10. Understanding HTTP Logs Part 2
11. Understanding Windows Log
12. Understanding Windows Event IDs
13. Windows Sysmon Log Analysis
14. Understanding Antivirus Logs

Section 6: Walkthrough SIEM use cases and Incident Handling Stages– 8Hrs

1. SIEM Use cases Part 1
2. SIEM Use cases Part 2
3. SIEM Use cases Part 3
4. Malware outbreak Analysis
5. Incident Handling stages

CYBER SECURITY SOC ANALYST TRAINING

Section 7: Introduction to Threat Hunting – 5Hrs

1. Threat Hunting – Scanning attack on Web Server
2. Threat Hunting – Brute Force Attack
3. Email Header Analysis

Section 8: Networking and Security Interview Questions – 4Hrs

1. What are networking devices?
2. What is IP address and IP address classification?
3. What is NAT and PAT?
4. Tell me few port numbers which you know?
5. How a Firewall works?
6. How VPN works?
7. What is Symmetric and Asymmetric Encryption?
8. Explain CIA triad?
9. What is difference between SSL and HTTPS?
10. How do you stay up to date on Cyber Security news and latest attacks?
11. What is the difference between Virus and Warm?
12. Explain SQL Injection Attack?
13. What is botnet?
14. What is Brute Force Attack?
15. SIEM related interview topics?

Section 9: SIEM Interview Questions – 2Hrs

1. SIEM Dashboard and Use cases
2. What are different event logs you analyze?

Section 10: SOC Process Interview Questions and Day to Day Activities – 4Hrs

1. What is Security Operation Center?
2. What are various Security Devices used in your organization?
3. How does a SOC Team manage or work in an organization?
4. What are the Roles and Responsibilities of SOC Engineer?
5. What are the fields in Sample Incident ticket – ServiceNow?
6. What are Service Level Agreements (SLA) for the SOC Incidents?
7. What is False Positive Analysis? Or what are various outcomes of Analysis?
8. How many Logs sources are there in your organization?
9. What are the steps in Incident Response Life Cycle?
10. Can you please explain what you will do after getting an alert? (Alert IR Flow)
11. How will you manage work in shifts?
12. How do you handle P1, P2, P3 and P4 incidents?

Section 11: SIEM Alert Analysis Interview Questions – 3Hrs

1. How do you analyze if receive a Brute Force Attack Alert?
2. What will you do if receive a Malware Attack Alert?
3. How do you analyze Phishing email attack?
4. How do you Analyze SQL Injection attack?
5. How do you analyze DDOS attack?
6. How do you analyze if a suspicious IP detected in outbound traffic?

Section 12: Discussion on Real Time Activities – 2Hrs

1. Discussion on Real Time Activities

Section 13: Course wrap up – 1Hrs

1. Course wrap up