


SOC Analyst with Splunk ES

BY KIRAN AMBADASU

Contact

 +91 75695 80831, +91 99599 64770

 +91 99599 64770

 splunkonlinetutorials@gmail.com

Course Curriculum

- 1 COURSE INTRODUCTION**
- 2 NETWORKING CONCEPTS FOR SOC ANALYSTS**
- 3 CYBERSECURITY CONCEPTS**
- 4 SPLUNK SIEM & SOC OPERATIONS**
- 5 SPLUNK SECURITY DASHBOARDS & ALERTS**
- 6 SIEM USE CASES & INCIDENT HANDLING**
- 7 THREAT HUNTING**
- 8 REAL-TIME OPERATIONS AND DISCUSSIONS**

Course Modules

01

COURSE INTRODUCTION

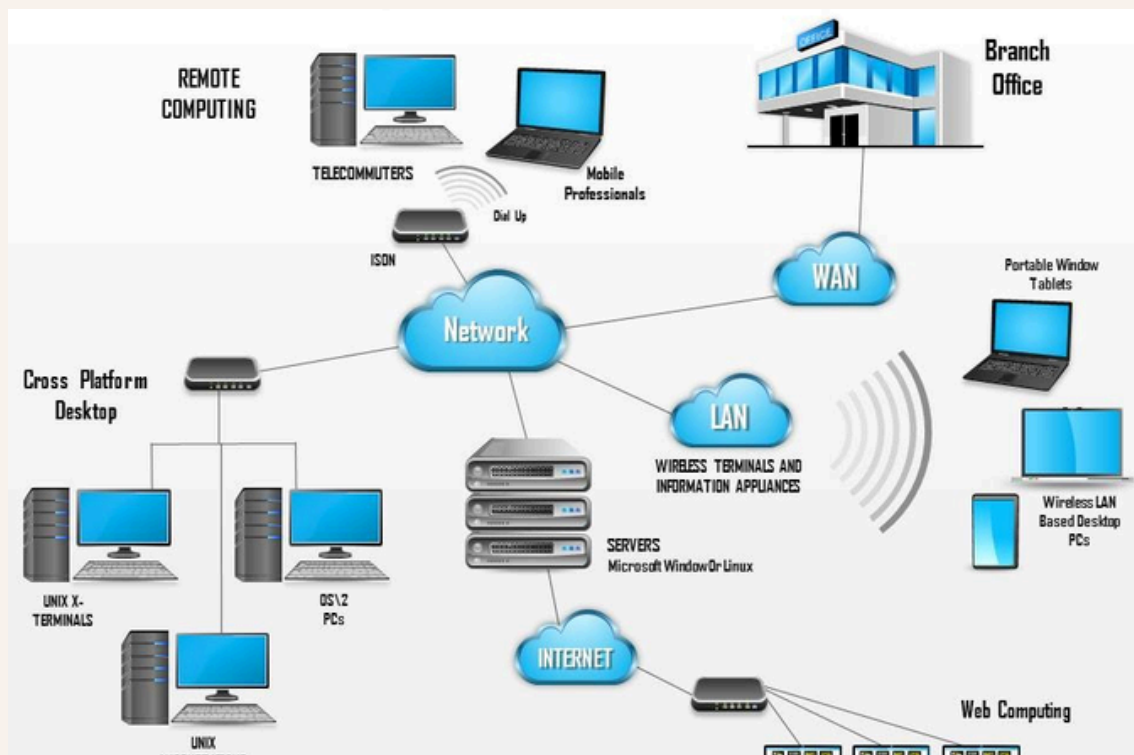
- Overview & Objectives
- Course Structure & Learning Path
- Understanding SOC Analyst Role
- High-Level Overview of Splunk ES

02

NETWORKING CONCEPTS FOR SOC ANALYSTS

2.1 Introduction to Organizational Networks

- Network Fundamentals: LAN, WAN, VPN
- Network Devices: Routers, Switches, Firewalls
- Importance of Network Security Monitoring



Course Modules

2.2 ISO/OSI Model – Key Layers & Security Implications

- Application & Presentation Layers (L7 & L6)
- HTTP/HTTPS, DNS, SMTP, FTP
- Data Encryption (SSL/TLS) & Encoding
- Session, Transport, Network & Data Link Layers (L5-L2)
- TCP vs. UDP (Reliability vs. Speed)
- IP Addressing, Subnetting, ARP Spoofing
- MAC Addressing

2.3 Public vs. Private IP Address Ranges

- IPv4 vs. IPv6
- NAT (Network Address Translation) & PAT
- Identifying Suspicious IP Traffic

2.4 Introduction to Web Technology

- Web Protocols (HTTP/HTTPS, WebSockets)
- Client-Server Architecture
- Common Web Vulnerabilities (SQLi, XSS, CSRF)



Course Modules

2.5 Understanding HTTP Protocol

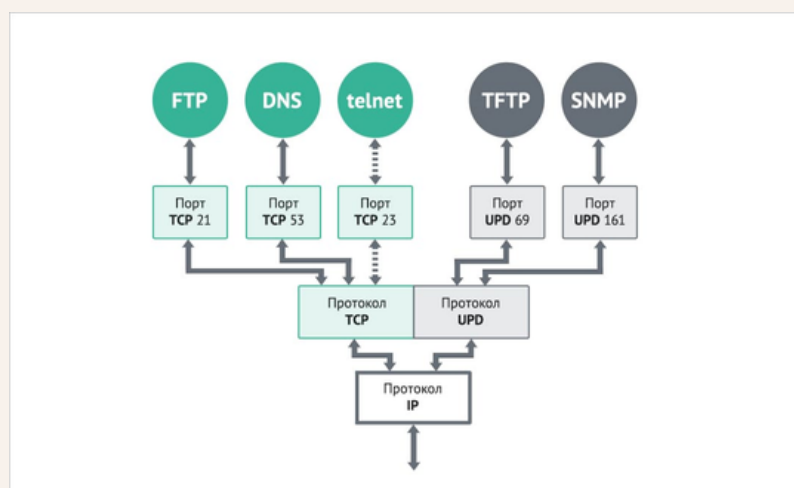
- HTTP Methods (GET, POST, PUT, DELETE)
- Status Codes & Headers
- Analyzing HTTP Logs for Anomalies

2.6 Understanding Service Ports

- Well-Known vs. Ephemeral Ports
- Common Ports & Associated Services (21-FTP, 22-SSH, 80-HTTP, 443-HTTPS)
- Detecting Unauthorized Port Scans

2.7 Key Protocols & Services

- SMB (445) – File Sharing & Exploits (EternalBlue)
- SMTP (25) – Email Spoofing & Phishing
- Telnet (23) – Risks of Unencrypted Communication
- SSH (22) – Secure Remote Access & Key-Based Auth
- FTP (20/21) – Secure Alternatives (SFTP/FTPS)
- MySQL (3306) – Database Security Best Practices



Course Modules

2.8 Windows OS for SOC Analysts

- Windows OS Types (Client vs. Server Editions)
- User & File Permissions (NTFS, Share Permissions)
- Windows Event Logs (Security, System, Application)

Key Utilities:

- Event Viewer – Log Analysis
- Task Manager & Resource Monitor – Process Tracking
- PowerShell – Security Auditing

2.9 In-Depth on Port Numbers

- Malicious Port Usage
- Port Scanning Techniques using Nmap
- Defending Against Port-Based Attacks

```
[→ ~ nmap scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-16 11:55 EST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 11:55 (0:00:00 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.071s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
22/tcp    open      ssh
53/tcp    open      domain
80/tcp    open      http
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
593/tcp   filtered  http-rpc-epmap
9929/tcp  open      nping-echo
31337/tcp open      Elite

Nmap done: 1 IP address (1 host up) scanned in 29.13 seconds
```

Course Modules

03

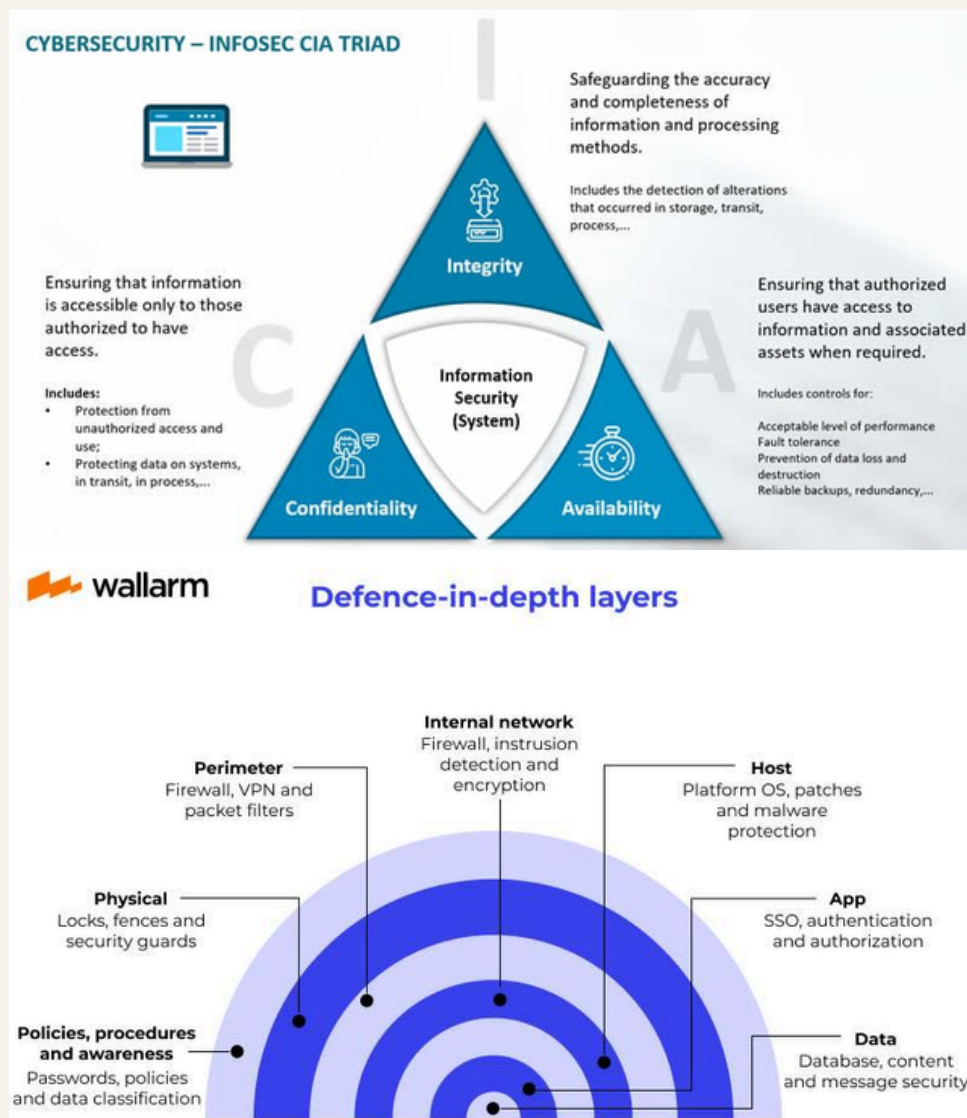
CYBERSECURITY CONCEPTS

3.1 Introduction to Security: CIA Triad, Encryption & Hashing

- Confidentiality, Integrity, Availability (CIA)
- Symmetric vs. Asymmetric Encryption (AES, RSA)
- Hashing Algorithms (MD5, SHA-1, SHA-256)

3.2 Defense-in-Depth Approach

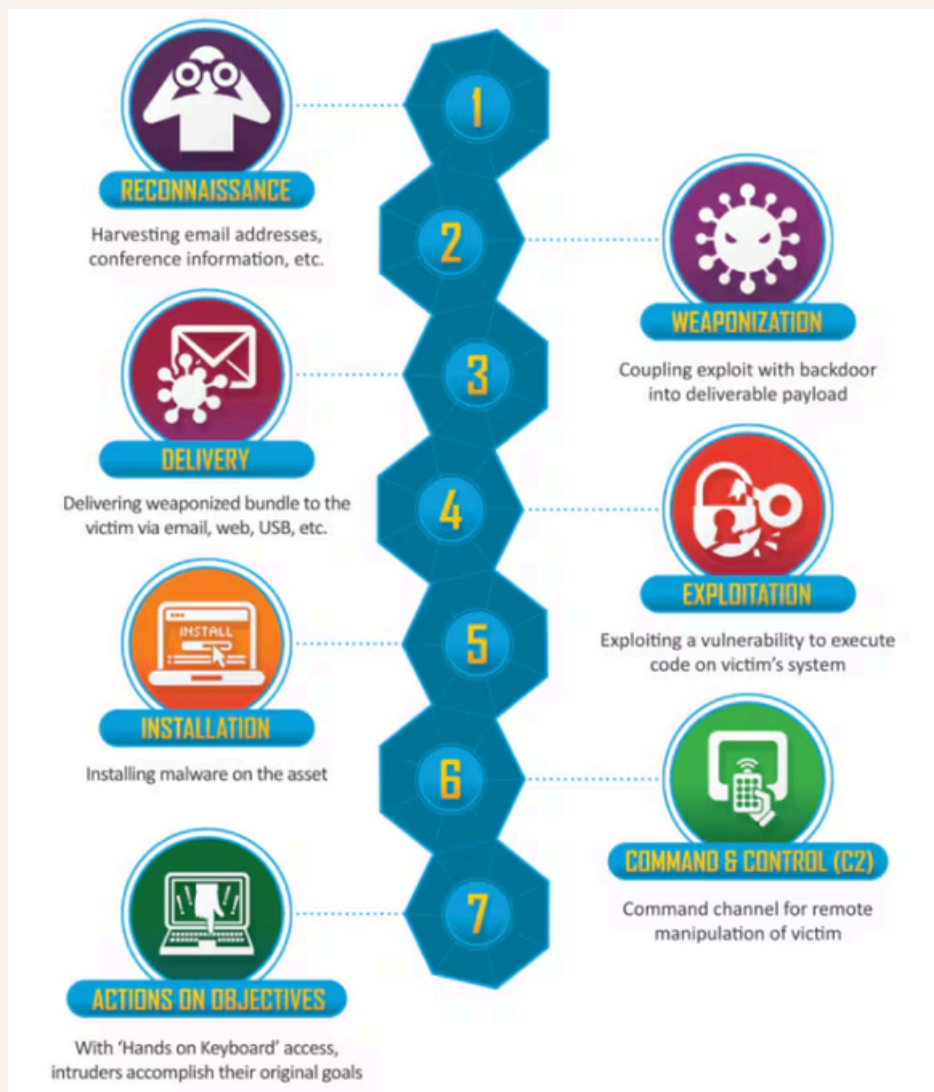
- Layered Security Controls (Firewalls, IDS/IPS, EDR)
- Zero Trust Architecture



Course Modules

3.3 Cyber Kill Chain / Phases of Attack

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control (C2)
- Actions on Objectives



Course Modules

3.4 Brute Force Attacks & Types

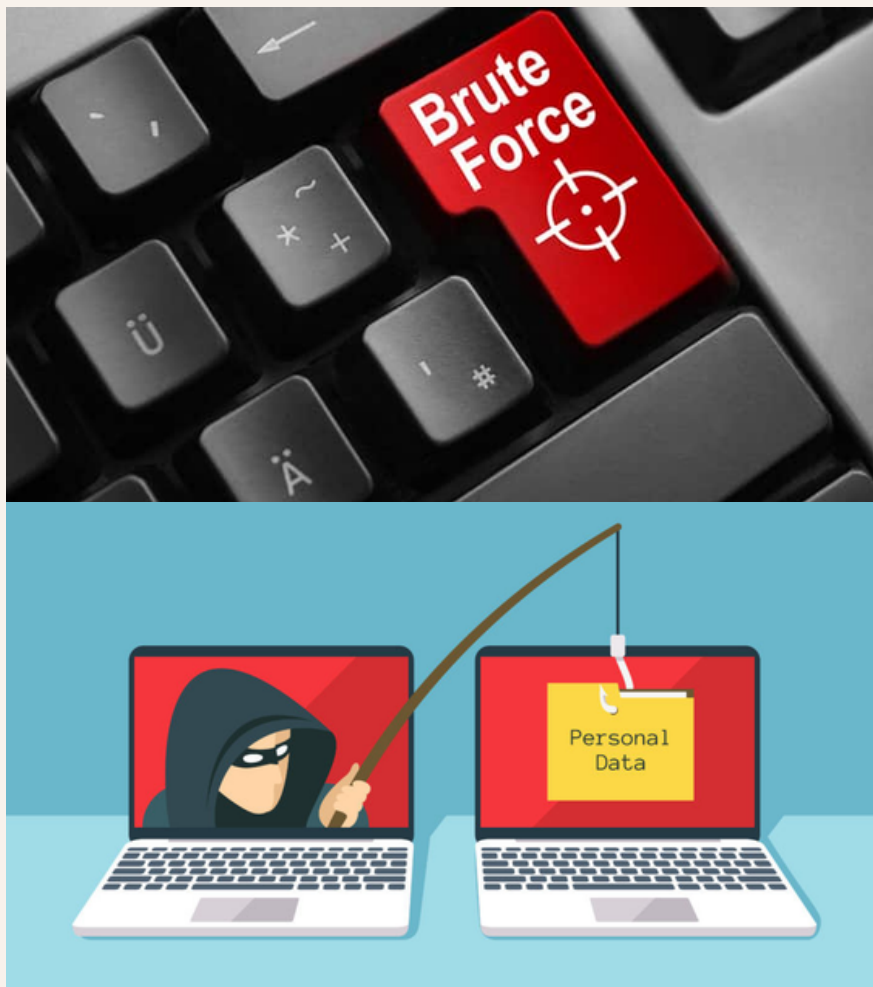
- Credential Stuffing vs. Dictionary Attacks
- Mitigation: Account Lockout Policies, CAPTCHA, MFA

3.5 Phishing & Spoofing Attacks

- Email Spoofing, CEO Fraud, Spear Phishing
- Detecting Phishing Attempts (SPF, DKIM, DMARC)

3.6 OWASP Top 10

- Top Risks: Injection, Broken Auth, XSS, Insecure APIs
- Real-World Exploit Examples



Course Modules

3.7 DNS Tunneling Attack

- How Attackers Exfiltrate Data via DNS
- Detection Methods (Anomalous DNS Query Lengths)

3.8 Malware Types & Attacks

- Trojans, Ransomware, Spyware, Rootkits
- Indicators of Compromise (IOCs)

3.9 MITRE ATT&CK and Frameworks

- Tactics, Techniques, and Procedures (TTPs)
- Understanding Techniques – Methods to Achieve Goals
- Sub-techniques – Specific Implementations of Techniques
- Procedures using Threat Intelligence, and Threat Detection
- Procedure Examples – Real-world Threat Actor Behaviors

The image displays the MITRE ATT&CK v17 matrix, a structured grid of attack techniques. The columns represent tactics, and the rows represent specific techniques. The tactics listed are: Execution (3 techniques), Persistence (7 techniques), Privilege Escalation (5 techniques), Defense Evasion (9 techniques), Credential Access (1 technique), Discovery (11 techniques), Lateral Movement (3 techniques), Collection (2 techniques), Command and Control (14 techniques), and Exfiltration (4 techniques). The techniques listed include: Account Manipulation (1), SSH Authorized Keys, Boot or Logon Initialization Scripts (1), RC Scripts, Compromise Host Software Binary, Create Account (1), Local Account, Scheduled Task/Job (1), Cron, Server Software Component (1), vSphere Installation Bundles, Valid Accounts (3), Default Accounts, Domain Accounts, Local Accounts, Account Manipulation (1), SSH Authorized Keys, Boot or Logon Initialization Scripts (1), RC Scripts, Escape to Host, Scheduled Task/Job (1), Valid Accounts (3), Default Accounts, Domain Accounts, Local Accounts, Deobfuscate/Decode Files or Information, Execution Guardrails, File and Directory Permissions Modification, Hide Artifacts (1), Run Virtual Instance, Impair Defenses (3), Impair Command History Logging, Disable or Modify System Firewall, Indicator Blocking, Indicator Removal (4), Clear Command History, File Deletion, Timestamp, Clear Persistence, Masquerading (1), Match Legitimate Name or Location, Obfuscated Files or Information, Valid Accounts (3), Default Accounts, Domain Accounts, Local Accounts, Brute Force (2), Password Guessing, Password Spraying, Credential Stuffing, Account Discovery (1), Local Account, File and Directory Discovery, Log Enumeration, Process Discovery, Remote System Discovery, Software Discovery, System Information Discovery, System Network Configuration Discovery (1), Internet Connection Discovery, System Network Connections Discovery, Exploitation of Remote Services, Lateral Tool Transfer, Remote Services (1), SSH, Data from Local System, Data Staged (2), Local Data Staging, Remote Data Staging, Application Layer Protocol (3), Web Protocols, File Transfer Protocols, DNS, Data Encoding (2), Standard Encoding, Non-Standard Encoding, Data Obfuscation (3), Junk Data, Steganography, Protocol or Service Impersonation, Dynamic Resolution (3), Fast Flux DNS, Domain Generation Algorithms, DNS Calculation, Encrypted Channel (2), Symmetric Cryptography, Asymmetric Cryptography, Fallback Channels, Hide Infrastructure, Ingress Tool Transfer, Multi-Stage Channels, Non-Application Layer Protocol, Non-Standard Port, Protocol Tunneling, Proxy (4), Internal Proxy, Data Transfer Size Limits, Account A, Exfiltration Over Alternative Protocol (3), Data Dest, Data Encry, Defacen, Internal, Inhibit Syst, Service Sh, System Sh, Exfiltration Over C2 Channel, Exfiltration Over Web Service (4), Exfiltration to Code Repository, Exfiltration to Cloud Storage, Exfiltration to Text Storage Sites, Exfiltration Over Webhook.

Tactic	Techniques
Execution (3 techniques)	Command and Scripting Interpreter (3)
Persistence (7 techniques)	Account Manipulation (1), SSH Authorized Keys, Boot or Logon Initialization Scripts (1), RC Scripts, Compromise Host Software Binary, Create Account (1), Local Account, Scheduled Task/Job (1), Cron, Server Software Component (1), vSphere Installation Bundles, Valid Accounts (3), Default Accounts, Domain Accounts, Local Accounts
Privilege Escalation (5 techniques)	Account Manipulation (1), SSH Authorized Keys, Boot or Logon Initialization Scripts (1), RC Scripts, Escape to Host, Scheduled Task/Job (1), Valid Accounts (3), Default Accounts, Domain Accounts, Local Accounts
Defense Evasion (9 techniques)	Deobfuscate/Decode Files or Information, Execution Guardrails, File and Directory Permissions Modification, Hide Artifacts (1), Run Virtual Instance, Impair Defenses (3), Impair Command History Logging, Disable or Modify System Firewall, Indicator Blocking, Indicator Removal (4), Clear Command History, File Deletion, Timestamp, Clear Persistence, Masquerading (1), Match Legitimate Name or Location, Obfuscated Files or Information, Valid Accounts (3), Default Accounts, Domain Accounts, Local Accounts
Credential Access (1 technique)	Brute Force (2), Password Guessing, Password Spraying, Credential Stuffing
Discovery (11 techniques)	Account Discovery (1), Local Account, File and Directory Discovery, Log Enumeration, Process Discovery, Remote System Discovery, Software Discovery, System Information Discovery, System Network Configuration Discovery (1), Internet Connection Discovery, System Network Connections Discovery
Lateral Movement (3 techniques)	Exploitation of Remote Services, Lateral Tool Transfer, Remote Services (1), SSH
Collection (2 techniques)	Data from Local System, Data Staged (2), Local Data Staging, Remote Data Staging
Command and Control (14 techniques)	Application Layer Protocol (3), Web Protocols, File Transfer Protocols, DNS, Data Encoding (2), Standard Encoding, Non-Standard Encoding, Data Obfuscation (3), Junk Data, Steganography, Protocol or Service Impersonation, Dynamic Resolution (3), Fast Flux DNS, Domain Generation Algorithms, DNS Calculation, Encrypted Channel (2), Symmetric Cryptography, Asymmetric Cryptography, Fallback Channels, Hide Infrastructure, Ingress Tool Transfer, Multi-Stage Channels, Non-Application Layer Protocol, Non-Standard Port, Protocol Tunneling, Proxy (4), Internal Proxy
Exfiltration (4 techniques)	Data Transfer Size Limits, Account A, Exfiltration Over Alternative Protocol (3), Data Dest, Data Encry, Defacen, Internal, Inhibit Syst, Service Sh, System Sh, Exfiltration Over C2 Channel, Exfiltration Over Web Service (4), Exfiltration to Code Repository, Exfiltration to Cloud Storage, Exfiltration to Text Storage Sites, Exfiltration Over Webhook

Course Modules

04

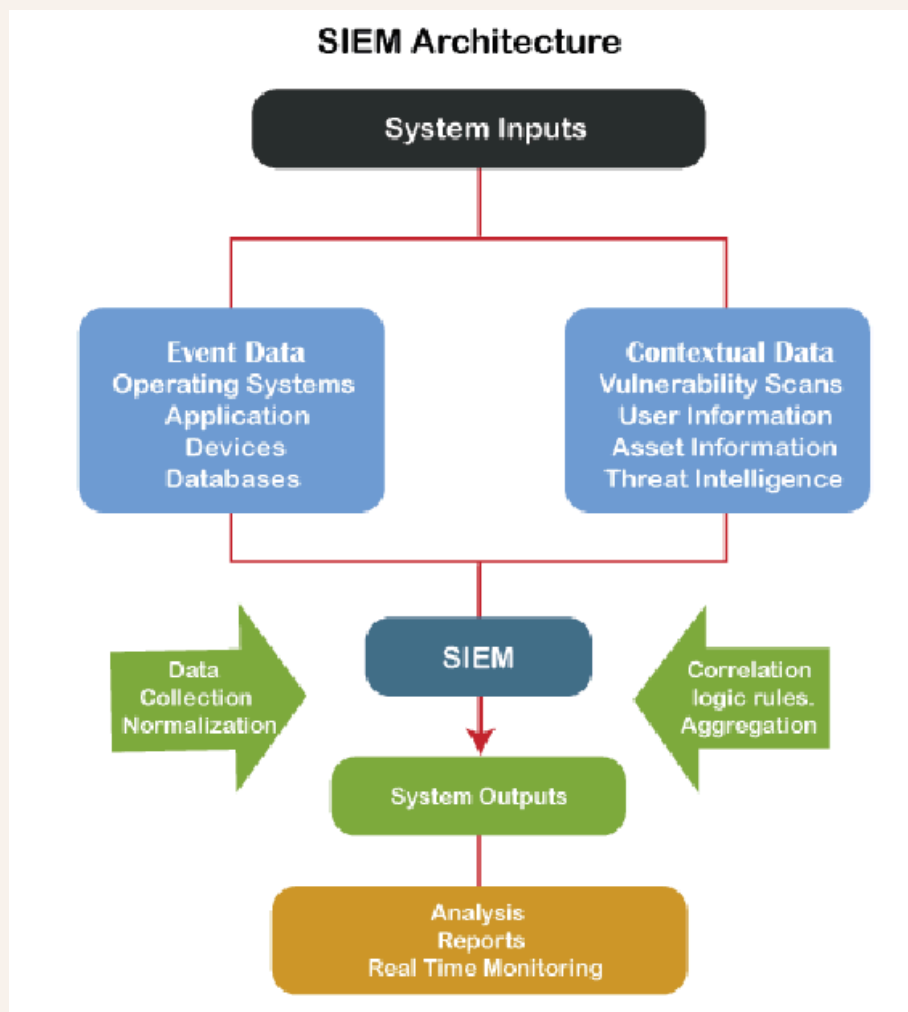
SPLUNK SIEM & SOC OPERATIONS

4.1 Splunk Installation & Setup

- Splunk Enterprise vs. Universal Forwarder
- Configuring Data Inputs

4.2 SOC Process & Responsibilities

- Incident Triage, Escalation, Response
- SIEM Architecture & Log Collection



Course Modules

4.3 Security Log Analysis in Splunk

- Firewall Logs (Blocked Traffic, Port Scans)
- IDS/IPS Alerts (Signature vs. Anomaly-Based)
- DNS Log Analysis (Detection, Exfiltration)
- HTTP Logs
- Antivirus Logs (Malware Detection Events)

4.4 Windows Log Analysis

- Critical Event IDs
(4625-Failed Login, 4688-Process Creation)
- Sysmon for Advanced Threat Detection



Course Modules

05 SPLUNK SECURITY DASHBOARDS & ALERTS

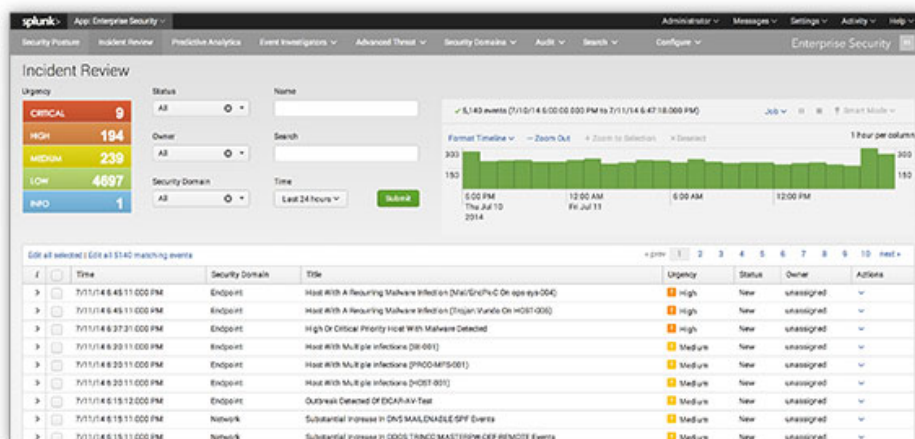
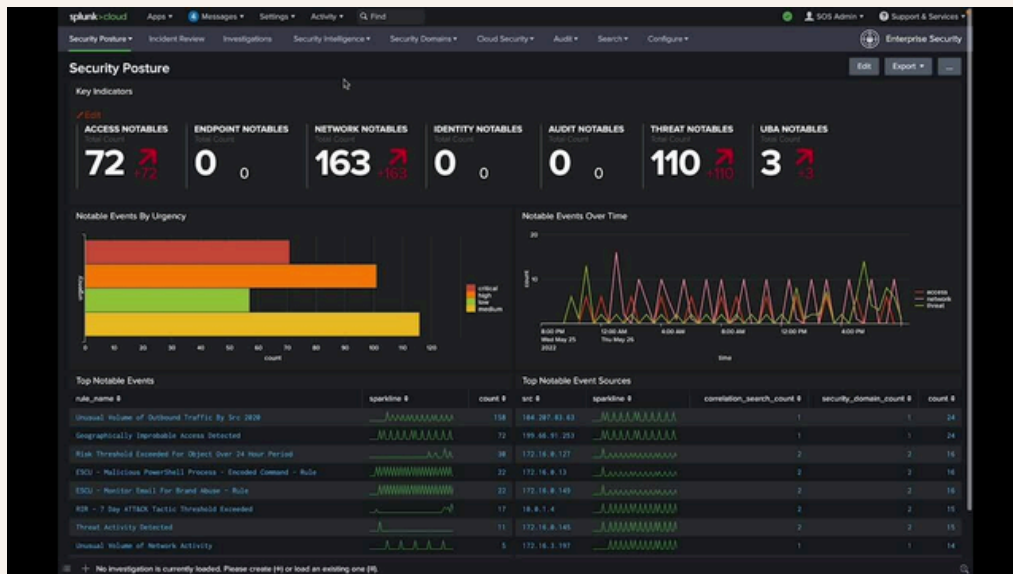
5.1 Security Dashboard Creation

- Visualizing Security Event use cases (Firewall, IDS/IPS, DNS Etc)
- Best practices for dashboard layout and usability

5.2 Custom Alerts & Correlation Rules

Various types of Security alerts including:

- Creation of correlation searches for suspicious events and patterns
- Creation of alerts by generating notable events



Course Modules

06

SIEM USE CASES & INCIDENT HANDLING

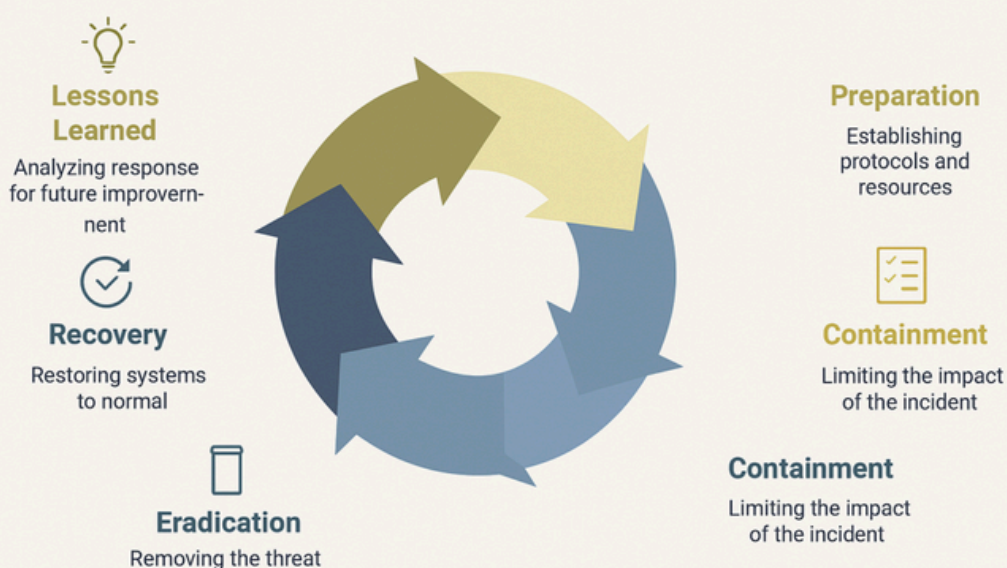
6.1 Real-World SIEM Use Cases

- Brute Force Attack Detection
- Brute Force Attack Investigation
- Email Header Analysis (Tracking Phishing Origins)

6.2 Incident Handling Stages (NIST Framework)

- Preparation
- Detection & Analysis
- Containment
- Eradication
- Recovery
- Lessons Learned

Incident Response Lifecycle



Course Modules

07 THREAT HUNTING

7.1 Proactive Threat Hunting Techniques

- Web Server Scanning Attack Analysis
- Brute Force Attack Investigation
- Email Header Analysis (Tracking Phishing Origins)




08 REAL-TIME OPERATIONS AND DISCUSSIONS


Each topic is supplemented with practical oriented sessions, use-case discussions, and real-world problem-solving techniques along with daily class recordings to ensure practical learning and operational confidence.


Thank you

FOR MORE DETAILS:

Contact

 +91 75695 80831, +91 99599 64770

 +91 99599 64770

 splunkonlinetutorials@gmail.com