jotHUB
A Professional Job Oriented Training Hub

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

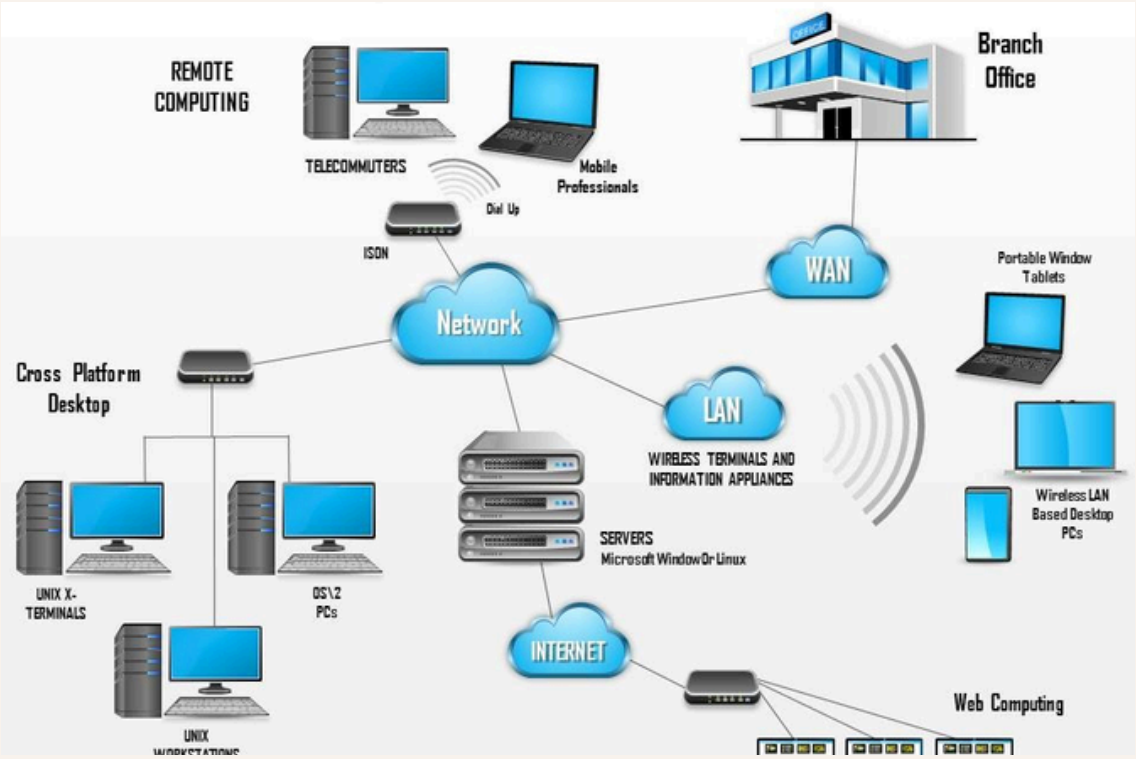
02 NETWORKING CONCEPTS FOR SOC ANALYSTS

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

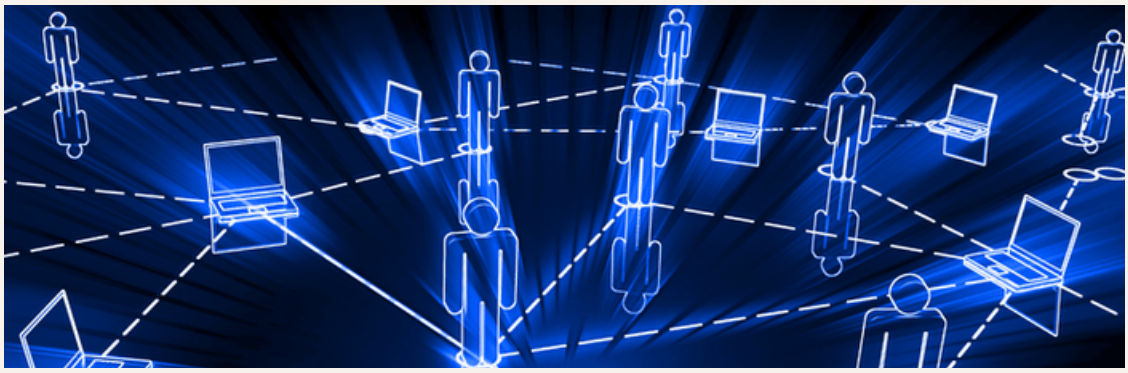
— Identifying Suspicious IP Traffic

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)

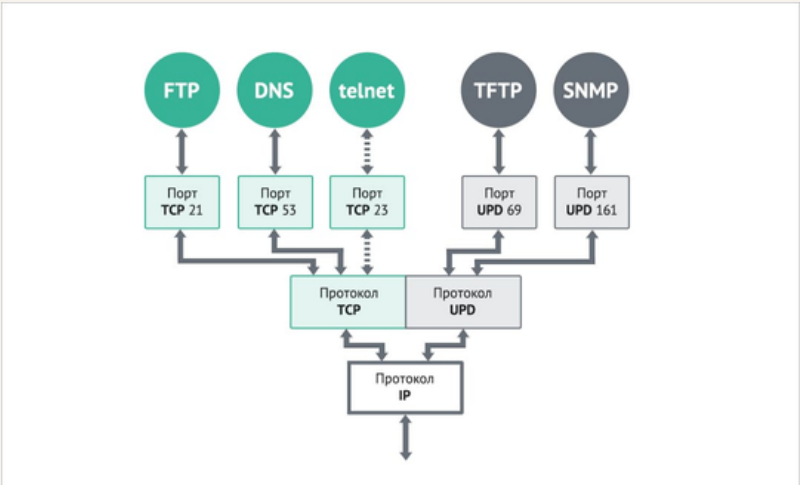
— SMTP (25) – Email Spoofing & Phishing

— 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

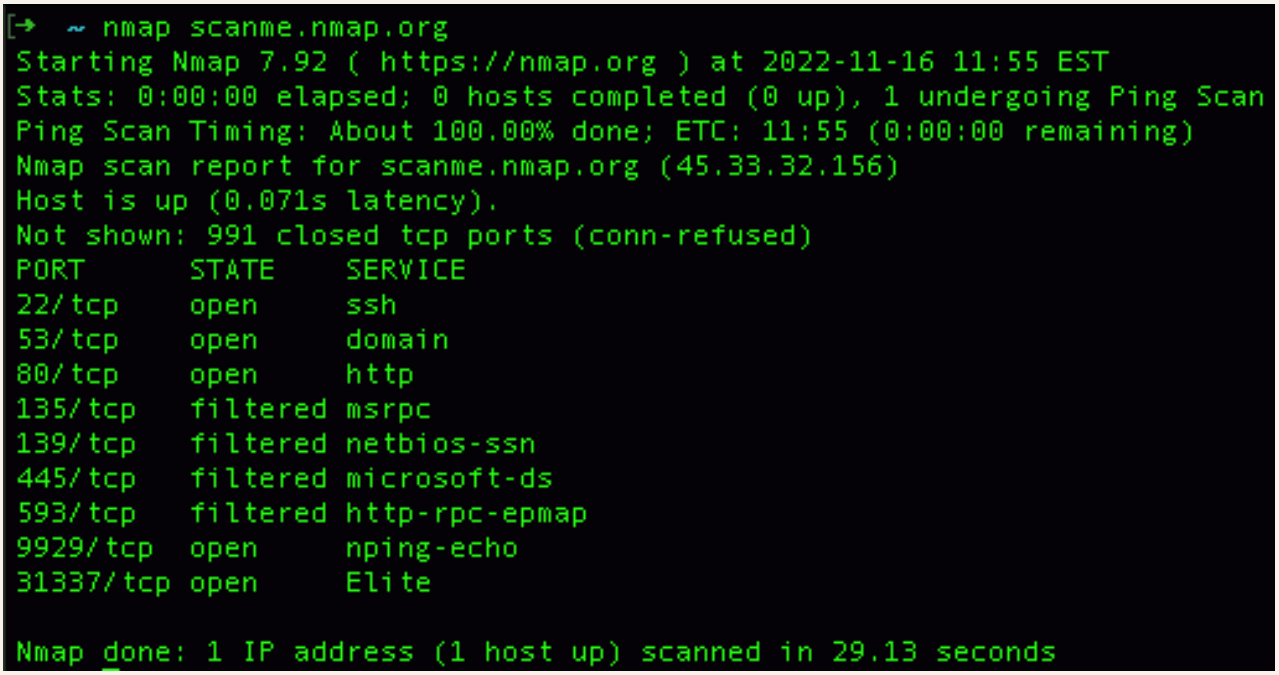
— PowerShell – Security Auditing

2.9 In-Depth on Port Numbers

— Malicious Port Usage

— Port Scanning Techniques using Nmap

— Defending Against Port-Based Attacks



Course Modules

03 CYBERSECURITY CONCEPTS

3.1 Introduction to Security:CIA Triad,Encryption&Hashing

— Confidentiality, Integrity, Availability (CIA)

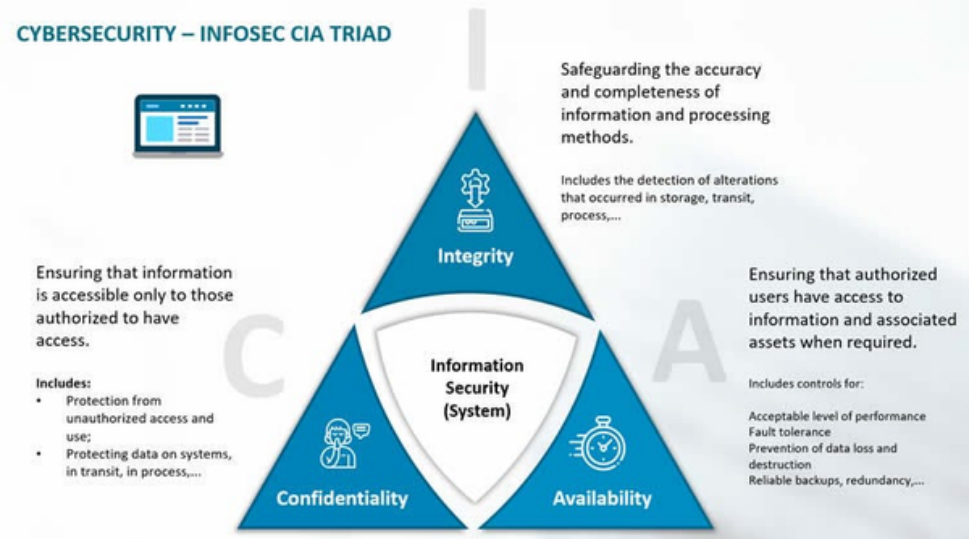
— Symmetric vs. Asymmetric Encryption (AES, RSA)

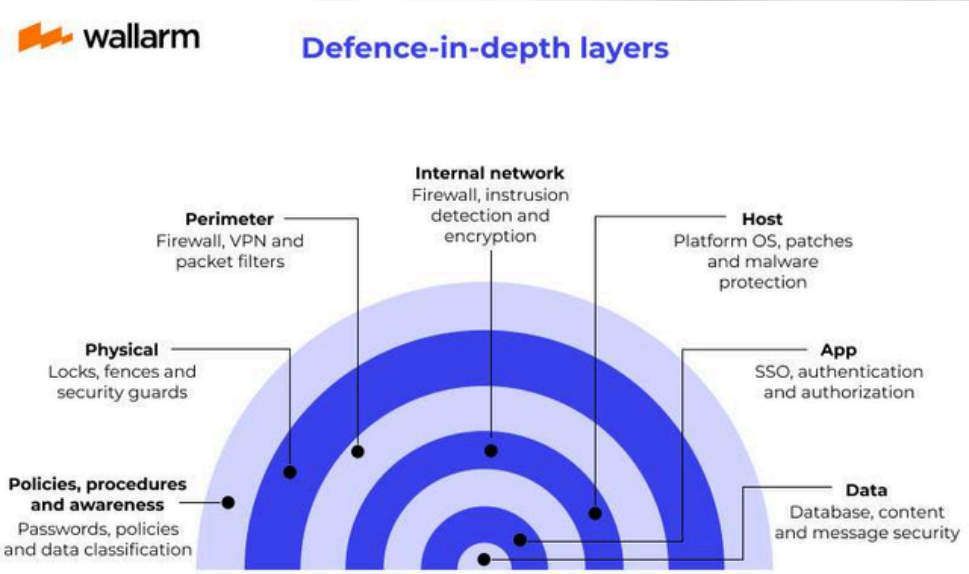
— Hashing Algorithms (MD5, SHA-1, SHA-256)

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

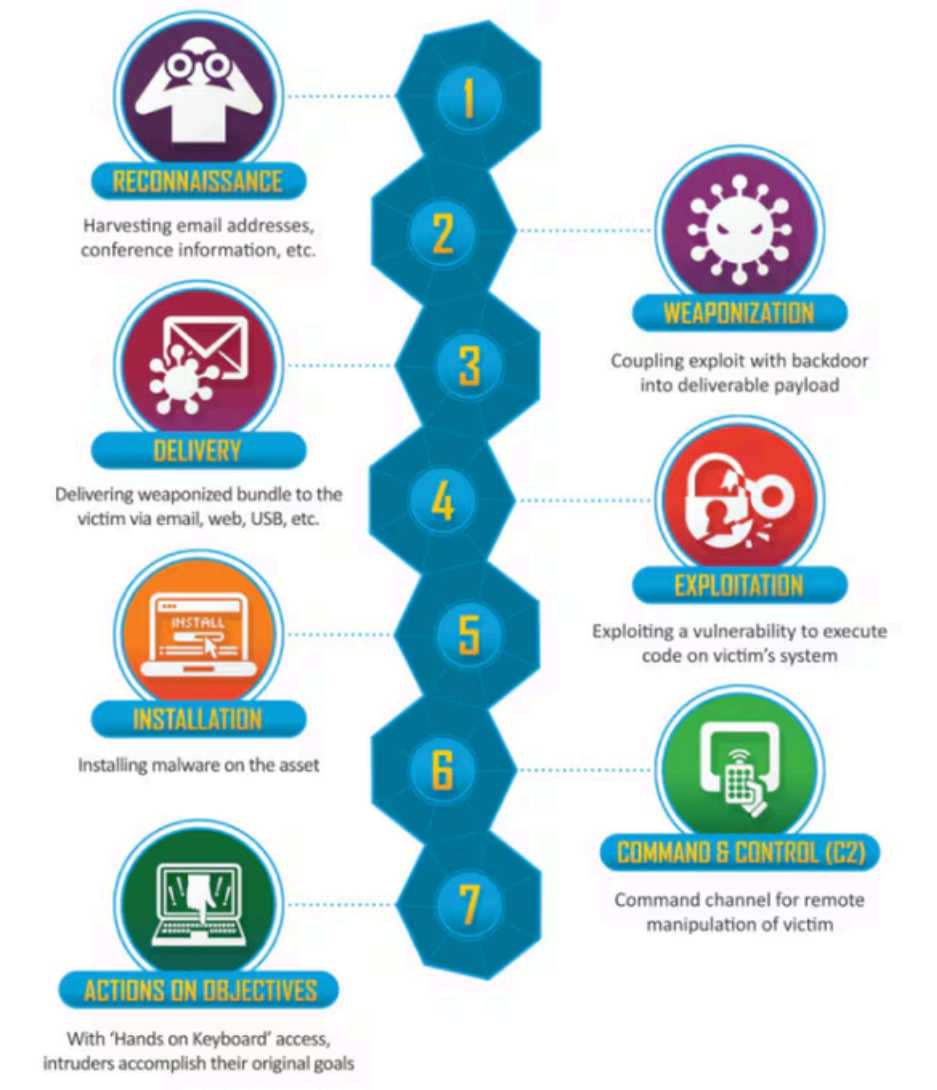
— Delivery

— 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

Course Modules

04 SPLUNK SIEM & SOC OPERATIONS

4.1 Splunk Installation & Setup

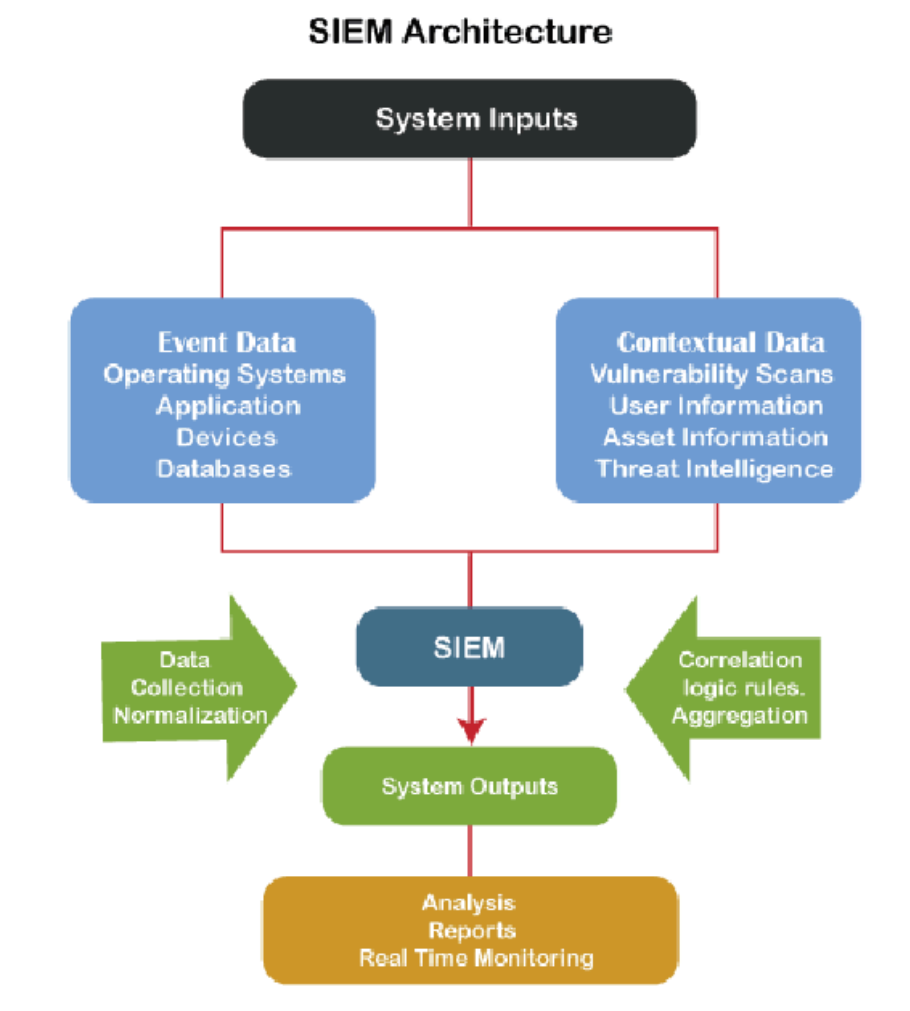
— Splunk Enterprise vs. Universal Forwarder

— 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)

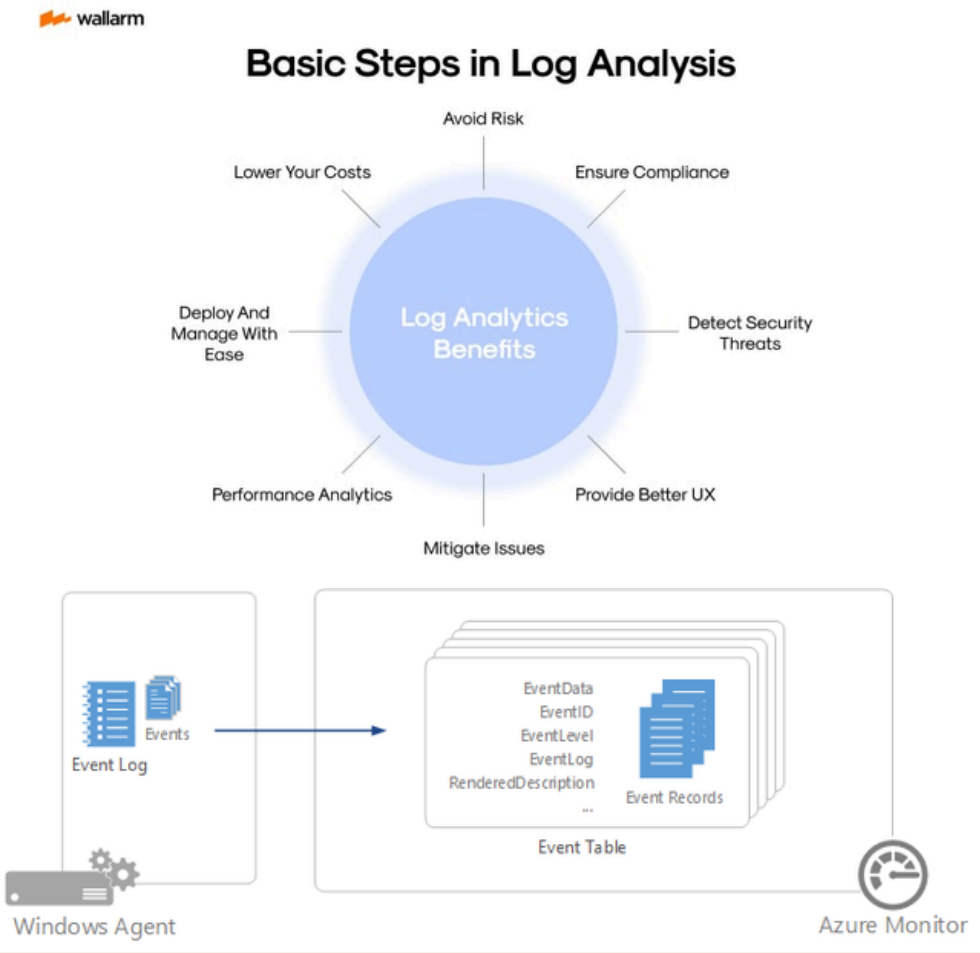
— HTTP Logs

— 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)

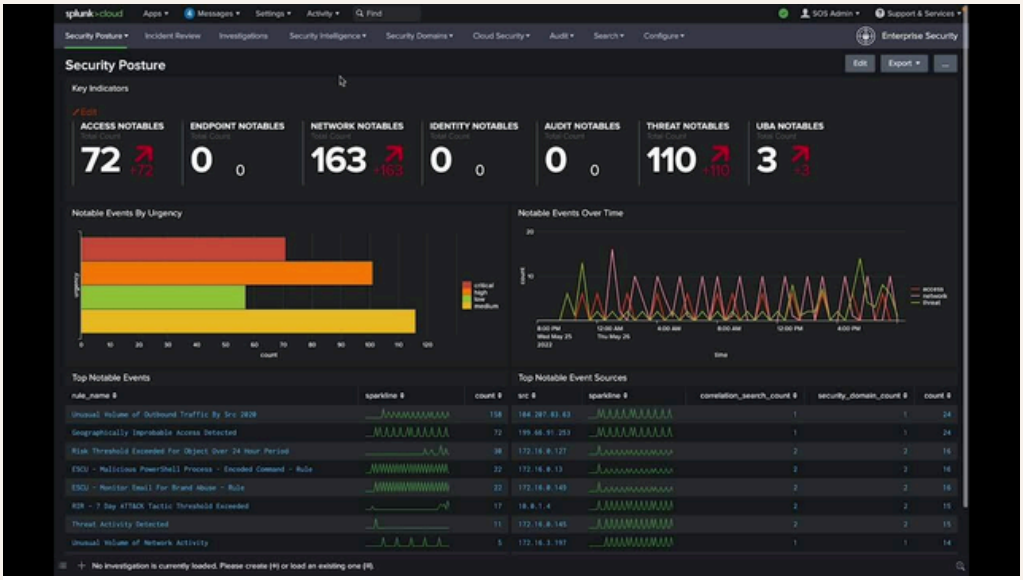
— Best practices for dashboard layout and usability

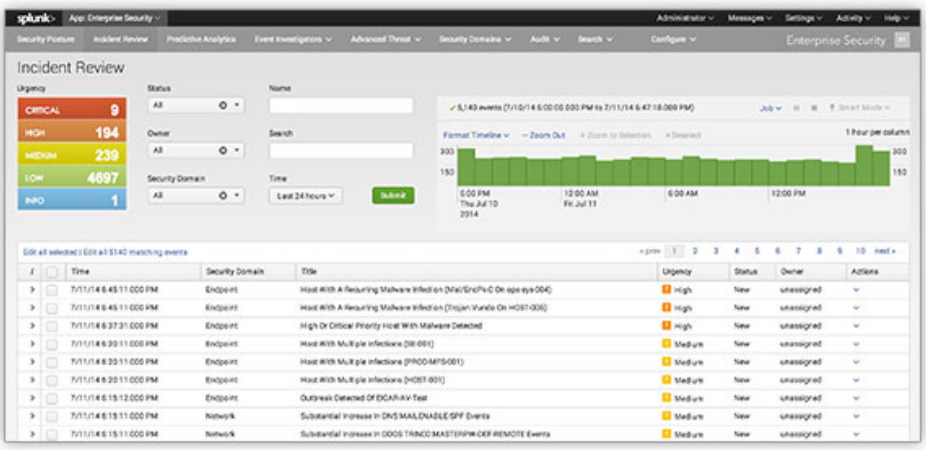
5.2 Custom Alerts & Correlation Rules

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

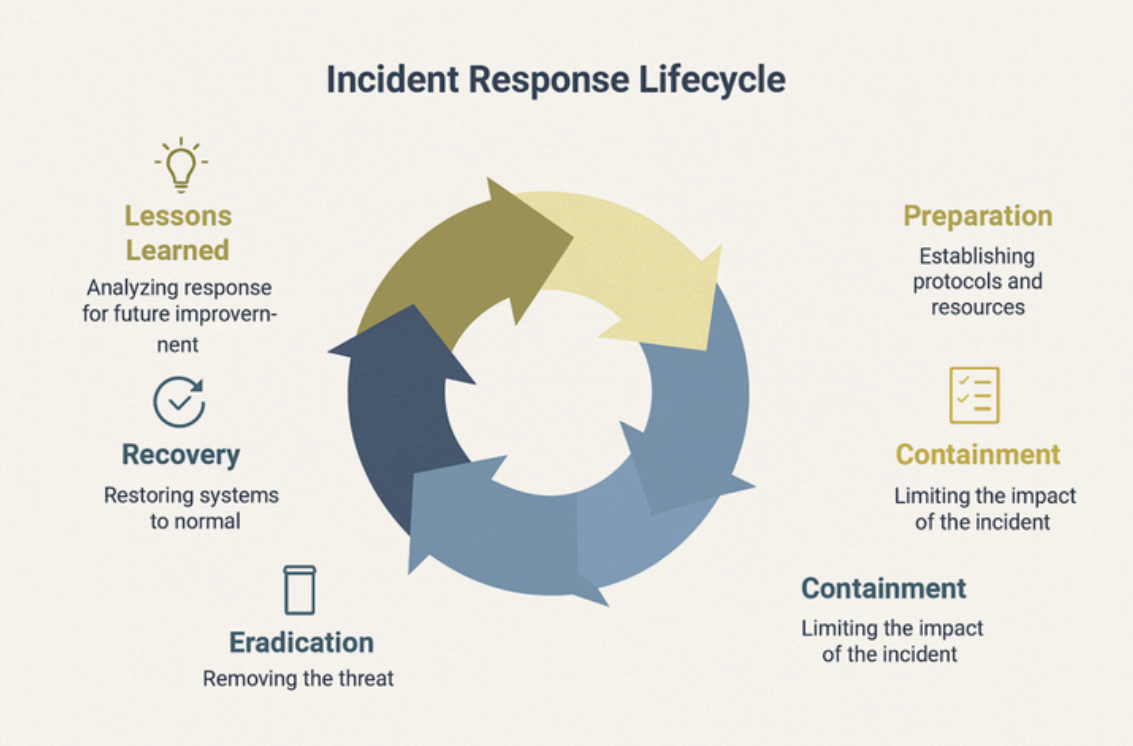
— Detection & Analysis

— Containment

— Eradication

— Recovery

— Lessons Learned



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