jotHUB
A Professional Job Oriented Training Hub

Future-Ready SOC Analyst with AI

BY KIRAN AMBADASU

Contact

+91 75695 80831, +91 99599 64770

+91 99599 64770

kiranambadasu@jothub.in

WHO SHOULD ENROLL IN THIS PROGRAM?

Cybersecurity is not learned by theory alone. Real-world SOC roles require practical exposure, incident investigation skills, and hands-on experience with industry tools. Our SOC Analyst Training Program is designed to transform learners into job-ready security professionals by combining security fundamentals, SIEM operations, threat detection techniques, and real incident scenarios.

Suitable For:

🎓 Fresh Graduates & Final-Year Students

Students who want to start their career in cybersecurity and build a strong foundation for SOC Analyst roles in leading organizations.

🔄 IT Professionals Planning a Career Transition

System administrators, network engineers, IT support professionals, and professionals from other domains who want to move into cybersecurity.

🚀 Aspiring SOC Analysts & Security Enthusiasts

Individuals who want to learn security monitoring, incident response, SIEM platforms, threat analysis, and the skills required to work in a Security Operations Center.

📈 Working Cybersecurity Professionals

Security professionals looking to enhance their expertise in SOC operations, SIEM technologies, threat hunting, detection engineering, and real-world incident handling.

THIS TRAINING PROGRAM HELPS YOU GAIN PRACTICAL CYBERSECURITY SKILLS, UNDERSTAND REAL SOC WORKFLOWS, AND DEVELOP THE CONFIDENCE REQUIRED TO ANALYZE THREATS, INVESTIGATE INCIDENTS, AND PERFORM EFFECTIVELY IN AN ENTERPRISE SECURITY ENVIRONMENT.

WHAT WILL YOU MASTER THROUGH THIS PROGRAM?

- **Build a strong foundation in Networking & Cybersecurity** — Understand networking concepts, common attack techniques, security controls, authentication, firewalls, IDS/IPS, endpoint security, and the fundamentals required to work in a SOC environment.
- **Learn how a real SOC operates** — Understand SOC architecture, analyst responsibilities, security monitoring, alert triage, escalation procedures, incident handling, ticketing, documentation, and day-to-day SOC workflows.
- **Gain hands-on experience with SIEM technologies** — Work with Splunk Enterprise, Splunk Enterprise Security, to collect, search, analyze, correlate, and visualize security events.
- **Develop practical threat detection & investigation skills** — Investigate suspicious activities such as brute-force attacks, malware, phishing, account compromise, abnormal network behavior, and other common security incidents using real-world scenarios.
- **Learn Endpoint Detection & Response (EDR)** — Understand endpoint telemetry, process activity, suspicious behavior, detection alerts, investigation techniques, and response workflows.
- **Apply Threat Intelligence & MITRE ATT&CK** — Learn how IOCs, IOAs, threat intelligence, attacker techniques, and MITRE ATT&CK can be used to improve detection, investigation, and threat-hunting activities.
- **Practice real-world incident response** — Work through simulated security incidents from initial alert detection to investigation, evidence analysis, containment, escalation, and closure.
- **Prepare for SOC Analyst interviews & real-world roles** — Develop the ability to explain your investigations, demonstrate practical knowledge, troubleshoot security alerts, and confidently discuss SOC scenarios during interviews.
- **Learn from industry-oriented training material** — Receive customized learning resources, practical documents, investigation references, and exercises designed around the skills expected from modern SOC professionals.

FROM UNDERSTANDING A SECURITY ALERT TO INVESTIGATING AND RESPONDING TO IT, THIS PROGRAM TAKES YOU THROUGH THE COMPLETE SOC JOURNEY — GIVING YOU THE PRACTICAL KNOWLEDGE AND CONFIDENCE TO STEP INTO A CYBERSECURITY ROLE.

3 KEY OBJECTIVES OF THIS TRAINING PROGRAM

1. Become Job-Ready for SOC Analyst Roles

- Preparation with frequently asked SOC Analyst interview questions and industry-based scenarios.
- Practice real-time security incident situations that analysts face in enterprise environments.
- Understand the complete responsibilities and daily workflow of a SOC Analyst.
- Build strong knowledge of networking, cybersecurity concepts, SIEM, EDR, threat intelligence, and incident response.
- Develop the ability to explain security investigations confidently during technical interviews.

2. Gain Practical Experience Through Real SOC Environment Training

- Hands-on learning with industry-relevant security platforms including Splunk, Splunk Enterprise Security, EDR solutions.
- Perform practical exercises on alert monitoring, investigation, threat detection, and incident handling.
- Experience real SOC workflows including ticket management, escalation process, documentation, and reporting.
- Work on simulated enterprise security incidents to understand how security teams operate.

3. Build Your Career & Increase Job Opportunities

- Guidance on creating a professional SOC Analyst resume aligned with industry expectations.
- Support in optimizing LinkedIn profiles and professional cybersecurity presence.
- Learn effective job search strategies for SOC Analyst and cybersecurity roles.
- Understand how recruiters evaluate cybersecurity candidates and what skills companies look for.
- Become part of a professional learning community with continuous career guidance and opportunities.

OUR GOAL IS NOT JUST TO TEACH CYBERSECURITY CONCEPTS, BUT TO TRANSFORM LEARNERS INTO CONFIDENT SOC PROFESSIONALS WHO CAN HANDLE REAL-WORLD SECURITY CHALLENGES AND BUILD SUCCESSFUL CAREERS IN CYBERSECURITY.

jotHUB
A Professional Job Oriented Training Hub

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 USING CORRELATION SEARCHES AND NOTABLE EVENTS

8 END POINT DETECTION & RESPONSE (EDR)

9 AI FOR SOC ANALYSTS

10 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

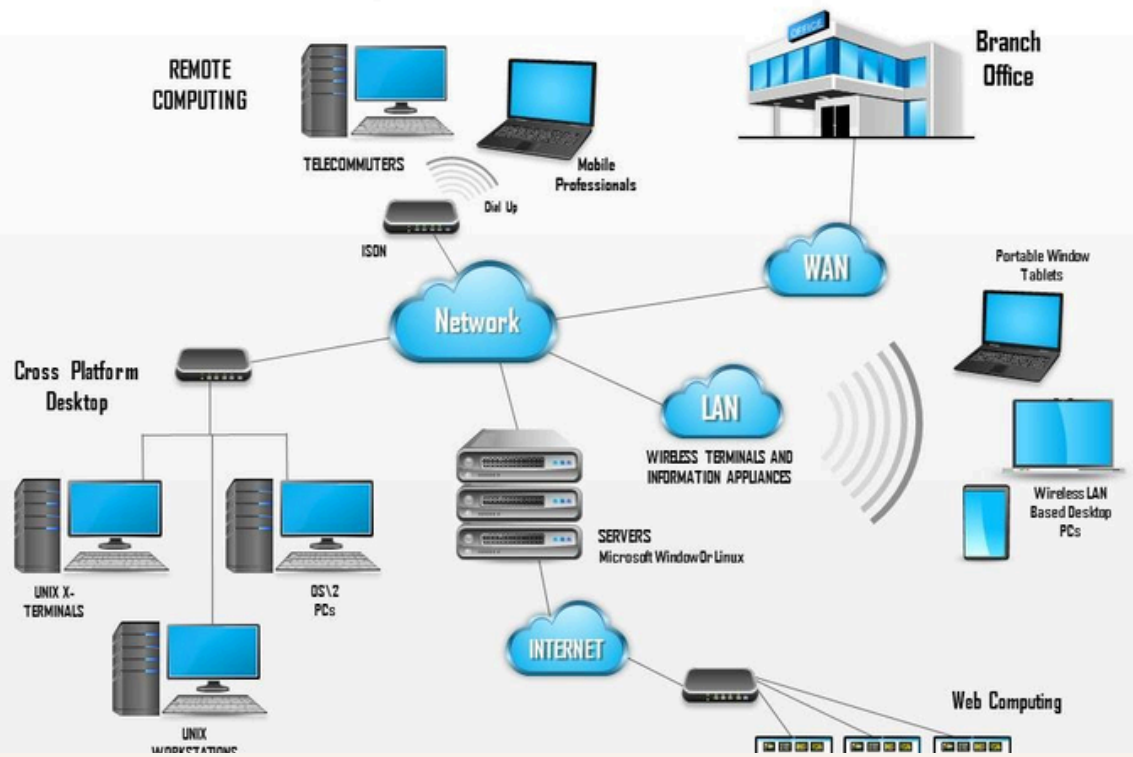
02 NETWORKING CONCEPTS FOR SOC ANALYSTS

2.1 Introduction to Organizational Networks

— Network Fundamentals: LAN, WAN, VPN

— Network Devices: Routers, Switches, Firewalls

— Importance of Network Security Monitoring



Course Modules

01 COURSE INTRODUCTION

— Overview & Objectives

— Course Structure & Learning Path

— Understanding SOC Analyst Role

— High-Level Overview of Splunk ES

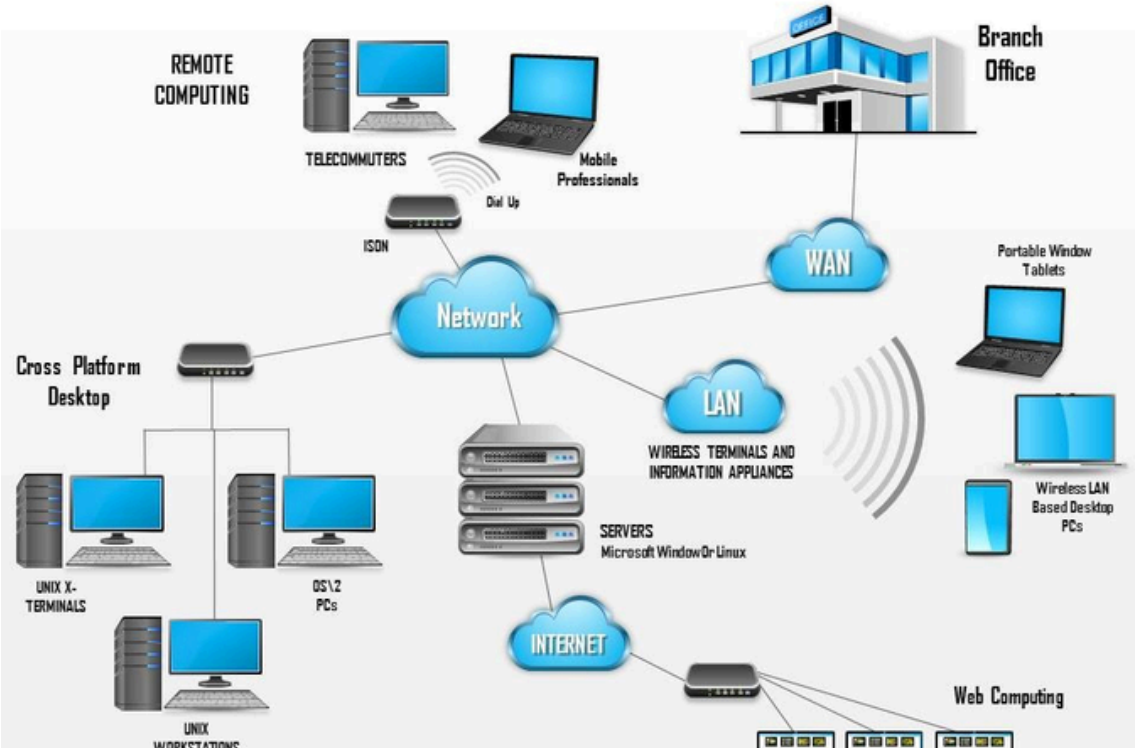
02 NETWORKING CONCEPTS FOR SOC ANALYSTS

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

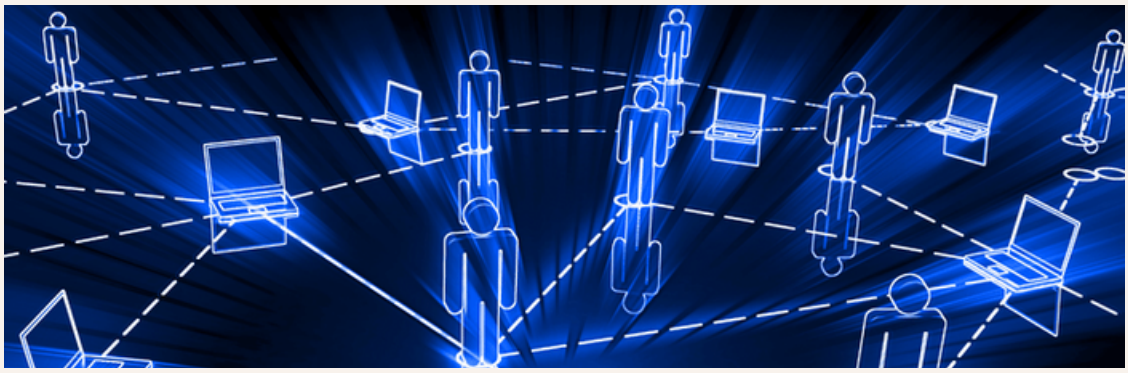
— Identifying Suspicious IP Traffic

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)

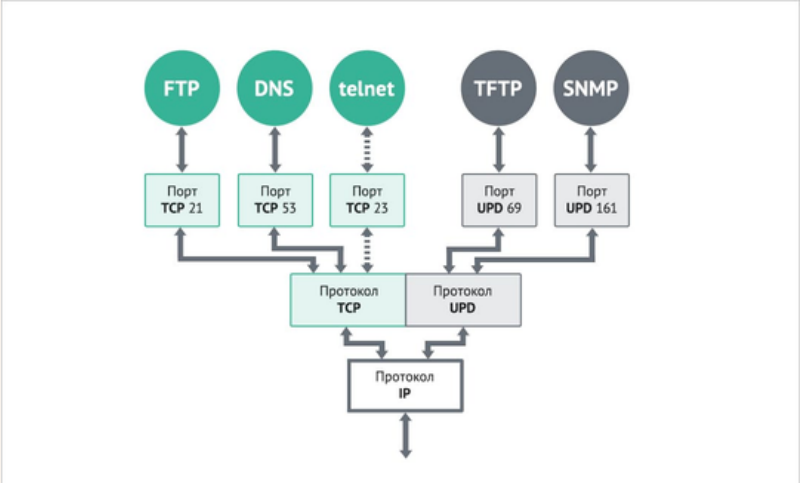
— SMTP (25) – Email Spoofing & Phishing

— 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

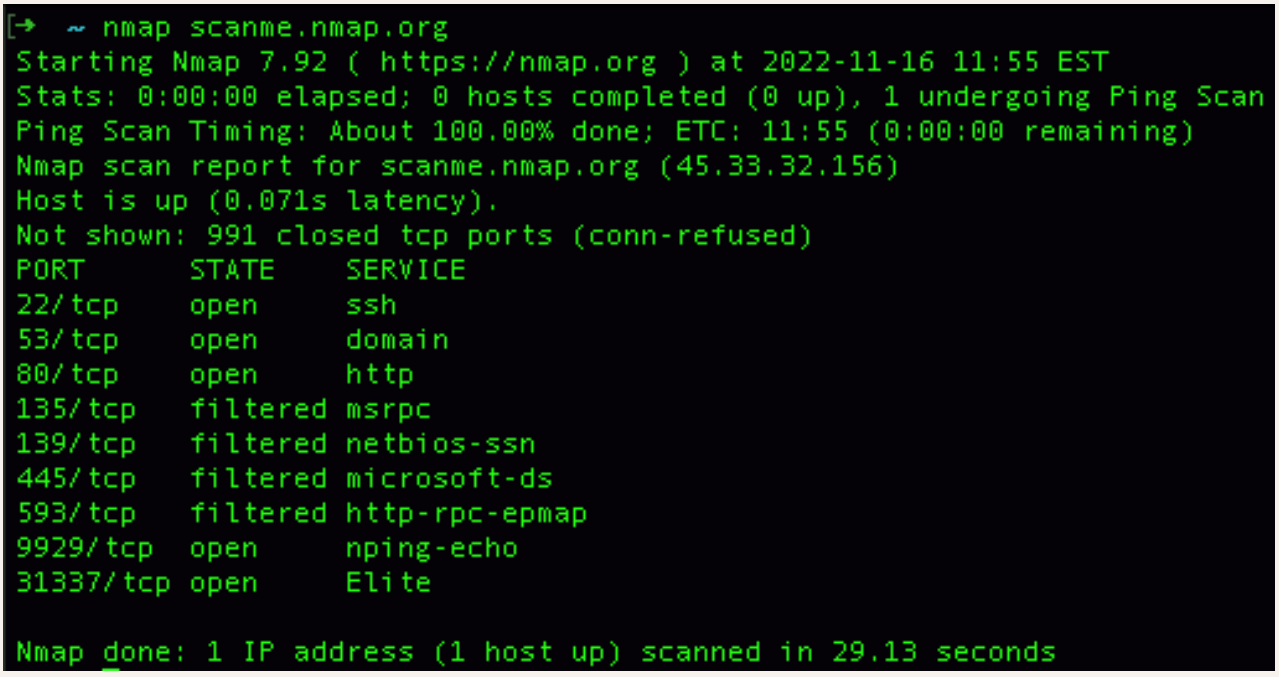
— PowerShell – Security Auditing

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)

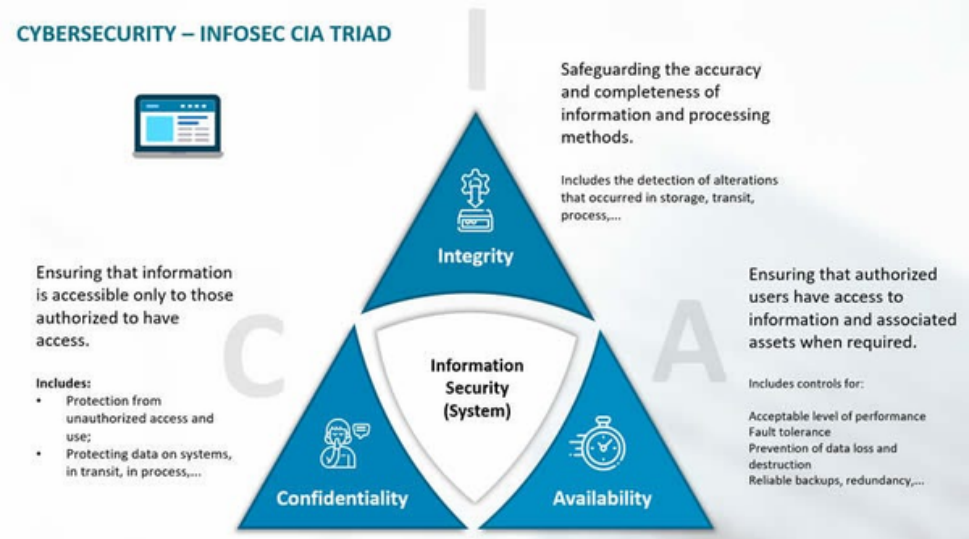
— Symmetric vs. Asymmetric Encryption (AES, RSA)

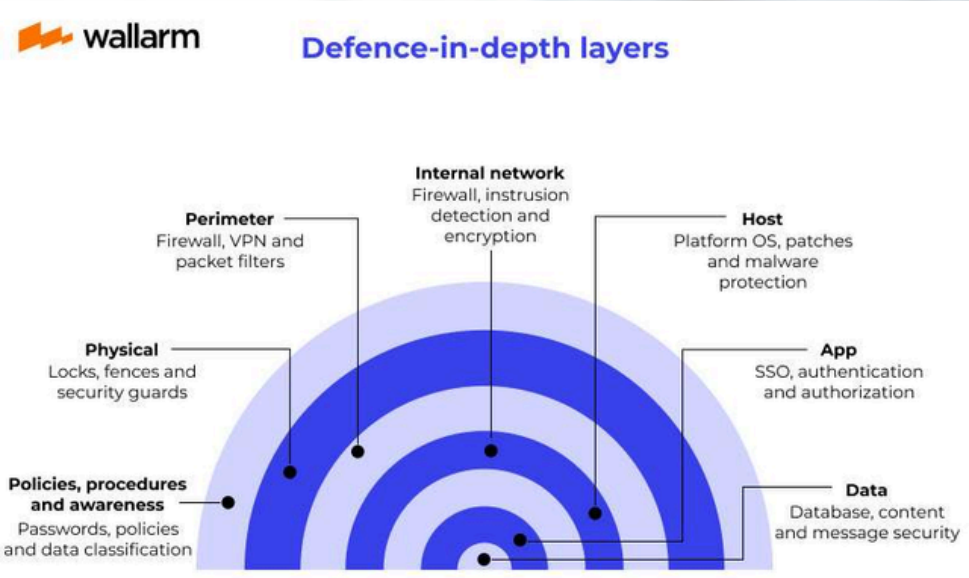
— Hashing Algorithms (MD5, SHA-1, SHA-256)

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

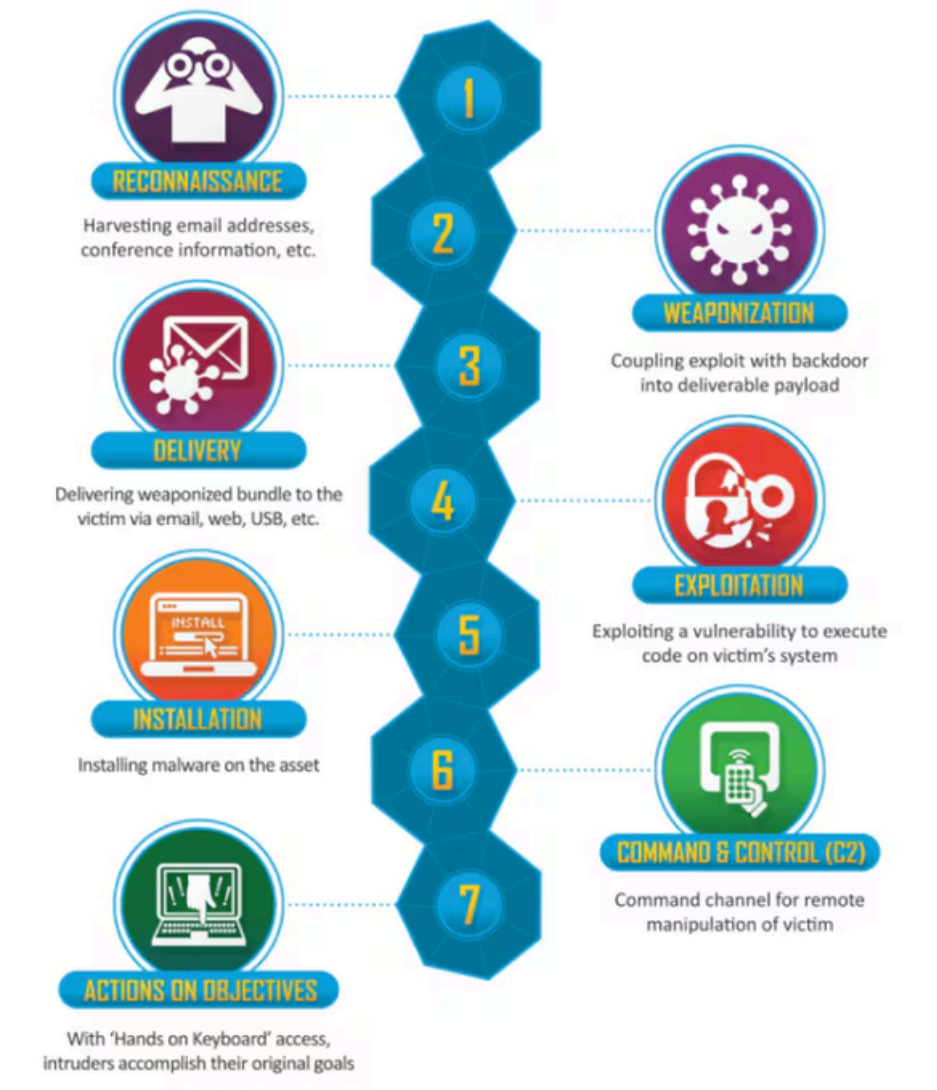
— Delivery

— 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

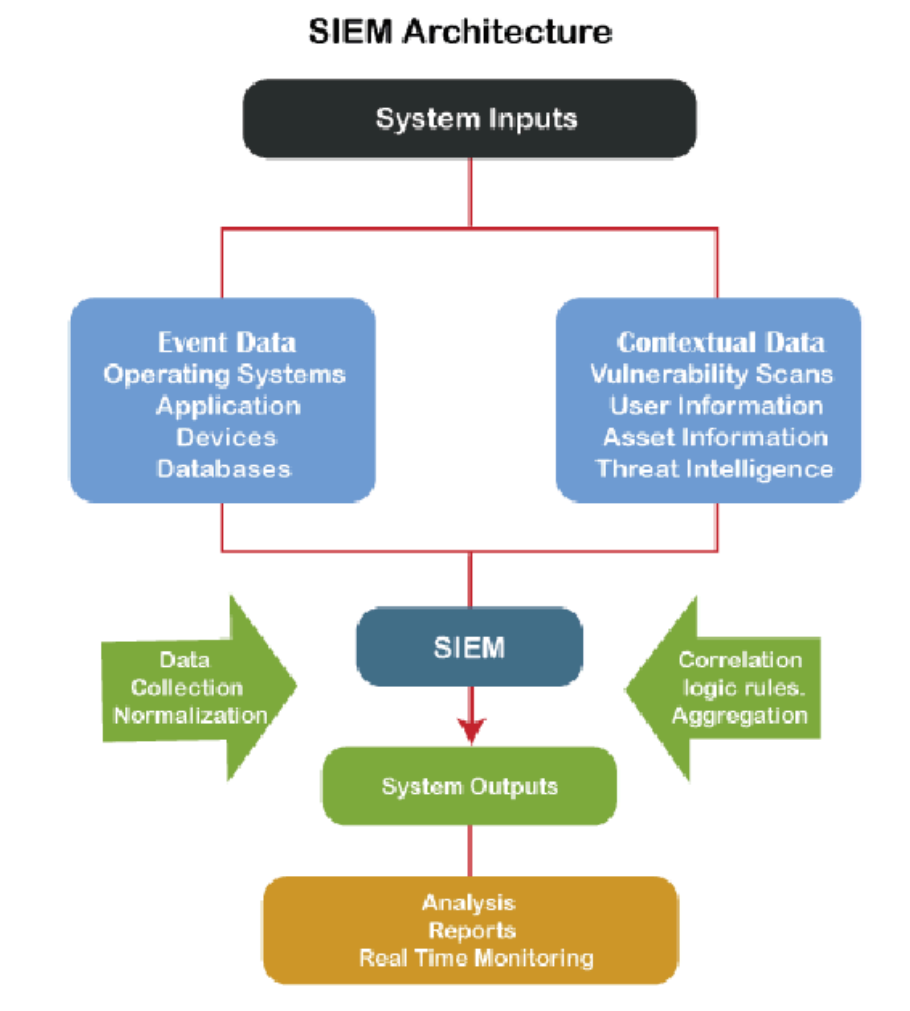
— Splunk Enterprise vs. Universal Forwarder

— 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)

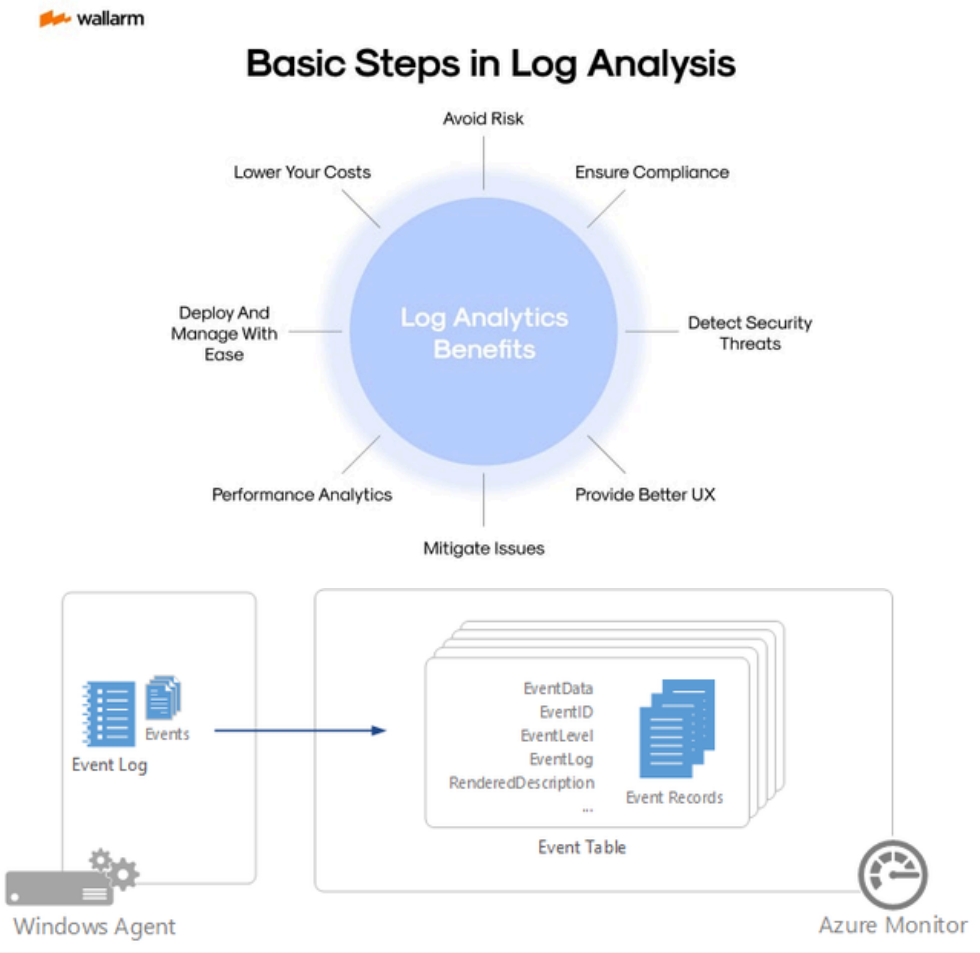
— HTTP Logs

— 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)

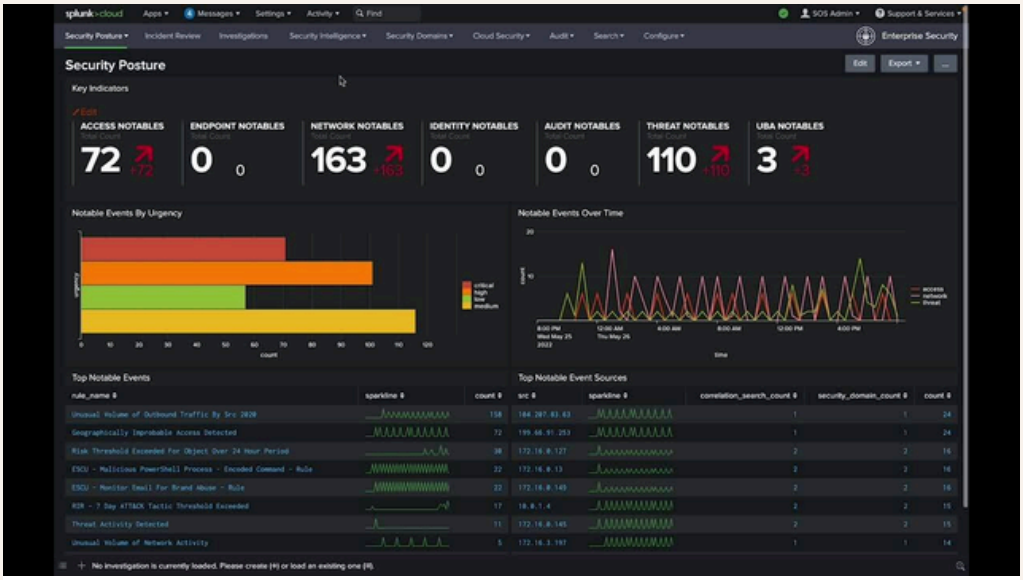
— Best practices for dashboard layout and usability

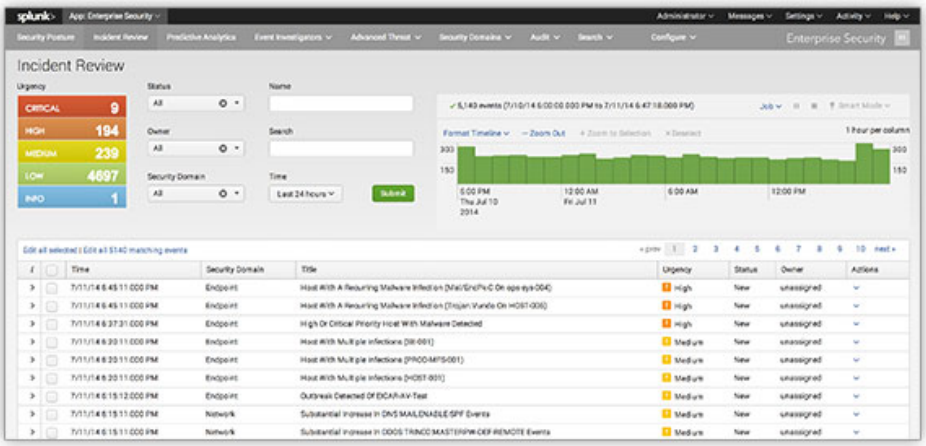
5.2 Custom Alerts & Correlation Rules

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

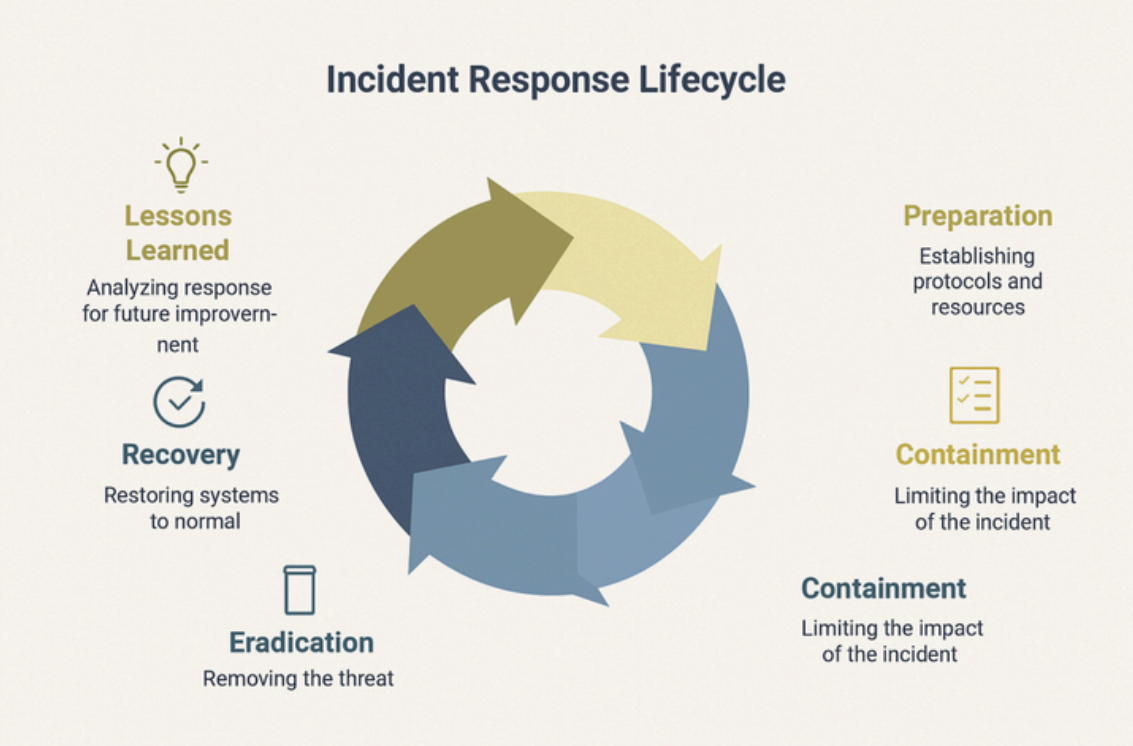
— Detection & Analysis

— Containment

— Eradication

— Recovery

— Lessons Learned



Course Modules

07 THREAT HUNTING

7.1 Proactive Threat Hunting Techniques

— Threat Hunting using Correlation Searches
— Threat Hunting using Notable Events
— Web Server Scanning Attack Analysis
— Brute Force Attack Investigation
— Email Header Analysis (Tracking Phishing Origins)

Course Modules

08 END POINT DETECTION & RESPONSE (EDR)

8.1 EDR Fundamentals

—What is EDR?
—Why EDR is required in a modern SOC
—EDR vs Traditional Antivirus
—EDR vs Next-Generation Antivirus (NGAV)
—EDR vs XDR
—EDR vs SIEM
—EDR architecture
—EDR agent and endpoint
—Role of EDR in the SOC

8.2 Endpoint Visibility & Telemetry

—What endpoint telemetry means
—Process creation events
—Parent-child process relationships
—Command-line telemetry
—File creation/modification events
—Registry activity
—Windows services
—Scheduled tasks

8.3 Understanding Process Trees

—What is a process tree?
—Parent vs child processes
—Normal vs suspicious process chains

Course Modules

08 END POINT DETECTION & RESPONSE (EDR)

8.4 EDR Detection Concepts

—Signature-based detection
—Behavioral detection
—IOC-based detection
—IOA-based detection
—Rule-based detection

8.5 MITRE ATT&CK + EDR

—Introduction to MITRE ATT&CK
—Mapping endpoint activity to ATT&CK
—Execution techniques
—Privilege escalation
—Credential access
—Lateral movement
—Command and control
—Exfiltration

8.6 EDR Response

—What is endpoint response?
—Kill a malicious process
—Quarantine a file
—Delete/remediate malware
—Isolate an endpoint
—When should a SOC analyst isolate an endpoint?
—When should an analyst not isolate an endpoint?
—EDR containment workflow

Course Modules

08 END POINT DETECTION & RESPONSE (EDR)

8.7 EDR + Threat Intelligence

—IOC fundamentals
—File hashes
—IP addresses
—Domains
—URLs
—Hash reputation
—IP/domain reputation
—Threat-intelligence feeds
—IOC vs IOA
—Using threat intelligence during EDR investigation

09 AI FOR SOC ANALYSTS

—Role of AI in Cyber security & Security Operations.
—Getting started with AI
—Using AI for Use case creation and log search for SIEM
—Using ChatGPT for Incident response
—Incident investigation using AI
—File based analysis
—Phishing email analysis
—Malware analysis using AI
—AI as Threat intelligence agent
—Interview & resume preparation using OpenAI.

Course Modules

10 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

kiranambadasu@jothub.in