



BATCH - 03

Powered SOC Analyst Practical Bootcamp

Defend smarter, respond faster

12 CPEs

Hands-on SOC Tools

Real Attack Scenarios

Incident Response



VIRUSTOTAL



Hugging Face



Deep Hat

Why Attend?

Modern cyber threats move fast, and SOC teams are expected to detect, investigate, and respond in real time. This bootcamp delivers hands-on experience in how real SOC environments operate, from SIEM-based detection to incident response and threat intelligence. It goes beyond theory by using real attack scenarios, log analysis, and investigation workflows.

The program also introduces how AI is transforming SOC operations through faster alert triage, log analysis, and threat insights. Designed for practical learning, it builds the skills needed to handle real-world security incidents confidently.

What sets this training apart:

Hands-On & Practical Learning

Focused on real-world SOC scenarios and exercises

Real SOC Workflows

Learn detection, triage, escalation, and response end-to-end

AI-Driven SOC Insights

Use AI for faster analysis, triage, and investigation support

SIEM & Log Mastery

Build strong foundations in log analysis and correlation

Incident Response Readiness

Understand how real incidents are handled and escalated

Career Growth

Earn 12 CPEs and strengthen your foundation for SOC career opportunities

Key Takeaways



Earn 8 CPE Credits



Understand SOC fundamentals, roles, and workflows



Explore AI applications in modern SOC operations



Learn SIEM basics and log correlation techniques



Gain hands-on experience with real security logs



Understand the incident response lifecycle and processes

Meet the Speaker



Sanyam

10+ Years of Experience

CEH | CSA | CND | CHFI | CTIA | CCISO | SOC | Security + Pentest +

Sanyam brings over a decade of expertise in cyber defense, web application security, and threat hunting. Known for his hands-on teaching and operational depth, he has mentored numerous professionals to transition into active SOC and DFIR roles.

His specializations include:

- Web App Security & Advanced Penetration Testing (Metasploit, Burp Suite, Nessus, Nmap)
- Threat Intelligence & Incident Response aligned with the Cyber Kill Chain
- Digital Forensics & Memory Analysis using Volatility and OSINT-based investigations
- SIEM and Endpoint Detection tools for monitoring and response
- Secure SDLC, DevSecOps implementation, and automation with Python & Shell scripting
- Cloud Security across AWS, GCP, and OVH platforms

Sanyam's sessions are highly practical and interactive, combining demos, challenges, and real investigation workflows drawn from real-world SOC environments.

Bootcamp Agenda

Day 1: SOC Foundations & Security Basics

- Information Security fundamentals (CIA triad)
- SOC architecture, roles (L1/L2/L3)
- SOC workflows (monitor → detect → respond)
- Security tools overview (SIEM, EDR, Threat Intel)

Day 2: SIEM & Log Analysis

- SIEM fundamentals (log ingestion, correlation)
- Log analysis techniques
- Alert triage workflow
- Use cases:
 - Failed login detection
 - Suspicious IP activity

Practical

- Work on:
 - Sample logs (Windows/Linux/auth logs)
 - Splunk-like queries:
 - Search logs
 - Filter anomalies
- Identify:
 - Brute force attack pattern
 - Suspicious login behavior

Day 3: Incident Response & Threat Intelligence

- Incident response lifecycle (NIST model)
- Alert escalation (L1 → L2 flow)
- Threat intelligence basics:
 - IOC vs TTP
 - Threat feeds

Practical

- Analyze:
 - Phishing email sample
 - Extract IOCs (IP, domain, hash)
- Enrich using:
 - VirusTotal
- Decide:
 - Severity level
 - Escalation path

Day 4: Digital Forensics + Threat Hunting + AI in SOC

Part 1: Digital Forensics

- What is Digital Forensics (SOC perspective)
- Types:
 - Endpoint forensics
 - Memory vs disk artifacts (high-level only)
- Key forensic artifacts:
 - Windows Event Logs
 - Process execution (cmd, PowerShell)
 - Login traces

Part 2: Threat Hunting

- Difference:
 - Detection vs Hunting
- Hypothesis-driven hunting
- Indicators vs behaviors
- Mapping to MITRE ATT&CK

Part 3: AI in SOC Operations

- Role of AI in SOC:
 - Alert triage automation
 - False positive reduction
 - Log summarization
- Practical SOC use cases:
 - Convert raw logs → human-readable insights
 - IOC summarization
 - Threat report drafting

Practical / Demo

1. Memory Analysis using Volatility Framework

2. Use AI to:

- Summarize incident
- Identify suspicious patterns
- Generate response recommendations



Contact us

 sales@infosectrain.com

 www.infosectrain.com