

AI SOC ANALYST

Certification Training



Tools



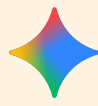
ChatGPT



Anthropic
Claude



Google AI
Studio



Gemini



Crew AI



Hugging Face



Ollama



LMStudio



Groq



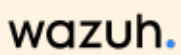
MITRE ATT&CK
Navigator



Nmap



MISP



Wazuh



Splunk



Microsoft
Sysinternals



FTK Imager



Terminal/Shell



Volatility



Maltego



Metasploit



Cyberchef



Wireshark



AlienValut



ITSM tool



Mx Toolbox



ELK



OpenVAS



Python



Suricata



Microsoft
Sentinel

Many
more...

Course Highlights



48-Hour LIVE Instructor-led Training



Beginner-to-job-ready learning path



Hands-on SIEM and log analysis (Splunk, ELK, Windows Event Logs)



AI-assisted SOC workflows



Practical phishing, malware, and threat labs



40+ Tools and Real-world SOC Case Studies



Vulnerability assessment and reporting practice



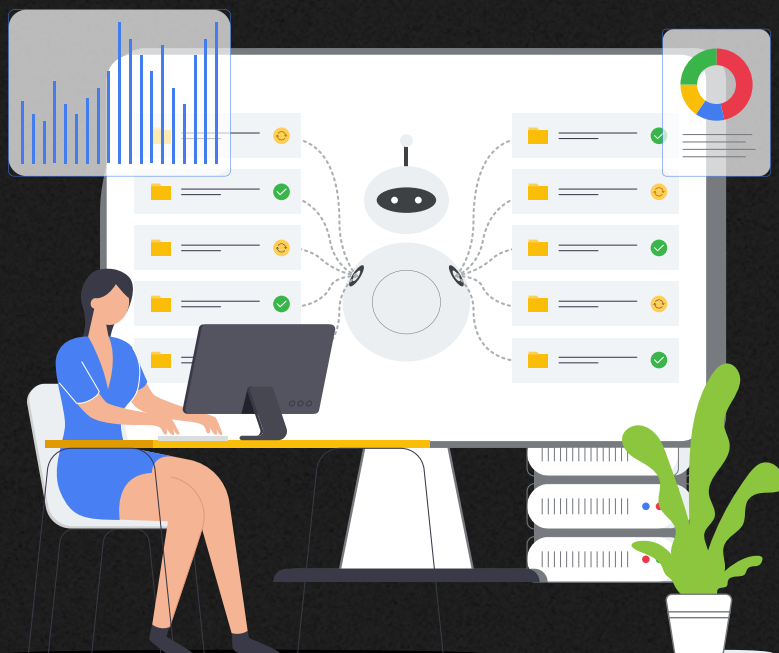
Mentoring & Post-training Support



Access to Recorded Sessions

About Course

The AI SOC Analyst Certification Training by InfosecTrain teaches participants how modern SOC's leverage AI to speed detection, reduce false positives, perform automated investigation, and improve response accuracy. The program explains SOC functions, network security foundations, threat intelligence, log analysis, vulnerability assessment, phishing & malware analysis, and AI-driven responses. Participants gain practical experience through guided labs using SIEM tools, AI models, and real security datasets.



Course Objectives

You will be able to:

- ✓ Build foundational SOC analysis skills with AI
- ✓ Use AI for alert triage, log summaries and investigations
- ✓ Detect phishing, analysing malware and anomalies with AI support
- ✓ Automate vulnerability reporting and IOC enrichment
- ✓ Assist in IR workflows using AI models
- ✓ Enhance SOC productivity with AI-driven tools



Target Audience

- ✓ Aspiring SOC Analysts (L1)
- ✓ Cybersecurity beginners entering SOC roles and aiming to use AI tools effectively
- ✓ Junior Security Analysts working with logs and alerts
- ✓ IT professionals transitioning into SOC operations
- ✓ Fresh graduates aiming for entry-level SOC positions

Pre-Requisites

- ✓ Basic understanding of networking & cybersecurity fundamentals
- ✓ Familiarity with Windows/Linux basics
- ✓ Suitable for beginners with no SOC or AI background



Exam Information

Certification Body	InfosecTrain
Exam Format	Multiple-choice Questions and Practicals
Number of Questions	50 Questions
Exam Duration	6 Hours
Passing Score	80%
Exam Language	English
Testing Mode	Online

Disclaimer: This is an InfosecTrain Certified Program, and all examinations and certifications are conducted and awarded solely by InfosecTrain.



Course Content

Module 1

Introduction to SOC

- ✓ What is a SOC?
 - ✓ Definition, role in cybersecurity defense
 - ✓ SOC structures: Centralized, Distributed, Virtual SOC's
- ✓ SOC Analyst Roles
 - ✓ L1: Monitoring, triage, escalation
 - ✓ L2 & L3: Deep investigation, threat hunting, forensics
- ✓ Key SOC Functions
 - ✓ Log monitoring, alert triage, threat detection, incident response
- ✓ SOC Maturity Model
 - ✓ From reactive → proactive → predictive SOC

Common SOC Tools

- ✓ SIEM, EDR, Threat Intel Platforms, Open-Source Security Analyst oriented models

Module 2

Introduction to AI for Cybersecurity

- ✓ What is AI?
 - ✓ AI vs ML vs DL vs NLP vs LLM
 - ✓ Predictive AI vs Generative AI
- ✓ Why AI in Cybersecurity?
 - ✓ Reducing false positives, handling large datasets, automated response
- ✓ AI in SOC – Use Cases
 - ✓ Log summarization, phishing detection, anomaly detection
 - ✓ AI-driven report generation, automated playbooks
- ✓ AI Limitations in SOC
 - ✓ Hallucinations, bias, explainability, data privacy concerns
- ✓ Open-Source and Free-Tier AI Tools
 - ✓ Free Tier proprietary LLMs, Ollama, LMStudio, Hugging Face models

Lab

- ✓ **Run an LLM locally (Phi-3 Mini / Mistral via Ollama)**
→ ask it to summarize sample Windows Event logs and classify alerts.

Module 3

Network Security & Threat Landscape

- ✓ Basics of Networking for SOC
 - ✓ OSI model, TCP/IP, ports & protocols
 - ✓ Common attacks (DDoS, brute force, phishing, ransomware)
 - ✓ Case studies of famous attacks
- ✓ Threat Intelligence
 - ✓ Threat intelligence types
 - ✓ IOC (Indicators of Compromise)
 - ✓ MITRE ATT&CK for SOC Analysts
- ✓ AI in Threat Intel
 - ✓ Using AI to summarize threat feeds
 - ✓ AI-assisted correlation of IOCs

Labs

- ✓ Gathering Threat Intel feeds using AI.
- ✓ Capture sample PCAP in Wireshark → use Python + AI model to identify anomalies

Module 4

AI in Vulnerability Management & Assessment

- ✓ Vulnerability Management Basics
 - ✓ What is a vulnerability? CVE, CVSS, exploitability
 - ✓ VM lifecycle: Scan → Assess → Prioritize → Remediate → Report
 - ✓ **Tools overview: Nessus (pro), OpenVAS (free), Nmap + NSE scripts**
 - ✓ SOC Analyst role vs. vulnerability management team
- ✓ AI in Vulnerability Assessment
 - ✓ AI for CVE explanation: simplify technical CVEs into analyst-friendly notes
 - ✓ AI for prioritization: map severity + exploitability + asset criticality
 - ✓ AI for remediation recommendations: patch, config change, or mitigation
 - ✓ AI in report drafting for management/non-technical audience

Labs

- ✓ **OpenVAS/NMAP Scan + AI Explanation**
- ✓ **AI-Generated Vulnerability Report**

Module 5

SIEM & AI-Assisted Log Analysis

- ✓ SIEM Fundamentals
 - ✓ Architecture, log sources, parsing, correlation rules
 - ✓ Popular tools: Splunk, ELK, Microsoft Sentinel
- ✓ Challenges in Log Analysis
 - ✓ High volume, repetitive patterns
- ✓ AI Integration
 - ✓ AI for log summarization and anomaly detection
 - ✓ ChatGPT prompt engineering for SIEM queries
 - ✓ AI-driven “Explain this log” and “Generate query”

Labs

- ✓ AI-powered analysis of Windows Event Logs (4624, 4625, 4670, etc.)
- ✓ Using AI to generate Splunk queries and summarize alerts
- ✓ Parse Suricata logs to elk via filebeat and use AI model to detect network Attack (Malicious Log detector to generate alerts)

Module 6

Phishing, Malware, and Insider Threats

- ✓ Phishing
 - ✓ Types (email, smishing, vishing, spear phishing, whaling)
 - ✓ Real case studies (Norfund, Colonial Pipeline)
- ✓ Malware
 - ✓ Introduction to Malware
 - ✓ Types of Malware
 - ✓ Malware Family Naming
 - ✓ Behavioral detection vs signature-based detection
- ✓ Insider Threats
 - ✓ Privilege misuse, data exfiltration patterns
- ✓ AI in Detection
 - ✓ AI-based phishing email detection
 - ✓ AI chatbot for suspicious email reporting
 - ✓ AI in malware recognition

Labs

- ✓ AI-based phishing email classification
- ✓ AI for static malware analysis

Module 7

Incident Response with AI

- ✓ IR Lifecycle
 - ✓ Preparation → Detection → Containment → Eradication
 - ✓ → Recovery → Lessons Learned
- ✓ AI in IR
 - ✓ AI-guided playbooks
 - ✓ Automating IOC enrichment (IP/URL/domain lookups)
 - ✓ AI-assisted RCA (Root Cause Analysis)

Labs

- ✓ Using AI to Assist in Phishing Incident Response
- ✓ Network Traffic Analysis using Wireshark + AI



Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on



www.infosectrain.com