SYLLABUS

CYBER SECURITY · COURSE HANDOUT 2026

SOC ANALYST

EM . LOG ANALYSIS . TRIAGE
MITRE ATT&CK . DETECTION
DENT RESPONSE . THREAT I

DURATION	LEVEL	MODULES	MODE
60 Hours	**Beginner to Advanced**	**8**	**Classroom · Online · Hybrid**

01 COURSE OVERVIEW

A security operations centre course built around alert triage, investigation and escalation. Learners work as a tier-one analyst would: reading logs, triaging alerts in a SIEM, mapping activity to MITRE ATT&CK, deciding what to escalate and writing the case notes that follow it.

The course runs on Splunk and Wazuh with simulated attack data, and closes with a timed incident simulation.

WHO IT IS FOR

- Graduates entering security operations
- IT support staff moving to security
- Network administrators on shift teams
- Analysts preparing for blue team roles

PREREQUISITES

Basic networking, Windows and Linux familiarity.

02 LEARNING OUTCOMES

01 Read and correlate Windows, Linux and network logs.

02 Triage alerts by severity and business impact.

03 Investigate with a SIEM and document findings.

04 Map observed behaviour to MITRE ATT&CK techniques.

05 Write detection rules and tune false positives.

06 Follow an incident response playbook.

07 Escalate with a clear, evidenced handover.

03 MODULE STRUCTURE

8 MODULES

01 SOC OPERATIONS

- SOC tiers and roles
- Ticketing
- Escalation paths
- Shift handover
- SLAs
- Documentation standards

02 LOG SOURCES

- Windows event logs
- Linux auditd
- DNS logs
- Sysmon
- Firewall and proxy logs
- Cloud logs

LAB

LOG WALKTHROUGH

03 SIEM FUNDAMENTALS

- Ingestion and parsing
- Search queries
- Correlation rules
- Normalisation
- Dashboards

TOOLS

SPLUNK · WAZUH · ELK STACK

04 ALERT TRIAGE

- Alert anatomy
- Enrichment
- Case notes
- True vs false positive
- Priority matrix

LAB

TRIAGE QUEUE EXERCISE

05 THREAT FRAMEWORKS

- MITRE ATT&CK
- Tactics and techniques
- Gap analysis
- Kill chain
- Detection coverage mapping

06 DETECTION ENGINEERING

- Rule writing
- Thresholds and baselines
- Testing detections
- Sigma rules
- Tuning

LAB

CUSTOM DETECTION RULE

07 THREAT INTELLIGENCE

- IOCs and IOAs
- Reputation lookups
- Malware triage basics
- Feeds
- Phishing analysis

TOOLS

VIRUSTOTAL MISP

08 INCIDENT RESPONSE

Playbooks	Containment decisions
Forensic capture	Communication
Reporting	Lessons learned

PROJECT

TIMED INCIDENT SIMULATION AND REPORT

04 ASSESSMENT & CERTIFICATION

Module assignments and labs	**25%**
Mini projects	**20%**
Internal assessments	**15%**
Final project and review	**40%**

CERTIFICATION

Learners who complete all modules, submit the final project and clear the review receive a course completion certificate from Kaizen Infinities Private Limited. Project work is documented for the learner's portfolio, and interview preparation is included in the closing sessions.

05 CAREER OUTCOMES

ROLES THIS PROGRAMME PREPARES FOR

SOC ANALYST (TIER 1/2) **SECURITY OPERATIONS ENGINEER** **INCIDENT RESPONSE ANALYST**
THREAT DETECTION ENGINEER **CYBER SECURITY ANALYST**

CALL US
+91 73051 33996

EMAIL US
apply@kaizeninfinities.com

VISIT OUR WEBSITE
www.kaizeninfinities.com