Jaipur Engineers
Your One-Stop IT & Staffing Ecosystem

CYBER SECURITY

SOC Analyst

SAMPLE PROJECT

Alert Triage and Incident Timeline



COURSE FEE

Fee on enquiry

JAIPUR, RAJASTHAN

+91 70146 92039

SOC Analyst

Core concepts



01

SOC roles, workflows and escalation criteria

02

Endpoint, identity and network log sources

03

SIEM queries and event correlation

Review the scope

Identify assets and trust boundaries in a supplied scenario.

SOC Analyst

Applied skills

- **Assets**
- **Controls**
- **Evidence**



04 Alert triage, severity and false-positive review

05 Incident timeline, containment and evidence handling

06 Detection tuning, metrics and handover reports

PROJECT DELIVERABLES

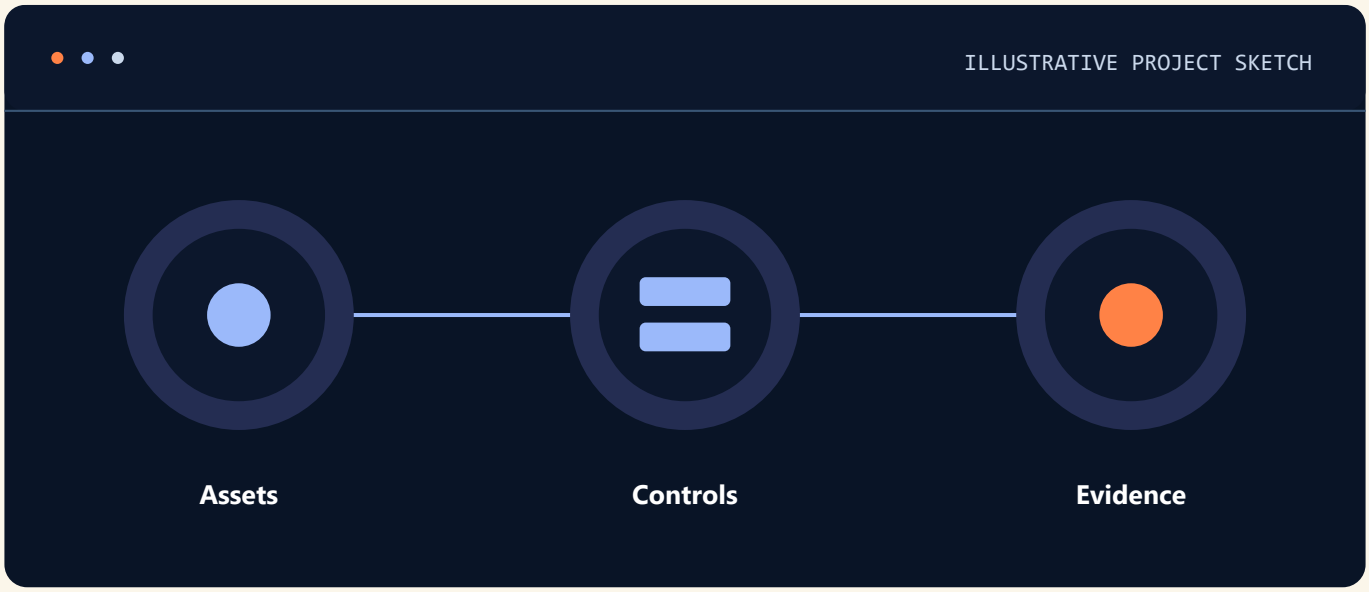
A security review, prioritised mitigations and the evidence needed to verify each fix.

SOC Analyst

Portfolio project

Alert Triage and Incident Timeline

Review synthetic endpoint and sign-in logs to decide which alerts to escalate and document the timeline.



Review the scope

Identify assets and trust boundaries in a supplied scenario.

Prioritise fixes

Rank the supplied findings and describe evidence for verifying each mitigation.

A security review, prioritised mitigations and the evidence needed to verify each fix.

SOC Analyst

Course fees

COURSE FEE

Fee on enquiry

Ask admissions for the course fee, available batches and enrolment details.

ADMISSIONS

+91 70146 92039

info@jaipurengineers.com

122/228, Indra Path, Thadi Market

Mansarovar, Jaipur, Rajasthan 302020

SCAN FOR MAP

Check course details

SOC Analyst

Course content

MODULES 01–02

01

Lessons & practice

- SOC roles
- Workflows
- Escalation criteria

HANDS-ON Write working escalation criteria for a practice alert queue.

02

Lessons & practice

- Endpoint
- Identity
- Network log sources

HANDS-ON Identify which identity, network and endpoint events support a sample incident timeline.

SOC Analyst

Course content

MODULES 03–04

03

Lessons & practice

- SIEM queries
- Event correlation

HANDS-ON Correlate synthetic logs by time and asset to investigate a supplied alert.

04

Lessons & practice

- Alert triage
- Severity
- False-positive review

HANDS-ON Separate a likely incident from a false positive and document the reasoning.

SOC Analyst

Course content

MODULES 05–06

05

Lessons & practice

- Incident timeline
- Containment
- Evidence handling

HANDS-ON

Build a timeline and recommend a containment action and preservation of evidence.

06

Lessons & practice

- Detection tuning
- Metrics
- Handover reports

HANDS-ON

Review detection quality and prepare a handover with metrics and open tasks.