SYLLABUS FOR BOARD OF STUDIES ADOPTION — generated from the live catalogue record

Security Operations Centre Analyst Simulation

S-05B · 3 days (configurable 1–5 days) · Informatics · Security · Years: 2nd, 3rd, PG

CONTENTS

1. Overview 2
2. Hours and credit position 2
3. Course outcomes 2
4. Course content — modules 2
5. Assessment scheme (100 marks) 2
6. CO–PO mapping 2
7. Every participant receives 3
8. Fee 3
9. Designed by 3

Catalogue S-05B · version 2 · generated 2026-10-09

OVERVIEW

Log analysis, SIEM basics, alert triage and a full incident response exercise.

SOC analyst is the most common entry role in cybersecurity; a realistic triage-and-response simulation makes students job-ready for a large, growing hiring pool.

HOURS AND CREDIT POSITION

Contact hours: 24 Guided project: 6 Self-study: 0 Notional total: 30

Credit claim: 1
30 notional hours ÷ 30 hours per credit (NSQF track, UGC Micro-credentials Guidelines §5.3.3) = 1 credits.

COURSE OUTCOMES

CO1. Describe the role and tiers of a security operations centre (K2)
CO2. Analyse log data to identify a suspicious event (K4)
CO3. Triage SIEM alerts by priority and enrich them with context (K4)
CO4. Apply the incident-response lifecycle to a simulated incident (K3)
CO5. Produce an incident report documenting findings and actions (K5)

COURSE CONTENT — MODULES

Hours shown are the recommended format; module time scales proportionally when the engagement runs 1–5 days.

Module 1 — SOC foundations (4h recommended)
Theory: The security operations centre, analyst tiers, the threat landscape
Lab: Map the SOC workflow
Output: SOC workflow diagram

Module 2 — Logs and telemetry (4h recommended)
Theory: Log sources, normalisation, what to collect
Lab: Normalise and read sample logs
Output: Log analysis notes

Module 3 — SIEM basics (4h recommended)
Theory: Searching, correlation rules, dashboards
Lab: Write correlation searches in a SIEM
Output: Correlation searches

Module 4 — Alert triage (4h recommended)
Theory: Prioritisation, false positives, enrichment
Lab: Triage a stream of alerts
Output: Triaged alert log

Module 5 — Incident response (4h recommended)
Theory: The incident-response lifecycle, containment, escalation
Lab: Walk an incident through the lifecycle
Output: Response runbook

Module 6 — Incident capstone (4h recommended)
Theory: A full simulated incident from alert to report
Lab: Run a simulated incident end to end
Output: Incident report

ASSESSMENT SCHEME (100 MARKS)

Continuous lab exercises — 40 marks
Capstone project & demonstration — 40 marks
Quiz & viva voce — 20 marks

CO–PO MAPPING

CO1 !' PO1 (strength 2)
The SOC model is foundational knowledge.

CO2 !’ PO4 (strength 2)
Log analysis is investigation of evidence.
CO3 !’ PO4 (strength 2)
Alert triage is investigative judgement.
CO4 !’ PO3 (strength 2)
Applying the response lifecycle is a structured solution.
CO5 !’ PO10 (strength 2)
The incident report is professional communication.

EVERY PARTICIPANT RECEIVES

- Certificate of completion
- Course material
- LMS access
- Interview question bank
- Mock interview & viva practice
- Optional nasscom NSQF assessment (priced per candidate on your quotation)

FEE

¹850 per student, incl. GST
Excludes the optional nasscom assessment where offered. Final pricing on your college's quotation.

DESIGNED BY

Venkat Kurela — Founder & Director, Kurela Cognisive Private Limited