GCC-FOCUSED · DUBAI

NG NETWORKS
TURNING ASPIRATION INTO VERACITY

CDS — Cyber Defence Specialist

16-Week Curriculum

Integrated SOC + GRC Security Analyst Programme. 48 live sessions · 96 hours · 3 evening/weekend sessions weekly · 24/7 lab portal · batch capped at 20. Each week: two taught sessions and one hands-on lab (S3); most weeks produce a portfolio artefact you keep.

PHASE 1 — SECURITY & SOC CORE (WEEKS 1–4)

1

Foundations of Security

Attacker mindset, kill chain & ATT&CK · networking for security · Lab: Wireshark packet analysis of a simulated attack

PORTFOLIO: WIRESHARK ANALYST FINDINGS NOTE

2

Operating Systems & Log Sources

Windows internals & Event IDs · Linux logs & permissions · Lab: build an attacker timeline from event logs

PORTFOLIO: WINDOWS EVENT LOG IOC SUMMARY

3

SIEM Fundamentals — Splunk

SIEM concepts · SPL queries, stats, timecharts · Lab: build a failed-logins dashboard

PORTFOLIO: SPLUNK DASHBOARD

4

SIEM — Microsoft Sentinel

Sentinel architecture · KQL & alert rules · Lab: triage 5 Sentinel incidents

PORTFOLIO: SIEM TRIAGE NOTE + QUERIES

PHASE 2 — SOC OPERATIONS (WEEKS 5–8)

5

Incident Response

NIST 800-61 lifecycle · UAE notification obligations (NESA, CBUAE) · Lab: ransomware simulation

PORTFOLIO: INCIDENT REPORT (NIST 800-61)

6

Endpoint Detection & Response

EDR telemetry & process trees · ATT&CK mapping · Lab: investigate an endpoint compromise, extract IOCs

PORTFOLIO: EDR INVESTIGATION NOTE + IOCS

7

Phishing & Email Security

SPF, DKIM, DMARC · header & URL analysis · Lab: analyse 3 phishing samples

PORTFOLIO: PHISHING ANALYSIS REPORT

8

Threat Intelligence Basics

IOCs vs TTPs, STIX/TAXII · OSINT tools · Lab: profile a threat actor

PORTFOLIO: THREAT ACTOR INTELLIGENCE NOTE

PHASE 3 — GRC CORE (WEEKS 9–13)

9 **ISO 27001 & ISMS**
ISO 27001:2022 clauses & Annex A · gap methodology · Lab: assess 10 controls for a case-study organisation
PORTFOLIO: ISO 27001 GAP ASSESSMENT

10 **Risk Management**
ISO 27005 / NIST RMF · register structure · Lab: build and populate a risk register
PORTFOLIO: RISK REGISTER

11 **Security Policy & Governance**
Policy hierarchy · writing effective policy · Lab: draft a complete Acceptable Use Policy
PORTFOLIO: SECURITY POLICY

12 **UAE & GCC Regulation**
NESA IA Standards · CBUAE CSCF · PDPL · Lab: build a compliance obligation register
PORTFOLIO: COMPLIANCE OBLIGATION REGISTER

13 **Third-Party Risk, BCM & Audit**
TPRM & vendor tiering · BIA, RTO/RPO · Lab: vendor assessment + BIA + audit findings
PORTFOLIO: VENDOR RISK ASSESSMENT · BIA · EXECUTIVE RISK REPORT

PHASE 4 — INTEGRATION & LAUNCH (WEEKS 14–16)

14 **Integrated Capstone**
Simulated financial-services breach — incident report + risk register update + compliance note
PORTFOLIO: INTEGRATED SOC + GRC CAPSTONE

15 **Executive Communication**
Communicating risk to the board · Lab: convert an incident into a 1-page board paper
PORTFOLIO: BOARD PAPER

16 **Career Launch & Mock Interview**
Portfolio & LinkedIn review · SOC + GRC interview bank, STAR technique · recorded mock interview with feedback
PORTFOLIO: INTERVIEW READINESS

The complete 6-month journey

Month 1: Foundation Bridge (career changers) → Months 2–5: this 16-week core → Month 6: Career Sprint & Placement — CV rebuild, mock interviews and employer submissions across the UAE and GCC, with support until you are placed. Certification alignment: CompTIA Security+ & CySA+ · ISO 27001 LA/LI · CISA foundation.

Programme fee: 15,000 AED — everything included · Batch capped at 20

Start your admission: admission@ngnetworks.in · ngnetworks.ae

We don't sell courses. We architect careers.