FORMATION COURTE · NIVEAU 2 · ELIGIBLE CPF

Cybersecurite Operationnelle — SOC & SIEM

Operez un SOC, analysez les logs SIEM, detectez et repondez aux incidents

FICHE FORMATION

Duree
3 jours (21h)

Tarif
1 590 EUR — Prix de lancement

Financement
CPF / Plan formation / OPCO

Modalite
Distanciel ou Presentiel

Prerequis
Formation Cyber Niveau 1 + notions reseaux TCP/IP

Organisme
ISEIG — NDA 11922503292

Objectifs de la formation

- Comprendre larchitecture et le fonctionnement dun SOC
- Utiliser un SIEM pour collecter, corréler et analyser les logs de securite
- Detecter les indicateurs de compromission (IOC) et les anomalies
- Conduire une investigation forensique de base
- Produire des rapports dincidents professionnels

Programme detaille

Jour 1 — Architecture SOC & Threat Intelligence

- Organisation dun SOC : tiers 1/2/3, processus, SLA
- Sources de Threat Intelligence et flux IOC
- MITRE ATT&CK; : frameworks et cas dusage

Jour 2 — SIEM en pratique

- Installation et configuration Microsoft Sentinel
- Regles de detection et alertes personnalisees
- Correlation devenements et threat hunting

Jour 3 — Investigation & Reponse

- Forensique Windows et Linux : artefacts, logs, memoire
- Playbooks de reponse aux incidents
- Redaction dun rapport dincident professionnel