

SOC - Tier 3.





Algemeen opleidingsniveau.

Geavanceerd Security Architect / Senior Technical Lead.

De afgestudeerde is voorbij reactieve incidentanalyse en beschikt over kennis en kennis en vaardigheden die gelijkstaan aan een Senior Cyber Security Engineer of Engineer of Lead DFIR Specialist.

Deze professional opereert op strategisch en architecturaal niveau en overziet overziet zowel aanvallen als verdedigingsstructuren in hun geheel.



Mate van zelfstandigheid.

Volledig autonoom.

De afgestudeerde werkt zonder supervisie, formuleert zelfstandig Threat Hunting-hypotheses, zet eigen onderzoeklijnen op en leidt de technische respons tijdens organisatiebrede security-incidenten.

Binnen de SOC fungeert hij/zij als het laatste escalatiepunt.

Direct toepasbaar in deze rollen.

Globale security teams, gespecialiseerde Incident Response-organisaties en high-maturity Cyber Defense Centers.

Geschikt voor functies zoals:



Senior SOC Analyst (Tier 3)



Detection Engineer



Senior Threat Hunter



DFIR Specialist

Tecnische vaardigheden.

Diepgaande expertise in:



Reverse Engineering van malware



Geavanceerd forensisch onderzoek (geheugen- en netwerkanalyse)



Security Automation & SOAR engineering



Detection engineering & strategie (YARA, Sigma)



Gedetailleerde kennis van APT TTP's en geavanceerde persistence-mechanismen

Soorten security-incidenten / cases.

Afhandeling van zeer complexe escalaties, zoals:



Zero-day exploits



Advanced Persistent Threats (APT's)



Living-off-the-Land (LoLBins) aanvallen



Custom-built ransomware



Diepgaande compromittering van cloud-infrastructuren



Analytisch niveau.

De Tier-3 professional analyseert niet alleen het incident, maar identificeert waarom de verdediging heeft gefaald.

Door te denken als een aanvaller voert hij/zij Root Cause Analysis uit en vertaalt dit naar structurele verbeteringen in de beveiligingsarchitectuur.

Aanpak bij incident afhandeling.

Strategisch en systemisch.

Waar Tier 2 het incident onder controle krijgt, richt Tier 3 zich op:



Eradicatie op architectuurniveau



Structurele preventie

De Tier-3 analist leidt de post-mortem analyses en vertaalt technische bevindingen naar lange termijn security roadmaps en verdedigingsstrategieën.



Belangrijkste sterke punten.

Proactieve innovatie.

De kernkracht ligt in Detection Engineering: het ontwerpen van detectielogica die ook de “unknown unknowns” zichtbaar maakt.

Daarnaast is deze professional zeer vaardig in:



Python



Generatieve AI

Hiermee bouwt hij/zij eigen security tooling en vormt een brug tussen software development en security operations.



Inzetadvies (type organisatie / complexiteit).

Ideaal voor:



Kritieke infrastructuur



Financiële instellingen



Grote technologiebedrijven

Met name waardevol in complexe hybride cloud-omgevingen, waar standaard security tooling tekortschiet en maatwerk, proactieve verdediging een bedrijfsnoodzaak is.



Opleidingsduur om dit niveau te bereiken.

Om dit expert-niveau te bereiken (uitgaande van bestaande Tier 1 & 2 kennis), zijn circa 250 contacturen vereist, verdeeld over:



Intensief (fulltime): ±10 weken



Specialistisch (parttime): 5–6 maanden

Deze duur stelt werkende professionals in staat om geavanceerde threat hunting- en engineeringconcepten direct toe te passen binnen hun eigen productieomgevingen tussen de lessen door.

Samenwerken met Trivian.

Trivian biedt organisaties maatwerktrajecten, partnerships en licentiemodellen voor structurele talentontwikkeling.

Wij werken samen met bedrijven, onderwijsinstellingen en overheden aan één doel: het versterken van digitale weerbaarheid door praktische kennis en real-world ervaring.



info@trivian.nl



www.trivian.nl