

SOC Analyst – Tier 1 + Tier 2





Algemeen opleidingsniveau.

De afgestudeerde beschikt over een professionele technische certificering die gelijkstaat aan een hoog niveau mbo/hbo-praktijkopleiding in Cyber Operations.

Hij/zij is voorbij het niveau van “algemene bewustwording” en beschikt over gespecialiseerde technische kennis, vergelijkbaar met het kennisniveau van een junior systeembeheerder gecombineerd met dat van een security specialist.

Mate van zelfstandigheid.



Tier 1-taken: volledig zelfstandig. In staat om SIEM-dashboards te monitoren, alerts te triëren en false positives zonder supervisie af te handelen.



Tier 2-taken: semi-zelfstandig. Kan host-based onderzoeken uitvoeren en Incident Response-playbooks volgen, maar heeft bij complexe remediatie of beslissingen met hoge impact soms begeleiding van een senior nodig.

Direct toepasbaar in deze rollen.

- SOC Analyst (Tier 1 / Tier 2)
- Junior Incident Responder
- Junior Security Researcher

Inzetbaar bij Managed Security Service Providers (MSSP's), interne Enterprise SOC's of Incident Response-teams

Diepgaande technische vaardigheden in:

- ✓ Besturingssysteem-internals (Windows/Linux)
- ✓ Netwerkprotocolanalyse (TCP/IP, SSL/TLS)
- ✓ Log-correlatie, query-ontwikkeling en query writing
- ✓ Vulnerability assessments
- ✓ Basis malware-analyse (statisch en dynamisch)

Ervaring met tools & omgevingen

Hands-on ervaring met enterprise-grade tooling, waaronder:

- ✓ SIEM-platformen (Splunk/Sentinel)
- ✓ Wireshark
- ✓ EDR-interfaces
- ✓ Linux command line (CLI)
- ✓ Forensische suites (Volatility/Autopsy)
- ✓ Cloud-consoles (AWS/Azure)



Soorten security-incidenten / cases die kunnen worden afgehandeld

In staat om onder andere de volgende incidenten zelfstandig af te handelen:

- ✓ Phishing-onderzoeken
- ✓ Brute-force aanvallen
- ✓ Malware-infecties
- ✓ Ongeautoriseerde laterale beweging
- ✓ Cloud-misconfiguraties
- ✓ Identity-based aanvallen (zoals account takeovers)





Analytisch niveau:

Gemiddeld tot gevorderd. De afgestudeerde ziet niet alleen “een alert”, maar begrijpt de context van de aanval door deze te koppelen aan het MITRE ATT&CK-framework en endpoint-events te correleren met netwerkverkeer.



Aanpak bij incidentafhandeling:

Methodisch en procesgedreven. Werkt volgens de NIST/SANS Incident Response-levenscyclus (Preparation → Detection → Containment → Eradication → Recovery).
Is getraind om iedere stap te documenteren in een ticketsysteem (Jira/TheHive) om een sluitende chain of evidence te waarborgen.





Belangrijkste sterke punten:

De grootste kracht is het effectief inzetten van AI-tools om het werk te versnellen: sneller queries schrijven dan traditionele analisten en complexe incidenten direct samenvatten in professionele, executive-ready rapportages.



Inzetadvies (type organisatie / complexiteit):

Sterk aanbevolen voor middelgrote tot grote organisaties of high-pressure MSSP-omgevingen. Het profiel komt het best tot zijn recht in omgevingen met grote hoeveelheden data, waar AI-productiviteit en een stevige basis in cloud-native security het meeste voordeel opleveren.



Opleidingsduur om iemand zonder voorkennis inzetbaar te maken:

Om dit niveau te bereiken vanaf nul en iemand volledig werk-ready te maken, zijn 600 contacturen nodig, verspreid over 6 tot 12 maanden. Let op: Korter dan 6 maanden bij een programma van 600 uur leidt in de praktijk vaak tot “knowledge burnout”: studenten leren tools bedienen, maar missen begrip van de onderliggende theorie en samenhang.

Toelating & Start.

De opleiding is toegankelijk voor iedereen met basiskennis van computers en een sterke motivatie om de overstap te maken naar cybersecurity.

IT-ervaring is een voordeel, maar geen vereiste — Trivian leert je de mindset, vaardigheden en discipline die nodig zijn om te slagen in dit snelgroeiende vakgebied.

Klaar voor de volgende stap?



info@trivian.nl



www.trivian.nl