TLP:GREEN

SOC ROLPROFIELEN

Monitoring & Detectie

Best Practice versie 1.0

Complexiteit document

Eenvoudig

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot de supplychain, netwerken, systemen en (gevoelige) informatie.

Monitoring- en detectiediensten zijn erop gericht om een veelheid aan loggegevens en andere (meta-)datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie te analyseren, aggregeren en correleren. Monitoring en detectiesystemen kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan.

Om monitoring- en detectiediensten effectief in te kunnen zetten zijn er diverse onderwerpen die binnen een organisatie moeten zijn ingericht. Dit document "SOC Rolprofielen" voorziet in tips en handvatten voor het standaardiseren van SOC rolprofielen. Het document ondersteunt daarmee organisaties die een Security Operations Center (SOC) willen realiseren of optimaliseren.

Achtergrond

VSSR levert verschillende kennisproducten. In dit document worden handvatten geboden voor het opstellen van uniforme rolprofielen voor een Security Operations Center (SOC). Uniforme rolprofielen ondersteunen de organisatie bij het wervings- en selectieproces.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor Senior Management op strategisch niveau, functionarissen die zijn belast met de werving en selectie van SOC medewerkers.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
1.0	2-10-2025	Initiële versie

1.2 Referenties

Document	Link
European Cybersecurity Skills Framework Role Profiles	European Cybersecurity Skills Framework Role Profiles | ENISA
European e-Competence Framework (e-CF)	European e-Competence Framework (e-CF) | European Skills, Competences, Qualifications and Occupations (ESCO)
VSSR-kennisdocumenten	VSSR (rijksapplicaties.nl)

1.3 Definities

Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

2 Inleiding

Standaard rolprofielen zijn essentieel voor het efficiënt en effectief functioneren van een organisatie. Ze bieden een duidelijk kader voor de verantwoordelijkheden, taken en verwachtingen die aan een specifieke rol zijn verbonden. Dit zorgt voor consistentie en transparantie binnen de organisatie, waardoor medewerkers precies weten wat er van hen wordt verwacht en hoe hun prestaties worden beoordeeld.

Daarnaast dragen uniforme rolprofielen bij aan een eerlijkere en objectievere beoordeling van medewerkers. Wanneer iedereen binnen dezelfde rol dezelfde criteria heeft, wordt het makkelijker om prestaties te vergelijken en te evalueren. Dit kan leiden tot een heldere beloningsstructuur en betere ontwikkelingsmogelijkheden voor in de loopbaan.

Ten slotte helpen uniforme rolprofielen bij het wervings- en selectieproces. Ze bieden een duidelijk beeld van wat de organisatie zoekt in een kandidaat, wat het makkelijker maakt om de juiste persoon voor de juiste rol te vinden. Dit draagt bij aan een betere pasvorm tussen de medewerker en de organisatie.

2.1 Doel

Dit document biedt een overzicht en structuur van de belangrijkste rollen binnen een Security Operations Center (SOC). Het doel is om organisaties een praktisch handvat te geven bij het (door)ontwikkelen van hun eigen SOC-rolprofielen. Door inzicht te geven in verantwoordelijkheden, competenties en specialisaties per functie, kunnen organisaties de profielen aanvullen en aanpassen aan hun eigen context, volwassenheidsniveau en dreigingslandschap. De rolprofielen zijn puur als handreiking opgesteld en kunnen afhankelijk van het formaat, dreigingslandschap of bestaande tooling van de organisatie anders ingericht worden.

2.2 Context

Binnen een Security Operations Center (SOC) zijn verschillende rollen nodig om effectief te kunnen reageren op digitale dreigingen. Hoewel de praktijk een breed scala aan functies kent, richt dit document zich specifiek op twee kernrollen: de SOC-Analist (in drie niveaus) en de SOC-Lead. Deze functies vormen de operationele basis van een SOC en zijn cruciaal voor zowel de dagelijkse detectie en respons op incidenten als voor de aansturing en coördinatie van het team. Andere rollen worden vooralsnog buiten de scope van dit document gelaten. In eventuele toekomstige versies van dit document, kunnen er additionele rollen worden toegevoegd.

3 SOC Rolprofielen

In dit hoofdstuk worden de diverse SOC-analist rolprofielen toegelicht en die van de SOC-Lead.

Het gekozen framework om de rollen te beschrijven, is gelijk aan het framework van ENISA om de "European Cybersecurity Skills Framework Role Profiles" te beschrijven.

In de tabel hieronder is een korte beschrijving van de componenten van het rolprofiel gegeven.

Sub-onderwerp	Beschrijving
Andere benaming	Alternatieve titel of naam voor de functie.
Samenvatting werk	Korte beschrijving van de belangrijkste taken en verantwoordelijkheden.
Doel	Het primaire doel of de bijdrage van de rol aan de organisatie.
Deliverables	Concrete resultaten of producten die de rol moet opleveren.
Werkzaamheden	Specifieke taken en activiteiten die bij de rol horen.
Vaardigheden	Specifiek leerbare capaciteiten om de rol uit te voeren
Kennis	Theoretische of technische informatie en expertise vereist voor de rol.
Competenties	Combinatie van vaardigheden en kennis om succesvol te zijn in een rol. • Niveau 1–2: Operationeel / uitvoerend • Niveau 3: Tactisch / coördinerend • Niveau 4–5: Strategisch / beleidsbepalend

Tabel 1: Beschrijving onderdelen rolprofiel

3.1 Analist-profielen

In dit hoofdstuk worden de diverse rolprofielen van de SOC-analist beschreven. Gegradeerd op junior, medior en senior niveau.

3.1.1 Junior

Junior SOC-Analist	
Andere benaming	– Cybersecurity Analyst – Information Security Analyst – Security Analyst – SOC Specialist – Incident Response Analyst – Security Incident Analyst – Network Security Analyst – Security Monitoring AnalystAI
Samenvatting werk	Is verantwoordelijke voor de monitoring van beveiligingsmeldingen, beoordeelt deze en escaleert verdachte activiteiten. Werkt volgens vaste procedures en richtlijnen. Heeft een uitvoerende en ondersteunende rol in het SOC-team.
Doel	Het analyseren van verdachte activiteiten via continue monitoring van systemen en netwerken, waarbij een eerste analyse en inschaling van beveiligingsmeldingen wordt gedaan.
Deliverables	➢ Correct ingeschatte en gedocumenteerde beveiligingsmeldingen. ➢ Tijdige escalaties van verdachte of kritieke incidenten. ➢ Dagelijkse logboeken en monitoringrapportages volgens standaardprocedures.
Werkzaamheden	– Alert Queue Monitoring – Alert Triage en kwalificatie – Incident registratie

	– Meldingen afhandelen – Team Mailbox – Werken met playbooks en runbooks – Escalatie naar level 2 – Documentatie van incidentafhandeling	
Vaardigheden	☑ Monitoring en analyse ☑ Basis Incident response ☑ Probleemoplossend vermogen ☑ Communicatievaardigheden	
Kennis	☑ Netwerkconcepten ☑ Beveiligingsconcepten ☑ SIEM ☑ Basis besturingssystemen	
e-Competences (e-CF)/ Competenties	B.1 - Application Development C.2 - Change Support D.1 - Information Security Management E.5 - Process Improvement	Niveau 1 Niveau 2 Niveau 1 Niveau 1

Tabel 2: Rolprofiel junior SOC-analist

3.1.2 Medior

Medior SOC-Analist	
Andere benaming	– Cybersecurity Analyst – Information Security Analyst – Security Analyst – SOC Specialist – Incident Response Analyst – Security Incident Analyst – Network Security Analyst – Security Monitoring Analyst
Samenvatting werk	Voert diepgaander onderzoek uit naar verdachte activiteiten en incidenten. Behandelt escalaties van de junior analist en neemt maatregelen voor mitigatie. Heeft een analytische rol met zelfstandigheid en technische diepgang. Ondersteund en helpt junior analisten en begeleid stakeholders bij incidentafhandeling. Draagt bij aan het optimaliseren en uitbreiden van het detecteren van verdachte activiteiten.
Doel	Het diepgaander analyseren van beveiligingsincidenten en het uitvoeren van gerichte responsmaatregelen en waar nodig verbeteringen aan te dragen in het proces. Het onderzoeken van oorzaken, patronen en mogelijke impact van aanvallen.
Deliverables	➢ Incidentanalyses met root cause analysis (RCA) en impactbepaling. ➢ Incidentrapportages inclusief response-acties en aanbevelingen. ➢ Verbeterde detectieregels, playbooks en use cases voor SIEM-systemen.
Werkzaamheden	– Incident onderzoek bij complexere, of hogere impact/prioriteit incidenten waarbij een Junior Analist vastloopt of versnelde escalatie noodzakelijk is. – Cross-incident correlatie en identificatie. – Identificatie van organisatieoverstijgende en/of grotere incidenten. – Vraagbaak voor Junior Analisten.

	– 24x7 on-call dienst. – Overleg met stakeholders bij incidenten. – Rapportage voor team en externe stakeholders. – Techniek naar functioneel kunnen vertalen en dit correct verwoorden in Operating Procedures. – Detecties ontwikkelen in het SIEM. – Ontwikkelen van Standard Operating Procedures. – Regelmatig controleren van afgehandelde onderzoeken en terugkoppeling geven aan Junior Analisten. – Begeleiden en ondersteunen van Junior Analisten. – Identificeren en terugkoppelen van operationele gaps in processen, procedures en kennis. – Meewerken aan post-incident reviews – Kwaliteitsborging van triage/playbooks	
Vaardigheden	☑ Vaardigheden Junior SOC-Analist ☑ Geavanceerde incident response ☑ Gevorderde analyse ☑ Kritisch denken ☑ Begeleiding medewerkers	
Kennis	☑ Junior SOC-Analist ☑ Gevorderde netwerkconcepten ☑ Gevorderde Beveiligingsconcepten	
e-Competences (e-CF)/ Competenties	B.6 - Systems Engineering C.4 - Problem Management D.1 - Information Security Management E.3 - Risk Management	Niveau 2 Niveau 3 Niveau 2 Niveau 2

Tabel 3: Rolprofiel medior SOC-analist

3.1.3 Senior

Senior SOC-Analist	
Andere benaming	– Cybersecurity Analyst – Information Security Analyst – Security Analyst – SOC Specialist – Incident Response Analyst – Security Incident Analyst – Network Security Analyst – Security Monitoring Analyst
Samenvatting werk	Leidt complexe incidentonderzoeken. Optimaliseert detectiemogelijkheden, begeleidt junior en medior analisten en helpt bij de ontwikkeling van de SOC-strategie. Indien nodig of gewenst specialiseert de SOC-analist zich op een vakgebied zoals malware analyse, forensisch onderzoek, pentesten, etc.
Doel	Het leiden van complexe incidentonderzoeken en coördineren van de volledige incidentrespons. Het optimaliseren van SOC-processen, tooling en strategische beveiligingsmaatregelen.
Deliverables	➢ Strategische rapportages over dreigingstrends en incidentstatistieken. ➢ Geavanceerde resultaten en aanbevelingen voor verbetering.

	➢ Ontwikkelde en geoptimaliseerde SOC-processen, procedures en automatiseringen.	
Werkzaamheden	– Last resort voor Junior/Medior Analisten bij technische vraagstukken. – Trend-onderzoek in alerting en verifiëren van Junior/Medior werk om te kunnen coachen. – Incident coördinatie bij organisatieoverstijgende incidenten. – 24x7 on-call dienst. – Incident coördinatie bij grotere en organisatieoverstijgende incidenten. – Vertegenwoordigen van het SOC bij externe overlegstructuren. – Houden van presentaties over het SOC. – Initiëren van en participeren in samenwerkingsverbanden. – Netwerken – Actief samenwerking opzoeken met andere SOC's binnen de overheid. – Complexe detective op basis van scenario analyse. – Controle en ondersteunen ontwikkelde detecties door Mediors. – Ontwikkelen en verbeteren van processen. – Op de hoogte zijn en blijven van marktontwikkelingen die kunnen bijdragen aan verbetering van het SOC. – Op de hoogte zijn en blijven van dreigingen en dit kunnen omzetten naar. verbetervoorstellen voor het SOC. – Dagelijkse aansturing Junior/Medior Analisten. – Aanvullen van de ontwikkelbacklog. – Ondersteunen en helpen van Junior- en Medior-analisten bij ontwikkeling. – Threat hunting – Voeren van post-incident reviews / lessons learned sessies – Advies geven over SOC-strategie of roadmap – Gebruik van MITRE ATT&CK, Cyber Kill Chain in analyses – Beoordelen van nieuwe tooling of integratiebehoeften	
Vaardigheden	☑ Medior SOC-Analist ☑ Coaching/mentoring ☑ Specialisatie (verdieping of verbreding)	
Kennis	☑ Medior SOC-analist ☑ Compliance en regelgeving ☑ Kennis bedreigingen en aanvalstechnieken	
e-Competences (e-CF)/ Competenties	C.3 - Service Delivery D.1 - Information Security Management D.4 - Purchasing E.2 - Project and Portfolio Management	Niveau 4 Niveau 3 Niveau 3 Niveau 3

Tabel 4: Rolprofiel senior SOC-analist

3.1.4 Overzichtstabel

Hier de tabel hieronder staat globaal aangegeven wat de voornaamste verschillen tussen de rollen zijn.

Aspect	Junior	Medior	Senior
Samenvatting werk	Monitort beveiligingsmeldingen, voert eerste analyses uit en escaleert incidenten.	Analyseert beveiligingsincidente, en ondersteunt threat hunting.	Leidt incidentonderzoeken, voert threat hunting uit en optimaliseert SOC-processen.
Doel van de rol	Detecteren en correct inschalen van incidenten via continue monitoring.	Behandelen en analyseren van complexe incidenten en verbeteren van detectie.	Strategisch aansturen van de SOC, dreigingen anticiperen en processen optimaliseren.
Deliverables	Logboekmeldingen Triageverslagen Escalaties	Incidentrapportages RCA-analyses Aangepaste detectieregels	Dreigingstrendrapportages Threat hunting-resultaten SOC-strategievoorstellen
Werkzaam-heden	Monitoren SIEM-alerts Triage uitvoeren Escalaties registreren	Incidentanalyse Aanpassen use cases	Coördineren van respons Threat hunting Ontwikkelen van processen en playbooks
Jaren ervaring	0–2 jaar	2–5 jaar	5+ jaar
Autonomie niveau	Laag – werkt onder toezicht en volgens vaste procedures.	Gemiddeld – werkt zelfstandig binnen kaders.	Hoog – stuurt processen aan en neemt beslissingen.
Vaardigheden	Basis loganalyse Alertinschatting Rapporteren	Netwerkanalyse Incidentanalyse	Leiderschap Strategisch inzicht Threat intelligence integratie
Kennis	Basis netwerkprotocollen SIEM-tools Cyberdreigingen (basics)	MITRE ATT&CK Incident lifecycle	Threat modeling Frameworks (NIST, ISO) Security architecture

Tabel 5: Overzicht rolprofielen SOC-analist

3.2 Management-profielen

In dit stuk zal het rolprofiel van de SOC-Lead beschreven worden.

3.2.1 SOC Lead

SOC-Lead	
Andere benaming	– Cybersecurity Operations Lead – Information Security Lead – Cyber Defense Opartions Lead – Operational Security Lead
Samenvatting werk	De SOC-Lead is verantwoordelijk voor het leiden en coördineren van het SOC-team, het waarborgen van de operationele efficiëntie en effectiviteit van beveiligingsbewakings- en incidentresponsprocessen, en het zorgen voor continue verbetering van de beveiligingspostuur van de organisatie.
Doel	Het doel van de SOC-Lead is om een proactieve en reactieve beveiligingsstrategie te implementeren en te handhaven, om beveiligingsincidenten te identificeren, te analyseren en te mitigeren, en om het SOC-team te leiden in hun dagelijkse activiteiten om de algehele beveiliging van de organisatie te waarborgen.
Deliverables	➢ Ontwikkelen en bijwerken van incidentresponsplannen ➢ Rapporten over de prestaties en effectiviteit van het SOC-team ➢ Organiseren van trainingen en workshops voor het team en andere medewerkers ➢ Functioneert als het inhoudelijk geweten voor de SOC-Manager en voor het team.
Werkzaamheden	– Leiden en coördineren van het SOC-team – Coördineren van de respons op beveiligingsincidenten – Rapporteren over beveiligingsincidenten en trends aan het management – Zorgen voor training en professionele ontwikkeling van het SOC-team – Procesverbetering en kwaliteitsborging – Strategische afstemming met CISO / IT-management – Budgetbeheer en resourceplanning – Stakeholdermanagement (intern en extern) – KPI’s en prestatiemetingen opstellen en bewaken – Tooling- en platformkeuzes coördineren – Security roadmap en visie voor het SOC ontwikkelen
Vaardigheden	☑ Leiderschapsvaardigheden om het team te motiveren en te leiden ☑ Communicatieve vaardigheden voor effectieve rapportage en teamcoördinatie ☑ Vermogen om complexe beveiligingsproblemen te analyseren en op te lossen ☑ Vaardigheid in het beheren van projecten en het coördineren van teamactiviteiten ☑ Vermogen om kritisch te denken en weloverwogen beslissingen te nemen
Kennis	☑ Diepgaande kennis van beveiligingsconcepten en -praktijken ☑ Kennis van netwerkbeveiliging en -architectuur ☑ Kennis van incidentresponseprocedures en -technieken ☑ Kennis van relevante compliance- en regelgevingsvereisten ☑ Kennis van verschillende beveiligingstools en -technologieën

e-Competences (e-CF)/ Competenties	A.7. Technology Trend Monitoring	Level 4
	B.2. Component Integration	Level 4
	C.4. Problem Management	Level 4
	D.1. Information Security Strategy Development	Level 3
	E.3. Risk Management	Level 4

Tabel 6: Rolprofiel SOC Lead

4 SOC Specialisatie-gebieden

In dit hoofdstuk wordt beschreven op welke gebieden een SOC(-medewerker) zich mogelijk kan specialiseren

In de tabel hieronder staan diverse specialisatiegebieden waarin een SOC(-medewerker) zich kan specialiseren. Deze specialisatiegebieden zijn aangegeven om als inspiratie/referentie te dienen om te kijken in welke gebieden een SOC(-medewerker) zich kan specialiseren.

Het gebied waarin een SOC(-medewerker) zich wilt specialiseren is altijd afhankelijk van de context, omgeving en dreigingslandschap waarmee het SOC te maken heeft. Er is dus niet een vaste route of specialisatie die altijd als eerste gekozen dient te worden. Zorg dat een eventuele specialisatie dus altijd aansluit bij het landschap en uitdagingen van de organisatie.

Specialisatiegebied	Kernactiviteiten & Verdieping
1. Incident Response	- Analyseren en afhandelen van incidenten - Containment-, herstel- en escalatieprocedures uitvoeren - Rapporteren en post-incidentanalyse uitvoeren
2. Threat Hunting	- Proactief zoeken naar verborgen dreigingen - Bouwen van hypothesen op basis van gedragspatronen - Werken met MITRE ATT&CK, log- en endpointanalyse
3. Digital Forensics	- Verzamelen en analyseren van digitale sporen - Analyseren van disk, geheugen, netwerkdata - Documenteren volgens juridische standaarden
4. Malware Analysis	- Statische & dynamische analyse van malware - Reverse engineering van binaries - Herkennen van persistente technieken & netwerkgedrag
5. SIEM Engineering / Use Case Development	- Ontwerpen van detectieregels en dashboards - Normaliseren en correleren van logdata - Verminderen van false positives
6. Threat Intelligence	- Verzamelen en analyseren van dreigingsdata - Maken van IoC's en TTP-profielen - Integratie van intel in het SOC-proces
7. SOC Automation en SOAR-Engineering	- Ontwerpen van playbooks en automatiseringen - API-integratie van SIEM, EDR, ticketingtools - Versnellen van incidentafhandeling
8. Vulnerability Management	- Identificeren van kwetsbaarheden via scanningtools - Prioriteren op basis van risico, impact en exposure - Afstemmen van mitigaties met IT-teams - Rapporteren over kwetsbaarheidsstatus en trends

Tabel 7: Specialisatiegebieden SOC

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://vssr.rijksapplicaties.nl/

vssr.info@minjenv.nl

Oktober 2025