Bijlage 04

SOC Use Case Roadmap

Gefaseerde implementatie en doorontwikkeling van detectiecapaciteit

Behorend bij

Raamovereenkomst Security Operations Center (SOC)

Status : Definitief

Versie : 1.0

Datum : 06-08-2026

Inhoudsopgave

1 Doel en uitgangspunten

Deze bijlage beschrijft de gefaseerde roadmap voor de implementatie en doorontwikkeling van SOC use cases binnen de dienstverlening.

De Opdrachtnemer:

- maakt primair gebruik van bestaande (out-of-the-box) detecties binnen de SIEM-oplossing (bijv. Microsoft Sentinel);
- vult deze waar nodig aan met maatwerk use cases;
- borgt uniformiteit en hergebruik van use cases tussen Deelnemers;
- optimaliseert use cases continu op basis van effectiviteit, dreigingsontwikkeling en operationele inzichten.

De roadmap richt zich primair op IT-detectie en wordt gedurende de looptijd uitgebreid naar OT-omgevingen (Operational Technology). Hierbij wordt aangesloten op de volwassenheid en gereedheid van Deelnemers en wordt gebruik gemaakt van een gefaseerde implementatieaanpak.

Use cases worden gefaseerd geïmplementeerd volgens het principe:

basisdetectie → verdieping → geavanceerde detectie en automatisering.

2 Fase 1 – Basisdetectie (initiële SOC-operationalisatie)

Doel: realiseren van snelle detectiedekking op kritieke bronnen en veelvoorkomende dreigingen.

Focus:

- Identiteit en toegang
- Endpoint security
- Netwerkbeveiliging
- E-mail en cloudgebruik

Use cases (indicatief):

1. Command & Control (C2) communicatie
2. Detectie van het uitschakelen of wijzigen van beveiligingstooling (EDR/AV/firewall/logging-agents). Dit is een klassieke ransomware-precursor en direct gekoppeld aan BIO 8.7/8.9 en NIS2 art. 21(2)(e)/(g). Staat nu pas als nr. 32 in Fase 2 — hoort qua compliance in Fase 1.
3. Detectie van manipulatie of verwijdering van logbestanden. BIO 8.15 (Logging) vereist bescherming van de integriteit van logs; NIS2 art. 21(2)(b)/(f) veronderstelt betrouwbare logdata als basis voor incidentdetectie en verantwoording. Staat nu pas als nr. 53 in Fase 3 — hoort qua compliance in Fase 1.
4. Detectie van onbekende/nieuwe (rogue) apparaten in het netwerk. Volgt uit BIO 5.9 (asset-inventarisatie) en NIS2 art. 21(2)(i) (assetbeheer). Ontbreekt volledig.
5. Detectie van ontbrekende/verouderde patches op kritieke systemen (kwetsbaarhedenbeheer). NIS2 art. 21(2)(e) noemt vulnerability handling expliciet als verplichte maatregel; BIO 8.8 (Management of technical vulnerabilities) is een kerncontrole. Ontbreekt volledig in de huidige roadmap.
6. Detectie van verwijdering/aantasting van back-ups (ransomware-indicator). BIO 8.13 (backup) en NIS2 art. 21(2)(c) (bedrijfscontinuïteit) vereisen dit expliciet. Ontbreekt volledig.
7. DNS queries naar bekende malafide domeinen
8. Endpoint malware detectie (EDR alerts)
9. Externe toegang tot kritieke systemen
10. Firewall deny spikes / scanning gedrag
11. Gebruik van gedeelde of generieke accounts
12. Login zonder MFA waar verwacht
13. Meerdere mislukte inlogpogingen (brute force)

14. Misbruik van service accounts
15. Nieuwe admin-accounts aangemaakt
16. Ongebruikelijke mailbox forwarding regels
17. Phishing detectie (mail filtering + user signals)
18. Uitvoering van verdachte processen
19. Verdachte bijlagen (macro's / executables)
20. Verdachte privilege-escalatie

3 Fase 2 – Verdieping en correlatie (verhoogde detectiekwaliteit)

Doel: verhogen van detectiekwaliteit door correlatie, context en gedragsanalyse.

Focus:

- Multi-source correlatie
- Insider threat detectie
- Cloud en SaaS verdieping
- Data access en gedrag

Use cases (indicatief):

21. Abnormaal gebruik van cloudapplicaties
22. Abnormaal gedrag van privileged users
23. Correlatie van login + endpoint activiteit
24. Data exfiltratie via DNS / HTTPS
25. Detectie van persistence mechanismen
26. Endpoint + netwerk correlatie
27. Impossible travel (onrealistische login patronen)
28. Inloggen vanaf afwijkende geografische locatie
29. Laterale beweging binnen netwerk
30. Massale data downloads
31. Misbruik van OAuth-applicaties
32. Misbruik van remote management tools
33. Netwerkverkeer naar risicolanden
34. Ongebruikelijke admin-activiteiten
35. Ongebruikelijke API-calls (SaaS)
36. Ongebruikelijke bestandslocaties / staging gedrag
37. Ongebruikelijke login tijden
38. Ongebruikelijke toegang tot gevoelige data
39. Pass-the-hash / credential misuse
40. Shadow IT detectie
41. Suspicious scheduled tasks / cron jobs
42. Uitschakelen van security tooling
43. Verdachte account lifecycle events
44. Verdachte wijzigingen in configuraties

4 Fase 3 – Geavanceerde detectie en automatisering (SOC-maturity)

Doel: proactieve detectie, automatisering en continue optimalisatie.

Focus:

- Threat intelligence integratie
- Gedragsanalyse (UEBA)
- Automatisering (SOAR)

- OT-integratie

Use cases (indicatief):

45. Afwijkend gedrag in industriële protocollen
46. Automatische incidentverrijking (SOAR)
47. Beaconing detectie (low & slow C2)
48. Continue tuning op basis van false positives/negatives
49. Cross-domein correlatie (IT/OT)
50. Detectie van afwijkende gedragsprofielen
51. Detectie van data staging voor exfiltratie
52. Detectie van manipulatie van logs
53. Detectie van stealthy persistence
54. Geautomatiseerde containment acties
55. Living-off-the-land technieken (LOLBins)
56. OT-anomaliedetectie (indien van toepassing)
57. Supply chain indicatoren
58. Threat intelligence correlatie (TAXII/STIX)
59. UEBA-gebaseerde anomaliedetectie

5 Uniformiteit en hergebruik

De Opdrachtnemer borgt dat:

- use cases centraal worden beheerd en gestandaardiseerd;
- verbeteringen en optimalisaties worden gedeeld tussen Deelnemers;
- use cases modulair en overdraagbaar zijn ingericht;
- documentatie volledig en actueel wordt bijgehouden.

Afwijkingen per Deelnemer zijn toegestaan indien noodzakelijk, maar worden geminimaliseerd.

6 Doorontwikkeling en lifecycle management

Use cases worden gedurende de looptijd:

- periodiek geëvalueerd op effectiviteit;
- aangepast op basis van dreigingsontwikkelingen;
- afgestemd op MITRE ATT&CK of vergelijkbare frameworks;
- opgeschoond bij veroudering of ineffectiviteit.

Nieuwe use cases worden iteratief toegevoegd via de overeengekomen governance- en ontwikkelstructuur.

7 OT-detectie en gefaseerde uitrol

De implementatie van OT-detectie vindt gefaseerd plaats en sluit aan op de gereedheid van Deelnemers.

Provincie Flevoland fungeert als eerste implementerende Deelnemer en heeft reeds een initiële OT-detectie ingericht voor een beperkt aantal objecten. Deze implementatie wordt bij aanvang van de overeenkomst overgedragen aan de Opdrachtnemer en geïntegreerd in de SOC-dienstverlening.

Overige Deelnemers starten gedurende de looptijd met OT-detectie. Hierbij wordt in beginsel aangesloten op:

- de architectuurkeuzes;
- de ingerichte detecties;
- en de geleerde lessen van Provincie Flevoland.

De Opdrachtnemer:

- ondersteunt Deelnemers bij de gefaseerde onboarding van OT-bronnen;
- houdt rekening met OT-specifieke randvoorwaarden (zoals beschikbaarheid, veiligheid en beperkte wijzigingsmogelijkheden);
- past detectie aan op OT-systemen en protocollen waar van toepassing;
- borgt dat detecties zoveel mogelijk uniform en herbruikbaar worden ingericht.

OT-detectie wordt initieel beperkt ingezet en groeit mee met de volwassenheid van de Deelnemers.

8 Resultaat

Deze gefaseerde aanpak leidt tot:

- snelle initiële detectiedekking;
- gecontroleerde groei in complexiteit;
- consistente kwaliteit over Deelnemers;
- maximale herbruikbaarheid van detecties;
- toekomstbestendige en overdraagbare SOC-dienstverlening.