SoC/SIEM in de praktijk

Hoe richt je een effectieve strategie in voor detectie, monitoring en respons?

Stefan Reijmers

13 maart 2025

Agenda

- 🦾 De Kracht van SIEM: De rol en impact van security monitoring in een dynamische wereld
- 👥 De sleutelrollen binnen een SOC – Van monitoring en detectie tot incident respons
- 🔐 SIEM & Privacy – Hoe vind je de juiste balans tussen beveiliging en compliance?
- ♻️ De evolutie van detectie – Hoe je dreigingen voorblijft met continue verbetering
- 🔎 SIEM selectie – Functionaliteit, schaalbaarheid en toekomst van security monitoring
- ❓ Vragen en antwoorden?

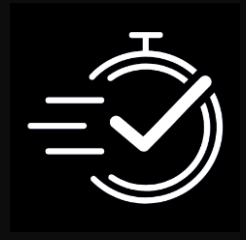
De Kracht van SIEM: De rol en impact van security monitoring in een dynamische wereld

“SIEM is het fundament van je beveiligingsstrategie. Het detecteert afwijkingen, analyseert patronen en zet signalen om in gerichte acties, zodat je dreigingen altijd een stap voor blijft.”

De Kracht van SIEM: De rol en impact van security monitoring in een dynamische wereld

logs verzamelen

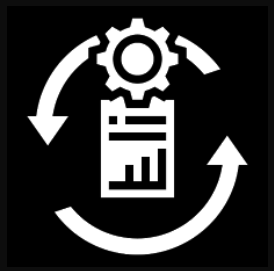
afwijking detecteren



analyse / triage

inperken dreiging

root cause anaylse



herstellen

De Kracht van SIEM: De rol en impact van security monitoring in een dynamische wereld

Logs verzamelen bronnen identificeren:

logs verzamelen

- Bepalen welke systemen, apparaten en applicaties logs genereren.
- Log aggregatie: Verzamel logs uit firewalls, endpoints, IDS/IPS, Active Directory, cloudservices, OT-systemen, enz.
- Normalisatie en parsing: Omzetten van logs naar een standaard formaat voor correlatie en analyse.
- Opslag en retentiebeheer: Definiëren hoe lang logs worden bewaard, afhankelijk van compliance en bedrijfsbehoeften.

Do’s

✅ Verzamel logs van alle kritieke systemen en beveiligingsapparaten, “kroon juwelen”.

Don’ts

❌Verzamelen van overbodige logs zonder filtering kunnen leiden tot "log ruis”.

De Kracht van SIEM: De rol en impact van security monitoring in een dynamische wereld

Detectie en monitoring:

afwijking detecteren

- Security monitoring: Continue bewaking van de loggegevens om verdachte activiteiten te identificeren.
- Threat intelligence integratie: Verrijken van logs met threat intelligence feeds (bijvoorbeeld MITRE ATT&CK en ThreatQ).
- Anomaly detection: Gebruik van User and Entity Behavior Analytics (UEBA) om afwijkingen te detecteren.
- SIEM Use Cases & detectie rules: Configuratie van correlatieregels om aanvallen en afwijkingen op te sporen.

Do’s

✅ Verrijk SIEM-events met threat intelligence en asset criticality om false positives te verminderen.

Don’ts

❌Cyberdreigingen evolueren continu, dus een SIEM-configuratie mag nooit statisch blijven.

De Kracht van SIEM: De rol en impact van security monitoring in een dynamische wereld

Incidentdetectie en analyse:

analyse / triage

- Automatische en handmatige triage van alerts: Bepalen welke incidenten direct aandacht nodig hebben op basis van impact en urgentie.
- Contextualisering van alerts: Verrijken met asset criticality en threat intelligence om de ernst van een dreiging beter te begrijpen.
- Correlatie van logs: Relateren van gebeurtenissen over meerdere systemen om complexe aanvallen te detecteren.
- False positive filtering: Fijn-afstemmen van detectieregels en handmatige verificatie om ruis te verminderen.

Do’s

✅ Prioriteer alerts op impact en urgentie met contextuele verrijking.

Don’ts

❌Blind reageren op alle alerts zonder prioritering.

De Kracht van SIEM: De rol en impact van security monitoring in een dynamische wereld

Beperken van de dreiging:

- Gebruik van SOAR (Security Orchestration, Automation, and Response): Automatiseren van reacties op bekende dreigingen.
- Eerste respons: Isoleren van getroffen systemen, blokkeren van verdachte IP’s of gebruikersaccounts.
- Threat hunting: Actief zoeken naar indicatoren van compromis (IoCs) en laterale bewegingen in het netwerk.

inperken dreiging

Do’s

✅ Na validatie isoleer getroffen systemen direct om verdere verspreiding te voorkomen.

Don’ts

❌ Te snel systemen uitschakelen of isoleren zonder juiste impactanalyse.

De Kracht van SIEM: De rol en impact van security monitoring in een dynamische wereld

Forensisch onderzoek en root cause analyse:

- Diepgaande loganalyse: Onderzoeken hoe de aanval heeft plaatsgevonden en welke tactieken en technieken zijn gebruikt.
- Malware analyse: Reverse engineering van malware indien relevant.
- Data exfiltratie-analyse: Controleren of er gevoelige gegevens zijn gestolen.

root cause anaylse

Do’s

✅ Bewaar en analyseer alle relevante logbestanden en systeem gegevens gestructureerd.

Don’ts

❌Wijzigen of verwijderen van bewijsmateriaal voordat het onderzoek is voltooid.

De Kracht van SIEM: De rol en impact van security monitoring in een dynamische wereld

Herstel en schoonmaak:


herstellen

- Herstel van systemen: Opnieuw installeren van gecompromitteerde systemen en toepassen van patches om kwetsbaarheden te verhelpen.
- Systeemhardening: Aanpassen van configuraties en beleidsregels om herhaling van het incident te voorkomen.
- Herstellen van operationele processen: Beoordelen of kritieke bedrijfsdiensten volledig operationeel zijn na het incident.
- Validatie en testen: Controle uitvoeren om te bevestigen dat de dreiging is geëlimineerd en de beveiliging is verbeterd.

Do’s

✅ Implementeer beveiligde patches en harden systemen vóór heractivatie.

Don’ts

❌Te snel systemen opnieuw online brengen zonder grondige validatie.

“Incidenten zijn geen fouten, maar kansen om de beveiliging en het SOC-proces te versterken. Leer van elk incident en verbeter continu je detectie, respons en beveiligingsmaatregelen.”

De sleutelrollen binnen een SOC – Van monitoring en detectie tot incident respons

Management
SOC Management

👤 **SOC Manager** – Overziet het hele SOC, rapporteert aan de CISO en zorgt voor strategie en teamcoördinatie.
👤 **Threat Intelligence Lead** – Beheert de threat intelligence en de intelligence resources.

Blue Team
Defensief

- **Tier 1 SOC Analisten** – Monitoring SIEM en EDR alerts, eerste triage.
- **Tier 2 Incident Responders** – Onderzoekt en mitigeert security incidenten.
- **Tier 3 Threat Hunters** – Proactief opsporen van verborgen bedreigingen.

Red Team
Offensief

- Voert penetratietests en 'adversary simulations' uit.
- Test de effectiviteit van de Blue Team-verdediging.

Yellow Team
Security Enginering

- Beheert SIEM-, EDR-, SOAR- en vulnerability management tools.
- Ontwikkelt en optimaliseert detectieregels.

White Team
Governance & Compliance

- Zorgt voor naleving van audits (ISO 27001, NIST, GDPR, DORA, NIS2).
- Rapporteert risico's en de beveiligingsstatus aan het management.

Green Team
Security Awareness & Training

- Voert bewustwordingstrainingen uit (zoals phishingtests awareness).
- Ondersteunt Purple Team-oefeningen.

Purple Team
Samenwerking Red & Blue

- Ondersteunt Purple Team-oefeningen.
- Voert gesimuleerde aanvallen uit en verbetert verdedigingstactieken.

CS-IRT

Hoewel het SOC en het CS-IRT nauw geïntegreerd zijn, bevindt het CS-IRT zich doorgaans buiten het SOC om een onafhankelijke, multidisciplinaire reactiemogelijkheid te waarborgen. Het SOC detecteert en escaleert bedreigingen, terwijl het CS-IRT het daadwerkelijke reactie- en herstelproces leidt.

De sleutelrollen binnen een SOC – Van monitoring en detectie tot incident respons

“Een SOC is geen enkelvoudig team, maar een gelaagde verdedigingsstructuur die monitoring, analyse, incidentrespons en proactieve verdediging combineert. Elke rol draagt bij aan de algehele cyberweerbaarheid van de organisatie.

SIEM & Privacy – Hoe vind je de juiste balans tussen beveiliging en compliance?

- ✅ Voorkom een “checkbox-mentaliteit“
- 🔄 Beveiliging als continu proces
- 🎯 Compliance als basis, security als einddoel
- 🧠 Menselijke factor en security awareness
- 🤝 Samenwerking tussen security en compliance teams

“Stop met vinkjes zetten, start met beveiligen. Cybersecurity is geen checklist, maar een mindset. Compliance helpt, maar security beschermt.”

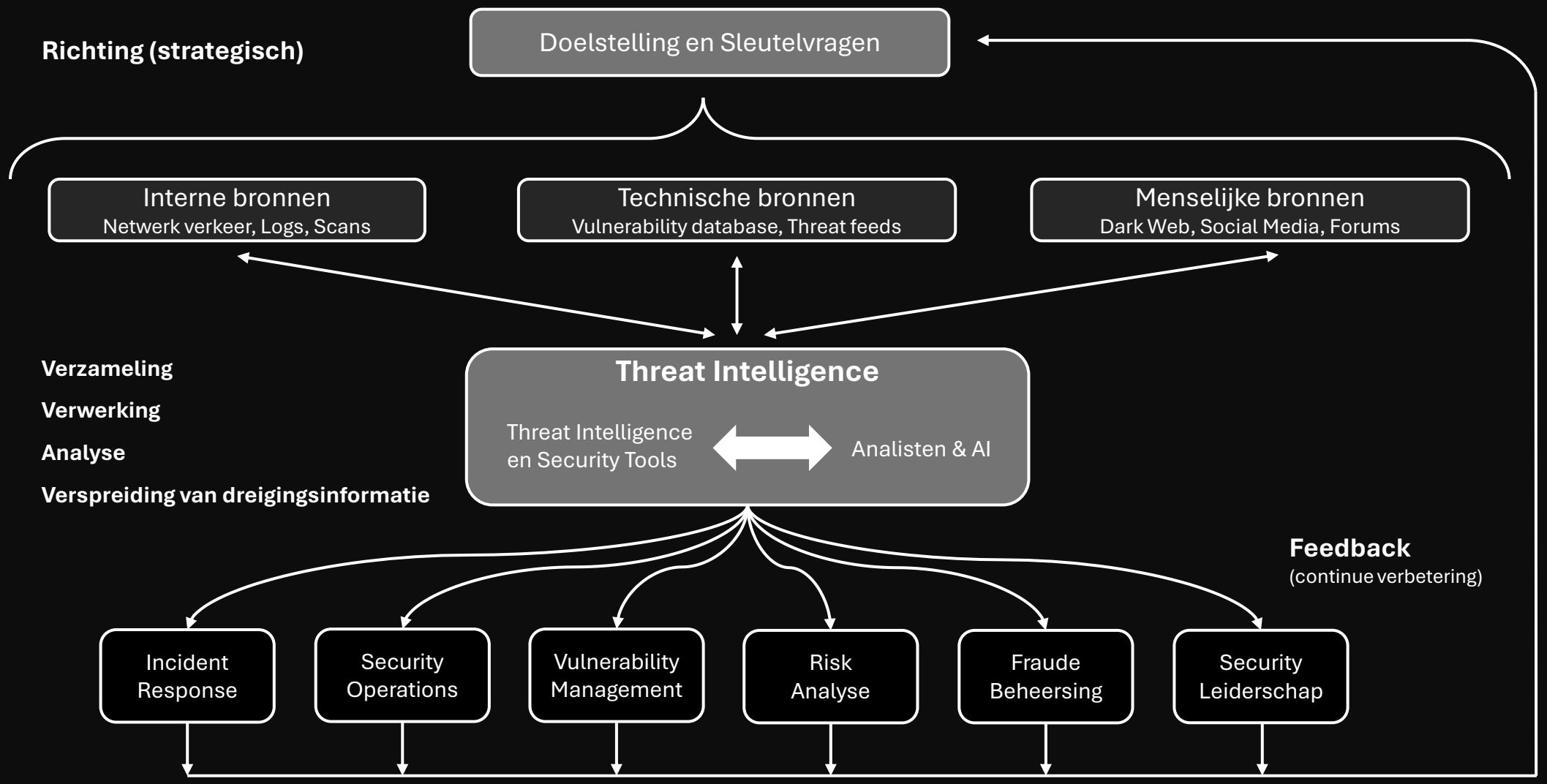
De evolutie van detectie – Hoe je dreigingen voorblijft met continue verbetering

🖐️ Van simpele logdetectie naar geavanceerde gedragsanalyse
- Eerste generatie: Handmatige loganalyse en signature-based detectie
- Tweede generatie: Geavanceerde correlatie en contextuele verrijking
- Derde generatie: AI, Machine Learning en Predictive Threat Detection

🔄 Continue verbetering in detectie
- Geavanceerde detectie met threat intelligence feeds & AI
- Proactieve dreigingsdetectie & threat hunting
- Continue optimalisatie & security awareness

⏩ De toekomst van detectie: Proactief en adaptief, blijf dreigingen voor
- ✔️ Van reactieve detectie naar real-time en voorspellende detectie
- ✔️ Dynamische threat intelligence en AI inzetten voor continue verbetering
- ✔️ Menselijke expertise combineren met geautomatiseerde technologieën
- ✔️ Continue validatie van detectiecapaciteit met Red/Purple Teaming

De evolutie van detectie – Hoe je dreigingen voorblijft met continue verbetering



SIEM selectie – Functionaliteit, schaalbaarheid en toekomst van security monitoring

Een modern SIEM moet verder gaan dan logbeheer – AI, machine learning en automatisering zijn essentieel voor snelle detectie en respons.

Van Reactief naar Proactief

- Traditionele SIEM-oplossingen focussen op logverzameling en analyse achteraf. Moderne SIEM-systemen gebruiken AI en machine learning om realtime dreigingen te detecteren en direct te reageren.

Snelle Detectie & Automatische Respons

- AI analyseert enorme hoeveelheden data en herkent afwijkend gedrag.
- Machine learning verfijnt detectieregels en verkleint false positives.
- Automatisering zorgt voor directe incidentrespons, zoals het blokkeren van verdachte activiteiten zonder menselijke tussenkomst.

Business-Driven Security

- Efficiëntie & kostenbesparing: Minder handmatige analyses, snellere incidentafhandeling.
- Risico gestuurde aanpak: Detectie en respons gebaseerd op business-impact.
- Compliance & governance: Voldoen aan regelgeving zonder extra overhead.

SIEM selectie – Functionaliteit, schaalbaarheid en toekomst van security monitoring

Kies een SIEM dat flexibel en schaalbaar is om toekomstig dataverkeer en bedrijfsuitbreidingen te ondersteunen.

✅ Cloud-native vs. On-premises

- Cloud SIEM (bijv. Microsoft Sentinel, Splunk Cloud): schaalbaar, flexibel en minder infrastructuurbeheer.
- On-prem SIEM (bijv. IBM QRadar, ArcSight): geschikt voor organisaties met strikte dataprivacy- en compliance-eisen.

✅ Data Ingestie & Performance

- Ondersteuning voor big data-verwerking zonder performanceverlies.
- Slimme event filtering en compressie om storage-kosten te minimaliseren.

✅ Modulaire en uitbreidbare architectuur

- Ondersteuning voor multi-tenancy en hybrid-cloudomgevingen.
- Integratiemogelijkheden met EDR/XDR, SOAR en threat intelligence-platforms.

📡 **OT & IoT Security Monitoring**

- SIEM's moeten Industrieel Control System (ICS) & Operational Technology (OT)-logs kunnen verwerken.
- Ondersteuning voor OT-specifieke dreigingsdetectie en Zero Trust voor IoT-apparaten.

“Een toekomstgericht SIEM is een intelligent en schaalbaar ecosysteem dat AI, XDR en real-time detectie in IT combineert. Ga van reactief naar proactief en neutraliseer dreigingen vóór ze toeslaan!”

Vragen en antwoorden?

❓ *Vragen en antwoorden?*