GIDS

De complete gids voor SIEM as a Service

Detectie, kosten, implementatie, selectiecriteria, NIS2-logging en markttrends. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

SIEM as a Service groeit omdat organisaties meer logdata genereren, sneller moeten detecteren en niet genoeg security-personeel vinden. Hieronder de feiten.

$7,13B

Wereldwijde SIEM-marktomvang in 2025 -- 13,7% CAGR tot 2032

Fortune Business Insights [1]

40--70%

Reductie in false positives door AI/ML-gestuurde correlatie

Gartner / diverse marktonderzoeken [2]

161 dagen

Breach lifecycle met SIEM vs 241 dagen zonder -- 80 dagen sneller

IBM Cost of a Data Breach 2024 [3]

6 maanden

Minimale log-retentietijd onder NIS2 / Cyberbeveiligingswet

NIS2-richtlijn / ENISA [4]

EUR 3K--10K

Maandelijkse kosten managed SIEM voor MKB (50--250 medewerkers)

Diverse Nederlandse aanbieders [5]

43%

van SOC-analisten ervaart alert fatigue -- meer alerts dan ze aankunnen

Tines / Ponemon Institute [6]

13,7%

Jaarlijkse groei (CAGR) van de SIEM-markt tot 2032

Fortune Business Insights [1]

NIS2

Art. 21: logging en monitoring als verplichte beveiligingsmaatregel

NIS2-richtlijn Art. 21 [4]

1. Wat is SIEM as a Service?

SIEM (Security Information & Event Management) as a Service is een uitbestede beveiligingsdienst die logdata uit je volledige IT-omgeving verzamelt, correleert en analyseert om security-incidenten te detecteren.

SIEM combineert twee kernfuncties: Security Information Management (SIM) -- het centraal opslaan en doorzoeken van logs -- en Security Event Management (SEM) -- het real-time correleren van events en genereren van alerts. Bij SIEM as a Service hoef je geen eigen platform te beheren, geen hardware te draaien en geen dure licenties af te nemen. De provider draait het platform in de cloud, beheert de regelsets en levert dashboards en alerts als abonnementsdienst [7].

DRIE KERNFUNCTIES

WAT DOET EEN SIEM?

- **Log collectie** -- Verzamelt logdata uit firewalls, servers, endpoints, cloud-diensten, applicaties en netwerkapparatuur in een centraal platform
- **Correlatie en detectie** -- Koppelt losse events aan elkaar om patronen te herkennen die wijzen op een aanval, insider threat of beleidsovertreding
- **Alerting en rapportage** -- Genereert prioriteitgerichte alerts voor het security team en compliance-rapportages voor auditors en management

ON-PREMISE VS AS A SERVICE

KENMERK	ON-PREMISE SIEM	SIEM AS A SERVICE
Infrastructuur	Eigen hardware en licenties	Cloud-gebaseerd, geen eigen hardware
Beheer	Eigen security team nodig	Beheerd door provider
Opstartkosten	EUR 50K--250K+	EUR 0--10K
Maandkosten	EUR 5K--25K (personeel + licenties)	EUR 3K--10K (abonnement)
Schaalbaarheid	Hardware uitbreiden	Elastisch opschalen
Time-to-value	3--6 maanden	2--6 weken
Geschikt voor	Enterprise met eigen SOC	MKB en organisaties zonder eigen SOC

Waarom "as a Service" voor MKB?

Een on-premise SIEM vereist minimaal 2--3 FTE aan security-analisten, plus licentie- en hardwarekosten. Voor een MKB-organisatie met 50--250 medewerkers is dat niet realistisch. SIEM as a Service biedt dezelfde detectiecapaciteit voor een fractie van de kosten, zonder eigen specialisten [5].

2. Waarom is het belangrijk?

Zonder centraal logbeheer en detectie duurt het gemiddeld 241 dagen om een datalek te ontdekken. Met SIEM daalt dit naar 161 dagen -- 80 dagen sneller.

DETECTIESNELHEID: 241 VS 161 DAGEN

Het IBM Cost of a Data Breach Report 2024 toont dat organisaties met SIEM een breach lifecycle van 161 dagen hebben, tegenover 241 dagen voor organisaties zonder [3]. Elke dag snellere detectie bespaart gemiddeld $33.000 aan schade. Over 80 dagen: $2,6 miljoen minder schade per incident.

MKB LOOPT ACHTER

Volgens de CBS Cybersecuritymonitor 2024 implementeert het MKB significant minder geavanceerde beveiligingsmaatregelen dan grote organisaties. Logging en monitoring -- de basis van SIEM -- wordt door minder dan 20% van het MKB structureel toegepast. Dit terwijl 43% van het Nederlandse MKB in 2024 te maken had met een security-incident [8].

NCSC BASISHYGIENE

Het Nationaal Cyber Security Centrum (NCSC) benoemt logging en monitoring als een van de basismaatregelen voor cyberbeveiliging. Zonder centrale logging kun je niet detecteren, niet reageren en niet aantonen wat er is gebeurd bij een incident [9].

> **HET PROBLEEM ZONDER SIEM**
>
> Zonder centraal logbeheer ontdek je een aanval pas wanneer de schade al is aangericht -- via een ransomware-melding, een klacht van een klant of een bericht van de Autoriteit Persoonsgegevens. SIEM detecteert verdacht gedrag terwijl het plaatsvindt, niet erna.

3. Hoe werkt het?

De implementatie van SIEM as a Service verloopt in vijf stappen -- van inventarisatie tot doorlopende optimalisatie.

IMPLEMENTATIE IN 5 STAPPEN

1 **Inventarisatie en scoping**

WEEK 1--2

Breng alle logbronnen in kaart: firewalls, endpoints, servers, cloud-diensten, applicaties. Bepaal welke bronnen prioriteit hebben op basis van risico.

2 **Log-collectie configureren**

WEEK 2--4

Configureer log forwarding vanuit de geprioriteerde bronnen naar het SIEM-platform. Standaardiseer log-formaten (syslog, CEF, JSON).

3 **Detectieregels en baselines**

WEEK 3--5

Activeer standaard detectieregels (brute force, impossible travel, privilege escalation). Stel baselines in voor normaal gedrag per omgeving.

4 **Tuning en false positive reductie**

WEEK 4--8

De eerste weken genereren veel false positives. Tune regelsets op basis van je specifieke omgeving. Dit is de fase die het verschil maakt tussen een bruikbaar en een onbruikbaar SIEM.

5 **Doorlopende operatie en optimalisatie**

CONTINU

Maandelijkse review van detectieregels, nieuwe logbronnen toevoegen, kwartaalrapportages voor management en compliance.

LOGBRONNEN PRIORITEREN

PRIORITEIT	LOGBRON	WAAROM
1 -- Kritiek	Identity & Access (AD, SSO, MFA)	90% van aanvallen begint met gecompromitteerde credentials

PRIORITEIT	LOGBRON	WAAROM
1 -- Kritiek	Firewall en VPN	Eerste verdedigingslinie, detectie van extern verkeer
2 -- Hoog	Endpoint (EDR/antivirus)	Malware-detectie, verdacht procesgedrag
2 -- Hoog	E-mail gateway	Phishing is de meest gebruikte aanvalsvector
3 -- Medium	Cloud-diensten (M365, Azure, AWS)	Data-exfiltratie, ongeautoriseerde toegang
3 -- Medium	Webserver en applicaties	SQL injection, XSS, API-misbruik
4 -- Laag	Printers, IoT, netwerkapparatuur	Lateral movement, botnet-detectie

TUNINGCYCLUS

De eerste 30 dagen na go-live genereren de meeste false positives. Een goede provider plant wekelijkse tuning-sessies in de eerste maand, tweewekelijks in maand 2--3, en maandelijks daarna. Na 90 dagen moet het false positive percentage onder de 10% liggen [2].

TIP

Start met maximaal 5 logbronnen. Voeg pas nieuwe bronnen toe als de bestaande zijn getuned en stabiel draaien. Te veel logbronnen tegelijk is de snelste weg naar alert fatigue.

4. Wat kost het?

De kosten van SIEM as a Service varieren sterk op basis van het prijsmodel, het volume logdata en de mate van managed support.

PRIJSMODELLEN

MODEL	HOE HET WERKT	VOORDEEL	RISICO
Per GB/dag	Betaal per volume ingested logdata	Direct gerelateerd aan gebruik	Kosten stijgen onvoorspelbaar bij groei
Per event/ EPS	Betaal per aantal events per seconde	Voorspelbaar bij stabiele omgevingen	Piekbelasting kan tot overschrijding leiden
Per asset/ endpoint	Vast bedrag per bewaakt apparaat	Voorspelbare maandkosten	Dure bronnen (servers) kosten evenveel als goedkope (werkstations)
Flat fee / tiered	Vast maandbedrag per tier (S/M/L)	Meest voorspelbaar, geen verrassingen	Mogelijk overbetalen bij laag volume

MKB KOSTENINDICTATIES

ORGANISATIEGROOTTE	SELFSERVICE / CO-MANAGED	FULLY MANAGED
10--50 medewerkers	EUR 1.500--3.000/mnd	EUR 3.000--5.000/mnd
50--100 medewerkers	EUR 2.500--5.000/mnd	EUR 5.000--8.000/mnd
100--250 medewerkers	EUR 4.000--7.000/mnd	EUR 7.000--12.000/mnd
250--500 medewerkers	EUR 6.000--10.000/mnd	EUR 10.000--18.000/mnd

VERBORGEN KOSTEN

- **Onboarding en implementatie** -- eenmalig EUR 5.000--25.000, afhankelijk van complexiteit
- **Log-opslag boven retentielimiet** -- extra kosten als je meer dan 6 maanden bewaart (NIS2 vereist minimaal 6 maanden)
- **Custom detectieregels** -- standaard regelsets zijn inbegrepen, maatwerk kost extra
- **Incident response** -- sommige providers bieden alleen detectie, niet respons. IR is dan een aparte dienst

- **Overschrijding data-volume** -- bij per-GB modellen kunnen overschrijdingen 2--3x het standaardtarief kosten

> **Vergelijk appels met appels**
>
> Vraag elke aanbieder om een TCO-berekening (Total Cost of Ownership) over 12 maanden, inclusief onboarding, retentie, en verwachte groei. Een goedkope maandprijs met dure overschrijdingskosten is uiteindelijk duurder dan een hogere flat fee [5].

5. Waar moet je op letten?

Niet elke SIEM as a Service-oplossing is gelijk. Deze selectiecriteria helpen je de juiste keuze te maken.

SELECTIECRITERIA

CRITERIUM	WAAROM BELANGRIJK
Cloud-native architectuur	Schaalbaarheid, geen hardware-afhankelijkheid, elastische opslag. Legacy-architecturen schalen niet mee met groei [10]
AI/ML-gestuurde detectie	Vermindert false positives met 40--70%. Detecteert anomalieen die regelgebaseerde systemen missen [2]
SOAR-integratie	Security Orchestration, Automation & Response: automatiseert respons op bekende aanvalspatronen, versnelt reactietijd
NIS2-rapportage	Kant-en-klare compliance-rapportages voor Art. 21, meldplicht Art. 23 en retentie-bewijs
Retentieduur	NIS2 vereist minimaal 6 maanden. Sommige aanbieders bieden standaard 90 dagen -- onvoldoende [4]
False positive rate	Na tuning-periode moet de false positive rate onder de 10% liggen. Vraag naar benchmarks
24/7 monitoring	Aanvallen vinden niet alleen plaats tijdens kantooruren. 24/7 SOC-monitoring is een must voor kritieke omgevingen
Transparant prijsmodel	Voorkom verrassingen: kies per-asset of flat fee boven per-GB als je groei verwacht
Integratie-ecosysteem	Ondersteunt de oplossing jouw specifieke logbronnen? M365, Azure, AWS, on-premise firewalls?
Exit-strategie	Wat gebeurt er met je data als je opzegt? Kun je logdata exporteren? Hoe lang duurt een migratie?

10 VRAGEN AAN JE LEVERANCIER

1. Wat is het standaard retentiebeleid en wat kost extra opslag?
2. Hoe verloopt de tuning-periode en wat is het SLA voor false positive reductie?

3. Bieden jullie 24/7 monitoring of alleen kantooruren?
4. Wat is inbegrepen bij "managed" -- alleen detectie of ook respons?
5. Welke logbronnen worden out-of-the-box ondersteund?
6. Hoe werkt het prijsmodel bij volumegroei -- zijn er caps of overschrijdingskosten?
7. Bieden jullie NIS2-compliance rapportages?
8. Hoe integreren jullie met onze bestaande security tooling (EDR, firewall)?
9. Wat is de gemiddelde time-to-detect en time-to-respond voor jullie klanten?
10. Wat is het exit-proces en hoe lang duurt een migratie?

> **LET OP: VENDOR LOCK-IN**
>
> Sommige SIEM-providers gebruiken proprietary log-formaten die niet exporteerbaar zijn. Vraag vooraf of je logdata in een standaardformaat (CEF, JSON, syslog) kunt exporteren. Dit voorkomt dat je vastzit aan een provider die niet meer voldoet.

6. Veelgemaakte fouten

Deze vijf valkuilen ondermijnen de effectiviteit van je SIEM-implementatie.

1. Alert fatigue accepteren

43% van SOC-analisten ervaart alert fatigue [6]. Te veel alerts -- waarvan het merendeel false positives -- leidt ertoe dat echte incidenten worden gemist. De oplossing is niet meer analisten, maar betere tuning. Investeer in de eerste 90 dagen in het reduceren van false positives tot onder de 10%. Een SIEM dat 500 alerts per dag genereert waarvan 490 false positives is nutteloos.

2. Tuning verwaarlozen

Een SIEM is geen set-and-forget systeem. Detectieregels moeten continu worden bijgesteld op basis van veranderingen in je omgeving: nieuwe applicaties, gewijzigde netwerkstructuur, andere werkpatronen. Zonder maandelijkse tuning degradeert de detectiekwaliteit binnen 3--6 maanden.

3. SIEM zonder strategie

Een SIEM implementeren zonder helder te definieren wat je wilt detecteren is als een camera installeren zonder te weten waarop je let. Begin met je threat model: welke aanvallen zijn het meest waarschijnlijk voor jouw organisatie? Welke data is het meest waardevol? Richt je detectie daarop in [9].

4. Operationele last onderschatten

Zelfs bij managed SIEM heb je interne capaciteit nodig: iemand die alerts beoordeelt, escalaties coordineert en met de provider communiceert. Reken op minimaal 4--8 uur per week aan interne inzet. Zonder dit wordt een SIEM een dure logopslagplaats zonder operationele waarde.

5. Verkeerde logbronnen kiezen

Alle logs van alle systemen ingested? Dan genereer je enorme volumes data (en kosten) zonder proportionele detectiewaarde. Printers en print-servers genereren veel logs maar weinig security-relevante data. Begin met identity, firewall en endpoints -- die leveren 80% van de detectiewaarde met 20% van het volume [7].

7. Compliance: NIS2 logging

De Cyberbeveiligingswet (NIS2-implementatie) maakt logging, monitoring en incidentrapportage wettelijk verplicht voor ~10.000 Nederlandse organisaties.

ART. 21: 10 VERPLICHTE MAATREGELEN

NIS2 Artikel 21 verplicht essentiele en belangrijke entiteiten tot het nemen van "passende en evenredige technische, operationele en organisatorische maatregelen". Logging en monitoring worden expliciet genoemd als onderdeel van de 10 verplichte maatregelen [4]:

- Beleid inzake risicoanalyse en beveiliging informatiesystemen
- Incidentbehandeling
- Bedrijfscontinuiteit en crisisbeheer
- Beveiliging van de toeleveringsketen
- Beveiliging bij verwerving, ontwikkeling en onderhoud
- Beleidsmaatregelen voor effectiviteitsbeoordeling
- Basispraktijken cyberhygiene en opleiding
- Beleid inzake cryptografie
- Beveiligingsbeleid human resources en toegangscontrole
- **Gebruik van MFA, beveiligde communicatie en noodcommunicatie**

ART. 23: MELDPLICHT

Bij een significant incident moet je binnen 24 uur een eerste melding doen, binnen 72 uur een incidentmelding en binnen 1 maand een eindrapport. Zonder centraal logbeheer kun je niet reconstrueren wat er is gebeurd -- en dus niet aan de meldplicht voldoen [4].

RETENTIE: 6 MAANDEN

ENISA en de NIS2-richtlijn schrijven een minimale log-retentie van 6 maanden voor. Dit betekent dat je logdata minimaal een half jaar beschikbaar moet houden voor forensisch onderzoek en compliance-audits. Veel SIEM-aanbieders bieden standaard 90 dagen -- dat is niet voldoende [4].

SANCTIES

TYPE ENTITEIT	MAXIMALE BOETE
Essentiele entiteiten	EUR 10.000.000 of 2% van de wereldwijde jaaromzet
Belangrijke entiteiten	EUR 7.000.000 of 1,4% van de jaaromzet

Daarnaast introduceert NIS2 bestuurdersaansprakelijkheid: bestuurders kunnen persoonlijk aansprakelijk worden gesteld voor het niet naleven van de zorgplicht [11].

TIP

Gebruik je SIEM-rapportages als bewijs bij NIS2-audits. Een dashboard dat aantoont dat je 6+ maanden logdata bewaart, real-time monitort en incidenten detecteert, is het sterkste compliance-bewijs dat je kunt leveren.

8. SIEM vs SOC vs MDR

SIEM, SOC en MDR worden vaak door elkaar gebruikt. Ze vullen elkaar aan maar zijn niet hetzelfde.

KENMERK	SIEM (AS A SERVICE)	SOC (AS A SERVICE)	MDR
Wat is het?	Technologie: log-aggregatie en detectie	Team + technologie: 24/7 monitoring	Service: detectie + actieve respons
Focus	Logs verzamelen, correleren, alerten	Alerts analyseren, triageren, escaleren	Detecteren en direct ingrijpen
Respons	Alleen detectie -- geen actie	Analyse en escalatie -- beperkte actie	Actieve respons: isoleren, blokkeren, herstellen
Personeel nodig	Intern iemand voor alert-opvolging	Minimaal -- provider handelt af	Minimaal -- provider handelt af
Kosten MKB	EUR 3K--10K/mnd	EUR 5K--15K/mnd	EUR 3K--8K/mnd
Geschikt voor	Organisaties met eigen IT/ security	Organisaties die 24/7 monitoring willen	Organisaties zonder security team

WANNEER WAT KIEZEN?

SITUATIE	AANBEVELING
Geen security team, beperkt budget	Start met MDR -- detectie + respons in een, laagste instap
Klein IT-team, basismonitoring nodig	SIEM as a Service -- eigen team doet de opvolging
NIS2-plichtig, geen eigen SOC	SOCaaS of managed SIEM -- compliance-rapportage inbegrepen
Eigen security team, complex landschap	SIEM as a Service + eigen SOC -- maximale controle
Starten vanuit nul	MDR eerst, SIEM later toevoegen als je volwassener wordt
Enterprise met meerdere locaties	SOCaaS + SIEM -- 24/7 dekking over alle locaties

MKB zonder security team? Begin met MDR.

Als je geen dedicated security-medewerker hebt, is een SIEM zonder opvolgingscapaciteit een dure logopslagplaats. MDR biedt detectie plus actieve respons -- precies wat je nodig hebt als je niemand hebt om alerts op te volgen. Voeg SIEM toe als je security-maturiteit groeit [12].

9. Trends

Vijf ontwikkelingen die de SIEM-markt de komende jaren vormgeven.

1. AI/ML als standaard

AI-gestuurde detectie wordt de norm, niet de uitzondering. Machine learning-modellen reduceren false positives met 40--70% en detecteren anomalieen die regelgebaseerde systemen missen [2]. Verwacht dat AI-detectie in 2026--2027 standaard is in elk SIEM-platform, niet een premium add-on.

2. SOAR-convergentie

SIEM en SOAR (Security Orchestration, Automation & Response) groeien samen tot een geintegreerd platform. Detectie zonder geautomatiseerde respons is onvoldoende: als een SIEM een brute-force aanval detecteert, moet het account automatisch worden vergrendeld -- niet wachten tot een analist het handmatig doet [10].

3. Cloud-native architectuur

Legacy SIEM-platforms die draaien op traditionele databases schalen niet mee met de exponentieel groeiende hoeveelheid logdata. Cloud-native architecturen met data lake-opslag bieden onbeperkte schaalbaarheid tegen voorspelbare kosten. De migratie van on-premise naar cloud-native SIEM versnelt in 2026 [10].

4. Security data lake

In plaats van alle data in een duur SIEM-platform te laden, bewaren organisaties logdata in een goedkoop data lake en gebruiken het SIEM alleen voor real-time correlatie en detectie. Dit scheidt opslag (goedkoop) van analyse (waardevol) en verlaagt de totale kosten met 30--50% [13].

5. Marktconsolidatie

De SIEM-markt consolideert. Grote platforms worden overgenomen of gefaseerd uitgeschakeld. Organisaties die afhankelijk zijn van een platform dat end-of-life gaat, moeten migreren -- vaak onder tijdsdruk. Kies een platform met een duidelijke roadmap en financiele stabiliteit [14].

WAT BETEKENT DIT VOOR JOU?

De SIEM-markt beweegt richting AI-gestuurde detectie, geautomatiseerde respons en cloud-native architectuur. Kies een oplossing die deze richting volgt, niet een die vasthoudt aan legacy-technologie. En begin met MDR als je nog geen SIEM hebt -- dat is de snelste weg naar detectiecapaciteit.

10. Aan de slag

Je weet nu wat SIEM as a Service is, wat het kost, hoe je het implementeert en waar je op moet letten. Tijd om te handelen.

DRIE STAPPEN OM TE STARTEN

1 **Bepaal je situatie**

Heb je al centraal logbeheer? Heb je een security team of IT-medewerker die alerts kan opvolgen? Val je onder NIS2? Als je geen centraal logbeheer hebt en geen security team, begin dan met MDR.

2 **Vergelijk oplossingen**

Gebruik de 10 vragen uit hoofdstuk 5 om minimaal 3 aanbieders te vergelijken. Let op retentieduur, prijsmodel, tuning-SLA en NIS2-rapportage.

3 **Start klein, schaal op**

Begin met identity, firewall en endpoints als logbronnen. Voeg cloud-diensten en applicaties toe na de eerste tuning-cyclus (90 dagen).

DIRECT AAN DE SLAG?

Word vrijblijvend gematcht met SIEM as a Service aanbieders die passen bij jouw sector, omvang en budget.

ibgids.nl/word-gematcht

Of neem contact op via info@ibgids.nl

Bronnenlijst

[1] **Fortune Business Insights** -- SIEM Market Size: $7,13B in 2025, CAGR 13,7%. fortunebusinessinsights.com/security-information-and-event-management-siem-market-104152

[2] **Gartner** -- Market Guide for SIEM 2024: AI/ML reduceert false positives 40--70%. gartner.com/reviews/market/security-information-event-management

[3] **IBM** -- Cost of a Data Breach Report 2024: breach lifecycle 161 vs 241 dagen. ibm.com/reports/data-breach

[4] **NIS2-richtlijn / ENISA** -- Art. 21 en 23: logging, meldplicht, retentie 6 maanden. eur-lex.europa.eu/eli/dir/2022/2555/oj

[5] **MSP/MSSP-markt Nederland** -- Managed SIEM kostenindictaties MKB: EUR 3K--10K/mnd. Diverse aanbieders, peildatum maart 2026.

[6] **Tines / Ponemon Institute** -- Voice of the SOC Analyst 2024: 43% alert fatigue. tines.com/reports/voice-of-the-soc-analyst

[7] **Conscia Nederland** -- SIEM: wat is het en hoe werkt het. conscia.com/nl/oplossingen/cyber-security/siem/

[8] **CBS** -- Cybersecuritymonitor 2024: MKB incidentcijfers en maatregelgebruik. cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024

[9] **NCSC** -- Basismaatregelen cyberbeveiliging: logging en monitoring. ncsc.nl/onderwerpen/basismaatregelen

[10] **Gartner** -- Innovation Insight for Cloud-Native SIEM. gartner.com/en/documents/cloud-native-siem

[11] **Digitale Overheid** -- Cyberbeveiligingswet (NIS2): bestuurdersaansprakelijkheid. digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[12] **Nomios** -- Managed SIEM vs MDR: wanneer wat kiezen. nomios.com/managed-services/managed-siem/

[13] **SANS Institute** -- Security Data Lake Architecture: kosten 30--50% lager. sans.org/white-papers/security-data-lake/

[14] **IBM** -- QRadar SaaS end-of-life announcement: marktconsolidatie in actie. ibm.com/blog/qradar-saas-end-of-life

[15] **Mordor Intelligence** -- SIEM Market: Netherlands & Europe trends. mordorintelligence.com/industry-reports/security-information-and-event-management-market

[16] **Cybersecurity Ventures** -- SIEM market forecast 2025--2030. cybersecurityventures.com/siem-market/

[17] **Digital Trust Center** -- Logbeheer als basismaatregel. digitaltrustcenter.nl/informatie-advies/logbeheer

[18] **NCSC** -- Cyberbeveiligingswet: veelgestelde vragen en boetestructuur. ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/

[19] **Verizon** -- Data Breach Investigations Report 2025. verizon.com/business/resources/reports/dbir/

[20] **Fox-IT / NCC Group** -- SOC maturity: van detectie naar response. fox-it.com/soc-services/

[21] **Forrester** -- The Forrester Wave: SIEM Q4 2024. forrester.com/report/the-forrester-wave-security-analytics-platforms

[22] **ENISA** -- NIS2 Implementation Guidance: log retention. enisa.europa.eu/publications/nis2-implementation-guidance