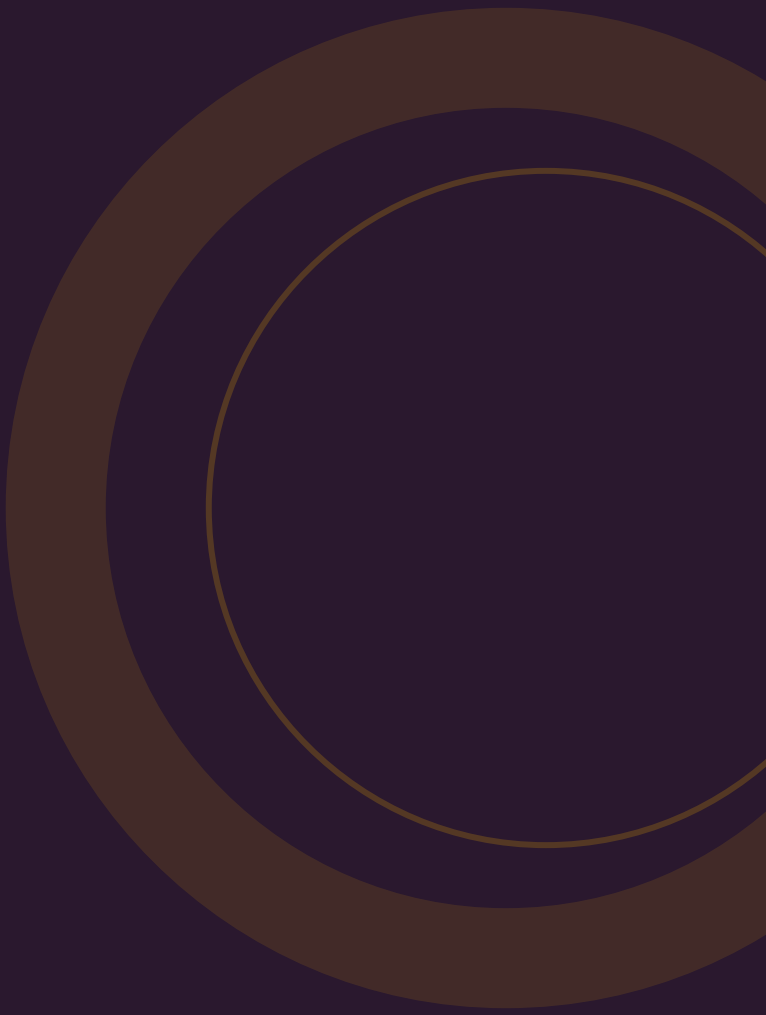
GIDS

De complete gids voor managed SIEM

Wat het kost, hoe het werkt, waar je op moet letten en hoe je de juiste aanbieder kiest. Met actuele Nederlandse marktdata.



Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

De belangrijkste cijfers over managed SIEM, het dreigingslandschap en de Nederlandse markt op een rij.

EUR 270K

Gemiddelde schade per cyberincident voor MKB in Nederland

Apex Security [1]

241 dagen

Gemiddelde tijd om een datalek te identificeren en te beperken -- laagste in 9 jaar

IBM Cost of Data Breach 2025 [2]

88%

van MKB-datalekken bevat ransomware -- bij grote organisaties is dit 39%

Verizon DBIR 2025 [3]

29 min

eCrime breakout time -- de tijd die aanvallers nodig hebben om zich lateraal te verplaatsen

CrowdStrike Global Threat Report 2026 [4]

40–60%

kostenbesparing bij managed SIEM ten opzichte van een eigen SIEM-implementatie

Comparitech / UnderDefense [5]

USD 8,6 mrd

Wereldwijde SIEM-marktomvang in 2026 -- groeiend met 6,5% CAGR

ResearchAndMarkets [6]

~10.000

Nederlandse organisaties die onder de Cyberbeveiligingswet (NIS2) vallen

Digitale Overheid [7]

121+

unieke ransomware-incidenten in Nederland in 2024 (Project Melissa)

NCSC Cybersecuritybeeld 2025 [8]

1. Wat is managed SIEM?

Managed SIEM is een dienst waarbij een externe aanbieder het volledige beheer van je Security Information & Event Management-systeem overneemt.

Een SIEM-systeem verzamelt loggegevens uit je hele IT-omgeving -- firewalls, servers, endpoints, cloud-diensten, netwerkapparatuur -- en correleert deze data om verdachte activiteiten te detecteren. Bij managed SIEM hoef je dat niet zelf te doen. De aanbieder beheert het platform, configureert de detectieregels, monitort 24/7 en escaleert bij verdachte activiteiten naar jouw team.

WAT DOET EEN MANAGED SIEM-DIENST?

- **Logverzameling** -- Automatisch logs ophalen uit al je IT-systemen
- **Correlatie en analyse** -- Patronen herkennen die wijzen op een aanval
- **24/7 monitoring** -- Een SOC-team bewaakt je omgeving dag en nacht
- **Alerting en escalatie** -- Bij verdachte activiteit word je direct geinformeerd
- **Rapportage** -- Periodieke rapporten over dreigingen, incidenten en trends
- **Compliance-ondersteuning** -- Logretentie en rapportage voor NIS2, ISO 27001

> **Managed SIEM vs SIEM as a Service:** Bij SIEM as a Service krijg je toegang tot een SIEM-platform in de cloud, maar moet je zelf de regels configureren en alerts beoordelen. Bij managed SIEM doet de aanbieder dit allemaal voor je. Je hoeft geen eigen security-analisten in dienst te hebben.

2. Waarom is managed SIEM belangrijk?

Aanvallers worden sneller, aanvallen complexer en de regelgeving strenger. Zonder professionele monitoring loop je als MKB-organisatie onacceptabele risico's.

HET DREIGINGSLANDSCHAP

De eCrime breakout time -- de tijd die een aanvaller nodig heeft om zich van het eerste gecompromitteerde systeem lateraal door je netwerk te bewegen -- is gedaald naar 29 minuten [4]. Dat betekent dat je minder dan een half uur hebt om een aanval te detecteren en te stoppen voordat de schade escaleert.

Ransomware is aanwezig in 88% van alle MKB-datalekken [3]. In Nederland werden in 2024 minimaal 121 unieke ransomware-incidenten geregistreerd [8]. De gemiddelde schade per cyberincident voor een MKB-organisatie bedraagt EUR 270.000 [1].

WAAROM MKB HET ZELF NIET KAN

Een eigen SIEM-implementatie kost in het eerste jaar EUR 50.000 tot 150.000 aan licenties, hardware en implementatie [5]. Daar komen 2-3 fulltime security-analisten bovenop die de alerts moeten beoordelen -- 24 uur per dag, 7 dagen per week. Voor de meeste MKB-organisaties is dat niet realistisch.

Managed SIEM biedt dezelfde functionaliteit voor 40-60% minder kosten [5], zonder dat je zelf personeel hoeft aan te trekken in een krappe arbeidsmarkt met meer dan 6.000 IT-security specialisten in Nederland [9].

> **DENK HIERAAN**
> 60% van kleine bedrijven gaat failliet binnen 6 maanden na een ernstig cyberincident. Managed SIEM is geen luxe maar een noodzakelijke investering in de continuiteit van je organisatie.

3. Hoe werkt managed SIEM?

Van onboarding tot dagelijkse monitoring: zo ziet het proces eruit.

1 Intake en scopebepaling

1-2 WEKEN

De aanbieder inventariseert je IT-omgeving: welke systemen, hoeveel endpoints, welke cloud-diensten. Samen bepaal je de scope en het gewenste serviceniveau.

2 Onboarding en configuratie

1-3 WEKEN

Log-collectors worden geinstalleerd, bronnen worden aangesloten op het SIEM-platform. De aanbieder configureert detectieregels, dashboards en escalatieprocedures.

3 Tuning en baseline

2-4 WEKEN

De eerste weken worden false positives weggetuned en wordt een baseline van normaal netwerkverkeer opgebouwd. Dit is kritiek voor betrouwbare alerting.

4 Operationele monitoring

DOORLOPEND

Het SOC-team monitort 24/7 je omgeving. Bij verdachte activiteit ontvang je een alert met context, impactbeoordeling en aanbevolen acties.

5 Rapportage en optimalisatie

MAANDELIJKS/KWARTAAL

Je ontvangt periodieke rapportages over gedetecteerde dreigingen, afgehandelde incidenten en aanbevelingen voor verbetering van je beveiligingshouding.

TIP

Vraag de aanbieder naar de gemiddelde tijd tot onboarding. Goede managed SIEM-aanbieders kunnen binnen 2-4 weken operationeel zijn, waar een eigen SIEM-implementatie 3-6 maanden kan duren.

4. Wat kost managed SIEM?

De kosten hangen af van het aantal endpoints, logvolume en gewenst serviceniveau. Hieronder een overzicht voor MKB-organisaties.

COMPONENT	BASIS	STANDAARD	PREMIUM
Endpoints	Tot 50	50-150	150-500
Monitoring	8×5	24/7	24/7 + dedicated analist
Logbronnen	5-10	10-25	25+
Maandelijks	EUR 1.500 - 2.500	EUR 2.500 - 5.000	EUR 5.000 - 10.000
Jaarlijks	EUR 18.000 - 30.000	EUR 30.000 - 60.000	EUR 60.000 - 120.000

ALTERNATIEVE PRIJSMODELLEN

MODEL	PRIJSRANGE	GESCHIKT VOOR
Per gebruiker/mnd	EUR 10 - 25 [10]	Organisaties met veel gebruikers, weinig servers
Per endpoint/mnd	EUR 5 - 25 [11]	Organisaties met veel apparaten
Per GB logdata/mnd	EUR 45 - 180 [11]	Organisaties met voorspelbaar logvolume
Vast bedrag/mnd	EUR 1.500 - 10.000 [11]	Organisaties die kostzekerheid willen

VERGELIJKING MET IN-HOUSE SIEM

KOSTENPOST	IN-HOUSE SIEM	MANAGED SIEM
Eerste jaar	EUR 50.000 - 150.000 [5]	EUR 18.000 - 60.000
Personeel (jaarlijks)	EUR 120.000 - 250.000 (2-3 FTE)	Inbegrepen
Implementatietijd	3-6 maanden	2-4 weken
24/7 dekking	Moeilijk voor MKB	Standaard

5. Waar moet je op letten bij de keuze?

Niet elke managed SIEM-aanbieder is hetzelfde. Let op deze selectiecriteria.

TECHNISCHE CRITERIA

- **Breedte van logbronnen** -- Kan de aanbieder alle relevante bronnen aansluiten? (firewalls, cloud, endpoints, applicaties)
- **Detectieregels en use cases** -- Hoeveel standaard detectieregels worden meegeleverd? Worden ze regelmatig bijgewerkt?
- **Threat intelligence integratie** -- Gebruikt de aanbieder actuele dreigingsinformatie voor detectie?
- **Retentieperiode** -- Hoe lang worden loggegevens bewaard? NIS2 kan specifieke eisen stellen.
- **Schaalbaarheid** -- Kan de dienst meegroeien als je organisatie groeit?

OPERATIONELE CRITERIA

- **Responstijd bij alerts** -- Wat is de gegarandeerde responstijd (SLA)?
- **Escalatieprocedure** -- Hoe en wanneer word je geinformeerd? Via welk kanaal?
- **Rapportage** -- Hoe vaak ontvang je rapporten? Welk detailniveau?
- **Onboarding-duur** -- Hoe snel kan de dienst operationeel zijn?
- **Exit-strategie** -- Wat gebeurt er als je wilt overstappen? Krijg je je data?

10 VRAGEN VOOR JE AANBIEDER

1. Hoeveel logbronnen kunnen jullie aansluiten en welke typen?
2. Wat is jullie gemiddelde MTTD (Mean Time to Detect)?
3. Hoeveel standaard detectieregels/use cases worden meegeleverd?
4. Hoe vaak worden detectieregels bijgewerkt op basis van nieuwe dreigingen?
5. Wat is de retentieperiode voor loggegevens en is die aanpasbaar?
6. Bieden jullie 24/7 monitoring of alleen kantooruren?
7. Hoe ziet het escalatieproces eruit bij een kritieke alert?
8. Ondersteunen jullie NIS2 compliance-rapportage?
9. Hoe lang duurt de onboarding en wat is daarvoor nodig van onze kant?
10. Wat zijn de opzegvoorwaarden en hoe verloopt een eventuele exit?

6. Veelgemaakte fouten

Voorkom deze valkuilen bij het kiezen en gebruiken van managed SIEM.

Fout 1: Alleen compliance-gedreven kiezen

Sommige organisaties implementeren managed SIEM puur omdat NIS2 het vereist, zonder na te denken over wat ze echt willen detecteren. Resultaat: een dure dienst die rapportages produceert maar geen echte dreigingen vindt. Zorg dat de scope aansluit bij je risicoanalyse, niet alleen bij een compliance-checklist.

Fout 2: Te weinig logbronnen aansluiten

Een SIEM is zo goed als de data die het ontvangt. Als je alleen je firewall aansluit maar niet je endpoints, cloud-omgeving en Active Directory, mis je het overgrote deel van de aanvallen. Sluit alle relevante bronnen aan, ook als dat meer kost.

Fout 3: Geen duidelijke escalatieprocedure

Je ontvangt een kritieke alert op vrijdagavond -- maar wie in jouw organisatie neemt actie? Zonder duidelijke escalatieprocedure aan jouw kant is de monitoring waardeloos. Stel vooraf vast wie bereikbaar is en welke acties ze mogen nemen.

Fout 4: Verwachten dat managed SIEM alles oplost

Managed SIEM detecteert dreigingen, maar lost ze niet automatisch op. Je hebt nog steeds een incident response-plan nodig en iemand die actie onderneemt. Overweeg een aanbieder die ook incident response biedt, of regel dit apart.

Fout 5: Niet tunen na de opstartfase

Na de eerste tuning-fase denken veel organisaties dat het klaar is. Maar je IT-omgeving verandert continu. Nieuwe applicaties, nieuwe medewerkers, nieuwe cloud-diensten -- de SIEM-configuratie moet mee-evolueren. Plan kwartaalreviews met je aanbieder.

7. NIS2 en regelgeving

De Cyberbeveiligingswet (NIS2) maakt professionele monitoring voor veel organisaties een wettelijke verplichting.

CYBERBEVEILIGINGSWET (NIS2)

De Cyberbeveiligingswet gaat naar verwachting in het tweede kwartaal van 2026 in werking [7]. Circa 10.000 Nederlandse organisaties vallen eronder. De wet kent drie kernverplichtingen:

- **Zorgplicht:** passende maatregelen nemen om de continuiteit van diensten te waarborgen
- **Meldplicht:** incidenten binnen 24 uur melden bij de toezichthouder
- **Registratieplicht:** registratie bij de toezichthouder

Managed SIEM helpt bij de zorgplicht (continue monitoring) en de meldplicht (snelle detectie van incidenten). De logretentie ondersteunt de verantwoordingsplicht.

BOETES

TYPE ENTITEIT	MAXIMALE BOETE
Essentieel	EUR 10 miljoen of 2% wereldwijde jaaromzet [7]
Belangrijk	EUR 7 miljoen of 1,4% wereldwijde jaaromzet [7]

Bestuurders kunnen persoonlijk aansprakelijk worden gesteld voor onvoldoende cybersecuritymaatregelen [7].

8. Managed SIEM vs SIEM as a Service vs SOC

Drie termen die vaak door elkaar worden gebruikt, maar fundamenteel verschillen.

KENMERK	SIEM AS A SERVICE	MANAGED SIEM	SOC AS A SERVICE
Platform	Cloud SIEM	Cloud SIEM	SIEM + meer
Configuratie	Klant	Aanbieder	Aanbieder
Monitoring	Klant	Aanbieder 24/7	Aanbieder 24/7
Alert-beoordeling	Klant	Aanbieder	Aanbieder
Incident response	Klant	Beperkt/adviserend	Inbegrepen
Threat hunting	Nee	Optioneel	Vaak inbegrepen
Geschikt voor	Organisaties met eigen SOC	MKB zonder eigen analisten	Organisaties die alles uitbesteden
Kosten (MKB/mnd)	EUR 500 - 2.000	EUR 1.500 - 5.000	EUR 3.000 - 10.000+

9. Trends 2025--2026

AI-gedreven detectie en correlatie

Machine learning maakt het mogelijk om anomalieen te detecteren die met handmatige regels onmogelijk te vangen zijn. AI analyseert patronen in miljoenen logregels en markeert afwijkingen automatisch. Organisaties met security AI detecteren breaches gemiddeld 80 dagen sneller [2].

Convergentie SIEM, SOAR en XDR

De grenzen tussen SIEM, Security Orchestration Automation and Response (SOAR) en Extended Detection and Response (XDR) vervagen. Aanbieders combineren steeds meer functionaliteiten in een geintegreerd platform, wat de effectiviteit verhoogt en de kosten per functie verlaagt.

Cloud-native SIEM wordt de standaard

On-premise SIEM-installaties worden zeldzamer. Cloud-native SIEM-platforms bieden betere schaalbaarheid, snellere onboarding en lagere beheerkosten. Voor MKB-organisaties is cloud-native de logische keuze.

10. Aan de slag

Klaar om managed SIEM te implementeren? Volg deze stappen.

1. **Breng je IT-omgeving in kaart**
   Inventariseer alle systemen, applicaties en cloud-diensten die logdata genereren. Dit bepaalt de scope.

2. **Bepaal je eisen**
   8×5 of 24/7 monitoring? Welke compliance-eisen? Hoeveel logretentie? Incident response nodig?

3. **Vraag offertes op**
   Vergelijk minimaal 3 aanbieders op prijs, scope, SLA en ervaring in jouw sector.

Bronnenlijst

[1] **Apex Security** -- SIEM voor het MKB: professionele beveiliging -- apexsecurity.nl/en/siem-voor-het-mkb-professionele-beveiliging-zonder-enterpriseprijskaartje/

[2] **IBM** -- Cost of a Data Breach Report 2025 -- ibm.com/reports/data-breach

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

[4] **CrowdStrike** -- 2026 Global Threat Report -- crowdstrike.com/en-us/global-threat-report/

[5] **Comparitech** -- Managed SIEM Services -- comparitech.com/net-admin/managed-siem-services/

[6] **ResearchAndMarkets** -- SIEM Market Global Forecast 2026-2032 -- researchandmarkets.com/reports/5675188/security-information-and-event-management-market

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

[8] **NCSC** -- Cybersecuritybeeld Nederland 2025 -- ncsc.nl/actueel/nieuws/2025/11/26/cybersecuritybeeld-2025

[9] **Mordor Intelligence** -- Netherlands Cybersecurity Market -- mordorintelligence.com/industry-reports/netherlands-cybersecurity-market

[10] **Securoot** -- Tarieven -- securoot.nl/tarieven/

[11] **UnderDefense** -- Managed SIEM Pricing Guide -- underdefense.com/blog/managed-siem-pricing-guide/

[12] **CBS** -- Cybersecuritymonitor 2024 -- cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true

[13] **Cybersecurity News** -- Managed SIEM Pricing 2025 -- cybersecuritynews.com/siem-pricing/

[14] **Nomios Group** -- Managed SIEM Services -- nomios.com/managed-services/managed-siem/

[15] **Kynexis** -- NIS2 boetes Cyberbeveiligingswet -- kynexis.nl/nis2-boetes-cyberbeveiligingswet-uitgelegd/