GIDS

De complete gids voor SOC as a Service

Wat het is, wat het kost, waar je op let, NIS2-compliance en de belangrijkste valkuilen. Met actuele marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Een eigen SOC is onbetaalbaar voor het MKB. SOC as a Service maakt 24/7 monitoring bereikbaar. Dit zijn de feiten.

EUR 1,5M+
Minimale jaarkosten voor een eigen intern SOC met 24/7 dekking
Lumifi / Arctic Wolf [1]

50--70%
Kostenbesparing van SOCaaS ten opzichte van een eigen SOC
Vectra / vanRoey [2]

204 dagen
Mediaan detectietijd (dwell time) zonder continue monitoring
Mandiant [3]

30--90 dagen
Doorlooptijd van contract tot volledig operationeel SOCaaS
Expel / ClearNetwork [4]

$4,88M
Gemiddelde kosten van een datalek wereldwijd (2024)
IBM Cost of a Data Breach [5]

Q2 2026
Verwachte inwerkingtreding Cyberbeveiligingswet (NIS2) -- monitoring verplicht
Digitale Overheid [6]

8--14 FTE
Minimum aantal analisten voor een eigen SOC met 24/7 bezetting
Expel / Blackpoint Cyber [7]

$10--20
Kosten per asset per maand voor SOCaaS -- instap voor MKB
UnderDefense / CP Cyber [8]

1. Wat is SOC as a Service?

SOC as a Service (SOCaaS) is een uitbestede beveiligingsdienst waarbij een externe partij 24/7 je IT-omgeving monitort, dreigingen detecteert en bij incidenten escaleert of ingrijpt.

Een Security Operations Center (SOC) combineert mensen, processen en technologie om cyberaanvallen te detecteren en te stoppen. Bij SOCaaS hoef je dat niet zelf op te bouwen -- de aanbieder doet dit voor meerdere organisaties tegelijk, waardoor de kosten worden gedeeld [1].

WAT DOET EEN SOC PRECIES?

- **Monitoren** -- 24/7 toezicht op je netwerk, endpoints, cloud en applicaties
- **Detecteren** -- Verdachte activiteiten herkennen via SIEM, threat intelligence en gedragsanalyse
- **Analyseren** -- Alerts onderzoeken, false positives filteren, ernst bepalen
- **Escaleren** -- Bij bevestigde dreigingen direct je team waarschuwen met context en advies
- **Rapporteren** -- Periodieke overzichten van dreigingen, trends en verbeterpunten

Het verschil met een intern SOC: je hoeft geen eigen analisten aan te nemen, geen SIEM-platform te beheren en geen 24/7-bezetting te regelen. De aanbieder doet dit met gespecialiseerde teams die dagelijks dreigingen afhandelen voor tientallen organisaties tegelijk.

> **In een zin**
>
> SOCaaS is "ogen op je netwerk" -- continue bewaking door specialisten, zonder dat je zelf een beveiligingsteam hoeft op te bouwen.

2. Waarom is het belangrijk?

De meeste MKB-organisaties hebben geen eigen security-team. SOCaaS overbrugt dat gat -- en de noodzaak groeit door wetgeving en dreigingen.

EEN EIGEN SOC IS ONBETAALBAAR VOOR MKB

Een intern SOC met 24/7 dekking vereist minimaal 8--14 analisten [7]. Alleen aan personeelskosten betaal je EUR 300.000--500.000 per jaar voor de basisbezetting, en EUR 1,5M--2,5M voor een volwassen SOC met tooling, licenties en infrastructuur [1]. De gemiddelde organisatie besteedt $2,86 miljoen per jaar aan een intern SOC [9].

PERSONEELSTEKORT IN CYBERSECURITY

De Nederlandse cybersecurity-arbeidsmarkt is krap. SOC-analisten verdienen EUR 45.000--100.000+ per jaar en ontvangen meerdere aanbiedingen binnen weken [10]. Nieuwe rollen als AI Security Specialist en Detection Engineer met ML-kennis zijn sterk in opkomst. Voor MKB-organisaties is het vrijwel onmogelijk om hiermee te concurreren.

NIS2 MAAKT MONITORING VERPLICHT

De Cyberbeveiligingswet (NIS2) treedt naar verwachting in Q2 2026 in werking. Organisaties met 50+ werknemers of EUR 10M+ omzet in aangewezen sectoren moeten continu monitoren en incidenten binnen 24 uur melden [6]. Zonder een vorm van continue monitoring -- SOCaaS, MDR of eigen SOC -- is compliance vrijwel onmogelijk.

EUR 300K--500K

Minimale jaarlijkse personeelskosten voor eigen SOC (5--6 FTE)

Glassdoor / brancheanalyse [10]

12--18 mnd

Doorlooptijd om een eigen SOC operationeel te krijgen

Expel [4]

DWELL TIME ZONDER MONITORING

Zonder continue monitoring duurt het gemiddeld 204 dagen voordat een inbraak wordt ontdekt [3]. Met SOCaaS of MDR gaat dit terug naar uren tot dagen. Elke dag dat een aanvaller onopgemerkt in je netwerk zit, vergroot de schade.

3. Hoe werkt het?

Van eerste gesprek tot 24/7 monitoring in 30--90 dagen. Dit is het typische traject.

IMPLEMENTATIETRAJECT

1 Assessment

1--2 WEKEN

Inventarisatie van je IT-omgeving, huidige tooling, detectie-gaps en risicoprofiel. Welke systemen heb je, waar zitten de blinde vlekken?

2 Onboarding en integratie

2--4 WEKEN

SIEM-koppelingen aanleggen, logbronnen aansluiten (endpoints, firewall, cloud, e-mail), playbooks configureren voor jouw omgeving.

3 Tuning en optimalisatie

2--4 WEKEN

False positives reduceren, alerts verfijnen, escalatieprocedures testen. Deze fase is cruciaal -- zonder tuning krijg je alert fatigue.

4 Volledig operationeel

WEEK 8--12

Gedefinieerde escalatieprocedures, runbooks, meetbare MTTD/MTTR. Vanaf hier draait het SOC op volle capaciteit [4].

WELKE LOGBRONNEN WORDEN AANGESLOTEN?

LOGBRON	WAT HET MONITORT	PRIORITEIT
Endpoints (EDR/XDR)	Verdacht gedrag op werkstations en servers	Must-have
Firewall / netwerk	Inkomend en uitgaand verkeer, anomalieen	Must-have
Cloud-omgeving	Azure AD, AWS, Microsoft 365 activiteit	Must-have
E-mail gateway	Phishing-pogingen, verdachte bijlagen	Belangrijk
Identiteit (IAM)	Ongebruikelijke inlogpogingen, rechtenwijzigingen	Belangrijk

LOGBRON	WAT HET MONITORT	PRIORITEIT
Applicatielogs	Verdachte activiteit in bedrijfskritieke applicaties	Optioneel

ALERTING EN ESCALATIE

SEVERITY	VOORBEELDEN	VERWACHTE RESPONSTIJD
Critical (P1)	Actieve inbraak, ransomware, data-exfiltratie	15--30 minuten
High (P2)	Malware detectie, gecompromitteerd account	30 min -- 1 uur
Medium (P3)	Verdachte inlogpogingen, beleidsovertredingen	1--4 uur
Low (P4)	Informatief, kleine afwijkingen	Volgende werkdag [11]

TIP

Sommige aanbieders claimen monitoring "binnen 30 minuten na onboarding." Dit is basismonitoring. Volledige operationele maturiteit -- met geoptimaliseerde detectieregels en lage false positive rates -- kost 8--12 weken.

4. Wat kost het?

SOCaaS is 50--70% goedkoper dan een eigen SOC. Maar de prijzen varieren sterk -- weet waar je voor betaalt.

PRIJSINDICATIES SOCAAS

SEGMENT	ENDPOINTS	GESCHATTE JAARKOSTEN	PER ENDPOINT/MAAND
Klein MKB	25--50	EUR 3.000 -- 12.000	EUR 10 -- 20
Middelgroot MKB	50--250	EUR 12.000 -- 72.000	EUR 10 -- 24
Groot MKB	250--1.000	EUR 30.000 -- 180.000	EUR 10 -- 15
Enterprise	1.000+	EUR 100.000+	Volume-korting [8]

PRIJSMODELLEN

MODEL	HOE HET WERKT	RISICO
Per endpoint/maand	Vast bedrag per gemonitord apparaat	Prijs stijgt lineair bij groei
Per gebruiker/ maand	Vast bedrag per gebruiker (alle devices)	Kan duurder zijn bij weinig devices
Flat-fee/maand	Vast maandbedrag ongeacht aantal endpoints	Overpaying bij weinig endpoints
Data-volume based	Gebaseerd op GB/dag log-ingestie	Onvoorspelbare kosten [12]

IN-HOUSE SOC VS SOCAAS

FACTOR	INTERN SOC	SOCAAS
Jaarkosten (1.000 endpoints)	EUR 1,5M -- 5M+	EUR 100.000 -- 400.000
Opstartijd	12--18 maanden	30--90 dagen
FTE nodig	Minimaal 8--14 analisten	0 (intern), aanspreekpunt nodig

FACTOR	INTERN SOC	SOCAAS
24/7 dekking	Lastig onder 12 FTE	Standaard inbegrepen
Talent risico	Hoog (schaarste NL markt)	Laag (aanbieder beheert) [2]

VERBORGEN KOSTEN

Let op data ingestion fees (extra kosten als logvolume boven limiet komt), onboarding/setup-kosten (EUR 5.000--25.000 apart), custom playbooks (maatwerkregels kosten extra) en incident surge pricing (extra kosten bij piekbelasting) [12].

Vuistregel

Alleen organisaties met 1.000+ endpoints en een security-budget van EUR 2M+ per jaar kunnen realistisch een intern SOC overwegen. Voor het MKB is SOCaaS de enige haalbare optie [1].

5. Waar moet je op letten?

Niet elke SOCaaS-aanbieder levert dezelfde kwaliteit. Deze selectiecriteria helpen je de juiste keuze te maken.

SOC-CMM MATURITY MODEL

Het SOC Capability Maturity Model (SOC-CMM) beoordeelt SOCs op vijf domeinen: Business, People, Process, Technology en Services. Vraag je aanbieder naar hun maturity level [13].

LEVEL	NAAM	MKB-RELEVANTIE
0--1	Non-existent / Initial	Veel MKB start hier -- onvoldoende
2	Managed	Minimaal nodig voor NIS2-compliance
3	Defined	Realistische ambitie -- feedbackloops en KPIs
4--5	Quantitatively Managed / Optimizing	Enterprise-niveau [13]

SLA-METRICS DIE ERTOE DOEN

METRIC	WAT HET MEET	BENCHMARK
MTTD	Mean Time to Detect -- hoe snel wordt een dreiging ontdekt	30 min -- 4 uur (top-performers)
MTTA	Mean Time to Acknowledge -- hoe snel wordt een alert erkend	5--15 minuten
MTTR	Mean Time to Respond -- hoe snel wordt gereageerd	<1 uur (excellent), 2--4 uur (goed)
Uptime	Beschikbaarheid monitoring-platform	99,9% -- 99,99%
False positive rate	Percentage foutieve alerts	<10% bij volwassen SOC [11]

10 VRAGEN AAN JE SOCAAS-AANBIEDER

1. Wat is jullie SOC-CMM maturity level?
2. Bieden jullie 24/7 monitoring met eigen analisten of via een derde partij?

3. Wat zijn de gegarandeerde MTTD en MTTR in de SLA?
4. Wat gebeurt er bij een actief incident -- escaleren jullie of grijpen jullie zelf in?
5. Welke logbronnen sluiten jullie standaard aan?
6. Hoe werkt het prijsmodel -- per endpoint, per gebruiker of flat-fee?
7. Zijn er data-ingestion limieten of overage fees?
8. Hoe lang duurt de onboarding tot volledige operationele maturiteit?
9. Hebben jullie ervaring in mijn branche?
10. Wat is de exit-strategie -- zijn logs en playbooks overdraagbaar? [14]

TIP

Vraag altijd naar referenties in jouw sector en doe een proof-of-concept van 30--60 dagen voordat je een meerjarig contract tekent.

6. Veelgemaakte fouten

Zeven valkuilen die de waarde van je SOCaaS-investering ondermijnen.

1. Verantwoordelijkheid volledig overdragen

De meest voorkomende fout: aannemen dat de aanbieder nu overal verantwoordelijk voor is. Het SOC monitort, maar jouw organisatie blijft eigenaar van incident response planning, business continuity en bestuurlijke aansprakelijkheid -- zeker onder NIS2. Stel een RACI-matrix op die exact beschrijft wie waarvoor verantwoordelijk is [14].

2. Vage SLAs zonder meetbare KPIs

Contracten zonder specifieke detectie- en responstijden laten je kwetsbaar. Wat is de maximale MTTD? MTTR? Zonder concrete cijfers is de SLA een marketingdocument. Eis meetbare KPIs: MTTD < 15 minuten, MTTR < 1 uur, maandelijkse rapportage met trendanalyse [11].

3. Geen eigen incident response plan

Geen enkele externe SOC kan voor jou plannen. Incident response planning, tabletop-oefeningen en crisismanagement blijven interne verantwoordelijkheid. Voer minimaal jaarlijks een tabletop-oefening uit met de SOCaaS-aanbieder [14].

4. Selectie puur op prijs

Kale monitoring zonder context levert een hoge false positive rate op. Vergelijk op basis van SLA's, MTTD/MTTR en inclusieve services -- niet alleen het maandbedrag. Vraag naar het SOC-CMM maturity level en referenties [15].

5. SOC als eenmalig project behandelen

Een SOC is geen go-live event -- het is een continue operationele discipline. Dreigingen evolueren, het IT-landschap verandert, detectieregels moeten meegroeien. Plan kwartaalreviews met de aanbieder, evalueer use cases en pas detectie aan op nieuwe dreigingen [14].

6. Onvolledige logbronnen aansluiten

Als het SOC alleen je firewall-logs ziet maar niet je cloud-omgeving of endpoints, heb je een vals gevoel van veiligheid. Breng alle logbronnen in kaart voor contracttekening en eis een integratieplan als onderdeel van de onboarding [15].

7. Geen branche-specifieke expertise eisen

Dreigingen verschillen per branche. Een aanbieder zonder ervaring in jouw sector begrijpt je compliance-eisen en dreigingslandschap niet. Kies een partner met bewezen sectorervaring en vraag om case studies [14].

DE KERNREGEL

SOCaaS is geen "set and forget." Het is een partnerschap. Maandelijkse review-meetings, wijzigingen doorgeven en proactieve threat hunting capabilities vragen -- dat is het verschil tussen een SOC dat werkt en een duur dashboard.

7. Compliance: NIS2

De Cyberbeveiligingswet maakt continue monitoring vrijwel verplicht. SOCaaS is voor MKB de meest realistische route naar compliance.

WAT IS NIS2?

De NIS2-richtlijn is de Europese cybersecurity-richtlijn die in Nederland wordt omgezet in de Cyberbeveiligingswet (Cbw). Het wetsvoorstel is op 4 juni 2025 ingediend bij de Tweede Kamer. Verwachte inwerkingtreding: Q2 2026 [6].

WIE VALT ERONDER?

Organisaties die actief zijn in aangewezen sectoren (energie, transport, gezondheidszorg, digitale infrastructuur, ICT-dienstverlening) en minimaal 50 werknemers hebben of een jaaromzet/balanstotaal van meer dan EUR 10 miljoen [16].

VERPLICHTINGEN RELEVANT VOOR SOCAAS

VERPLICHTING	WAT HET INHOUDT	SOCAAS-RELEVANTIE
Zorgplicht	Risicoanalyse, incidentbeheersing, continuiteitsplanning, MFA	SOCaaS helpt bij monitoring, detectie en incident response
Meldplicht	Eerste melding binnen 24 uur, uitgebreid binnen 72 uur, eindrapport binnen 1 maand	SOCaaS versnelt detectie en onderzoek voor snelle melding
Supply chain security	Beveiliging van de toeleveringsketen	SOCaaS-aanbieder moet zelf ook compliant zijn
Bestuurdersaansprakelijkheid	Bestuurders zijn persoonlijk aansprakelijk voor naleving	Aantoonbare monitoring versterkt positie [17]

BOETES NIS2

Essentiele entiteiten: tot EUR 10.000.000 of 2% van de wereldwijde jaaromzet. Belangrijke entiteiten: tot EUR 7.000.000 of 1,4% van de jaaromzet [17].

SOCAAS ALS NIS2-ENABLER

SOCaaS is niet expliciet verplicht onder NIS2, maar de zorgplichtmaatregelen vereisen dat organisaties risico's monitoren en incidenten beheersen. In de praktijk is een vorm van continue monitoring -- SOCaaS, MDR of eigen SOC -- vrijwel noodzakelijk om aan de zorgplicht te voldoen [6].

Een SOC 2 Type II-rapport van je aanbieder toont aan dat de maatregelen "effectief" zijn, wat NIS2 expliciet eist [18].

> **Praktisch**
>
> Organisaties die hun security operations centraliseren via een SOC (intern of uitbesteed) kunnen incidenten sneller afhandelen en beter rapporteren. Voor MKB zonder eigen SOC-team is SOCaaS de meest realistische route naar NIS2-compliance.

8. SOC vs MDR vs SIEM vs MSSP

Vier afkortingen die vaak door elkaar worden gebruikt -- maar fundamenteel verschillen. Dit overzicht helpt je de juiste oplossing te kiezen.

TERM	TYPE	WAT KRIJG JE?	RESPONS
SIEM	Technologie	Gecentraliseerd logbeheer, correlatie en analyse van security events	Geen -- alleen data
SOCaaS	Managed service	24/7 monitoring, detectie en escalatie als dienst	Meldt en escaleert naar jouw team
MDR	Managed service	SOC + detectie + actieve respons (isoleren, blokkeren, containment)	Grijpt zelf in
MSSP	Managed service	Breed security-beheer, device-management, alerts doorgeven	Reactief, minder diepgang [19]

SOCAAS VS MDR -- HET KERNVERSCHIL

ASPECT	SOCAAS	MDR
Focus	Monitoring, detectie, escalatie	Monitoring, detectie + actieve respons
Bij een incident	Meldt en adviseert -- jij moet handelen	Isoleert endpoints, blokkeert IP's, schakelt accounts uit
Aanpak	Vaak alert-driven (reactief)	Proactief (threat hunting + containment)
Snelheid	Notificatie binnen 30 min -- 2 uur	Actieve respons in minuten
Instapprijs	Lager	Hoger, maar meer waarde per EUR [19]

> **Praktisch**
>
> SOCaaS is "ogen op je netwerk", MDR is "ogen + handen op je netwerk." Voor organisaties zonder eigen security team is MDR doorgaans de betere keuze omdat je geen eigen incident response capaciteit nodig hebt.

WANNEER WELKE KIEZEN?

SITUATIE	ADVIES
MKB zonder security-team	MDR -- laat een specialist het doen
MKB met beperkt IT-team	SOCaaS als instap, MDR als budget het toelaat
Enterprise met eigen SOC	Co-managed SOC of SIEM + MDR
Compliance-gedreven (NIS2)	SOCaaS of MDR -- beide voldoen aan monitoring-eisen

9. Trends 2025--2026

De SOCaaS-markt verandert snel. Vijf ontwikkelingen die je moet kennen.

1. Autonomous SOC en AI-agents

AI-agents nemen taken van L1-analisten over: alert-samenvatting, onderzoek plannen, bewijs analyseren en remediatie-beslissingen nemen met minimale menselijke interventie. De transitie gaat van statische SOAR-playbooks naar agentic AI die kan redeneren en handelen [20]. Dit drukt de kosten en vergroot de capaciteit.

2. Platform-consolidatie

84% van bedrijven streeft naar unified platforms [20]. Tool consolidation wordt de default strategie: minder platforms betekent minder overhead. De grenzen tussen SOCaaS, MDR, SIEM en XDR vervagen.

3. SOC + cyberverzekering bundeling

Aanbieders combineren SOC-diensten met een cyberverzekeringspolis in een pakket. Dit verlaagt het risico voor de verzekeraar en geeft de klant een totaaloplossing: preventie, detectie en financiele dekking in een contract.

4. NIS2-effect: vraagpiek

De verwachte inwerkingtreding van de Cyberbeveiligingswet in Q2 2026 drijft een golf van nieuwe vraag. Duizenden organisaties die nu geen continue monitoring hebben, moeten dat voor de deadline regelen [6].

5. Outcome-based pricing

Een nieuw prijsmodel waarbij je betaalt per afgehandeld incident in plaats van per endpoint. Dit verschuift het risico naar de aanbieder en maakt kosten voorspelbaarder voor MKB [8].

$6,8--8,4B

Wereldwijde SOCaaS-markt in 2025 -- groeit naar $15--29B in 2034

Precedence Research / Fortune BI [21]

9--14% CAGR

Jaarlijkse groei van de SOCaaS-markt tot 2035

MarketsandMarkets / Mordor Intel [21]

WAT BETEKENT DIT VOOR JOU?

AI maakt SOCaaS goedkoper en effectiever. NIS2 maakt het verplicht. De markt consolideert naar geintegreerde platformen. Als je nog geen continue monitoring hebt, is 2026 het moment om te starten.

10. Aan de slag

Je weet nu wat SOCaaS is, wat het kost en waar je op moet letten. Tijd voor actie.

VIJF STAPPEN OM TE STARTEN

1. **Breng je IT-landschap in kaart**
   Hoeveel endpoints, welke cloud-omgevingen, welke kritieke systemen? Dit bepaalt de scope en kosten.

2. **Bepaal je behoeftes**
   Heb je alleen monitoring nodig (SOCaaS) of ook actieve respons (MDR)? Heb je een intern IT-team dat alerts kan opvolgen?

3. **Vergelijk aanbieders**
   Gebruik de 10 vragen uit hoofdstuk 5. Vraag naar SOC-CMM level, SLA-garanties en sectorervaring.

4. **Start met een proof-of-concept**
   30--60 dagen pilot op je kritieke systemen. Meet de kwaliteit van alerts en de snelheid van escalatie.

5. **Wijs een interne eigenaar aan**
   Een security-coordinator (hoeft geen FTE te zijn) die het aanspreekpunt is voor de SOCaaS-aanbieder en escalaties opvolgt.

DIRECT AAN DE SLAG?

Word vrijblijvend gematcht met SOCaaS- en MDR-aanbieders die passen bij jouw organisatie, sector en budget.

ibgids.nl/word-gematcht

Of neem contact op via info@ibgids.nl

Bronnenlijst

[1] **Lumifi / Arctic Wolf** -- Kosten eigen SOC: EUR 1,5M--5M+/jaar. lumificyber.com/blog/what-does-it-cost-to-build-a-security-operations-center-soc/ en arcticwolf.com/resources/blog/how-much-does-it-cost-to-build-a-soc/

[2] **Vectra / vanRoey** -- SOCaaS 50--70% kostenbesparing vs intern SOC. vectra.ai/topics/soc-as-a-service en vanroey.be/managed-soc-vs-in-house-waarom-uitbesteden-loont/

[3] **Mandiant** -- Mediaan dwell time 204 dagen zonder continue monitoring.

[4] **Expel / ClearNetwork** -- Implementatie SOCaaS: 30--90 dagen tot volledig operationeel. expel.com/cyberspeak/managed-soc-implementation-timeline/ en clearnetwork.com/what-is-soc-as-a-service-complete-guide/

[5] **IBM** -- Cost of a Data Breach 2024: gemiddeld $4,88 miljoen. ibm.com/reports/data-breach

[6] **Digitale Overheid** -- Cyberbeveiligingswet (NIS2), verwacht Q2 2026. digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[7] **Expel / Blackpoint Cyber** -- Minimaal 8--14 FTE analisten voor 24/7 SOC. expel.com/blog/how-much-does-it-cost-to-build-a-24×7-soc/ en blackpointcyber.com/blog/cost-build-soc-vs-mdr/

[8] **UnderDefense / CP Cyber** -- SOCaaS pricing: $10--20/asset/maand. underdefense.com/blog/ai-soc-pricing-guide/ en cpcyber.com/soc-as-a-service-pricing/

[9] **Ponemon Institute** -- Gemiddelde organisatie besteedt $2,86M/jaar aan intern SOC.

[10] **Cyber Security District** -- Cybersecurity hiring trends Netherlands 2026, salaris SOC-analist EUR 45K--100K+. cybersecuritydistrict.com/top-cybersecurity-hiring-trends-in-the-netherlands-for-2026/

[11] **UnderDefense / KR Group** -- SOC SLA-metrics en severity-classificatie. underdefense.com/blog/sla-cybersecurity-soc-detection-response/ en underdefense.com/blog/soc-metrics/

[12] **TechMagic / CorsicaTech** -- SOCaaS prijsmodellen en verborgen kosten. techmagic.co/blog/managed-soc-pricing en corsicatech.com/blog/the-secrets-of-soc-as-a-service-pricing/

[13] **SOC-CMM** -- SOC Capability Maturity Model, 5 domeinen en 26 aspecten. soc-cmm.com/

[14] **CM-Alliance / CyberStash** -- SOC outsourcing fouten en preventie. cm-alliance.com/cybersecurity-blog/6-real-reasons-why-soc-outsourcing-fails en cyberstash.com/common-mistakes-to-avoid-when-building-or-outsourcing-a-soc/

[15] **Exeon Analytics / Serveline** -- SOC-fouten en hoe ze te vermijden. exeon.com/blog/how-to-avoid-soc-mistakes/ en serveline.co.uk/blog/soc-as-a-service

[16] **Ondernemersplein** -- NIS2-richtlijn: wie valt eronder. ondernemersplein.overheid.nl/wetswijzigingen/nis2-richtlijn-beschermt-netwerk-en-informatiesystemen-tegen-cyberbeveiligingsrisicos/

[17] **NCSC** -- NIS2 zorgplicht, meldplicht en boetestructuur. ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor/zorgplicht

[18] **CertificeringsAdvies Nederland** -- SOC 2 Type II als compliance-bewijs. certificeringsadvies.nl/informatiebeveiliging/soc-2/

[19] **Orange Cyberdefense / N-able** -- SOC vs MDR vs SIEM vs MSSP verschillen. orangecyberdefense.com/nl/blog/managed-detection-response/soc-siem-mdr-edr-wat-zijn-de-verschillen en n-able.com/blog/mdr-vs-soc-as-a-service

[20] **Palo Alto Networks / Exaforce** -- Autonomous SOC en AI-agents, 84% streeft naar unified platforms. paloaltonetworks.com/blog/2025/11/2026-predictions-for-autonomous-ai/ en exaforce.com/learning-center/top-ai-soc-platforms-2025

[21] **Precedence Research / Fortune BI / MarketsandMarkets** -- SOCaaS marktgrootte en CAGR. precedenceresearch.com/soc-as-a-service-market en fortunebusinessinsights.com/soc-as-a-service-market-108879