GIDS

De complete gids voor SOAR

Security Orchestration, Automation & Response. Automatisering, kosten, ROI, implementatie en NIS2-compliance voor het MKB.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

SOAR transformeert security operations door automatisering en orchestratie. De cijfers spreken voor zich.

80%
Reductie in Mean Time to Respond (MTTR) met SOAR-automatisering
Expert Insights [1]

4.484
Gemiddeld aantal security alerts per dag dat een SOC-team verwerkt
Grand View Research [2]

70%
Van security alerts wordt genegeerd door sheer volume (alert fatigue)
CyberSecFeed [3]

USD 1,87 mrd
Wereldwijde SOAR-markt in 2025, groeiend met 18,5% per jaar
ResearchAndMarkets [4]

241 dagen
Gemiddelde doorlooptijd om een breach te detecteren en beheersen (laagste in 9 jaar)
IBM Cost of Data Breach 2025 [5]

200–300%
ROI binnen 18 maanden na SOAR-implementatie
Phoenix Cyber [6]

EUR 10 mln
Maximale NIS2-boete voor essentiële entiteiten bij nalatigheid
Kynexis [7]

24 uur
Maximale meldtermijn bij significante incidenten onder de Cyberbeveiligingswet
Digitale Overheid [8]

1. Wat is SOAR?

SOAR staat voor Security Orchestration, Automation and Response. Het is een categorie security-tooling die drie kernfuncties combineert om security operations efficienter en sneller te maken.

Een SOAR-platform verbindt je bestaande security-tools -- zoals SIEM, EDR, firewalls en threat intelligence feeds -- en automatiseert de opvolging van alerts via zogenaamde playbooks. Waar een SOC-analist normaal handmatig elke alert moet beoordelen, verrijken en opvolgen, neemt SOAR dit grotendeels over [1].

DRIE KERNFUNCTIES

Orchestratie: Het koppelen en coordineren van verschillende security-tools zodat ze samenwerken als een geheel. Als je SIEM een verdachte login detecteert, kan SOAR automatisch de bijbehorende EDR-data opvragen, de reputatie van het IP-adres checken en de firewall-logs raadplegen.

Automatisering: Repetitieve taken worden uitgevoerd via playbooks -- geautomatiseerde workflows. Denk aan het verrijken van alerts met threat intelligence, het blokkeren van kwaadaardige IP-adressen of het isoleren van een geinfecteerd endpoint.

Response: Gestructureerd incident management met case management, escalatie, rapportage en samenwerking. Elk incident krijgt een volledig audit trail.

> **Voor wie is SOAR?** SOAR is relevant voor organisaties met een SOC (intern of extern) die dagelijks tientallen tot duizenden security alerts verwerken. Voor MKB is managed SOAR via een MSSP vaak de meest praktische optie.

2. Waarom is SOAR belangrijk?

De druk op security teams groeit. Meer alerts, complexere aanvallen en strengere regelgeving maken handmatige afhandeling onhoudbaar.

SOC-teams verwerken gemiddeld 4.484 security alerts per dag [2]. Van die alerts wordt 62% handmatig beoordeeld, waarbij analisten dagelijks bijna 3 uur besteden aan handmatige review. Het gevolg: 70% van alle alerts wordt genegeerd [3]. Dit is alert fatigue, en het is een van de grootste risico's in cybersecurity.

DE BUSINESS CASE

Een datalek kost gemiddeld USD 4,44 miljoen [5]. Organisaties die AI en automatisering inzetten, verkorten hun breach lifecycle met 80 dagen en besparen gemiddeld USD 2,2 miljoen per incident [5]. SOAR levert een ROI van 200-300% binnen 18 maanden [6].

Concreet: een phishing-incident dat voorheen 2-3 uur kostte om te onderzoeken en beheersen, wordt met SOAR-playbooks in 15 minuten afgehandeld [9]. Over een jaar bespaar je hiermee honderden analysturen.

MKB-TIP

Je hoeft geen eigen SOC te hebben om van SOAR te profiteren. Managed SOAR via een MSSP biedt dezelfde automatisering tegen voorspelbare maandelijkse kosten, zonder de complexiteit van een eigen platform.

3. Hoe werkt SOAR? Het proces

Van alert tot oplossing in vijf stappen -- grotendeels geautomatiseerd.

1 Alert intake en classificatie

SECONDEN (GEAUTOMATISEERD)

SOAR ontvangt alerts van je SIEM, EDR of andere bronnen. Het platform classificeert de alert automatisch op basis van type, ernst en context.

2 Verrijking en contextualisering

SECONDEN (GEAUTOMATISEERD)

Het platform haalt automatisch aanvullende informatie op: IP-reputatie, threat intelligence, gebruikershistorie, gerelateerde alerts. Dit bespaart analisten gemiddeld 30-45 minuten per alert.

3 Playbook-uitvoering

SECONDEN TOT MINUTEN

Op basis van het alerttype wordt het juiste playbook geactiveerd. Dit voert geautomatiseerde stappen uit: blokkeren, isoleren, melden, escaleren. SOAR reduceert de remediation-tijd met 90% [1].

4 Analist review (indien nodig)

MINUTEN TOT UREN

Complexe of onbekende situaties worden geescaleerd naar een analist. SOAR biedt alle context en aanbevelingen, zodat de analist snel kan beslissen.

5 Case management en rapportage

DOORLOPEND

Elk incident wordt vastgelegd met een volledig audit trail. Rapportages worden automatisch gegenereerd voor compliance en management review.

4. Wat kost SOAR?

SOAR-kosten varieren sterk afhankelijk van het model: zelf beheren of uitbesteden.

MODEL	PRIJSINDICATIE	GESCHIKT VOOR
Managed SOAR (basis)	EUR 1.500 - 3.500/maand [10]	MKB, geen eigen SOC
Managed SOAR (standaard)	EUR 3.500 - 7.500/maand	MKB met SIEM, 24×7 nodig
Managed SOAR (premium)	EUR 7.500 - 15.000/maand	Groot MKB, complex IT-landschap
Enterprise licentie (zelfbeheer)	Vanaf EUR 90.000/jaar [11]	Eigen SOC, 10+ analisten
Open source (Shuffle, TheHive)	Gratis + interne uren [12]	Technisch MKB, experimenteel

VERBORGEN KOSTEN

90% van security professionals geeft aan dat SOAR aanzienlijke initiële investering vereist voor het bouwen van playbooks en workflows [10]. Daarnaast moet je rekening houden met:

- Integratiekosten met bestaande tools (SIEM, EDR, firewall)
- Training van analisten en beheerders
- Continue playbook-onderhoud en optimalisatie
- Eventuele infrastructuurkosten (on-premise)

> **LET OP**
> Vergelijk managed SOAR altijd all-in. Sommige aanbieders rekenen apart voor integraties, playbook-aanpassingen en extra alertvolume. Vraag om een vaste maandprijs inclusief alle componenten.

5. Waar moet je op letten bij de keuze?

10 vragen die je moet stellen bij het selecteren van een SOAR-oplossing.

SELECTIECRITERIA

- **Integraties:** Ondersteunt het platform je huidige SIEM, EDR en firewalls?
- **Playbook-bibliotheek:** Worden standaard playbooks meegeleverd, of moet je alles zelf bouwen?
- **Schaalbaarheid:** Kan het platform meegroeien met je alertvolume?
- **Gebruiksvriendelijkheid:** Is de interface geschikt voor je team, of heb je dedicated SOAR-engineers nodig?
- **Cloud vs. on-premise:** Past het deployment-model bij je IT-strategie?

10 VRAGEN VOOR JE AANBIEDER

1. Welke integraties zijn beschikbaar met onze bestaande security-stack?
2. Hoeveel standaard playbooks worden meegeleverd?
3. Wat is de implementatiedoorlooptijd voor een MKB-omgeving?
4. Hoe wordt het alertvolume geprijsd -- per alert, per bron of vast?
5. Wie onderhoudt de playbooks na implementatie?
6. Wat is jullie ervaring met organisaties van onze omvang?
7. Hoe wordt gerapporteerd over MTTR en andere KPI's?
8. Ondersteunen jullie NIS2-rapportage en incidentmelding?
9. Wat gebeurt er als we van SIEM-leverancier wisselen?
10. Kunnen jullie referenties geven van vergelijkbare MKB-klanten?

6. Veelgemaakte fouten

Deze valkuilen zien we regelmatig bij SOAR-implementaties.

1. SOAR implementeren zonder SIEM

SOAR automatiseert de opvolging van alerts, maar die alerts moeten ergens vandaan komen. Zonder een goede SIEM (of vergelijkbaar) als bron van alerts heeft SOAR weinig om mee te werken.

2. Te veel automatiseren in het begin

Begin met 3-5 playbooks voor de meest voorkomende alerttypen (phishing, malware, brute force). Bouw van daaruit op. Organisaties die direct 50 playbooks willen, raken verstrikt in complexiteit.

3. Playbooks niet onderhouden

Dreigingen veranderen, tools worden geupgraded, processen verschuiven. Playbooks die niet regelmatig worden getest en bijgewerkt, worden een risico in plaats van een oplossing.

4. Geen metrics bijhouden

Als je niet meet, weet je niet of SOAR waarde levert. Monitor minimaal: MTTR, percentage geautomatiseerd afgehandelde alerts, false positive rate en analysturen per incident.

5. Het team niet meenemen

SOAR verandert de werkwijze van analisten fundamenteel. Zonder training en change management ontstaat weerstand. Betrek het team vroeg bij het ontwerpen van playbooks.

6. Vendor lock-in onderschatten

Als je SOAR diep geintegreerd is met een specifiek SIEM of EDR-platform, wordt het wisselen kostbaar. Kies voor een platform met brede integratiemogelijkheden.

7. Compliance: NIS2 en regelgeving

De Cyberbeveiligingswet maakt geautomatiseerde incident response steeds relevanter.

NIS2 / CYBERBEVEILIGINGSWET

De Cyberbeveiligingswet, de Nederlandse implementatie van de NIS2-richtlijn, treedt naar verwachting in Q2 2026 in werking [8]. Circa 10.000 Nederlandse organisaties vallen onder deze wet.

De wet stelt drie kernverplichtingen:

1. **Zorgplicht:** Passende technische en organisatorische maatregelen treffen
2. **Meldplicht:** Significante incidenten melden binnen 24 uur [8]
3. **Registratieplicht:** Registreren via het NCSC-portaal

Boetes kunnen oplopen tot EUR 10 miljoen of 2% van de wereldwijde jaaromzet voor essentiële entiteiten, en EUR 7 miljoen of 1,4% voor belangrijke entiteiten [7]. Bestuurders zijn persoonlijk aansprakelijk.

> **SOAR en NIS2:** SOAR helpt direct bij de meldplicht door automatische detectie, classificatie en escalatie van incidenten. Waar handmatige processen uren kosten, kan SOAR binnen minuten een melding voorbereiden.

AVG / GDPR

De AVG vereist melding van datalekken bij de Autoriteit Persoonsgegevens binnen 72 uur. SOAR-playbooks automatiseren de datalekcaclassificatie en kunnen automatisch een conceptmelding genereren.

8. Verschil SOAR, SIEM en XDR

SOAR wordt vaak verward met SIEM en XDR. Hier is het verschil.

ASPECT	SIEM	SOAR	XDR
Hoofdfunctie	Logverzameling en detectie	Automatisering en response	Geintegreerde detectie en response
Input	Logs van alle bronnen	Alerts van SIEM, EDR, etc.	Telemetrie van endpoints, netwerk, cloud
Output	Alerts en dashboards	Geautomatiseerde acties	Gecorreleerde alerts en response
Automatisering	Beperkt	Kern van het platform	Ingebouwd
MKB-geschiktheid	Managed SIEM	Managed SOAR	Vaak all-in SaaS

In de praktijk convergeren deze drie categorieen. Veel leveranciers bieden inmiddels gecombineerde platforms die SIEM, SOAR en XDR-functionaliteit in een oplossing bundelen.

9. Trends 2025--2026

De SOAR-markt ontwikkelt zich snel. Deze trends bepalen de richting.

AI-gestuurde SOAR

AI en machine learning verbeteren automatische triage, suggereren response-acties en identificeren patronen die menselijke analisten missen. Organisaties die AI inzetten, verkorten hun breach lifecycle met 80 dagen [5].

Convergentie SIEM + SOAR + XDR

De grenzen tussen SIEM, SOAR en XDR vervagen. Leveranciers bieden steeds vaker unified security operations platforms die alle drie de functies combineren.

MKB-adoptie versnelt

Het MKB is de snelst groeiende gebruikersgroep met 51,6% marktaandeel in 2025 [13]. Cloud-native SOAR en managed services maken de technologie bereikbaar voor kleinere organisaties.

NIS2 als katalysator

De meldplicht van 24 uur onder de Cyberbeveiligingswet maakt geautomatiseerde incident response geen luxe meer, maar een noodzaak. SOAR-adoptie zal hierdoor versnellen in Nederland.

10. Aan de slag

Klaar om je incident response te automatiseren? Zo begin je.

EERSTE STAPPEN

1. **Inventariseer je security-stack:** Welke tools gebruik je nu? SIEM, EDR, firewall, threat intelligence?
2. **Bepaal je top-3 use cases:** Welke alerttypen kosten de meeste tijd? Phishing, malware, brute force?
3. **Kies je model:** Zelf beheren, managed service of hybride?
4. **Start klein:** Begin met 3-5 playbooks en bouw van daaruit op.
5. **Meet en optimaliseer:** Monitor MTTR, automatiseringsgraad en analysturen.

Bronnenlijst

[1] **Expert Insights** -- SOAR Statistics 2025 -- expertinsights.com/network-security/soar-statistics-2025

[2] **Grand View Research** -- SOAR Market Report 2030 -- grandviewresearch.com/industry-analysis/security-orchestration-automation-response-market-report

[3] **CyberSecFeed** -- Security Automation SOAR Guide 2025 -- docs.cybersecfeed.com/blog/security-automation-soar-guide-2025

[4] **ResearchAndMarkets** -- SOAR Market Report 2026 -- researchandmarkets.com/reports/6226435/security-orchestration-automation-response

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

[6] **Phoenix Cyber** -- ROI Security Automation -- phoenixcyber.com/blog/roi-security-automation-orchestration/

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

[8] **Digitale Overheid** -- Cyberbeveiligingswet -- digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[9] **Swimlane** -- SOAR Playbooks Guide -- swimlane.com/blog/soar-playbooks/

[10] **Torq** -- Hidden Costs of SOAR -- torq.io/blog/hidden-costs-soar/

[11] **CSO Online** -- SOAR Buyer's Guide -- csoonline.com/article/3622920/soar-buyers-guide-11-security-orchestration-automation-and-response-products-and-how-to-choose.html

[12] **AiMultiple** -- Open Source SOAR Tools -- aimultiple.com/open-source-soar

[13] **Future Market Insights** -- SOAR Market 2035 -- futuremarketinsights.com/reports/security-orchestration-automation-and-response-soar-market

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

[15] **Palo Alto Networks** -- Cortex XSOAR ROI -- paloaltonetworks.com/blog/security-operations/build-your-customized-cortex-xsoar-roi-report/

[16] **ENISA** -- Threat Landscape 2025 -- enisa.europa.eu/publications/enisa-threat-landscape-2025

[17] **Verizon** -- DBIR 2025 -- verizon.com/business/resources/reports/dbir/