GIDS

De complete gids voor Extended Detection & Response (XDR)

Wat het is, hoe het werkt, wat het kost, NIS2-compliance en de juiste keuze voor jouw organisatie. Met actuele marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

XDR correleert signalen over je hele IT-omgeving en stopt aanvallen sneller dan losse tools. Dit zijn de feiten.

31,2% CAGR

Jaarlijkse groei XDR-markt -- van $7,9B (2025) naar $30,9B (2030)

MarketsandMarkets [1]

79%

Minder false positives met XDR ten opzichte van losse tools

Forrester TEI / Microsoft [2]

29 dagen

Kortere breach lifecycle (detectie + containment) met XDR

IBM Cost of a Data Breach [3]

$4,44M

Gemiddelde kosten datalek wereldwijd -- $1,9M lager met AI-security

IBM Cost of a Data Breach 2025 [3]

200--400%

ROI over 3 jaar bij XDR-implementatie volgens onafhankelijk onderzoek

Forrester TEI studies [2]

85%

Kortere onderzoekstijd bij complexe incidenten

Forrester TEI / Microsoft [2]

51%

Van alle datalekken wordt veroorzaakt door kwaadaardige cyberaanvallen

IBM Cost of a Data Breach 2025 [3]

80 dagen

Kortere breach lifecycle bij organisaties met AI-gebaseerde security

IBM Cost of a Data Breach 2025 [3]

1. Wat is XDR?

Extended Detection & Response (XDR) is een cybersecurity-platform dat detectie, analyse en geautomatiseerde respons combineert over meerdere beveiligingsdomeinen: endpoints, netwerk, cloud, e-mail en identiteit.

Waar traditionele tools elk een stukje van je IT-omgeving bewaken, correleert XDR data uit al deze bronnen in een centraal platform. Het resultaat: dreigingen worden sneller en met meer context gedetecteerd dan met losse tools [4].

HET VERSCHIL MET EDR

XDR is de architecturele evolutie van EDR. Waar EDR alleen kijkt naar wat er op een apparaat gebeurt (endpoint), ziet XDR de volledige aanvalsketen over alle lagen van je IT-omgeving [5].

HOE XDR ANDERS WERKT DAN LOSSE TOOLS

- **Zonder XDR:** Endpoint-tool meldt verdacht PowerShell-commando (alert 1). Firewall logt uitgaande connectie (alert 2). SIEM meldt beide events apart (alert 3). Resultaat: 3 losse tickets voor 1 aanval.
- **Met XDR:** Alle signalen worden automatisch gecorreleerd tot 1 incident met volledige context, tijdlijn en geautomatiseerde respons-suggestie [4].

> **In een zin**
>
> EDR is tactisch (tool op het endpoint). XDR is architectureel (platform dat alles verbindt). SIEM is analytisch (log-aggregatie). MDR is operationeel (uitbestede dienst met mensen).

2. Waarom is het belangrijk?

Moderne aanvallen raken meerdere lagen tegelijk. Losse tools zien elk een fragment -- XDR ziet het geheel.

CROSS-LAYER CORRELATIE

Een phishing-mail leidt tot een gecompromitteerd account, dat wordt gebruikt om lateraal te bewegen naar een server, waar data wordt ge-exfiltreerd via een versleutelde verbinding. Elke laag genereert een los signaal. Zonder correlatie worden deze signalen apart behandeld -- of helemaal gemist. XDR verbindt de punten automatisch [4].

ALERT REDUCTIE

SOC-teams zonder XDR besteden gemiddeld 3 uur per incident aan handmatige triage [6]. Hash-based deduplicatie in XDR elimineert direct 50%+ van dubbele alerts [7]. Organisaties rapporteren tot 79% minder false positives na XDR-implementatie [2].

UNIFIED PLATFORM

In plaats van 5--10 losse security-tools met elk een eigen dashboard, console en alertstroom, centraliseert XDR alles in een platform. Dit verlaagt de operationele overhead, vereenvoudigt training en maakt het beheerbaar voor kleinere IT-teams.

3 uur

Gemiddelde handmatige triage per incident zonder XDR

ESG Research [6]

50%+

Directe alert-reductie door deduplicatie en correlatie

Fidelis Security [7]

ZONDER CORRELATIE BEN JE BLIND

70%+ van enterprise-organisaties ontvangt meer dan 1.000 security-alerts per dag. Zonder XDR of een vergelijkbaar correlatie-platform worden de meeste van deze alerts niet onderzocht [8].

3. Hoe werkt het?

XDR verzamelt data uit alle lagen, correleert signalen en reageert automatisch. Dit is het technische proces.

DATA COLLECTIE

DATABRON	WAT HET LEVERT	PRIORITEIT
Endpoints	Procesactiviteit, bestandswijzigingen, verdacht gedrag op werkstations en servers	Must-have
Netwerk	Verkeerspatronen, DNS-queries, uitgaande connecties, laterale beweging	Must-have
Cloud	Activiteit in Azure, AWS, GCP -- configuratiewijzigingen, ongebruikelijke toegang	Must-have
Identiteit (IAM)	Inlogpogingen, rechtenwijzigingen, impossible travel, compromised accounts	Must-have
E-mail	Phishing-pogingen, verdachte bijlagen, kwaadaardige links	Belangrijk
Applicaties	Verdachte activiteit in bedrijfskritieke software	Optioneel [9]

CORRELATIE EN DETECTIE

XDR normaliseert data uit alle bronnen naar een gemeenschappelijk schema en past vervolgens detectieregels toe die meerdere bronnen combineren. Een verdachte inlogpoging (identiteit) gevolgd door een onbekend proces (endpoint) en een uitgaande verbinding naar een onbekend IP (netwerk) wordt gecorreleerd tot een incident [4].

AUTOMATED RESPONSE

Bij bevestigde dreigingen kan XDR automatisch actie ondernemen:

- **Endpoint isoleren** -- een besmet apparaat direct afsnijden van het netwerk
- **Account blokkeren** -- een gecompromitteerd account uitschakelen
- **IP blokkeren** -- kwaadaardig verkeer stoppen op firewallniveau
- **Playbook triggeren** -- voorgedefinieerde respons-acties automatisch uitvoeren

IMPLEMENTATIETRAJECT

1 Assessment en planning

1--2 WEKEN

Inventarisatie IT-omgeving, databronnen, bestaande tools, gap-analyse.

2 Pilot deployment

2--4 WEKEN

Uitrol op beperkte set kritieke assets. Validatie van detectie en integraties.

3 Uitbreiding

2--4 WEKEN

Schalen naar extra domeinen (cloud, e-mail, identiteit). Fine-tuning detectieregels.

4 Optimalisatie

2--4 WEKEN

KPI-meting, playbook-aanpassing, integratie met upstream/downstream tools [9].

Best practice

Begin altijd met endpoints (hoogste risico), voeg daarna e-mail en identiteit toe, en breid uit naar netwerk en cloud. Elke fase inclusief tuning en validatie voordat je naar de volgende gaat. Totale doorlooptijd: 6--14 weken [9].

4. Wat kost het?

XDR-kosten varieren sterk op basis van scope, leverancier en bestaande licenties. Dit zijn de indicatieve prijzen.

INDICATIEVE JAARKOSTEN PER BEDRIJFSGROOTTE

BEDRIJFSGROOTTE	ENDPOINTS	INDICATIEVE JAARKOSTEN	TOELICHTING
Klein MKB (10--25 pers.)	15--30	EUR 1.500 -- 5.000	Basisoplossing, bijv. E5 Security add-on
Middelgroot MKB (25--100 pers.)	30--120	EUR 5.000 -- 25.000	Mid-tier XDR met netwerk + endpoint
Groot MKB (100--250 pers.)	120--300	EUR 15.000 -- 60.000	Full-stack XDR met integraties
Enterprise (250+ pers.)	300+	EUR 50.000 -- 200.000+	Enterprise-grade met dedicated support [10]

PRIJSINDICATIES PER ENDPOINT

TYPE OPLOSSING	PRIJSMODEL	INDICATIE
E5 Security add-on	Per gebruiker/ maand	~EUR 11/gebruiker/maand (bij bestaande E3-licentie)
Standalone endpoint protection	Per device/maand	~EUR 4,80/device/maand
Mid-tier XDR	Per endpoint/ maand	~EUR 6--7/endpoint/maand (inclusief MDR-support)
Enterprise XDR	Per endpoint/jaar	EUR 55--184/endpoint/jaar (afhankelijk van modules)
Premium XDR	Per endpoint/jaar	EUR 74+/endpoint/jaar (custom pricing bij volume) [10]

Besparing voor bestaande Microsoft 365-gebruikers

Organisaties die al Microsoft 365 E3 gebruiken, kunnen XDR activeren via de E5 Security add-on voor ~EUR 11/gebruiker/maand. Dit is de goedkoopste instap voor XDR in Nederland vanwege de hoge M365-adoptie [10].

ROI VAN XDR

METRIC	VERBETERING	BRON
ROI over 3 jaar	200--400%	Forrester TEI studies [2]
Terugverdientijd	3--6 maanden	Forrester TEI studies [2]
False positives reductie	Tot 79%	Forrester TEI [2]
Onderzoekstijd complex incident	85% korter	Forrester TEI [2]
Breach-kosten reductie	9% lager gemiddeld	IBM Cost of a Data Breach [3]
Minder FTE nodig	Handmatige triage grotendeels geautomatiseerd	ESG Research [6]

TIP

Enterprise-klanten onderhandelen doorgaans 20--30% volumekorting. Vraag altijd naar meerjarige contractkortingen en bundel-deals als je al licenties hebt bij dezelfde leverancier.

5. Waar moet je op letten?

De keuze tussen open XDR en native XDR bepaalt je flexibiliteit, kosten en vendor lock-in. Dit zijn de selectiecriteria.

OPEN XDR VS NATIVE XDR

ASPECT	OPEN XDR	NATIVE XDR
Definitie	Vendor-agnostisch platform dat data van meerdere leveranciers integreert	Geintegreerd platform van een enkele leverancier
Vendor lock-in	Geen -- tools zijn uitwisselbaar	Sterk -- afhankelijk van 1 ecosysteem
Time-to-value	Langer (integraties moeten opgezet)	Korter (alles werkt out-of-the-box)
Flexibiliteit	Hoog -- tools vervangen zonder impact	Laag -- wisselen vereist migratie hele stack
Kosten	Potentieel lager (behoud bestaande investeringen)	Potentieel hoger (vervanging bestaande tools)
Geschikt voor	Multi-vendor omgeving	Organisaties al sterk in 1 ecosysteem [11]

INTEGRATIE MET BESTAANDE TOOLS

INTEGRATIEBRON	PRIORITEIT	TOELICHTING
Endpoint agents	Must-have	EDR/XDR agent op alle werkstations en servers
E-mail gateway	Must-have	Microsoft 365 / Google Workspace integratie
Identiteit (IAM)	Must-have	Azure AD / Entra ID voor identity-based threat detection
Firewall/netwerk	Belangrijk	Logs van next-gen firewalls
Cloud workloads	Belangrijk	AWS, Azure, GCP security telemetrie
SIEM (indien aanwezig)	Optioneel	Integratie met bestaand SIEM voor compliance [9]

10 VRAGEN AAN JE XDR-AANBIEDER

1. Is dit een open of native XDR-platform? Welke databronnen worden daadwerkelijk gecorreleerd?
2. Welke endpoints, cloud-omgevingen en identiteitsbronnen worden ondersteund?
3. Hoe werkt de integratie met onze bestaande tools -- moeten we iets vervangen?
4. Wat is de automatische respons-capaciteit -- isolatie, blokkering, account-lockout?
5. Hoeveel reductie in false positives kunnen we verwachten na tuning?
6. Wat is het prijsmodel -- per endpoint, per gebruiker, per GB log-ingestie?
7. Bieden jullie managed XDR (met analisten) of alleen het platform?
8. Hoe lang duurt de implementatie tot volledig operationeel?
9. Welke data-standaarden worden gebruikt (ECS, OCSF) voor correlatie?
10. Wat is de exit-strategie bij contractbeeindiging? [12]

ADVIES VOOR NEDERLANDS MKB

Gebruik je al Microsoft 365 E3/E5? Dan is native XDR via de E5 Security add-on de logische en goedkoopste keuze. Werk je met meerdere leveranciers? Kies open XDR om vendor lock-in te voorkomen [11].

6. Veelgemaakte fouten

Zeven valkuilen bij XDR-implementatie die je effectiviteit ondermijnen.

1. Te veel databronnen tegelijk aansluiten

Begin met endpoints, breid gefaseerd uit. Te veel bronnen tegelijk leidt tot ruis en false positives. Elke fase moet tuning en validatie bevatten voordat je de volgende bron aansluiting [12].

2. Geen tuning na deployment

XDR out-of-the-box genereert te veel alerts. Zonder tuning ontstaat alert fatigue -- precies wat je wilde voorkomen. Plan minimaal 2--4 weken tuning na elke uitbreidingsfase [12].

3. Verwachten dat XDR alles oplost

XDR is een platform, geen SOC. Zonder mensen die alerts opvolgen en playbooks onderhouden is het een duur dashboard. Je hebt minimaal 1--2 FTE security-expertise nodig, of je besteedt het uit via managed XDR/MDR [13].

4. "XDR-washing" niet herkennen

Veel leveranciers hebben bestaande EDR of SIEM hernoemd naar "XDR." Vraag altijd welke databronnen daadwerkelijk gecorreleerd worden. Als het antwoord alleen "endpoints" is, heb je EDR met een nieuw label [12].

5. Schema-mismatches negeren

Als verschillende tools data in verschillende formats leveren, kan XDR niet correleren. Controleer of je aanbieder standaarden als ECS (Elastic Common Schema) of OCSF (Open Cybersecurity Schema Framework) ondersteunt [7].

6. Geen incident response playbooks

XDR detecteert, maar zonder gedefinieerde playbooks voor containment en escalatie blijven alerts liggen. Definieer voor elke severity-classificatie een playbook met verantwoordelijkheden en tijdlijnen [12].

7. Werkende tools vervangen zonder ROI-analyse

Bij native XDR moet je soms werkende tools vervangen door het ecosysteem van de XDR-leverancier. Evalueer of die vervanging daadwerkelijk meerwaarde biedt -- behoud wat werkt, vervang wat tekortschiet [11].

HET KERNPROBLEEM: ALERT FATIGUE

Zonder XDR genereert je security-stack tientallen tot honderden losse alerts per dag. Analisten verbranden op handmatige triage. XDR lost dit op door correlatie en deduplicatie -- maar alleen als het correct is geimplementeerd en getuned.

7. Compliance: NIS2

De Cyberbeveiligingswet eist continue monitoring en snelle incidentrespons. XDR helpt op beide fronten.

STATUS NIS2 IN NEDERLAND

De Cyberbeveiligingswet (Cbw) -- de Nederlandse omzetting van NIS2 -- is op 4 juni 2025 ingediend bij de Tweede Kamer. Verwachte inwerkingtreding: Q2 2026 [14].

HOE XDR HELPT BIJ NIS2-COMPLIANCE

NIS2-EIS	HOE XDR HELPT
Continue monitoring	24/7 realtime monitoring over endpoints, netwerk, cloud en identiteit
Incidentdetectie	Geautomatiseerde detectie van aanvallen via cross-layer correlatie
Meldplicht (24 uur)	Versnelde triage waardoor de 24-uurs meldtermijn bij CSIRT haalbaar wordt
Incidentrespons	Geautomatiseerde containment: isolatie endpoints, blokkeren accounts
Supply chain security	Cross-domain correlatie detecteert laterale beweging vanuit leveranciers
Logging en audit trail	Alle detecties en acties worden gelogd voor compliance-rapportage [14]

WAT NIS2 WEL EN NIET VOORSCHRIJFT

NIS2 schrijft geen specifieke technologie voor -- het eist "passende en evenredige technische, operationele en organisatorische maatregelen." XDR is een van de meest effectieve manieren om aan de monitoring- en detectie-eisen te voldoen, maar het is niet verplicht. Alternatieven zijn EDR + SIEM + SOC, of MDR als managed service [15].

> **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. Bestuurders zijn persoonlijk aansprakelijk [14].

Praktisch

Wat NIS2 expliciet vereist: continu monitoren, realtime waarschuwingen, automatische of snelle handmatige respons, meldplicht binnen 24 uur en effectieve escalatiepaden. XDR dekt elk van deze punten [15].

8. XDR vs EDR vs MDR vs SIEM

Vier oplossingen die vaak door elkaar worden gebruikt maar fundamenteel verschillen. Dit overzicht helpt je de juiste keuze te maken.

CRITERIUM	EDR	XDR	EDR + SIEM	MDR
Scope	Alleen endpoints	Endpoints + netwerk + cloud + email + identiteit	Endpoints + logs	End-to-end (uitbesteed)
Kosten (MKB)	EUR 2--5/ endpoint/mnd	EUR 4--15/endpoint/mnd	EUR 8--20/ endpoint/mnd	EUR 10--35/ endpoint/mnd
Interne expertise	Gemiddeld	Hoog	Zeer hoog	Minimaal
Correlatie	Geen cross-domain	Automatisch cross-domain	Handmatig (SIEM-rules)	Door externe analisten
Geschikt voor	Klein MKB, eenvoudige IT	Middelgroot+ met security-team	Enterprise met SOC	MKB zonder security-team [13]

WANNEER WELKE KIEZEN?

SITUATIE	ADVIES
Klein MKB (< 50 pers.), geen security-team	MDR -- laat een specialist het doen
Klein MKB, al Microsoft 365 E3/E5	XDR via E5 Security add-on -- activeer wat je al hebt
Middelgroot MKB (50--250 pers.), beperkt team	XDR (managed of self-managed) -- balans zichtbaarheid en beheersbaarheid
Enterprise (250+ pers.), eigen SOC	XDR + SIEM -- XDR voor realtime, SIEM voor compliance en forensics
Complexe multi-cloud omgeving	Open XDR -- vendor-agnostisch voor maximale flexibiliteit
NIS2-plichtig, geen SOC	Managed XDR of MDR -- voldoet aan monitoring-eisen zonder eigen SOC [13]

XDR vs MDR: niet OF maar EN

XDR is een platform, MDR is een dienst. Ze zijn complementair. XDR is de technologie die detecteert en correleert. MDR is het team dat XDR-output interpreteert en actie onderneemt. De vraag is niet "XDR of MDR" maar "zelf beheren (XDR) of uitbesteden (MDR met XDR)?" [13]

9. Trends 2025--2026

De XDR-markt groeit met 31% per jaar en verandert snel. Vier ontwikkelingen die je moet kennen.

1. AI-native XDR

AI wordt ingebouwd in het XDR-platform zelf -- niet als add-on maar als kernfunctionaliteit. AI-agents die onderzoeken plannen, bewijs analyseren en remediatie-beslissingen nemen met minimale menselijke interventie. De transitie gaat van statische detectieregels naar adaptieve AI die leert van nieuwe dreigingen [16].

2. SOAR-convergentie

Security Orchestration, Automation & Response (SOAR) wordt onderdeel van XDR-platformen in plaats van een los product. Dit versnelt de responstijd en elimineert de noodzaak voor aparte automatiseringstools [16].

3. Identity-centric security

Identiteit wordt de nieuwe perimeter. XDR-platformen verleggen focus van netwerk- en endpoint-detectie naar identity-based threat detection: impossible travel, anomale rechtenwijzigingen, gecompromitteerde service accounts. Dit sluit aan bij de Zero Trust-beweging [4].

4. NIS2-gedreven adoptie

De Cyberbeveiligingswet drijft een golf van XDR-adoptie in Nederland. Organisaties die nu geen continue monitoring hebben, moeten dat voor Q2 2026 regelen. De MSSP-markt groeit met 16,2% CAGR tot 2027, grotendeels gedreven door managed XDR-diensten [1].

$30,9B

Verwachte XDR-markt in 2030 -- groei van 31,2% CAGR

MarketsandMarkets [1]

$2,35B

Nederlandse cybersecurity-markt in 2025 -- groeit naar $3,79B in 2031

Mordor Intelligence [17]

WAT BETEKENT DIT VOOR JOU?

AI maakt XDR slimmer en betaalbaarder. NIS2 maakt monitoring verplicht. De grenzen tussen XDR, MDR en SIEM vervagen. Als je nu kiest, kies dan een platform dat meegroeit met deze trends -- geen legacy tool met een nieuw label.

10. Aan de slag

Je weet nu wat XDR is, wat het kost en hoe je de juiste oplossing kiest. Tijd voor actie.

VIJF STAPPEN OM TE STARTEN

1. **Breng je IT-landschap in kaart**

   Hoeveel endpoints, welke cloud-omgevingen, welke identiteitsbronnen? Gebruik je al Microsoft 365? Dit bepaalt of native of open XDR de juiste keuze is.

2. **Bepaal je capaciteit**

   Heb je 1--2 FTE security-expertise intern? Dan kan je XDR zelf beheren. Zo niet: kies managed XDR of MDR.

3. **Vergelijk oplossingen**

   Gebruik de 10 vragen uit hoofdstuk 5. Let op open vs native XDR, daadwerkelijke correlatie-capaciteit en integratie met bestaande tools.

4. **Start met een pilot**

   Begin met endpoints als eerste databron, voeg na validatie e-mail en identiteit toe. Meet de impact op alert-volume en detectiekwaliteit.

5. **Definieer playbooks**

   Stel voor elke severity een playbook op: wie doet wat, binnen welke tijd, met welke escalatie. Zonder playbooks is XDR een alarmsysteem zonder brandweer.

DIRECT AAN DE SLAG?

Word vrijblijvend gematcht met XDR- 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] **MarketsandMarkets** -- XDR Market: $7,92B (2025) naar $30,86B (2030), CAGR 31,2%. marketsandmarkets.com/Market-Reports/extended-detection-response-market-52119574.html

[2] **Forrester TEI studies** -- ROI 200--400% over 3 jaar, 79% minder false positives, 85% snellere investigatie. tehtris.com/en/press-releases/tehtris-xdr-ai-platform-delivers-277-roi/ en secureworks.com/resources/wp-forrester-tei-study-managedxdr

[3] **IBM** -- Cost of a Data Breach 2025: $4,44M gemiddeld, 29 dagen snellere detectie met XDR, $1,9M lager met AI-security. ibm.com/reports/data-breach

[4] **Microsoft** -- Wat is XDR: cross-layer correlatie en detectie. microsoft.com/nl-nl/security/business/security-101/what-is-xdr

[5] **Cyberlab / ON2IT** -- MDR, EDR, XDR: Detection & Response afkortingen. cyberlab.nl/detection-response-afkortingen/ en on2it.net/blog/mdr-vs-edr-vs-xdr/

[6] **ESG Research** -- SOC-teams besteden ~3 uur per incident aan handmatige triage zonder XDR.

[7] **Fidelis Security** -- XDR alert deduplicatie elimineert 50%+ dubbele alerts. fidelissecurity.com/threatgeek/xdr-security/xdr-integration-best-practices-for-your-security-stack/

[8] **Brancheanalyse** -- 70%+ enterprise ontvangt >1.000 alerts/dag; zonder SOC/XDR worden deze niet onderzocht.

[9] **TechTarget / OpenEDR** -- XDR implementatie: assessment, pilot, uitbreiding, optimalisatie. techtarget.com/searchsecurity/tip/How-to-evaluate-and-deploy-an-XDR-platform en openedr.com/blog/how-to-deploy-xdr/

[10] **Virteva / Cynet / G2** -- XDR pricing: per endpoint, per gebruiker, per licentietier. virteva.com/microsoft-defender-xdr-guide/ en cynet.com/endpoint-security/sentinelone-pricing-packages-core-control-and-complete/

[11] **TechTarget / Cybereason / Heimdal** -- Open XDR vs native XDR: vergelijking en keuzecriteria. techtarget.com/searchsecurity/feature/The-differences-between-open-XDR-vs-native-XDR en cybereason.com/blog/evaluating-open-xdr-vs.-native-xdr

[12] **Check Point / Venn** -- 7 XDR best practices en veelgemaakte fouten. checkpoint.com/cyber-hub/threat-prevention/what-is-xdr-extended-detection-and-response/7-xdr-best-practices/ en venn.com/learn/endpoint-security/xdr/

[13] **SentinelOne / Palo Alto / Sysdig** -- XDR vs EDR vs MDR vs SIEM: wanneer welke kiezen. sentinelone.com/cybersecurity-101/xdr/understanding-the-difference-between-edr-siem-soar-and-xdr/ en sysdig.com/learn-cloud-native/edr-vs-xdr-siem-vs-mdr-vs-soar

[14] **Digitale Overheid / NCSC** -- Cyberbeveiligingswet (NIS2), verwacht Q2 2026, boetestructuur. digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/ en ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor

[15] **eSentire / Kynexis** -- NIS2 compliance checklist en XDR-relevantie. esentire.com/resources/library/nis2-directive-compliance-checklist en kynexis.nl/nis2-checklist-cyberbeveiligingswet/

[16] **CrowdStrike / Seqrite** -- AI-native XDR en SOAR-convergentie trends. crowdstrike.com/en-us/cybersecurity-101/endpoint-security/extended-detection-and-response-xdr/ en seqrite.com/blog/xdr-transforming-soc-operations/

[17] **Mordor Intelligence** -- Nederlandse cybersecurity-markt: $2,35B (2025) naar $3,79B (2031). mordorintelligence.com/industry-reports/europe-soc-as-a-service-market