Kaspersky Next XDR Expert

Groter beter sneller meer

kaspersky

Een doorbraak, of onnodig?

XDR: Extended Detection and Response

Dit acroniem komt vaak ter sprake, maar zoals bij alle relatief jonge technologieën weet niet iedereen precies wat het is of wat het voor hun bedrijf kan betekenen. Eén ding is zeker: XDR betekent een strategische verschuiving van reactief naar proactief, want 'alleen maar afwachten' is niet voldoende in cyberbeveiliging. Slimmeriken zien XDR als een strategie in plaats van alleen een product.

Dus is XDR gewoon de nieuwste overbodige technologie om in een behoefte te voorzien, of is het echt een potentiële doorbraak?
De behoefte is er zeker, of het nu gaat om het wereldwijde tekort aan vaardigheden, overwerkt IT-beveiligingspersoneel, een dreigingslandschap dat altijd in beweging is, een overvloed aan waarschuwingen, uiteenlopende tools, gebrekkige informatie over bedreigingen of het steeds groter wordende aanvalsoppervlak.
IDC zegt dat XDR "een ontwrichtende kracht zal zijn, die invloed zal hebben op de verkoop van SIEM, EDR, SOAR, netwerkintelligentie en bedreigingsanalyseplatforms, en ook op leveranciers van informatie over externe bedreigingen"[1]. Forrester gelooft dat gedifferentieerde XDR-technologie "op korte termijn Endpoint Detection and Response (EDR) en op lange termijn SIEM zal verdringen"[2].

Voor wie is XDR bedoeld?

XDR is bedoeld voor organisaties met een volwassen beveiligingsbeleid, die één platform nodig hebben om een compleet en samenhangend beeld te krijgen van wat er in hun infrastructuur gebeurt.

XDR wordt een ontwrichtende kracht - IDC

Meer apparaten, meer applicaties, meer netwerkverkeer, meer gegevens, meer bedreigingen...

Voor wie is XDR bedoeld, en welke uitdagingen kan het oplossen?

XDR is bedoeld voor organisaties met een volwassen beveiligingsbeleid, die één platform nodig hebben om een compleet en samenhangend beeld te krijgen van wat er in hun infrastructuur gebeurt.

De uitdagingen op het gebied van cyberbeveiliging waarmee deze organisaties worden geconfronteerd, komen veelvuldig voor. ESG Research ondervroeg IT- en cyberbeveiligingsprofessionals[3] bij organisaties met 100 of meer werknemers, waarvan meer dan 80% in ondernemingen in verschillende branches werkt. Dit zijn enkele van de belangrijkste bevindingen:

Moeilijkheden om de operationele vereisten van SOC-technologieën bij te houden

Het beheren van beveiligingsactiviteiten is de laatste twee jaar moeilijker dan ooit, omdat het moeilijk is om de operationele behoeften van SOC-technologieën bij te houden, namelijk de schaalbaarheid van de gegevenspijplijn, het verdelen van de verwerkingsengines, het toevoegen van opslagcapaciteit enzovoort.

[1] Bron: IDC Wereldwijde analyse van beveiligingsproducten: From Power Point to Power Product, Where Is XDR Right Now? 2022

[2] Bron: Forrester, Extended Detection and Response (XDR) - A Battle Between Precedent and Innovation, Allie Mellen, Senior Analyst, 2021

[3] Bron: ESG Research Report, SOC Modernization and the Role of XDR, 2022

Het groeiende en voortdurend veranderende aanvalsoppervlak en het algemene dreigingslandschap

Meer apparaten, meer applicaties, meer netwerkverkeer, meer gegevens, meer bedreigingen. Het dreigingslandschap is voortdurend in beweging en cyberbedreigingen worden steeds omvangrijker en complexer naarmate er meer nieuwe tools bijkomen. Tegelijkertijd is de drempel voor hackers lager dan ooit, met aan de ene kant van het spectrum laaggekwalificeerde kopers van goedkope verpakte bedreigingen op het dark web en aan de andere kant hoogopgeleide, geduldige hackers die complexe aanvallen opzetten. En denk ook aan bedreigingen van binnenuit en kwetsbaarheden in de toeleveringsketen.

Het grote aantal handmatige processen dat nodig is om de beveiliging te beheren

Er moeten meer beveiligingsgegevens worden verzameld en verwerkt waarvan de handmatige verwerking inefficiënt en ineffectief is. Dit veroorzaakt dat de schaalbaarheid wordt beïnvloed, dat er te veel wordt vertrouwd op directe menselijke betrokkenheid en dat de effectiviteit van het omgaan met bedreigingen in het algemeen afneemt.

Een onvermogen om detectieregels te ontwikkelen

Door een gebrek aan tijd, middelen en vaardigheden is het niet mogelijk om detectieregels te ontwikkelen, beveiligingscontroles te verfijnen en bedreigingen snel en efficiënt te identificeren en aan te pakken. Organisaties hebben niet altijd de juiste vaardigheden of het juiste personeel om beveiligingsanalyses en -activiteiten bij te houden. Dat brengt ons meteen bij het volgende probleem...

Het wereldwijde tekort aan vaardigheden

Ondanks het feit dat er wereldwijd 4,7 miljoen professionals in cyberbeveiliging werkzaam zijn, is er nog steeds een gat van 3,4 miljoen dat moet worden opgevuld. Maar dit lukt niet. Dit gat groeit twee keer zo snel als de beroepsbevolking, met een stijging van 26,2% op jaarbasis.[4]

[4] Bron: (ISC)², Cybersecurity Workforce Study, 2022

Bestaande tools kunnen

geavanceerde bedreigingen vaak moeilijk detecteren en onderzoeken, terwijl er gespecialiseerde vaardigheden nodig zijn om ze te gebruiken en te beheren.

Tools niet geschikt voor doel

Als de tools zelf een deel van het probleem worden, dan zal er iets moeten veranderen. Bestaande tools kunnen geavanceerde bedreigingen vaak moeilijk detecteren en onderzoeken, terwijl er nog steeds gespecialiseerde vaardigheden nodig zijn om ze te gebruiken en te beheren. Uit onderzoek[5] blijkt dat de huidige tools vaak niet effectief zijn in het in kaart brengen van waarschuwingen terwijl IT-beveiligingsmedewerkers worstelen met meerdere losse, ongelijksoortige tools die uiteenlopende gegevens verwerken. Dit is inefficiënt, lastig, rommelig en duur. Een andere uitdaging is dat de huidige tools niet berekend zijn op het groeiende aanvalsoppervlak en dat er grote gaten zitten in de detectie- en reactiemogelijkheden in de cloud.[6]

Geen wonder dat de CISO er gestrest uitziet.

Het goede nieuws is dat SecOps verbeteren een prioriteit is en wordt gefinancierd: 88% van de organisaties gaat dit jaar meer uitgeven en 66% zegt dat het consolideren van tools voorrang heeft. De ontwikkeling en implementatie van moderne applicaties is sneller geworden, waardoor nieuwe vaardigheden nodig zijn.[7]

88%

van de organisaties geeft dit jaar meer uit aan het verbeteren van SecOps

66%

zegt dat het consolideren van hulpmiddelen voorrang heeft

Wat doet XDR

Dit is hoe XDR deze uitdagingen het hoofd kan bieden.

XDR detecteert geavanceerde dreigingen beter

De capaciteiten van XDR om bedreigingen op te sporen strekken zich uit over endpoints, netwerken en cloudomgevingen. Het systeem maakt gebruik van machine learning-algoritmen en gedragsanalyses om geavanceerde bedreigingen zoals malware, ransomware en APT's (geavanceerde, hardnekkige bedreigingen) te identificeren.

Geautomatiseerde respons- en herstelacties

XDR automatiseert respons- en herstelacties, zodat organisaties bedreigingen snel kunnen indammen en potentiële schade kunnen minimaliseren. Het kan aangetaste endpoints automatisch afzonderen of isoleren, kwaadaardige activiteiten blokkeren en kwetsbaarheden herstellen, waardoor handmatige inspanningen en responstijd worden verminderd.

Integreert met endpoint beveiligingstools

Integratie met EPP is van groot belang. XDR maakt gebruik van rijke endpoint telemetrie en gedragsanalyses om gedetailleerde inzichten te verschaffen in endpoint activiteiten. Het maakt gebruik van geavanceerde machine learning-algoritmen om verdacht gedrag en aanvalsindicatoren (IOA's) te identificeren, waarmee geavanceerde bedreigingen vroegtijdig kunnen worden opgespoord.

[5] Bron: ESG Research Report, SOC Modernization and the Role of XDR, mei 2022

[6] Bron: ESG Research Report, SOC Modernization and the Role of XDR, 2022

[7] Bron: ESG Research Report, SOC Modernization and the Role of XDR, mei 2022

Waar past XDR in het ecosysteem van EDR, MDR, SOAR en SIEM

De hint zit in de X, die voor 'uitgebreid' staat. XDR breidt de mogelijkheden van EDR uit om complexe bedreigingen op meerdere infrastructuurniveaus proactief te detecteren en hier automatisch op te reageren om ze tegen te gaan.

Een geïntegreerde aanpak is essentieel

Door verschillende tools en beveiligingstoepassingen te integreren en gegevens op o.a. endpoints, netwerken, clouds, web- en mailservers enzovoort te monitoren, kan XDR meer bedreigingen detecteren en elimineren en tegelijkertijd het beheer van informatiebeveiliging vereenvoudigen door productoverschrijdende interactie te automatiseren.

Forrester verwacht dat XDR in de meeste gevallen de platformen voor beveiligingsanalyse niet volledig zal vervangen, en merkt op dat "XDR momenteel in ontwikkeling is, en [we] verwachten dat de platformen voor beveiligingsanalyse en XDR binnen vijf jaar met elkaar in botsing zullen komen".

SIEM heeft toepassingsmogelijkheden die verder gaan dan het opsporen van bedreigingen. Het aanpassingsvermogen van SOAR is nuttig, maar als het aankomt op het detecteren van en reageren op bedreigingen, zijn de geavanceerde analyses van de uitgebreide bescherming van XDR ongeëvenaard.

Levert realtime zichtbaarheid

XDR biedt realtime inzicht in hoe je organisatie is beveiligd. Het verzamelt en analyseert gegevens van verschillende bronnen, zoals endpoints, servers, firewalls en cloudplatforms, om zo uitgebreide inzichten in actuele bedreigingen en verdachte activiteiten te verkrijgen in één console. Dit maakt het programma pas echt proactief. Het jaagt proactief op bedreigingen en reageert sneller op incidenten. Een holistische kijk helpt beveiligingsteams om verdachte activiteiten en potentiële beveiligingsincidenten efficiënter te identificeren.

Contextualiseert gegevens en informatie over bedreigingen

Door optimaal gebruik te maken van hoogwaardige informatie over bedreigingen en een uitgebreide database met gegevens over bedreigingen, biedt XDR nuttige contextuele aanvullende informatie over bedreigingen en aanvallers. Deze uitgebreide informatie over bedreigingen vereenvoudigt onderzoekswaarschuwingen en de afhandeling van incidenten, technieken en beweegredenen van de personen die bedreigingen uitvoeren. Zo kunnen ze effectiever reageren op bedreigingen en proactieve verdedigingsmaatregelen nemen.

Maakt gestroomlijnde beveiligingsoperaties mogelijk

Als ze goed geïntegreerd zijn, passen de beste oplossingen moeiteloos in je huidige infrastructuur om het beste resultaat uit je automatisering te halen. Ook zorgen ze voor volledige zichtbaarheid en bewustzijn zonder dat je externe beveiligingsoplossingen die al in gebruik zijn, hoeft te vervangen. En vergeet niet dat integratie in combinatie met een uitgebreid overzicht van beveiligingsincidenten en gebruikersgedrag, de naleving ondersteunt.

XDR levert duidelijk waarvoor het bedoeld is: beheersbaarheid, stabiliteit en die o zo belangrijke voorsprong. Maar niet alle XDR-oplossingen zijn gelijk. Hoe kies je de oplossing die bij je past?

5 belangrijke punten bij het vergelijken van XDR-leveranciers en -oplossingen

Dit is hoe XDR deze uitdagingen het hoofd kan bieden.

1

Er is een direct verband tussen de kwaliteit van een XDR-oplossing en de synergie tussen het EPP en het EDR van de leverancier

Een EDR-oplossing voor geavanceerde opsporing van en reactie op geavanceerde cyberbedreigingen op endpoint niveau is een belangrijk onderdeel van XDR. Tegelijkertijd heeft EDR een robuust Endpoint Protection Platform (EPP) nodig om enorme aantallen massabedreigingen automatisch uit te filteren. Kijk daarom goed naar de functies voor endpoint beveiliging en controleer of alle soorten endpoints worden ondersteund: pc's, laptops, virtuele machines, mobiele apparaten en verschillende besturingssystemen.

2

Bijgewerkte informatie over bedreigingen en een volledig beeld van de tactieken en technieken van cybercriminelen zijn cruciaal om cyberbedreigingen tegen te gaan

Het is geen hogere wiskunde. Elke XDR-oplossing biedt beide mogelijkheden, plus extra context om het onderzoek naar en de reactie op incidenten te verbeteren en te versnellen.

3

Integratie met externe oplossingen is duurzamer en kosteneffectiever

De integratie van een XDR-oplossing met oplossingen van derden is een ander belangrijk punt, omdat interoperabiliteit de aanschaf vanaf het begin tot een duurzamere investering maakt. Een XDR-oplossing die vele en betrouwbare integratiemogelijkheden biedt, verzamelt meer gegevensbronnen en levert een completer beeld van wat er in je infrastructuur gebeurt.

4

Onafhankelijke beoordelingen, wereldwijde erkenning en onafhankelijke testresultaten zijn belangrijk

Wanneer je investeert in iets dat zo belangrijk is voor je bedrijf als cyberbeveiliging, mag je onafhankelijke beoordelingen niet negeren. Vraag naar de resultaten van onafhankelijke onderzoeken. Kijk naar de internationale erkenning van Forrester, IDC en anderen. Worden de oplossingen wereldwijd toegepast? Vraag naar casestudy's.

5

Is je investering klaar voor de toekomst?

Technologie staat niet stil. Vooral voor zoiets als XDR, wat nog een relatief jonge technologie is, moet je uitzoeken hoe de routekaart van een leverancier eruit ziet voor verdere ontwikkeling.

Waarom Kaspersky?

Het meest getest. Het meest bekroond. Beveiliging door Kaspersky.

Kaspersky is een gevestigd, wereldwijd cyberbeveiligingsbedrijf met een sterke staat van dienst betreft beveiligingsexpertise. We beschermen al meer dan 25 jaar organisaties over de hele wereld en we hebben vele prijzen en lofbetuigingen ontvangen voor onze producten en services. Tussen 2013 en 2022 hebben Kaspersky-producten:

587

587 eerste plaatsen behaald

685

de top drie behaald

827

deelgenomen aan 827 onafhankelijke tests en beoordelingen

In 2023 werd Kaspersky door het toonaangevende wereldwijde technologieonderzoeks- en adviesbureau ISG uitgeroepen tot Leider in de markt voor XDR-oplossingen. ISG definieert 'leiders' als bedrijven die een uitgebreid product- en service-aanbod hebben en innovatieve kracht en concurrentiestabiliteit vertegenwoordigen.

Meer informatie

Kaspersky Extended Detection and Response

Meer informatie

www.kaspersky.nl

#kaspersky
#bringonthefuture