kaspersky BRING ON THE FUTURE

XDR vs. SIEM vs. SOAR

Krijg je hoofdpijn van al die acroniemen? Laten we eens kijken wat er achter deze kleine letters schuilgaat...

Inleiding

SIEM, SOAR, MDR, EDR, EPP, XDR... voel je je verloren, verdwaald in een jungle vol cyberbeveiligingsacroniemen? Dat is begrijpelijk — daarom hebben we deze handige gids samengesteld om de verschillen tussen drie van de grootste uit te leggen: SIEM, SOAR en XDR. Wat is het verhaal achter deze acroniemen? Hoe komt het dat de industrie deze verwarrende, overlappende termen heeft ontwikkeld? Betekenen ze wel iets anders, of zijn het gewoon marketingtrucs? Wat zijn de gelijkenissen en verschillen? Vullen ze elkaar aan of zijn het elkaar tegenpolen?

Kom, ga met ons mee op deze zoektocht! Laten we onze hakmessen van kennis oppakken, door het woud van acroniemen en jargon hakken en uitkomen op een open plek van helder begrip!

SIEM

Security information and event management (SIEM) is een verzameling tools en services die security events management (SEM) en security information management (SIM) combineren in één platform. SIEM verzamelt, bundelt, analyseert en bewaart logboekgegevens van de hele IT-infrastructuur voor verschillende gebruiksscenario's, waaronder governance en naleving, en op regels gebaseerde correlatie-matching voor verdachte activiteiten.

Hoe werkt SIEM?

De eerste SIEM-services werden al in 2005 ontwikkeld, met het oorspronkelijke doel om logboeken en gebeurtenissen uit de IT-infrastructuur van organisaties — inclusief endpoints, applicaties en netwerkapparaten — te bundelen en te bewaren voor nalevingsrapporta-gedoeleinden. De SIEM voert correlaties uit op deze gegevensset, zoekt naar patronen of gebeurtenissen die kunnen wijzen op verdacht gedrag en genereert een waarschuwing voor het Security Operations Center (SOC). Beveiligingsanalisten zagen al snel de mogelijkheid om deze waarschuwingen niet alleen voor nalevings- en governance-doeleinden te gebruiken, maar ook om proactiever kwaadaardige activiteiten in het ecosysteem vast te stellen en de voortgang ervan te stoppen.

SIEM-beperkingen

Het probleem was dat SIEM-services niet waren ontworpen voor het specifieke doel om incidenten te detecteren en hierop te reageren. Dit maakte ze om een aantal redenen ietwat lastig om mee te werken:

- Te veel waarschuwingen — De enorme gegevensset die SIEM levert, moet handmatig worden gefilterd, verwerkt en geanalyseerd, wat niet handig is voor beveiligingsanalisten die aanvallen proberen te voorkomen in een snel bedreigingslandschap.

- Geen context — Om nieuwe, complexe, geraffineerde aanvallen aan te pakken, moeten beveiligingsanalisten een gecontextualiseerd beeld hebben van het bedreigingslandschap van de organisatie, in plaats van de losgekoppelde gegevensstromen die door SIEM worden geleverd.

- Te passief — Het blokkeren van verdachte processen, in quarantaine plaatsen van bestanden en andere responsmogelijkheden behoren niet tot de mogelijkheden; het is in principe een passieve, analytische tool.

Beveiligingsprofessionals hebben geprobeerd om deze problemen op te lossen door extra tools naast SIEM te gebruiken of door nieuwe generaties te ontwikkelen met plug-ins voor machine learning en gedragsanalyse. Maar de vraag naar een tool die waarschuwingen van betere kwaliteit geeft en snellere, geautomatiseerde processen mogelijk maakt, bleef bestaan.

SOAR

Beveiligingsbeheer en geautomatiseerde respons-tools (SOAR) kwamen op in 2015 om een aantal van de bovengenoemde fouten in SIEM-systemen op te lossen. SOAR-platformen nemen gegevens op uit verschillende bronnen binnen de infrastructuur, waaronder beheersystemen en platformen met informatie over bedreigingen, en maken prioriteitsanalyses. Beveiligingsteams kunnen vervolgens geautomatiseerde reacties op nieuwe bedreigingen in meerdere fases en met meerdere oplossingen configureren, met de integratie van een aan een API-gekoppeld ecosysteem van beveiligingstools op het SOAR-platform.

Hoe werkt SOAR?

Deze keer is de naam eigenlijk best nuttig! Dit is waarom:
SOAR-tools automatiseren. Hoewel deze tools vaak het meest bekend staan om hun mogelijkheid om incidentresponsprocessen te automatiseren, kunnen ze eigenlijk een breed scala aan workflows automatiseren, waaronder het scannen op kwetsbaarheden, logboekanalyse, beheer van gebruikerstoegang, triage van bedreigingen en nog veel meer.
Dit doen ze met behulp van 'draaiboeken' — sets van vooraf geconfigureerde regels die door specifieke gebeurtenissen worden geactiveerd, die het systeem vertellen welke stappen hierna moeten worden genomen in een specifieke workflow. De meeste SOAR-oplossingen komen met honderden kant-en-klare draaiboeken voor de meest voorkomende taken van SOC-teams. Teams kunnen vervolgens hun eigen draaiboek configureren om andere, specifiekere repetitieve processen te automatiseren.

Vervolgens beginnen ze. Terwijl automatisering verwijst naar de machinegestuurde uitvoering van individuele taken binnen een enkele workflow, verwijst uitvoering naar de coördinatie van meerdere aparte tools en processen in een grotere workflow, waarbij alle relevante gegevens worden gebundeld in een enkel platform voor geconsolideerde, bruikbare informatie.

De relatie tussen SIEM en SOAR

Een SIEM wordt doorgaans gebruikt in combinatie met SOAR-tools in een soort assistent-manager relatie: de SIEM verzamelt alle logboeken, correleert ze om waarschuwingen te zoeken en geeft deze informatie door aan de SOAR, die vervolgens het voortouw kan nemen bij responsacties.

SOAR-beperkingen

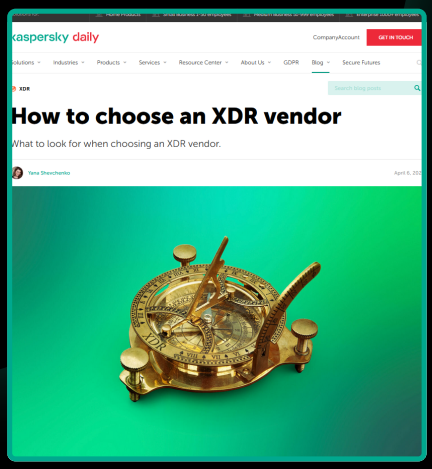
Klinkt allemaal goed, toch? Het punt is dat het onderhouden van een goed geconfigureerd SOAR-platform dat integreert met partnertools de doorlopende inspanning vereist van een hooggekwalificeerde, volwaardige SOC — een hulpbron waar veel organisaties momenteel niet over beschikken, gezien het gebrek aan vaardigheden op het gebied van de huidige cyberbeveiliging.

Zonder zulk vakkundig, zorgvuldig onderhoud kunnen SOAR-analisten eindigen met te veel waarschuwingen met lage prioriteit, false positives en een algemene onsamenhangende gegevensset als gevolg van alle verschillende verzuilde tools die in het platform zijn opgenomen — precies wat ze probeerden te vermijden.

Hoe kies je een XDR-leverancier?

Veel cyberbeveiligingsleveranciers zijn met hun eigen oplossingen meegegaan met de XDR-trend. Hoe weet je of je een goed product krijgt? Bekijk onze handige gids:

https://www.kaspersky.nl/blog/choosing-xdr-vendor/44063/



XDR

XDR is een beveiligingsoplossing op locatie of in de cloud, die ruwweg in twee categorieën valt: native en hybride. Native XDR is een gebundeld pakket tools van één leverancier, terwijl Hybrid XDR andere oplossingen van derden in je ecosysteem integreert. De term 'XDR' werd voor het eerst gebruikt in 2018, waarbij de 'X' staat voor 'eXtended' (uitgebreid) : XDR gaat verder dan traditionele endpointdetectie-, respons- en beschermingstools (EDR en EPP) door gegevens van meerdere beveiligingslagen, waaronder e-mail, cloud en netwerk, te verzamelen en correleren, om uitgebreide bescherming te bieden over de hele IT-infrastructuur.

Het is dus één platform dat een reeks tools coördineert en machine learning en automatisering gebruikt om beveiligingsteams te helpen het hele beveiligingsecosysteem te beschermen... klinkt een beetje als SOAR, of niet? Maar er zijn sommige fundamentele verschillen. Laten we eens kijken...

XDR vs. SOAR: Wat is het verschil?

1. XDR-oplossingen zijn verankerd in endpointgegevens en optimalisatie — dit betekent dat incidentdetectie en -respons een centraal ontwerpkenmerk is, waardoor ze geavanceerde analysemogelijkheden hebben die SOAR-tools meestal niet hebben. XDR-tools zijn meesters in het detecteren van onbekende en zero-day-dreigingen en maken gebruik van krachtige kunstmatige intelligentie, algoritmen op basis van machine learning en informatie over bedreigingen om een organisatie volledig te beschermen. Aan de andere kant kunnen SOAR-tools een veel breder scala aan gebruiksscenario's bieden, omdat ze alle processen binnen de infrastructuur — niet alleen incidentrespons — kunnen uitvoeren en automatiseren.

2. XDR kan worden beschouwd als iets vergelijkbaars met SOAR-lite — een gestroomlijnde interface die met één klik automatisch reageert op binnenkomende bedreigingen en waarschuwingen. Dit kan veel handiger zijn voor een organisatie die niet over de middelen beschikt om de complexiteit van een goed geconfigureerd SOAR-platform te onderhouden.

3. Met XDR is een soepele cross-productintegratie mogelijk — of het nu gaat om tools van één leverancier of producten van derden, XDR blinkt uit in naadloze interoperabiliteit. SOAR-tools hebben vaak moeite om alle aparte, verzuilde tools in hun stack te integreren; XDR breekt deze silo's af voor een efficiënte, alles-in-één respons op bedreigingen.

Gaat XDR SIEM en SOAR vervangen?

De jury is hier nog niet over uit, aangezien XDR een relatief nieuwe technologie is die continu verder wordt ontwikkeld. Op dit moment bevelen de meeste experts een geïntegreerde aanpak aan, omdat elke oplossing voordelen heeft die de andere aanvullen:

- SIEM — de SIEM heeft gebruiksscenario's buiten bedreigingsdetectie, zoals logboekbeheer, naleving en het analyseren van gegevens die niet gerelateerd zijn aan bedreigingen.
- SOAR — de SOAR-draaiboeken die je in grote mate kunt aanpassen zijn handig voor het uitvoeren en automatiseren van processen binnen de infrastructuur van de organisatie.
- XDR — als het aankomt op het detecteren van en reageren op bedreigingen, bieden de geavanceerde analyses van een XDR-oplossing een uitgebreide bescherming die ongeëvenaard is.

Op zoek naar een beproefde aanpasbare oplossing voor je experts?
Kaspersky Expert Security, XDR op basis van een cloud-native EDR-oplossing, geeft je organisatie een verbeterde zichtbaarheid en functionaliteit voor detectie en automatische responslogica op basis van AI voor alle endpoints en het netwerk, waardoor een breed scala aan geautomatiseerde incidentresponsscenario's mogelijk wordt. De ingebouwde geavanceerde technologie voor detectie en analyse van het platform wordt aangevuld met toonaangevende informatie over bedreigingen. De geïntegreerde architectuur van Kaspersky XDR biedt gecentraliseerd beheer vanaf één webconsole. Ga voor meer informatie naar go.kaspersky.com/expert.

www.kaspersky.nl