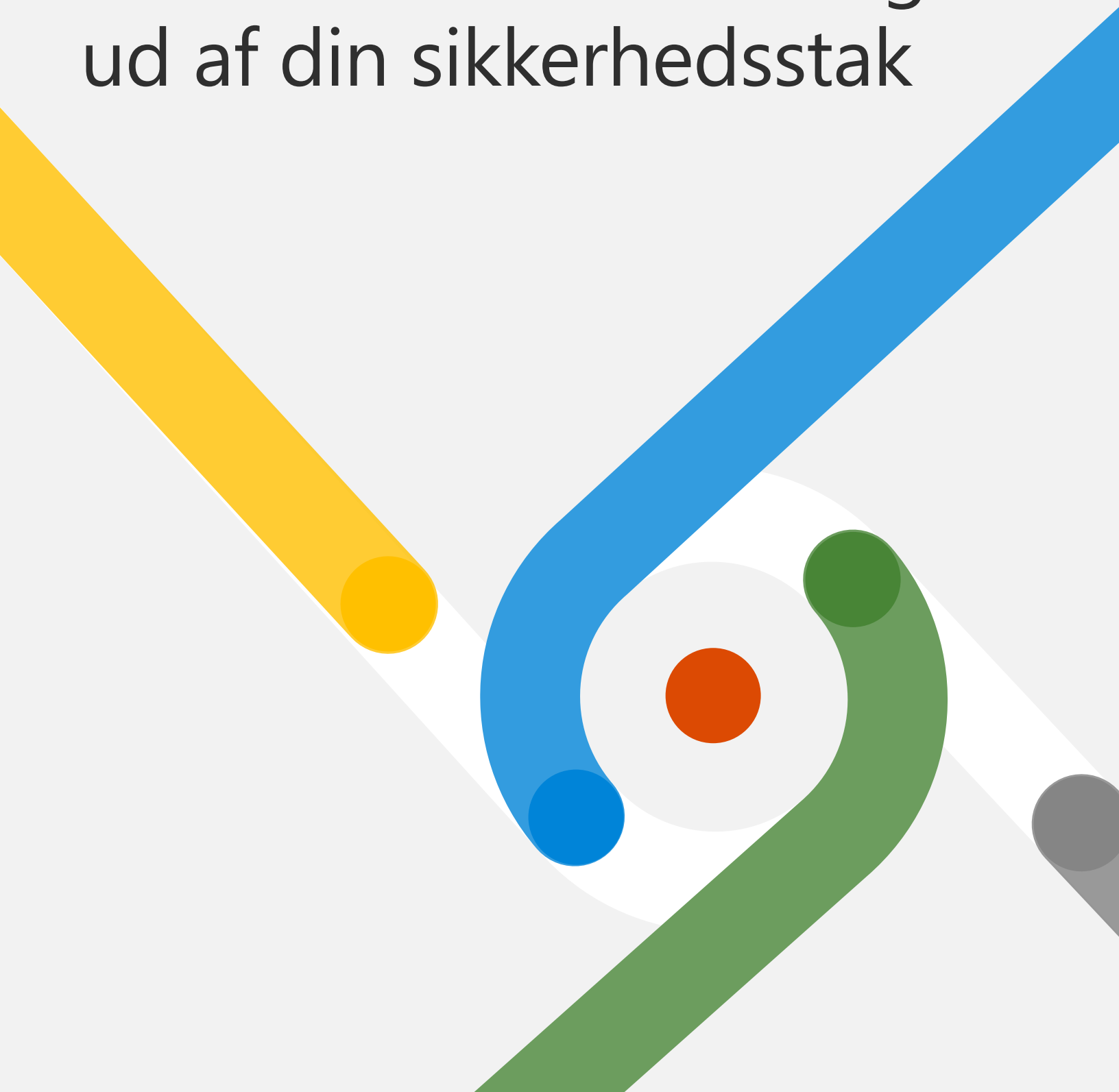
Microsoft Security

Optimering af SIEM

Sådan får du mest muligt ud af din sikkerhedsstak



Indhold

Introduktion

I mere end ti år har SecOps-teams anvendt SIEM-systemer (Security Information and Event Management) til at overvåge og analysere sikkerhedsadvarsler på tværs af deres digitale infrastruktur.

Efterhånden som omfanget og raffineringen af cyberangreb er vokset, har sikkerhedsteams føjet en lang række værktøjer til deres SIEM-systemer i et forsøg på at øge synligheden af sårbarheder og aktive trusler.

I hele forløbet har SIEM-systemer været en effektiv tilføjelse til SecOps-værktøjskassen. Organisationer investerer fortsat kraftigt i løsningen. En Gartner-rapport viser, at "SIEM-markedet voksede fra 3,41 milliarder USD i 2020 til 4,10 milliarder USD i 2021 – en årlig vækstrate på 20 % sammenlignet med et fald på 3,9 % året før."[1]

Efterhånden som organisationer flytter mere af deres it-stak til en cloud-løsning, følger der cloud-baserede sikkerhedsværktøjer med. En række cloud-baserede tjenester kan supplere SIEM-løsninger med specifikke sikkerhedsmanagementfunktioner og hjælpe SecOps-teams med at identificere problemer, lukke sårbarheder og reagere på aktive trusler. Men disse tjenester har også tilføjet lag af kompleksitet og ufiltreret støj, der faktisk kan øge risikoen i stedet for at reducere den.

Ud over øget kompleksitet og risiko kan denne vækst af supplerende tjenester også have økonomiske konsekvenser – især på et tidspunkt, hvor beslutningstagerne for sikkerhed føler et større pres for at reducere omkostningerne.[2]

SecOps-teams har brug for en bedre løsning til at identificere, beskytte og forsvare sig mod en konstant skiftende angrebsflade. XDR-platforme (Extended detection and response) er en måde at styrke en cloud-baseret SIEM på for at opnå bedre trusselsbeskyttelse, smartere telemetri, avanceret automatisering og øget effektivitet.

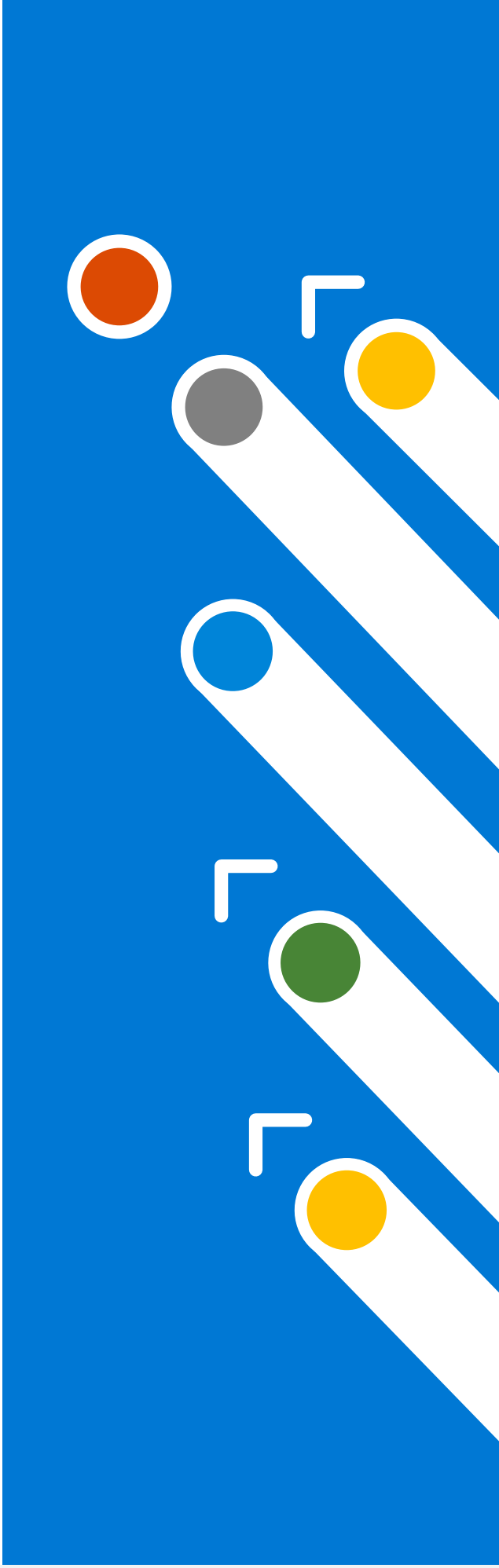
En løsning, der integrerer SIEM og XDR, kan også hjælpe organisationer med at gøre mere med mindre, ved at konsolidere individuelle værktøjer og øge automatisering og integration på måder, der reducerer managementomkostningerne for SecOps.

I denne e-bog undersøger vi udfordringerne ved at bruge punktløsninger med SIEM og forklarer, hvordan integration af SIEM med XDR kan gøre SecOps mere omkostningseffektiv og håndterbar, samtidig med at beskyttelsen forbedres på tværs af virksomheden.

1

For mange løsninger tilføjer omkostninger og kompleksitet

Et kludetæppe af sikkerhedsværktøjer og -strategier gør det vanskeligt at opfylde kravene i nutidens distribuerede virksomhed. Engangsløsninger inden for sikkerhed kan være dyre at vedligeholde, tidskrævende at implementere og bidrager uundgåeligt til en skræmmende blanding af konsoller og rapporter, der er svære at overvåge og administrere.



Det er blevet vigtigere og vigtigere at reducere kompleksiteten i sikkerhedsinfrastruktur. En Gartner-undersøgelse viser, at "75 % af organisationerne gik efter en konsolidering af sikkerhedsleverandører i 2022 mod 29 % i 2020."[3]

Færre værktøjer på hånden muliggør mere problemfri integration med SIEM og en bedre koordineret registrering og respons. Alle komponenterne i sikkerhedsstakken kan nemmere fungere sammen for at finde og fjerne sofistikerede modstandere, uanset hvor de lurer.

I betragtning af den enorme mængde sikkerhedssignaler, der genereres af det digitale økosystem, har moderne løsninger også brug for indbygget kunstig intelligens (AI) og automatisering til at behandle rutineopgaver og filtrere advarsler af høj værdi fra al denne støj. SIEM er nødt til at udvikle sig, så det rækker ud over synligheds- og logdata, for at give SecOps-teams en mere proaktiv tilgang til at identificere og afhjælpe trusler, samtidig med at mange opgaver automatiseres og tilbydes på et forenklet niveau af management, som reducerer risikoen.

3 ud af 4

Tre ud af fire organisationer gik efter en konsolidering af sikkerhedsleverandører i 2022.

Hvis det skal ske, er det vigtigt at flytte til en cloud-baseret SIEM. Integration med en XDR-løsning (udvidet registrering og svar) kan forbedre effektiviteten og omkostningseffektiviteten af sikkerhedsaktiviteter endnu mere. En Forrester Consulting Total Economic Impact™ (TEI)-undersøgelse på vegne af Microsoft viste, at organisationer, der implementerer integreret Microsoft SIEM og XDR, oplevede betydelige omkostningsbesparelser og en stigning i effektiviteten af sikkerhedsaktiviteter. Dette var nogle af fordelene for den sammensatte organisation, der er repræsentativ for de interviewede kunder:

- **Microsoft SIEM og XDR reducerede omkostningerne til en ældre SIEM-løsning, der er forbundet med on-premises-infrastruktur, og løbende management-ansættelse, hvilket medførte en besparelse på næsten 1,6 mio. USD årligt på konsolidering af leverandører.**

- **Microsoft SIEM og XDR reducerede omkostningerne til sikkerhedsbrud med 3,9 mio. USD over tre år.**

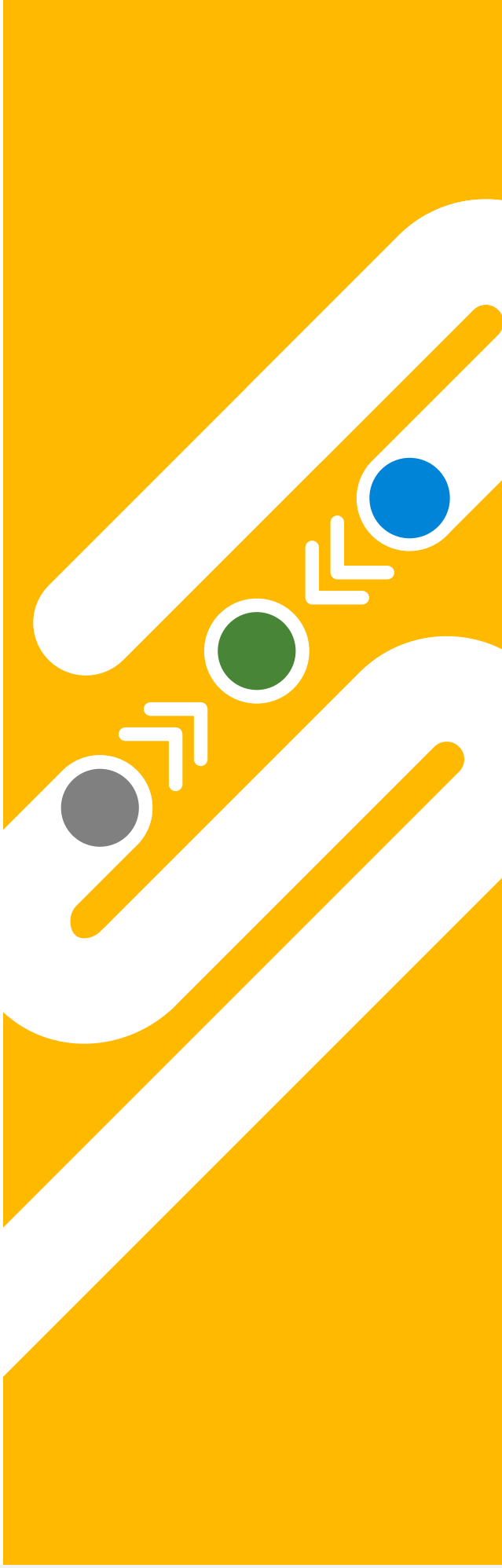
207 % ROI

Microsoft SIEM og XDR genererede en nutidsværdi (NPV) på 11,92 mio. USD og et investeringsafkast på 207 % over tre år.

2

Identificer, hvilke cloud-baseredde tjenester du kan konsolidere med en integreret løsning

Da virksomhedens sikkerhedsgrænser kom uden for virksomhedens mure, tilføjede SecOps-teams en række tredjepartsværktøjer og -tjenester for at styrke SIEM. Men da organisationer nu går efter at reducere omkostningerne, kompleksiteten og risikoen, kan mange af disse løsninger konsolideres med en mere omfattende, integreret løsning.



Mange almindelige cloud-baserede tjenester kan styrke SIEM-konfigurationer. De tilbyder vigtige funktioner, der kan hjælpe et SIEM-system med at forbedre beskyttelsen, men det udgør en række udfordringer at integrere og administrere dem.

Derfor er følgende værktøjer og tjenester et godt sted at kigge først under overvejelsen af, hvor man skal konsolidere.

Eksempler på værktøjer og tjenester, du bør overveje i forbindelse med konsolidering med en integreret løsning

Cloud Access Security Broker (CASB)
En CASB fungerer som et "tæppe" oven på en cloud-baseret SIEM. Den indsamler logoplysninger fra flere kilder og eksponerer unormale hændelser og trusler, hvilket gør SIEM cloud-fokuseret og giver den de oplysninger, der er nødvendige for afhjælpning.

Cloud Security Posture Management (CSPM)
CSPM automatiserer identifikation og afhjælpning af risici på tværs af cloud-infrastrukturer og anvender også bedste praksis for cloud-sikkerhed i multicloud-miljøer.

Cloud Workload Protection Platform (CWPP)
CWPP'er er sikkerhedsløsninger, der er målrettet mod de unikke beskyttelseskrav i workloads i moderne hybrid- og multicloud-miljøer. De hjælper sikkerhedsteams med at opdage og beskytte workloads i on-premises- og public cloud-miljøer.

Endpoint Detection and Response (EDR)
EDR afgør, om der er installeret malware på en endpoint-enhed, og finder måder at reagere på. Når de er installeret, indsamler EDR-løsninger data fra mange forskellige kilder og gemmer dem i en central database.

NDR (Network Detection and Response)
NDR anvender AI og sikkerhedsundersøgelser til at registrere og reagere på cyberangreb i realtid for at holde øje med skjult hackeradfærd i workloads i skyen og hybrid cloud samt i on-premises-virksomhedsnetværk.

Håndtering af sikkerhedsrisici
Håndtering af sikkerhedsrisici er en kontinuerlig, proaktiv og ofte automatiseret proces, der beskytter dine computersystemer, netværk og virksomhedsapplikationer mod cyberangreb og brud på datasikkerheden.

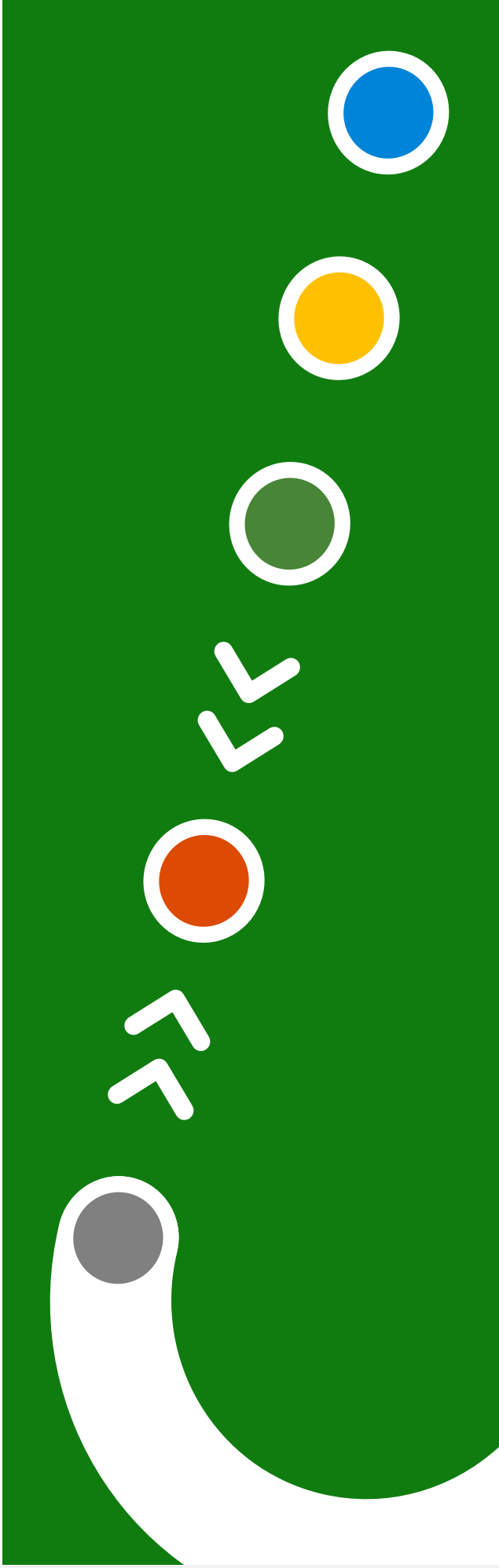
Forebyggelse af datatab (DLP)
DLP giver en balance mellem beskyttelse og produktivitet, hvilket sikrer, at de korrekte adgangskontroller er på plads, og at politikker er angivet til at forhindre handlinger såsom forkert lagring eller udskrivning af følsomme data.

Secure Web Gateway (SWG)
SWG er en websikkerhedstjeneste, der filtrerer uautoriseret trafik fra at få adgang til et bestemt netværk. Målet med en SWG er at stille skarpt på trusler, før de trænger ind i en virtuel perimeter.

3

Få mere ud af SIEM med XDR

En cloud-baseret SIEM-løsning giver værdifuld indsigt, hvilket giver SecOps-teams en omfattende kommando- og kontroloplevelse på tværs af hele virksomheden. Den kan indsamle og analysere data på tværs af hele organisationen for at registrere, undersøge og reagere på hændelser, der går på tværs af siloer. Den kan også forbedre SecOps-effektiviteten med tilpassede analyser og indbygget automatisering.



I stedet for at overlægge flere punktløsninger, der tilføjer kontraproduktiv kompleksitet, bør CCIO'er overveje at integrere XDR som et mere effektivt supplement til SIEM, der hjælper med at indsamle og behandle telemetri fra hele it-stakken i et enkelt dashboard. XDR giver dybde inden for viden om specifikke trusler, mens SIEM giver bred synlighed i forhold til styringen af sikkerhedsaktiviteter set fra et fugleperspektiv.

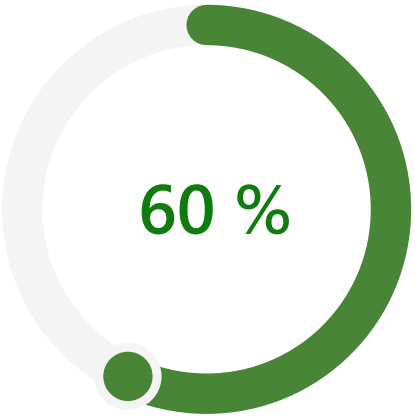
XDR gør, at sikkerhedsstyring rækker ud over endpoints, for at hjælpe SecOps-teams med at undersøge angreb ved at undersøge specifikke ressourcer på tværs af platforme og cloud-løsninger. XDR anvender trusselsviden på aggregerede data for mere effektivt at identificere tendenser, så SecOps-teams hurtigere kan opdage sårbarheder, opdage angreb og reagere ved hjælp af automatisk afhjælpning. Teknologien kan hjælpe med at reducere antallet af advarsler, som sikkerhedsteamet skal undersøge, ved at anvende korrelations- og adfærdsanalyse på konsoliderede trusselsdata for at eliminere falske positiver og advarsler med lav pålidelighed.

Microsoft's XDR-løsning omfatter Microsoft 365 Defender og Microsoft Defender for Cloud, som automatisk indsamler, korrelerer og analyserer sikkerhedssignaler og trusselsadvarselsdata, der involverer endpoints, brugere, applikationer, Internet of Things og cloud-workloads. Den bruger AIog automatiseringsfunktioner til at stoppe angreb hurtigere og afhjælpe berørte aktiver.

En Forrester Consulting Total Economic Impact™ (TEI)-undersøgelse viste, at organisationer, der implementerer integreret Microsoft SIEM og XDR, reducerede risikoen for et sikkerhedsbrud med 60 %, reducerede den tid, det tager at undersøge trusler, med 65 %, og reducerede den tid, det tager at reagere på trusler, med 88 % for den sammensatte organisation, der er repræsentativ for de interviewede kunder.

På grund af dens dybdegående funktionalitet og automatiseringsfunktioner kan XDR også hjælpe CCIO'er med at håndtere de presserende udfordringer i forbindelse med talentkløften inden for cybersikkerhed. En (ISC)2 Cybersecurity Workforce Study anslår, at den globale mangel på talenter i arbejdsstyrken inden for cybersikkerhed er på 3,4 millioner mennesker. SecOps-teams er efterspurgte dygtige sikkerhedsmedarbejdere og bliver ofte overvældet af advarsler og et efterslæb af hændelser, der skal undersøges og potentielt afhjælpes.

Forrester Consulting TEI-undersøgelsen viste – for den sammensatte organisation – at Microsoft SIEM og XDR reducerede den tid, det tager at oprette en ny projektmappe, med 90 %, og tiden til at onboarde nye sikkerhedsmedarbejdere blev reduceret med 91 %. Forbedret undersøgelse af og responstid på trusler sparede yderligere 2,7 mio. USD over tre år.



Microsoft SIEM og XDR reducerede risikoen for et sikkerhedsbrud med 60 %.

Microsoft anerkendes som Leader i 2022 Gartner® Magic Quadrant™ for SIEM

Microsoft havde også den højeste "Ability to Execute"-placering (leveringsdygtighed) i 2022 Gartner Magic Quadrant for Security Information and Event Management-rapporten.[4] Forskellige brancheanalytikere har konsekvent angivet Microsoft som førende inden for sikkerhed, overholdelse af angivne standarder, identitet og management. Få mere at vide

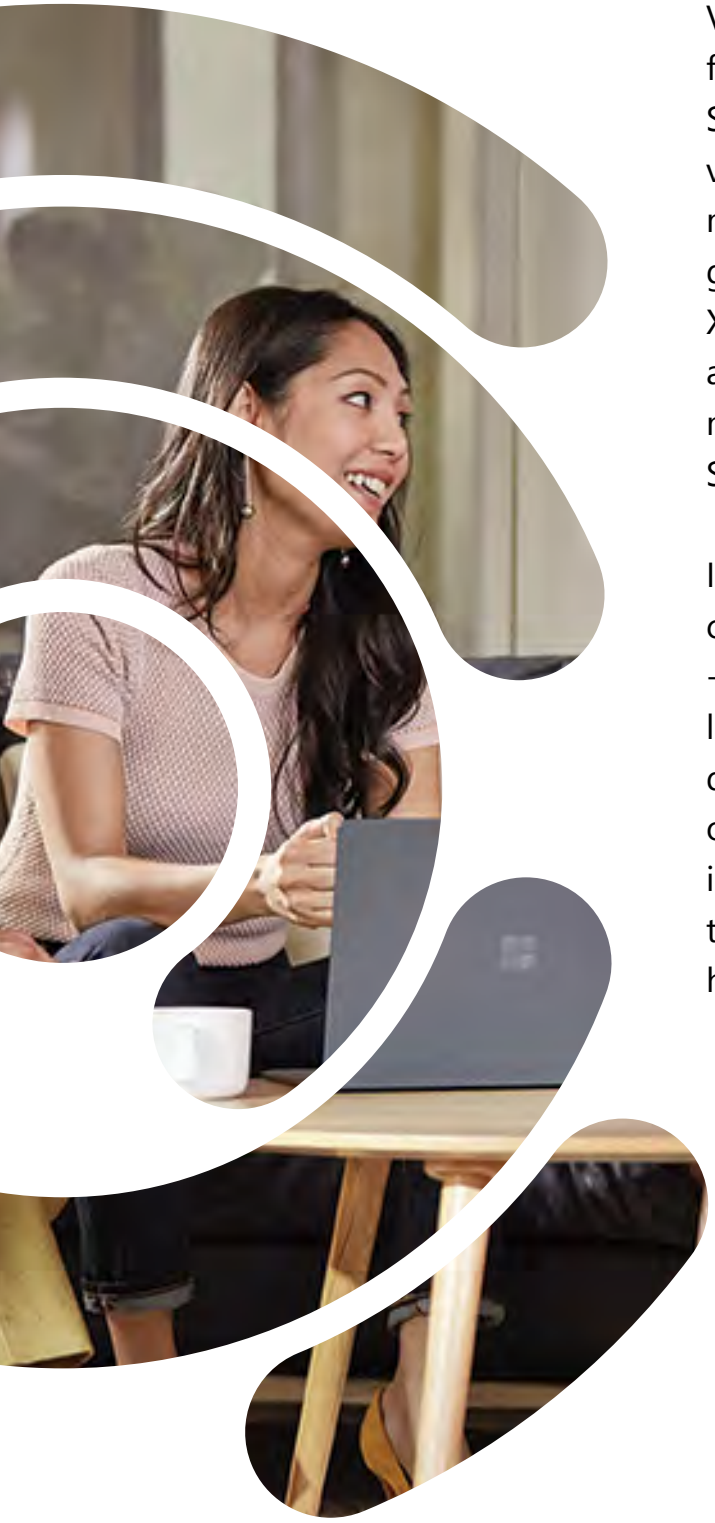
4

Integration og synkronisering gør trusselssammenhængen større

Ved at integrere SIEM og XDR kan systemer dele endnu flere hændelser, skemaer og advarsler, hvilket giver SecOps-teams en samlet visning og mulighed for problemfrit at dykke ned i individuelle hændelser for at give mere sammenhæng. Sammen giver Microsoft Sentinel, Microsoft Defender for Cloud og Microsoft 365 Defender en bred og dyb synlighed på tværs af organisationer og forbedrer samtidig SecOps' effektivitet og responstider.

Connectorer giver organisationer mulighed for at streame data fra Microsoft XDR-løsningen til Microsoft Sentinel, så SecOps-teams kan se, analysere og reagere på Defender-advarsler – og de hændelser, de genererer – i en bredere organisatorisk sammenhæng.

Et team, der bruger Kusto Query Language (KQL) til at udforske Log Analytics i Microsoft Sentinel, kan f.eks. bruge den samme forespørgsel i Microsoft 365 Defender til at se på ydeevnerelaterede data eller følge op på en advarsel. Oplysningerne mellem de to systemer synkroniseres i begge retninger, så sikkerhedsanalytikere nemt kan flytte fra det ene værktøj til det andet for at identificere, afhjælpe og lukke en hændelse. Når en hændelse, der indeholder en sikkerhedsadvarsel, lukkes i ét system, lukkes den tilsvarende advarsel i det tilsluttede system automatisk.



Ved at tilføre XDR-data til SIEM kan organisationer få mere værdi ud af begge teknologier. Et integreret SIEM- og XDR-miljø har et enkelt dashboard til visning og management af trusler på tværs af multicloud-, on-premises- og hybridmiljøer. Dette giver mulighed for, at milliarder af signaldata fra XDR og andre kilder kan reduceres til tusindvis af advarsler og snesevis af hændelser – og dermed minimere advarselstræthed og falske positiver for SecOps-team.

Integration hjælper SecOps-teams med at udføre centraliseret, kontekstbaseret trusselsregistrering, -analyse og -respons. SIEM-platforme tilbyder logmanagement- og arkiveringsfunktioner for XDR-data, så de er tilgængelige for trusselsundersøgelse og efterforskningsanalyse. Dette kan give bedre indsigt i tidligere sikkerhedshændelser, så der kan træffes foranstaltninger til at forhindre, at de samme hændelser sker igen.

Integreret forebyggelse af, registrering af og respons på trusler med Microsoft SIEM og XDR

Angreb eskalerer i hyppighed og raffinement, og ældre værktøjer kan ikke længere holde trit med det skiftende trusselslandskab. CCIO'er har brug for en mere effektiv og omfattende løsning, især da mange føler et organisatorisk pres for at gøre mere med mindre.

Microsofts vision for SIEM og XDR er at levere en enkelt, integreret løsning, der hjælper SecOps-teams med at stoppe angreb og beskytte deres organisationer. Microsoft SIEM- og XDR-løsninger strækker sig ud over indbyggede og hybride modeller for at sikre, at dybden af automatiseret korrelation fra XDR integreres med bredden af en cloud-baseret SIEM, så kompleksiteten reduceres, omkostningerne sænkes og risikostatussen styrkes.

De avancerede sikkerheds- og overholdelsesfunktioner i Microsoft 365 E5 kan give besparelser på op til 60 % i forhold til sammenlignelige selvstændige løsninger fra flere leverandører.[5]
Se, hvor mange punktløsninger du kan fjerne fra dit regnskab med Microsoft 365 E5 >

Find ud af, hvordan integreret trusselsbeskyttelse kan hjælpe dit sikkerhedsteam med at gøre mere med mindre.

Få mere at vide >

[1] Gartner, "Magic Quadrant for Security Information and Event Management," Pete Shoard, Andrew Davies, Mitchell Schneider, 10. oktober 2022.
[2] Undersøgelse blandt 501 beslutningstagere i USA inden for sikkerhed, bestilt af Microsoft fra bureauet Vital Findings, marts 2022.
[3] Gartner-pressemeddelelse, "Gartner Survey Shows 75 % of Organizations Are Pursuing Security Vendor Consolidation in 2022," 13. september 2022.
[4] Gartner, "Magic Quadrant for Security Information and Event Management," 10. oktober 2022.
[5] Illustrativ sammenligning baseret på Web Direct-/basisprisen for Microsoft 365 E5-overholdelses- og sikkerheds-add-ons til Microsoft 365 E3 (24 USD pr. bruger) sammenlignet med priser for flere leverandører baseret på offentligt tilgængelige estimerede priser for andre leverandørløsninger (63 USD pr. bruger).