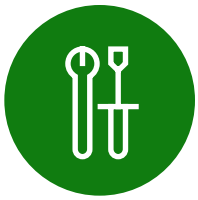
Microsoft Security

Tre grunner til å bytte til integrert trusselbeskyttelse

Innhold

Innledning



Gjennomsnittsbedriften bruker nå over 30 forskjellige sikkerhetsverktøy, og ofte er de atskilte og «skrudd på» utenfra.

Vår sikkerhet står ved et vendepunkt. Nettangrep blir stadig mer avanserte samtidig som organisasjoner fortsetter å håndtere utfordringer som gjelder alt fra mangel på arbeidskraft og kostnadsbalansering til innføring av hybridarbeid.

Og sikkerhetsmarkedet er mer fragmentert og komplekst enn noensinne. Gjennomsnittsbedriften bruker nå over 30 forskjellige sikkerhetsverktøy, og ofte er de atskilte og «skrudd på» utenfra. Dette gir sikkerhetsavdelinger begrenset innsyn og innsikt.

Sikkerhets- og samsvarsledere ønsker en bedre forståelse av de nyeste risikoene og truslene, men de må også vite hva som fungerer, hva som ikke fungerer, og hvor de har hull og mangler.

Selv om omfanget av dagens sikkerhetsutfordringer kan virke overveldende, er det grunn til optimisme for sikkerhetssjefer som ønsker å forbedre effektiviteten til sikkerhetsoperasjonene. Svaret ligger i en integrert, ende-til-ende-tilnærming til nettrusselbeskyttelse, som vil hjelpe organisasjoner:

Første grunn: Gjør mer med mindre

Konsolider punktløsninger og reduser sikkerhetskostnader.

Andre grunn: Hjelp sikkerhetsavdelingen med å fokusere på de viktigste oppgavene

Bruk verktøy som øker effektiviteten og gjør selv junioranalytikere mer kompetente.

Tredje grunn: Øk de ansattes produktivitet

Beskytt organisasjonen din slik at ansatte kan jobbe og innovere uten å bekymre seg.

Denne tilnærmingen er mulig ved å integrere en løsning for utvidet oppdagelse og respons (XDR) med et skybasert system for administrasjon av sikkerhetsinformasjon og -hendelser (SIEM) som bruker kunstig intelligens (KI) og automatisering. Den integrerte løsningen kan hjelpe sikkerhetsavdelingen din med å ha en mer prediktiv, proaktiv og forebyggende tilnærming til angrep i hele bedriften.

Første grunn

Gjør mer med mindre

Ved å konsolidere verktøy med Microsofts integrerte løsning kan du også spare penger ved å betale for bare det du bruker.

Mange organisasjoner har tilnærmet seg sikkerhetsverktøy ved å fokusere på de beste punktløsningene. Dessverre kan denne tilnærmingen gjøre det vanskeligere for sikkerhetspersonell å identifisere og reagere på trusler raskt. Den kan også ha en negativ innvirkning på IT-kostnader og sluttbrukerproduktivitet.

Når organisasjoner i stedet søker å gjøre mer med mindre, kan en integrert tilnærming som Microsofts SIEM og XDR være til hjelp. Den kan redusere kompleksiteten ved å konsolidere individuelle verktøy – og fordi en slik integrert løsning er innebygd i skyen, kan den også forbedre ytelse og skalering.

Ved å konsolidere verktøy med Microsofts integrerte løsning kan du også spare penger ved å betale for bare det du bruker. Og ved å øke bruken av automatisering og integrasjon kan du også redusere sikkerhetskostnadene som går med til å administrere løsninger.

«Det er enkelt å starte prosessen med å ta i bruk nye sikkerhetsverktøy fordi du forventer at hullene er store. Derfra skjønner du snart at verktøy fra ulike leverandører kan være overlappende. En slik overlapping kan være ønskelig for å ha en fordelings- og kontrollmekanisme på plass, **men den kan koste oss mye økonomisk.**»

Jonathan Cassar
Teknologisjef, MITA

1,6 millioner

dollar i årlige besparelser fra leverandørkonsolidering

Forrester Consulting fikk i oppdrag av Microsoft å gjennomføre en TEI-undersøkelse (Total Economic Impact™) for å undersøke hvilken potensiell avkastning bedrifter kan oppnå ved å ta i bruk SIEM og XDR fra Microsoft. Her er noen av de viktigste funnene for en hypotetisk sammensatt organisasjon med 8000 ansatte og et sikkerhetspersonell på 10:

- **Nesten 1,6 millioner dollar i årlige besparelser fra leverandørkonsolidering**. Investeringen i SIEM og XDR fra Microsoft gjør at den sammensatte organisasjonen kan redusere kostnaden for tidligere SIEM (560 000), tilknyttet lokal infrastruktur (over 360 000), tre XDR-punktløsninger (192 000) samt kostnaden for administrasjonen av disse (480 000).
- **Reduksjon i risikoen for et vesentlig sikkerhetsbrudd med 60 %.** Med en mer effektiv arbeidsflyt for sikkerhetsundersøkelser og -respons, forbedret automatisering av sikkerhetsrespons og forbedret evne til å beskytte alle databehandlingsmiljøer, inkludert beskyttelse av flere skyer, reduserer den sammensatte organisasjonen risikoen for sikkerhetsbrudd tilsvarende en årlig besparelse på 1,6 millioner dollar.
- **Generering av avkastning på 207 %.** De representative intervjuene og den økonomiske analysen viser at en sammensatt organisasjon opplever fordeler verdt 17,68 millioner dollar over tre år kontra kostnader på 5,76 millioner dollar. I sum gir dette en netto nåverdi på 11,92 millioner dollar.

Andre grunn

Hjelp ssikkerhets-avdelingen med å fokusere på de viktigste oppgavene

Det er viktig å integrere SIEM og XDR for å koordinere varsler, prioritere de største truslene og koordinere handling i hele bedriften.

Sikkerhetsavdelinger overveldes av alle signalene de må analysere. I tillegg har mange av signalene lav kvalitet som er vanskelige, om ikke umulige, å oppdage manuelt og utbedre. Med økende trusler er det vanskelig for en overbelastet sikkerhetsavdeling å holde koken, spesielt når den skal analysere data fra flere punktløsninger. Tildeling av flere ressurser for å tette hull og mangler er ikke svaret, siden det er en pågående utfordring å finne nok dyktige sikkerhetsarbeidere.

Derfor er det viktig å integrere SIEM og XDR for å kunne korrelere varsler, prioritere de største truslene og koordinere tiltak i hele bedriften med avansert kunstig intelligens og automatisering som oppdager og reduserer trusler proaktivt.

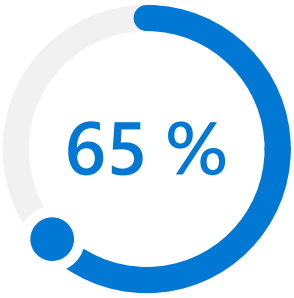
Tenk for eksempel at ett enkelt signal på lavt nivå ikke får mye oppmerksomhet fra en tradisjonell SIEM. Men ved hjelp av kunstig intelligens kan en skybasert SIEM imidlertid automatisk sammenligne dette signalet med signaler fra andre kilder i hele organisasjonen, og samkjøre flere datasett for å finne angrep i flere trinn.

Integrert SIEM og XDR frigjør sikkerhetsressurser samtidig som de gir selv junioranalytikere flere muligheter og større tro på seg selv.

Systemet vil deretter normalisere, analysere og korrelere dataene, samtidig som det gir kontekst om hvordan nettangrepet kom inn i infrastrukturen, sammen med tidslinjen for hvordan det spredte seg. Dette gjør at sikkerhetssenterteamene kan visualiserer bruddet – fra én enkelt konsoll – og løse det på en effektiv måte.

> Mange sikkerhetssjefer skjønner ikke **kostnaden de pålegger sine medarbeidere med 20 forskjellige glassruter** eller punktløsninger samt tilknyttede årlige kostnader ... ved å holde oss til én enkelt leverandør har vi fått bukt med mye av de ansattes oppgitthet rundt verktøy.»
>
> **Terence Jackson**
> Sjef for informasjonssikkerhet og personvern, Thycotic

En organisasjon skal ikke måtte trenge spesialkompetanse for å kunne nyttiggjøre seg sikkerhetsløsningen sin. Integrert SIEM og XDR frigjør sikkerhetsressurser samtidig som de gir selv junioranalytikere flere muligheter og større tro på seg selv.



Microsofts integrerte tilnærming med SIEM og XDR reduserte tiden for trusselundersøkelser med 65 %.

Forrester Total Economic Impact™ (TEI)-studien som Microsoft bestilte, viser følgende effektivisering av sikkerheten i studiens sammensatte organisasjon:

- **65 % raskere trusselundersøkelser og 88 % raskere trusselrespons.** Microsofts integrerte tilnærming til trusselundersøkelse og -respons med kombinert SIEM og XDR gjør arbeidsflyten mer effektiv for den sammensatte organisasjonens sikkerhetspersonell. De trenger ikke lenger å hoppe fra verktøy til verktøy for å identifisere trusler, og automatiseringsfunksjoner forbedrer sikkerhetsresponsen ytterligere.
- **90 % raskere oppretting av ny arbeidsbok og 91 % raskere introduksjon av nytt sikkerhetspersonell.** Microsofts integrerte tilnærming med kombinert SIEM og XDR gjør også andre sikkerhetsoppgaver mer effektive. Siden SIEM-logger er integrert i hele løsningspakken, er oppretting av arbeidsbøker nesten automatisert, og én enkelt pålogging gjør at nytt sikkerhetspersonell kan introduseres nesten 16 uker raskere.

Tredje grunn

Øk de ansattes produktivitet

En integrert SIEM- og XDR-løsning kan hjelpe organisasjonen din med å øke sluttbrukernes produktivitet.

I tillegg til at organisasjoner kan gjøre mer med mindre og effektivisere sikkerhetsoperasjoner kan en integrert SIEM- og XDR-løsning hjelpe dem med å øke sluttbrukernes produktivitet.

Sikkerhetsavdelinger vet godt at når sikkerheten er vanskelig i bruk, da slutter folk å bry seg. Når brukeropplevelsen blir et hinder snarere enn til hjelp for ansattes produktivitet, kan det gjøre en organisasjon mer åpen for økt sikkerhetsrisiko og høyere kostnader. Svake passord eller passord på avveie, usikret tilgang via personlige enheter eller uhindret deling av sensitive data er bare noen av utfordringene.

> Tidligere brukte vi sløve instrumenter når noen mistenkte et problem. Vi lukket ting ned og avsluttet tilgangen, noe som påvirket virksomheten negativt. Og det hele var åpenbart for alle fordi ting sluttet å fungere midlertidig. I Microsoft Sentinel har vi en skalpell slik at vi kan reagere med kirurgisk presisjon. **Bedriften vet vanligvis ikke engang når vi reagerer på en trussel**, og det er et veldig viktig tegn på at vi har lykkes.»
>
> **Rick Gehringer**
> Informasjonssjef, Wedgewood

Nesten

68 000

Microsofts SIEM- og XDR-løsning forbedret produktiviteten til andre ansatte med nesten 68 000 timer totalt årlig.

En tilnærming med integrert SIEM og XDR hjelper deg med å levere sømløse brukeropplevelser som gjør at medarbeiderne dine er både produktive og trygge i alt de gjør i løpet av en dag. Tilnærmingen kan redusere produktivitetshindringer, for eksempel å måtte slå av tjenester eller isolere for så å gjenskape maskiner gjennom avbildning. Men integrert SIEM og XDR kan også gi produktivitetsgevinst for sluttbrukere, for eksempel med mer selvbetjent sikkerhetsstøtte, bedre instrumentbord og rapportering samt bedre responsevne og raskere oppstartstider fordi man kjører færre sikkerhetsagenter.

I Forrester Total Economic Impact™ (TEI)-studien som ble bestilt av Microsoft, opplever den hypotetiske sammensatte organisasjonen med 8000 ansatte en økning i ansattes produktivitet ved å ta i bruk SIEM og XDR fra Microsoft:

- **Forbedring av ansattes produktivitet med nesten 68 000 timer totalt årlig.** Microsofts SIEM og XDR forhindrer at ineffektive sikkerhetsprosesser påvirker andre ansatte negativt. Studiens sammensatte organisasjon sparer for eksempel 4000 timer årlig takket være IT-teknikernes nye muligheter for selvbetjening av sikkerhetsoppdateringer og anbefalinger. Den nye sikkerhetstilnærmingen muliggjør også ekstern sikkerhetsbasert feilsøking på ansattes maskiner og reduserer antall sikkerhetsagenter som kjører på dem. Slik spares nesten 64 000 timer årlig i sluttbrukerproduktivitet.

Sikkerhet har blitt en viktig faktor for å lykkes med teknologi. Derfor trenger organisasjoner sikkerhetstiltak som bygger så gir så mye robusthet som mulig mot moderne angrep – for å sikre og muliggjøre produktivitet og innovasjon som fremmer vekst.

Få integrert nettrusselbeskyttelse med SIEM og XDR

Denne integrasjonen av bransjeledende produkter leverer nettrusselforebygging, -oppdagelse og -respons i én enkelt løsning.

Microsoft tilbyr den første og eneste integrerte SIEM- og XDR-løsningen, som gir ende-til-ende-synlighet på tvers av alle skyer og plattformer. Denne integrasjonen av bransjeledende produkter leverer nettrusselforebygging, -oppdagelse og -respons i én enkelt løsning.

Microsofts SIEM- og XDR-løsning bruker kunstig intelligens og automatisering, samt dype, vedvarende investeringer i nettrusseloppdagelse og -analyse – med ekspertinnsikt og innsyn i 43 billioner signaler hver dag. Med integrasjon på tvers av disse produktene har sikkerhetssjefer mer kontekst enn noen gang til å jakte på og håndtere kritiske nettrusler raskere:

Microsoft Sentinel

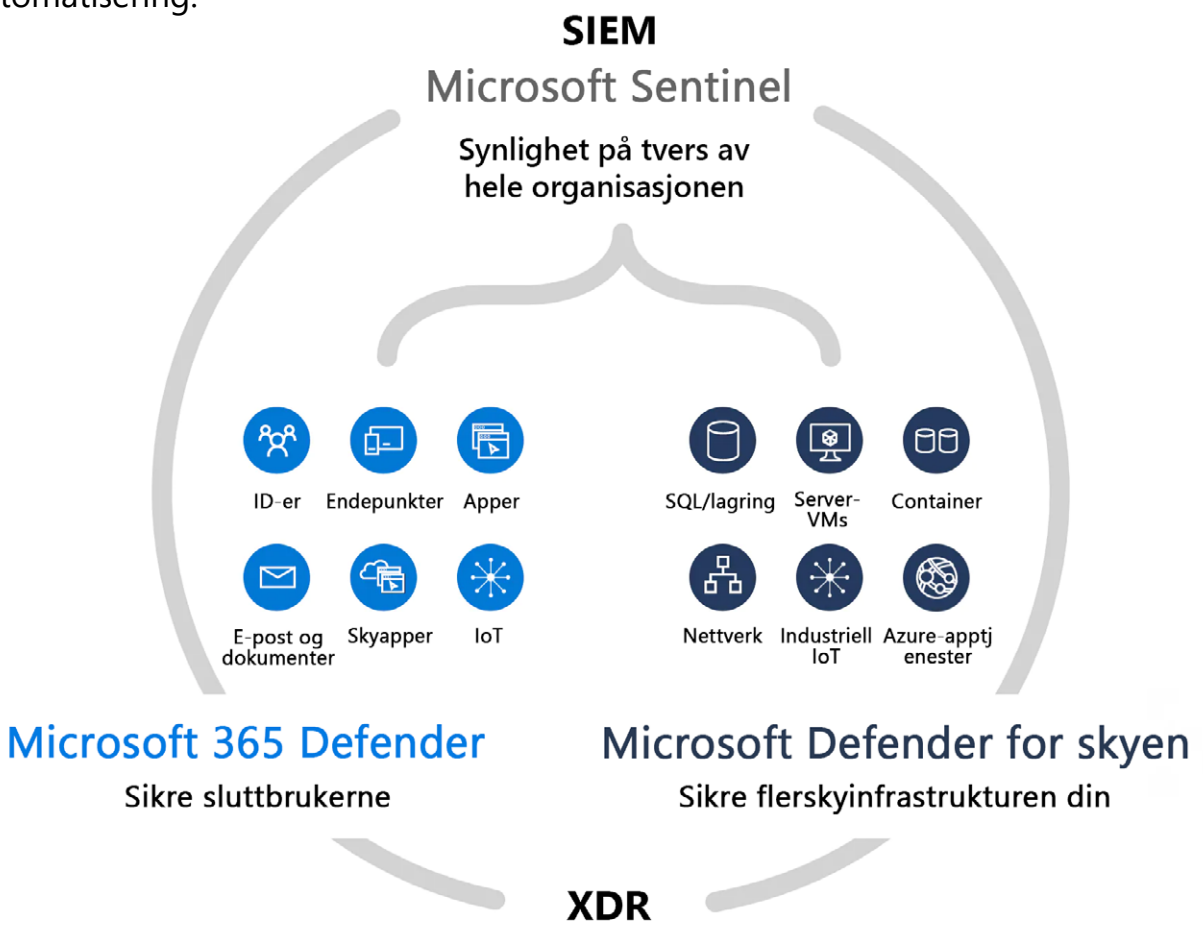
Se hele bedriften i fugleperspektiv med Microsofts skybaserte SIEM. Samle sikkerhetsdata fra nesten hvilken som helst kilde og bruk kunstig intelligens til å skille støy fra reelle hendelser, korreler varsler på tvers av komplekse nettangrepskjeder, og sett fart på nettrusselresponsen med innebygd orkestrering og automatisering.

Microsoft Defender XDR

Forebygg og oppdag nettangrep på tvers av identiteter, endepunkter, apper, e-post, data og skyapper med XDR-funksjoner. Undersøk og reager på nettangrep med førsteklasses beskyttelse som leveres klare for bruk. Jakt på trusler og koordiner responsen enkelt fra ett enkelt instrumentbord.

Microsoft Defender for skyen

Beskytt fler- og hybridskyarbeidsbelastninger med innebygde XDR-funksjoner. Sikre servere, lagringsplasser, databaser, beholdere og annet. Fokuser på det viktigste med prioriterte varsler.



Ikke legg til sikkerhet utenpå. Ha sikkerheten innebygd.

Gi de riktige personene de riktige verktøyene og de riktige dataene. Forsvar bedriften din mot moderne angrep med en skybasert, integrert ende-til-ende-løsning.

Finn ut mer om integrert nettrusselbeskyttelse med Microsofts SIEM- og XDR-løsninger >

Microsoft Security