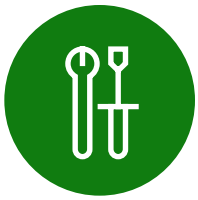
Microsoft Security

Kolme syytä siirtyä integroituun uhkien torjuntaan

Sisältö

Esittely



Keskivertoyrityksessä on nyt käytössä yli 30 erilaista tietoturvatyökalua, jotka ovat usein hajanaisia ja päälle liimattuja.

Tietoturva on taivepisteessä. Kyberhyökkäykset muuttuvat yhä kehittyneemmiksi, ja organisaatiot kohtaavat myös muita haasteita – aina työvoiman osaamisvajeesta ja kustannusten tasapainottamisesta hybridityön tuomiin paineisiin.

Samalla tietoturvamarkkinat ovat hajanaisemmat ja monimutkaisemmat kuin koskaan aiemmin. Keskivertoyrityksessä on nyt käytössä yli 30 erilaista tietoturvatyökalua, jotka ovat usein hajanaisia ja päälle liimattuja, mikä vaikeuttaa tietoturvatiimien työtä.

Tietoturvasta ja vaatimustenmukaisuudesta vastaavat johtajat haluavat paremman käsityksen uusimmista riskeistä ja uhkista, mutta heidän on myös tiedettävä, mitkä ratkaisut toimivat ja mitkä eivät – tietoturva-aukkoja unohtamatta.

Vaikka nykypäivän tietoturvahaasteet saattavat tuntua ylivoimaisilta, toimintojensa tehokkuutta ja vaikuttavuutta parantavilla tietoturvajohtajilla on myös aihetta optimismiin. Vastaus piilee integroidussa, kattavassa lähestymistavassa kyberuhkien torjuntaan. Tämä tuo organisaatiolle seuraavat edut:

Syy 1: Tee enemmän vähemmällä

Yhdistä erilliset ratkaisut ja vähennä tietoturvatoimien (SecOps) kustannuksia.

Syy 2: Anna tietoturvatiimien keskittyä tärkeisiin, arvoa tuottaviin tehtäviin

Käytä työkaluja, jotka parantavat tehokkuutta ja kokemattomienkin työntekijöiden kyvykkyyttä.

Syy 3: Paranna työntekijöiden tuottavuutta

Suojaa organisaatiotasi tavalla, joka poistaa työntekijöiden epävarmuustekijät ja antaa heidän luoda sekä innovoida.

Tämä lähestymistapa on mahdollista integroimalla laajennettu tunnistus- ja vasteratkaisu (XDR) pilvipohjaiseen SIEM-järjestelmään, joka hyödyntää tekoälyä ja automaatiovalmiuksia. Integroitu ratkaisu voi tietoturvakeskustasi kehittymään ennakoivaksi ja ennaltaehkäiseväksi. Näin voit torjua hyökkäyksiä koko yrityksen laajuudella.

1. syy

Tee enemmän vähemmällä

Yhdistämällä työkalut Microsoftin integroituun ratkaisuun voit myös säästää rahaa, sillä maksat vain siitä, mitä käytät.

Monet organisaatiot ovat valinneet tietoturvatyökalut keskittyen alan parhaisiin yksittäisiin ratkaisuihin. Valitettavasti tämä lähestymistapa voi itse asiassa heikentää tietoturva-ammattilaisten mahdollisuuksia havaita uhkia ja reagoida niihin nopeasti. Sillä voi myös olla kielteinen vaikutus IT-kuluihin ja loppukäyttäjien tuottavuuteen.

Kun organisaatiot haluavat tehdä enemmän vähemmällä, Microsoftin SIEM:n ja XDR:n kaltainen integroitu lähestymistapa voi olla hyödyksi. Se voi vähentää monimutkaisuutta yhdistämällä erillisiä työkaluja – ja koska integroitu ratkaisu toimii luontaisesti pilvessä, se voi myös parantaa suorituskykyä ja skaalattavuutta.

Yhdistämällä työkalut Microsoftin integroituun ratkaisuun voit myös säästää rahaa, sillä maksat vain siitä, mitä käytät. Voit myös vähentää ratkaisujen hallintaan tarvittavia tietoturvan yleiskustannuksia lisäämällä automaatiota ja integraatiota.

> Uusien tietoturvatyökalujen käyttöönoton aloittaminen on helppoa, koska täytettävät aukot ovat suuria. Jatkaessasi saatat kuitenkin pian havaita, että eri toimittajien työkalut voivat sisältää päällekkäisiä ominaisuuksia. Tällainen päällekkäisyys voi olla toivottavaa tarkistusten kannalta, **mutta siitä voi myös aiheutua merkittäviä kustannuksia.**"
>
> **Jonathan Cassar**
> Teknologiajohtaja, MITA

1,6 miljoonan dollarin

säästöt vuosittain toimittajakonsolidoinnilla

Microsoft antoi Forrester Consultingille tehtäväksi tehdä Total Economic Impact™ (TEI) -tutkimuksen ja tarkastella sijoitetun pääoman tuottoa, jonka yritykset voivat saavuttaa ottamalla käyttöön Microsoftin SIEM:n ja XDR:n. Tässä on joitakin keskeisiä havaintoja hypoteettisesta organisaatiosta, jossa on 8 000 työntekijää ja 10 tietoturva-ammattilaista:

- **Toimittajakonsolidointi tuo lähes 1,6 miljoonan dollarin säästöt vuosittain.** Investoimalla Microsoftin SIEM- ja XDR-ratkaisuihin organisaatio voi vähentää aiemman SIEM-ratkaisun kustannuksia (560 000 $), siihen liittyvän paikallisen infrastruktuurin kustannuksia (yli 360 000 $), kolmen XDR-pisteratkaisun kustannuksia (192 000 $) sekä näiden jatkuvia hallintakustannuksia (480 000 $).

- **Tietomurtojen riski pienentyy 60 prosenttia.** Entistä tehokkaampien tietoturvatutkimusten ja reagointityönkulkujen, parannetun tietoturva-automaation sekä kaikkien tietojenkäsittely-ympäristöjen (monipilviympäristöt mukaan lukien) parannetun varmistuskyvyn ansiosta organisaation tietomurtoriski pienentyy, mikä tuo vuosittain 1,6 miljoonan dollarin säästöt.

- **Sijoitetun pääoman tuotto 207 %.** Haastattelujen ja taloudellisen analyysin perusteella selvitettiin, että organisaatio saa 17,68 miljoonan dollarin hyödyn kolmen vuoden aikana ja kustannukset ovat 5,76 miljoonaa dollaria, jolloin nettonykyarvoksi tulee 11,92 miljoonaa dollaria.

2. syy

Anna tietoturvatiimien keskittyä tärkeisiin, arvoa tuottaviin tehtäviin

On tärkeää integroida SIEM ja XDR, jotta ne voivat korreloida hälytyksiä, priorisoida suurimmat uhkat sekä koordinoida toimintaa koko yrityksessä.

Analysoitavien signaalien valtava määrä voi olla liikaa monille tietoturvatiimeille. Usein mukana on myös matalan resoluution signaaleja, joiden havaitseminen ja torjuminen manuaalisesti voi olla vaikeaa tai jopa mahdotonta. Uhkien lisääntyessä ylikuormitetun tietoturvakeskuksen voi olla vaikea pysyä tilanteen tasalla, etenkin kun tietoja yritetään analysoida useista pisteratkaisuista. Useampien resurssien allokointi aukkojen paikkaamiseen ei ole vastaus, koska pätevien tietoturva-ammattilaisten löytäminen on jatkuva haaste.

Siksi on tärkeää linjata SIEM ja XDR, jotta ne voivat korreloida hälytyksiä, priorisoida suurimmat uhkat sekä koordinoida toimintaa koko yrityksessä. Kehittynyt tekoäly ja automaatiot havaitsevat ja torjuvat uhkia ennakoivasti.

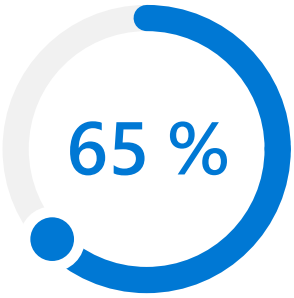
On syytä pohtia esimerkiksi sitä, että yksittäinen matalan tason signaali ei välttämättä saa kovinkaan paljon huomiota perinteiseltä SIEM-ratkaisulta. Tekoälyä käyttämällä pilvipohjainen SIEM voi kuitenkin automaattisesti verrata tätä signaalia koko organisaation muihin signaaleihin sekä korreloida useita datajoukkoja monivaiheisten hyökkäysten löytämiseksi.

Integroitu SIEM- ja XDR-ratkaisu vapauttaa tietoturvatiimien resursseja ja tuo kokemattomillekin analyytikoille uudenlaista varmuutta ja kyvykkyyttä.

Järjestelmä normalisoi, analysoi ja korreloi datan ja tarjoaa samalla kontekstuaalista tietoa siitä, kuinka kyberhyökkäys on tunkeutunut infrastruktuuriin ja minkälaisella aikajanalla se on levinnyt. Näin tietoturvatiimit voivat visualisoida tietomurron yksittäisestä konsolista käsin ja puuttua siihen tehokkaasti.

> Monet tietoturvajohtajat eivät ymmärrä, minkälaista **kuormitusta 20 erilaista näkymää** tai pisteratkaisua tuovat tietoturvatiimeille, puhumattakaan niihin liittyvistä vuotuisista kustannuksista... vaihtamalla yhteen toimittajaan olemme keventäneet työtaakkaa huomattavasti."
>
> **Terence Jackson**
> Tietoturva- ja tietosuojajohtaja, Thycotic

Organisaation ei pitäisi tarvita syvällistä asiantuntemusta tietoturvaratkaisun arvon hyödyntämiseen. Integroitu SIEM- ja XDR-ratkaisu vapauttaa tietoturvatiimien resursseja ja tuo kokemattomillekin analyytikoille uudenlaista varmuutta ja kyvykkyyttä.



Microsoftin SIEM- ja XDR-ratkaisujen integroitu lähestymistapa vähensi uhkien tutkimiseen käytettävää aikaa 65 prosenttia.

Microsoftin tilaamassa Forrester Total Economic Impact™ (TEI) -tutkimuksessa havaittiin organisaation tietoturvatiimien tehokkuuden parantuneen seuraavasti:

- **Uhkien tutkimiseen käytettävä aika vähentyi 65 prosenttia ja uhkiin reagoimiseen käytettävä aika 88 prosenttia.** Microsoftin SIEM- ja XDR-ratkaisujen integroitu lähestymistapa tietoturvauhkien tutkimiseen ja niihin reagoimiseen tekee näistä työnkuluista entistä tehokkaampia organisaation tietoturva-ammattilaisten kannalta. Heidän ei enää tarvitse siirtyä useiden työkalujen välillä uhkien tunnistamiseksi, ja tietoturvan automatisointiominaisuudet tehostavat reagoinnin työnkulkuja entisestään.

- **Uuden työkirjan luomiseen käytettävä aika vähentyi 90 prosenttia ja uusien tietoturva-ammattilaisten perehdyttämiseen käytettävä aika vähentyi 91 prosenttia.** Microsoftin SIEM- ja XDR-ratkaisujen integroitu lähestymistapa tehostaa myös muita tietoturva-ammattilaisten työnkulkuja. Koska SIEM-lokit on integroitu eri ratkaisuihin, työkirjan luonti on lähes automaattista. Yksittäinen kirjautuminen mahdollistaa puolestaan uusien tietoturva-ammattilaisten perehdyttämisen lähes 16 viikkoa aiempaa nopeammin.

3. syy

Paranna työntekijöiden tuottavuutta

Integroitu SIEM- ja XDR-ratkaisu voi auttaa organisaatiotasi parantamaan loppukäyttäjien tuottavuutta.

Sen lisäksi, että integroitu SIEM- ja XDR-ratkaisu auttaa tekemään enemmän vähemmällä ja parantamaan tietoturvatiimien tehokkuutta, se voi auttaa organisaatiotasi parantamaan loppukäyttäjien tuottavuutta.

Tietoturvatiimit tietävät, että jos tietoturvasta tehdään hankalaa, ihmiset löytävät keinoja sen kiertämiseksi. Jos loppukäyttäjien kokemukset pikemminkin haittaavat kuin edistävät työntekijöiden tuottavuutta, se voi altistaa organisaation uusille tietoturvariskeille ja suuremmille kustannuksille. Heikot tai kadonneet salasanat, suojaamaton käyttö omilla laitteilla tai arkaluonteisten tietojen rajoittamaton jakaminen ovat vain osa haasteista.

> Aiemmin käytimme karkeita menetelmiä, kun joku havaitsi epäillyn ongelman. Sammutimme järjestelmät ja estimme niiden käytön, mikä vaikutti negatiivisesti liiketoimintaan. Ongelma tuli myös kaikkien tietoon, sillä järjestelmät olivat tilapäisesti pois käytöstä. Microsoft Sentinel on kuin skalpelli, jonka avulla voimme reagoida tapahtumiin kirurgisesti. **Muut yrityksessä eivät yleensä edes tiedä, milloin reagoimme uhkaan**, ja se on todella tärkeä onnistumisen mittari."
>
> **Rick Gehringer**
> Tietohallintojohtaja, Wedgewood

Lähes
68 000

Microsoftin SIEM ja XDR paransivat muiden työntekijöiden tuottavuutta yhteensä lähes 68 000 tunnilla vuodessa.

Integroitu SIEM- ja XDR-lähestymistapa auttaa tarjoamaan saumattoman käyttökokemuksen, joka varmistaa työntekijöiden tuottavuuden ja turvallisuuden. Se voi vähentää tuottavuutta heikentäviä vaikutuksia, kuten palvelujen sammuttamis- tai eristämistarvetta ja näköistiedostojen uusimista. Integroitu SIEM- ja XDR-ratkaisu voi myös luoda uusia mahdollisuuksia loppukäyttäjien tuottavuuden parantamiseen, muun muassa tietoturvatuen itsepalvelun, parempien raporttien ja raporttinäkymien sekä entistä sujuvammin toimivan järjestelmän myötä, sillä tietoturva-agentteja tarvitaan vähemmän,

Microsoftin tilaamassa Forrester Total Economic Impact™ (TEI) -tutkimuksessa havaittiin, että Microsoftin SIEM:n ja XDR:n käyttöönotto paransi työntekijöiden tuottavuutta hypoteettisessa 8 000 työntekijän organisaatiossa:

- ✓ **Muiden työntekijöiden tuottavuus kasvoi yhteensä lähes 68 000 tunnilla vuodessa.** Microsoftin SIEM ja XDR ehkäisevät tehottomien tietoturvaprosessien kielteisiä vaikutuksia muihin työntekijöihin. Esimerkiksi IT-ammattilaisten mahdollisuus asentaa tietoturvapäivitykset itsepalveluna säästää organisaatiolta vuosittain 4 000 työtuntia. Se mahdollistaa myös tietoturvaongelmien vianmäärityksen etänä työntekijöiden laitteissa ja vähentää niissä suoritettavien tietoturva-agenttien määrää, mikä säästää lähes 64 000 tuntia vuodessa loppukäyttäjien tuottavuudessa.

Tietoturvasta on tullut teknologisen menestyksen olennainen mahdollistaja. Siksi organisaatiot tarvitsevat tietoturvatoimia, jotka tuovat mahdollisimman paljon resilienssiä nykyaikaisia hyökkäyksiä vastaan – näin turvataan tuottavuus ja innovaatiot, jotka edistävät liiketoiminnan kasvua.

Toteuta integroitu kyberuhkien torjunta SIEM- ja XDR-ratkaisuilla

Tämä alan johtavien tuotteiden integraatio mahdollistaa kyberuhkien ehkäisemisen, havaitsemisen ja torjumisen yhdessä kokonaisvaltaisessa ratkaisussa.

Microsoft tarjoaa markkinoiden ensimmäisen ja ainoan integroidun SIEM- ja XDR-ratkaisun, joka tuo kattavan näkyvyyden kaikkiin pilvipalveluihin ja alustoihin. Tämä alan johtavien tuotteiden integraatio mahdollistaa kyberuhkien ehkäisemisen, havaitsemisen ja torjumisen yhdessä kokonaisvaltaisessa ratkaisussa.

Microsoftin SIEM ja XDR hyödyntävät tekoälyn ja automaation tehoa sekä jatkuvaa panostustamme kyberuhkien havaitsemiseen ja analysointiin – asiantuntijamme tarkkailevat päivittäin 43 biljoonaa signaalia. Näiden tuotteiden integraation myötä tietoturvatiimeillä on entistä paremmat valmiudet havaita kriittiset kyberuhat ja reagoida niihin nopeasti:

Microsoft Sentinel

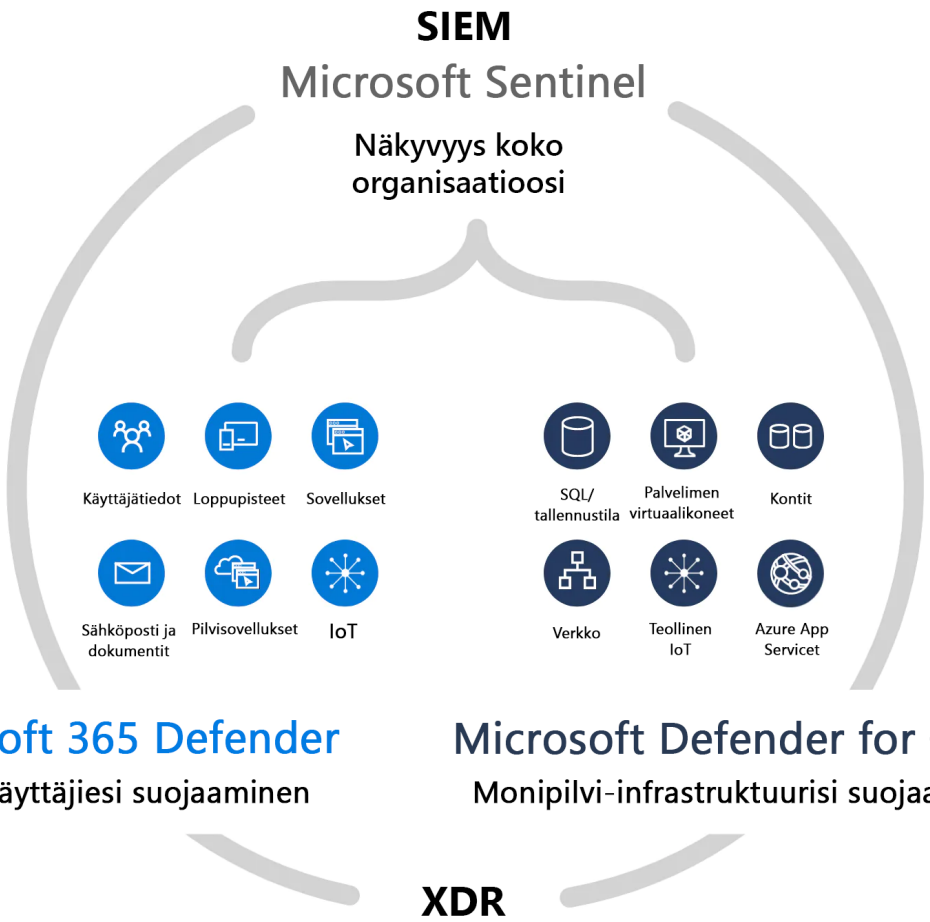
Microsoftin pilvipohjainen SIEM-ratkaisu antaa kattavan kuvan koko yrityksestä. Koosta tietoturvatietoja lähes mistä tahansa lähteestä ja poimi olennaiset tiedot tekoälyn avulla, korreloi hälytykset monimutkaisiin kyberhyökkäysketjuihin ja nopeuta kyberuhkiin reagointia sisäänrakennetun orkestroinnin ja automaation avulla.

Microsoft Defender XDR

Estä ja havaitse identiteetteihin, päätepisteisiin, sovelluksiin, sähköpostiin, tietoihin ja pilvisovelluksiin kohdistuvat kyberhyökkäykset XDR:n avulla. Tutki kyberhyökkäyksiä ja reagoi niihin luokkansa parhaalla, heti käyttövalmiilla tietoturvaratkaisulla. Voit etsiä uhkia ja koordinoida reaktiotoimet helposti yhdessä raporttinäkymässä.

Microsoft Defender for Cloud

Suojaa monipilvi- ja hybridipilvityökuormasi sisäänrakennetuilla XDR-ominaisuuksilla. Turvaa palvelimet, tallennustila, tietokannat, kontit ja muut kohteet. Priorisoidut hälytykset auttavat sinua keskittymään siihen, mikä on tärkeintä.



Älä rakenna erillistä tietoturvaa. Sisällytä se toimintoihin.

Tuo oikeat työkalut ja tiedot oikeiden ihmisten saataville. Puolustaudu nykyaikaisilta hyökkäyksiltä kattavalla, pilvipohjaisella, integroidulla ratkaisulla.

Lue lisätietoja integroidusta kyberuhkien torjunnasta Microsoftin SIEM- ja XDR-ratkaisuilla >

Microsoft Security