KERROKSELLISELLA KYBERTURVALLA SUOJAA EDISTYNEITÄ UHKIA VASTAAN

Teosto lisäsi näkyvyyttä ja sai vauhtia reagointiin laajemmalla tietoturvapaletilla

F-Secure

Yritys:
Teosto ry

TEOSTO

Toimiala:
Voittoa tavoittelematon

Maa:
Suomi

Tuotteet:
F-Secure Elements Endpoint Detection and Response, F-Secure Elements Vulnerability Management, F-Secure Elements Endpoint Protection

Muutokset IT-infrastruktuurissa ja kyberturvaympäristössä saivat Teoston hakemaan uusia ratkaisuja haavoittuvuuksien hallintaan ja uhkien havaitsemiseen. Arkkitehtuurin yhtenäistämiseksi myös päätelaitteiden suojaus päivitettiin pilvipohjaiseksi.

Tavoitteena ajantasainen tilannekuva IT-ympäristöstä

Teosto on vuonna 1928 perustettu perinteikäs musiikin säveltäjien, sanoittajien, sovittajien ja kustantajien tekijänoikeusjärjestö, joka kerää tekijänoikeuskorvaukset musiikin käytöstä ja maksaa ne tekijöille. Järjestön ansiosta musiikin tekijät voivat keskittyä työhönsä ja luoda uutta musiikkia.

Järjestön toiminnassa on yhtäläisyyksiä private banking-palveluihin – musiikin tekijät luovuttavat immateriaalioikeutensa Teostolle jälleenmyytäväksi ja hallinnoitavaksi. Tekijänoikeuksien hallintaan ei ole valmiita tietojärjestelmiä, vaan kriittisimmät järjestelmät ovat Teoston ja muiden alan järjestöjen kehittämiä. Julkisuudessakin mielenkiinnon kohteena olevien musiikin tekijöiden ja asiakkaiden henkilö- ja taloustietojen suojaaminen on Teostolle kriittisen tärkeää.

Teoston IT-arkkitehtuurissa on tapahtunut suuria muutoksia viime vuosien aikana. Uudet teknologiat, kuten pilvipalvelut ja robotiikka, ovat lisänneet IT-ympäristön monimutkaisuutta entisestään.

Uhkien ja haavoittuvuuksien kiihtyvä lisääntyminen sekä alati muuttuvat pilvipalvelut ovat kasvattaneet IT- ja tietoturvapäällikkö Harri Ahokkaan ”yhden miehen SOC-palvelun” työkuormaa: ”Nykymaailmassa tekemistä on entistä enemmän ja se on tehtävä nopeammin. Ratkaisuna ei voi olla, että asioita tehdään manuaalisesti. Pitää pystyä käyttämään automaatiota sen eri muodoissa.”

”

F-Secure Case Study

TEOSTO RY

Jotta jokainen voi kokea musiikin voiman.

Teosto on musiikin säveltäjien, sanoittajien, sovittajien ja kustantajien tekijänoikeusjärjestö, jonka tavoitteena on mahdollistaa musiikin ammattimainen tekeminen ja käyttäminen. Keräämme korvaukset musiikin käytöstä ja tilitämme ne edelleen musiikin tekijöille, jotta he voivat luoda lisää musiikkia.

VAATIMUKSET JA VALINTAPERUSTEET:

- Ajantasainen tilannekuva
- Käyttäytymispohjainen uhka-analyysi
- Jatkuva haavoittuvuuksien hallinta
- Yhtenäinen kokonaisratkaisu
- Sujuva yhteistyö ja kumppanuus toimittajan kanssa

HYÖDYT

- Joustavuus, nopeus ja kustannustehokkuus
- Jatkuva ajantasainen ymmärrys päätelaitteiden tapahtumista selkeässä muodossa
- Kyky havainnoida ja torjua edistyneitä hyökkäyksiä
- Vahvempi suojaus monikerroksellisuudella
- Yhteistyön jatkuvuus

”Tavoitteena olivat hyvät haavoittuvuuksien hallinnan prosessit ja toisaalta jatkuva tilannekuvan ylläpitäminen, mikä olisi mahdollisimman tosiaikainen ja todellinen.”

Harri Ahokas,
IT ja tietoturvapäällikkö

IT-ympäristön monimutkaistuminen nosti esille tarpeen ymmärtää tilannekuvaa entistä paremmin, kuitenkaan lisäämättä työmäärää. ”Tavoitteena olivat hyvät haavoittuvuuksien hallinnan prosessit ja toisaalta jatkuva tilannekuvan ylläpitäminen, mikä olisi mahdollisimman tosiaikainen ja todellinen.”

Harrin mukaan on valtava riski, jos ei tiedä, mitä IT-ympäristössä tapahtuu: ”Asioita tapahtuu niin nopeasti, että ilman hyvää käsitystä omasta infrastruktuurista, hyökkäyspinnasta ja ilman haavoittuvuuksien hallinnan hiottuja prosesseja, riskitaso olisi meille liian korkea.”

”

Ratkaisut haavoittuvuuksien hallintaan ja uhkien tunnistamiseen tutulta toimittajalta

Teostolla oli aiemmin käytössä paikallinen päätelaitesuojausratkaisu F-Securelta. Koska ratkaisu miellytti, siitä oli kertynyt osaamista, ja toimivaan yhteistyöhön sekä tukipalveluihin oltiin tyytyväisiä, Harri Ahokas päätyi testaamaan F-Securen EDR- ja haavoittuvuuksien hallintaratkaisuja.

Teostolla ei ollut aiemmin käytössä käytösmalleihin perustuvaa analytiikkaa tai työkaluja edistyneiden hyökkäysten havainnointiin ja torjuntaan päätelaitetasolla. ”Meidän pitää pystyä tunnistamaan poikkeavuuksia, ei pelkästään ennalta tunnettuja haittaohjelmia tai viruksia”, Harri sanoo. F-Secure Elements Endpoint Detection and Response -ratkaisulla saatiin näkyvyys ja kyvykkyys tunnistaa edistyneitä hyökkäyksiä ja reagoida tapahtumiin: ”F-Secure Elements EDR on käyttöliittymältään hyvä ja siinä on helppo päästä kiinni tapahtumaketjuihin. Onneksi vielä ei olla jouduttu penkomaan mitään tositilannetta.”

”F-Secure Elements EDR on käyttöliittymältään hyvä ja siinä on helppo päästä kiinni tapahtumaketjuihin.”

Harri Ahokas,
IT ja tietoturvapäällikkö

Haavoittuvuusskannaukset oli aikaisemmin ostettu palveluna, mutta vuosittain tapahtuvia kartoituksia ei koettu riittäviksi. ”On tärkeää saada tiheästi päivittyvä tilannekuva ja ymmärrys joka päivä, eikä vain kerran vuodessa. Maailma muuttuu nopeasti uhkien ja haavoittuvuuksien suhteen”, Harri sanoo. F-Secure Elements Vulnerability Management -ratkaisun suorituskyky, pilvipohjaisuus ja kustannustehokkuus olivat ratkaisevia valintakriteereitä jatkuvuuden lisäksi.

”On tärkeää saada tiheästi päivittyvä tilannekuva ja ymmärrys joka päivä, eikä vain kerran vuodessa. Maailma muuttuu nopeasti uhkien ja haavoittuvuuksien suhteen.”

Harri Ahokas,

Samalla kun suojauskerroksia lisättiin päivitettiin myös päätelaitteiden suojaus aiemmasta paikallisesta F-Secure Business Suitesta pilvipohjaiseen F-Secure Elements Endpoint Protection -ratkaisuun. Uusi päätelaitesuojaus toi kaivattua käyttäytymiseen perustuvaa lisäsuojaa entiseen verrattuna. ”Arkkitehtuurihyödyn takia muutos oli järkevä. Siirtyminen Business Suitesta F-Secure Elements EPP:hen oli sujuvaa, sellainen puolen päivän tai päivän operaatio. Meidän sadan endpointin ympäristössä se on aika suoraviivaista toimintaa.” Kaiken kaikkiaan uusien ratkaisujen käyttöönotto sujui nopeasti ja ongelmitta.

Useampi tietoturvaratkaisu antaa aikaa reagointiin

Teoston Harri Ahokkaan näkemyksen mukaan toimiva kyberturvallisuusportfolio on monipuolinen. Yhteen ratkaisuun ei kannata luottaa, vaan suojakerroksia on oltava useita. ”Useampi lukko hidastaa murtautujaa ja lisää todennäköisyyttä sen havaitsemiseen, peliaika kun on pidempi.”

Uuden haavoittuvuuksien skannausratkaisun ansiosta Teoston tietoturvariskien hallinta on tehostunut ja raportteja voidaan tuottaa aina tarvittaessa. ”F-Secure Elements Vulnerability Management on tuonut joustavuutta, nopeutta ja on kustannustehokas verrattuna siihen, miten olemme aiemmin toimineet kyseisellä osa-alueella.”

”F-Secure Elements Vulnerability Management on tuonut joustavuutta, nopeutta ja on kustannustehokas verrattuna siihen, miten olemme aiemmin toimineet kyseisellä osa-alueella.”

Harri Ahokas,
IT and Security Manager

Harri sanoo myös, että EDR-ratkaisu on lisännyt ymmärrystä siitä, mitä päätelaitteilla tapahtuu: ”Se tuottaa mielenkiintoista dataa selkeässä muodossa. Saman tiedon hankkiminen on mahdollista monellakin työkalulla, mutta kompleksisen tapahtumaketjun esitysmuodon takia on tehokkaampaa ajankäyttöä seurata sitä tuota kautta.” Vastaavanlaisten ratkaisujen käyttö vaatii usein paljon osaamista, mutta F-Secure Elements Endpoint Detection and Response saa Harrilta kehuja: “Onhan se ehdottoman helpoksi tehty ja nopea käyttää.”

Harrin mukaan kyberturvallisuutta ei voi taklata ainoastaan teknisillä ratkaisuilla, vaan haasteellisin rajapinta ovat ihmiset. Käyttäjien koulutus ja säännöllinen kyberturvallisuusasioista viestiminen ovatkin avainrooleissa Teostolla. Lisäksi tarvitaan osaamista ja ymmärrystä siitä, mitä tavoitellaan ja mitä ongelmaa ollaan ratkaisemassa: ”Teknologiat itsessään eivät luo kyberturvallisuutta. Kyllä se on se tietty osaaminen – on se sitten kumppanin kautta saatua tai itsellä olemassa olevaa.”

Kokonaisratkaisu on nyt Teostolle arkkitehtuurisesti järkevä. Kaikki päätelaitesuojauksen ratkaisut ovat yhdeltä toimittajalta ja pilvipohjaisia tuoden selkeyttä ja tehokkuutta ylläpitoon. Viimeaikaisten IT-arkkitehtuuri- ja kyberturvapanostusten ansiosta lähitulevaisuudessa ei ole näköpiirissä suuria muutoksia: ”Lähinnä pyritään ylläpitämään nykytasoa ja tarvittaessa totta kai reagoimaan erilaisiin muutoksiin."

F-SECURE

Miten edistynyt hyökkäys havaitaan? Apuna käytetään edistyksellisintä analytiikkaa ja koneoppimista. Se ei kuitenkaan riitä. Täytyy ajatella kuten rikolliset.Kukaan ei hallitse kyberturvallisuutta kuten F-Secure. F-Secure on tehnyt kyberturvallisuuden johtavia innovaatioita jo 30 vuoden ajan ja suojannut kymmeniätuhansia yrityksiä ja miljoonia yksityishenkilöitä. F-Securen kokemus päätelaitteiden suojauksesta sekä uhkien havaitsemisesta ja niihin reagoinnista on vertaansa vailla. Niinpä se pystyy suojaamaan yrityksiä ja yksityishenkilöitä niin edistyneiltä kyberhyökkäyksiltä kuin tietomurroilta ja laajalti levinneiltä kiristyshaittaohjelmilta. F-Securen edistynyt teknologia yhdistää koneoppimisen ja maailmankuulujen tietoturvalaboratorioiden asiantuntemuksen yhdeksi kokonaisuudeksi nimeltä Live Security. F-Securen tietoturva-asiantuntijat ovat osallistuneet Euroopassa useampaan kyberrikostutkintaan kuin minkään muun markkinoilla toimivan yhtiön edustajat, ja sen tuotteita myyvät tuhannet jälleenmyyjät sekä yli 200 laajakaista- ja mobiilipalveluntarjoajaa ympäri maailman. Vuonna 1988 perustettu F-Secure on listattu NASDAQ OMX Helsinki Ltd:ssä.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure