Jarmo Huovinen

Tuotantoverkkoympäristön kyberturvallisuuden parantaminen tekoälyyn perustuvilla ratkaisuilla

Metropolia Ammattikorkeakoulu

Insinööri (YAMK)

Älykäs teollisuus

Insinöörityö

23.5.2023

Tiivistelmä

Tekijä:	Jarmo Huovinen
Otsikko:	Tuotantoverkkoympäristön kyberturvallisuuden parantaminen tekoälyyn perustuvilla ratkaisuilla
Sivumäärä:	84 + 6 liitettä
Aika:	23.5.2023
Tutkinto:	Insinööri (YAMK)
Tutkinto-ohjelma:	Älykäs teollisuus
Ammatillinen pääaine:	Älykäs teollisuus
Ohjaajat:	Ville Hapuoja, verkko- ja tietoturvatiimin päällikkö Jukka Karppinen, Lehtori

Energiateollisuuden kybertietoturvallisuus on tärkeä aihe, sillä energiayhtiöt ovat erittäin riippuvaisia tietojärjestelmistä ja tietoliikenneverkoista toimiakseen tehokkaasti. Kasvava tietomäärä ja verkkoihin liittyvät haasteet, kuten haittaohjelmat ja tietomurrot, tekevät energiateollisuuden kybertietoturvallisuuden ylläpitämisestä entistä haastavampaa. Koneoppiminen ja tekoäly ovat kasvavassa roolissa energiateollisuuden kybertietoturvallisuuden kehittämisessä. Nämä teknologiat mahdollistavat kerätyn tiedon nopean analysoinnin ja poikkeavuuksien havaitsemisen verkon liikenteessä, laitekannassa ja ohjelmistoversioissa. Tällä tavalla tietoturvauhkia voidaan havaita nopeasti ja estää niitä aiheuttamasta suurempaa haittaa energiateollisuudelle. Tutkimuksessa arvioitiin Microsoft Defender for IoT- ja Nozomi Networks -ratkaisuja energiayhtiön kybertietoturvan parantamiseksi. Tutkimuksen tavoitteena on kehittää tehokkaita, luotettavia ja kattavia menetelmiä parantamaan energiayrityksen tietoturvaa. Molemmat ohjelmistot hyödyntävät koneoppimista ja tekoälyä. Testitapaukset laadittiin NIST:n suositusten pohjalta, jotta voitaisiin paremmin ymmärtää, kuinka kyberturvallisuuden ratkaisut toimivat käytännössä ja kuinka tehokkaasti ne havaitsevat tietoturvauhkat. Testien perusteella suosittelemme energiayhtiöille Nozomi Networksin ratkaisua, sillä se on yhteensopivampi OT-arkkitehtuurin kanssa ja mahdollistaa kustannustehokkaan verkkoliikenteen monitoroinnin.

Avainsanat: Kyberturvallisuus, koneoppiminen, Microsoft Defender for IoT, Nozomi Networks, NIS2, NIST, Purdue malli, tekoäly, toiminnallinen teknologia

Tämän opinnäytetyön alkuperä on tarkastettu Turnitin Originality Check -ohjelmalla

Abstract

Author:	Jarmo Huovinen
Title:	Improving the cyber security of Operational technology network environments with Artificial Intelligence based solutions.
Number of Pages:	84 + 6 appendices
Date:	23 May 2023
Degree:	Master of Engineering
Degree Programme:	Automation Engineering
Professional Major:	Electrical Power Engineering
Supervisors:	Ville Hapuoja, Head of Network & Security Team Jukka Karppinen, Lecturer

Cybersecurity in the energy industry is an important topic, as energy companies are highly dependent on information systems and telecommunications networks to operate efficiently. The increasing amount of data and challenges related to networks, such as malware and data breaches, make maintaining cybersecurity in the energy industry increasingly difficult. Machine learning and Artificial Intelligence (AI) are playing a growing role in the development of cybersecurity in the energy industry. These technologies enable the rapid analysis of collected data and the detection of anomalies in network traffic, device inventory and software versions. This way cybersecurity threats can be quickly detected and prevented from causing greater harm to the energy industry. The aim of the study is to develop efficient, reliable**,** and comprehensive methods to improve the cybersecurity of energy companies. Microsoft Defender for IoT and Nozomi Networks solutions were selected for the study because both of them are based on machine learning and AI. These solutions enable the rapid detection of cybersecurity threats and prevent potential attacks before they cause damage. Test cases were developed based on the recommendations of the National Institute of Standards and technology (NIST) to analyze the operational benefits of improving cybersecurity in the energy industry. Test cases help to understand how solutions work in practice and how effective they are in detecting cybersecurity threats.

Keywords: Artificial Intelligence, Cyber Security, Machine learning, Microsoft Defender for IoT, Microsoft Sentinel, NIS 2, NIST, Nozomi Networks, Operational technology.

Sisällys

Lyhenteet

AI	Artificial Intelligence, Tietokone tai tietokoneohjelma, joka kykenee tekemään älykkäinä pidettäviä toimintoja.
AMA	Microsoft Azure Monitoring Agent.
AMQP	Advanced Message Queuing Protocol, Avoin standardi sovelluskerroksen protokolla.
CMC™	Nozomi Networks Central Management Console ™ (CMC), Nozomi keskitetty hallinta.
CSF	Cybersecurity Framework, Viitekehys, johon koottu kansallisista strategioista hyväksi todettuja käytäntöjä.
DCS	Distributed Control System, Hajautettu automaatiojärjestelmä.
DMZ	De-militarized Zone, Demilitarisoitu vyöhyke.
EDR	Endpoint Detection and Response -agentti. Päätelaitteiden uhkien havaitsemiseen tarkoitettu tietoturvaohjelmisto, jonka avulla voidaan tutkia epäiltyjä tietoturvaongelmia ja tarvittaessa eristää tietokone pois verkosta.
ENISA	The European Union Agency for Cybersecurity. Euroopan unionin kyberturvallisuusvirasto.
GDPR	General Data Protection Regulation , EU:n ja ETA-alueen yleinen tietosuoja-asetus.
Guardian™	Nozomi Networks toiminnanohjausjärjestelmä.
HMI	Human Machine Interface. Ihmisen ja koneen välinen rajapinta.
HTTPS	Hypertext Transfer Protocol Secure, Salattu selainprotokolla.
ICS	Industrial Control System, Teollisuuden ohjausjärjestelmä.
IEC 62443	Sarja kansainvälisiä standardeja kyberturvallisuudesta teollisuuden ohjausjärjestelmissä.

IoT	Internet of Things, Teollinen internet, esineiden ja laitteiden, palveluiden, ohjelmistojen sekä järjestelmien liittämistä yhteen Internetin avulla.
IIoT	Industry Internet of Things, Teollinen langaton internet.
IT	Information Technology, Informaatiotekniikka, tietotekniikka.
IDS	Intrusion Detection System, Hyökkäyksen ja tunkeutumisen tunnistusjärjestelmä.
IPS	Intrusion Protection System, Hyökkäyksen ja tunkeutumisen estojärjestelmä.
ISA-95	International Society of Automation – 95, Standardi, joka määrittelee rajapinnat eri teollisuuden automaatiojärjestelmien ja yrityksen hallintojärjestelmien välille.
ML	Machine Learning, tekoälyn osa-alue, jonka tarkoituksena on saada ohjelmisto toimimaan entistä paremmin pohjatiedon ja mahdollisen käyttäjän toiminnan perusteella.
M2M	Machine to Machine. Laitteiden välistä automaattista kommunikointia koneelta koneelle
MODBUS	Sarjaliikenneprotokolla, jota käytettään teollisuudessa ohjelmoitavien logiikkapiirien kanssa.
MS Sentinel	Microsoft Sentinel, Skaalautuva, pilvipohjainen SIEM-ratkaisu tietoturvauhkien tunnistamiseen, tutkintaan, reagointiin ja ennakoivaan etsintään.
NTA	Network Traffic Analysis (NTA), Verkkoliikenteen analysointityökalu
NIS2	Euroopan unionin verkko- ja tietoturvadirektiivi.
NIST	National Institute of Standards and Technology, Yhdysvaltain standardisointi- ja teknologiainstituutti.
OT	Operational technology, Toiminnallinen teknologia.
PLC	Programmable Controller, Ohjelmoitava logiikkaohjain
POC	Proof-of-Concept, Soveltuvuusselvitys, käsitteen toimivaksi todistaminen, myös konseptin validointi.

RDC	Remote Desktop Connection, Etätyöpöytäyhteys.
SaaS	Software as a Service, Ohjelmisto palveluna. SaaS on pilvipalvelumalli, jossa ohjelmistojen käyttö ja hallinta tapahtuu pilvessä.
SPAN	Switched Port Analyzer, Kytkimessä oleva erillinen portti, kutsutaan portin peilaukseksi, joka kopioi kytkimen verkkoliikennettä ja välittää sen SPAN-portista verkkoanalyysiä varten.
SCADA	Supervisory Control and Data Acquisition, Tiedonkeruu ja valvonta.
SIEM	Security Information and Event Management, keskitetty tapahtumatietojen ja lokien keräys järjestelmä.
SOC	Security Operations Center, tietoturvavalvomo.
SOAR	Security Orchestration Automated Response, ohjelmisto, joka käsittelee uhkien ja haavoittuvuuksien hallintaa, tietoturvatapauksiin vastaamista ja tietoturvatoimintojen automaatiota.
SSH	Secure Shell, Tietoliikenteeseen tarkoitettu salausprotokolla.
TAP	Test Access Point, Verkkomonitorointityökalu, jolla voidaan valvoa ja analysoida verkon läpi kulkevaa liikennettä tietyn portin kautta häiritsemättä muuta liikennettä.
TLS	Transport Layer Security, Salausprotokolla.
VPN	Virtual Private Network, Loogisesti erotettu suojattu verkko-osa.
VXLAN	Virtual eXtensible Local Area Network, Tunnelointiprotokolla, tunneloi Ethernet- (taso 2) -liikenteen IP-verkon (taso 3) kautta.

1 Johdanto

1.1 Tutkimuksen tausta

Operatiivisen tekniikan (OT) tietoturva on uusi alue useimmille organisaatioille, koska teollisuuden ohjausverkot ovat historiallisesti olleet erillään yritysten IT-verkoista. Yritysten luottaessa yhä enemmän teolliseen esineiden internet-teknologiaan (Internet of Things, IoT) ja jatkuvaan IT- ja OT-yhteyteen innovoinnin edistämisessä, kasvava kyberhyökkäysten riski voi johtaa turvallisuus- ja ympäristöhäiriöihin sekä teollisuuslaitosten seisokit taloudellisiin menetyksiin.

Nykyään organisaatiot ajattelevat perinteisten riskien havaitsemisen ja niihin reagoimisen paradigmojen lisäksi joustavuutta, mikä voi auttaa niitä kestämään tietoturvahäiriöitä ja toipumaan niistä nopeasti. Toiminnan tehokkuuden ja sähköjärjestelmien luotettavuuden parantamiseksi hyödynnetään tekoälyteknologiaa näkyvyyden ja hallinnan lisäämiseksi.

Tämän päivän muuttuvat kyberturvallisuusuhkakuvat, trendit ja taloudellinen ilmapiiri sähkömarkkinoilla sanelevat jatkuvan tarpeen parantaa sähköjärjestelmien luotettavaa toimintaa. Sähkömarkkinoiden vapauttaminen, sekä lainsäädäntö sähköalalla ovat molemmat asettaneet uusia vaatimuksia alan toimijoiden turvallisuuden parantamiseksi.

Teollisuusverkkojen ja esineiden internetin (IoT) laajamittainen käyttöönotto on tuonut mukanaan monia etuja, mutta se on myös luonut uusia haavoittuvuuksia ja turvallisuusuhkia. Kriittisen infrastruktuurin laitosten on otettava käyttöön entistä kehittyneempiä tietoturvatoimenpiteitä suojautuakseen edistyneiltä ja kohdennetuilta hyökkäyksiltä. Monet ovat investoineet peruspuolustustekniikoihin, kuten haittaohjelmien torjuntaohjelmistoihin ja palomuureihin sekä automaatiotoimittajien ja tietoturvakonsulttien suosittelemiin parhaisiin käytäntöihin. Näiden toimenpiteiden pitäisi suojata toimintaa tavallisilta hakkereilta ja riittää matalan riskin häiriösietoisille operaatioille. Mutta tämä ei riitä kriittisen infrastruktuurin laitoksille, jotka kohtaavat edistyneiden ja kohdennettujen

hyökkäysten uhkia. Näiden organisaatioiden on seurattava järjestelmiä jatkuvasti ja tutkittava epäilyttävää käyttäytymistä verkkoliikenteessään.

1.2 Haaste: IoT:n aiheuttamat turvallisvallisuusriskit

IoT edellyttää laajempaa verkkojen avaamista Internetiin, mikä luo uusia turvallisuusriskejä kuten organisaatioiden kyvykkyyden valvoa ja suojata esineiden internetin resursseja. OT- verkot ohjaavat yhteiskunnan kriittisimpiä toimintoja, joista tärkeimpiä on sähköverkot. OT-verkoissa hyödynnettäviä tekniikoita ei tyypillisesti ole suunniteltu turvallisuutta silmällä pitäen, eikä niitä voida suojata perinteisillä tietoturvasuojauksilla.

1.3 Haaste: näkyvyyden hyödyntäminen verkon hallinnassa ja suojauksessa

Älykkäiden laitteiden ja verkkojen käyttöönoton myötä IoT- ja teollisuuden ohjausjärjestelmien (Industrial Control System, ICS) ei yksinkertaisesti ole mahdollista hallita tehokkaasti, saati sitten suojata ilman näkyvyyttä hallittaviin kohteisiin. Hallinnan näkyvyys edellyttää ulkoisia avauksia, jotka altistavat hyökkäyksille, joissa samaa näkyvyyttä voidaan hyödyntää ulkoisten haavoittuvuuksien selvittämiseen. Mikäli ympäristöt ovat laajalti hajautettuja, luotettavan ja hyödyllisen tiedon oikea-aikaisesta keräämisestä tulee tärkeämpää mutta vaikeampaa.

1.4 Riskit

Järjestelmien sekä ohjelmistojen haavoittuvuudet ovat tyypillinen väylä kyberhyökkäyksille, jotka voivat vahingoittaa vakavasti teollisuuden ohjausjärjestelmiä. Vaikka seisokit perinteisessä IT-ympäristössä voivat johtaa liiketoiminnan keskeytyksiin, tietoturvarikkomuksilla OT-ympäristöissä voi olla paljon tuhoisampia vaikutuksia. Näistä esimerkkinä ovat kalliit tuotantoseisokit.

2 Tutkimustehtävä

2.1 Tutkimuskysymykset

Tutkimustehtävänä on selvittää verkkoyhtiön toimeksiantona, miten uudet tekoälyyn ja koneoppimiseen pohjautuvat tekniikat ja ratkaisut parantavat OT-verkkojen näkyvyyden integroitumista verkkoyhtiön IT-infrastruktuuriin sekä luovat kyberturvaan paremman kokonaiskuvan. Erityisesti kone- ja syväoppimisarkkitehtuureja käytetään nykyään sähköteollisuuden älykkäissä kyberturvallisuuden ratkaisuissa, joissa tekoälyn odotetaan olevan yksi keino kehittää energiateollisuuden turvallisuutta, taloudellisuutta ja luotettavuutta.

Verkkoyhtiön verkko koostuu lähtökohtaisesti erillisistä toimistoverkkoympäristöistä (IT) ja tuotantoverkkoympäristöistä (OT). Voimalaitokset ja sähköasemat käyttävät tyypillisesti useita eri laitetoimittajien reaaliaikaisia prosesseja tuottamaan tietoa järjestelmien tilasta, mikä johtaa valtavaan tietomäärään. Tietojen samanaikainen analysointi ja seuranta sekä niihin liittyvien poikkeamien havainnointi kyberhyökkäyksissä on haastava tehtävä.

Ilman ICS-näkyvyyttä on vaikea pysyä ajan tasalla, mitä tapahtuu verkon tai sähköaseman tasolla. Yksi pienikin muutos voi vaikuttaa luotettavuuteen, turvallisuuteen tai johtaa taloudellisiin menetyksiin. Vaikka nopea reagointi uhkiin ja poikkeavuuksiin on kriittistä, ongelmien havaitseminen vaatii reaaliaikaisen näkyvyyden laitteistoille ja yhteyksille.

2.2 Tavoitteet

Tavoitteena on löytää ratkaisu, joka pohjautuu tekoälyyn ja koneoppimiseen, mikä auttaa verkkoyhtiön IT- ja OT-osastoja yhteisen päämäärän saavuttamiseksi parantamaan kyberturvallisuutta, tehostamaan verkon kokonaisnäkyvyyttä ja nopeuttamaan ongelmatilanteiden selvittämistä mahdollisimman tehokkaasti.

Ratkaisun tulee pystyä käsittelemään sähköasemilta ja voimalaitoksilta kerättävää tietoa reaaliajassa, ottaen huomioon OT:n erityisvaatimukset sekä integroitua saumattomasti IT-järjestelmiin ja infrastruktuuriin. IT-tietoturva on ratkaisevan tärkeää, jotta sen tiedot pysyvät turvassa ja hallinnassa. Tämä eroaa OT-tietoturvasta perustavanlaatuisilla tavoilla, eikä vain siksi, että IT- ja OT-järjestelmät vaativat erilaista turvallisuuden valvontaa, vaan niiden omaisuudella on eri merkitykset ja vaikutukset. Lisäksi niillä on erilaiset tavoitteet omaisuuden turvaamiseen ja sen merkitykseen liittyen.

Tämän vuoksi on tärkeää, että ratkaisu ymmärtää ja ottaa huomioon nämä erot IT- ja OT-tietoturvan välillä, tarjoten kattavan ja tehokkaan suojauksen molemmille osa-alueille. Ratkaisun tulee myös helpottaa IT:n ja OT:n välistä yhteistyötä ja tiedonvaihtoa, jotta verkkoyhtiö voi reagoida nopeasti ja tehokkaasti mahdollisiin turvallisuusuhkiin tai ongelmatilanteisiin.

Yhteistyö IT- ja OT-osastojen välillä on siis erityisen tärkeää, koska se auttaa ymmärtämään ja käsittelemään molempien osa-alueiden erityispiirteitä ja vaatimuksia. Se mahdollistaa myös yhteisten toimintamallien ja parhaiden käytäntöjen kehittämisen, mikä puolestaan lisää koko organisaation kyberturvallisuutta ja tehokkuutta. Kun otetaan huomioon, että tietotekniikka on pääasiassa digitaalista ja OT fyysistä, nämä erot eivät ole yllättäviä.

2.3 Tutkimusmenetelmät

Tutkimus vertailee kahta eri toimittajan arkkitehtuuria, joilla pyritään löytämään kustannustehokas, skaalautuva, turvallinen ja luotettava ratkaisu. Testien ja asiantuntijahaastattelujen avulla etsitään ratkaisua, joka vastaa verkkoyhtiön vaatimuksia (taulukko 6) ja on tarvittaessa yhteensopiva Microsoft Sentinel SIEM-ratkaisun kanssa. Microsoft Sentinel on pilvipohjainen Security Information Event Management (SIEM) ja Security Orchestration Automated Response (SOAR) -toiminnot sisältävä ratkaisu. SOAR:in avulla voidaan automatisoida toistuvat ja ennustettavat toiminnot. Sentinelin avulla voidaan nopeasti tunnistaa ja reagoida tietoturvauhkiin, vähentäen manuaalista työtä ja parantaen

reagointiaikaa. Tutkimus auttaa verkkoyhtiötä parantamaan kyberturvallisuuttaan ja saamaan paremman näkyvyyden järjestelmiinsä.

Tavoitteena on löytää integroitava ratkaisu, joka ei vaikuta järjestelmien suorituskykyyn, samalla kun se parantaa verkkoyhtiön reagointikykyä mahdollisiin tietoturvauhkiin.

2.4 Koneoppiminen

Usein kysytään, mitä tekoäly on ja mitä se voi tehdä. Pohjimmiltaan katsomme tekoälyä tietojenkäsittelytieteen osana, joka yrittää saada koneet toimimaan ihmisten tavoin. Koneoppiminen voi kuulostaa petollisen yksinkertaiselta, jolloin on helppo olettaa, että tarvitsee vain kerätä tiedot ja suorittaa ne joidenkin algoritmien läpi. Kun tiedot ovat kerätty, todellisuus on hyvin erilainen: tiedot pitää voida vielä yhdistää algoritmien avulla. Algoritmien tavoitteena on luoda järjestelmiä, jotka pystyvät käyttämään tietoja ja oppimaan niistä ilman erillistä ohjelmointia.

Koneoppiminen voidaan tuoda yleensä yritykseen kahdella tavalla. Ensimmäisessä yksi tai kaksi työntekijää alkaa soveltaa koneoppimista saadakseen käsityksen tiedoista, joihin heillä on jo pääsy. Tämä vaatii tietyn määrän tietotieteen asiantuntemusta ja alan tietämystä – taitoja, joista on pulaa. Toisessa, tehokkaammassa vaihtoehdossa, ostetaan koneoppimista käyttävä ratkaisu, kuten tietoturvaohjelmisto tai sovellusten suorituskyvyn hallintaratkaisu. Tämä on ylivoimaisesti helpoin tapa alkaa oivaltaa joitakin koneoppimisen etuja, mutta haittapuolena on, että yritys on riippuvainen toimittajasta eikä kehitä omia koneoppimiskykyjään.

Koneoppiminen on siis älykkäiden tietokonejärjestelmien kehittämiseen käytetty menetelmä, joka hyödyntää algoritmeja datan mallien tunnistamiseen. Nämä mallit mahdollistavat ennusteiden tekemisen ja auttavat järjestelmiä suorittamaan tehtäviä ilman erillistä ohjelmointia. Koneoppiminen on keskeinen osa-alue tekoälyssä.

Teoriassa yleisen tekoälyn saavuttanut tietokonejärjestelmä pystyisi ratkaisemaan syvästi monimutkaisia ongelmia, soveltamaan harkintaa epävarmoissa tilanteissa ja sisällyttämään aiemman tiedon nykyiseen päättelyynsä. [1.]

2.5 Rajaukset

Tutkimuksessa käytetään (kuva 1) NIST-viitekehysmallia (National Institute of Standards and Technology), josta tutkimukseen rajataan tunnista ja havaitse -toiminteet (Identify and Detect) hyödyntäen testiin valittuja tekoälyyn pohjautuvia ohjelmistoja, jotka on suunniteltu tähän käyttöön ja tukevat ensisijaisesti tutkimusta. Molemmat ratkaisut tukevat myös suojaus- (Protect) ja palautustoiminteita (Recover), joita emme tutkimukseen ottaneet.

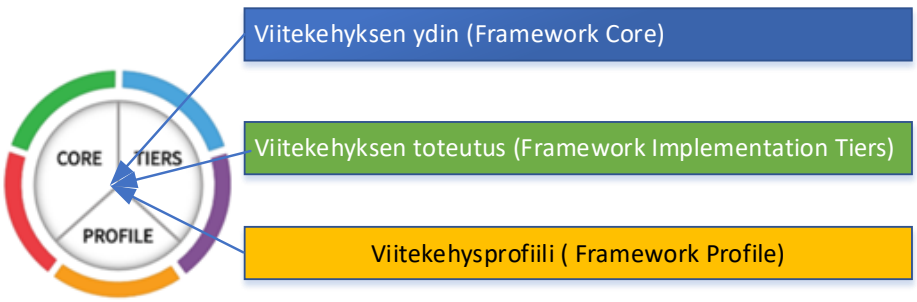
Kuva 1. NIST:n kyberturvallisuusviitekehys [2.]

3 NIST:n viitekehyksen perusteet

OT-kyberturvallisuudelle on tarjolla lukuisia puolustukseen liittyviä ohjeistuksia, joista Yhdysvaltain kansallinen standardi- ja tiedeinstituutti NIST on ottanut johtoaseman kriittisen infrastruktuurin tarjoajille. NIST on virasto, joka toimii puolueettomana tieteellisen tiedon ja käytäntöjen lähteenä mukaan lukien kyberturvallisuuskäytännöt. Virasto edistää ja ylläpitää mittausstandardeja sekä ohjeita organisaatioiden riskien arvioimiseksi. Seurauksena voimakkaasti lisääntyneisiin tietoturvauhkiin, Yhdysvaltojen presidentti

Barack Obama antoi helmikuussa 2013 toimeenpanevan päätöksen Executive Order 13636:n, jonka otsikkona oli "Kriittisen infrastruktuurin kyberturvallisuuden parantaminen." Päätös kehotti kehittämään kyberturvallisuuskehyksen, jossa hahmotellaan kriittisen infrastruktuurin eri alojen parhaat käytännöt kyberturvallisuusriskien tehokkaalle hallitsemiselle. Tuloksena NIST julkaisi helmikuussa 2014 (CSF) kriittisen infrastruktuurin kyberturvallisuuden parantamiseen tarkoitetun viitekehyksen ensimmäisen version 1.0. Kyberturvallisuuskehyksen kehitys on ollut alusta alkaen yhteistyötä, johon osallistuivat eri sidosryhmät hallituksesta, teollisuudesta ja korkeakouluista.

Kehys sai vuonna 2016 päivityksen, joka sisälsi informatiivisten viitteiden päivittämisen, ohjeiden selventämisen toteutustasoille ja kyberuhkatiedustelun sijoittamisen ydinkehykseen. Vuoden 2018 alussa kehys päivitettiin versioon 1.1, joka sisälsi päivityksiä todentamiseen ja kyberturvallisuusriskin itsearviointiin, kyberturvallisuuden hallintaan toimitusketjussa sekä haavoittuvuuksien paljastamiseen. Versio 1.1 on edelleen yhteensopiva version 1.0 kanssa. Kehyksessä puututaan kyberturvallisuusriskeihin asettamatta uusia sääntelyvaatimuksia valtion tai yksityisen sektorin organisaatioille. Kehys on kirjoitettu hyvin ymmärrettävässä muodossa ja tarjoaa yhteisen kielen, joka on tunnettu kriittisen infrastruktuurin kyberturvallisuuden parantamisessa ja riskienhallinnassa. Viitekehys tarjoaa selkeät ohjeet yrityksen organisaatiolle, ollen pikemminkin opas riskien arvioimiseksi ja turvallisuuskysymysten ratkaisemiseksi. Kehysprofiilit ovat toimintojen, luokkien ja alaluokkien linjauksia liiketoiminnan vaatimusten sekä riskin sietokyvyn kanssa. Viitekehys muodostuu kolmesta osa-alueesta, jotka määrittelevät toiminnot, joille kuvaavat vaatimukset pannaan täytäntöön (Kuva 2).



Kuva 2. NIST:n viitekehyksen kolme osa-aluetta. [2.]

Toiminnot antavat organisaatioille mekanismin tarkastella ja ymmärtää organisaatioiden lähestymistapaa kyberturvallisuusriskien hallintaan ja auttaa heitä priorisoimaan ja saavuttamaan kyberturvallisuustavoitteet.

NIST-kyberturvallisuuskehyksen ensimmäinen osa-alue on tietoturvaohjeet (Framework Core). Tietoturvaohjeet sisältävät enimmäkseen ohjaustietoja ja kyberturvallisuustoimia eli se esittelee alan standardit tavalla, joka auttaa organisaatioita puuttumaan kyberriskeihin käyttämällä helposti ymmärrettävää yhteistä kieltä. [2.]

NIST:n viitekehyksen toinen osa-alue on tietoturvaperiaatteet (Framework Implementation Tiers), jonka kehyskomponentti toimii organisaation tapana arvioida nykyinen kyberturvallisuustaso. Yksinkertaisesti sanottuna NIST-kyberturvallisuuskehyksen käyttöönottotasot auttavat organisaatioita arvioimaan, mikä standarditaso on paras heidän kyberturvallisuusohjelmalleen.

Tämä auttaa organisaatioita tarjoamalla kontekstin, miten organisaatio itse ja kumppanit suhtautuvat kyberturvallisuusriskien hallintaan. Tasot auttavat organisaatioita arvioimaan kyberturvallisuuden kypsyyttä ja ohjaamaan resurssejaan riskinottohalun, prioriteettien ja budjetin mukaan. Ne edistävät selkeää kommunikointia ja kehityksen seurantaa. [2.]

NIST-kyberturvallisuuskehyksen kolmannen osa-alueen kehysprofiilin (Framework Profile) avulla organisaatio voi tehdä suunnitelman organisaation tavoitteiden mukaisten kyberriskien minimoimiseksi ja keskittyä useampaan kuin yhteen profiiliin havaitakseen heikot kohdat sekä mahdollisuudet parantaa kyberturvallisuustoimintaa ja saavutuksia. [2.]

NIST-kyberturvallisuusviitekehyksen versio 1.1 (CSF) koostuu kuvan 1 mukaisesti viidestä keskeisimmästä toiminnosta: Havainnointi, Suojaaminen, Tunnistaminen, Reagointi ja Palautuminen. Kaikki nämä ovat yhdessä tärkeitä ja tarjoavat kuvan kyberturvallisuusriskien hallinnasta. Kuitenkin monet näistä toiminnoista ovat ei-teknisiä, joihin liittyvät henkilöstön koulutus ja asianmukaiset prosessit

Taulukko 1. NIST-kyberturvallisuuskehyksen viisi perustoimintoa [2.]

Tunnista (Identify) Mikä on yritykselle tärkeää ja mitkä ovat riskit
Suojaudu (Protect) Suojatoimet tiedon oikeallisuuden, eheyden ja saatavuuden varmistamiseksi (CIA)
Havaitse (Detect*)* Tietoturvatapahtuman havainnointi, poikkeamat, tietoturvarikkomukset
Reagoi (Respond) Asianmukaiset toimet havaittuun kyberturvallisuuspoikkeamaan
Palauta (Recover) Tukee palauttamista normaaliin toimintaan kyberturvallisuus tapahtuman vaikutuksesta. Esimerkiksi palautus suunnitelmat, parannukset ja viestintä

Uutena teknisenä tavoitteena on mukauttaa nykyiset kyberturvallisuuden parhaiden käytäntöjen menetelmät sekä työkalut siten, että niitä voitaisiin soveltaa myös sähköalalla. NIST pystyy vastaamaan näihin tavoitteisiin, joissa OT-verkkojen ainutlaatuiset vaatimukset pystytään tunnistamaan ja jotka edellyttävät uusia menetelmiä. [3.]

Tutkimuksessa perehdyttiin nimenomaan Tunnista-toimintoon (Identify) ja Havaitse-toimintoon (Detect), joista Havainnointi on NIST:n ensimmäinen osuus. Havainnointi on myös kyberturvallisuuskehyksen perusta. Tämä auttaa ymmärtämään kyberturvallisuusriskien hallintaa ja määrittele sopivat toiminnot kyberturvallisuuspoikkeaman tunnistamiseen sekä oikea-aikaiseen löytämiseen.

Tunnista-toiminto edellyttää organisaation ja toimintaympäristön ymmärtämistä, jotta kyberturvallisuus voidaan kohdentaa ja priorisoida nykyisten riskienhallinnan ja tavoitteiden mukaisesti. Tunnistus sisältää omaisuudenhallinnan ja riskien arvioinnin, kun taas havaitse-toiminto sisältää jatkuvan seurannan ja tapahtumien käsityksen muiden toimintojen ohella. Aina kun verkossa havaitaan epänormaalia toimintaa, järjestelmien tulisi varoittaa ylläpitohenkilöstöä. Kaksi yleistä tapaa havaita ja torjua rikkomuksia ovat tunkeutumisen havaitsemisjärjestelmät (IDS) ja tapahtumien seuranta. Tapahtumien

seuranta on toisaalta tapa havaita mahdolliset rikkomukset tai epäilyttävä toiminta. Se sisältää lokien keräämisen, hallinnan ja analyysin. Tämä antaa mahdollisuuden arvioida manuaalisesti tapahtuman alkuperää koskevia tietoja, tunnistaa suuntaukset ja tehdä päätöksiä mahdollisten ongelmien välttämiseksi. [2.]

Suojaus-toiminnon (Protect) tavoitteena on kehittää ja toteuttaa asianmukaiset suojaustoimet kriittisten palvelujen toiminnan varmistamiseksi. Suojaus-toiminto rajoittaa tai hillitsee mahdollisen kyberturvallisuustapahtuman vaikutuksia sekä tukee kykyä estää hyökkäykset mahdollisuuksien mukaan. Kehyksen suojaus -toiminto toimii oppaana ja sanelee tarvittavat tulokset tavoitteen saavuttamiseksi. [3.]

Paras tapa pysäyttää verkkohyökkäys on estää sitä tapahtumasta, mutta nykypäivän hakkerit voivat usein vesittää tämän strategian. Tämän vuoksi ennakoiva lähestymistapa tietoturvaan on välttämätöntä ja määrittää toimintatavat reagoida uhkaan, kun se havaitaan sekä kuinka toipua tapahtuman jälkeen.

Reagointi-toiminto (Respond) määrittää asianmukaiset toimet havaittuun kyberturvallisuuspoikkeamaan. Tämä NIST-kyberturvallisuuskehyksen toiminto auttaa ymmärtämään ennakoivia toimia, mikäli uhka ilmenee ennen kuin se tapahtuu. Tähän sisältyy mahdollisia parannuksia tulevaisuuden haavoittuvuuksien ehkäisemiseksi, reagointisuunnittelua sekä sisäistä että ulkoista viestintää.

Liiketoiminnan jatkuvuudella ja sen parantamisella on suuri rooli Palauttaminen-toiminnossa (Recover). Häiriötilanteen aikana saadut kokemukset tunnistetaan ja hyödynnetään palautussuunnitelmien päivittämiseksi ja parantamiseksi, jotta poikkeamien kohteena olevat järjestelmät ja omaisuus saadaan palautettua normaaliin toimintaan.

Historiallisten tapahtumalokien tiedot voivat antaa lisätietoja ja todisteita uhkan lähteestä ja paljastaa häiriötilanteen koko kuvan. Verkkohyökkäyksen tai rikkomuksen sattuessa organisaatiot tarvitsevat selkeän toimintasuunnitelman vaikutusten rajoittamiseksi. Tunnistamisen ja vasteen välinen aika on kriittinen, joten hyvin toteutetut reagointisuunnitelmat minimoivat nopeuden tuotannon palautumisen. [2.]

Kyberturvallisuuden perinteiset toiminnot, ennaltaehkäisy ja havainnointi, eivät yksin riitä digitaalisessa maailmassa. Uusien uhkien ennustaminen ja rutiinien automatisointi auttavat hallitsemaan kasvavia riskejä ja vapauttamaan asiantuntijoiden aikaa monimutkaisempiin tehtäviin. Pilvipohjaisten järjestelmien yleistyessä pelkät ennaltaehkäisyn ja havainnoinnin perusteet, kuten virustorjunta, heikentävät palomuurien tehokkuutta. Kehykseen mukautuminen edellyttää kaikkien kyberturvallisuusominaisuuksien, projektien, prosessien ja päivittäisten toimintojen luettelointia ja niiden liittämistä yhteen näistä viidestä toimintotarpeesta. [3.]

4 Operatiivinen tekniikka

Operatiivisella tekniikalla (OT) tarkoitetaan laitteistoa ja ohjelmistoja, joita käytetään yrityksen tai organisaation sisällä fyysisten laitteiden, prosessien sekä tapahtumien ohjaamiseen ja säätämiseen. Operatiivinen tekniikka on yleisimmin käytössä teollisissa ympäristöissä. Usein teollisen ympäristön laitteisiin ei saa tai edes voida tehdä ohjelmistopäivityksiä eikä muutoksia vuosikausiin. Laitteet ovat pitkälle erikoistuneita ja toimivat harvoin standardoiduissa käyttöjärjestelmissä, kuten iOS tai Windows, jotka vaativat yleensä toimiakseen mukautettuja ohjelmistoja. Vaikka operatiivinen tekniikka ja tietotekniikat ovat yhä enemmän yhteydessä toisiinsa, on niillä olemassa useita merkittäviä eroja, joista sekä tietotekniikan että OT-henkilöstön on hyvä olla tietoisia

4.1 Operatiivisen tekniikan erot tietotekniikkaan

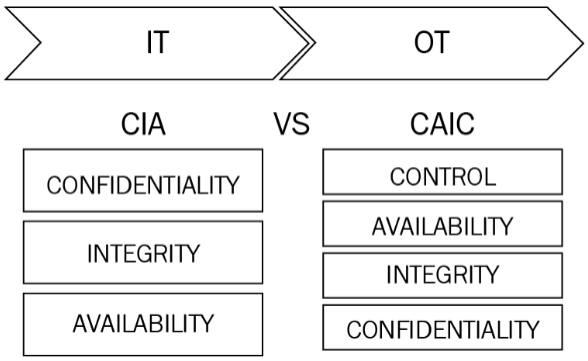
Tietotekniikka (IT) käsittää laajasti kaiken tietoteknologiaan liittyvän, kuten laitteistot, ohjelmistot, verkot ja tietojärjestelmät. IT on olennainen osa organisaatioiden toimintaa ja tarjoaa työkalut tiedon käsittelyyn, kommunikaatioon ja tietojen hallintaan. IT-infrastruktuuri muodostaa usein organisaatioiden perustan, ja sen avulla voidaan toteuttaa liiketoimintaprosesseja tehokkaasti. IT-järjestelmät tarvitsevat jatkuvaa ylläpitoa, päivityksiä ja tietoturvaa varmistaakseen toimintansa ja suojatakseen arkaluontoisia tietoja.

Pääsy tietotekniikkaohjelmiin ja niihin liitettyihin laitteisiin on tyypillisesti vähemmän rajoitettua kuin OT-laitteisiin.

OT- ja IT-tekniikat toimivat eri ympäristöissä ja palvelevat eri tarkoituksia. OT sisältää pääasiassa teollisuusympäristöissä täysin erilaisia komponentteja, jotka usein ovat päätelaitteita ilman näyttöjä tai muita hallintalaitteita. Esimerkiksi PLC:t kommunikoivat teollisuusprotokollien, kuten Modbus tai Profinetin avulla. Niiltä puuttuvat usein myös palomuurit ja virustorjunta ja ne ovat ohjelmoituja eri tavalla kuin tietokoneet. Suurin ero OT- ja IT-laitteiden välillä on, että OT-laitteet hallitsevat fyysistä maailmaa, kun IT-järjestelmät taas hallitsevat tietoja.

IT-tietoturvan kannalta on ratkaisevan tärkeää, että jokaisessa organisaatiossa tiedot voidaan pitää turvassa ja hallinnassa. Kuvassa 3 on esitetty, miten OT:ssa laitteiden ja prosessien turvallisuus ja saatavuus hallitsevat. Toisin kuin tietotekniikan tietoturva, OT-suojaus keskittyy fyysisten prosessien ja omaisuuden suojaamiseen. OT:ssa tärkeintä on aina turvallisuus ja saatavuus, joka tarkoittaa sitä, että tuotantolaitosten on oltava kestäviä ja jatkuvasti toiminnassa.

Suurin ero IT-turvallisuuteen verrattuna on kuitenkin se, että useimmat tietoturvapäälliköt ja SOC-tiimit (Security Operations Center) eivät tällä hetkellä näe OT-riskiään juuri lainkaan. Heillä ei ole useita hallinta- ja telemetriatasoja, kuten IT- ympäristöissä, jolloin OT-riski muuttuu suoraan liiketoimintariskiksi.



Kuva 3. CIA ja CAIC malli [5.]

IT-kyberturvallisuuden standardi tunnetaan luottamuksellisuuden (Confidentiality), eheyden (Integrity) ja saatavuuden (Availability) CIA-kolmiona.

OT-kyberturvallisuuden standardi vaatii kuitenkin laajemman ja uudelleen järjestetyn prioriteettijärjestyksen eli valvonta (Control), saatavuus, eheys ja luottamuksellisuus eli CAIC. [5.] Omaisuuden hallinnan ylläpitäminen ja toiminnan turvaamisen varmistaminen ovat OT-kyberturvallisuuden ensisijainen tavoite.

OT-kyberturvallisuudelle on tiedon saatavuus toiseksi tärkein tavoite. OT on läsnä kaikissa elintärkeissä infrastruktuureissa, joissa tuotannon on yleensä oltava käytettävissä 24/7/365. Tiedon eheys on kolmanneksi tärkein tavoite etenkin siinä määrin, kun se varmistaa turvallisuuden ja saatavuuden. OT-tietojen luottamuksellisuus on paljon vähemmän huolestuttavaa kuin IT-tietojen luottamuksellisuus. [11.]

OT-järjestelmissä on tärkeää varmistaa, että fyysiset prosessit sujuvat turvallisesti ja luotettavasti, sillä häiriöt voivat aiheuttaa merkittäviä taloudellisia menetyksiä tai vaarantaa ihmishenkiä. Tämän vuoksi OT-järjestelmien suunnittelussa korostuu luotettavuus, pitkäikäisyys ja turvallisuus. Järjestelmissä käytetään usein vanhempaa teknologiaa kuin IT-järjestelmissä, sillä OT-järjestelmien toiminnassa korostuu stabiilius ja pitkäikäisyys. OT-laitteiden suunnittelussa pyritään varmistamaan niiden toimintavarmuus myös pitkän käyttöiän aikana, joten uusimmat teknologiat eivät välttämättä ole tarpeen. [5.]

OT-järjestelmien turvallisuus on erityisen tärkeää, sillä niiden toimintahäiriöt voivat aiheuttaa suuria riskejä fyysiselle turvallisuudelle. Tämän vuoksi OT-järjestelmien suojaus ja valvonta ovat erittäin tärkeitä. OT-järjestelmien verkkoyhteyksiä rajoitetaan ja valvotaan tarkasti, ja käyttäjien käyttöoikeuksia rajoitetaan vain tarvittaviin toimintoihin. Lisäksi OT-järjestelmissä käytetään usein erikoistuneita turvallisuusratkaisuja, jotka on suunniteltu erityisesti OT-järjestelmien suojaamiseen.

Vaikka OT-järjestelmissä käytetään vanhempaa teknologiaa kuin IT-järjestelmissä, niiden suojaaminen kyberuhkilta on yhä tärkeämpää. Siksi OT-järjestelmien kyberturvallisuuteen on kiinnitettävä huomiota ja käytettävissä olevia keinoja on hyödynnettävä

niiden suojaamiseksi. Tärkeitä toimenpiteitä ovat esimerkiksi järjestelmien säännöllinen päivittäminen ja haavoittuvuuksien tarkistaminen sekä käyttäjien tietoturvatietoisuuden lisääminen. [5.]

4.2 Tietoturvakorjaukset

IT-komponentit kehittyvät nopeasti ja niiden käyttöikä on suhteellisen lyhyt, jolloin verkko voi näyttää täysin erilaiselta vain muutaman vuoden välein. Tietoturvakorjaus ei toimi samalla tavalla OT:ssa, koska komponenttien korjaaminen edellyttää usein laitteiden täydellisen huoltokatkon. Huoltokatkojen vuoksi OT-komponentteja päivitetään harvoin. [5.]

4.3 Laitekanta

OT-ympäristöille on tyypillistä, ettei laitekantaa valvota eikä tiedetä automaatioympäristön komponenttien ajankohtaista tilatietoa. Koska OT-ympäristöä ei voida suoraan kontrolloida, jää tärkeimmäksi lähtökohdaksi ymmärtää ja tunnistaa tarkalleen, millä komponenteilla ympäristö on rakennettu. Tämän lisäksi pitää selvittää eri komponenttien kriittisyysasteet eli luokitella, mitkä ovat tärkeitä ja mitkä vähemmän tärkeitä. Tämä antaa lähtökohdan hyökkäyksiltä suojautumiseen, sillä komponentteja on paljon ja priorisointia vaaditaan. Yksinkertaisin ja työläin tapa on kartoittaa koko ympäristö käsin. Jos ympäristön rakentanut taho ja ylläpitäjät ovat dokumentoineet tekemisensä, helpottuu työ huomattavasti. Valitettavan harvoin OT-ympäristön dokumentointi on toteutettu hyvin. [11.]

Jos laitekanta on tiedossa, luokitellaan laitteet eri kriittisyysluokkiin ja niiden mahdollisia haavoittuvuuksia pyritään löytämään sekä mahdollisimman usein myös tarkistamaan. Tätä on kuitenkin vaarallista tehdä perinteisillä IT-työkaluilla, koska vanhemmat OT-laitteet ovat hyvin herkkiä aktiiviselle skannaukselle. Pahimmillaan tällainen tarkistus häiritsee tehtaan toimintaa ja jopa katkaisee tuotannon.

OT-ympäristöön on vaikeaa lisätä IT-ympäristöistä tuttuja tietoturvakomponentteja, kuten Antivirus- tai EDR-agentteja, jolloin komponenttien tilan valvominen on hankalaa. Esimerkiksi OT-komponentteihin on olemassa suuri määrä haittaohjelmistoja, jotka aiheuttavat selkeitä virhetoimintoja laitteiden väliseen kommunikaatioon, jota harvoin valvotaan. Monessa ympäristössä on havaittu, että OT-komponentit yrittävät ottaa yhteyksiä huomaamatta ulkomaailmaan tai pilveen. Tällöin IT-valvonta ei siihen reagoi, vaikka IT-palomuuri havaitsee yrityksen, koska sillä on harvoin oikea tilannekuva OT-ympäristön kommunikoinnista.

4.4 Piilevä uhka

OT-ympäristöihin kohdistuvat kyberhyökkäykset ovat kasvava uhka. Hankalimmasta ja tuhoisimmasta päästä on hiljainen ja pidempiaikainen tunkeutuminen yrityksen tietoverkkoon APT-hyökkäyksellä (Advanced Persistent Threat). Tällaiset uhkat kohdentuvat useimmiten valtioihin ja suuryrityksiin, joista viime aikoina saatu esimerkkejä Venäjän hyökkäyssodassa Ukrainaan. APT-hyökkäyksillä pyritään usein vakoilemaan kohteen järjestelmiä ja varastamaan arkaluonteista tietoa. Tällaiset hyökkäykset voivat olla erittäin hienovaraisia ja kestää useita kuukausia tai jopa vuosia, ennen kuin ne havaitaan. Tämän vuoksi niitä on vaikea torjua ja niiden vaikutukset voivat olla hyvin laajat. OT-ympäristöjen turvallisuus on monimutkainen kokonaisuus, joka edellyttää yhteistyötä eri alojen asiantuntijoiden välillä. Turvallisuus liittyy läheisesti myös fyysiseen turvallisuuteen, ja sen takaamiseksi on tarpeen käyttää monipuolisia turvallisuusratkaisuja ja kehittää tietoturvakulttuuria organisaatiossa.

5 NIS-direktiivi

Erittäin tärkeitä omaisuuseriä (Assets) tai järjestelmiä kutsutaan kriittisiksi infrastruktuureiksi. Mahdollisella häiriöllä tai epäonnistumisella tarjotuissa palveluissa on huomattavia seurauksia niin kansalaisten turvallisuudelle kuin peruselämisen tarpeiden kattamiseen. Kriittiset infrastruktuurit ovat etulinjassa miljoonien ihmisten terveyden ja turvalli-

suuden takaamisessa. Siksi näiden organisaatioiden olisi toteutettava lisätoimenpiteitä turvallisuutensa ja yksityisyytensä suojelemiseksi.

Elokuussa 2016 astui voimaan ensimmäinen EU:n laajuinen kyberturvallisuuslainsäädäntö eli verkko- ja tietojärjestelmien turvallisuutta koskeva direktiivi, joka tunnetaan nimellä NIS-direktiivi. Direktiivin tavoitteena on parantaa kyberturvallisuutta kaikkialla EU:ssa ehdottamalla turvatoimia kriittisten infrastruktuurien (tärkeiden palvelujen operaattorit ja digitaalisten palvelujen tarjoajat) kyberturvallisuustason nostamiseksi ja varmistamalla myös jäsenvaltioiden valmiudet vaatimalla niiltä asianmukaista varustusta.

Kyberturvallisuuden uhkien maisema on tähän päivään mennessä muuttunut dramaattisesti NIS1-direktiivin julkaisemisesta. Digitaalisesta muutoksesta on tullut maailmanlaajuisesti tunnettu käsite ja monet organisaatiot ottavat käyttöön uusia strategioita ja malleja. EU:n kriittisiä infrastruktuureja vastaan tehdään usein erilaisia ja monimutkaisia hyökkäyksiä ja tietoverkkorikollisuudella on yhä useammin taloudelliset tarkoitusperät. Lisäksi puolustuskehä on laajentunut ja kriittisten infrastruktuurien on kohdattava enemmän kyberuhkia ja otettava käyttöön uusia ratkaisuja sekä teknisiä toimenpiteitä häiriöiden välttämiseksi. [6.]

5.1 Päivitetty direktiivi NIS2

Kaikkiin digitalisaation aiheuttamiin uusiin uhkiin puuttumiseksi ja turvallisuusvaatimusten vahvistamiseksi komissio on ehdottanut verkko- ja tietoturvadirektiivin uudistamista. Toisin kuin edeltäjänsä (NIS1), NIS2-direktiivi laajentaa soveltamisalaansa sisällyttämällä siihen uusia aloja (keskikokoisia ja suuria yrityksiä) niiden taloudellisen ja yhteiskunnallisen merkityksen perusteella. NIS2-direktiivissä ehdotetaan eron poistamista olennaisten palvelujen tarjoajien ja tärkeiden palvelujen tarjoajien välillä. Kriittisten infrastruktuurien kokonaisuuksien on siten jatkuvasti panostettava enemmän uhkien havaitsemiseen, ehkäisyyn ja lieventämiseen keskittyen turvavalvonnan ja -ominaisuuksien tehokkuuteen – ei vain niiden olemassaolon todentamiseen. [6.]

NIS2 perustuu alkuperäisen NIS-direktiivin vaatimuksiin ja sen tavoitteena on edelleen suojella EU:n kriittistä infrastruktuuria ja organisaatioita kyberuhkilta ja saavuttaa korkea yhtenäinen turvallisuustaso kaikkialla EU:ssa. Tämän tavoitteen saavuttamiseksi NIS2 vaatii jäsenvaltioita toteuttamaan useita lisätoimenpiteitä mukaan lukien alla mainitut tavoitteet:

- Laatia häiriötilanteiden torjuntasuunnitelma, joka on koordinoitu muiden jäsenmaiden suunnitelmien kanssa
- Perustetaan kansallinen kyberturvan hätäryhmä
- Julkisen ja yksityisen sektorin yhteistyön vahvistaminen
- Tiedonvaihdon parantaminen jäsenvaltioiden välillä

Yhteistyö jäsenvaltioiden välillä auttaa niitä parantamaan puolustustaan kyberhyökkäyksiä vastaan sekä tarjoaa tukea ja ohjausta yrityksille ja yksityishenkilöille Täten EU varmistaa, että sen kansalaisia suojataan kasvavilta verkkouhkariskeiltä. [7, 8, 9.]

Kansainvälisten järjestöjen on myös varmistettava, että NIS-lainkäyttöalueella olevat laitokset ja toiminnot ovat verkko- ja tietoturvadirektiivin mukaisia. Noudattaminen on pakollista ja sen laiminlyönnistä voi seurata merkittäviä sakkoja, jotka voivat olla 2 prosenttia yrityksen liikevaihdosta tai maksimissaan jopa 10 miljoonaa euroa. Vuodesta 2016 lähtien Euroopan unioni on asettanut tehostettuja tietoturvastandardeja ydinyrityksille verkko- ja tietoturvadirektiivin (NIS) kautta. Tätä tekstiä tarkistettiin äskettäin ja Euroopan komissio, parlamentti ja neuvosto ilmoittivat 12. toukokuuta 2022 uudesta NIS2-direktiivistä.

Euroopan komissio odottaa organisaatioiden tieto- ja viestintätekniikan tietoturvamenojen kasvavan enintään 22 prosenttia ensimmäisten vuosien aikana NIS2:n käyttöönoton jälkeen ja 12 prosentin lisäys on arvioitu organisaatioille, jotka jo kuuluvat nykyisen verkko- ja tietoturvadirektiivin soveltamisalaan. [10, 18.]

Raportointitoimenpiteitä on myös virtaviivaistettu ja laajennettu sisältämään ilmoituksen kaikista merkittävistä uhkista, jotka voivat johtaa merkittävään vaaratilanteeseen. Raportit on tehtävä toimivaltaisille viranomaisille (kunkin jäsenvaltion nimeämiä) tai CSIRT:lle (Computer Security Incident Response Team). Tapahtumat, jotka voivat vaikuttaa haitallisesti palveluihin, on ilmoitettava palvelun asiakkaille. Raportointi on tehtävä ilman tarpeetonta viivytystä, mikä yleensä tarkoittaa alustavaa ilmoitusta viranomaisille 24 tunnin sisällä tapahtumasta, mutta se voidaan tietyissä olosuhteissa pidentää 72 tuntiin. [10,18.]

Tärkeisiin yksiköihin, mukaan lukien digitaalisten palvelujen tarjoajat, tiettyjen kriittisten tuotteiden valmistajat sekä posti- ja kuriiripalvelut, sovelletaan reaktiivista valvontajärjestelmää, jossa valvonta käynnistyy tapahtuman viitteistä. Tärkeät kokonaisuudet koskevat enimmäkseen keskisuuria ja suuria yksiköitä, joissa palveluiden mahdollisella häiriöllä olisi vakavia yhteiskunnallisia tai taloudellisia seurauksia.

Euroopan parlamentti ja Eurooppa-neuvosto ovat hyväksyneet NIS2:n tekstin 16.1.2023 ja hyväksymisen jälkeen jäsenvaltioilla on 21 kuukautta aikaa saattaa NIS 2 osaksi kansallista lainsäädäntöä. [7,8,9.]

Taulukko 2. NIS2 lisäykset

NIS 1	**NIS2 lisäykset**
Energia	Yleisten sähköisten viestintäverkkojen tai -palvelujen tarjoajat
Kuljetus	Jätevesi ja jätehuolto
Terveys	Avaruus ja ilmailu
Vesi	Posti- ja kuriiripalvelut
Digitaalinen infrastruktuuri	Julkishallinto
	Digitaaliset palvelut, kuten sosiaalisen verkostoitumisen alustat ja datakeskuspalvelut.
	Tiettyjen kriittisten tuotteiden valmistus (esimerkiksi lääkkeet, lääkinnälliset laitteet ja kemikaalit)

5.2 NIS2-direktiivin mukainen toiminta (organisaatiossa)

NIS2-direktiivi saa organisaation omaksumaan riskiperusteisen lähestymistavan kyberturvallisuuteen. Sellaisenaan organisaatiolla on oltava tehokas riskienhallintaprosessi, määritelty hallintorakenne ja määritetyt roolit ja vastuut kyberkestävyyteen liittyen. Jotta yrityksistä tulisi kybertietoisia, jatkuvasti muuttuvaan uhkamaisemaan sopeutuvia organisaatioita, on kehitetty arviointikehys määrittelemään hyviä käytäntöjä. Lisäksi viittaukset alan standardeihin on annettu jokaiselle verkko- ja tietoturvadirektiivissä määritellylle tavoitteelle. Velvoite parempaan tietoturvaan on olennaista tietoon perustuvien päätösten tekemisessä, joissa tiedonkeruun ja analyysin merkitys kasvaa. Tämän vuoksi on tarpeellista arvioida kyberturvallisuuden parhaat käytännöt uudelleen myös OT:n suojaamiseksi. Tietoturva on periaatteeseen perustuva lähestymistapa, jolla organisaatio osoittaa olevansa yhteensopiva verkko- ja tietoturvadirektiivin kanssa. Avain tehokkaaseen verkkoseurantaan on tietojen käyttäminen tarkan riskinäkymän antamiseen.

Tämän tutkimuksen kohteena olevat tietoturvaratkaisut, Nozomi Networks ja Microsoft Defender for IoT, tukevat molemmat liitteessä 1 esitettyjä NIS2:n vaatimuksia. Yksityiskohtaisen omaisuuden tunnistaminen ja OT-verkkojen löytyminen auttavat energiayhtiön organisaatiota saamaan syvällisen näkyvyyden OT- ja IoT-verkkojensa tilaan. Tietojen avulla pystytään tunnistamaan ympäristöissä aktiiviset riskit ja uhkat. Tarjoamalla kontekstuaalisia hälytyksiä energiayhtiö voi reagoida nopeasti ICS-ympäristöissään oleviin uhkiin. Mukautettavien käyttöliittymien ja raportoinnin avulla voidaan vähentää tavoitteellisesti liiketoiminnan riskejä ja noudattamaan näissä myös liitteen 1 mukaisia NIS-direktiivin määräyksiä.

5.3 Kyberturvallisuusvaatimusten lisääminen koskee IT- ja OT-integraatiota

Kyberturvallisuus on nykyään siis yhä enemmän kokonaisuuksien hallintaa kuin tekniikkaa, jossa riskien vähentäminen ja mahdollisten ongelmien ennakointi ei takaa jokaisen uuden uhkan poistamista. Jatkuva prosessien ja liikenteen seuranta on tällöin

ratkaisevan tärkeää uhkien tunnistamisessa ja diagnosoinnissa sekä prosessipoikkeamien ymmärtämisessä.

Palomuureja ja tunkeutumisen havaitsemislaitteita IoT-verkoissa on harvoin, koska niitä ei yksinkertaisesti ole vaadittu. Verkot ovat olleet eristettyjä lähiverkkoja ilman Internet-yhteyttä, joskin IoT:n käyttöönoton myötä eristystä ei enää ole. Järjestelmien ja sovellusten turvaaminen onkin nyt suuri huolenaihe. Kehittyneiden yritysohjelmistojen, erityisesti analytiikan laaja käyttö, kannustaa organisaatioita integroimaan perinteisiä IT-järjestelmiä ja OT-infrastruktuuria.

Perinteiset OT-järjestelmätn komponentit ja ominaisuudet, kuten vanhentuneet päätelaitteet, heikot tietoturvaominaisuudet, integraatiohaasteet IT-järjestelmien kanssa, päivitysten hallintaongelmat ja puutteellinen kyberturvallisuusosaaminen aiheuttavat kyberturvallisuushaasteita. Lisäksi kyberturvallisuuden perusominaisuuksien puuttuminen, kuten käyttäjän todennus ja salaustekniikat, tekee niistä haavoittuvia kyberhyökkäyksille ja luvattomalle käytölle. Tämä korostaa tarvetta parantaa OT-järjestelmien tietoturvaa ja integroida nämä ominaisuudet niiden suojaamiseksi.

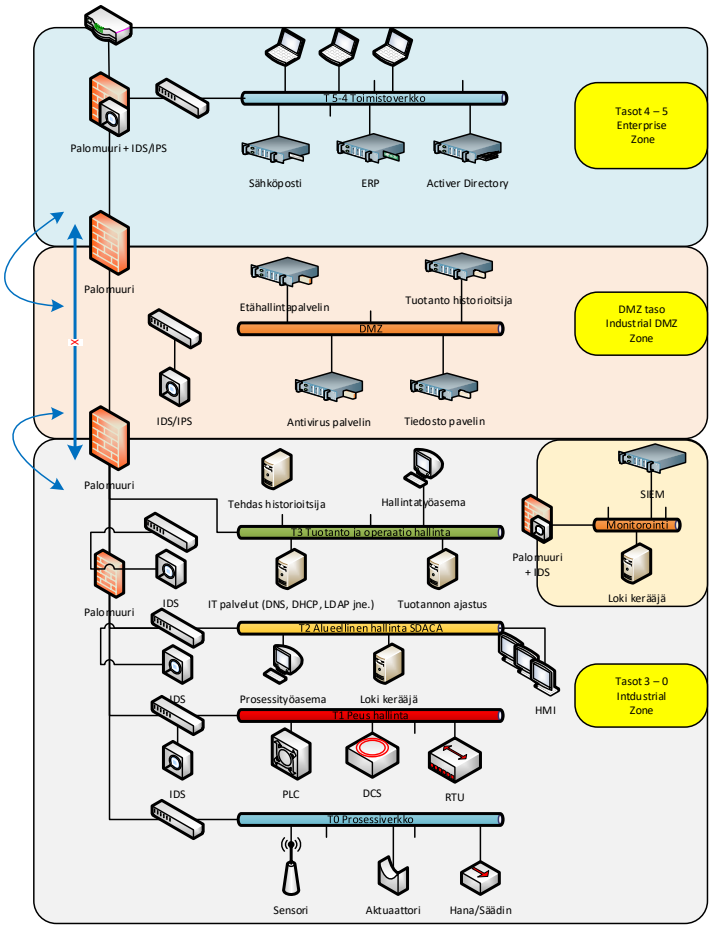
6 Miten IoT ja pilvi parantavat Purdue-mallia?

Kyberpuolustuksen vahvistamiseksi OT- ja IoT-ympäristöissä tarvitaan monitahoinen lähestymistapa, joka yhdistää teknologioita, valvontaa, prosesseja, koulutusta, yhteistyötä ja riskienhallintaa. Näin voidaan parantaa tietoturvaa ja suojautua kyberuhkilta.

Purdue Reference Model on osa Purdue Enterprise Reference Architecture:a (PERA) (kuva 3), jota käytetään ohjaamaan koko tuotantoa tietokoneiden avulla. IEC 62443-standardien mukaisesti OT-segmentointia pidetään parhaana käytäntönä OT- ja IoT- ja SCADA-järjestelmien välisen viestinnän ohjauksessa. Segmentointi on siinä keskeinen osa kyberpuolustusstrategiaa, joka on suunniteltu estämään haittaohjelmien leviäminen kriittisiin sovelluksiin ja OT-prosesseihin.

Purdue-malli on siis valmistajien yleisesti käyttämä kehys, jonka avulla pystytään hallitsemaan ja vähentämään ICS-teollisuuden riskejä. [9,10,16]. Purdue-mallin ymmärtäminen (kuva 4) auttaa hahmottamaan datan virtausta eri segmentoitujen verkkojen läpi ja sitä, kuinka eri verkkoalueet ja niiden elementit suojataan. Tietoturva toteutetaan segmentoimalla verkko eri vyöhykkeisiin, jolloin jokaiselle vyöhykkeelle voidaan määrittää sopivat suojausmekanismit. Esimerkiksi palomuurit, VPN-yhteydet, salaus ja pääsynvalvonta voivat olla osa näitä suojatoimia.

Purdue-mallin avulla voidaan siis varmistaa, että tieto liikkuu vain tarvittavien tasojen välillä ja että kriittiset järjestelmät sekä komponentit ovat suojattuja mahdollisilta kyberhyökkäyksiltä. Taulukosta 3 näemme sen tarkempia pääperiaatteita.



Kuva 4. Esimerkki Purdue-mallista.

Taulukko 3. Purdue-mallin pääperiaatteet [16.]

• Jakaa toiminnalliset verkot eri tasoihin. Tasomallissa jokainen taso voi kommunikoida vain lähinaapureidensa kanssa. Kun taustalla olevan prosessin turvallisuustaso kiristyy, muidenkin tasojen vaatimukset luokitellaan tiukemmin.
• Segmentointi ja hierarkia, järjestelmäkomponentit ja omaisuuserät on selvästi määritelty ja ryhmitelty erillisiin kerroksiin.
• Kerrosten väliset rajat ovat loogisia paikkoja verkon segmentointiin kerrosten välisen pääsyn hallitsemiseksi.

Purdue-mallin avulla loppukäyttäjät, integraattorit ja toimittajat voivat tehdä yhteistyötä sovellusten integroimiseksi yritysverkkoon ja prosessi-infrastruktuuriin. Nykyinen Purdue-arkkitehtuuri mallintaa OT: n ja IT: n kuudeksi toiminnalliseksi tasoksi, jotka vaihtelevat tasolta 0 tasolle 5 ja ulottuvat kolmelle turvavyöhykkeelle.[9] Turvavyöhykkeet, joita kutsutaan erillisalueiksi, ovat alueita, joiden välillä on sekä fyysisiä että tietoteknisiä suojamuureja, kuten palomuurit, estämässä luvatonta pääsyä ja parantamassa kyberturvallisuutta. [5,16.]

Purdue-malli on edelleen merkityksellinen, sillä se tarjoaa hyvän lähtökohdan OT- ja IT-järjestelmien integroinnille sekä teollisuusohjausjärjestelmien turvallisuuden hallinnalle. Malli auttaa ymmärtämään eri järjestelmien toiminnallisuutta ja niiden keskinäistä riippuvuutta sekä sen avulla voidaan myös luoda selkeämpi kuva järjestelmän turvallisuudesta ja hallinnasta. Mallin avulla voidaan myös erottaa selkeästi eri turvatasot ja niiden välillä olevat suojaukset ja turvamekanismit. Turvavyöhykkeiden käyttö auttaa erottamaan eri järjestelmien toiminnallisuudet toisistaan ja mahdollistaa niiden paremman turvallisuuden hallinnan. Vaikka Purdue-malli on edelleen käyttökelpoinen, on tärkeää muistaa, että se ei ole ainoa tapa hallita teollisuusohjausjärjestelmien turvallisuutta. Purdue-mallia voidaan ja pitää soveltaa moderniin IIoT-ympäristöön, mutta sen päivitykset ovat tarpeen sen soveltamiseksi paremmin nykyajan vaatimuksiin. Seuraavalla sivulla taulukossa 4 kuvataan tarkemmin Purdue-viitemallin eri tasoilla olevia toimintoja.

- tasot 4 ja 5 käsittävät yritysvyöhykkeet
- tasot 0–3 käsittävät teollisuusvyöhykkeet
- demilitarisoitu vyöhyke (DMZ) liikennevirtojen hallintaan yritys- ja teollisuusvyöhykkeiden välissä

Taulukko 4. Purdue-viitemallin yleiset toiminnot [16.]

Tasot	**Toiminnot**
Taso 5 Yritysverkot	Laajempi joukko yrityksen IT-järjestelmiä, mukaan lukien yhteydet julkiseen Internetiin
Taso 4 IT- järjestelmät	Yritysjärjestelmät, jotka voivat sisältää tietokantapalvelimia, sovelluspalvelimia ja tiedostopalvelimia
Taso 3 DMZ- vyöhyke	Järjestelmät, jotka tukevat koko tehtaan ohjaus- ja valvontatoimintoja. Yhdistävät myös alemman tason tiedot, jotka on siirrettävä korkeamman tason liiketoimintajärjestelmiin
Taso 2 Prosessien valvonta	Ohjauslogiikka taso 1 sisältää järjestelmiä, jotka analysoivat ja toimivat ohjauslogiikan tietojen perusteella. Järjestelmät sisältävät ihmisen ja koneen välisen rajapinnan (HMI); valvonta- ja tiedonhankintaohjelmistot (SCADA)
Taso 1 Prosessienhallinta	Ohjauslaitteet, ohjelmoitavat logiikkaohjaimet, jotka seuraavat ja ohjaavat tason 0 laitteita ja turvalaitteita
Taso 0 Fyysiset prosessit/toimilaitteet	Fyysiset laitteet, jotka tunnetaan valvottavina laitteina. Esimerkiksi venttiilit, pumput, anturit, toimilaitteet, kompressorit

Tyypillisesti DMZ on toteutettu liikennevirran ohjaamiseksi laitosverkkoon ja siitä ulos palomuureilla [10.]. Malli tarjoaa tavan hallita järjestelmien välistä kommunikointia. Purdue-mallia ei alun perin luotu kyberturvallisuusarkkitehtuuriksi, mutta koska liiketoiminnan tarve tietojen jakamiseen yritysvyöhykejärjestelmien ja tuotantovyöhykejärjes-

telmien välillä on kasvanut vuosien varrella, turvallisuusalan ammattilaiset ovat omaksuneet sen turvallisempien verkkojen rakentamiseksi.

Purdue-malli on suunniteltu alun perin käytettäväksi perinteisemmissä teollisuuden ohjausjärjestelmissä, mutta sitä pyritään nyt soveltamaan myös uudempiin IoT-laitteisiin ja pilvipalveluihin. Tämä johtuu siitä, että vanhempiin teollisuusjärjestelmiin liittyvät haasteet ovat edelleen olemassa ja niitä on tarpeen ratkaista myös uusissa järjestelmissä. Purdue-mallia muokataan vastaamaan paremmin nykyaikaisia tarpeita ja haasteita, jotka liittyvät muun muassa IoT:n ja pilvipalvelujen käyttöön OT-ympäristöissä. [11,16.] Euroopan unionin kyberturvallisuusvirasto (ENISA) on ehdottanut uutta, kuvan 5 mukaista arkkitehtuuria Purdue-mallista.

Kuva 5. Euroopan unionin kyberturvallisuusvirasto (ENISA) ehdotus uudesta IIoT-Purdue mallista. [12.]

Ajatuksena olisi ottaa käyttöön kolmitasoinen teollinen IoT-alusta, joka kommunikoi suoraan tason 1 IoT-laitteiden kanssa. Mallin päätavoitteena on rajoittaa tai estää tietoliikennettä tasojen välillä. Perinteisessä Purdue-mallissa, jossa IIoT-laitteet olisivat osa OT:n kerrosta, ne lähettäisivät tietonsa kerrokseen 3, joka kommunikoisi kerroksille 4 ja 5. [12,16.] Tyypillisesti kunkin kerroksen tietojen on kuljettava palomuurin DMZ:n läpi yrityksen ja tuotantoalueiden välillä ennen kuin ne saavuttavat seuraavan tason ylös-

tai alaspäin. Perinteiset Purdue-tasot voitaisiin jopa ohittaa sallimalla laitteiden kommunikointi IoT-yhdyskäytävän kautta suoraan pilvipalvelujen kanssa. [11.] Tällöin pilvipalveluiden käyttö lisää vähintäänkin yhden tason Purdue-malliin perinteisen yritysvyöhykkeen yläpuolelle. Data ei IIoT-käyttäjille enää ole kokonaan yrityksen sisällä, jolloin Purdue-mallia voidaan pitää vanhentuneena näissä ympäristöissä. [11.]

Täytyy kuitenkin muistaa, että Purdue-malli kuvastaa OT-verkon hierarkkisuutta ja ohjaa verkon suojauksen suunnittelua. OT-verkon IIoT-laitteiden turvallisuus on yhtä tärkeää kuin kaikkien muiden verkkoon kytkettyjen koneistoa pyörittävien komponenttien turvallisuus. IIoT-laitteiden tietojen lähettäminen suoraan pilveen ja tietojen suojaaminen tulee haasteeksi. [12.]

Purdue-malli jakaa siis kyberturvallisuuden vaiheiksi, jotka vähentävät kyberriskejä asteittain. Kukin vaihe käsittelee tiettyä ja helposti ymmärrettävää turvallisuuskysymystä. Näitä ovat yksittäisten laitteiden suojaaminen, puolustaminen ulkoisilta hyökkäyksiltä, haittaohjelmien sisällyttäminen ohjausjärjestelmään, epäilyttävän toiminnan valvontajärjestelmät sekä kehittyneiden uhkien havaitsemisen ja verkkotapahtumien aktiivinen hallinta. Vaiheessa on mukana joukko toimia ja tekniikoita sekä resursseja, joita voidaan käyttää tavoitteiden saavuttamiseen.

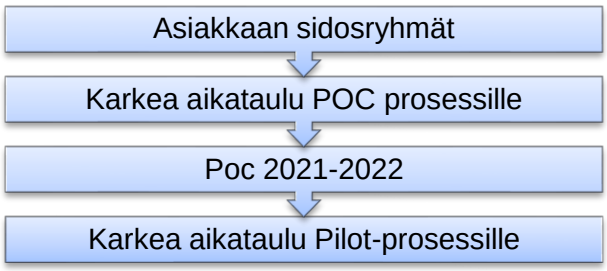
Teollisuuden ICS-kyberturvallisuusohjeet ja -standardit keskittyvät yleensä saamaan yritykset investoimaan yleisiä kyberhyökkäysskenaarioita vastaan vähintään vähimmäissuojaukseen. Tämä vastaa suunnilleen Purdue-mallin kolmea ensimmäistä tasoa ja voi olla sopiva pieniriskisten teollisuudenalojen yrityksille, jotka kestävät joitain prosessin häiriöitä. Tähän tarvitaan mallin korkeampien tasojen tarjoamaa riskinhallintaa, joka edellyttää kaikkien tarpeettomien riskien välttämistä. Viimeaikaiset tapahtumat erityisesti sähköverkoissa osoittavat, että kriittisen infrastruktuurin toiminta on myös kehittyneiden sekä hyvillä resursseilla varustettujen hyökkäysryhmien kohteita. [14.]

7 Tutkimusprojektin suunnittelu

Projekti aloitettiin vuonna 2021 soveltuvuusselvitys suunnitelman (Proof of Concept, POC) laadinnalla kahden toimittajan, Microsoftin Defender for IoT ja Nozomi Networksin tietoturvaratkaisuista. POC:issa määriteltiin verkkoyhtiön tarpeisiin pohjautuvat käyttötapaukset (taulukot 5,6), ja miten ne vastaavat verkkoyhtiön tarpeita sekä vaatimuksia. Käyttötapauksissa POC:n tuli olla yhteydessä liitteessä 1 määriteltyihin testitapauksiin, eikä niinkään teknisiin odotuksiin, kuten suunnittelemattomien seisokkien vähentämiseen tai laadun parantamiseen.

Kun testisuunnitelma oli laadittu (Liite 1), seuraava vaihe oli testausten suorittaminen määritetyssä verkkoyhtiön OT-verkossa. Testauksen aikana tarkasteltiin molempien ratkaisujen kyvykkyyksiä ja eroja, keskittyen erityisesti omaisuuden hallintaan ja tuotannon tilan arviointiin. Tämä antoi tärkeää tietoa OT-verkon liikenteestä, valittujen verkkojen segmentoinnista ja kokonaistopologian rakenteesta, mikä auttoi vertailussa ja lopullisessa päätöksenteossa.

VXLAN-teknologian käyttöönotto testausympäristössä mahdollisti paremman näkyvyyden suurempaan OT-laitekantaan ja osoitti, kuinka tehokkaasti kumpikin ratkaisu pystyi hyödyntämään tätä teknologiaa. Tämä auttoi projektin osallistujia ymmärtämään, kuinka hyvin kumpikin ratkaisu kykeni vastaamaan verkkoyhtiön tarpeisiin ja vaatimuksiin, ja miten ne voivat tukea laajempaa OT-infrastruktuuria. Projektille luotiin karkea aikataulu alla olevan suunnitelman mukaisesti.



Testaaminen perustui NIST Cyber Security Framework -viitekehyksen mukaisiin tunnistamis- ja havainnointitoimintoihin, joihin molemmat tutkittavat ratkaisut on ensisijaisesti

suunniteltu. Testauksen avulla tarkasteltiin niiden kyvykkyyksiä ja eroja omaisuuden hallintaan (taulukko 5) ja tuotannon tilan arviointiin (taulukko 6) määriteltyjen vaatimusten mukaisesti. Näin oli tarkoitus saada perustason selvitystä OT-verkon liikenteestä, valittujen verkkojen segmentoinnista sekä kokonaistopologian rakenteesta.

Taulukko 5. Omaisuuden hallinta

• Laitteiden liitännät
• OT-toimittajat ja niiden protokollat
• Hälytysten ja ilmoitusten luominen epänormaalista käyttäytymisestä
• Automaattinen omaisuuden etsintä ja hallinta
• Uudet laitteet
• Raportointinäkyvyys

Taulukko 6. Tuotannon tila

• Tietoturvapoikkeaminen havainnointi ja niihin reagointi
• Verkkoympäristö ja laitteiden väliset yhteydet
• Jatkuva verkkotoiminnan seuranta
• Haavoittuvuuden arviointi ja riskienhallinta
• Valitun verkkosegmentin kokonaistopologian rakenne

Tuntemattomien ja tunnettujen uhkien monitorointiin ja tietoturvapoikkeaminen havainnointiin käytettiin tuotteiden koneoppimiseen ja tekoälyyn pohjautuvia toimittajan algoritmeja. Monipuolinen lähestymistapa kyberturvallisuuteen on avainasemassa haettaessa vastauksia seuraaviin omaisuudenhallinnan peruskysymyksiin:

- Mitä verkossa on?
- Miten laitteet kommunikoivat?
- Onko Internetiin kytkettynä jotain, mitä ei pitäisi olla?

Tunnista toiminto on ensimmäinen ja yksi NIST-kyberturvallisuuskehyksen viidestä ydinkehystoiminnosta muodostaen perustan kehyksen kaikille toiminnoille. Tunnistamisen avulla haetaan näkyvyyttä edellä mainittuihin kysymyksiin. Tämä auttaa kybertietoturvauhkien tunnistamisessa ja keskittyy ymmärtämään prosesseja, omaisuutta, infrastruktuuria sekä riskejä.

Ratkaisujen suhteellisen uudet Network Detection and Response (NDR) -tuotteet keskittyvät uhkien havaitsemiseen analysoimalla verkkoliikennettä reaaliajassa. Koneoppimisen avulla voidaan havaita tarkasti jopa salakavala uhkakäyttäytyminen ja piilotetut riskit. Jokainen verkon yli kommunikoiva laite voidaan tunnistaa tarkkailemalla sen toimintaa.

Lisäksi verkkoliikenteestä voidaan poimia suuri määrä yksityiskohtia, kuten käyttöjärjestelmätietoja, käytössä olevia sovelluksia ja käyttäjiä, jotka ovat käyttäneet laitetta tai laitteita, jotka ovat kommunikoineet kohdelaitteen kanssa julkiseen Internetiin.

Sensorit keräävät OT-tietoja reaaliajassa, jolloin tuloksena saadaan nopea omaisuuden tunnistaminen, kybertapahtumat, kriittiset prosessipoikkeamat sekä hälytykset. Käytännössä passiivinen valvonta on lähes aina verkkoliikenteen ”haistelemista”, eli verkon liikennevirran peilaamista sensorille. Se ei vaadi lisäohjelmistojen asentamista päätelaitteisiin, eikä täten kuormita verkon resursseja.

8 Tutkitut tietoturvaratkaisut

8.1 Microsoft Defender for IoT

Microsoft Defender for IoT on tietoturvaratkaisu, joka tunnettiin aiemmin nimellä CyberX, jonka Microsoft osti vuonna 2020. Vuonna 2013 perustetulla CyberX:llä on pitkä historia kriittisissä infrastruktuureissa OT-verkkojen suojaamisesta ja verkkoturvallisuuden havainnoinnista. [15.]. Defender for IoT on agentiton ratkaisu, joka on suunniteltu tarjoamaan jatkuvaa suojausta IoT- ja OT-laitteille sekä -verkoille. Se tarjo-

aa laajan valikoiman ominaisuuksia, jotka auttavat tunnistamaan ja hallitsemaan haavoittuvuuksia, havaitsemaan ja vastaamaan uhkiin sekä seuraamaan laitteiden suorituskykyä. Ratkaisu ei vaadi muutoksia olemassa oleviin ympäristöihin, mikä tekee siitä helpon integroida olemassa oleviin järjestelmiin. Se voidaan ottaa käyttöön paikallisesti tai yhdistää Azure-pilveen, mikä mahdollistaa laajemman hallinnan ja valvonnan tarjoamisen. Microsoft Defender for IoT käyttää tekoälyä ja koneoppimista havaitakseen uhkia ja haavoittuvuuksia laitteissa ja verkoissa. Se tarjoaa myös kattavan tietoturvan hallintaratkaisun, joka auttaa yrityksiä hallitsemaan tietoturvapolitiikkoja ja noudattamaan säännöksiä. Sen agentittomuus ja yhteensopivuus olemassa olevien ympäristöjen kanssa tekee siitä helpon ottaa käyttöön ja hallita.

Ratkaisu koostuu kahdesta pääkomponentista eli Microsoft Defender for IoT Managementista ja Microsoft Defender for IoT Sensorista. Microsoft Defender for IoT Management antaa mahdollisuuden hallita ja analysoida useista sensoreista koottuja hälytyksiä yhteen käyttöliittymän hallintanäkymään, josta saadaan yleiskuva verkkojen tilasta. Microsoft Defender for IoT Sensor etsii ja valvoo jatkuvasti verkkolaitteita. Sen sensorit keräävät verkkoliikennettä käyttämällä passiivista, agentitonta valvontaa IoT- ja OT-laitteissa. Sensorit kytkeytyvät SPAN-porttiin (Switched Port Analyzer) tai verkkoliitäntään ja aloittavat välittömästi syvän pakettitarkistuksen (DPI) IoT- ja OT-verkkoliikenteessä. Molemmat komponentit voidaan asentaa joko erilliseen laitteeseen tai virtuaalikoneeseen.

Microsoft Defender for IoT integroituu hyvin muihin Microsoftin IoT-tietoturvatuotteisiin Azure IoT -palveluiden kautta, jossa sen keskeinen integraatiopainopiste on Sentinel SIEM -järjestelmä. Tämä antaa kattavan kuvan verkkoliikenteestä, sen toiminnasta ja mahdollisista uhkista. Koneoppimisen avulla tunnistetaan verkkoon kohdistuvat hyökkäykset, joita muut työkalut eivät välttämättä havaitse. Vakiokokoonpanossa valvontaan Microsoft ehdottaa käytettäväksi Sentinelin käyttöliittymän paneelia, joka vastaanottaa kaikki ilmoitukset Defender for IoT -näytöltä.

Hälytykset perustuvat havainnointi- ja analytiikkamekanismeihin, jotka liittyvät teollisuuden haittaohjelmien, poikkeamien havaitsemiseen myös sensoritasolla. Tavoitteena on siis laajentaa näkyvyyttä myös verkossa hallittujen laitteiden ulkopuolelle. Defender

for IoT voi hyödyntää Azure IoT Hubia uudempien IoT- ja OT-laitteiden tietoturva-arvioinneissa. IoT- ja OT-laitteita voidaan hallita myös agenttien kautta, kun taas vanhat hallitsemattomat laitteet voidaan suojata ilman agenttia.

Ratkaisun integrointi kolmansien osapuolten tietoturvatyökalujen kanssa on myös valmiina, esimerkkeinä Splunk, IBM QRadar ja ServiceNow, jotka toimivat saumattomasti laitetoimittajien, kuten Rockwell Automationin, Schneider Electricin, GE: n, Emersonin, Siemensin, Honeywellin, ABB:n ja Yokogawan, teknologian kanssa. Lähtökohtaisesti Defender for IoT tarjoaa monikerroksisen strategian. Taulukko 7 esittelee Microsoftin Defender for IoT -ratkaisun keskeisimmät ominaisuudet, jotka auttavat yrityksiä parantamaan kyberturvallisuuttaan erityisesti teollisen internetin (IoT) ja toiminnan teknologian (OT) ympäristöissä. [23.]

Taulukko 7. Defender for IoT:n keskeisimmät ominaisuudet

Omaisuuden etsintä ja verkko-topologian kartoitus	Tämän toiminnon ansiosta yritykset saavat selkeän näkymän laitteistaan, niiden välisten yhteyksien luonteesta ja verkon rakenteesta, mikä mahdollistaa tehokkaamman valvonnan ja suojauksen.
Haavoittuvuuksien hallinta	Defender for IoT auttaa tunnistamaan ja korjaamaan haavoittuvuuksia IoT- ja OT-ympäristöissä. Se kattaa alustat, sovelluspäivitykset ja tietoturva-aukot. Riskipisteet ja automaattinen uhkamallinnus mahdollistavat hyökkäysreittien priorisoinnin ja ennaltaehkäisyn.
Jatkuva uhkien havaitseminen	Defender for IoT tunnistaa nopeasti poikkeavat tai luvattomat toiminnot verkossa käyttäen IoT/OT Aware -analytiikkaa ja uhkatietoa mahdollisiin uhkiin reagoimiseen.

Nämä keskeiset ominaisuudet tekevät Microsoftin Defender for IoT -ratkaisusta tehokkaan työkalun IoT- ja OT-ympäristöjen kyberturvallisuuden parantamiseksi. Ne auttavat

tunnistamaan ja hallitsemaan riskejä tehokkaasti ja suojaamaan kriittistä infrastruktuuria kyberhyökkäyksiltä.

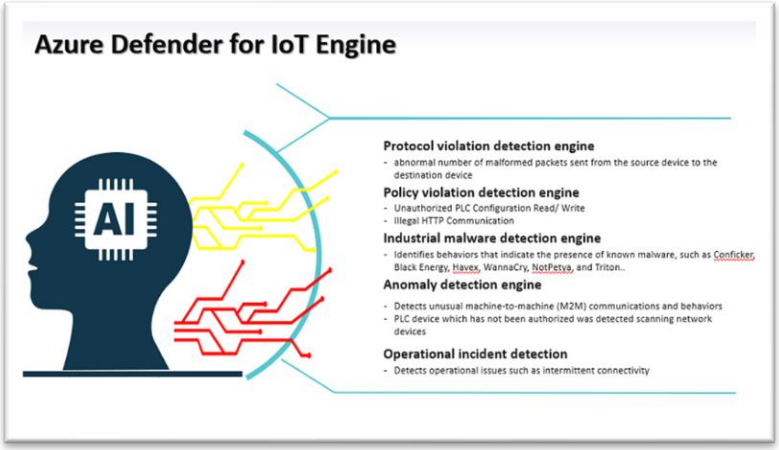
Defender for IoT soveltaa käyttäytymisanalytiikkaa ja koneoppimistekniikoitaan laitteiden löytämiseen ja luokitteluun sekä IoT-hyökkäyksien suojaamiseen, havaitsemiseen ja niihin vastaamiseen. Tämä mahdollistaa myös Defender for IoT:n soveltamisen globaaleihin IoT- ja OT-uhkatietoihin. Defender for IoT -alustalla on kyvykkyys arvioida kyberriskejä ja tuottaa haavoittuvuuksista hyviä ja laadukkaita riskiarviointiraportteja, jotka sisältävät objektiivisen riskipisteen sekä priorisoidut, yksityiskohtaiset käytännön suositukset haavoittuvuuksien korjaamiseksi.

Tämä luo hyvän perustan tietoturvan hallinnalle ja keinon arvioida riskien pienenemistä IoT:ssa sekä teollisuuden ohjausjärjestelmissä (Industry Control System, ICS). Defender for IoT pystyy tunnistamaan sekä operatiivisen teknologiaan että IT-verkkoihin kohdistuvat uhkat, joiden havaitseminen on ollut aiemmin haastavaa [14,15]. Se hyödyntää patentoitua M2M-tietoista käyttäytymisanalytiikkaa ja koneoppimista, jossa sääntöjen tai allekirjoitusten manuaalinen määritys ei ole tarpeen, joka on ratkaisulle merkittävä etu.

Defender for IoT käyttää skannaus- ja valvontatekniikoita, jotka mahdollistavat omaisuuden löytämisen, haavoittuvuuksien hallinnan sekä jatkuvan uhkien seurannan tuhansissa laitteissa, joita voidaan käyttää tehtaissa ja rakennuksissa. Käyttäytymisanalyysi-alusta integroituu helposti Azure-tietoturvaan, jossa tarjotaan käyttäjän päästä päähän -suojausta (end-to-end) hallituissa ja hallitsemattomissa IoT-laitteissa. Agenttivapaa tekniikka kerää sekä IoT- että OT-pohjaisia tietoja omaisuusprofiileista, riskeistä ja mahdollisista haavoittuvuuksista. Omaisuuden perustason käyttäytymistä käytetään tunnistamaan poikkeamat, jotka saattavat osoittaa turvallisuusuhkia.

Hälytykset perustuvat reaaliaikaiseen ennalta tallennettuun liikenteeseen, jossa tiedon kerääminen, käsittely, analysointi sekä hälytykset tapahtuvat suoraan sensorilta (vain metatiedot siirretään hallintakonsoliin). Hälytys on osoitus murtautumisesta tai hyökkäyksestä, joiden vuoksi hälytykset on tutkittava ja korjattava.

Itseoppivien analytiikkamoottoreiden tehtävänä on käynnistää erilaisia hälytyksiä ilman tarvetta määritellä erityisiä sääntöjä tai päivittää hyökkäysmalleja. Nämä moottorit arvioivat OT-verkkoliikennettä reaaliajassa mahdollisten poikkeavuuksien, haittaohjelmien, protokollarikkomusten ja muiden verkon perustoiminnan poikkeamien varalta käyttämällä ICS-spesifistä käyttäytymis- ja data-analytiikkaa (kuva 6). [17.]



Kuva 6. Defender for IoT -sensorin viisi itseoppivaa analytiikkamoottoria [24.]

Protokollamoottorin (Protocol violation detection) tehtävänä on havaita poikkeamat aiemmin opitusta liikenteestä, esimerkiksi uuden laitteen liityttyä verkkoon tai jos laitteessa on muutettu konfiguraatiota, kuten esimerkiksi ohjelmistoversiota. Hälytykset kuvaavat havaittuja poikkeamia pakettirakenteessa, Jotka poikkeavat protokollan määrityksistä. Näistä esimerkeiksi käyvät Modbus-poikkeamat tai vanhentuneiden toimintojen koodisignaalit.

Sääntörikkomusten havaitsemismoottorin (Policy violation) tehtävänä on havaita poikkeamat opitusta lähtötilanteesta, joka määrittää ICS-verkkojen perustason. Tämä tarkoittaa, että järjestelmä oppii verkon perustason vähemmän aikaa vievällä tavalla kuin perinteiset matemaattiset menetelmät tai analytiikka, jotka on suunniteltu IT-verkoille.

Sääntörikkomusten havaitsemismoottori tarkkailee verkon käyttöä ja vertaa sitä opittuun lähtötilanteeseen. Jos havaitaan poikkeamia, kuten epätavallista liikennettä, ei-

tyypillisiä yhteyksiä tai muita poikkeamia, järjestelmä lähettää hälytyksen, joka kuvaa havaitun poikkeaman ja sen sijainnin. Tämä auttaa havaitsemaan mahdollisia sääntörikkomuksia ja suojaamaan IIoT- ja OT-verkkoja. Sääntörikkomusten havaitsemismoottori on erittäin tärkeä turvallisuusratkaisu, sillä se auttaa organisaatioita havaitsemaan mahdolliset hyökkäykset tai virheet verkoissa ja torjumaan niitä ennen kuin ne aiheuttavat vahinkoa.

Microsoft Defender for IoT:n haittaohjelmien tunnistusmoottori (Industrial malware detection) toimii eri tavalla kuin perinteinen allekirjoituspohjainen analyysi. Sen sijaan tunnistusmoottori perustuu käyttäytymiseen ja käyttää koneoppimista tunnistaakseen haitallisen toiminnan. Moottori tarkkailee kohdelaitteen toimintaa ja vertaa sitä tunnettuihin haittaohjelmiin, kuten Conficker, Black Energy, WannaCry, NotPetya ja Triton. Se etsii käyttäytymismalleja, jotka ovat tyypillisiä haittaohjelmille: yritys murtautua järjestelmään, tiedostojen salaaminen, hävittäminen tai epätavalliset verkkoyhteydet. Jos tunnistusmoottori havaitsee haitallista toimintaa, se lähettää hälytyksen, joka kuvaa havaitun toiminnan ja sen sijainnin. Tämä auttaa organisaatioita havaitsemaan ja torjumaan haittaohjelmia, jotka voivat uhata IIoT- ja OT-ympäristöjä.

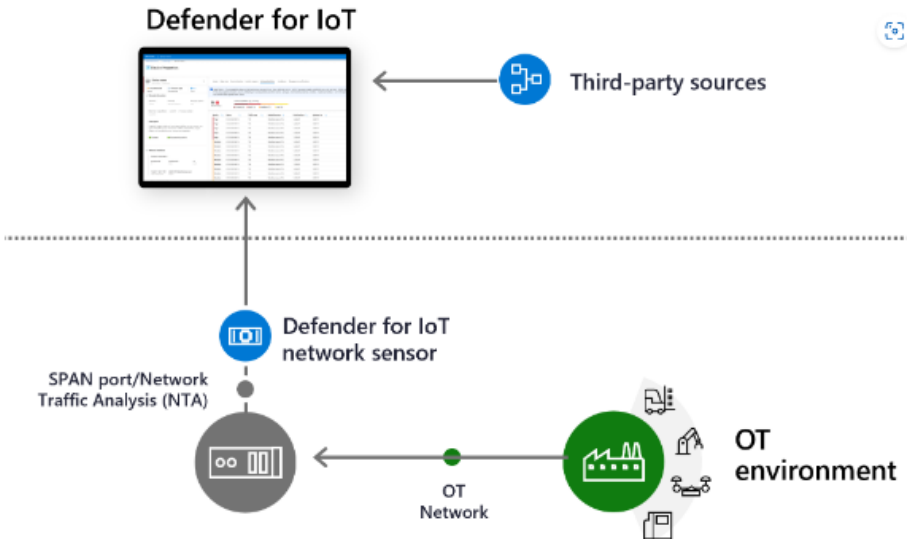
Microsoft Defender for IoT:n haittaohjelmien tunnistusmoottori on tärkeä, sillä perinteiset allekirjoituspohjaiset analyysit voivat olla tehottomia uusien ja muunneltujen haittaohjelmien tunnistamisessa. Sen sijaan käyttäytymispohjainen analyysi auttaa tunnistamaan haitallisen toiminnan, joka voi olla merkki mahdollisesta hyökkäyksestä tai uhkasta IIoT- ja OT-ympäristöille.

Poikkeamien havaitsemismoottori (Anomaly detection) tunnistaa odottamattomat koneiden väliset M2M-tiedonsiirrot (Machine to Machine) ja käyttäytymisen. Koska alusta mallintaa ICS-verkkoja deterministisinä tilojen ja siirtymien sarjoina, sen oppimiseen kuluu vähemmän aikaa kuin yleisillä matemaattisilla menetelmillä tai analytiikalla, jotka alun perin suunniteltiin IT-ympäristöille eivätkä välttämättä sovellu suoraan OT-ympäristöön. Anomaly detection -moottori havaitsee poikkeamat nopeasti ja vähentää väärän positiivisen havaitsemisen mahdollisuutta. Esimerkkejä poikkeamien havaitsemismoottorin ilmoituksista ovat esimerkiksi liialliset SMB-kirjautumisyritykset ja havaittu PLC-skannaus. Toinen esimerkki on laite, joka suorittaa verkkoskannauksia, mutta jota

ei ole luokiteltu skannaavaksi laitteeksi. Tässä tapauksessa liikenne tulkitaan epätavalliseksi tiedonsiirroksi, mikä käynnistää hälytyksen. Hälytykset kuvaavat havaittuja toimintahäiriöitä tai toimivia yksiköitä, esimerkiksi kun PLC-laite pysähtyy tai käynnistyy (Operational Engine). [17.]

8.2 MS Arkkitehtuuri

Monikerroksinen hajautettu arkkitehtuuri (kuva 7) on suunniteltu skaalautumaan myös suurissa ja maantieteellisesti hajautetuissa ympäristöissä, joissa voi olla useita etätoimipisteitä maan, alueen, liiketoimintayksikön tai vyöhykkeen mukaan. Pilveen yhdistettyjen sensoreiden havaitsemat tiedot näkyvät paikallisessa sensorikonsolissa, mutta ne voidaan myös lähettää IoT-keskittimen kautta muihin Azure-palveluihin, kuten Microsoft Sentinel:iin. Microsoft Defenderin IoT:n Sentinel:lle lähettämät hälytykset laukaisevat analytiikan tunnistusmoottorit, joiden tarkoituksena on havaita uhkia ja ratkaista mahdollisia tapahtumia (Incident). Paikallisesti kytketyllä sensorilla havaitut tiedot näkyvät konsolissa. Tunnistustiedot jaetaan myös paikallisen hallintakonsolin kanssa, jos sensori on yhdistetty siihen. Liikenteen sieppaamiseen käytetään paikallista verkkosensoria, joka on asennettu virtuaalisena tai fyysisenä laitteena ja kytketty SPAN-porttiin.



Kuva 7. Defender fot IoT -arkkitehtuurikuva [30.]

Verkkoliikenneanalyysi (Network Traffic Analyzer, NTA) voidaan myös toteuttaa passiivisena seurantana sensorilla, joka kerää verkkoliikenteen metatietoja analysointia ja tarkkailua varten. Verkkoliikenteen analyysi on kriittinen osa nykyaikaisia uhkien havaitsemis- ja reagointikäytäntöjä, koska monet toiminta- ja turvallisuusongelmat voidaan tutkia toteuttamalla NTA sekä verkon reunalla että verkon ytimessä. Liikenneanalyysityökalulla voidaan havaita esimerkiksi suuret lataukset, suoratoistot tai epäilyttävä saapuva tai lähtevä liikenne.

NTA tarjoaa myös organisaatiolle paremman näkyvyyden verkoissa oleviin uhkiin päätepisteen ulkopuolella. Palomuurin lokitiedot ovat hieman ongelmallisia, jos verkko on hyökkäyksen kohteena. Tällöin lokitiedot eivät ole käytettävissä palomuurin resurssikuormituksen vuoksi tai hakkerit ovat ylikirjoittaneet ne (tai joskus jopa muuttaneet niitä), mikä voi pahimmillaan johtaa tärkeiden rikosteknisten tietojen menettämiseen.

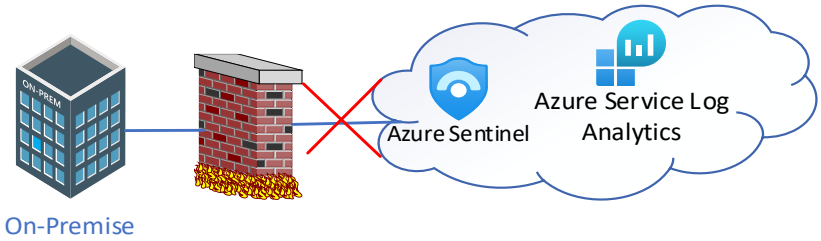
NTA:n lisäksi käytetään syvää pakettien tarkistusta (Deep Packet Inspection, DPI), joka tarjoaa eniten lisätietoa verkkoliikenteestä. Tämä auttaa ymmärtämään, kuinka esimerkiksi sovelluksia käytetään ja verkkoliikennettä tarkkaillaan epäilyttävien haittaohjelmien tai muiden tietoturvatapahtumien varalta. DPI tarjoaa hyvän näkyvyyden verkkoon ja mahdollistaa verkko- ja tietoturva ylläpitäjien perehtyä pienimpiin yksityiskohtiin.

Defender for IoT tarjoaa joustavuutta käyttöönottotavoissa, mikä on suuri etu erilaisissa käyttöympäristöissä. Se voidaan ottaa käyttöön Azure-pilvessä, paikallisena ratkaisuna tai hybridinä, joka yhdistää molemmat vaihtoehdot. Tämä joustavuus tekee Defender for IoT:stä sopivan ratkaisun moniin skenaarioihin, kuten pienen kaistanleveyden tai korkean latenssin yhteyksissä, laitteiden vanhoissa käyttöjärjestelmissä tai erittäin suojatuissa ympäristöissä.

Paikallisessa konesaliratkaisussa Defender for IoT -sensorilaite ja siihen liitetty hallintakonsoli ovat yhteydessä paikalliseen SIEM-järjestelmään (esimerkiksi Splunk, Qradar), mutta ne eivät ole yhteydessä Azuren pilvipalveluun kuten kuvassa 8. Tässä ratkaisussa sekä sensori että hallintakonsoli voivat olla virtuaalisia tai fyysisiä laitteita.

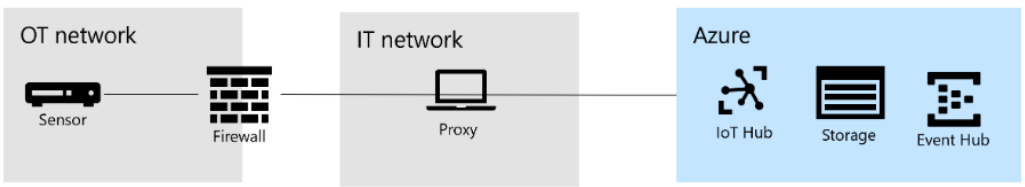
Sensori vaatii kaksi verkkoliitäntäkorttia toimiakseen paikallisessa konesaliratkaisussa. Ensimmäinen verkkoliitäntäkortti (NIC 1) on liitettävä OT-verkkoon verkkoliikenteen seurantaa ja analysointia varten. Toinen verkkoliitäntäkortti (NIC 2) on liitettävä IT-verkkoon hallintaa ja yhteyttä muihin järjestelmiin varten.

Tämän joustavan käyttöönottomahdollisuuden ansiosta Defender for IoT sopii hyvin monenlaisiin käyttötilanteisiin ja -ympäristöihin, tarjoten kattavan ja tehokkaan tietoturvallisuusratkaisun sekä OT- että IT-verkoille.



Kuva 8. Defender for IOT konesaliratkaisuna. [32.]

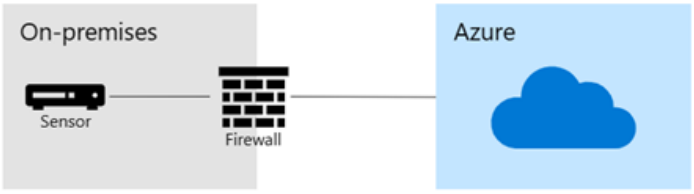
Hybridiratkaisussa Defender for IoT yhdistää paikallisen ja pilvipohjaisen ratkaisun parhaat puolet. Tässä ratkaisussa kommunikointi Defender for IoT -sensorilta Azure-pilveen tapahtuu IT-verkon DMZ-alueella olevan välityspalvelimen kautta. Tämä lähestymistapa parantaa tietoturvaa ja varmistaa, että OT- ja IT-verkkojen välillä on asianmukainen eristys. Kun tiedonsiirto tapahtuu OT-segmentissä olevan sensorin ja Azuren pilvipalvelun välillä, välityspalvelin käyttää salattua SSL-tunnelia tiedon siirtämiseen. Tämän ansiosta välityspalvelin ei tarkasta, analysoi eikä tallenna välimuistiin mitään tietoja, mikä lisää tietoturvaa ja yksityisyyttä (kuva 9).



Kuva 9. Defender for IoT hybridiratkaisuna. [32.]

Tämä hybridiratkaisu mahdollistaa joustavan ja tehokkaan tavan hyödyntää sekä paikallisen että pilvipohjaisen ratkaisun etuja. Se tarjoaa korkean tietoturvatason ja mahdollistaa eri verkkotyyppien (OT ja IT) tehokkaan eristämisen, mikä on tärkeää monimutkaisissa ja kriittisissä teollisuuden ohjausjärjestelmissä.

Azure-pilvipohjaisessa ratkaisussa, kuten kuvassa 10, Defender for IoT -sensori voidaan yhdistää etäpaikoista suoraan internetin kautta Azure Defender for IoT -portaaliin. Tämä tarkoittaa, että sensorin tiedonsiirto ei tarvitse kulkea yrityksen sisäisen verkon kautta, mikä voi tarjota paremman tietoturvan ja joustavuuden.



Kuva 10.Azuren Defender for IoT:n kytkentä suoraan Internettiin. [32.]

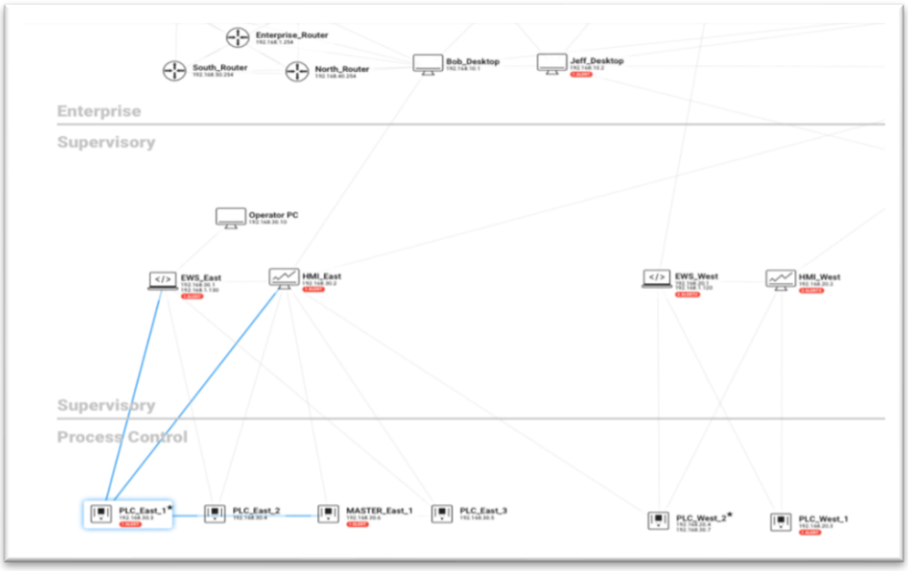
Tässä skenaariossa sensori kommunikoi suoraan Azure-pilvipalvelun kanssa ja kaikki tiedonkeruu, käsittely, analysointi sekä hälytykset tapahtuvat pilvipalvelussa. Tämä voi olla erityisen hyödyllistä, kun organisaatiolla on useita etätoimipaikkoja tai laajalle levinnyt infrastruktuuri, joka vaatii keskitettyä hallintaa ja valvontaa.

Azure-pilvipohjainen ratkaisu tarjoaa myös etuja, kuten skaalautuvuuden, joustavuuden ja helpon integroitavuuden muihin pilvipalveluihin. Lisäksi pilvipohjaiset ratkaisut voivat helpottaa päivityksiä ja ylläpitoa, koska ne voidaan toteuttaa keskitetysti pilvessä ilman, että jokaiseen paikalliseen laitteeseen tarvitsee tehdä erillisiä muutoksia.

On kuitenkin huomioitava, että tämä ratkaisu saattaa herättää huolenaiheita tietoturvasta ja yksityisyydestä, koska tiedot siirtyvät internetin kautta. Tämän vuoksi on tärkeää varmistaa, että tiedonsiirto on salattu ja käytettävät tietoturvaprotokollat ovat asianmukaiset. Sensori (kuvassa 10) voidaan siis yhdistää etäpaikoista suoraan Internetin

kautta Azuren Defender for IoT -portaaliin ilman, että tarvitsee käyttää yrityksen verkon reititystä.

Topologiakaavio OT-verkkoympäristöissä perustuu tyypillisesti Purdue-malliin, joka on ensimmäinen vaihe verkon segmentointiprojekteissa, jossa Purdue-tasot voivat toimia aloitusvyöhykkeinä segmentointia varten. Segmentointi on vain yksi osa monikerroksista puolustusstrategiaa. Kuvassa 11 esitetyssä Defender for IoT -ratkaisussa Purdue-mallin mukainen näkyvyys auttaa hahmottamaan, miten laitteet on kytketty toisiinsa ja niiden mahdolliset yhteydet IT-verkkoihin. Laitteet voidaan esittää digitaalisella kartalla eri värein ja suodattaa tunnisteiden perusteella, kuten käytetyt protokollat, kyselyvälit, vakioportit ja aliverkot.



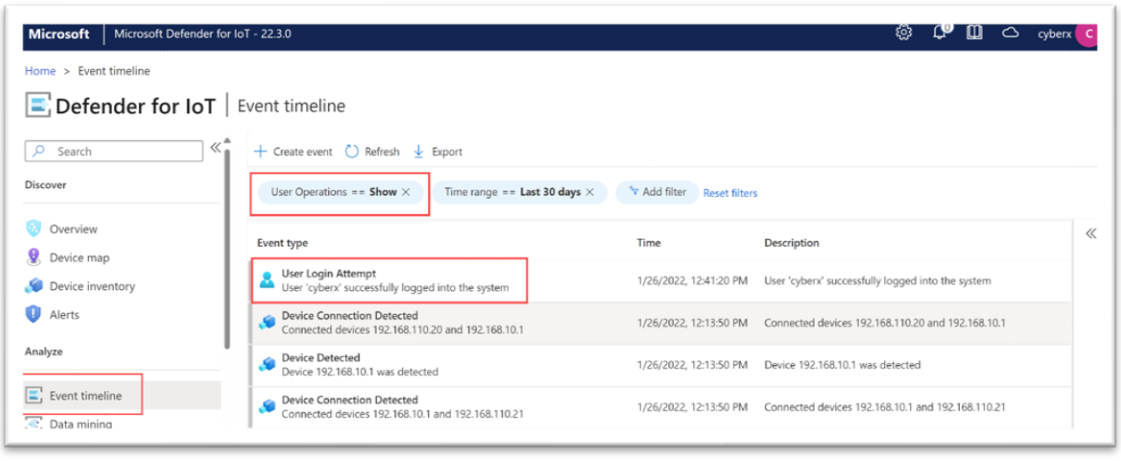
Kuva 11. Defender for IoT:n Purdue-näkymä laiteyhteyksistä. [34.]

Defender for IoT käyttää erikoistunutta OT-tietoista analytiikkaa kerätäkseen tietoa ympäristöstä. Tämän avulla ratkaisu pystyy tunnistamaan laitteen tila- ja kokoonpanotiedot, oppimaan normaalista verkon käyttäytymisestä ja hälyttämään haavoittuvuuksista tai tapahtumista, jotka saattavat viitata tietoturvaongelmaan.

Näin ollen Defender for IoT tarjoaa kattavan näkymän organisaation OT-verkkoon ja sen laitteisiin, mikä auttaa parantamaan tietoturvaa ja havaitsemaan mahdolliset ongelmat nopeasti. Tämän ansiosta yritykset voivat reagoida tehokkaammin tietoturvaongelmiin ja suojata kriittistä infrastruktuuriaan paremmin.

Defender for IoT hyödyntää patentoitua IoT- ja OT-tietoista käyttäytymisanalytiikkaa sekä Layer-7 Deep Packet Inspection (DPI) -tekniikkaa. Näiden avulla ratkaisu voi analysoida ja havaita paitsi perinteisiä allekirjoituspohjaisia uhkia, myös edistyneitä IoT- ja OT-uhkia, jotka perustuvat poikkeavaan tai luvattomaan toimintaan. Tämä laajentaa turvallisuusominaisuuksia ja auttaa paremmin suojaamaan kriittisiä laitteita ja järjestelmiä.

Hälytykset voidaan tarkastella Defender for IoT -hallintapaneelista tai tapahtumalokista. Ne voidaan ryhmitellä vakavuuden tai tyypin mukaan, mikä helpottaa hälytysten hallintaa ja priorisointia. Kuvassa 12 esitetty tapahtumalokinäkymä tarjoaa käsityksen tapahtumista ja hälytyksistä, jolloin organisaation tietoturva-asiantuntijat voivat nopeasti tunnistaa ja reagoida mahdollisiin uhkiin. [12.]



Kuva 12.Esimerkki tapahtumalokinäkymästä. [35.]

Toisin kuin Nmap (Network Mapper) ja muut skannerit, Defender for IoT käyttää passiivista verkkoliikenneanalyysia (NTA) tunnistamaan laitteet. Lisäksi voidaan nähdä, mi-

ten yhteydet muodostuvat IoT/OT-verkon kautta, sekä kuinka paljon jokainen laite kuluttaa kaistanleveyttä.

Defender for IoT -alusta ryhmittelee laitteistot automaattisesti ja niiden perusteella ominaisuudet (portit, protokollat, TCP-sovellustyyppi, valmistaja) ja luo yksityiskohtaisen verkon topologiakaavion. Defender for IoT tunnistaa myös aliverkkojen välisen liikenteen, joka voidaan helposti eristää IT/OT-segmenteistä ja valita, mitkä laitteet sijoitetaan demilitarisoidulle vyöhykkeelle (DMZ). [20.]

Microsoft Defender for IoT -alusta on vakaa ja turvallinen ja sen toiminnot ovat myös tehokkaita erityyppisten ja -muotoisten tietojen sujuvaan käsittelyyn. Tuotteen käyttöönotto on vaivatonta myös IT-käyttäjille, mikä mahdollistaa tietouhkien hallinnan ja pilvipalveluiden seurannan helposti.

Tietojen analytiikka tarjotaan reaaliajassa ja useiden kehitysprojektien dataraporttien hankkiminen tämän ohjelmiston kautta on tehokasta. Käyttöliittymän rakenne ja uhkien hallinta ovat siten hyviä tässä paketissa. Lisäksi Defender for IoT tarjoaa saumattoman integroinnin moniin SOC-työkaluihin yhtenäisen IT/OT-tietoturvan hallinnan varmistamiseksi.

Nykyaikaisen SOC:n on kyettävä korreloimaan kaikki hälytysten ympärillä esiintyneet sensoritiedot muihin lähteisiin täydellisen kuvan muodostamiseksi. Microsoft Defender for IoT -sensorilla on rajalliset valmiudet integroida tietonsa Azure Sentineliin, sillä sensorialusta tukee vain hälytysten lähettämistä Sentinelille.

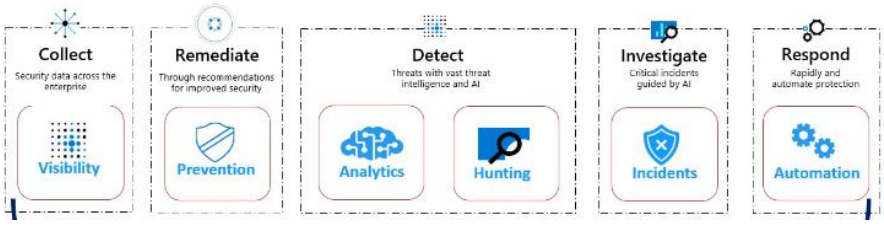
Tällä hetkellä sekä Microsoft Defender for IoT:n, että Microsoft Defender for Cloud:in ottaminen käyttöön Microsoft Sentinel -työtilassa samanaikaisesti voi johtaa päällekkäisiin hälytyksiin. Microsoft suositteleekin Microsoft Defender for Cloud -dataliittimen irrottamista ennen yhteyden muodostamista Microsoft Defender for IoT:iin. [17.]

8.3 Microsoft Sentinel

Tutkimuksessa oli vaatimuksena yhdistää Nozomi Networks ja Microsoft Defender for IoT Microsoft Sentineliin myöhempää käyttötarkoitusta varten tietoturvatiimeille helpottamaan kriittisten uhkien nopeaa löytämistä ja ratkaisemista.

Microsoft Sentinel, entinen Azure Sentinel, esiteltiin vuonna 2019 auttamaan organisaatioita modernisoimaan tietoturvatoimintoja pilvessä. Tuolloin tietoturvatyöryhmät, joilla oli paineita laajentaa kattavuutta kasvavaan digitaaliseen ympäristöön ja torjua lisääntyviä uhkia sekä parantaa tehokkuutta, alkoivat etsiä pilvestä vaihtoehtoja kalliille ja huonosti toimiville järjestelmille Tämä vähentää tarpeetonta työtaakkaa ja antaa enemmän aikaa reagoida organisaation todellisiin uhkiin. [21.]

Microsoft Sentinel käyttää skaalautuviin koneoppimisalgoritmeihin perustuvaa Fusion-korrelaatiomoottoria, joka havaitsee automaattisesti monivaiheiset hyökkäykset ja tunnistaa niistä yhdistelmät epänormaalista käyttäytymisestä tai epäilyttävästä toiminnasta. Sentinelin ratkaisu koostuu kuvan 13 toiminnoista: kohteen tunnistamisesta, uhkien havainnoinnista, näkyvyydestä ja uhkiin reagoimisesta. Ratkaisulla saadaan siten kokonaiskuva eri lokilähteistä, eli mitä ja missä milloinkin tapahtuu. Kokonaiskuvasta voidaan tunnistaa ja hallita yleisimpiä tietoturvapoikkeamia automaatioiden avulla. Sentineliä voidaan ajatella tällöin ratkaisuna, joka lisää SIEM-ominaisuuksia lokianalytiikkatyötilan päälle. [25.]



Kuva 13.Sentinel-arkkitehtuuri. [35.]

Microsoft Sentinel on suunniteltu vastaamaan nykyaikaisiin tietoturvahaasteisiin. Sen pääasiallinen toiminnallisuus ja älykkyys perustuvat sen saamiin lokitietoihin. Sentinel

käyttää valmiita liitäntöjä lokilähteiden tietojen vastaanottamiseen ja näkymien muodostamiseen. Sentinel sisältää oletusarvona Defender for IoT -dataliitännän, joka lähettää hälytykset Log Analytics -työtilaan toimenpiteitä varten.

Azure Analytics on välttämätön hälytysten korreloimiseksi tietoturvaryhmän havaitsemiin tapahtumiin. Heti käyttöönotettuna siinä on sisäänrakennetut mallit uhkien havaitsemissääntöjen määrittämiseksi ja automaattinen reagointi uhkiin. Uhkien havaitseminen, reagointi ja tutkiminen on Azure Analyticsin avulla tietoturvatoimintojen analyytikolle helpompaa. Kun kaikki olennaiset tiedot ovat yhdessä paikassa, voidaan tiedot korreloida nopeasti ja aloittaa korjaukset. Taulukossa 8 on lueteltu keskeisimmät Sentinellin vahvuudet. [26.]

Taulukko 8. Sentinelin vahvuuksia

• Pilvilaajuisen datan kerääminen käyttäjistä, laitteista, sovelluksista ja infrastruktuurista sekä paikallisesti että useista pilvistä.
• Tunnistaa uhkat ja minimoi vääriä positiivisia tuloksia käyttämällä Microsoftin analytiikkaa ja sen uhkatietokantaa.
• Tekoälyn käyttäminen uhkien tutkimiseen ja Microsoftin kyberturvallisuuskokemuksen hyödyntämiseen epäilyttävän toiminnan tunnistamiseen.
• Nopea reagointi tapahtumiin sisäänrakennetun orkestroinnin ja yleisen tehtäväautomaation avulla.

SIEM-alustat lähettävät tyypillisesti paljon tietoturvahälytyksiä niin suurilla volyymeillä, että tietoturvan hallintakeskus SOC voi niistä nopeasti ylikuormittua. Tällöin on riskinä, että tärkeät tapahtumat voivat jäädä huomiotta tai huomaamatta altistaen organisaation hyökkäyksille. Sentinel voi käyttää tehokkaita koneoppimisalgoritmeja automaatioalustan avulla automatisoidakseen vastaukset lukuisiin hälytyksiin ja tapahtumiin, joita SIEM vastaanottaa päivittäin. Sentinel korreloi hälytykset tapahtumiin ja tunnistaa

hyökkäykset lokitietojen perusteella. Haitallinen liikenne voidaan analysoida ja käsitellä nopeasti sisäänrakennetun automatisoinnin avulla. [20.]

Sentinelin toiminta pohjautuu siihen tuotuihin tietoturvatapahtumia sisältäviin lokitietoihin, joita se kerää käyttäjiltä, laitteilta, sovelluksilta ja infrastruktuurilta sekä useista pilvipalveluista. Sentinel sisältää huomattavan määrän valmiita liityntätapoja, joilla dataa voidaan tuoda nopeasti ja varmasti Sentinelin käsiteltäväksi. SIEM-ratkaisu ilman lokilähteitä on arvoton. Lokidatan sisään tuominen ratkaisun käytettäväksi on pakollinen vaatimus, jotta toimintoja voidaan hyödyntää. Lokimuodot vaihtelevat mutta monet lähteet tukevat CEF-pohjaista (Common Event Format) muotoilua. Tämä muoto sisältää enemmän tietoa kuin tavallinen Syslog-muoto ja esittää tiedot jäsennetyssä avainarvojärjestelyssä. Microsoft Sentinel -agentti, joka on itse asiassa Log Analytics -agentti, muuntaa CEF-muotoiset lokit muotoon, jonka Log Analytics voi ottaa vastaan ja lähettää ne edelleen Microsoft Sentinel -työtilaan.

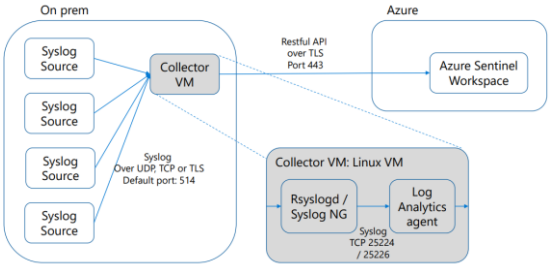
Päätelaitteissa, joihin ei voi asentaa Log Analytics -agenttia suoraan, on määritettävä Linux-palvelin lokien keräämiseen ja lähettämiseen Microsoft Sentinel -työtilaan. Linux-palvelin voidaan toteuttaa fyysisenä tai virtuaalisena laitteena paikallisessa konesaliympäristössä, Azuren virtuaalikoneessa tai toisessa pilvessä. Linux-palvelimessa on alla kuvatut kaksi osaa, jotka osallistuvat lokien siirtoprosessiin:

- Syslog daemon, joko rsyslog:ina tai syslog:na, jotka keräävät lokit
- Log Analytics Agent, joka välittää lokit Microsoft Sentinelille

Kuvassa 14 Log Analytics -agentti käyttää HTTPS-protokollaa yhdistääkseen Azure Sentinel -työtilaan ja välittääkseen tietoja eri Syslog-lähteistä. Microsoft Sentinel pystyy integroimaan minkä tahansa tietolähteen, joka tukee Syslog-protokollaa, ja tarjoaa reaaliaikaisen lokitietojen suoratoiston. Useimmat paikalliset tietolähteet hyödyntävät agenttipohjaista integraatiota yhteyden muodostamiseen.

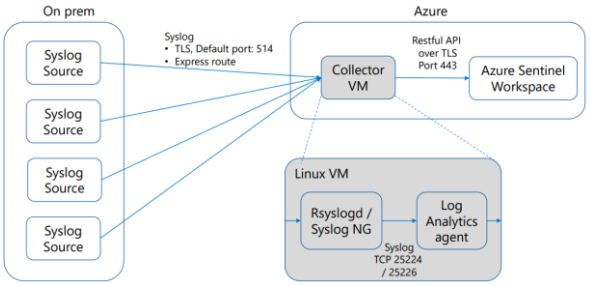
Tämä mahdollistaa tehokkaan seurannan ja tietoturvan hallinnan erilaisten tietolähteiden välillä, mikä parantaa organisaation kykyä havaita ja reagoida tietoturva-

tapahtumiin nopeasti. Azure Sentinel tarjoaa keskitetyn näkymän tietoturvatiedustelulle ja analysoinnille, mikä auttaa organisaatioita parantamaan tietoturvaansa ja vastaamaan nykypäivän monimutkaisiin uhkiin. [36].



Kuva 14. Syslog-viestit lähetään CEF-muodossa Azure Sentinelin työtilaan Syslog-agentin kautta [36.]

Toinen vaihtoehto on ohjata lokitiedot suoraan Azuren pilveen kuvan 15 mukaisesti, jolloin lokilähteet lähettävät Syslog- ja CEF-lokeja TLS:n kautta (koska esimerkiksi lokin edelleen lähettäjä on pilvessä). Tällöin käyttäjän on määritettävä Syslog-daemon (rsyslog tai syslog-ng) kommunikoimaan TLS:ssä. [36.]



Kuva 15. Lokitiedot suoraan Azure pilveen. [36]

Microsoft Sentinel automatisoi monia prosesseja, mikä auttaa nopeaan reagointiin ja vähentää SOC-tiimin hallinnollista ja analyyttistä taakkaa. Tavoitteena on vähentää laajalle levinnyt "valppausväsymys", jolla säännöllisesti ylityöllistään tietoturva-analyytikot.

Nykyään Sentinelillä ei ole kovin montaa käyttötapaa SIEM:nä IoT-ympäristöissä. Tämä johtuu pääasiassa siitä, että sisäänrakennetun IoT-dataliittimen nykyinen rajoitus ei synkronoi kaikkia Defender for IoT -hälytyksiä Sentineliin, ja tietyistä synkronoiduista hälytyksistä puuttuu tärkeitä metatietoja, kuten IP-osoite ja laitteen MAC-tiedot.

Elokuusta 2022 lähtien on ollut mahdollista ottaa Azure Monitoring Agent -agentti käyttöön automaattisesti. Tämän uuden parannuksen ansiosta on vihdoin mahdollista siirtyä kokonaan Microsoft Monitoring Agentista (MMA) ja siirtyä uuteen, moderniin Azure Monitoring Agentiin (AMA) Defender for Endpointille (MDE) ja Defender for Cloudille (MDC). Azure Monitoring Agent mahdollistaa useita etuja ja uusia ominaisuuksia.

9 Nozomi Networks

Nozomi Networks on yritys, joka on erikoistunut tarjoamaan teollisuuden ohjausjärjestelmiin (ICS) tarkoitettuja kyberturvallisuus- ja verkon näkyvyysratkaisuja. Yrityksen tarjoamat passiiviset verkkoliikenteen kerääjät (RC) käyttävät edistynyttä koneoppimista ja tekoälyä havaitakseen uhkia, tunnistaakseen omaisuutta ja haavoittuvuuksia sekä tarkastellakseen verkkoliikennettä kattavasti. Nozomi Networks on toiminut alalla vuodesta 2013 lähtien ja on tunnettu innovatiivisista ratkaisuistaan, jotka parantavat kyberturvallisuutta.

Yksi Nozomi Networksin tarjoamista tuotteista on Guardian™, joka tarjoaa laajan valikoiman tietoturvatoimintoja, kuten haavoittuvuuksien havaitsemisen ja arvioinnin, tunkeutumisen havaitsemisen, tietoturvatapahtumien hallinnan, tietoturva-analyysin ja raportoinnin. Guardian™ on suunniteltu erityisesti teollisuuden ohjausjärjestelmien tarpeisiin, auttaen parantamaan kriittisten järjestelmien kyberturvallisuutta ja varmistamaan niiden käytettävyyttä ja toimintavarmuutta. Guardian™ on erittäin joustava ratkaisu, sillä se voidaan ottaa käyttöön paikallisesti tai pilvessä, mikä tekee siitä sopivan monenlaisiin ympäristöihin ja käyttötarkoituksiin. Sen hyvä skaalautuvuus mahdollistaa sen käytön esimerkiksi öljy- ja kaasuteollisuudessa, voimalaitoksissa, vesihuollossa, logistiikassa ja monissa muissa kohteissa. Tämä tarkoittaa, että Guardian™ voi vastata monenlaisiin tarpeisiin ja vaatimuksiin, jotta voidaan tarjota tehokasta kyberturvallisuut-

ta ja parantaa verkon näkyvyyttä eri teollisuudenaloilla. Ratkaisut kattavat automatisoitujen teollisuuden ohjausverkkojen (IT, OT ja IoT) inventaarion, visualisoinnin ja valvonnan, jotka korvaavat manuaalisen työn tekoälyn käytön avulla. Reaaliaikainen näkyvyys parantaa verkon näkyvyyttä ja ymmärrystä verkon rakenteesta ja toiminnasta. Verkkokaaviosta saadaan virtuaalikuva, jonka avulla voidaan tunnistaa kunkin komponentin rooli, määrittää riskitaso sekä tunnistaa hyökkäykset (kuva 16).

Kuva 16. Nozomi Networks verkon visualisointikaavio kuva [38.]

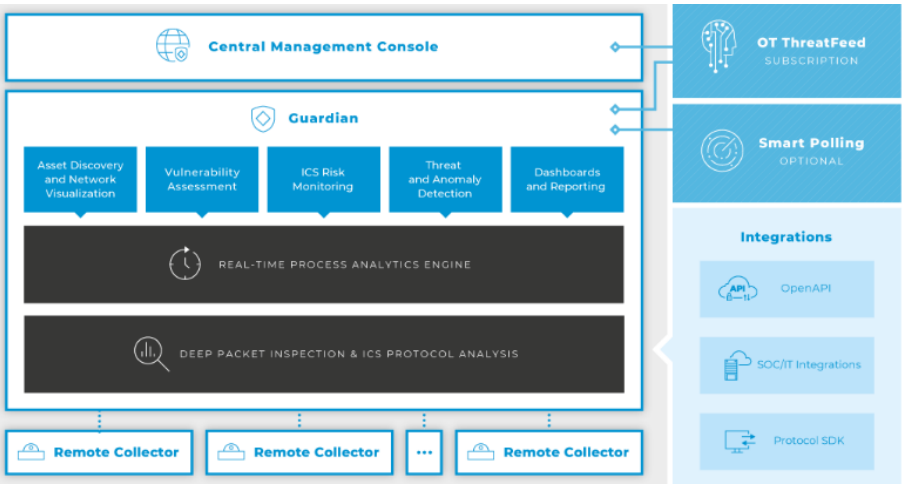
9.1 Nozomi Networks Arkkitehtuuri ja komponentit

Ratkaisu perustuu kuvan 17 mukaiseen modulaarisen arkkitehtuuriin. Sen toiminta perustuu reaaliaikaiseen tiedonkeruuseen sekä analysointiin, jotka mahdollistavat kattavan näkyvyyden teollisuusohjausverkkoihin. Tiedot kerätään Guardian-laitteilla, jotka voivat olla joko fyysisiä laitteita tai virtuaalikoneita, ja ne analysoivat ohjausjärjestelmän verkkoliikennettä edistyneen koneoppimisanalyysin avulla.

Kerätty tieto välitetään Nozomi Networks Central Management Console -hallintakonsoliin (CMC) tai Guardianiin, jotka tarjoavat käyttäjälle reaaliaikaisen näkyvyyden verkon tilaan ja mahdollistaa havaittujen uhkien nopean tunnistamisen ja korjaamisen.

CMC tarjoaa myös mahdollisuuden tarkastella historiatietoja ja raportteja, joita voidaan käyttää verkon tilan ymmärtämiseen ja suorituskyvyn parantamiseen.

Nozomi Networksin arkkitehtuuri on suunniteltu tukemaan sekä paikallista että pilvipohjaista käyttöä, jolloin käyttäjät voivat valita parhaiten heidän tarpeisiinsa sopivan toteutustavan. Lisäksi Nozomi Networksin arkkitehtuuri on suunniteltu integroitumaan muiden tietoturvaratkaisujen kanssa, jolloin käyttäjät voivat hyödyntää jo olemassa olevia järjestelmiään ja investointejaan. Se kerää reaaliaikaista tietoa ilman ulosmenevää liikennöintiä, joten se ei häiritse verkon suorituskykyä tai toimintaa.



Kuva 17. Nozomi Networksin ratkaisun modulaarinen arkkitehtuuri [36.]

- Central Management Console on valinnainen moduuli, jossa on keskitetty hallinta ja päivittyvä uhkatietokanta.
- Guardian analysoi passiivisesti verkon liikennettä.

Real-time Process Analytics Engine analysoi prosessinohjausmuuttujia, havaintoja haittaohjelmatoiminnasta ja kriittisistä tiloista, jotka voivat vaikuttaa luotettavuuteen ja toimintaan. Reaaliaikainen prosessianalyysimoottori on teknologia, joka mahdollistaa ohjausjärjestelmän reaaliaikaisen valvonnan ja analyysin. Moottori pystyy tunnistamaan anomaliat, riskit ja haavoittuvuudet, joiden avulla voidaan nopeasti reagoida mahdollisiin uhkiin. Prosessianalyysimoottori käyttää edistyksellisiä algoritmeja, koneoppimista ja tekoälyä tietojen analysoinnissa, jotta se voi tunnistaa hälyttävät tilanteet ja ilmoittaa

niistä välittömästi. Tämä auttaa käyttäjiä havaitsemaan ja ratkaisemaan tietoturvaongelmia ennen kuin ne aiheuttavat vakavia vaurioita ohjausjärjestelmälle tai tuotannolle.

Deep Packet Inspection Protocol Analysis

Yksityiskohtainen ICS-viestinnän analyysi OSI-mallin kaikilla seitsemällä tasolla. DPI on tekniikka, jota käytetään verkkoliikenteen syvälliseen tarkasteluun ja analysointiin. Nozomi Networksin DPI-moottorit analysoivat verkkoliikennettä havaitakseen poikkeavuuksia, haittaohjelmia ja muita uhkia. DPI mahdollistaa tarkat ja reaaliaikaiset havainnot verkkoliikenteestä. Toiminto on tärkeä osa Nozomi Networksin ratkaisua, joka auttaa varmistamaan teollisuudenohjausjärjestelmien turvallisuuden ja suorituskyvyn.

Remote Collector

Sensori on liikenteen tietojen keräämiseen keskittyvä laite, joka toimii passiivisena verkkoliikenteen kerääjänä teollisuusverkoissa. Sensorit on suunniteltu asennettaviksi teollisuusverkkoon, jossa ne keräävät verkkoliikenteen tiedot eri lähteistä. Näitä lähteitä voivat olla esimerkiksi kytkimet, reitittimet ja muut verkkolaitteet. Sensorien tarkoituksena on kerätä ja lähettää verkkoliikenteen tiedot keskitettyyn hallinta- ja analysointiyksikköön (CMC) tai Guardian-laitteeseen. Tässä yksikössä tiedot analysoidaan ja tallennetaan jatkokäsittelyä ja raportointia varten.

Nozomi Networks Smart Polling™

Ohjelmiston lisäosa, joka on suunniteltu auttamaan organisaatioita tunnistamaan tietoturvaongelmat ja haavoittuvuudet. Smart Polling kerää laajaa tietoa kaikista verkon resursseista, mukaan lukien käyttöjärjestelmä, laiteohjelmisto, korjaustiedostot ja asennetut ohjelmistot. Tämän tiedon avulla organisaatio voi tunnistaa haavoittuvuuksia ennen niiden hyödyntämistä, mikä parantaa tietoturvaa ja vähentää riskiä. Smart Polling tunnistaa myös ympäristöön kuulumattomat laitteet ja omaisuudet, mikä auttaa organisaatiota varmistamaan, että vain tunnetut laitteet ovat yhteydessä verkkoon. Lisäksi Smart Polling mahdollistaa tarkan haavoittuvuuden arvioinnin, mikä helpottaa nopeaa ja tehokasta reagointia mahdollisiin uhkiin.

Asset Intelligence™

Asset Intelligence™ auttaa organisaatioita tunnistamaan keskeiset tietoturvahälytykset OT- ja IoT-tapahtumista. Se hyödyntää Guardianin sensorien havaitsemistekniikkaa, joka päivittyy reaaliajassa IT- ja OT-laitetietoihin perustuen. Tämä mahdollistaa tärkeiden tietoturvahälytysten tunnistamisen ja turhien hälytysten vähentämisen jopa 70 prosentilla, mikä auttaa organisaatioita keskittymään olennaisiin OT- ja IoT-tapahtumiin ja reagoimaan niihin nopeammin

Tämä työkalu tarjoaa syvällisemmän käsityksen verkon laitteista ja resursseista, mahdollistaen poikkeavuuksien ja tietoturvariskien varhaisen havaitsemisen. Se analysoi jatkuvasti verkon tapahtumia ja tarjoaa reaaliaikaista näkemystä tietoturvaympäristön tilasta. Lisäksi se sisältää monipuolisen valikoiman muita työkaluja, kuten haavoittuvuuksien hallinnan, uhkien arvioinnin ja reagointisuunnitelmien laatimisen, jotka auttavat organisaatioita parantamaan tietoturvaa ja vähentämään riskejä.

Nozomi Guardian™ -analyysi

Nozomi Networksin kehittämä Nozomi Guardian™ -analyysi on reaaliaikainen prosessianalyysi, joka hyödyntää koneoppimista ja tekoälyä teollisuuden ohjausjärjestelmien (Industrial Control Systems, ICS) tietoturvan parantamiseksi. Analyysi perustuu verkkoliikenteen syvälliseen tarkasteluun, joka tunnistaa normaalit ja poikkeavat toimintatilat sekä havaitsee mahdolliset uhkat ja hyökkäykset. Guardian™-analyysi auttaa organisaatioita havaitsemaan ja torjumaan häiriöitä, parantamaan järjestelmän käytettävyyttä ja luotettavuutta sekä suojaamaan kriittisiä laitteita ja infrastruktuuria. Lisäksi se mahdollistaa syvällisen diagnostiikan ja hienovaraisten ongelmien tunnistamisen, mikä edistää tehokasta tietoturvan hallintaa ja kyberhyökkäysten ehkäisyä ICS-ympäristöissä.

Nozomi Guardian™ -analyysi tarjoaa kattavan näkymän ohjausjärjestelmänverkkoihin ja auttaa organisaatioita vahvistamaan puolustuskykyään sekä suojaamaan toimintansa jatkuvuutta.

Yara-säännöt

Yara-säännöt ovat työkaluja, joita käytetään haittaohjelmien tunnistamiseen ja analysointiin. Ne perustuvat haittaohjelmien käyttämiin taktiikoihin sekä tekniikoihin ja auttavat havaitsemaan epäilyttäviä toimintoja verkkoliikenteessä. Ne ovat joko käyttäjän määrittelemiä tai valmiita sääntöjä, joita voidaan soveltaa eri käyttötapauksiin. Säännöt voivat tunnistaa erilaisia haittaohjelmia, kuten troijalaisia, matoja ja muita uhkia. Niiden käyttö edellyttää kuitenkin tietämystä haittaohjelmien toiminnasta ja tunnusmerkeistä, jotta säännöt voidaan määritellä oikein ja saada mahdollisimman tarkkoja tunnistuksia. Tietoturva asiantuntijat voivat hyödyntää Yara-sääntöjä haittaohjelmien tunnistamisessa, jolloin ne auttavat nopeuttamaan ja tehostamaan haittaohjelmien analysointia. Yara-säännöt ovat myös avointa lähdekoodia ja ilmaisia käyttää, joten ne ovat kätevä työkalu tietoturvayhteisöille.

Packet-säännöt

Packet-säännöt ovat Nozomi Guardian -ratkaisun kolmas analyysimenetelmä, jossa sääntöjen avulla käyttäjä voi määrittää sääntökriteerin vastaamaan haitallista pakettia, jonka perusteella Guardian siten voi havaita potentiaalisia uhkia. Nozomi tarjoaa valmiita Packet-sääntöjä, jotka kattavat yleisimmät ja tunnetuimmat uhkat ja hyökkäysvektorit.

Näitä sääntöjä voidaan myös laajentaa käyttäjän tarpeiden mukaan. Packet-säännöt ovat hyödyllisiä haitallisten pakettien tunnistamisessa, koska ne voivat havaita tietyn protokollan tai verkkoliikenteen ominaisuuksia, jotka ovat yhteisiä tietyille uhkille. Esimerkiksi Packet-säännön avulla voidaan havaita haitallinen liikenne, joka käyttää tiettyä porttia tai tiettyä tiedonsiirtoprotokollaa, tai joka sisältää tiettyjä merkkijonoja tai kuvioita.

STIX (Structured Threat Information eXpression)

Neljäntenä uhkien havaitsemismenetelmänä Nozomi Networks Guardian käyttää STIX-sääntöjä, joiden avulla se voi tunnistaa, analysoida ja jakaa tietoturvaa uhkaavia tietoja

tehokkaasti ja järjestelmällisesti. STIX on kyberturvallisuuden standardi, joka on suunniteltu auttamaan organisaatioita jakamaan tietoturvaa uhkaavia tietoja ja tunnistamaan hyökkäysvektoreita. STIX-sääntöjen avulla Guardian voi paremmin ymmärtää erilaisia uhkakuvia ja havaita niitä aikaisemmin, mikä auttaa organisaatioita reagoimaan nopeasti mahdollisiin hyökkäyksiin ja vähentämään niistä aiheutuvia riskejä. Nozomi Networks Guardianin STIX-säännöt mahdollistavat erilaisten uhkien, kuten haittaohjelmien, haavoittuvuuksien ja muiden hyökkäystapojen tunnistamisen. Tämä tarkoittaa, että Guardian pystyy tunnistamaan ja reagoimaan laajempaan kirjoon uhkia kuin monet muut tietoturvatuotteet. Lisäksi STIX-sääntöjen avulla Guardian voi hyödyntää yhteisön laatimia tietoturva-analyyseja, joiden avulla se voi pysyä ajan tasalla uusista uhkista ja parantaa niiden tunnistamista.

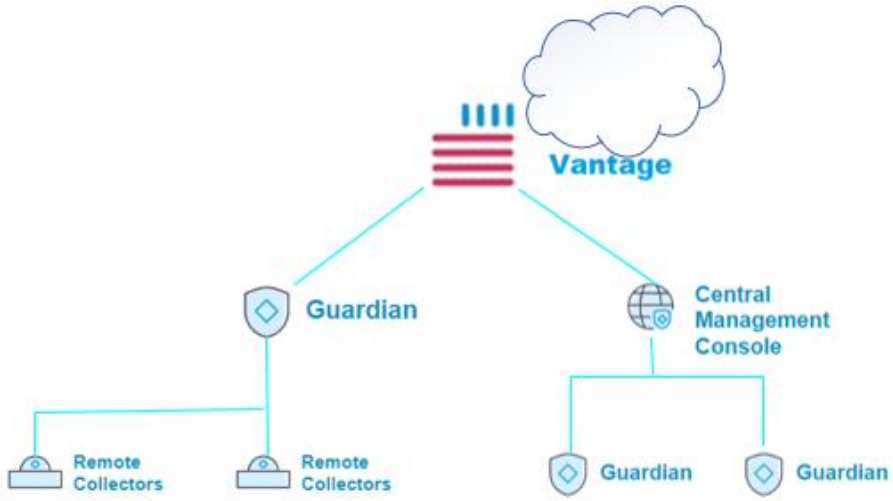
Guardianin STIX-sääntöjen avulla voidaan määrittää ja hallita tietoturvakäytäntöjä tehokkaammin sekä hyödyntää tietoturvayhteisön asiantuntemusta. Tämä auttaa parantamaan organisaation kykyä tunnistaa ja reagoida uhkiin sekä suojata kriittistä infrastruktuuria ja laitteita. Tämän seurauksena Nozomi Networks Guardianin STIX-säännöt voivat tarjota organisaatioille tehokkaan ja joustavan tavan parantaa tietoturvaa ja suojata tärkeitä teollisuusverkkoja ja IoT-laitteita.

9.2 Nozomi Vantage SaaS -pilvi

Nozomi Networks Vantage™ on vuonna 2021 julkistettu pilvipohjainen kyberturvallisuusratkaisu, joka perustuu SaaS-arkkitehtuuriin (Software as a Service). Tämä tarkoittaa, että Vantage on ohjelmisto, joka toimitetaan ja käytetään pilvipalveluna, eikä sitä asenneta käyttäjän omalle laitteelle. Vantage tarjoaa tehokasta data-analytiikkaa, joka parantaa merkittävästi kyberturvallisuutta ja näkyvyyttä. Alusta on suunniteltu vastaamaan nopeasti kehittyvien IoT-yhteensopivien infrastruktuurien vaatimuksiin ja tarjoaa tekoälypohjaisen ratkaisun riskien tunnistamiseksi ja hallitsemiseksi.

Vantageen voidaan lähettää tietoja kahdella tavalla: Guardian-sensorit lähettävät tietoja Vantagelle pilvestä konsolidoitua hallintaa varten mistä tahansa ja milloin tahansa.

CMC-laitteet voivat lähettää tietoja suoraan Vantagelle datan analysointia varten verkon reunalla tai julkisessa pilvessä (kuva 20).



Kuva 18. Tiedot Vantageen voidaan lähettää kahdella tavalla.

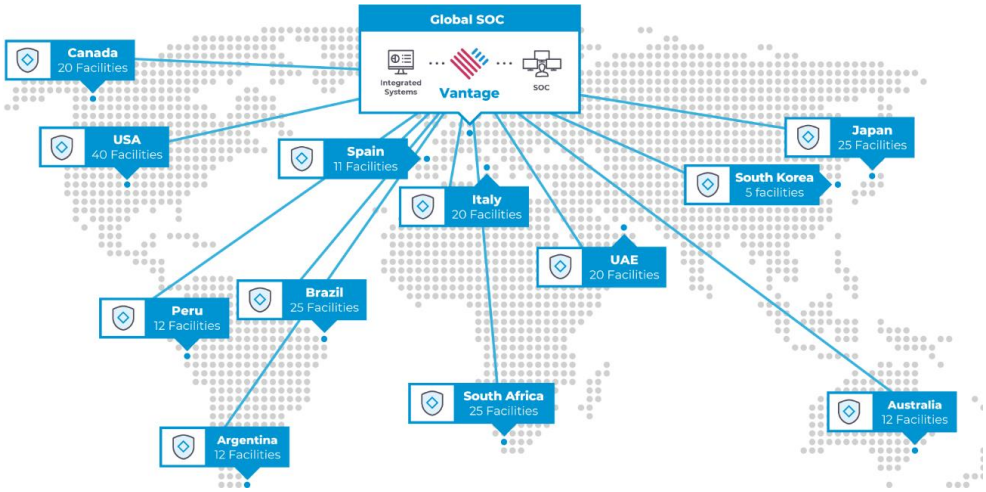
Yksi Vantagen merkittävimmistä piirteistä on sen monipuolinen tietojen keruu ja analysointi. Alusta hyödyntää koneoppimista ja tekoälyä tunnistamaan ja ennakoimaan kyberuhkia sekä poikkeamia laitteiden ja verkkoyhteyksien toiminnassa. Tämän avulla voidaan paremmin suojautua monimutkaisilta ja kehittyneiltä kyberhyökkäyksiltä, jotka saattavat kohdistua kriittisiin infrastruktuureihin. Vantage-ratkaisun joustavuus ja helppo integrointi erilaisten toimittajien järjestelmiin mahdollistavat keskitetyn tietoturvan, näkyvyyden ja verkkovalvonnan. Tämä parantaa hallinnan joustavuutta ja mahdollistaa resurssien tehokkaamman käytön.

Lisäksi Vantage tarjoaa monipuoliset raportointi- ja visualisointityökalut, jotka auttavat käyttäjiä ymmärtämään verkon tilan ja tekemään tietoon perustuvia päätöksiä. Näitä ovat muun muassa reaaliaikainen näkymä verkon tilaan, hälytyslokit, raportit uhkien havaitsemisesta ja yksityiskohtaiset kuvaukset havaituista uhkista.

Vantage-alustan Asset Intelligence -ominaisuus mahdollistaa tarkemman havainnoinnin poikkeamista, mikä auttaa nopeaan reagointiin ja tehokkaampaan kyberuhkien hallintaan. Vantage on suunniteltu helposti skaalautuvaksi, jolloin se pystyy helposti seu-

raamaan suuria määriä OT- ja IoT-laitteita nopeasti muuttuvissa ympäristöissä. Tämä mahdollistaa Vantagen käytön useiden toimittajien ympäristöissä ja parantaa hallinnan joustavuutta. Vantage-alusta on helppo ottaa käyttöön ja ylläpitää, sillä se toimii pilvestä lähes maksuttomasti tarjoten jatkuvaa ylläpitoa.

Vantagen lähes rajoittamattoman skaalautuvuuden ansiosta sillä voidaan helposti seurata suuria määriä OT- ja IoT-laitteita nopeasti muuttuvissa ympäristöissä. Merkityksellistä on, että Vantage-alusta skaalautuu useiden toimittajien ympäristöihin keskitetyn tietoturvan, näkyvyyden ja verkkovalvonnan ansiosta ja parantaa siten hallinnan joustavuutta (kuva 21).

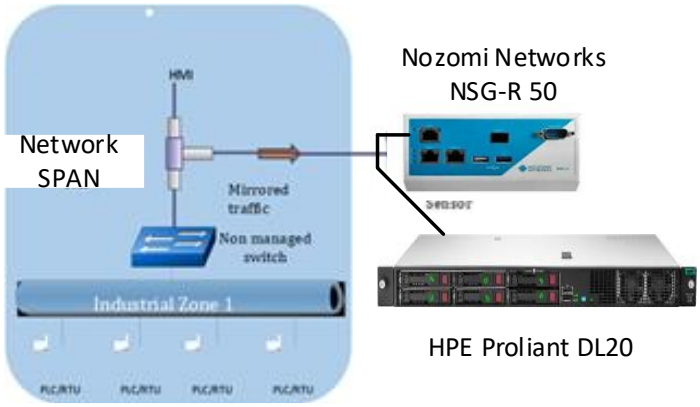


Kuva 19.Vantagella voidaan hallinnoida Guardianeja mistä tahansa. [36.]

Yhteenvetona voidaan todeta, että Guardian ja Vantage-alustojen avulla voidaan havaita ja torjua kyberuhkia reaaliaikaisesti ja vähentää merkittävästi riskiä laitteiden, prosessien ja ihmisten turvallisuudelle. Lisäksi Nozomin skaalautuvat ja helppokäyttöiset ratkaisut helpottavat tietoturvan hallintaa ja ylläpitoa, mikä säästää aikaa ja rahaa. Vantage mahdollistaa myös tietoturvatietojen jakamisen kumppaneiden, toimittajien ja muiden sovellusten kanssa keskitetystä pilvivarastosta avaamatta verkkoa ulkoisille käyttäjille. Sen liittymähinnoittelu helpottaa kustannusten skaalaamista ja hallintaa vaatimusten kasvaessa.

10 Tutkimustulokset

Verkkoliikenteen analysointiin käytettiin Nozomi Networksin NSG-R 50 -keräintä ja Microsoftin HPE Proliant DL20 -palvelinta, jotka asennettiin sähköaseman verkkokytkimen SPAN-peiliportteihin. Tämä mahdollisti tarkan verkkoliikenteen analysoinnin ja potentiaalisten tietoturvariskien havaitsemisen (kuva 20).



Kuva 20. Liikenteen analysoinnin toteutus SPAN-peiliportin kautta.

Molemmat ratkaisut hyödynsivät tekoälyä ja koneoppimista ICS-mallinnuksessaan. Oppimisvaiheessa ne pystyivät rakentamaan tarkan käyttäytymismallin, joka sisälsi tiedot laitteista, havaitut protokollat ja tiedostonsiirrot laitteiden välillä. Oppimistilan aikana molemmat ratkaisut oppivat normaalin käyttäytymisen kuuden viikon ajanjakson aikana, jonka jälkeen oppimistila poistettiin käytöstä. Tämän jälkeen poikkeamat opitusta liikenteestä laukaisivat hälytyksiä. Kun oppimisjakso oli päättynyt ja oppimistila oli poistettu käytöstä, sensorit saattoivat havaita epätavalliset korkeat perusmuutokset, jotka johtuivat normaalista IT-toiminnasta, kuten DNS- ja HTTP-pyynnöistä. Tämä saattoi aiheuttaa tarpeettomia hälytyksiä ja järjestelmäilmoituksia, mutta molemmat ratkaisut paransivat tarkkuuttaan viimeisimmissä ohjelmistoversioissaan, joissa oppiminen ja suojaukseen siirtyminen tapahtuu automaattisesti.

Tarpeettomien hälytysten ja ilmoitusten määrän vähentämisen hoitavat Nozomin Networks Dynamic Learning ja Microsoftin Smart IT Learning -toiminnot. PoC-testauksien jälkeen verkkoyhtiön kanssa käytiin yhdessä läpi tulosten yhteenveto (kuva 21).

Kuva 21. POC testauksen yhteenveto.

10.1 Laitteiden tunnistaminen ja löytyminen

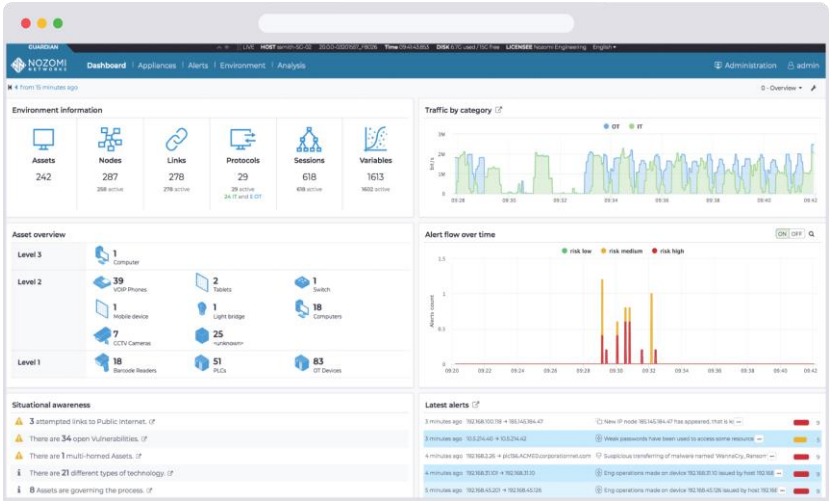
Sensorit oli asennettu alueelliseen sähkökeskukseen keräämään tietoja operatiivisesta verkosta, josta molemmat laitteet löysivät 48 verkko- ja OT-päätelaitetta. Laitteiden skannaus tapahtui passiivisesti ilman laitteiden aktiivista kyselyä. Molempien ratkaisujen verkkoselainpohjaiset, graafiset käyttöliittymät tarjosivat hyvän yleiskuvan verkosta, prosesseista, hälytyksistä, raporteista ja haavoittuvuuksista reaaliajassa. Laajensimme testiä lisäämällä VXLAN-liikenteen samoihin SPAN-portteihin, jotka olivat jo kytkettyinä Nozomin ja Microsoft Defender for IoT -laitteisiin. Saimme näin kerättyä liikennettä segmenteistä, joiden liikenne reititetään erikseen samassa laitteessa, johon OT-laitteet olivat kytkettyinä. VXLAN:in kautta kerätty liikenne ei sisällä päätelaitteiden MAC-osoitteita, minkä takia yksinkertainen MAC-osoitteen perusteella oleva tunnistaminen ei ole mahdollista. Tämä johtaa siihen, että Nozomin on kuunneltava liikennettä tavallista pidempään pysyäkseen määrittelemään ja profiloimaan päätelaitteet. Paras vaihtoehto helpottaa ja nopeuttaa tunnistamista on hakea OT-laitevalmistajan automaatiohallintajärjestelmästä tämän tunnistamattoman päätelaitteen konfiguraatiotiedot, ja ladata ne manuaalisesti Nozomille. Nozomi tunnistaa liikennöivän laitteen IP-osoitteen perusteella ja rikastaa tietokantaansa laitteen muut omaisuustiedot, kuten MAC-osoitteen ja sarjanumerotiedot. Nozomi Networks löysi 487 laitetta mutta laajennettua testiosuutta emme pystyneet suorittamaan Defender for IoT:lla, koska se ei vielä tukenut VXLAN-liikennettä.

Käytimme tasapuoliseen arviontiin testin tuloksia ilman VXLAN:ia.

10.2 Käyttöliittymät

Käyttöliittymät tarjoavat helpon tavan tarkastella ja valvoa verkkoa. Yhtenäinen näkymä kaikista resursseista ja niiden toiminnasta auttaa havaitsemaan poikkeamat ja mahdolliset ongelmat nopeasti. Käyttöliittymien avulla voidaan myös seurata liikennettä ja tunnistaa hälytykset, jotka voivat osoittaa verkkoturvariskin. Tämä auttaa varmistamaan, että verkko toimii tehokkaasti ja turvallisesti.

Nozomi Networksin käyttöliittymän (kuva 22) avulla käyttäjä voi tarkastella haavoittuvuuksia, poikkeamia ja muita turvallisuusriskejä koko verkossa tai yksittäisissä laitteissa. Järjestelmä tarjoaa automaattiset havainnot, jotka tunnistavat yksittäisten laitteiden tai koko verkoston haavoittuvuudet. Lisäksi käyttäjä voi seurata aktiivisia uhkia ja havainnoida, miten järjestelmä vastaa niihin.

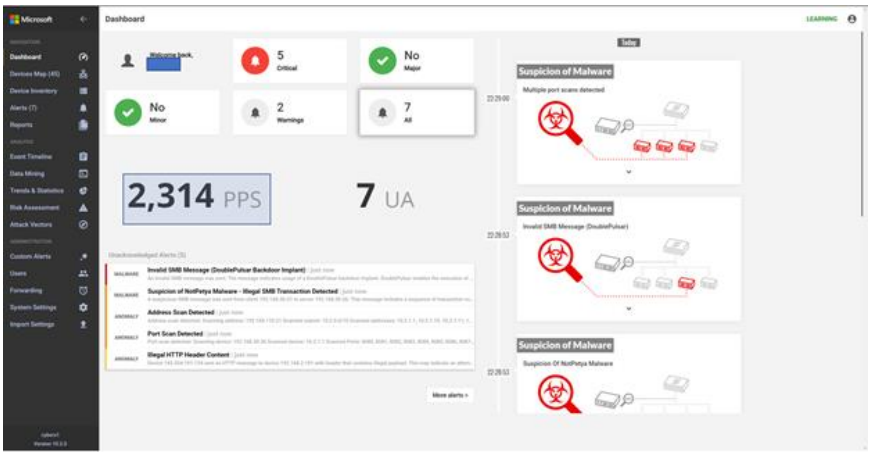


Kuva 22. Kuvassa on esimerkki Nozomi Networksin käyttöliittymän pääsivusta. [48.]

Nozomi Networksin käyttöliittymä mahdollistaa myös useiden hälytysten ja ilmoitusten luomisen. Esimerkiksi käyttäjä voi luoda hälytyksiä yhteyksistä, jotka ylittävät tietyt kynnysarvot, tai laitteiden toiminnasta, joka poikkeaa normaalista käytöksestä. Tämä aut-

taa käyttäjiä havaitsemaan ja reagoimaan nopeasti poikkeamiin ja muihin turvallisuusriskeihin.

Microsoft Defender for IoT:n käyttöliittymä (kuva 23) tarjoaa myös kattavan yleiskuvan koko verkosta. Käyttöliittymässä on graafisia esityksiä verkosta, hälytyksistä ja tärkeimmistä turvallisuusindikaattoreista. Käyttäjä voi myös tarkastella tiettyjen laitteiden turvallisuustilaa ja nähdä niiden yksityiskohdat, kuten käyttöjärjestelmän version ja laitteeseen liittyvät ohjelmistot.



Kuva 23. Defender for IoT -käyttöliittymän pääsivu. [41.]

Microsoft Defender for IoT -ratkaisu tarjoaa mahdollisuuden luoda käyttäjäkohtaisia mukautettuja näkymiä, joissa näytetään tietoa tärkeimmistä laitteista, haavoittuvuuksista ja hälytyksistä. Käyttäjät voivat myös määrittää hälytykset, jotka lähetetään automaattisesti sähköpostitse tai tekstiviestinä, kun tiettyjä ehtoja täyttyy. Lisäksi ratkaisussa on mahdollisuus määrittää automaattisia toimintoja, jotka käynnistyvät tiettyjen hälytysten tai tapahtumien yhteydessä, esimerkiksi automaattinen laitteen eristäminen verkon ulkopuolelle. Kaiken kaikkiaan Microsoft Defender for IoT tarjoaa käyttäjille helppokäyttöisen ja automatisoidun ratkaisun, joka auttaa vähentämään turvallisuusriskejä ja mahdollistaa nopean reagoinnin mahdollisiin uhkiin.

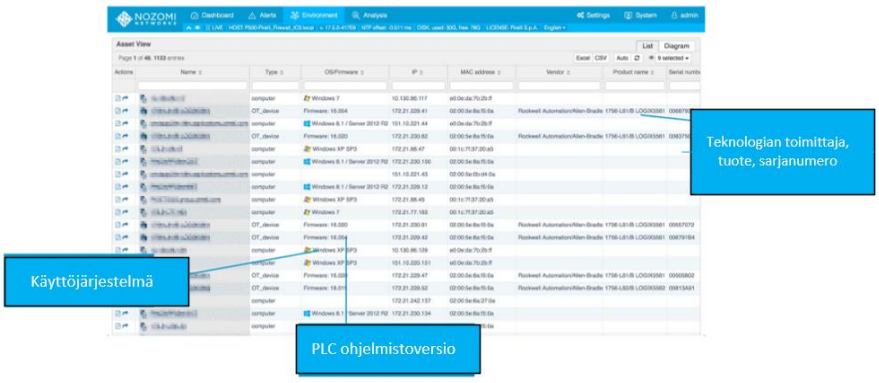
Kokonaisuudessaan molemmat ratkaisut tarjoavat hyvän näkyvyyden tietoturvatapahtumiin ja mahdollistavat nopean havaitsemisen ja reagoinnin uhkiin. Käyttöliittymät ovat

selkeitä ja helppokäyttöisiä, ja ne tarjoavat mahdollisuuden tarkastella verkon toimintaa eri tasoilla ja yksityiskohtaisesti.

10.3 Automaattinen omaisuuden löytyminen

Nozomi Networksin havainnot osoittavat, että päätelaitteiden tiedot olivat osittain saatavilla, mutta VXLAN-kytkennän vuoksi niiden MAC-osoitteet eivät sisältyneet liikenteeseen. Passiivinen skannaus ei myöskään pystynyt keräämään kaikkia sarjanumeroita eikä päätelaitteiden rooleja, koska ne sijaitsivat eri vyöhykkeiden VLAN-verkoissa.

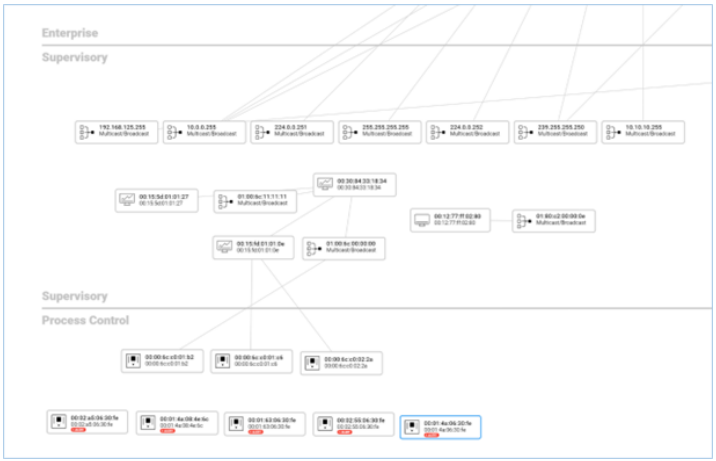
Kuitenkin haavoittuvuustiedot, ohjelmistot ja ohjelmiston päivitykset pystyttiin tunnistamaan. Tämän tiedon voi löytää käyttöliittymän Assets-valikosta, josta esimerkkilistaus löydetyistä laitteista kuvassa 24. Tämä auttoi parantamaan ymmärrystä laitteiden välisistä yhteyksistä ja tietoliikenteestä niiden välillä, vaikka tarkkaa MAC-osoite- ja roolitietoa ei ollut käytettävissä. Tieto on arvokasta verkkojen toiminnan ja tietoliikenteen analysoinnissa sekä turvallisuuden parantamisessa.



Kuva 24. Esimerkki: Asset Inventory -laitelistauksesta. [46.]

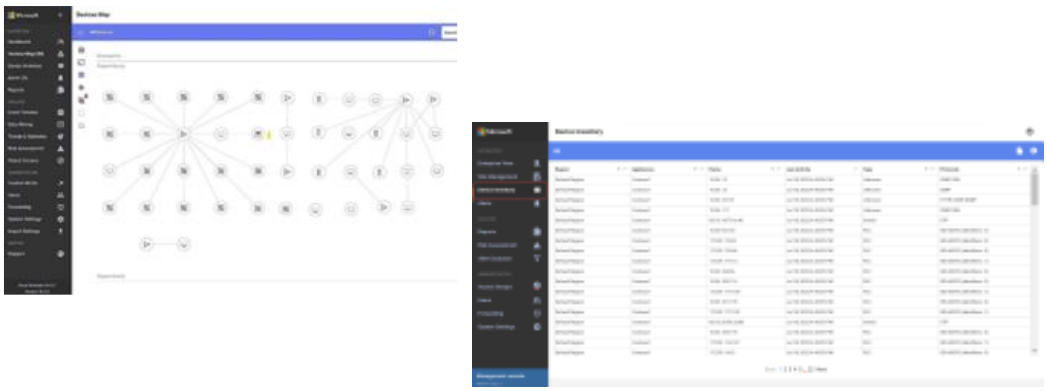
Microsoft Defender for IoT:n käyttöliittymän Asset Map -kartta (kuva 25) on tehokas ja helppokäyttöinen työkalu, joka auttaa visualisoimaan ja hallitsemaan verkon resursseja ja laitteita. Kartta on keskeinen väline tarjoten havainnollisen kuvan verkon komponen-

teista ja niiden välisestä vuorovaikutuksesta Purdue-mallin mukaan. Se mahdollistaa nopean reaktion tietoturvauhkiin, edistäen tehokasta ja kattavaa tietoturvan ylläpitoa.



Kuva 25. Esimerkki: Defender for IoT Asset Map. [19.]

Asset Map -kartta esittää nämä tasot eri värein ja ikonein, jolloin käyttäjät voivat helposti havaita ja erottaa eri laitetyypit ja resurssit. Kartta myös näyttää laitteiden väliset yhteydet, jotta käyttäjät voivat nähdä, miten tieto liikkuu eri tasojen välillä ja miten laitteet kommunikoivat keskenään. Käyttöliittymän laiteinventaarion (Device Inventory, kuva 26) avulla saadaan tärkeää lisätietoa laiteluettelosta, joka auttaa organisaatioita tunnistamaan resurssien keskinäisen kommunikoinnin ja keräämään arvokasta tietoa laitteista, jotka voivat kommunikoida OT-verkosta internetiin.

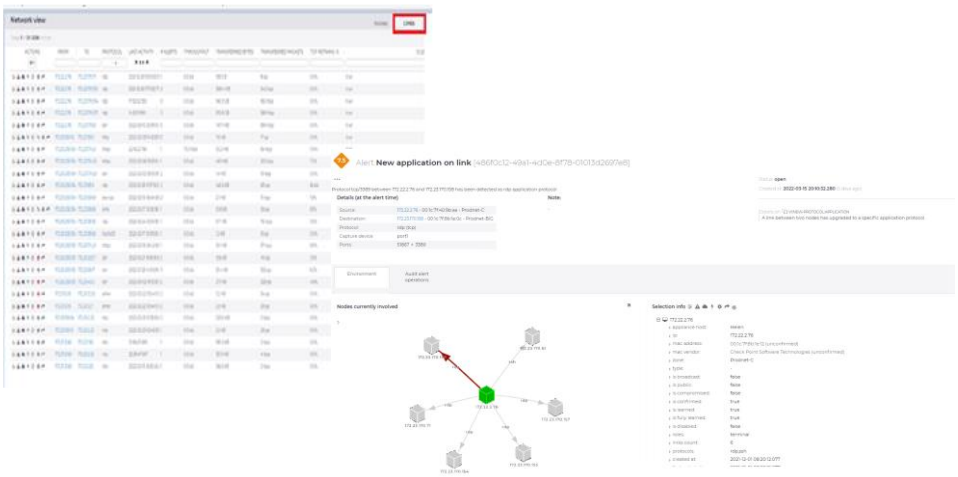


Kuva 26.Tarkennetut tiedot: Defender for IoT Device inventory Map. [43.]

Vaikka Asset Map -kartta ei pysty keräämään täydellisesti päätelaitteiden MAC-osoitteita, se tarjoaa kuitenkin selkeän ja helposti ymmärrettävän näkymän ICS-verkon tilasta ja mahdollisista uhkista. Tämä auttaa reagoimaan nopeasti mahdollisiin ongelmiin ja estämään vakavammat häiriöt tai vahingot verkoille Asset Inventory Map tunnistaa IT-, OT- ja IoT-laitteita, joista IT-osasto ei ehkä ole virallisesti tietoinen, jolloin se auttaa tietoturvatiimejä tunnistamaan verkon topologian ja arkkitehtuurin perusteella ympäristön yksittäiset vikakohdat. Saamme tällöin myös tiedon, mihin muihin päätelaitteisiin tai osoitteisiin laite on ollut viimeksi yhteydessä, sekä tiedot, milloin se on ensimmäisen kerran ilmestynyt näkyviin ja milloin viimeksi ollut aktiivinen. Defender for IoT tuo graafisesti paremmin esille Purdue-mallin ja siihen liittyvät tasot kuin Nozomin ratkaisu, josta on esimerkkitapaus kuvassa 27.

10.4 Linkit (Links)

Nozomi Networks linkit ovat point-to-point-yhteyksiä kahden eri laitteen eli assetin välillä. Linkit voivat olla OSI 2 -tason tai OSI 3 -tason yhteyksiä, jotka muodostavat protokollan tai protokollien kautta yhteyden kahden eri laitteen välille. Mielenkiintoiset tiedot kuten aikaväli, tiedon määrä, tiedon nopeus ja tiedon eheys ovat muun muassa listattuna links-osiossa (kuva 27).

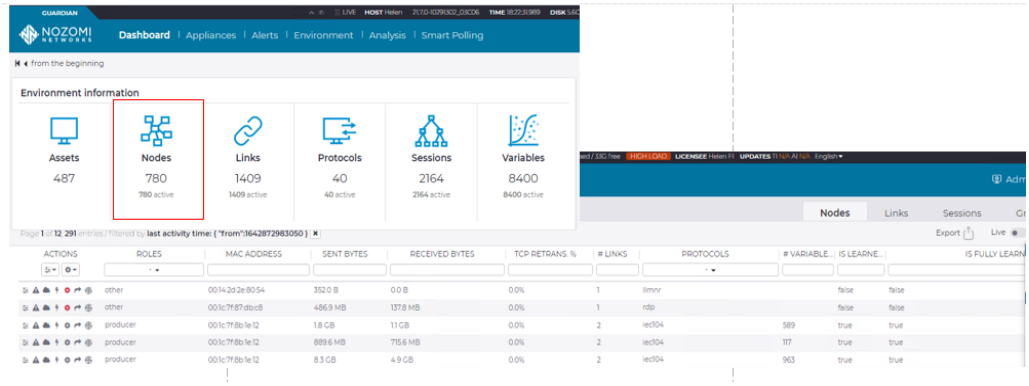


Kuva 27. Esimerkki Nozomi Networksin linkkinäkymästä.

Defender for IoT:n tärkeä ominaisuus on sen kyky analysoida verkkoliikennettä. Tämä analyysi perustuu tiedonlouhintaan (Data Mining) ja SPAN-portista kerättyihin liikennetietoihin. Tämä tarkoittaa sitä, että Defender for IoT ei valvo linkkejä suoraan, vaan sen sijaan se analysoi verkkoliikennettä havaitakseen mahdollisia tietoturvauhkia. Lisäksi Defender for IoT:n passiiviset laitteet luokitellaan ei-aktiivisiksi laitteiksi, jos ne ovat olleet passiivisina yli 60 päivää. Tämä auttaa varmistamaan, että vain aktiiviset laitteet ovat suojattuina tietoturvariskeiltä.

10.5 Liityntäpisteet (Nodes)

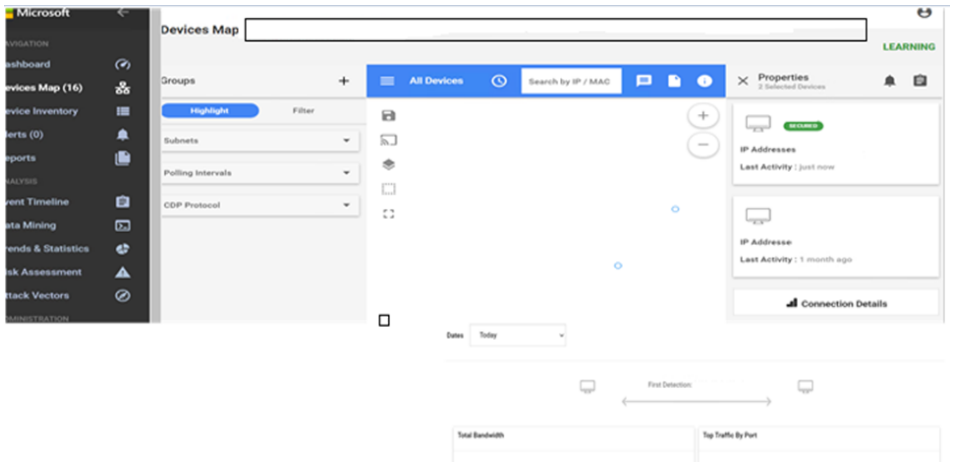
Nozomi Networks käyttää liityntäpisteistä käsitettä Nodes (kuva 28). Liityntäpisteiden kautta saadaan tietoa ICS-verkon topologiasta, joka auttaa ymmärtämään verkon rakennetta ja tunnistamaan mahdolliset tietoturvauhkat. Liityntäpisteiden avulla voidaan myös valvoa ja hallita verkossa olevia laitteita ja varmistaa, että ne toimivat oikein ja turvallisesti. Päätelaitteessa voi olla useampia liityntäpisteitä, esimerkiksi 24-porttisessa kytkimessä niitä voi olla 25, mutta Nozomi Networks listaa vain ne liityntäpisteet, jotka näkyvät verkossa ja ovat aktiivisia.



Kuva 28. Esimerkki Nozomi Networksin liityntäpistenäkymästä. [45.]

Microsoft Defender for IoT:n Device Map -kartalta löytyy yksityiskohtaisia tietoja laitteen liityntäpisteistä, ominaisuuksista ja verkkoyhteyksistä. Nämä tiedot auttavat ymmärtä-

mään verkon topologiaa, tunnistamaan mahdollisia tietoturvauhkia ja estämään epäilyttävää verkkoliikennettä. Lisäksi ratkaisu hyödyntää oppivaa koneoppimista ja käyttäytymisperusteista analyysiä, mikä mahdollistaa nopean ja tehokkaan tietoturvauhkien tunnistamisen (kuva 29).



Kuva 29. Esimerkki Defender for IoT -liityntäpisteistä. [46.]

Mikäli tavoitteena on saada yksityiskohtainen kuva verkon tilasta, tilan poikkeamista ja normaalista käyttäytymisestä, Nozomi Networksin ratkaisu on sopiva valinta. Sen sijaan, jos halutaan laajat liityntäpistetiedot ja tehokas tietoturvauhkien tunnistaminen käyttämisperusteisen analyysin avulla, Microsoft Defender for IoT on suositeltava vaihtoehto.

10.6 Protokollien tunnistus

Nozomi Networks ja Microsoft Defender for IoT tukevat laajaa valikoimaa erilaisia IoT-, OT-, ICS- ja SCADA-protokollia. Esimerkkejä näistä protokollista ovat Modbus, DNP3, BACnet, OPC UA, SNMP, EtherNet/IP, Siemens S7 ja Melsec-Q.Nozomi Networks ilmoittaa tukevansa yli 2 000 protokollaa ja Microsoft Defender for IoT puolestaan ilmoittaa tukevansa yli 3 000. Laaja protokollatuki mahdollistaa turvallisen ja tehokkaan laitteiden ja järjestelmien integroinnin, samalla kun mahdollisia tietoturvauhkia havaitaan ja torjutaan. Yksityiskohtaisia vertailuja näiden kahden ratkaisun protokollatuen

välillä on vaikea tehdä, koska ne tukevat niin monia eri protokollia. Energiayhtiön tulisi tarkastella omaa käyttöympäristöään ja sen protokollatarpeita ja valita ratkaisu sen perusteella, mikä tarjoaa parhaan tuen niille protokollille, joita organisaatio käyttää.

10.7 Istunnot (Sessiot)

Nozomi Networksin ja Microsoft Defender for IoT:n istuntotietojen ja yhteyksien havaitsemisessa on kuitenkin tärkeää huomata, että molemmat tuotteet keräävät ja esittävät tietoa eri tavalla. Nozomi Networksin Sessions-osio näyttää kaikki havaitut istunnot päätelaitteiden välillä, kun taas Defender for IoT:llä yhteydet on löydettävä tiedonlouhintaraportin avulla laitteen IP-osoitteen perusteella. Tämä voi vaikuttaa siihen, kuinka nopeasti ja helposti tietoturvariskit voidaan havaita ja torjua.

Lisäksi molemmat ratkaisut voivat havaita erilaisia tietoturvatapahtumia riippuen siitä, miten ne keräävät ja analysoivat dataa. Esimerkiksi Nozomi Networks keskittyy tunnistamaan syklisiä prosesseja ja poikkeamia muuttujatiedossa, kun taas Defender for IoT käyttää syvää pakettitarkistusta ja käyttäytymiseen perustuvia mallinnusmoottoreita havaitakseen epäilyttävää toimintaa verkossa. Ratkaisut tarjoavat myös hyödyllistä tietoa tietoturvasta ja riskienhallinnasta, mutta niiden tarkkuus ja kattavuus voivat vaihdella. On tärkeää ymmärtää, miten tuotteet keräävät ja analysoivat tietoa, jotta voidaan hyödyntää niiden tarjoamaa tietoa tehokkaasti ja tarkasti. Istuntotaulukko voi olla erittäin hyödyllinen tietoturvatarkoituksissa, koska se antaa yksityiskohtaista tietoa siitä, mitä laitteet tekevät verkossa. Raportin avulla voidaan havaita potentiaalisia tietoturva-aukkoja ja kehittää tarvittavia toimenpiteitä suojaamiseksi.

10.8 Prosessitilan näkyvyys ja muuttujatiedot

Yksittäisen prosessin seuranta ja ymmärtäminen perustuu tunnettuun käyttäytymiseen, joka perustuu kunkin sovelluksen vaiheisiin ja menettelyihin. Jos prosessi ei toimi odotetusti, voimme raportoida, että jotain poikkeavaa on tapahtunut. Kriittisten poikkeamien havaitseminen, jotka vaativat nopeita toimenpiteitä, mahdollistaa integroinnin

soveltuvan palomuurin kanssa reaaliajassa ja poikkeaman hallinnan estämällä kaikki vakavat järjestelmää vahingoittavat komentojen muutokset.

Nozomi Networks keskittyy erityisesti syklisten prosessien ja muuttujatietojen seurantaan, kun taas Microsoft Defender for IoT käyttää syvää pakettitarkistusta ja käyttäytymiseen perustuvia mallinnusmoottoreita havaitakseen epäilyttävää toimintaa verkossa. Molemmat tuotteet tarjoavat tietoa tietoturvasta ja riskienhallinnasta, mutta niiden tarkkuus ja kattavuus voivat vaihdella. Syklisten prosessien ja muuttujatietojen seuranta voi auttaa havaitsemaan piileviä ongelmia ja mahdollisia haavoittuvuuksia, jotka voivat johtua esimerkiksi laitteen ohjelmistovirheistä. Tämä auttaa myös tietoturva-asiantuntijoita tunnistamaan anomaliatiedot, jotka voivat olla merkkejä hyökkäyksestä. Esimerkiksi jos laite on lähettänyt tavallista enemmän dataa tai datan jaksottaisesti, Nozomi Networksin järjestelmä havaitsee poikkeaman ja lähettää hälytyksen.

Microsoft Defender for IoT:n syvä pakettitarkistus ja käyttäytymiseen perustuva mallinnusmoottori auttaa havaitsemaan erilaisia tietoturvatapahtumia ja poikkeamia verkossa. Tämä voi sisältää epäilyttäviä yhteyksiä, käyttöliittymän tunkeutumisyrityksiä, virheellisiä käyttöoikeuksia ja muita tietoturvapoikkeamia. Defender for IoT käyttää myös tekoälyä ja koneoppimista havaitsemaan uusia tietoturvauhkia ja mukautumaan uusiin haasteisiin. Tuote tarjoaa myös prosessitilan näkyvyyden laitteisiin, mutta sen näkökulma on hieman erilainen. Defender for IoT käyttää syvää pakettitarkistusta ja käyttäytymiseen perustuvia mallinnusmoottoreita havaitsemaan epäilyttävää toimintaa verkossa. Tuote tarkkailee ja analysoidaan prosessien tilaa, mutta sen fokus on laajempi ja se pyrkii havaitsemaan kaikenlaista haitallista toimintaa verkossa.

Molemmat tuotteet tarjoavat arvokasta tietoa prosessitilan havainnoinnista ja ovat hyödyllisiä tietoturvan kannalta. Nozomi Guardian keskittyy erityisesti prosessitilan havainnointiin, kun taas Microsoft Defender for IoT tarjoaa laajemman kattavuuden havaita haitallista toimintaa verkossa. Muuttujatiedon keräämiseen suositellaan 2–4 viikon oppimisaikaa, koska prosessiteollisuudessa syklit voivat olla jopa näin pitkiä. Tämä antaa järjestelmälle riittävästi aikaa kerätä tietoa eri prosesseista ja niiden toiminnasta, jotta se voi oppia tunnistamaan normaalin käyttäytymisen ja sykliset prosessit. Kun oppimisaika on päättynyt, kaikki havaitut sykliset prosessit lukitaan järjestelmään. Tämä

mahdollistaa tarkemman ja tehokkaamman hälytysjärjestelmän, joka pystyy tunnistamaan ja reagoimaan poikkeaviin tapahtumiin välittömästi. Lukitsemalla sykliset prosessit, järjestelmä voi keskittyä poikkeavuuksiin, jotka voivat viitata potentiaalisiin uhkiin, kuten kyberhyökkäyksiin, teknisiin ongelmiin tai muihin tietoturvariskeihin. Tällainen oppimisprosessi auttaa varmistamaan, että hälytysjärjestelmä on herkkä ja tarkka, eikä aiheuta liiallista määrää vääriä hälytyksiä. Tämä puolestaan parantaa tietoturva-asiantuntijoiden kykyä keskittyä todellisiin uhkiin ja vastata niihin nopeasti ja tehokkaasti. On kuitenkin tärkeää huomata, että prosessien ja järjestelmien muutokset voivat vaikuttaa oppimisjakson aikana kerättyihin tietoihin. Siksi on suositeltavaa päivittää ja tarkistaa tiedot säännöllisesti, jotta järjestelmä pysyy ajan tasalla ja voi jatkossakin tarjota tehokasta suojaa.

10.9 Muuttujatiedot (Variables)

Nozomi Networks ja Microsoft Defender for IoT käyttävät erilaisia tapoja kerätä ja analysoida muuttuja- ja prosessitietoja. Nozomi Networks kerää muuttujatietoa päätelaitteista ja havaitsee poikkeamat syklisessä muuttujatiedossa, jolloin se tekee hälytyksen, joka voi olla merkki kyberhyökkäyksestä tai muusta poikkeamasta. Nozomi Networks tarjoaa reaaliaikaista näkyvyyttä prosessitilaan, joka hyödyntää havainnointia prosesseista. Tämä auttaa havaitsemaan poikkeamia prosessitilassa ja mahdollisia tietoturvariskejä.

Microsoft Defender for IoT kerää muuttuja- ja prosessitietoja, mutta toisin kuin Nozomi Networks Guardian, se ei tarjoa suoraa reaaliaikaista näkymää niistä. Sen sijaan Defender for IoT tarjoaa tiedonlouhintaraportteja (Data Mining Report), joista käyttäjät voivat hakea tarvittavat tiedot. Tämä tarkoittaa, että Defender for IoT -käyttäjien on aktiivisesti haettava tietoja ja tulkittava niitä itse, mikä voi olla aikaa vievää ja vaativaa.

Defender for IoT perustuu mukautettuihin hälytyksiin, jotka perustuvat liikenteestä opittuun toimintaan, jotta voidaan havaita poikkeavuuksia ja kyberhyökkäyksiä. Tämä lähestymistapa käyttää koneoppimista ja tunnistusmoottoreita oppimaan normaalin verk-

koliikenteen käyttäytymismallit, jolloin se voi tunnistaa poikkeamat, jotka voivat viitata uhkiin.

Lähestymistavan välillä on eroja mutta molemmat ovat tärkeitä tietoturvajärjestelmien kannalta. Nozomi Networks Guardian tarjoaa reaaliaikaisen näkymän OT-ympäristöön ja kontekstitietoisiin tapauksiin, mikä auttaa tunnistamaan ja reagoimaan uhkiin nopeasti. Microsoft Defender for IoT puolestaan tarjoaa monikerroksisen lähestymistavan tunnistusmoottoreiden ja koneoppimisen avulla, mikä auttaa tunnistamaan epänormaalin käyttäytymisen ja potentiaaliset kyberhyökkäykset.

10.10 Verkkokäytäntöjen hallinta

10.10.1 Hälytykset

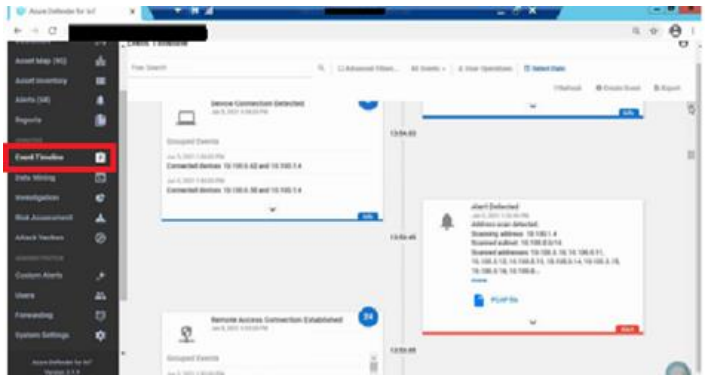
Hälytykset perustuvat havainnointiin ja analyyttisiin mekanismeihin, jotka lähettävät hälytyksen epänormaalista verkkokäyttäytymisestä tai poikkeavasta opitusta verkkoliikenteestä. Molemmat ratkaisut, Nozomi Networks Guardian ja Microsoft Defender for IoT käyttävät pisteytystä tai luokitustasoja määrittääkseen haavoittuvuuksien vakavuusasteen. Korkeampi pistemäärä tai luokitustaso tarkoittaa suurempaa riskiä järjestelmille.

Nozomi Networks Guardian käyttää useita eri moottoreita, jotka on ryhmitelty kymmeniin kontekstitietoisiin tapauksiin tehokkaan korrelaatiomoottorin avulla. Nozomi tarjoaa valmiita hälytyksiä, joita kutsutaan sormenjälkitunnisteiksi (Signatures), jotka voivat ilmetä jo liikenteen oppimisvaiheessa. Guardian luo itsenäisesti tapahtuman, joka perustuu joko toistuvaan hälytykseen tai tiettyihin kombinaatioihin hälytyksiä. Tapahtumien ja hälytysten riskiarvoja voi muokata itse, ja ne päivittyvät jatkuvasti Networks Threat Intelligence™ -palvelun tietokannan kautta.

Toisin kuin Nozomi Networks, joka hyödyntää sormenjälkitunnistukseen perustuvaa teknologiaa, Microsoft Defender for IoT käyttää erilaista lähestymistapaa. Defender for IoT nojaa viiteen erilaiseen tunnistusmoottoriin (kuva 6) pakettidatan analysoimiseksi

sensorilaitteessa. Nämä moottorit tarjoavat erilaisia toimintoja. Esimerkiksi Anomaly Detection Engine keskittyy lähettävän laitteen käyttäytymiseen perustuviin hälytyksiin. Se analysoi datan jatkuvasti ja luo hälytyksiä, jos se havaitsee normaalista poikkeavaa toimintaa, mikä voi viitata potentiaaliseen uhkaan. Toisaalta Malware Detection Engine on suunniteltu tunnistamaan ja hälyttämään mahdollisista haittaohjelmista tai palvelunestohyökkäyksistä kohdelaitteessa. Tämä moottori käyttää kehittyneitä tunnistusalgoritmeja ja tietokantoja tunnetuista haittaohjelmista varmistaakseen, että se voi havaita ja torjua useimmat uhat nopeasti ja tehokkaasti.

Tapahtumien aikajanaosio (Event Timeline) tarjoaa kronologisen näkymän (kuva 30), josta voidaan analysoida hyökkäystä tai tapahtumaa edeltänyt ja sitä seurannut tapahtumaketju. Yhteenveto näistä tapauksista saadaan luettelomuodossa, josta näkyvät lyhyt kuvaus hälytyksestä ja sen vakavuustasosta.



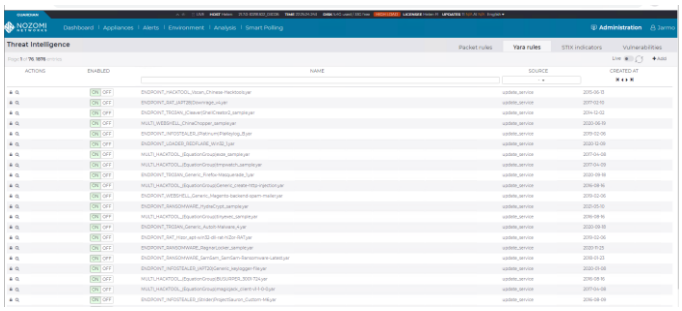
Kuva 30.Microsoft Defender for IoT esimerkki Event Timeline -toiminnasta.

Molemmilla ratkaisuilla on kyky korreloida yksittäisiä tapahtumia ja piirtää niistä automaattisesti looginen sekvenssi. Tämä auttaa tietoturva-asiantuntijoita hahmottamaan teollisuusverkon tilanteen ja reagoimaan mahdollisiin uhkiin nopeasti ja tehokkaasti.

Riskien ja haavoittuvuuden arviointinäkyvyys

Nozomi Networks Threat Intelligence™ -palvelu tarjoaa jatkuvasti päivittyvän tietokannan tunnetuista hyökkäyksistä ja haittaohjelmista, joiden avulla Guardian-sensorit voivat havaita uusia uhkia ja reagoida niihin nopeasti. Yara-sääntöihin perustuva analyysi

mahdollistaa myös tunnettujen hyökkäysten ja haittaohjelmien havaitsemisen reaaliajassa. Riskien ja haavoittuvuuksien arvioinnissa Nozomi Networksin ratkaisut tarjoavat kattavan näkyvyyden verkkoympäristöön ja pystyvät tunnistamaan mahdolliset tietoturvauhkat ennen kuin ne aiheuttavat suurempaa haittaa. Kuvassa 31 esimerkki jatkuvasti päivittyvästä Yara-säännöstöstä.

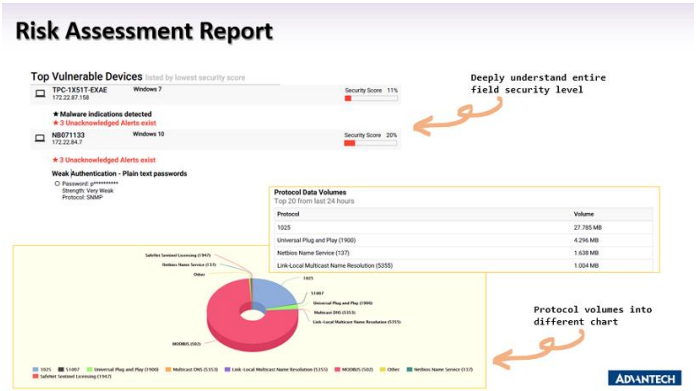


Kuva 31. Esimerkki Yara säännöistä Nozomi Network Threat Intelligence™ kohdasta, josta löytyvät päivitetyt ja yksityiskohtaiset uhkia koskevat tiedot. [44.]

Defender for IoT käyttää useita tekniikoita haavoittuvuuksien ja riskien arvioinnissa. Yksi tärkeimmistä on syvä pakettitarkistus, joka auttaa havaitsemaan tiettyjen laitteiden tai verkon osien haavoittuvuuksia ja alttiutta erilaisille hyökkäyksille. Lisäksi Defender for IoT käyttää käyttäytymiseen perustuvia mallinnusmoottoreita, jotka analysoivat laitteiden toimintaa ja havaitsevat poikkeavuuksia tai epäilyttävää käyttäytymistä, jotka voivat olla merkkejä tietoturvariskeistä.

Microsoft Defender for IoT hyödyntää aktiivisesti Microsoftin Threat Intelligence -palvelua, joka toimittaa jatkuvasti päivitettyjä tietoja tuoreimmista tietoturvariskeistä ja uhkista. Tämä resurssi on korvaamaton, sillä se mahdollistaa Defender for IoT:lle uusien haavoittuvuuksien ja riskien tunnistamisen pikaisesti ja tehokkaasti, mikä on erityisen tärkeää digitaalisen maailman nopeasti kehittyvässä ja muuttuvassa turvallisuusympäristössä.Yhdistettynä muihin käytössä oleviin teknologioihin, kuten Anomaly Detection Engineen ja Malware Detection Engineen, Defender for IoT tarjoaa erittäin tarkan haavoittuvuuksien ja riskien arviointikyvyn. Tämä auttaa organisaatioita suojaamaan laitteitaan ja verkkojaan tietoturvariskeiltä, mikä on keskeistä luotettavan ja turvallisen toimintaympäristön ylläpitämisessä.

Havainnoista laaditaan yksityiskohtainen tietoturvahaavoittuvuuden arviointiraportti (kuva 32), joka tarjoaa syvällisen käsityksen haavoittuvuusarvioinnin tuloksista. Raportti sisältää paitsi havaitut haavoittuvuudet ja niihin liittyvät riskit, myös suositellut toimenpiteet niiden korjaamiseksi. Tämä mahdollistaa organisaatioiden nopean reagoinnin tunnistettuihin riskeihin ja parantaa niiden kykyä ennakoida ja torjua tulevia uhkia.



Kuva 32. Esimerkki Riskarviointiraportion pääsivusta. [40.]

Molempien tuotteiden jatkuvat uhkien havainnointialgoritmit tuottavat monipuolisia hälytyksiä, jos järjestelmissä tapahtuu poikkeavaa toimintaa tai kriittisiä muutoksia.

10.10.2 Integraatiot pilveen

Nozomi Networks Vantage ja Microsoft Azure Sentinel ovat molemmat kyberturvallisuusratkaisuja, mutta ne on suunniteltu hieman erilaisiin tarkoituksiin ja ympäristöihin. Alla niiden vertailua seuraavien näkökohtien perusteella:

Käyttötarkoitus

Nozomi Networks Vantage on erityisesti suunniteltu operatiivisen teknologian (OT) ja esineiden internetin (IoT) ympäristöihin. Se keskittyy teollisuusautomaatioon ja kriittiseen infrastruktuuriin, kuten sähköverkkoihin, öljy- ja kaasuteollisuuteen sekä valmistavaan teollisuuteen. Azure Sentinel taas on pilvipohjainen SIEM-järjestelmä ja SOAR-

ratkaisu, joka on suunniteltu suojaamaan laaja-alaisesti IT-ympäristöjä, kuten pilvi- ja hybridiratkaisuja sekä paikallisia palvelimia.

Analytiikka ja tekoäly

Nozomi Networks Vantage käyttää tekoälyä ja koneoppimista erityisesti OT- ja IoT-laitteiden valvontaan, havaitsemaan poikkeamat ja tunnistamaan mahdolliset uhkat. Azure Sentinel taas hyödyntää Microsoftin AI-teknologiaa ja koneoppimista tarjotakseen älykkään tietoturva analytiikan ja vastauksen erilaisiin tietoturvahälytyksiin koko organisaation IT-ympäristössä.

Integroitavuus

Vantage voidaan integroida muihin tietoturva-, hallinta- ja valvontajärjestelmiin, ja se on yhteensopiva monenlaisten OT- ja IoT-laitteiden kanssa. Azure Sentinel puolestaan integroituu hyvin muiden Microsoftin tuotteiden kanssa ja tukee monia muita tietoturvatyökaluja ja -palveluita.

Asennus ja hallinta

Nozomi Networks Vantage on helppo ottaa käyttöön ja se toimii pilvipohjaisesti, mikä tarjoaa lähes maksuttoman asennuksen ja jatkuvan ylläpidon. Azure Sentinel on myös pilvipohjainen ratkaisu, joka voidaan ottaa käyttöön nopeasti ja skaalata tarpeen mukaan.

Kustannukset

Vertailtavat ratkaisut käyttävät erilaista hinnoittelumallia. Nozomi Networks Vantage perustuu yleensä laitteiden määrään ja liittymien määrään, kun taas Azure Sentinel käyttää pääasiassa tietojen tallennus- ja käsittelymäärien perusteella määritettyä hinnoittelua.Sentinelin puutteena on, että tietyistä synkronoiduista hälytyksistä puuttuu tärkeitä metatietoja, kuten IP-osoite ja laitteen MAC-tiedot. Kyberturvallisuudessa IP-osoitteet ja MAC-tiedot ovat kuitenkin tärkeitä tietoja, joita tarvitaan tietoturva-

analyysien tekemiseen ja hyökkäysten havaitsemiseen. Kun näitä tietoja puuttuu, hälytyksen merkitys voi jäädä epäselväksi ja sen aiheuttamaa riskiä on vaikea arvioida. Siksi on suositeltavaa toteuttaa integraatio, joka mahdollistaa tärkeiden metatietojen välittämisen hälytyksissä Sentinelin ja muiden järjestelmien välillä. Tällöin kyberturvallisuuden ammattilaiset voivat tehdä parempia päätöksiä ja vastata nopeammin mahdollisiin uhkiin. Toiminallisuuden integrointi ei kuulunut Proof of Concept -suunnitelmiin, mutta se on mahdollista toteuttaa.

10.10.3 Palomuuri

Nozomi Networks ja Defender for IoT on suunniteltu saumattomaan integraatioon useimpien johtavien palomuurialustojen, kuten Palo Alton, CheckPointin ja Fortinetin kanssa. Ne mahdollistavat kaksisuuntaisen tiedonvaihdon, jonka ansiosta ne voivat vastaanottaa ja lähettää tärkeitä tietoturvatietoja reaaliajassa. Molemmat järjestelmät on varustettu automaattisella reagointikyvyllä poikkeavuuksien tai epäilyttävän toiminnan havaitsemiseen liikenteessä. Esimerkiksi, jos järjestelmä havaitsee mahdollisen uhan tai epäilyttävän liikennemallin, se pystyy automaattisesti muuttamaan palomuurisääntöjä estääkseen kyseisen liikenteen. Tämä automaattinen toiminnallisuus voi tarjota huomattavaa lisäsuojaa, mutta se vaatii myös organisaatioilta perusteellista riskiarviointia ja huolellista suunnittelua ennen käyttöönottoa. Automaattiset toimet voivat joskus aiheuttaa odottamattomia sivuvaikutuksia tai häiriöitä järjestelmissä, joten riskien hallinta on välttämätöntä. Palomuuritoiminnallisuuden integrointi ei sisältynyt alkuperäiseen Proof of Concept -suunnitelmaan.

10.11 Verkkopolitiikan ja suojausten hallinta

Verkon seuranta ja muutokset

Nozomi Networks- ja Microsoft Defender for IoT -ratkaisut tarjoavat tehokkaan tavan seurata ja analysoida verkkoliikennettä sekä havaita mahdollisia muutoksia ja uhkia. Molemmat näistä ratkaisuista tarjoavat yksityiskohtaista näkyvyyttä havaittuihin verk-

koihin, laiteryhmiin ja yksittäisiin laitteisiin auttaen organisaatioita ymmärtämään ja hallitsemaan verkkonsa toimintaa paremmin. Lisäksi saamme yksityiskohtaisen näkyvyyden jokaiseen yhteyteen, mukaan lukien kaikki verkon sisällä olevat järjestelmät, joihin esimerkiksi etäkäyttäjä muodostaa yhteyden. Tämä sisältää käytetyt protokollat sekä läpikäydyt VLAN-verkot, mikä auttaa varmistamaan, että kaikki verkon osat ovat turvattuja ja hallittuja. Vaikka kokoonpano- tai laiteohjelmistomuutoksia ei havaittu tai tehty testin aikana, on tärkeää, että energiayhtiö jatkuvasti seuraa ja arvioi verkkonsa tilaa sekä mahdollisia muutoksia. Tämä auttaa tunnistamaan ja reagoimaan mahdollisiin uhkiin ja haavoittuvuuksiin nopeasti, varmistaen samalla verkon ja laitteiden turvallisuuden ja eheyden.

Valmiit käyttöliittymämallit

Nozomi Networks Guardian ja Microsoft Defender for IoT on suunniteltu tarjoamaan räätälöityjä käyttöliittymiä eri toimialojen tarpeisiin, kuten energiateollisuuteen ja teollisuusautomaatioon. Molemmat alustat tarjoavat käyttöliittymiä, joiden avulla käyttäjät voivat nopeasti ja tehokkaasti tarkastella kriittisiä tietoja ja havaita poikkeamia normaalista käyttäytymisestä. Microsoft Defender for IoT:n käyttöliittymä ja Nozomi Network Guardianin käyttöliittymä eroavat toisistaan muutamilla keskeisillä alueilla. Tarkemmin näiden kahden ratkaisun käyttöliittymiä ja niiden pääpiirteitä liitteessä 3 olevassa vertailussa. Yhteenvetona voidaan todeta, että molemmat ratkaisut tarjoavat käyttäjille selkeät ja ymmärrettävät näkymät, joiden avulla voidaan seurata ja hallita verkon tietoturvaa tehokkaasti.

Raportointiominaisuudet

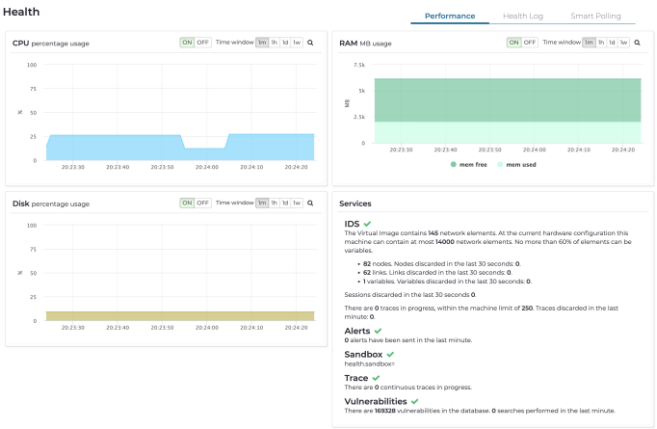
Raportit ovat keskeisiä työkaluja laitteiden ja verkkojen tietoturvan ymmärtämiseen ja parantamiseen. Ne auttavat nopeasti havaitsemaan poikkeavuuksia ja tietoturvariskejä. Nozomi Networks ja Microsoft Defender for IoT tarjoavat kattavia raportointijärjestelmiä teollisuusverkkojen, OT-ympäristöjen ja IoT-laitteiden tietoturvan hallintaan.

Nozomi Networksin raportointi keskittyy liitteessä 4 mainittuihin alueisiin, tarjoten kattavan raportoinnin teollisuusverkkojen ja OT-ympäristöjen tietoturvasta. Tähän sisältyy

esimerkiksi laitteistojen, ohjelmistojen, verkkoliikenteen ja järjestelmän käyttöoikeuksien tarkastelu. Näiden tietojen avulla organisaatiot voivat tunnistaa ja korjata mahdolliset tietoturva-aukot sekä ennaltaehkäistä riskejä. Microsoft Defender for IoT puolestaan tarjoaa laajemman näkökulman IoT- ja OT-laitteiden tietoturvaan. Sen raportointiominaisuudet sisältävät monia eri näkökohtia, jotka auttavat ymmärtämään ja parantamaan IoT- ja OT-ympäristöjen tietoturvaa. Raportoinnissa keskitytään liitteessä 5 mainittuihin alueisiin, kuten laitteiden tunnistamiseen, verkon segmentointiin, haavoittuvuuksien hallintaan ja hyökkäysten havaitsemiseen. Molemmat ratkaisut tarjoavat kattavan näkymän verkkoon ja sen tietoturvaan.

10.11.1 Laitteiston toimintotilan seuranta

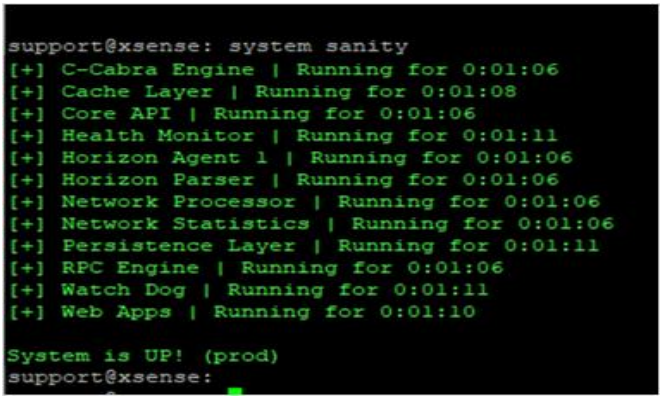
Nozomi Networksin hallintapaneeli tarjoaa laajan näkymän sensorilaitteiden toimintaan ja tilaan. Tämä sisältää tärkeitä tietoja, kuten laitteiden ohjelmistoversiot, toimintatilat, liikennemäärät sekä muistin ja suorittimen kuormitukset (kuva 33). Nämä tiedot ovat arvokkaita valvontahenkilöstölle, sillä ne auttavat ymmärtämään laitteiden nykyisen tilan ja mahdollistavat mahdollisten ongelmien havaitsemisen varhaisessa vaiheessa. Valvontahenkilöstö voi myös arvioida laitteiden suorituskyvyn trendejä ja tehdä ennakoivia päätöksiä laitteistojen ylläpidon ja päivitysten suhteen. Esimerkiksi, jos havaitaan, että tiettyjen laitteiden kuormitus on jatkuvasti korkea, se voi viitata tarpeeseen päivittää laitteisto tai optimoida sen konfiguraatiota.



Kuva 33. Nozomi Networks hallintapaneelinäkymä sensorin tilatiedoista.

Laitteiston tilan seuranta: Defender for IoT -laitteisto tarjoaa rajoitetun valvonnan sensorilaitteiden tilatiedoista, kuten ohjelmistoversioiden ja toimintatilojen seurannasta. Tiedot voidaan tarkistaa CLI-komentokehotteen avulla SSH-konsolin kautta, vaikka tämä ei ole yhtä käyttäjäystävällistä kuin Nozomi Networks -ratkaisun hallintapaneeli.

Vaikka Defender for IoT -appliance tarjoaa tehokkaan tietoturvaratkaisun IoT- ja OT-ympäristöille, sen rajalliset ominaisuudet sensorilaitteiden tilatietojen seurannassa ja käyttöliittymän käyttäjäystävällisyydessä voivat asettaa haasteita käyttäjille. Sensorin suorituskykytietojen saamiseen ei ole selkeitä mekanismeja. Järjestelmän tilatietojen tarkistaminen tapahtuu rajallisesti CLI-komentokehotteella SSH-konsolin kautta (kuva 34). Sensorien tilan valvota kuormitustilanteissa on haasteellisempaa kuin Nozomi Networksissa. [30.]

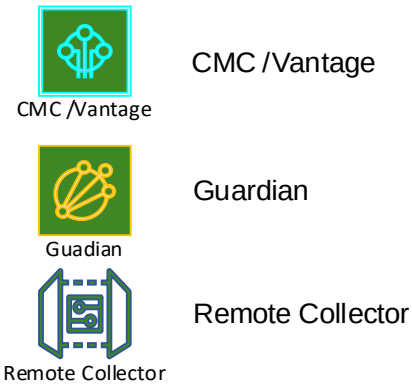


Kuva 34. Defender for IoT -sensorin tilatiedot. [30.]

10.11.2 Laajennettavuus

Nozomi Networksin kolmeportainen arkkitehtuuri mahdollistaa skaalautuvuuden pienistä erittäin suurien IT- ja OT-ympäristöjen valvontaan. Arkkitehtuuri tarjoaa joustavuutta ja skaalautuvuutta yritysten verkkoturvallisuuden tarpeisiin. Sen avulla organisaatiot voivat suojata ja valvoa erikokoisia IT- ja OT-ympäristöjä tehokkaasti samalla kun ne varmistavat tietoturvan ja yksityisyyden säilymisen. Mikäli OT-verkkoympäristössä on pieniä satelliitteja, kuten sähköalan ala-asemia, on hyvä vaihtoehto käyttää pienempiä

ja edullisempia tiedonkeruulaitteita, kuten Remote Collectoreita, Guardianien sijaan. Remote Collector on suunniteltu keräämään ja pakkaamaan verkkoliikennettä näiltä pienemmiltä ala-asemilta ennen sen siirtämistä TLS-tunnelin kautta omaan Guardian-isäntäkoneeseen. Tämä mahdollistaa tehokkaan verkkoliikenteen analysoinnin ja seurannan, samalla kun se vähentää kustannuksia verrattuna useamman Guardianin käyttämiseen. Arkkitehtuuri koostuu seuraavista komponenteista (kuva 35).



Kuva 35. Nozomi Networksin kolmiportainen arkkitehtuurimalli

Guardian: Guardian

Toimii verkkotiedon kerääjänä, joka valvoo ja analysoi verkkoliikennettä ja tunnistaa mahdollisia uhkia tai poikkeamia. Guardianeja voidaan asentaa verkkoympäristöön useampia tarpeen mukaan, jolloin ne pystyvät seuraamaan ja suojaamaan laajempaa infrastruktuuria.

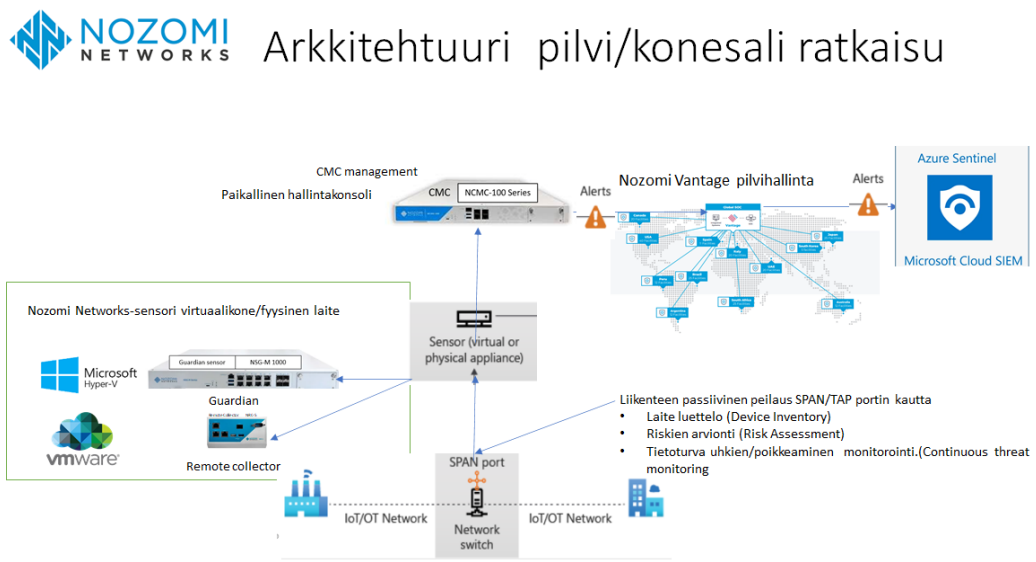
Centralized Management Controller (CMC) tai Vantage

Jos halutaan yhdistää useamman Guardianin tiedot yhteen paikkaan, se voidaan tehdä joko CMC:n tai Vantagen avulla. CMC on paikalliseen verkkoon asennettava tiedonkeruulaite, joka keskittää eri Guardianeista kerätyn tiedon yhteen paikkaan. Vantage on pilvipohjainen tiedonkeruulaite, joka tarjoaa keskitetyn hallinnan kaikille Nozomin lisensseille ja kerää tiedot useammasta Guardianista.

Remote Collector Tämä komponentti on vastuussa kerätyn tiedon siirtämisestä Guardianilta CMC:lle tai Vantagelle. Remote Collector takaa, että kaikki OT-ympäristöstä kerätty tieto pysyy paikallisena Nozomin näkökulmasta.

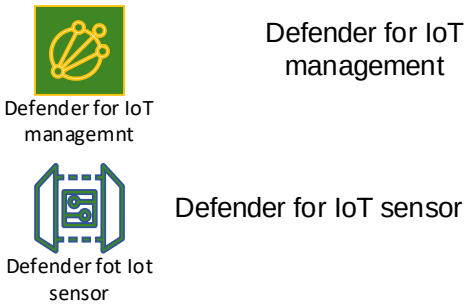
Mikäli OT-verkkoympäristössä on pieniä satelliitteja, kuten sähköalan ala-asemia, on hyvä vaihtoehto käyttää pienempiä ja edullisempia tiedonkeruulaitteita, kuten Remote Collectoreita, Guardianien sijaan. Remote Collector on suunniteltu keräämään ja pakkaamaan verkkoliikennettä näiltä pienemmiltä ala-asemilta ennen sen siirtämistä TLS-tunnelin kautta omaan Guardian-isäntäkoneeseen. Tämä mahdollistaa tehokkaan verkkoliikenteen analysoinnin ja seurannan, samalla kun se vähentää kustannuksia verrattuna useamman Guardianin käyttämiseen.

Pienin Guardian-malli (R50) tukee jopa kymmenen keruulaitteen liittämistä, mikä mahdollistaa laajemman OT-verkkoympäristön valvonnan. Tämä järjestely on kustannustehokas ja joustava tapa suojata ja valvoa pienempiä satelliitteja tai ala-asemia ja varmistaa, että koko OT-verkko on suojattu mahdollisilta uhkilta ja haavoittuvuuksilta. Kuvassa 37 esimerkkiehdotus konesali- tai pilviratkaisun arkkitehtuurista.



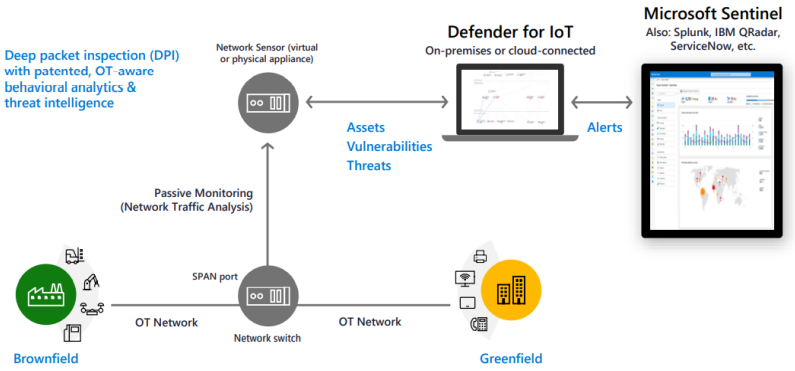
Kuva 36. Nozomi Networks -ratkaisumalliehdotus

Defender for IoT:n ratkaisu perustuu kaksiportaiseen arkkitehtuuriin (kuva 37) ja mahdollistaa myös skaalautuvuuden pienistä erittäin suureen OT-ympäristöjen valvontaan.



Kuva 37.Defender for IoT kaksiportainen arkkitehtuurimalli

Defender for IoT:n hallintapaneelista saadaan kokonaiskuva verkojen toimivuudesta, mikä auttaa SOC-tiimejä hallitsemaan ja analysoimaan hälytyksiä yhdestä keskitetystä hallintapaneelista. Sen avulla voidaan kerätä ja analysoida reaaliaikaista dataa useista sensoreista, jotta hälytykset voidaan tunnistaa ja reagoida niihin nopeasti. Sensorit keräävät ICS-verkkoliikennettä passiivisesti (agentittomasti) IoT- ja OT-laitteista. Avoin käyttöjärjestelmäalusta tukee kustannustehokkaasti sekä paikallisia konesali- että pilvipohjaisia käyttöönottoratkaisumaleja (kuva 38). Pilviratkaisussa sensorit on yhdistetty Microsoftin Azureen ja eroavat paikallisesti hallituista sensoreista siten, että tiedot näkyvät konsolissa ja tunnistustiedot jaetaan paikallisen hallintakonsolin kanssa, jos sensori on yhdistetty siihen.



Kuva 38. Defendef for IoT arkkitehtuuri. [39.]

Microsoftin uhkien tiedustelupaketit voidaan myös automaattisesti ladata pilvipalveluihin yhdistetyille sensoreille. Pilveen yhdistettyjen sensoreiden havaitsemat tiedot näkyvät paikallisessa sensorikonsolissa, mutta ne voidaan myös lähettää IoT-keskittimen kautta muihin Azure-palveluihin kuten Microsoft Sentineliin, Azure Machine Learningiin ja Azure Stream Analyticsiin. IoT-keskitin mahdollistaa turvallisen kaksisuuntaisen viestinnän laitteiden välillä käyttämällä useita avoimia protokollia, kuten AMQP, HTTPS, käyttämällä laitekohtaisia käyttöoikeuksia ja pääsynhallintaa.

Molempien ratkaisujen kanssa paikallisesti hallittuihin sensoreihin joudutaan uhkatietokantapaketit lataamaan manuaalisesti. Käyttöönottomallit ovat ratkaisuissa joustavia ja niihin voidaan soveltaa pilvipohjaista tai konesalikäyttöönottomallia, joissa ne skaalautuvat ja soveltuvat sekä hajautettuihin että laajoihin ympäristöihin.

10.11.3 Integrointi Sentineliin

Tietoturva-arkkitehtuurin on käsiteltävä muutakin kuin vain omaisuusluetteloa ja näkyvyyttä, minkä vuoksi se myös vaatii integroinnin muihin valvontajärjestelmiin. Microsoft Sentinelin käyttö datankeruussa oli yksi verkkoyhtiölle olleista lisävaatimuksista. Tätä ominaisuutta emme soveltuvuusselvityksessä (Proof of Concept, POC) kuitenkaan testanneet, mutta käsittelen sen mahdollisuuksia myöhempään integrointiin.

Integrointi Microsoft Sentinelin kanssa tarjoaa tehokkaan tavan hyödyntää tekoälyä ja laajaa käyttäjäkuntaa uhkien havaitsemiseen. Sentinel pystyy keräämään tietoja pilvimittakaavassa kaikilta käyttäjiltä, laitteilta ja sovelluksilta, ja integrointi tietoturvaratkaisun kanssa voi avata tehokkaita mahdollisuuksia uhkien korrelaatioon, automaatioon ja lisätä näkyvyyttä IT- ja OT-ympäristöissä. Sentinelin pilvipohjaisuus mahdollistaa turvallisen integraation paikallisten API-liittymien kanssa ja tarjoaa edullisia hallintakustannuksia modernin SOC:n mahdollistamiseksi.

Integrointi Microsoft Defender for IoT -sensorin kanssa antaa mahdollisuuden soveltaa käyttäytymisanalytiikkaa ja koneoppimistekniikoita laitteiden löytämiseen, luokitteluun

sekä IoT-hyökkäyksien suojaamiseen, havaitsemiseen ja niihin vastaamiseen. Lisäksi se tarjoaa mahdollisuuden hyödyntää maailmanlaajuista IoT- ja OT-uhkatietokantaa.

On tärkeää huomioida, että OT-verkko vaatii erilaisia lähestymistapoja valvontaan. Integroinnin on oltava huolellisesti harkittu ja toteutettu, jotta se ei aiheuta turvallisuusriskiä verkossa. Käyttöönoton yhteydessä on varmistettava, että tietoturvaratkaisu integroituu IT-ympäristön ja palveluntoimittajan SOC:n kanssa käytettävään teknologiaan ja että turvallisuusvaatimukset täyttyvät kaikissa integraation vaiheissa.

Sentinelin integrointi tietoturvaratkaisuun voi myös parantaa sensorin käyttäytymisanalytiikkaa ja koneoppimistekniikoita laitteiden löytämiseen, luokitteluun sekä IoT-hyökkäyksien suojaamiseen, havaitsemiseen ja niihin vastaamiseen. Tämä antaa mahdollisuuden soveltaa maailmanlaajuista IoT- ja OT-uhkatietokantaa ja hyödyntää Sentinelin pilvimittakaavan keräämiä tietoja.

On kuitenkin tärkeää varmistaa, että integrointi tietoturvaratkaisun ja Sentinelin välillä toteutetaan turvallisesti ja huolellisesti. Integraation yhteydessä on huomioitava erilaiset lähestymistavat, joita OT-verkko vaatii valvontaan, ja varmistettava, että kaikki turvallisuusvaatimukset täyttyvät. Lisäksi on varmistettava, että tietoturvaratkaisu integroituu saumattomasti IT-ympäristön ja palveluntoimittajan SOC:n kanssa käytettävään teknologiaan. Integrointi Sentinelin kanssa on yksi osa kokonaisvaltaista tietoturva-arkkitehtuuria, ja se ei yksinään riitä suojaamaan verkkoa. On huolehdittava myös muista tietoturvanäkökohdista, kuten vahvoista salasanoista, monikerroksisesta tunnistautumisesta ja päivitetyistä tietoturvaohjelmistoista.

Mahdollisen Integroinnin myötä tietoturva-arkkitehtuurin kokonaiskuva voi parantua, kun eri järjestelmien tiedot saadaan kerättyä ja korreloimaan toisiinsa. Sentinelin avulla organisaatio voi myös täyttää monia tietoturvanormeja ja -sääntöjä, kuten GDPR- ja NIS2-direktiivien vaatimukset.

11 Testauksen tiivistelmä

Testauksen tavoitteena oli selvittää, kuinka tehokkaasti passiiviset verkkoskannauslaitteet voivat kerätä tietoja verkkoyhtiön OT-ympäristöstä. Kaksi eri toimittajaa, Microsoftin IoT Defender ja Nozomi Networks otettiin mukaan vertailuun. Nozomi Networks valittiin, koska palvelutoimittaja tarjoaa sille OT-SOC-palvelua, ja Microsoftin IoT Defender valittiin, koska Microsoftilla on vahva asema energiayhtiössä.

Ratkaisujen arvioinnissa käytettiin sekä toimittajien materiaaleja että testiympäristöstä saatuja tutkimustuloksia. Molemmat ratkaisut tarjoavat tehokkaan tietoturvan IoT- ja OT-laitteille, haavoittuvuuksille ja uhkille. Niiden avulla saadaan yhtenäinen tietoturvatapahtumien näkyvyys, joka on keskeinen tekijä kriittisten teollisten prosessien suojaamisessa.

Näkyvyyden ansiosta voidaan tehdä tietoon perustuvia liiketoimintapäätöksiä ja yksityiskohtaisia riskiarvioita. Ratkaisut yhdistävät havaitsemisen ja reagoinnin nopeisiin korjauksiin. Agentiton ratkaisu mahdollistaa kattavan uhkien seurannan koko verkkoyhtiön verkkoliikenteessä, jopa salatussa liikenteessä. Ratkaisut tarjoavat automaattisen löytämisen hallituille ja hallitsemattomille IT-laitteille ja OT-resursseille perustuen niiden attribuutteihin.

Käyttäytymismallinnuksen, koneoppimisen ja globaalin uhkatietokannan avulla molemmat ratkaisut pystyvät nopeasti ja suurella varmuudella havaitsemaan erilaisia uhkia. Ratkaisut keskittyvät omaisuuden tunnistamiseen ja liikennevirran passiiviseen analysointiin, jossa ne käyttävät omia poikkeavuusmoottoreitaan havaitakseen poikkeamat normaalista verkkotoiminnasta.

Molempien ratkaisujen tärkein etu on helppo käyttöönotto ja minimaalinen vaikutus tuotantolaitteisiin ja energiayhtiön verkkoon. Pilvipohjaiset käyttöönottomallit tarjoavat lisääntynyttä yksinkertaisuutta, skaalautuvuutta ja vähemmän manuaalista työtä tietoturvatiimeille. Verkon visualisointi parantaa ymmärrystä ICS-verkon rakenteesta, järjestelmätietoisuudesta ja toiminnasta, ja tarjoaa nopeasti tietoa erilaisten kartoitusten, taulukoiden ja raporttien kautta.

Testauksen aikana huomioitiin erilaiset verkkoliikenteen keräämisen vaiheet, kuten SPAN- ja VXLAN-liikenteen tunnistaminen. Tulokset osoittivat, että molemmat verkkoskannauslaitteet pystyivät havaitsemaan päätelaitteita samassa VLAN:ssa, mutta niiden kyky kerätä yksityiskohtaisia tietoja heikkeni, kun päätelaitteet sijaitsivat muilla turvavyöhykkeillä. Nozomi suoriutui paremmin, kun VXLAN:t lisättiin passiiviseen skannaukseen ja sen avulla pystyttiin havaitsemaan paremmin VXLAN-järjestelmän takana olevat päätelaite.

Verkkoyhtiön OT-ympäristö on suunniteltu noudattamaan parhaita käytäntöjä, joka on jaettu turvavyöhykkeisiin Purdue-mallin mukaisesti. Tämä asettaa haasteita passiiviselle skannauslaitteelle, joka ei pysty näkemään koko verkon liikennettä. On suositeltavaa kerätä liikennettä erikseen jokaiselta turvavyöhykkeeltä, mutta tämä voi aiheuttaa korkeita kustannuksia, jos jokaiseen verkkosegmenttiin asennetaan erillinen OT-IDS-laite. Vaikka Nozomi Networks ja Microsoft Defender for IoT ovat tehokkaita OT-tietoturvaratkaisuja, on syitä (Liite 6), miksi Nozomi saattaa sopia paremmin verkkoyhtiön ympäristöön. Nozomi tarjoaa erikoistuneempaa tukea ja integroituu paremmin Siemens-laitteiston kanssa, mikä on tärkeä tekijä verkkoyhtiölle. Lisäksi Nozomi Networks on luonut syvemmät integraatiot teollisuusalan toimijoiden ja asiakkaiden kanssa, mikä takaa asiakkaille laajaa osaamista teollisuuden tietoturvasta ja asiantuntevaa tukea ongelmatilanteissa. Vaikka Microsoftilla on myös vahva tuki ja kumppaniverkosto, Nozomi todennäköisesti tarjoaisi erikoistuneempaa ja kohdennettua tukea teollisuusympäristöille.

Kokonaisuutena ottaen Nozomi Networksin ratkaisu on suositeltavampi verkkoyhtiölle, sillä se vastaa paremmin verkkoyhtiön OT-ympäristön tarpeisiin ja resursseihin. Nozomi tarjoaa kustannustehokkaan ja turvallisen tavan seurata verkon liikennettä, ja hyödyntää etäkeräilijöitä kattavan näkyvyyden saavuttamiseksi. Tämä tekee Nozomi Networksin ratkaisusta turvallisen valinnan verkkoyhtiön OT-tietoturvaan.

12 Pohdinta

Ratkaisujen tutkiminen vaati monipuolista osaamista tekoälyn, koneoppimisen ja kyberturvallisuuden alueilta sekä ymmärrystä verkkoyhtiön IT- ja OT-ympäristöistä. Soveltuvuusselvityksen (Proof of Concept, POC) tarkoituksena oli varmistaa, että Microsoft Defender for IoT ja Nozomi Networks Guardian ovat sopivia energiayhtiön kyberturvallisuuden parantamiseen ja täyttävät lupaamansa edut. Testauksessa tarkasteltiin myös, kuinka hyvin nämä ratkaisut vastaavat tulevan NIS2-direktiivin vaatimuksia.

Nozomi Networks Guardian ja Microsoft Defender for IoT ovat molemmat IoT-OT-tietoturvaratkaisuja, mutta niiden välillä havaittiin myös eroavaisuuksia. Nozomi Networks Guardian keskittyy erityisesti teollisten protokollien ja laitteiden tietoturvaan ja tarjoaa perusteellisen analyysin OT-verkoista sekä yksityiskohtaisia raportteja verkon suorituskyvystä ja turvallisuudesta. Ohjelmisto sisältää reaaliaikaisen uhkien havaitsemisen ja ehkäisyn, verkkoanalyysin ja uhkien hallinnan. Se tarjoaa myös teollisuuden verkkojen tietoturvan, joka auttaa täyttämään tietoturva vaatimukset.

Microsoft Defender for IoT on laajempi IoT-OT-tietoturvaohjelmisto, joka tarjoaa kattavan tietoturvan kaikille IoT-OT-laitteille, mukaan lukien päätelaitteet, verkkoinfrastruktuuri ja ohjaimet. Se tarjoaa myös reaaliaikaista seurantaa ja havaitsee turvallisuusuhkia sekä tuottaa riskiarvioita ja suosituksia turvallisuuden parantamiseksi. Molemmat ratkaisut hyödyntävät hyvin tekoälyä ja koneoppimista laitteiden käyttäytymisen seuraamiseen ja poikkeamien havaitsemiseen. Microsoft Defender for IoT tarjoaa myös laajat integraatiomahdollisuudet muiden Microsoftin ratkaisujen kanssa, mikä voi helpottaa hallintaa ja käyttöönottoa energiayhtiössä, joka käyttää jo muita Microsoftin tuotteita.

Nozomi Networks Guardian ja Microsoft Defender for IoT tukevat NIS2-direktiivin vaatimuksia. Ne tarjoavat kattavan näkymän verkkoon sen eri osiin sekä havaitsevat poikkeavuuksia ja mahdollisia hyökkäyksiä reaaliajassa. Nozomi Networks Guardian käyttää tekoälyä ja koneoppimista poikkeavuuksien havaitsemiseen verkon käyttäytymisessä ja ilmoittaa niistä mahdollisimman nopeasti. Se pystyy havaitsemaan myös verkon sisäisiä hyökkäyksiä, joita perinteiset tietoturvaratkaisut eivät välttämättä havaitse.

Guardian tukee useita protokollia ja integroituu myös muihin tietoturvajärjestelmiin, mikä helpottaa kokonaisvaltaisen näkymän ylläpitoa verkkoon. Microsoft Defender for IoT käyttää samoin tekoälyä ja koneoppimista laitteiden käyttäytymisen seuraamiseen ja poikkeamien havaitsemiseen ja pystyy tunnistamaan poikkeamat laitteiden käyttäytymisessä sekä ilmoittamaan niistä mahdollisimman nopeasti. Tämä auttaa tunnistamaan mahdolliset uhkat ennen kuin ne aiheuttavat vahinkoa järjestelmille.

Microsoft Defender for IoT ja Nozomi Networks Guardian ovat ratkaisuja, jotka tarjoavat kattavan näkyvyyden OT- ja IT-ympäristöön sekä mahdollisuuden havaita laitteita ja poikkeavuuksia reaaliajassa. Lisäksi nämä ratkaisut ovat integroitavissa muihin tietoturvajärjestelmiin, kuten Microsoft Sentineliin, joka mahdollistaa laajamittaisen tiedonkeruun ja tehokkaan uhkien tunnistamisen.

Tutkimus korostaa tarvetta kattavalle ja jatkuvasti päivitettävälle tietoturvastrategialle, joka kattaa sekä IT- että OT-ympäristöt. Yksittäisten ratkaisujen, kuten Microsoft Defender for IoT:n ja Nozomi Networks Guardianin, käyttö yksin ei riitä tietoturvan varmistamiseen. Tarvitaan myös yhteistyötä IT- ja OT-tiimien välillä sekä teknologia-alustojen yhteiskäyttöä ja tietojen jakamista. Pilvipohjaiset sovellukset ja analytiikka voivat auttaa vastaamaan näihin haasteisiin ja tarjoamaan tarvittavan kokonaisnäkyvyyden verkkoon. On tärkeää huomata, että tietoturvastrategiaa on päivitettävä säännöllisesti, koska uhkatilanteet muuttuvat ja kehittyvät jatkuvasti.

NIST Cyber Security Framework -viitekehyksen mukaiset tunnistamis- ja havainnointitoiminnot olivat keskeisiä testauksen aikana, koska ne auttoivat arvioimaan kunkin ratkaisun tehokkuutta ja eroja näiden toimintojen suhteen. Nämä testitulokset olivat arvokkaita vertailtaessa ratkaisuja keskenään ja auttoivat projektin osallistujia tekemään perustellun päätöksen valittavasta ratkaisusta. Soveltuvuusselvitys (POC) oli ratkaisevan tärkeä vertailtaessa ja arvioitaessa Microsoftin Defender for IoT- ja Nozomi Networks -tietoturvaratkaisuja. Testauksen avulla saatiin selkeä kuva kunkin ratkaisun kyvykkyyksistä ja eroista. Näiden tietojen perusteella voitiin tehdä perusteltu päätös siitä, kumpi ratkaisu vastasi parhaiten verkkoyhtiön tarpeisiin ja vaatimuksiin.

Sekä Microsoft Defender for IoT että Nozomi Networks Guardian ovat sopivia ratkaisuja energiayhtiön kyberturvallisuuden parantamiseen. Molemmat ratkaisut tarjoavat reaaliaikaisen näkyvyyden OT-verkkoon ja mahdollistavat poikkeamien havaitsemisen ja analysoinnin. Microsoft Defender for IoT tarjoaa laajan valikoiman turvallisuusominaisuuksia, mukaan lukien edistykselliset analyysityökalut, mahdollisuuden reagoida nopeasti hälytyksiin ja vahvan integraation muiden Microsoftin tietoturvaratkaisujen kanssa. Se on myös helppo integroida olemassa oleviin IT-järjestelmiin ja infrastruktuuriin. Nozomi Networks Guardian taas on suunniteltu erityisesti ICS-ympäristöihin ja se tarjoaa kattavan näkyvyyden OT-verkkoon sekä mahdollisuuden havaita ja torjua kyberuhkia. Se on myös helppo integroida olemassa oleviin IT-järjestelmiin.

Molempien ratkaisujen POC-testaukset osoittivat, että ne tukevat NIS2-direktiivin vaatimuksia. Microsoft Defender for IoT:lla on myös Microsoftin laaja tuki- ja yhteistyöverkosto, mikä tekee siitä houkuttelevan ratkaisun energiayhtiön tarpeisiin, vaikka Nozomi Networksin ratkaisua suositellaan erityisesti ICS-ympäristöjen suojaamiseen. Lopullinen valinta riippuu kuitenkin verkkoyhtiön tarpeista ja olosuhteista.

Tilanne OT-kybertietoturvassa on kuitenkin jatkuvasti muuttuva ja globaali, sillä IoT- ja OT-laitteiden käyttö laajenee ja niiden merkitys kasvaa. Tämä luo uusia haasteita kyberturvallisuudelle, koska hakkereilla on mahdollisuus käyttää edistyneitä tekniikoita hyökkäysten tekemiseen. Lisäksi NIS2-direktiivin vaatimukset lisäävät paineita organisaatioille varmistaa kyberturvallisuutensa. Venäjän hyökkäys Ukrainaan on herättänyt huolestuneisuutta kriittisen infrastruktuurin suojaamisen tarpeesta, erityisesti kyberuhkien kuten DDoS-hyökkäystensuhteen, jotka kohdistuvat verkkosivustoihin ja infrastruktuuriin. Tämä korostaa tarvetta vahvistaa tietoturvatoimenpiteitä ja varautumista kyberhyökkäyksiin, jotta voidaan suojata kriittiset järjestelmät ja palvelut. Vaikka tekoäly ja koneoppiminen ovat hyödyllisiä tutkimuksessa ja analytiikassa, niitä voidaan käyttää myös edistyneiden hyökkäysten tekemiseen hakkerien toimesta. Tämä korostaa tarvetta varmistaa, että organisaatioilla on tarvittava osaaminen ja asiantuntemus IoT- ja OT-turvallisuudesta, jotta ne voivat vastata muuttuviin uhkiin ja haasteisiin.

Liite 1. Testitulokset

Vertailussa mitataan, tukeeko Defender for IOT ja Nozomi Networks määriteltyjä toiminnallisuuksia. Kukin toiminnallisuus on pisteytetty toteutuksen laadukkuuden mukaan. Lisäksi asiakas voi määrittää toiminnallisuuskohtaisesti painokertoimen ja laskea tämän avulla painotetun pisteytyksen oman organisaation todellisten tarpeiden mukaan.

Testatut ominaisuudet ja arviot	+/- Defender for IoT	+/- NOZOMI NETWORKS	+/- Defender for IoT	+/- NOZOMI NETWORKS	Painokerroin/asiakas
Laitteiden löytyminen ja visualisointi	√	√	3	3	
Verkon näkyvyys ja visualisointi	√	√	3	2	
Haavoittuvuuksien hallinta ja riskien monitorointi	√	√	3	3	
Tapahtumien havaitseminen	√	√	2	3	
Automaattinen omaisuuden löytyminen	√	√	3	3	
Valmiit käyttöliittymä mallit ja raportointi ominaisuudet	√	√	3	2	
Integraatioita Microsoftin ympäristöihin	√	≈ osittain	ei testattu	ei testattu	
Kunkin IoT-sensorin suorituskyvyn ja käytettävyyden valvonta (CPU, muisti, liikenne)	0	√	1	3	
Hyödyntää tekoälyä tarjotakseen perussyyanalyysiä	√	√	3	3	
Verkkotoiminnan seuranta	√	√	2	3	

Käyttöliittymän mukauttaminen	0	√	1	3	
Toimii pilvessä MS Sentinelin kanssa	√	√	ei testattu	ei testattu	
Skaalautuva suuriin verkkoihin	√	√	ei testattu	ei testattu	
Verkkoon tehdyt muutokset näkyvät reaaliajassa	√	√	3	3	
Tuotantoprosessien valvonta	√	√	1	3	
Palvelun tarjoat					
Käyttöönottomallit	√	√	3	3	
			40	43	

Pisteet

0 = ei ominaisuutta

1 = heikoin

2 = keskitasoinen

3 = paras

Liite 2 NIS2 vaatimukset

Taulukko 9. Molemmat testatut tietoturvaratkaisut tukevat alla olevia NIS2 -vaatimuksia [33.]

Tavoite	**Periaate**	**Yhteenveto**
Turvallisuus-riskien hallinta	A1. Hallintotapa	Organisaatiolla on asianmukaiset johtamiskäytännöt ja -prosessit, jotka ohjaavat sen lähestymistapaa verkko- ja tietojärjestelmien turvallisuuteen.
	A2. Riskien hallinta	Organisaatio ryhtyy tarvittaviin toimenpiteisiin tunnistaakseen, arvioidakseen ja ymmärtääkseen olennaisten palveluiden toimitusta tukevien verkkoon ja tietojärjestelmiin kohdistuvia turvallisuusriskejä.
	A3. Omaisuuden hallinta	Kaikki, mitä tarvitaan tärkeiden palvelujen verkkojen ja tietojärjestelmien toimittamiseen, ylläpitoon tai tukemiseen, määritellään ja ymmärretään.
	A4. Toimitusketju	Organisaatio ymmärtää ja hallitsee keskeisten palveluiden toimitusta tukevien verkkojen ja tietojärjestelmien turvallisuusriskejä, jotka syntyvät riippuvuudesta ulkopuolisiin toimittajiin.
Kyberhyökkäyksiä vastaan suojaminen	B1. Palvelujen suojauskäytännöt ja -prosessit	Organisaatio määrittelee, toteuttaa, kommunikoi ja panee täytäntöön asianmukaiset käytännöt ja prosessit, jotka ohjaavat sen yleistä lähestymistapaa keskeisten palveluiden toimittamista tukevien järjestelmien ja tietojen turvaamiseen.
	B2. Pääsyn hallinta	Organisaatio ymmärtää, dokumentoi ja hallinnoi pääsyä keskeisten palveluiden toimittamista tukeviin järjestelmiin ja toimintoihin.
	B3. Tiedon turvaaminen	Sähköisesti tallennetut tai välitetyt tiedot on suojattu sellaisilta toimilta, kuten luvattomalta käytöltä, muuttamiselta tai poistamiselta, jotka voivat häiritä olennaisia palveluita.

	B4. Järjestelmien turvaamien	Verkko- ja tietojärjestelmät sekä keskeisten palvelujen toimittamisen kannalta kriittiset teknologiat on suojattu kyberhyökkäyksiltä. Organisaation ymmärrys olennaisten palvelujen riskeistä kertoo vahvan ja luotettavan käytön suojatoimenpiteitä.
	B5. Henkilöstön tietoturva-ohjeistus ja koulutus.	Henkilökunnalla on asianmukaiset tiedot ja taidot hoitaa organisaatioroolinsa mukaiset työtehtävänsä tehokkaasti verkkoliikenteen ja tietojärjestelmien turvallisuus huomioiden.
Tavoite	Periaate	**Yhteenveto**
Kyberturva tapahtumien havainnointi	C1. Tietoturva tapahtuminen valvonta	Organisaatio seuraa keskeisten palveluiden toimitusta tukevien verkkojen ja järjestelmien tietoturvatilannetta mahdollisten tietoturvaongelmien havaitsemiseksi ja turvatoimien jatkuvan tehokkuuden seuraamiseksi.
	C2. Ennakoiva tietoturvatapahtumien löytäminen	Organisaatio havaitsee verkossa haitallisen toiminnan, joka vaikuttaa tai voi vaikuttaa olennaisten palvelujen toimittamiseen. Haitallinen toiminta havaitaan myös niissä tilanteissa, joissa tavallisen allekirjoituspohjaisen suojauksen eston/tunnistuksen ratkaisuja ei ole mahdollista käyttää.
Kyberturvallisuustapahtumien vaikutus	D1. Reagointi ja palautuksen suunnittelu	On olemassa hyvin määritellyt ja testatut tapahtumienhallintaprosessit, joilla pyritään varmistamaan olennaisten palveluiden jatkuvuus järjestelmä- tai palveluvian sattuessa.
	D2. Tapahtumista oppiminen	Tapahtuman sattuessa ryhdytään toimiin sen juurisyyn ymmärtämiseksi ja varmistetaan, että asianmukaisiin korjaaviin toimiin ryhdytään vastaavien tapahtumien välttämiseksi jatkossa.

Liite 3 Nozomi Networks vs. Defender for IoT käyttöliittymät

Toiminnot	Nozomi Networks	Microsoft Defender for IoT
Käyttöliitty-mä	Teollisuusverkkojen ja OT-ympäristöjen hallintaan optimoitu käyttöliittymä: selkeä, helppokäyt-töinen, tarjoaa käyttäjille kattavan tietoturva-analyysin verkkoon.	Saumattomasti integroitunut Azure Security Centeriin ja Microsoft Sentineliin, selkeä käyttöliittymä, helppokäyttöinen, nopea yleiskat-saus verkon tietoturvaan.
Visuaalisuus	Monipuoliset visualisoinnit lait-teista, yhteyksistä, haavoittu-vuuksista & uhista. Auttaa ym-märtämään verkon rakenteen, nopea ongelmien havaitseminen.	Visuaaliset esitykset laitteista, yhteyksistä, haavoittuvuuksista; helppo navigointi verkon kartalla, yksityiskohtaisten tietojen tarkas-telu eri laitteista
Hälytykset	Reaaliaikaiset hälytykset haavoit-tuvuuksista, hyökkäyksistä, tieto-turvariskeistä; räätälöitävä, käyt-täjän tarpeisiin muokattavissa, priorisoi hälytyksiä vakavuuden perusteella.	Reaaliaikaiset hälytykset haavoit-tuvuuksista, hyökkäyksistä ja tieto-turvariskeistä; mukautettavissa käyttäjän tarpeisiin, priorisoi häly-tyksiä vakavuuden mukaan, teho-kas tietoturvan hallinta.

Liite 4 Nozomi Networks raportoinnin keskeiset alueet

Toiminnot	Sisältö
Haavoittuvuusanalyysi	Paljastaa turvallisuusaukot ja auttaa organisaatioita minimoida riskejä. Tiedot sisältävät haavoittuvuuksien vakavuuden ja vaikutukset verkon toimintaan.
Verkkoliikenteen analyysi	Raporteista saadaan yksityiskohtainen kuvaus verkon liikenteestä, kuten datavirrat, protokollat ja laitteiden yhteydet. Verkkoliikenteen analyysi auttaa organisaatioita havaitsemaan poikkeamia ja riskejä.
Laitteiden inventaario ja konfiguraatio	Laitteiden inventaario ja konfiguraatiotiedot auttavat organisaatioita ymmärtämään verkkolaitteidensa ominaisuuksia ja asetuksia. Tämä mahdollistaa laitteiden hallinnan, ajantasaisuuden varmistamisen ja tietoturvakäytäntöjen parhaan mahdollisen noudattamisen.
Hyökkäysvektorien analyysi	Hyökkäysvektoreita koskevat raportit tarjoavat arvokasta tietoa niiden laajuudesta ja esiintymistiheydestä, auttaen tietoturvatiimejä tunnistamaan ja ehkäisemään potentiaalisia hyökkäyksiä tehokkaammin.
Tapahtumien ja hälytysten seuranta	Raportit sisältävät tietoja verkon tapahtumista ja hälytyksistä, mukaan lukien mahdolliset tietoturvaloukkaukset, epäilyttävät toiminnot ja laitteiden toimintahäiriöt. Tapahtumien ja hälytysten seuranta auttaa organisaatioita reagoimaan nopeasti mahdollisiin ongelmiin ja estämään niiden eskaloitumisen.
Trendianalyysi	Raportit sisältävät tietoa verkkoturvallisuuden kehityksestä ja trendeistä aikajänteellä. Analyysi auttaa organisaatioita havaitsemaan verkon käyttäytymismuutoksia ja tehostamaan tietoturvatoimenpiteitään.

Liite 5 Defender for IoT -raportoinnin keskeiset alueet

Toiminnot	Sisältö
Tietoturvaraportit	Raportit sisältävät yksityiskohtaisia tietoja havaituista haavoittuvuuksista, uusista tunnistetuista laitteista ja muista tietoturvaan liittyvistä tapahtumista.
Hyökkäystunnistus ja hälytykset	Tunnistaa automaattisesti tunnettuja ja tuntematto-mia hyökkäyksiä OT- ja IoT-verkoissa käyttämällä koneoppimista ja käyttäytymisanalyysiä. Järjestelmä luo hälytyksiä ja ilmoituksia, jotka auttavat organisaa-tion tietoturva-asiantuntijoita reagoimaan nopeasti uhkiin ja suojaamaan kriittistä infrastruktuuria
Tapahtumahistoria ja trendit	Raportoinnin avulla voimme seurata tapahtu-mahistoriaa ja tunnistaa turvallisuustrendejä. Tämä auttaa havaitsemaan toistuvia ongelmia, kohdista-maan resursseja tehokkaasti ja priori-soimaan turval-lisuusparannuksia.
Integroitavuus muihin tietoturvatyökaluihin	Defender for IoT voidaan integroida muihin tietotur-varatkaisuihin, kuten SIEM-järjestelmiin (esimerkisi Sentinel) ja ITSM-työkaluihin, mikä mahdollistaa keskitetyn tietoturva raportoinnin ja hallinnan koko organisaatiossa.
Yksityiskohtainen laiteanalyysi	Yksityiskohtaiset laiteanalyysiraportit tarjoavat tieto-turva-asiantuntijoille kattavan näkymän laitteiden toimintaan ja tietoturvaan. Näiden tietojen avulla he voivat tunnistaa ja korjata heikkouksia, ennaltaeh-käistä riskejä ja kehittää tehokkaita tietoturvastrate-gioita.
Reaaliaikainen näky-vyys	Reaaliaikaiset raportit tarjoavat jatkuvan kuvan koko OT- ja IoT-ympäristöstä, sisältäen laitteet, niiden vä-listä kommunikointia, käytetyt protokollat ja verkko-tiedot, mikä mahdollistaa nopean reagoinnin ja tieto-turvan tehokkaan hallinnan.

Liite 6 Nozomi Networksin edut vs. Defender for Iot

Toiminnot	Sisältö
Etäkeräilijät (Remote Collectors)	Nozomi käyttää etäkeräilijöitä (Remote Collectors), jotka voidaan asentaa eri tietoturva vyöhykkeille. Tämä mahdollistaa liikenteen keräämisen erikseen turvavyöhykkeeltä ilman, että jokaiselle aliverkolle tarvitsee asentaa erillinen OT-IDS-laite. Tämä voi vähentää kustannuksia ja yksinkertaistaa ylläpitoa.
Mukautettavuus	Nozomi tarjoaa laajan valikoiman mukautusvaihtoehtoja, joiden avulla voidaan räätälöidä ratkaisut omiin tarpeisiin ja vaatimuksiin. Tämä voi olla erityisen hyödyllistä, jos OT-ympäristössä on erityisvaatimuksia tai ainutlaatuisia haasteita, joihin Defender for IoT ei välttämättä pysty vastaamaan yhtä hyvin.
Erikoistuneet analyysityökalut	Nozomi tarjoaa monia erikoistuneita työkaluja ja analyysimenetelmiä, jotka on suunniteltu erityisesti teollisuusympäristöjen haavoittuvuuksien ja uhkien havaitsemiseksi. Nämä työkalut voivat tarjota syvällisempää analyysiä ja paremman ymmärryksen OT-ympäristön turvallisuudesta verrattuna Defender for IoT -ratkaisuun.
Teollisuuden erityisosaaminen	Nozomi on keskittynyt nimenomaan teollisuuden tietoturvaan ja OT-ympäristöihin, joten ratkaisu on suunniteltu vastaamaan erityisesti teollisuuden tarpeisiin ja haasteisiin. Vaikka Microsoft Defender for IoT tarjoaa monipuolisen ratkaisun, se ei välttämättä ole yhtä erikoistunut teollisuusympäristöihin kuin Nozomi.

Lähdeluettelo

1. Reasons Enterprises Are Slow to Adopt Machine Learning. Verkkodokumentti. https://www.appdynamics.com/blog/product/8-reasons-enterprises-are-slow-to-adopt-machine-learning/. Luettu 21.12.2020
2. Framework for Improving Critical Infrastructure Cybersecurity. Verkkodokumentti. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Luettu 21.12.2020
3. NIST Cybersecurity Framework Overview. Verkkodokumentti. https://www.n-able.com/blog/nist-framework-cybersecurity. Luettu 1.2.2021
4. NIST Cybersecurity Framework vs ISO 27001/27002 vs NIST 800-53 vs Secure Controls Framework. Verkkodokumentti. https://www.complianceforge.com/faq/nist-800-53-vs-iso-27002-vs-nist-csf.html. Luettu 13.2.2021
5. A Comprehensive Guide to Operational Technology (OT) Cybersecurity. Verkkodokumentti. https://www.missionsecure.com/ot-cybersecurity. Luettu 21.2.2021
6. How ISO 27002:2022 can help critical infrastructures achieve compliance with NIS2 directive. Verkkodokumentti. https://www.netcompany-intrasoft.com/blog/how-iso-270022022-can-help-critical-infrastructures-achieve-compliance-nis2-directive. Luettu 14.3.2021
7. Critical infrastructure and cybersecurity. Verkkodokumentti. https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en. Luettu 18.3.2021
8. Kyberturvallisuus: miten EU torjuu kyberuhkia? Verkkodokumentti. https://www.consilium.europa.eu/fi/policies/cybersecurity/#challengeswww.consilium.europa.eu/. Luettu 15.4.2022
9. EBOOK European NIS Directive Compliance Guide. Verkkodokumentti. https://6940570.fs1.hubspotusercontent-na1.net/hubfs/6940570/NIS-Directive-Implementation-Guide.pdf?hsCtaTracking=2f5ae9f4-3376-4b4c-8f91-8d8dc7eb8cb6%7C7c94cee9-2464-4d7a-9c8b-b32c1ea42dba
10. How EU Legislators Can Improve the NIS 2.0 Directive. Verkkodokumentti. https://www.paloaltonetworks.com/blog/2022/01/how-eu-legislators-can-improve-the-nis-2-0-directive/. Luettu 28.10.2022

11. Is the Purdue Model Relevant in a World of Industrial Internet of Things (IIoT) and Cloud Services? Verkkodokumentti. https://www.missionsecure.com/blog/purdue-model-relevance-in-industrial-internet-of-things-iiot-cloud. Luettu 25.5.2021
12. Practices for Security of Internet of Things – ENISA. (pdf)
13. Building ICS cyberdefenses using NIST guidelines, Purdue Model, IEC 62443 standards. Verkkodokumentti. <https://industrialcyber.co/it-ot-collaboration/building-ics-cyberdefenses-using-nist-guidelines-purdue-model-iec-62443-standards. Luettu 13.5.2021
14. What Is the Purdue Model for ICS Security? Verkkodokumentti. https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security. Luettu13.6.2021
15. Go inside the new Azure Defender for IoT including CyberX. Verkkodokumentti. https://www.microsoft.com/en-us/security/blog/2020/11/25/go-inside-the-new-azure-defender-for-iot-including-cyberx/. Luettu 22.5.2021
16. How Microsoft Defender for IoT can secure your IoT devices. Verkkodokumentti. https://www.microsoft.com/en-us/security/blog/2021/11/02/how-microsoft-defender-for-iot-can-secure-your-iot-devices/ 5.12.2021
17. Microsoft Defender for IoT documentation for organizations. Verkkodokumentti. https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/
18. ITI Issues Global Policy Principles for Security Incident Reporting. Verkkodokumentti. https://www.itic.org/news-events/news-releases/iti-issues-global-policy-principles-for-security-incident-reporting. Luettu 9.9.2021
19. Critical Infrastructure: What is NIS2? Verkkodokumentti. https://www.logpoint.com/en/blog/critical-infrastructure-what-is-nis2/. Luettu 2.12.2022
20. How azure sentinel different from other SIEM leaders? Verkkodokumentti. https://techcommunity.microsoft.com/t5/azure-sentinel/how-azure-sentinel-different-from-other-siem-lead ers/m-p/1 509 426. Luettu 26.12.2021
21. What Is Microsoft Sentinel? Verkkodokumentaatio. https://aspiretss.com/cloudautomation/MicrosoftSentinel. Luettu 15.9.2022
22. Azure Sentinel and its Components | Complete Guides. Verkkkodokumentti. http://www.xenonstack.com/blog/azure-sentinel-and-its-components/ Luettu 20.2.2023

23. Chapter 6 Azure Defender for IoT. e-kirja. https://learning.oreilly.com/library/view/microsoft-azure security/9780137343461/xhtml/ch06.xhtml#ch06lev1sec1. Luettu 2.1.2021
24. Microsoft Azure Defender for IoT. Verkkodokumentti. https://www.advantech.com/en/products/19bc1aad-9be7-4664-9964-2f3893c6695f/microsoft-azure-defender-for-iot/mod_ecf9fe94-1709-44d4-a62f-a64a61525e24. Luettu 15.8.2021
25. Microsoft Sentinel vs. Microsoft Defender for Cloud. Verkkodokumentti. https://www.predicagroup.com/blog/azure-sentinel-vs-azure-security-center/. Luettu 11.11.2022
26. Nozomi Networks launches Vantage. Verkkodokumentti. https://securityonscreen.com/nozomi-networks-launches-vantage/. Luettu 27.11.2021
27. SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security. Verkko-dokumentti. https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final. Luettu 28.11.2020
28. Get CEF-formatted logs from your device or appliance into Microsoft Sentinel. Verkkodokumentti. < https://learn.microsoft.com/en-us/azure/sentinel/connect-common-event-format. Luettu 1.10.2022
29. System architecture for OT system monitoring. Verkkodokumentti. https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/architecture. Luettu 2.2.2021
30. Troubleshoot the sensor and on-premises management console - Microsoft De-fender for IoT | Microsoft Learn. Verkkodokumentti. https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/overview. Luettu 3.3.2021
31. How the Nozomi Networks Solution Supports the NIST Cybersecurity Framework. Verkkodokumentti. https://www.fbcinc.com/source/virtualhall_images/AFCEA_21/Nozomi/Nozomi-Networks-NIST-CSF-Compliance-Mapping-Guide.pdf. Luettu 5.4.2021
32. OT sensor cloud connection methods. Verkkodokumentti. https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/architecture-connections. Luettu 1.3.2023
33. NIS2 Directive compliance mapping guide. Verkkodokumentti.

https://www.nozominetworks.com/landing/nis-2-directive-compliance-mapping-guide/ Luettu 21.12.2022

34. Microsoft Defender for IoT Verkkodokumentti. https://4sysops.com/archives/overview-microsofts-security-portfolio-under-the-defender-brand/ Luettu 21.1.2023
35. View the event timeline. Verkkodokumentti https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/how-to-track-sensor-activity/ Luettu 22.1 2023
36. Get CEF-formatted logs from your device or appliance into Microsoft Sentinel. Verkkodokumentti.https://learn.microsoft.com/en-us/azure/sentinel/connect-common-event-format/ Luettu 1.11.2022
37. Nozomi Networks Solution Architecture. Verkkodokumentti. https://www.ikarussecurity.com/en/about-ikarus/partner/ikarus-technology-partner/nozomi-networks/ Luettu 9.9.2022
38. Central Management Console. Verkkodokumentti. https://www.maps.com.mx/nozomi-quickly-detect-ot-iot-threats/ Luettu 5.4.2022
39. Continuously monitor your networks and automation systems. Verkkodokumentti. https://www.nozominetworks.com/products/guardian/ Luettu 2.3.2021
40. Risk Assesment Report. Verkkodokumentti. https://www.advantech.com/en/products/19bc1aad-9be7-4664-9964-2f3893c6695f/microsoft-azure-defender-for-iot/mod_ecf9fe94-1709-44d4-a62f-a64a61525e24/ Luettu 30.2.2022
41. Validate the Sensor. Verkkodokumentti**.** https://techcommunity.microsoft.com/t5/microsoft-defender-for-iot-blog/how-to-quick-start-with-defender-for-iot-sensor-onboarding-and/ba-p/2278028 / Luettu 12.6.2022.
42. Continuously monitor your networks and automation systems. Verkkodokumentti. https://www.nozominetworks.com/products/guardian/ Luettu 18.4.2021
43. View the device inventory. Verkkodokumentti. https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/how-to-investigate-all-enterprise-sensor-detections-in-a-device-inventory?tabs=manually / Luettu 3.3.2022

44. Threat Intelligence. Verkkodokumetti. https://www.nozominetworks.com/labs/ Luettu 21.4.2022
45. What’s the difference between an asset and a node. Verkkodokumentti. https://community.nozominetworks.com/knowledgebase/difference-between-asset-and-node.html / Luettu 25.5.2021
46. Asset Inventory. Verkkodokumentti. https://passport.exclusive-networks.it/upload/workdoc/Nozomi_OT_Security_webinar18072919.pdf / Luettu 15.10.2022
47. Defender for IoT device inventory. Verkkodokumentti. https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/device-inventory#device-inventory-column-data / Luettu 2.2.2023
48. Continuously monitor your networks and automation systems. Verkkodokumentti. https://www.nozominetworks.com/products/guardian/ Luettu 12.12.2021