Liite: OSINT

Janne Taponen, Teollisuusautomaation tietoturva-asiantuntija, F-Secure Oyj

Avoimia lähteitä hyödyntävä tiedustelu eli OSINT (Open-Source Intelligence) on alun perin 1940-luvun alkupuolelta lähtöisin oleva sotilastiedustelun käyttämä termi informaation keräämiseen vieraiden valtojen avoimista lähteistä, esim sanomalehdet, radiolähetykset ja lehtiartikkelit. OSINT:n avulla eri maiden sotilastiedustelut pyrkivät saamaan käsiinsä julkista informaatiota, joka saattaa vahingossa paljastaa kriittisiä yksityiskohtia vihollisesta osaavalle katsojalle. [bellingcat]

Internetin räjähdysmäinen kasvu 1990-luvun puolivälin jälkeen sekä 2001 New Yorkissa tapahtuneet terrori-iskut ja niitä seuranneet terrorismin vastaiset sodat nostivat ensimmäisen ja toisen maailmansodan jälkeen unohtuneen avoimien lähteiden tiedustelun uudelleen tärkeäksi osaksi sotilastiedustelua ja strategisen tilannekuvan muodostamista.

Tekniikoiden ja menetelmien tullessa laajempaan tietoon, internet sekä avoimien tietolähteiden eksponentiaalinen lisääntyminen ovat tuoneet, aiemmin vain sotilasorganisaatioiden resursseilla mahdollisen, tiedustelun lähes jokaisen saataville. Tätä muutosta ovat erityisesti vauhdittaneet monipuoliset ja helposti käytettävät internetin hakukoneet.

Nykyään avoimista lähteistä tehtävää tiedustelua voi yksinkertaisimmillaan olla esimerkiksi tuotearvostelujen etsiminen keskustelufoorumeilta, tuntemattoman puhelinnumeron selvittämistä internetin hakukoneen avulla tai vaikka lisätietojen hakemista uudesta työnantajasta tai ostettavasta asunnosta. Julkisten hankintojen kilpailutuksissa käytettävä HILMA-järjestelmä on valitettavasti myös hyökkääjille tehokas ”tietolähde”, sillä siellä hankinnan yksityiskohdista on käytännössä pakko julkisesti kertoa ”liikaa” (esim. hankinnan kohteen tietoturvavaatimukset, jotka paljastavat yksityiskohtia kohteen lisäksi myös kohdeorganisaation tietoturvallisuudesta).

Tiedon luokittelu

Lukijalle saattaa herätä kysymys mitä yhteistä on 1940-luvun sotilastiedustelutekniikoilla ja puhelinnumeron omistajan selvittämisellä hakukonetta käyttämällä, ja erityisesti miten nämä liittyvät automaation tietoturvaan. Vastaus kysymykseen on tiedon luokittelu. Yhdestä lähteestä löytyvä pieni tiedon jyvänen saattaa itsenäisenä yksikkönä olla täysin merkityksetön, mutta tietylle katsojalle, joka on haalinut tietoa myös sadoista muista lähteistä, tämä pieni tiedon jyvänen saattaa olla ainoa puuttuva palanen laajemman ymmärryksen muodostamiseksi.

Esimerkiksi lehdistötiedotteessa oleva kuva teollisuuslaitoksen uudesta järjestelmästä tai uuden tuotantolinjan avajaisista, jossa kuvan taustalla näkyy valvomonäyttö, saattaa olla suurimmalle osalle kuvan näkevistä pelkkä lehdistökuva ilman sen suurempaa merkitystä. Kuitenkin esimerkiksi aktiivisesti yrityksestä ja sen laitoksista informaatiota keräävälle hyökkääjälle samainen kuva saattaa sisältää huomattavan määrän arvokasta tietoa. Näitä pieniä tiedon jyväsiä saattaa olla esim. näkyvissä olevat järjestelmätoimittajien nimet, valvomonäytössä näkyvät kuvat prosessiin liittyvistä laitteista, valvomonäytössä näkyvät identifioivat tiedot kuten IP-osoitteet, DNS-nimet, hälytykset, kuvissa olevat henkilöt, yms.

Tiedon arvo riippuu loppukädessä tiedon katsojasta ja katsojan keräämästä muusta informaatiosta, sekä kyvystä yhdistää pienistä tiedonjyväsistä laajempi tilannekuva, aivan kuten jo 1940-luvun sotilastiedustelijatkin tekivät.

Automaatiojärjestelmiä vastaan tehtävän kohdennetun hyökkäyksen elinkaari

Jotta on mahdollista ymmärtää mitkä tiedot ja tiedonjyväset mahdollisesti paljastavat kriittistä tietoa, on tärkeää ymmärtää automaatiojärjestelmiä vastaan tehtävän kohdennetun hyökkäyksen elinkaari [SANS]. OSINT on yleensä nimenomaan kohdennetuissa hyökkäyksissä käytettävä tekniikka, sillä hyökkääjä pyrkii hankkimaan itselleen mahdollisimman paljon tietoa ennen varsinaisen hyökkäyksen aloittamista, jotta kiinnijäämisen riski pienenisi ja rajalliset hyökkäysresurssit saataisiin kohdennettua oikeisiin kohteisiin. Vaikka OSINT-tekniikoita hyödynnetään pääasiassa hyökkäyksen tiedusteluvaiheessa, käyttävät monet hyökkääjät sitä myös hyökkäyksen muissa vaiheissa täydentämään esimerkiksi sisäverkoista löydettyä tietoaineistoa.

Kuva 1 Automaatiojärjestelmiä vastaan tehtävät hyökkäykset lähtevät usein liikkeelle IT- ja toimistoverkon järjestelmistä, joihin hyökkääjä hankkii ensin pääsyn.

Ensimmäisessä vaiheessa hyökkääjä pyrkii keräämään mahdollisimman paljon tietoa kohteestaan, sekä etsimään mahdollisesti haavoittuvia järjestelmiä. Varsinainen tunkeutuminen tapahtuu yleensä joko kerätyn tiedon pohjalta löytyneen haavoittuvan järjestelmän kautta tai hyödyntämällä sosiaalisen hakkeroinnin (social engineering) tekniikoita, esim. kohdennettuja kalastelusähköposteja (phishing). Nykyään monet hyökkäykset alkavatkin juuri sähköpostin mukana tulleen liitetiedoston kautta, jolloin hyökkääjä pääsee monesti suoraan kohteensa sisäverkkoon.

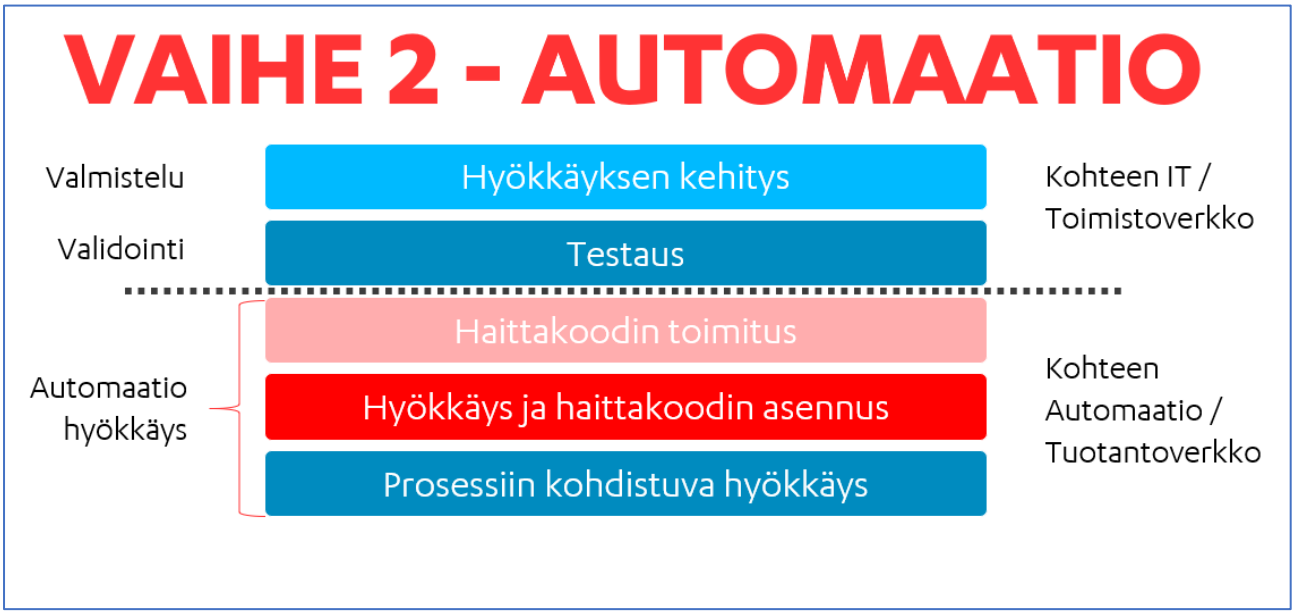
Sisäverkkoon päästyään pyrkivät hyökkääjät yleensä ensimmäisenä varmistamaan oman etähallintansa luotettavuuden ja saamaan pysyvän pääsyn kohteen järjestelmiin (persistence). Pysyvä pääsy pitää huolen, että mikäli yhteys hyökkääjään katkeaa, pystyy hän saamaan sen kohteeseen uudelleen.

Pysyvän pääsyn saatuaan pyrkivät hyökkääjät yleensä laajentamaan pääsyään muihin sisäverkon järjestelmiin ja keräämään mahdollisimman paljon tietoa esim. käyttäjätunnuksia. Tavoitteena hyökkääjällä on saavuttaa riittävän laaja pääsy eri laitteisiin ja palveluihin yrityksen sisällä, jotta pääsy lopulliseen kohteeseen, kuten automaatioverkkoihin tulee mahdolliseksi.

Vaikka automaatioverkot olisi erotettu oikeaoppisesti palomuurilla, monesti IT ja automaatioverkkojen välillä on kuitenkin järjestelmiä, jotka keskustelevat keskenään, hyvä esimerkki näistä on MES (manufacturing execution system, tuotannonohjausjärjestelmä), joka sijaitsee yleensä automaatioverkon puolella ja ERP (enterprise resource planning, toiminnanohjausjärjestelmä), joka taas yleensä sijaitsee IT verkon puolella. MES ja ERP järjestelmien välillä menee kuitenkin usein suuria määriä dataa, kuten esimerkiksi ostotilaukset (purchase order), reseptiikka, tuotetut määrät ja

varastosaldot. Tästä syystä monesti myös palomuurin sääntökanta ERP ja MES järjestelmien välisen kommunikaation osalta on saattanut jäädä liian avoimeksi.

Hyökkääjän ottaessa haltuun enemmän ja enemmän yrityksen järjestelmiä mahdollistuu monesti näiden järjestelmien kautta pääsy myös automaatioverkkoon ja näin ollen mahdollistuu hyökkäyksen toinen vaihe.



Kuva 2 Vaiheessa 2 hyökkääjä on hankkinut pääsyn automaatioverkon laitteisiin ja pyrkii tekemään kohdistetun hyökkäyksen näihin resursseihin.

Automaatioverkkoon päästyään hyökkääjillä on yleensä muutamia päävaihtoehtoja, se miten hyökkääjä pyrkii etenemään hyökkäyksessä, riippuu lopullisesta tavoitteesta. Tavoitteita voi olla esimerkiksi nopea ja tuhoisa hyökkäys, jossa ympäristöön laitetaan vaikka kiristyshaittaohjelma (ransomware), joka leviää tuotantoa ylätasolla hallinnoiviin, yleensä Windows-pohjaisiin järjestelmiin. Tämän tyylinen hyökkäys on resurssitarpeeltaan huomattavasti vaatimattomampi kuin kohdennetun tavoitteen täyttäminen, esimerkiksi tuotteen laadun asteittainen heikentäminen muuttamalla prosessin parametreja. Kohdennetun hyökkäystavoitteen täyttäminen vaatii yleensä merkittävän määrän tutkimusta ja selvitystyötä prosessiin liittyen, sekä monialaisen hyökkäysorganisaation. Monialaisen siksi, että yleensä prosessin parametrien kontrolloitu muuttaminen vaatii automaatiolaitteiden murtamisen lisäksi myös kyseisen toimialan kuten kemian tai prosessitekniikan syvällistä osaamista.

OSINT työkalut ja tietolähteet

OSINT-tiedusteluun käytettäviä työkaluja ja tietolähteitä on nykyään erittäin suuri määrä. Valmiita työkaluja on kehitetty mm. puhelinnumeroiden ja sähköpostiosoitteiden hakemiseen ja domainien (verkkotunnus, esim. ”suomi.fi”) kartoitukseen. Hyvä lähtökohta OSINT-tiedustelun tekemiselle on OSINT Framework-sivusto [osintframework], joka tarjoaa kattavan yleiskuvan erilaisista ilmaisista

OSINT-työkaluista ja tietolähteistä. Sivustolla eri työkalut ja tietolähteet on (graafisesti) jaoteltu aihealueittain, joten kokematonkin käyttäjä löytää hyvin helposti käyttökelpoisia OSINT-työkaluja.

Tässä kappaleessa pyritään käymään läpi muutamia helppokäyttöisiä työkaluja ja tietolähteitä, joita käyttämällä OSINT-tiedustelussa voi päästä hyvään alkuun. Ihmisiin kohdistuva OSINT tiedustelu, sekä siihen liittyvät työkalut, on tarkoituksella jätetty pois.

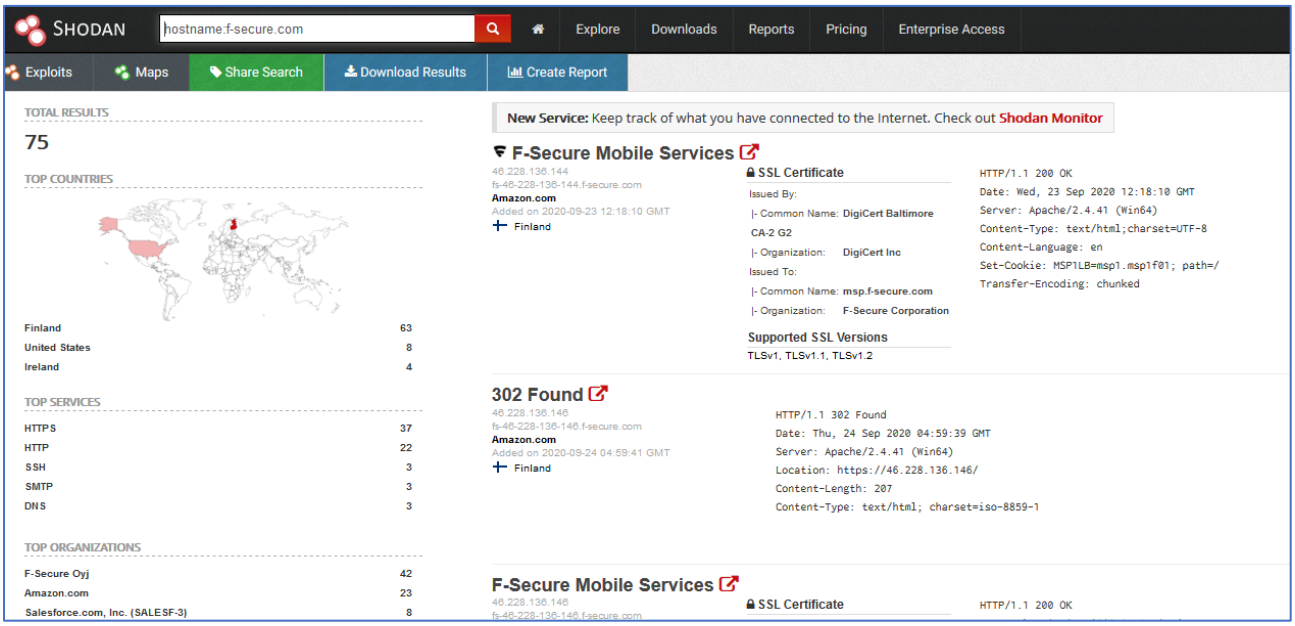
Hakukoneet ovat usein hyödyllisimpiä yleiskäyttöisiä työkaluja, kuten esimerkiksi Google, Bing ja DuckDuckGo. Jo pelkästään näitä hakukoneita oikein käyttämällä on mahdollista löytää huomattava määrä (piiloon jäänyttä) tietoa. Tällaista tietoa voivat olla esimerkiksi yrityksen nettisivujen kautta vahingossa vuodetut luottamukselliset dokumentit tai piiloon jääneet sisäänkirjautumissivut (login-sivut). Esimerkiksi Googlen hakukoneelle löytyy erittäin kattava tietokanta (Google Hacking Database, GHDB) [ghdb], josta löytyy valtava määrä erilaisia kohdennettuja Google-hakuja. Hakujen avulla on mahdollista etsiä esim. SAP:n login-sivuja, automaatiolaitteisiin sisäänrakennettujen web-palvelimien etusivuja, tai vaikkapa salasanoja sisältäviä tiedostoja. Haut toimivat myös hyvinä esimerkkeinä siitä, miten Googlen erilaiset hakuoperaattorit toimivat. Hakuoperaattoreilla voi tehostaa ja tarkentaa Google-hakuja huomattavasti.

Organisaation julkisen IP-osoiteavaruuden, avoimien porttien, sekä käytössä olevien verkkotunnusten ja aliverkkotunnusten hakuun on olemassa myös erinomaisia helppokäyttöisiä työkaluja. Näitä käydään läpi seuraavaksi.

SHODAN-HAKUKONE

Shodan-hakukoneen (www.shodan.io) palvelimet käyvät jatkuvasti läpi koko internetiä ja indeksoivat siihen liitettyjä laitteita. Shodanin kautta on siis mahdollista hakea (lähes) mitä tahansa julkiseen internetiin liitettyä laitetta. Vastauksen saatuaan Shodan indeksoi laitteen avoimet portit, niissä mahdollisesti pyörivät palvelut, näistä saadut vastaukset ja esimerkiksi palvelinohjelmistojen versiotiedot.

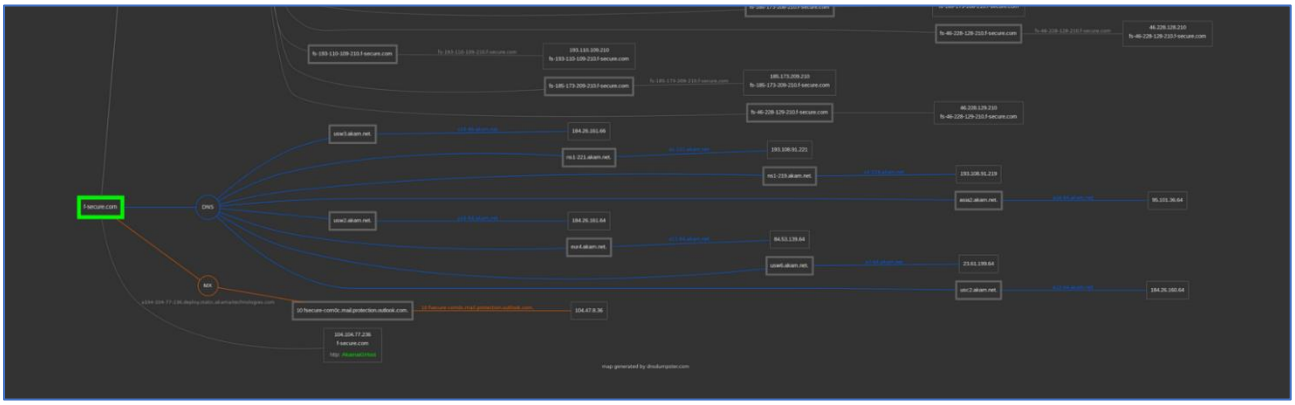
Rekisteröimällä Shodaniin (ilmaisen) käyttäjätunnuksen saa mahdollisuuden käyttää myös Shodanin laajempia hakutyökaluja ja hakuoperaattoreita. Erinomaisia esimerkkejä Shodan-hauista voi löytää myös GitHub-sivuilta [shodan-haut].



Kuva 3 Shodan-hakukoneen tuloksia, esimerkkinä ”f-secure.com” -haku.

DNSDUMPSTER-Hakukone

DNSDumpster hakukone tekee hakuja moniin erilaisiin tietolähteisiin DNS-nimeä käyttämällä. Yksinkertaisimmillaan tämä voi olla esimerkiksi organisaation verkkotunnus, kuten ”*suomi.fi*”. Hakujen tuloksena DNSDumpster palauttaa tiedot haetusta DNS-nimestä, siihen liittyvät IP-osoitteet, sekä mahdolliset muut DNS-nimet, esimerkiksi aliverkkotunnukset. Haetuista tiedoista DNSDumpster pyrkii muodostamaan selkeän puurakenteen, joka kertoo miten löydetyt tulokset liittyvät toisiinsa.



Kuva 4 DNSDumpster hakukoneen luoma domain-puurakenne.

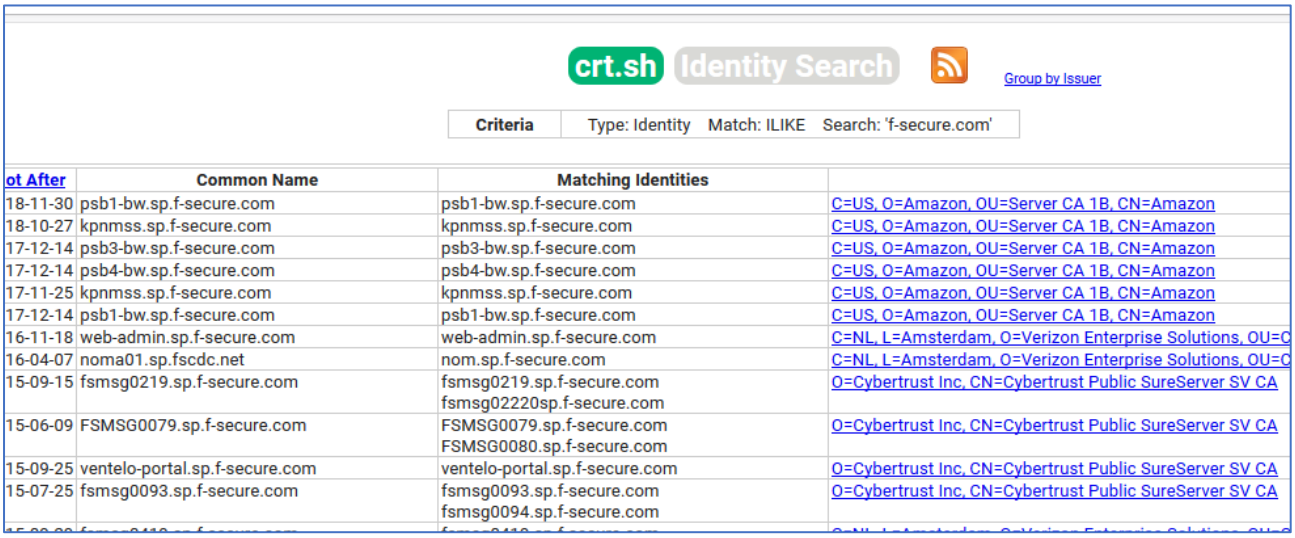
CRT.SH-Sertifikaattihakukone

Nykyään suurin osa internetiin kytketyistä laitteista käyttää jonkinlaista sertifikaattia. Usein sertifikaateilla varmennetaan vastapuolen identiteetti. Toisaalta sertifikaattien sisältämiä julkisia avaimia voidaan käyttää tietoliikenteen salaamiseen. Paras esimerkki, tästä normaalille käyttäjälle yleensä näkymättömästä infrastruktuurista, on internetselaimen ”vihreä lukko”-kuvake osoiterivillä.

Tämä ”vihreä lukko”-kuvake tarkoittaa sitä, että datayhteys on salattu ja vastapuolen identiteetti on varmennettu.

Identiteettien varmistusketjun ja sertifikaattien on oltava läpinäkyviä, ts. kaikkien osapuolten tulee olla mahdollista varmistaa, että käytössä olevat sertifikaatit ovat autenttisia, voimassaolevia, ja että luotettava organisaatio on myöntänyt (allekirjoittanut) ne.

Läpinäkyvyys mahdollistaa taustalla käytettävän julkisten avainten menetelmän (public-key cryptography) toiminnan, mutta myös altistaa tietyille ongelmille. Sertifikaatit nimittäin sisältävät suuren määrän tietoa, sekä hakijaorganisaatioista että kohteista, joille sertifikaatti on myönnetty. Käyttämällä crt.sh-hakukonetta on mahdollista hakea esim. yrityksen tai verkkotunnuksen perusteella kaikkia myönnettyjä sertifikaatteja. Hakujen avulla on mahdollista muodostaa kuva yrityksen käyttämistä aliverkkotunnuksista ja monesti hakutuloksista löytyy myös ei-julkisia ja sisäisten järjestelmien osoitteita, jos niille on haettu oma sertifikaattinsa.



crt.sh Identity Search Group by Issuer

Criteria Type: Identity Match: ILIKE Search: 'f-secure.com'

ot After	Common Name	Matching Identities	
18-11-30	psb1-bw.sp.f-secure.com	psb1-bw.sp.f-secure.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
18-10-27	kpnmss.sp.f-secure.com	kpnmss.sp.f-secure.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
17-12-14	psb3-bw.sp.f-secure.com	psb3-bw.sp.f-secure.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
17-12-14	psb4-bw.sp.f-secure.com	psb4-bw.sp.f-secure.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
17-11-25	kpnmss.sp.f-secure.com	kpnmss.sp.f-secure.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
17-12-14	psb1-bw.sp.f-secure.com	psb1-bw.sp.f-secure.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
16-11-18	web-admin.sp.f-secure.com	web-admin.sp.f-secure.com	C=NL, L=Amsterdam, O=Verizon Enterprise Solutions, OU=C
16-04-07	noma01.sp.fscdc.net	nom.sp.f-secure.com	C=NL, L=Amsterdam, O=Verizon Enterprise Solutions, OU=C
15-09-15	fsmsg0219.sp.f-secure.com	fsmsg0219.sp.f-secure.com fsmsg02220sp.f-secure.com	O=Cybertrust Inc, CN=Cybertrust Public SureServer SV CA
15-06-09	FSMSG0079.sp.f-secure.com	FSMSG0079.sp.f-secure.com FSMSG0080.sp.f-secure.com	O=Cybertrust Inc, CN=Cybertrust Public SureServer SV CA
15-09-25	ventelo-portal.sp.f-secure.com	ventelo-portal.sp.f-secure.com	O=Cybertrust Inc, CN=Cybertrust Public SureServer SV CA
15-07-25	fsmsg0093.sp.f-secure.com	fsmsg0093.sp.f-secure.com fsmsg0094.sp.f-secure.com	O=Cybertrust Inc, CN=Cybertrust Public SureServer SV CA

Kuva 5 CRT.SH -hakukoneen tuloksia löydetyistä domain-nimistä

Theseus- ja Google Scholar-hakukoneet

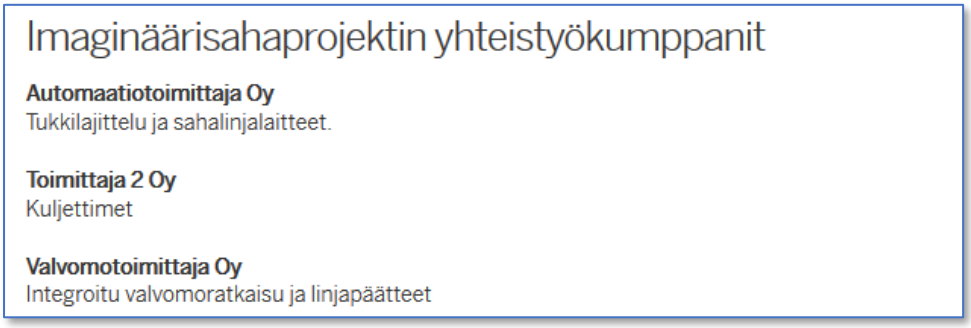
Suomessa ammattikorkeakoulut ja yliopistot julkaisevat uudet päättötyöt oletusarvoisesti kaikkien saataville. Tämä tapa mukailee normaalia tiedeyhteisön ja ylemmän asteen oppilaitosten käytäntöä, jossa tutkimustuloksia pyritään jakamaan ja näin mahdollistamaan hyödyntäminen muissa tutkimuksissa. Päättötyöt kuitenkin sisältävät usein myös huomattavan määrän tietoa päättötyön teettäneestä yrityksestä, sen laitteistoista ja/tai tuotteista. Theseus- (www.theseus.fi) ja Google Scholar-hakukoneet (https://scholar.google.fi) indeksoivat oppilaitosten julkaisemia päättötöitä ja tutkimusraportteja. Hakukoneita käyttämällä on mahdollista helposti löytää yritysten teettämät julkiset päättötyöt ja ladata ne itselleen.

Miten hyökkääjät käyttävät OSINT:n avulla löydettyjä tietoja

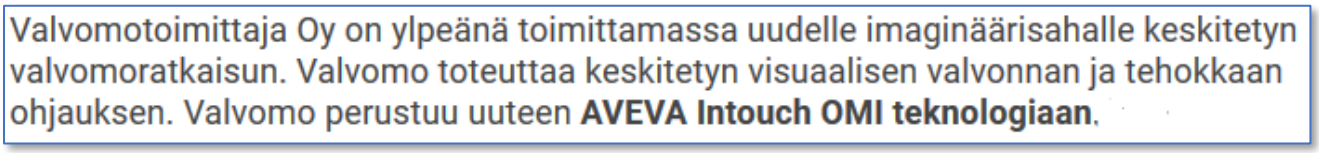
Hyökkääjät pyrkivät yleensä minimoimaan oman näkyvyytensä ja jättämään mahdollisimman vähän jälkiä erityisesti ennen varsinaista hyökkäystä. OSINT-menetelmien avulla passiivisesti kerätyt tiedot mahdollistavat hyökkäysten tarkan suunnittelun. Tässä kappaleessa on esitelty lyhyesti ja hyvin yksinkertaistetusti esimerkki hyökkäyksen valmistelusta kuvitteellisen metsäteollisuuden toimijan sahaa vastaan.

Järjestelmien, järjestelmätoimittajien ja yhteistyökumppaneiden selvitys

Ensimmäisessä vaiheessa hyökkääjä pyrkii kartoittamaan laajasti kohteesta saatavilla olevaa tietoa. Tällaisia voivat olla esimerkiksi lehdistötiedotteissa olevat tiedot yhteistyökumppaneista, järjestelmätoimittajista ja toimitetuista järjestelmistä. Löydettyjen tietojen perusteella on yleensä mahdollista löytää tarkempia tietoja esim. toimittajien omilta sivuilta ja heidän vastaavista aiemmista toimituksistaan.



Kuva 6 Kuvakaappaus imaginäärisahaprojektin kuvitteelliselta nettisivulta

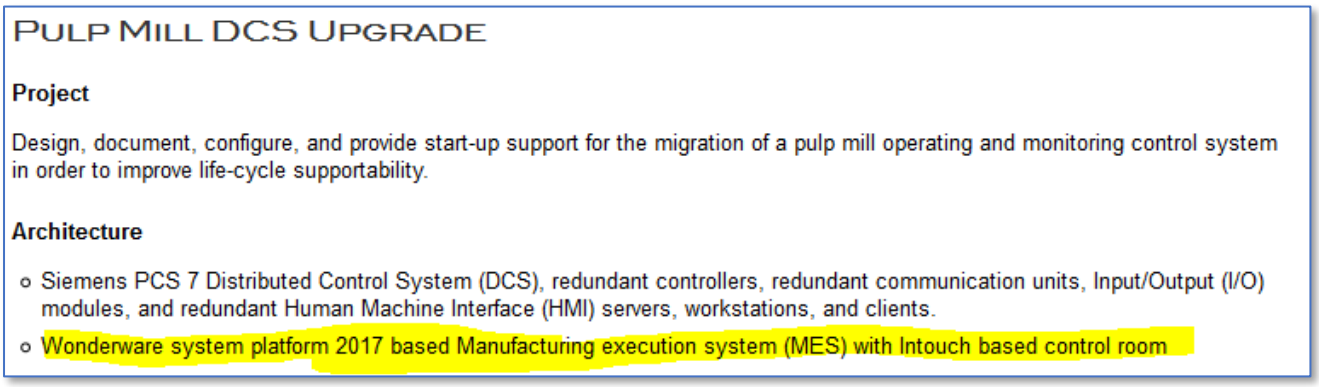


Kuva 7 Kuvankaappaus valvomotoimittajan kuvitteellisilta nettisivuilta

Lehdistötiedotteista löydettyjen tietojen avulla hyökkääjä kiinnittää huomionsa integroidun valvomoratkaisun toimittajaan, sillä suurella todennäköisyydellä kyseinen järjestelmä sisältää laajat yhteydet Imaginäärisahan muihin järjestelmiin. Lisää tietoja kaivamalla hyökkääjä löytää myös lehdistötiedotteen, jossa kerrotaan Imaginäärisahan käyttävän valvomotoimittajan uutta pilvipohjaista tietovarastoa tuotantodatan keskitettyyn tallentamiseen.

Järjestelmien tietojen selvittäminen mahdollisimman tarkasti

Kohdennettuja Google-hakuja käyttämällä hyökkääjän on mahdollista löytää tarkkoja case-study esimerkkejä Valvomotoimittaja Oy:n aikaisemmista toimituksista metsäteollisuuteen. Kaikissa case-study esimerkeissä valvomoratkaisu ja sen taustalla toimiva tuotannonohjausjärjestelmä perustuvat saman valmistajan tuotteisiin ja versioihin.



PULP MILL DCS UPGRADE

Project

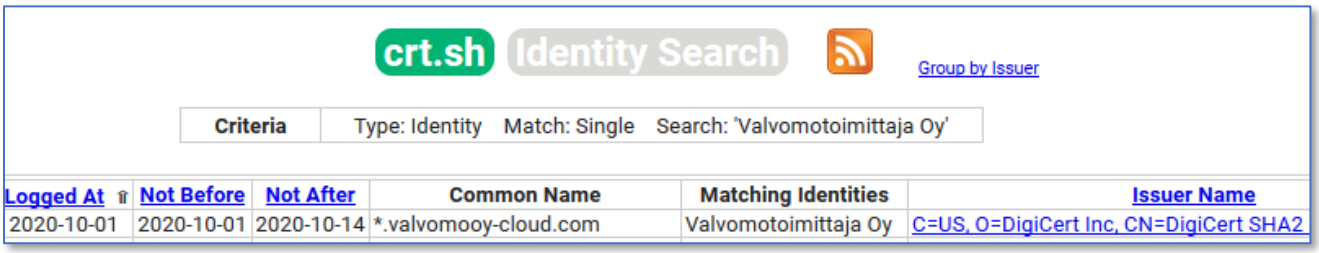
Design, document, configure, and provide start-up support for the migration of a pulp mill operating and monitoring control system in order to improve life-cycle supportability.

Architecture

- Siemens PCS 7 Distributed Control System (DCS), redundant controllers, redundant communication units, Input/Output (I/O) modules, and redundant Human Machine Interface (HMI) servers, workstations, and clients.
- Wonderware system platform 2017 based Manufacturing execution system (MES) with Intouch based control room

Kuva 8 Kuvakaappaus kuvitteellisen valvomotoimittajan aiemman toimituksen case-studysta

Seuraavaksi hyökkääjä pyrkii selvittämään lisätietoja, kuten mahdolliset IP-osoitteet ja avoimet portit Valvomotoimittaja Oy:n käyttämästä pilvipohjaisesta tiedontallennusjärjestelmästä. Hyökkääjä aloittaa etsimällä kaikki Valvomotoimittajan omistamat sertifikaatit ja näitä sertifikaatteja mahdollisesti käyttävät palvelimet.

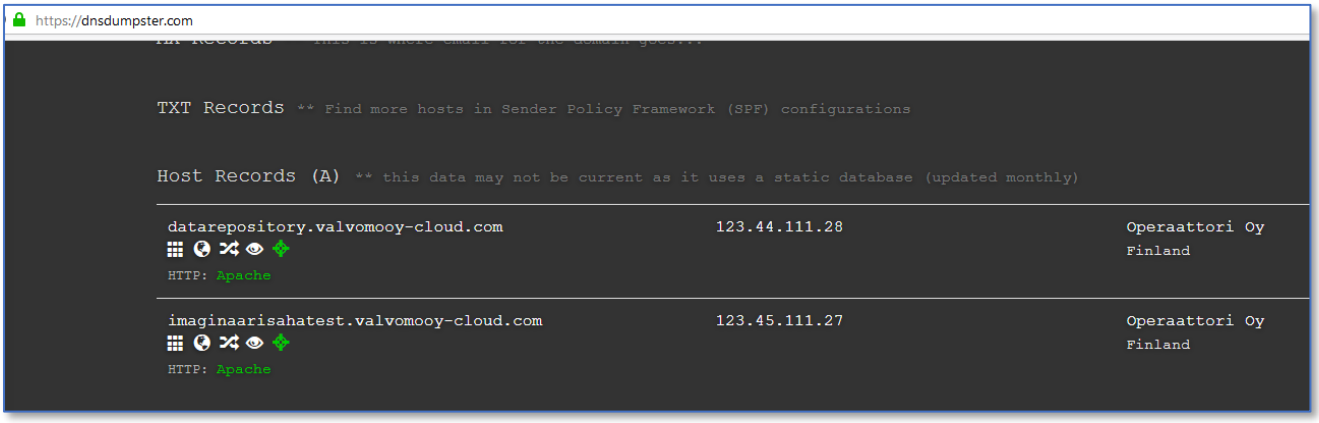


crt.sh Identity Search Group by Issuer

Criteria	Type: Identity	Match: Single	Search: 'Valvomotoimittaja Oy'

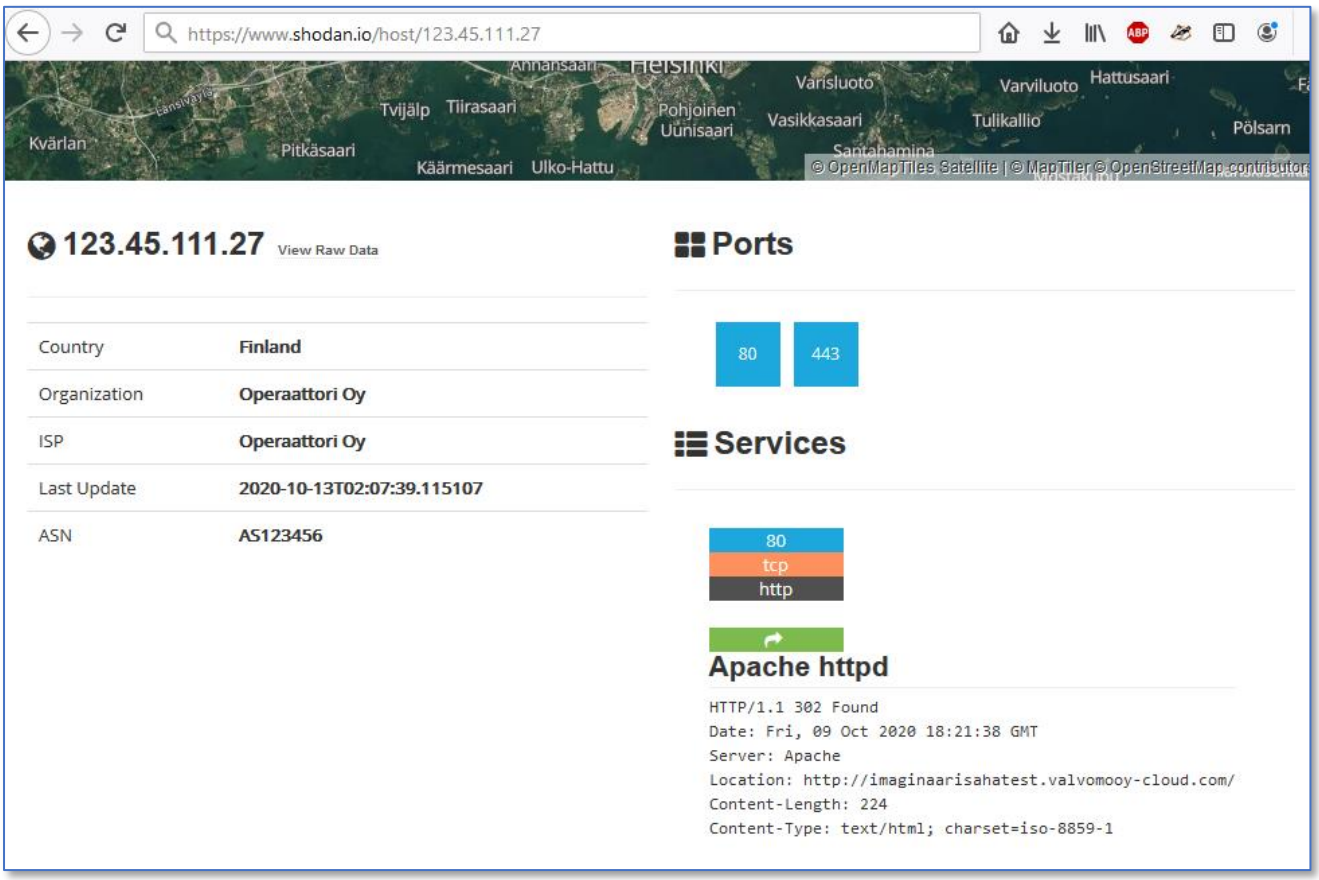
Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
2020-10-01	2020-10-01	2020-10-14	*.valvomooy-cloud.com	Valvomotoimittaja Oy	C=US, O=DigiCert Inc, CN=DigiCert SHA2

Kuva 9 Valvomotoimittajan käyttämien sertifikaattien haku



Kuva 10 Sertifikaatteihin liitettyjen DNS-nimien ja IP-osoitteiden selvittäminen

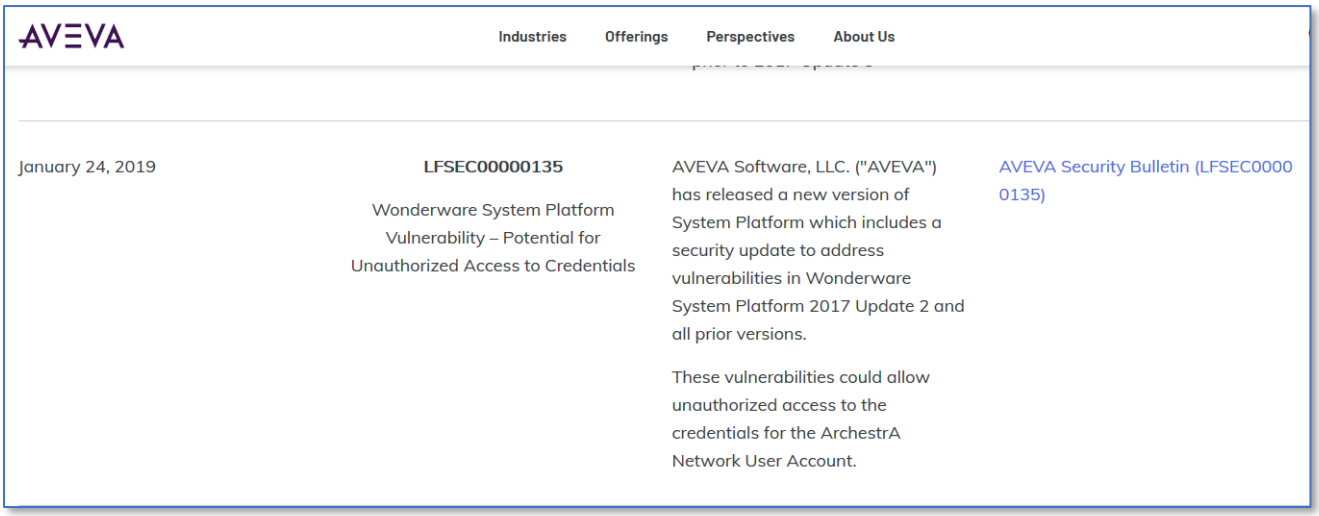
Hyökkääjä löytää kaksi palvelinta sertifikaatti- ja DNS-nimihauilla, sekä näiden palvelimien julkiset IP-osoitteet. Toisen palvelimen DNS-nimi viittaa Imaginäärisahan kehitys- ja testausympäristöön. Käyttämällä Shodan-hakukonetta hyökkääjä löytää kaksi avoinna olevaa porttia testauspalvelimella. Porteissa pyörii Apache -webpalvelinohjelmisto. Näiden tietojen avulla hyökkääjän on mahdollista etsiä lisää tietoa webpalvelinohjelmiston tunnetuista haavoittuvuuksista, sekä kohdistaa hyökkäyksiä suoraan kyseistä testipalvelinta vastaan.



Kuva 11 Sertifikaatteihin liitettyjen DNS-nimien ja IP-osoitteiden selvittäminen

Tunnettujen haavoittuvuuksien etsiminen

Edellä löydettyjen tietojen avulla on mahdollista löytää myös muita mahdollisia hyökkäyskohteita Imaginäärisahaan liittyvistä järjestelmistä. Valvomotoimittaja Oy oli maininnut lehdistötiedotteissaan käyttävänsä Wonderware MES ja Intouch -järjestelmiä valvomojärjestelmänsä pohjana. Case-studeista löytyneen tiedon avulla hyökkääjä voi olettaa, että myös Imaginäärisahalla käytössä oleva ohjelmistoversio on vuodelta 2017. Tämän perusteella hyökkääjän on mahdollista etsiä järjestelmästä löytyviä tunnettuja haavoittuvuuksia, kuten esimerkiksi käyttäjätunnuksien luvaton käyttöönotto. Tämän avulla hyökkääjä kykenee valmistelemaan hyökkäystä merkittävästi jo ennen varsinaista pääsyä Imaginäärisahan ympäristöön.



Kuva 12 Tuotannonohjausjärjestelmän tunnettu haavoittuvuus.

Miten kartoitat oman organisaatiosi julkisen hyökkäyspinta-alan, eli käytännön ohjeita OSINT tekemiseen

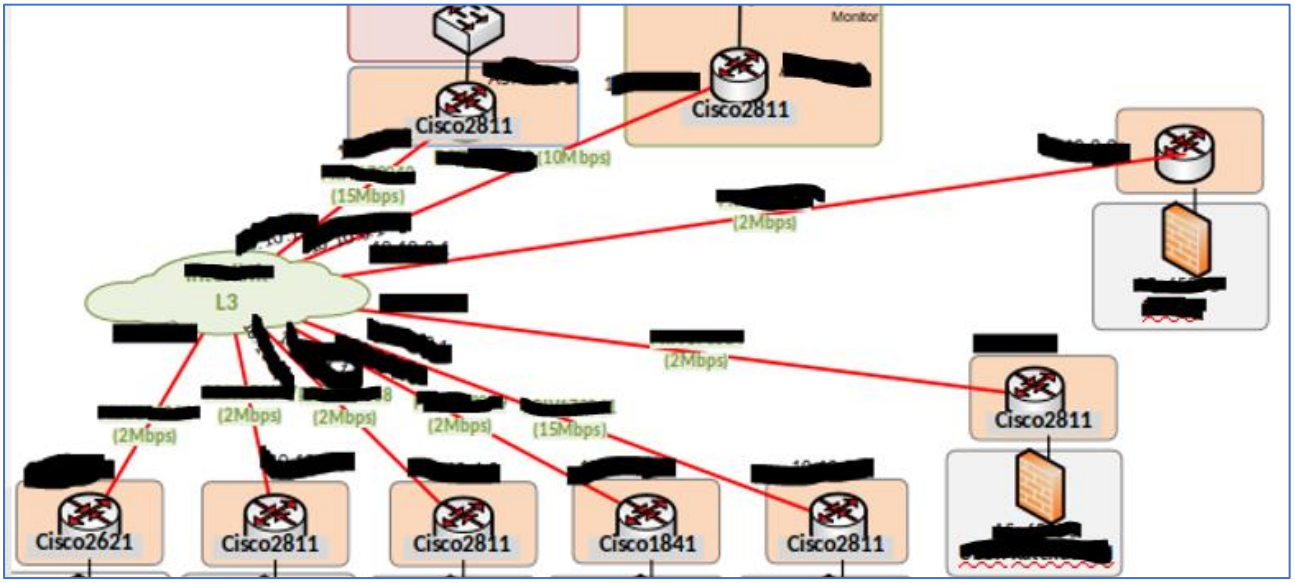
Kappaleissa 0 ja 0 käytyjä tekniikoita ja tietolähteitä hyödyntäen jokaisen on mahdollista kartoittaa omaa julkisesti näkyvää hyökkäyspinta-alaansa. Tässä kappaleessa listataan yksinkertaisia toimenpiteitä, joiden avulla voit selvittää mitä tietoa organisaatiostasi on löydettävissä.

- Tee Google hakuja yrityksesi nimellä, käytä Googlen hakuoperaattoreita ja esimerkkejä GHDB tietokannasta [ghdb]. Hyviä haettavia kohteita ovat esimerkiksi doc, docx ja pdf -päätteiset tiedostot.
- Käy läpi yrityksestäsi julkaistut artikkelit ja uutiset, kiinnitä erityishuomiota julkaisuissa käytettyihin kuviin ja näissä näkyvään informaatioon.
- Hae Theseus- ja Google-scholar hakukoneilla yrityksesi teettämiä päättötöitä ja tarkista mitä informaatiota niistä löytyy.
- Luo crt.sh ja dnsdumpster -työkaluja hyödyntämällä listaus yrityksesi verkkotunnuksista ja tarkista mitkä näistä domaineista tulisi olla yleisessä tiedossa. Löytyykö joukosta esimerkiksi testi- ja kehitysympäristöjä, jotka merkittävästi lisäävät hyökkäyspinta-alaa (ne eivät yleensä ole yhtä hyvin suojattuja kuin tuotantoympäristöt).
- Tarkista Shodan-hakukonetta käyttämällä yrityksesi julkisten IP-avaruuksien avoimet portit, sekä avoimissa porteissa pyörivät palvelut ja näihin liittyvät julkisesti tiedossa olevat haavoittuvuudet. Haavoittuvuuksia voi palvelun nimellä ja versionumerolla hakea esimerkiksi Mitre -nimisen yrityksen ylläpitämästä haavoittuvuuslistauksesta. [mitre]

OSINT:iin liittyvää materiaalia löytyy huomattavasti kirjoista ja internetistä. Eräs hyvä lähdeteos on Michael Bazzellin kirjoittama kirja “Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information”.

Esimerkkejä OSINT:n avulla löydetyistä luottamuksellisista tiedoista

Julkaisemisen riskiarvio oli seuraavissa kuvissa pettänyt, sillä mustatut kohdat paljastivat liian luottamuksellista tietoa kyseisistä kohteista.



Kuva 13 Päättötyöstä löytynyt teollisuusyrityksen verkkoarkkitehtuurikuva.

Kuva 14 Päättötyöstä löytynyt tarkka kuvaus prosessin toimintalogiikasta.

3.1 Control System

The [redacted] Control System consist of:

- Main PLC cabinet [redacted]-0001 installed in Electrical Equipment Room – safe area
- 3 Remote I/O cabinets [redacted]1000, [redacted]2000, [redacted]3000 installed in the [redacted] in the hazardous area - Ex Zone 1
- VFD cabinet for [redacted] installed in Switchboard Room – safe area
- Operator Station (delivered by [redacted])

Main PLC cabinet [redacted]-0001 includes:

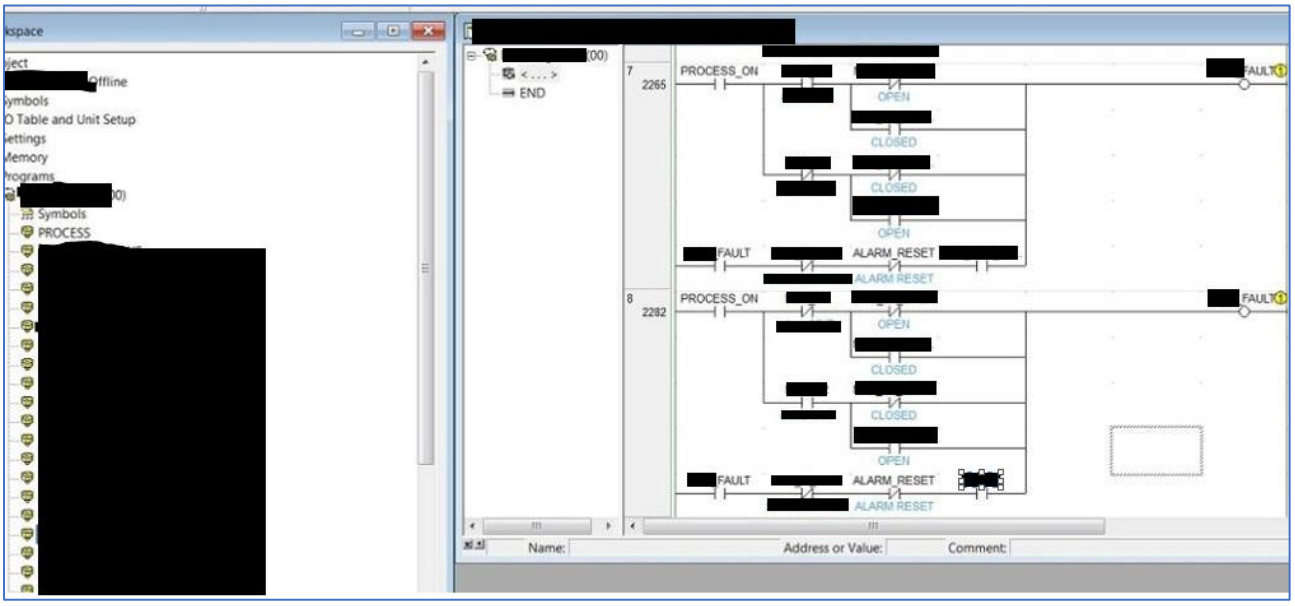
- Redundant PLC process controller – S7-400 with CP communication processors (Profibus DP redundant communication to [redacted])
- S7-1200 controller to separate safety functions from process algorithms - to handle all [redacted] signals
- ET200M I/O station for a local inputs and outputs signals
- [redacted] module for external service functionality

Remote I/O cabinets contains:

- ET200isp Ex I/O stations with Ex I/O modules.

For more details please refer to Topology Block Diagram – [redacted] doc. Id. [redacted]

Kuva 15 Virustotal-palvelusta löytynyt täydellinen kuvaus automaatiojärjestelmästä.



Kuva 16 Kuvakaappaus päättötyöstä, prosessin ohjauslogiikkaa.

2019-02-26	2019-02-01	2020-02-01	sip[redacted]	[redacted]	C=FI, O
2019-02-14	2019-02-14	2021-02-13	secureprintq3[redacted]		C=FI, O
2019-02-14	2019-02-14	2021-02-13	secureprintq2[redacted]		C=FI, O
2019-02-14	2019-02-14	2021-02-13	secureprintmanager[redacted]		C=FI, O
2019-02-01	2019-01-25	2021-01-24	www.[redacted]		C=FI, O
2019-02-01	2019-02-01	2020-02-01	sip.[redacted]		C=FI, O
2019-01-25	2019-01-25	2021-01-24	www.[redacted]		C=FI, O
2019-01-09	2019-01-09	2020-01-09	[redacted]yatest[redacted]		C=FI, O
2019-01-09	2019-01-09	2021-01-08	[redacted]ya[redacted]		C=FI, O
2019-01-09	2019-01-09	2020-01-09	[redacted]dev[redacted]		C=FI, O
2018-12-14	2018-12-14	2020-12-13	[redacted]test[redacted]		C=FI, O
2018-12-14	2018-12-14	2020-12-13	[redacted]		C=FI, O

Kuva 17 DNS-osoitteita sisäisiin resursseihin, sekä kehitys- ja testausympäristöihin.

Lyhenne- ja selitysluettelo

- OSINT = Open-source intelligence, tiedustelu avoimista lähteistä
- IP-osoite = Internet Protocol. Internetin verkkokerroksen protokolla
- DNS = Domain Name System. Internetin nimipalvelu

Viitteet

[bellingcat] = Bellingcat, A Brief History of Open Source Intelligence, 17.9.2020, https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/
[osintframework] = https://osintframework.com/, 24.9.2020
[ghdb] = https://www.exploit-db.com/google-hacking-database, 24.9.2020
[shodan-haut] = https://github.com/jakejarvis/awesome-shodan-queries, 24.9.2020
[SANS] = https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297, 13.10.2020
[mitre] = https://cve.mitre.org/, 13.10.2020

...
Tämä on liite kirjaan:
Automaation tietoturva – Kriittisen tuotannon turvaaminen
(ISBN: 978-952-5183-58-0, ISSN 1455-6502, SAS julkaisusarja nro 51, © Suomen Automaatioseura ry, www.automaatioseura.fi/AutomaationTietoturva)