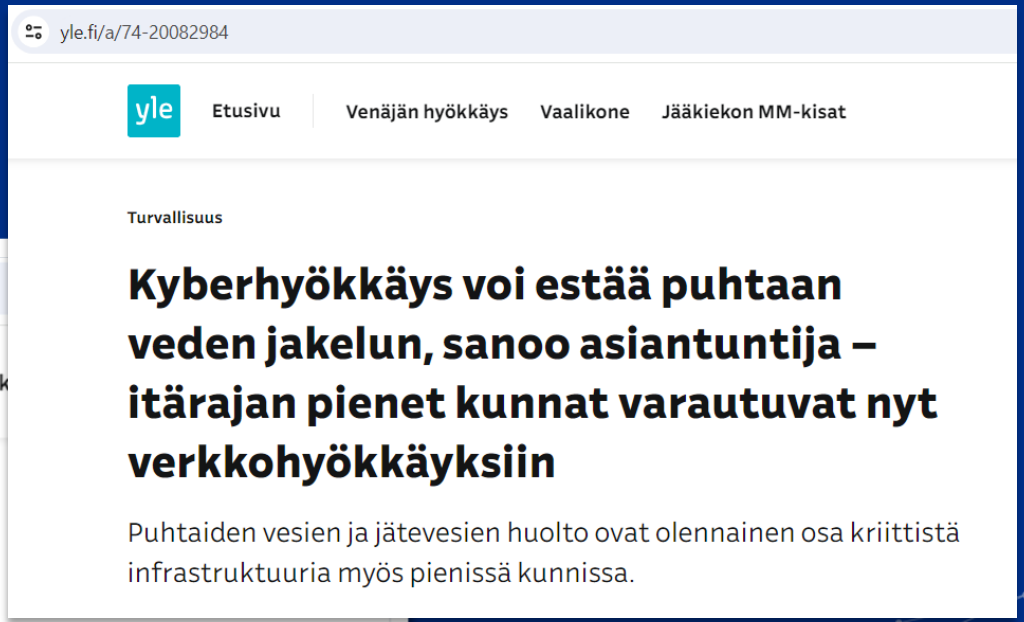
OT-ympäristön murtotestaamisen haasteet

28.5.2024

Anne Hautakangas

Huhtikuu 2024



Kuka?

ANNE HAUTAKANGAS

ACCOUNT DIRECTOR – INSTA

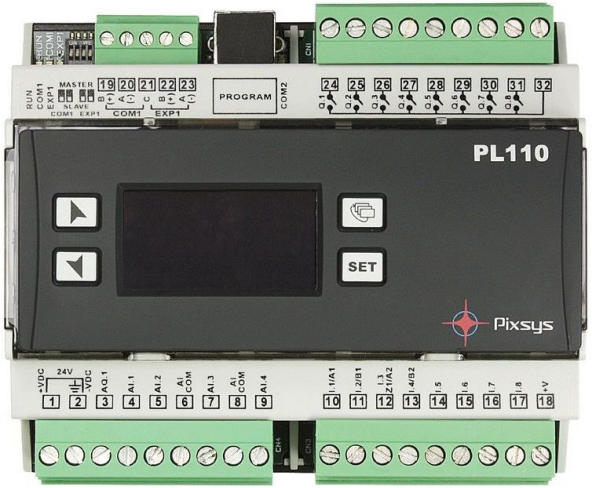
Hyökkääjän näkökulma

Ketä hyökkääjät ovat

Esimerkissä käytetyt laitteet ja ohjelmistot on valittu sattumanvaraisesti. Esitys ei ole indikaatio niiden tietoturvan heikkoudesta tai paremmuudesta.

Esimerkeissä käytetyt menetelmät ovat helposti toistettavissa.

Mieti kuitenkin ennen kuin klikkaat.



SIMATIC S7-300 station

vulnerabilities simatic s7-300

All Images Videos News Books More Tools

CISA (.gov)
https://www.cisa.gov › ics-advisories › icsa-16-348-05

Siemens S7-300/400 PLC Vulnerabilities (Update E)

10 Mar 2020 — 1. EXECUTIVE SUMMARY · CVSS v3 7.5 · ATTENTION: **Exploitable remotely/low skill level to exploit** · Vendor: Siemens · Equipment: SIMATIC S7-300 ...

Siemens
https://cert-portal.siemens.com › pdf › ssa-492828 PDF

Denial-of-Service Vulnerability in SIMATIC S7-300 CPUs ...

10 Nov 2020 — A vulnerability in S7-300 might allow an attacker to **cause a Denial-of-Service condition on port 102** of the affected devices by sending ...

3 pages

CVE-ID	
CVE-2018-16561	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A vulnerability has been identified in SIMATIC S7-300 CPUs (All versions < V3.X.16). The affected CPUs improperly validate S7 communication packets which could cause a Denial-of-Service condition of the CPU. The CPU will remain in DEFECT mode until manual restart. Successful exploitation requires an attacker to be able to send a specially crafted S7 communication packet to a communication interface of the CPU. This includes Ethernet, PROFIBUS, and Multi Point Interfaces (MPI). No user interaction or privileges are required to exploit the security vulnerability. The vulnerability could allow causing a Denial-of-Service condition of the core functionality of the CPU, compromising the availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known. Siemens confirms the security vulnerability and provides mitigations to resolve the security issue.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://cert-portal.siemens.com/productcert/pdf/ssa-306710.pdf

Assigning CNA

Siemens

Date Record Created

20180906	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20180906)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A


Google
Bing
YAHOO!
Yandex
Ask
Baidu 百度
DuckDuckGo
wow

SHODAN | Explore | Downloads | Pricing | country:fi | Account

TOTAL RESULTS

1,648,241

TOP CITIES

Helsinki	1,218,550
Tuusula	115,601
Lappeenranta	50,025
Tampere	31,986
Oulu	27,868

More...

TOP PORTS

80	245,602
22	225,166
443	219,812
161	54,608
8080	35,908

More...

TOP ORGANIZATIONS

Hetzner Online GmbH	863,307
Elisa Oyj	133,354
DNA Oyj	105,443

View Report | Download Results | Historical Trend | Browse Images | View on Map

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out Gravwell

193.105.96.66 2024-04-16T20:24:04.853437

hobart.webinaarivalmennukset.fi
Innocode Oy
Finland, Helsinki

```
SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDOGVEk5sf2CnyPd8q8vV0JlIh7AN9zyMWcPlUAToVyzj1Z
5EQuNz12ji3MtTrXKTd/3zpNqwjyl5XSeD6ubURtNhJfDWmioHp+ayiZTosbh753PCShd0waU2gJ
y4VWE/WsPdy/rpI233DMygaODnOdT3FsEi1TF6WPgMTTrjzepUHc3S8u84wJ/Y8Fq50VyzpCzmTa
lS399F+oN+uJzG/rgqx2vU7...
```

HTTP Server Test Page powered by CentOS-WebPanel.com 2024-04-16T20:23:55.460414

95.216.112.166
static.166.112.216.95.clients.your-server.de
Hetzner Online GmbH
Finland, Helsinki

```
HTTP/1.1 200 OK
Date: Tue, 16 Apr 2024 20:23:53 GMT
Server: Apache/2.4.57 (Unix) OpenSSL/1.0.2k-fips
Last-Modified: Sat, 19 Aug 2023 08:21:22 GMT
ETag: "13cd-6034254946480"
Accept-Ranges: bytes
Content-Length: 5069
Vary: Accept-Encoding,User-Agent
Content-Type: text/html
```

85.23.67.208 2024-04-16T20:23:46.909459

85-23-67-208.bb.dnainternet.fi
DNA Oyj
Finland, Helsinki

honeypot

SHODAN | Explore | Downloads | Pricing | country:FI "Siemens, simatic" port:161 | Account

TOTAL RESULTS

16

TOP CITIES

Helsinki	9
Kirkkonummi	2
Lappeenranta	2
Kajaani	1
Kauniainen	1

More...

TOP ORGANIZATIONS

	6
	3
	2
	2
	1

More...

TOP PRODUCTS

View Report | Download Results | Historical Trend | View on Map

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out Gravwell

Finland, Helsinki

2024-04-16T13:55:21.899418

```
SNMP:
  Uptime: 1
  Description: Siemens, SIMATIC, S7-300
  Service: 72
  Versions:
    1
    3
  Engineid Format: octets
  Contact: Corporate IT
  Engine Boots: 2
  Engineid Data: 80004fb805666565366636386233646239000 1c980
  Enterprise: 20408
  Objectid: 0.0
  Engine Time: 4:34:20
  Location: BE...
```

Finland, Helsinki

2024-04-16T13:46:36.362491

```
SNMP:
  Uptime: 1
  Description: Siemens, SIMATIC, S7-300
  Service: 72
  Versions:
    1
    3
```

kyberturvallisuuskeskus.fi/fi/ilmoita

Lomakkeesi on lähetetty. Kiitos asioinnista. Voit tallentaa hakemuksesi tiedot itsellesi sivun alalaidan "Tulosta lomake"-painikkeesta.

Kyberturvallisuuskeskus yhteydenotto

1 Anna lisätiedot — 2 Tarkista tiedot — 3 Vahvistus

Tapahtuman tiedot

Olen

Yksityishenkilö

Ilmoitan poikkeamasta joka koskee

Organisaatiota

Ilmoitukseni koskee

Laitetta

Ongelmani koskee

Muuta tapahtumaa

Kuvaus

Olen työstämässä työnantajalleni OT-verkkojen tietoturvaan liittyvää esitystä ja hain siihen taustatietoa Shodanin kautta. Löysin Shodanista useampia Siemens Simatic S7-300 kontrollereita. Yksi niistä kuuluu energiayhtiölle, mikä herätti huolen, että onko laite tarkoituksella julkisessa internetissä.

Reply Reply All Forward IM

cert@traficom.fi Hautakangas Anne 3.5.2024

[FICORA #1274274] Kyberturvallisuuskeskus yhteydenotto

We removed extra line breaks from this message.

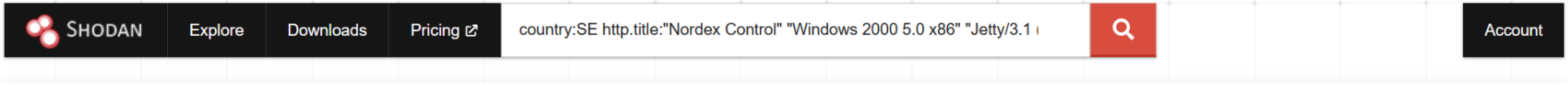
Hei Anne,

Kiitos paljon ilmoituksestanne. Otamme mielellämme näitä tietoja vastaan. Meille voitte ilmoittaa jatkossakin näitä luottamuksellisesti. Me voimme ilmoittaa nämä haavoittuvuudet organisaatiolle tarkistettavaksi.

Oikein mukavaa viikonloppua!

Ystävällisin terveisin,
Päivystäjä

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
cert@traficom.fi
P. 029 534 5000
Dynamicum, Erik Palménin aukio 1, 00560 Helsinki PL 320, 00059 TRAFICOM www.traficom.fi,
www.kyberturvallisuuskeskus.fi



TOTAL RESULTS

1

View Report | Download Results | Historical Trend | View on Map

Product Spotlight: Keep track of what you have connected to the Internet. Check out Shodan Monitor

Nordex Control - Wind Farm Portal (ver. 11.06.13) Urup

2024-03-27T11:13:25.146721

[redacted]

Sweden, Stockholm

SSL Certificate

Issued By:
|- Common Name:
Nordex-Issuing-CA-2-2015

Issued To:
|- Common Name:
192.168.8.211

|- Organization:
Nordex

Supported SSL Versions:
SSLv3, TLSv1

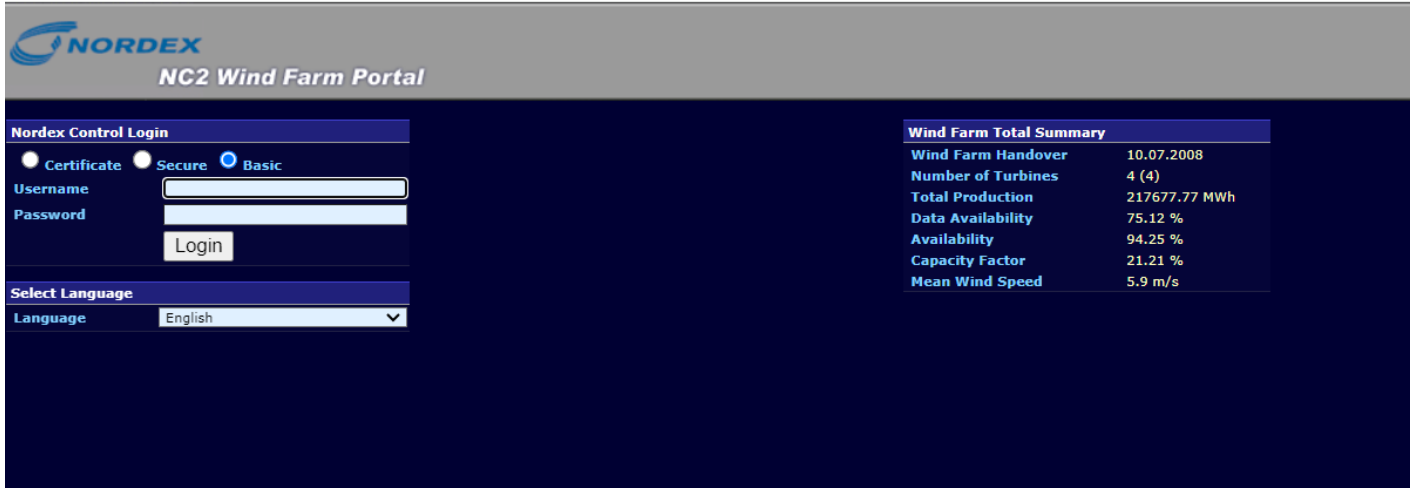
Diffie-Hellman Fingerprint:
Java 7/Hardcoded 768-bit prime

Vulnerabilities

FREAK

Logjam

```
HTTP/1.1 200 OK
Date: Wed, 27 Mar 2024 11:13:24 GMT
Server: Jetty/3.1.8 (Windows 2000 5.0 x86)
Servlet-Engine: Jetty/3.1 (JSP 1.1; Servlet 2.2; java 1.6.0_14)
Content-Type: text/html;charset=8859_1
Set-Cookie: jsessionid=208lfe17p;Path=/11_06_13
Set-Cookie2: jsessionid=208lfe17p;Version=1;P...
```



[redacted]

Nordex Control - Wind Farm Portal (ver. 1.07.00)

Nordex Control Login. Username. Password. Select Language. Language. English, Deutsch, Nederlansk. Wind Farm Total Summary. Wind Farm Handover, 12.07.2008.

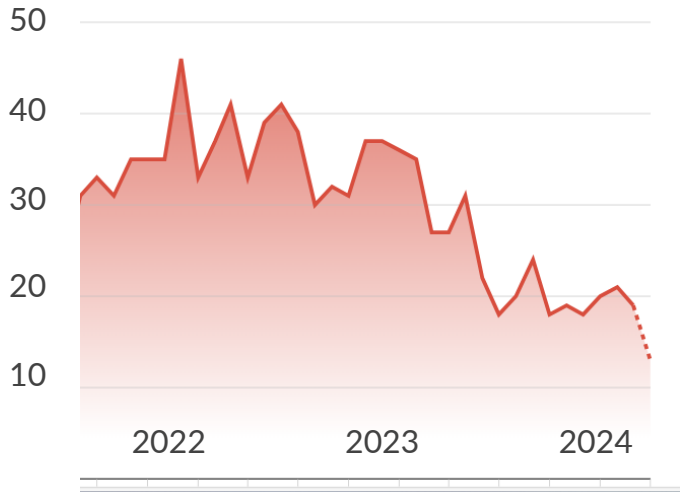
[redacted]

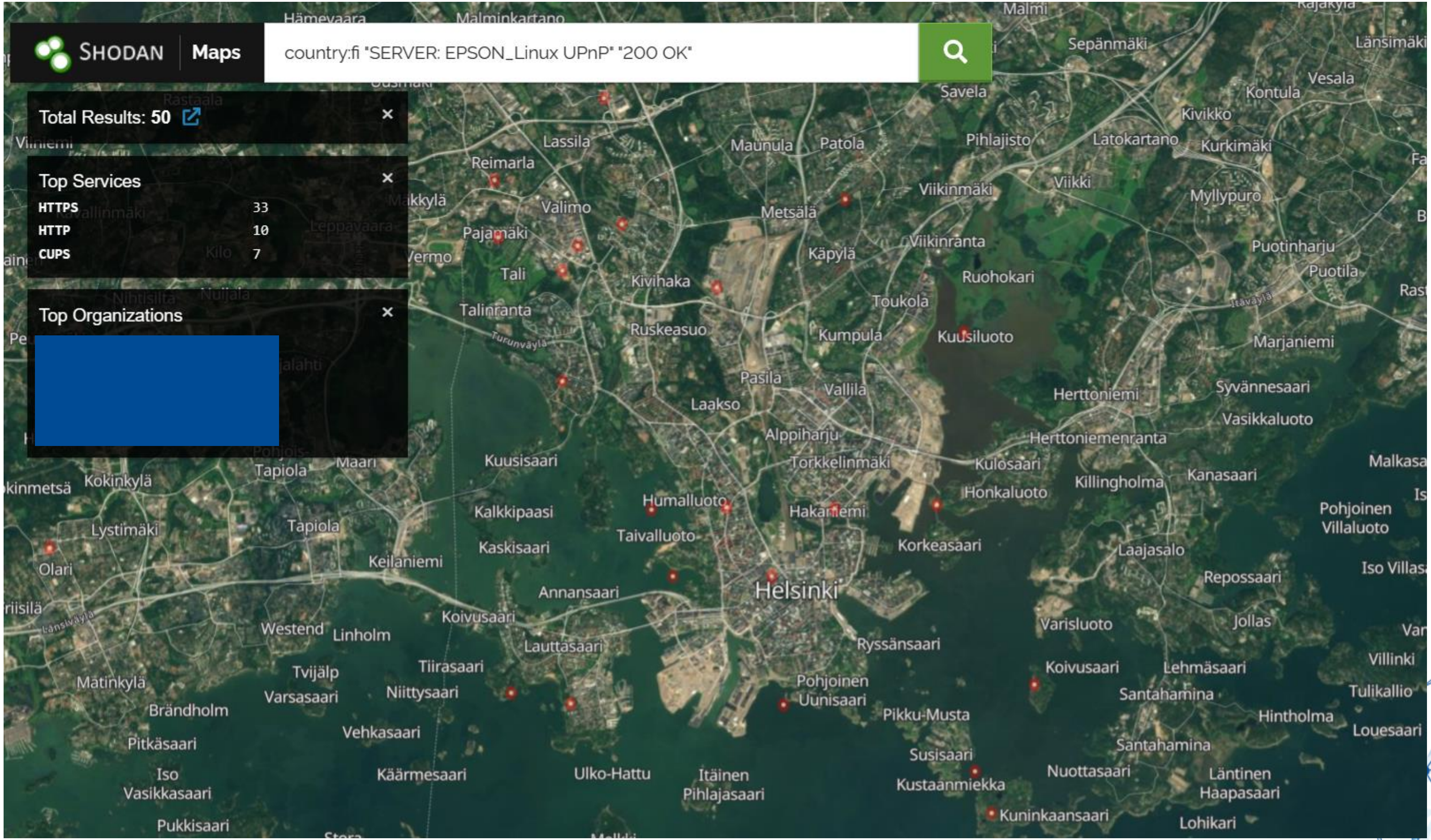
Nordex Control 13.8 [redacted]

Number of Turbines, 4 (4) ; Total Production, 215643.53 MWh ; Data Availability, 74.93 % ; Availability, 94.39 %.

Kehityksen suunta

Hakutermeinä: country:FI ” Schneider Electric”




SHODAN Maps
country:fi "SERVER: EPSON_Linux UPnP" "200 OK"
Total Results: 50
Top Services
HTTPS 33
HTTP 10
CUPS 7
Top Organizations
[redacted]
Helsinki
Pasila
Vallila
Laakso
Kumpula
Käpylä
Herttoniemi
Laajasalo
Lauttasaari
Tapiola
Olari
Matinkylä
Santahamina

Puolustajan haasteet

INSTA

Tietoturva on yksinkertaista.

Tietoturva on yksinkertaista.

Tee vain asiat oikein.

Tietoturva on yksinkertaista.

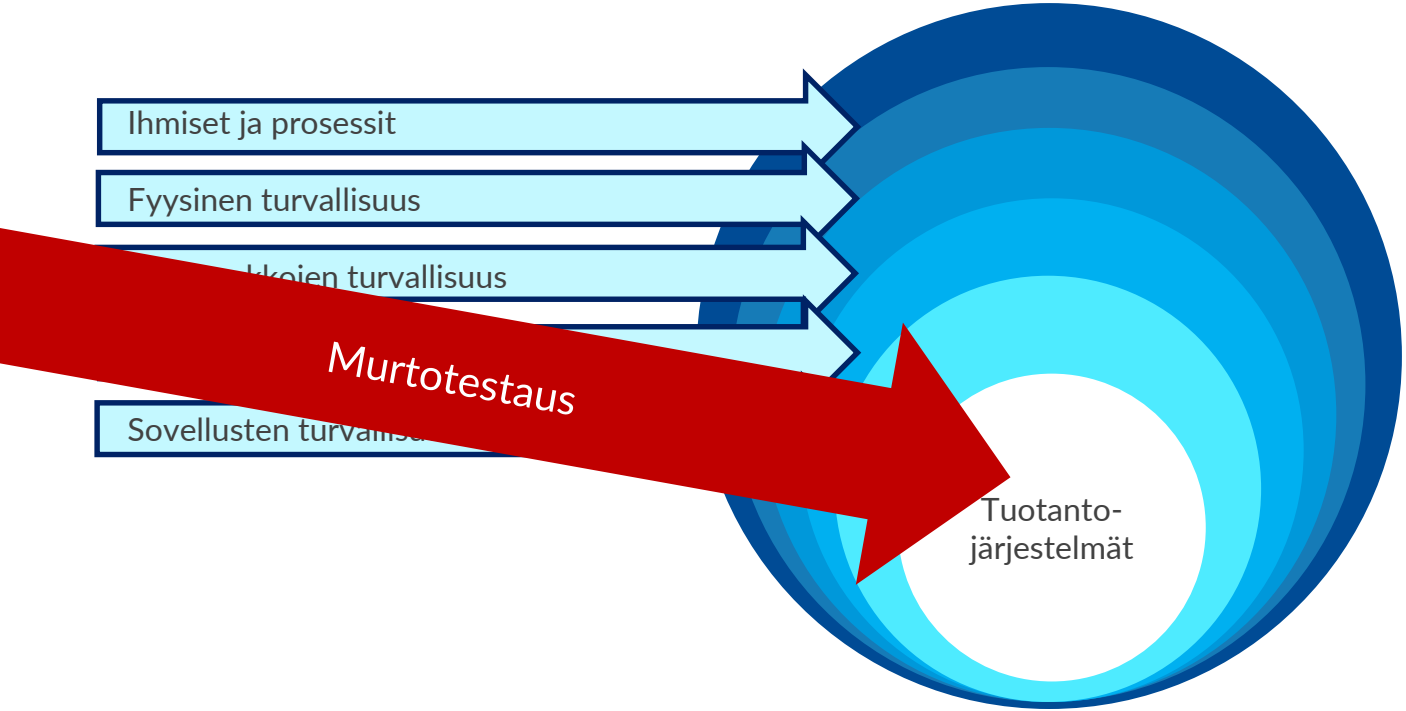
Tee vain asiat oikein.

Joka ikinen kerta.

Tietoturvan todellisuus

- Kehityksen vauhti uusissa teknologioissa on kova
- Kehityksen vauhti haavoittuvuuksia hyödyntävissä haittaohjelmissa on yhtä kova
- Liiketoiminnan ja kehityksen erilaiset prioriteetit
- Lakimuutokset (esim. GDRP, NIS2, DORA..) syövät resursseja
- Ihmisten inhimillisyys (unohtaminen, väärinkäsitykset, muu elämä)
- Henkilöstön vaihtuvuus ja osaamisen katoaminen
- Henkilöstön vaihteleva tekninen osaaminen
- Ei tunnisteta järjestelmän tai oman työn tärkeyttä eikä siksi suojella sitä asianmukaisesti
- Jatkuva kiire
- Epäselvät vastuut
- ....

Turvallisuutta sipulimallilla



OT-ympäristöjen murtotestaus ja niiden haasteet

- Tyypillisesti testaukset tehdään tuotantoympäristössä
  - Toiminta ei saa häiriintyä eikä henkilö- tai ympäristöturvallisuus vaarantua
    - Tehtävät toimet mitoitetaan kohteen mukaisesti. Automaatiolaitteita sisältäviä verkkoja ei kohdella samalla tavalla kuin toimistoverkkoja ja esimerkiksi haavoittuvuuksien todentamista ei tehdä ellei sitä voida tehdä turvallisesti.
- Yleisimpiä tarkastuskohteita:
  - Wifi-verkot
  - Toimisto- ja hallintoverkot
  - OT-verkot
  - OT-laitteet

Tyypillisiä löydöksiä

- Verkkojen eriytys internetistä ei ole toivotulla tasolla.
- Tuotanto- ja hallinto- ja toimistoverkkojen eritys ei ole kaikilta osin vedenpitävä
- Tietoa tuotannossa olevista haavoittuvuuksista
  - Tunnistetaan kriittiset kohteet ja suojataan niitä tehokkaammin.
- Lista verkossa olevista (ja unohtuneista) laitteista


Kiitos!
INSTA