Business from technology

**ASAF-teemapäivä 10.5.2017: Turva-automaation uudet vaatimukset ja automaation tietoturva**

# Automaation kyberturvallisuuden kehitysprojektin tulokset (KYBER-TEO 2014-2016) ja tulevaisuus

Pasi Ahonen, johtava tutkija,
VTT Technical Research Centre of Finland



## Tausta 2008-2016

## Miten automaation kyberturvallisuusyhteistyötä kehitettiin?

| Vuosi | Päätehtävä | Projekti |
|---|---|---|
| 2008-2009 | 1. LÖYTÄÄ KEHITYSKOHTEET: – Mitkä ovat yhteiset kipupisteet? | TITAN “Tietoturvaa teollisuusautomaatioon” |
| 2009-2010 | 2. SELVITTÄÄ PERUSTEET: –Analysoida nykyiset käytännöt | TITAN |
| 2011-2012 | 3. KÄSITTELY TEEMOITTAIN: –Teematyöpajat | TEO-TT ”Teollisuuden tietoturvan kansallinen kehittäminen teematyöpajoissa” |
| 2011-2012 | 4. HANKINTA: –Yhteiset vaatimukset ja ohjeet | COREQ-VE ”Yhteinen tietoturvavaatimuskanta teollisuudelle” |
| 2012-2013 | 5. YRITYSTAPAUKSET: –Tuki yritystapauksille | COREQ-ACT ”Tietoturvan aktiiviset teollisuus-caset” |
| 2014-2016 | 6. LISÄÄ YRITYSTAPAUKSIA: –Tuki kolmella työpaketilla | KYBER-TEO ” Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen” |

Tiedonjako → HVK

## Kansallinen hankekokonaisuus 2014-2016

# *”Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen” KYBER-TEO*

**Pääasiakas: Huoltovarmuuskeskus.**

**Asiakkaat: n. 10 osallistuvaa teollisuus- ja palveluyritystä kunakin projektivuonna.**




**Palveluja kyberturvallisuuden ja jatkuvuuden varmistamiseksi!**

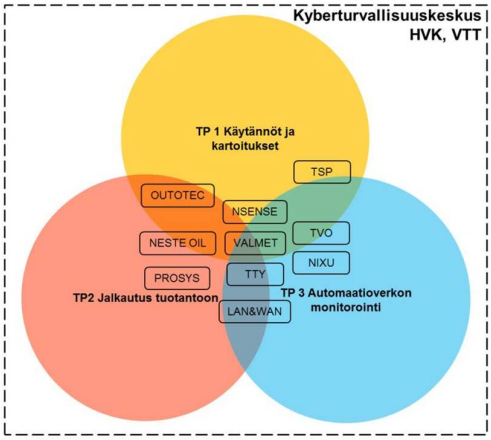
**29.4.2015 : Tulosjulkaisun esittelytilaisuus Hiltonissa yhdessä Huoltovarmuuskeskuksen kanssa**

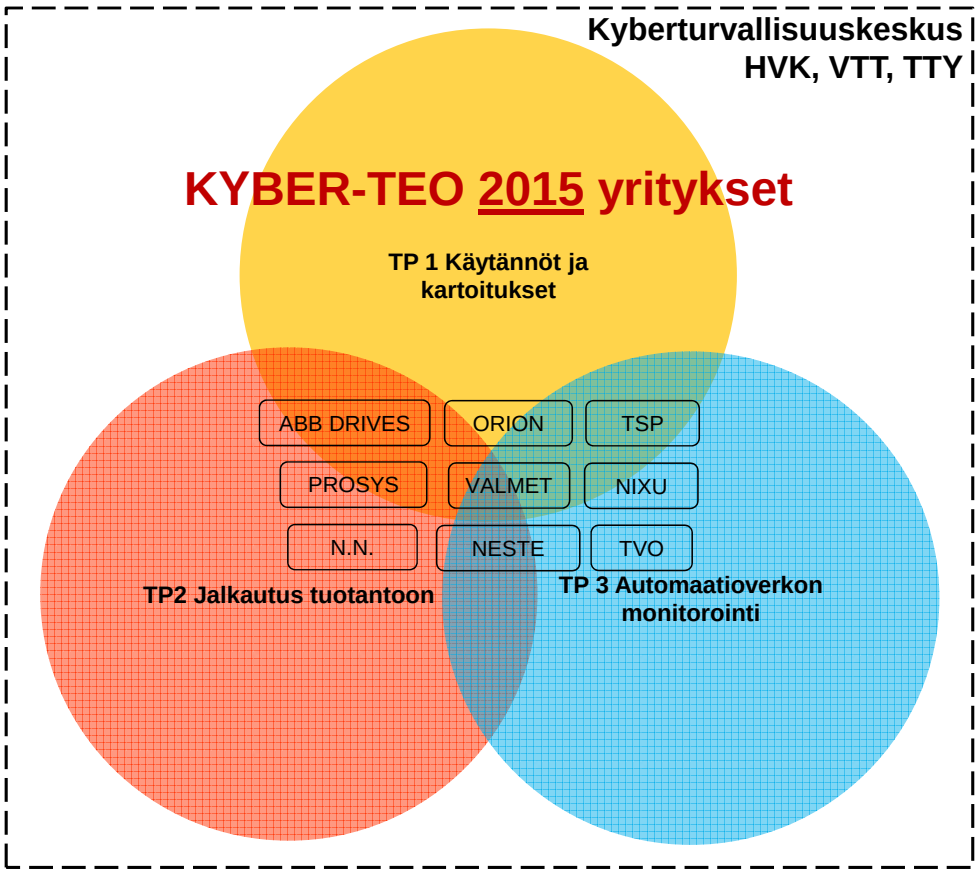
**Paikalla n. 100 teollisuuden ammattilaista**
**Painettu julkaisu: 1. painos 700 kpl.**
**Verkkojulkaisu: http://www.huoltovarmuus.fi/static/pdf/839.pdf**

## Julkaisemme yhteenvetoja projektiemme julkisista tuloksista!

***KYBER-TEO = Toimeksiantokokonaisuus 2014 – 2016, ”Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen”***

***KYBER-TEO 2014***






## KYBER-TEO kokonaisuus

**Pääasiakas**: Huoltovarmuuskeskus (HVK)
Tuki: Kyberturvallisuuskeskus
Projektin veto ja toteutus: VTT
Tutkimusalihankinta: TTY

**Kunkin vuoden (2014, 2015, 2016) KYBER-TEO osallistujayritykset määräytyivät kahdenkeskisten neuvottelujen (yritys / VTT) tuloksena**



# Uusi julkaisu:
# KYBER-TEO Tuloksia 2014 - 2016
## Julkisten tulosten kooste

**Tekijät: Pasi Ahonen, et.al.**

# Uusi julkaisu:
# KYBER-TEO Tuloksia 2014 - 2016
## Julkisten tulosten kooste

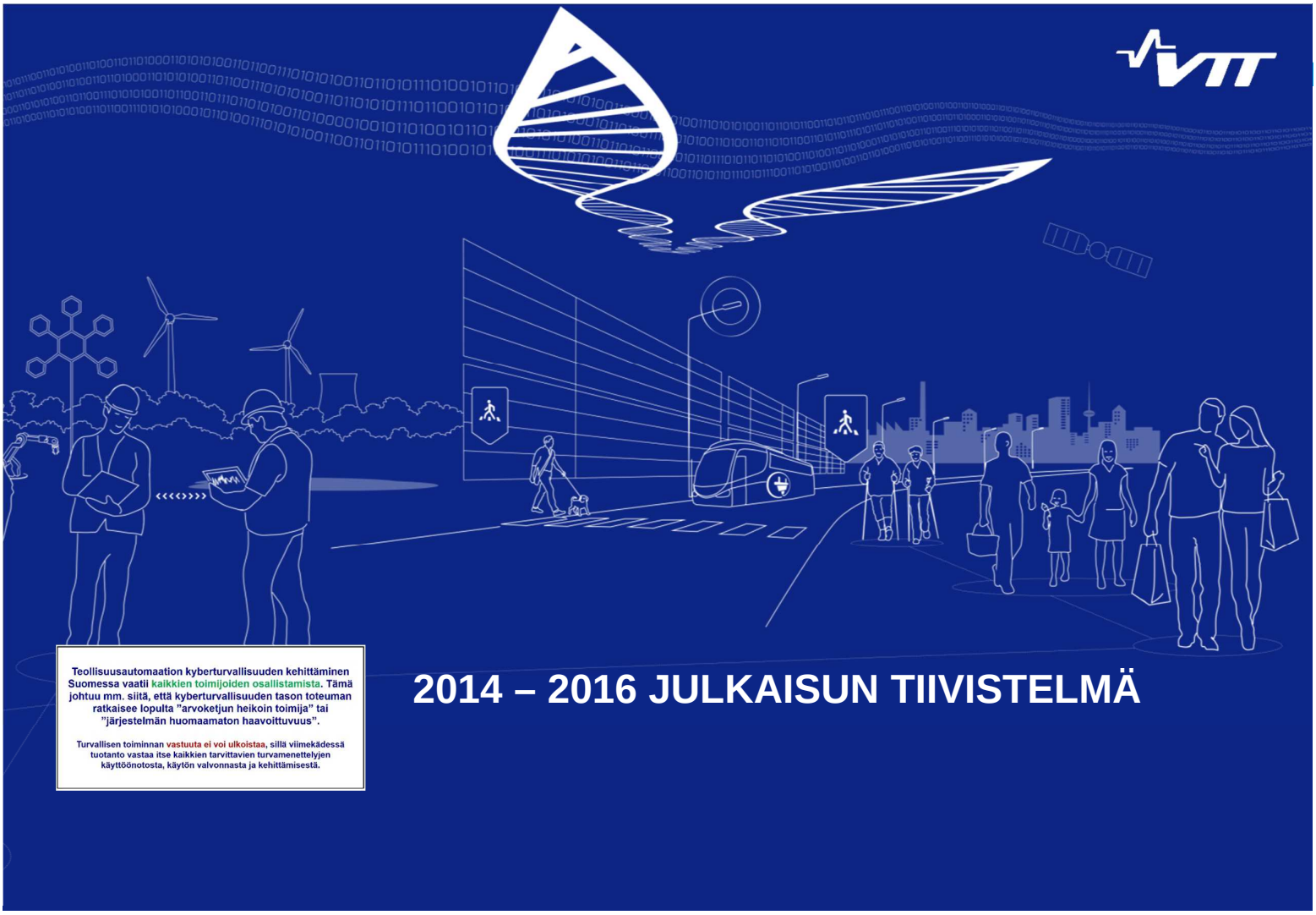
**Tekijät: Pasi Ahonen, et.al.**






# Uusi julkaisu:
# KYBER-TEO Tuloksia 2014 - 2016
## Julkisten tulosten kooste

**Tekijät: Pasi Ahonen, et.al.**



Teollisuusautomaation kyberturvallisuuden kehittäminen Suomessa vaatii kaikkien toimijoiden osallistamista. Tämä johtuu mm. siitä, että kyberturvallisuuden tason toteuman ratkaisee lopulta "arvoketjun heikoin toimija" tai "järjestelmän huomaamaton haavoittuvuus".

Turvallisen toiminnan vastuuta ei voi ulkoistaa, sillä viimekädessä tuotanto vastaa itse kaikkien tarvittavien turvamenettelyjen käyttöönotosta, käytön valvonnasta ja kehittämisestä.

# 2014 – 2016 JULKAISUN TIIVISTELMÄ



## OTTEITA HUOLTOVARMUUSKESKUKSEN SAATTEESTA

- Käytännön kybertoimintaympäristöjä on kehitetty yhteistyössä huoltovarmuuskriittisten yritysten kanssa.
- Varsinkin kyberturvallisuustestaustoimintaan ja harjoitustoimintaan kehitettiin toimintamalleja, jotka koettiin käytännön harjoituksissa hyödyllisiksi.
- Samoin on saatu aikaiseksi yrityksiä hyödyttäviä tuloksia teollisuusautomaation edellyttämän elinkaaritarkastelun huomioonottamiseksi.
- Myös monitorointi, eli tietoturvapoikkeamien havainnointikyvyn parantaminen, on ollut vahvasti mukana KYBER TEO -projekteissa.

# 2014 – 2016 JULKAISUN TIIVISTELMÄ (1/3)

**Kyberturvallisuuden kehittäminen edellyttää lähes aina tietoisuuden perustasoa, jolloin yrityksen päättäjät ja käytännön toimijat ymmärtävät riittävästi kyberuhkien todellisista vaikutuksista ja kohdistumisesta omaan toimintaansa.**

**Vasta tämän jälkeen yritykseen voi syntyä tarvittava vastuiden määrittely ja resursointi mm. tuotantoon soveltuvien kyberturvallisuusuhkien havaitsemiseen, torjuntaan ja ennakkovarautumiseen.**



# 2014 – 2016 JULKAISUN TIIVISTELMÄ (2/3)

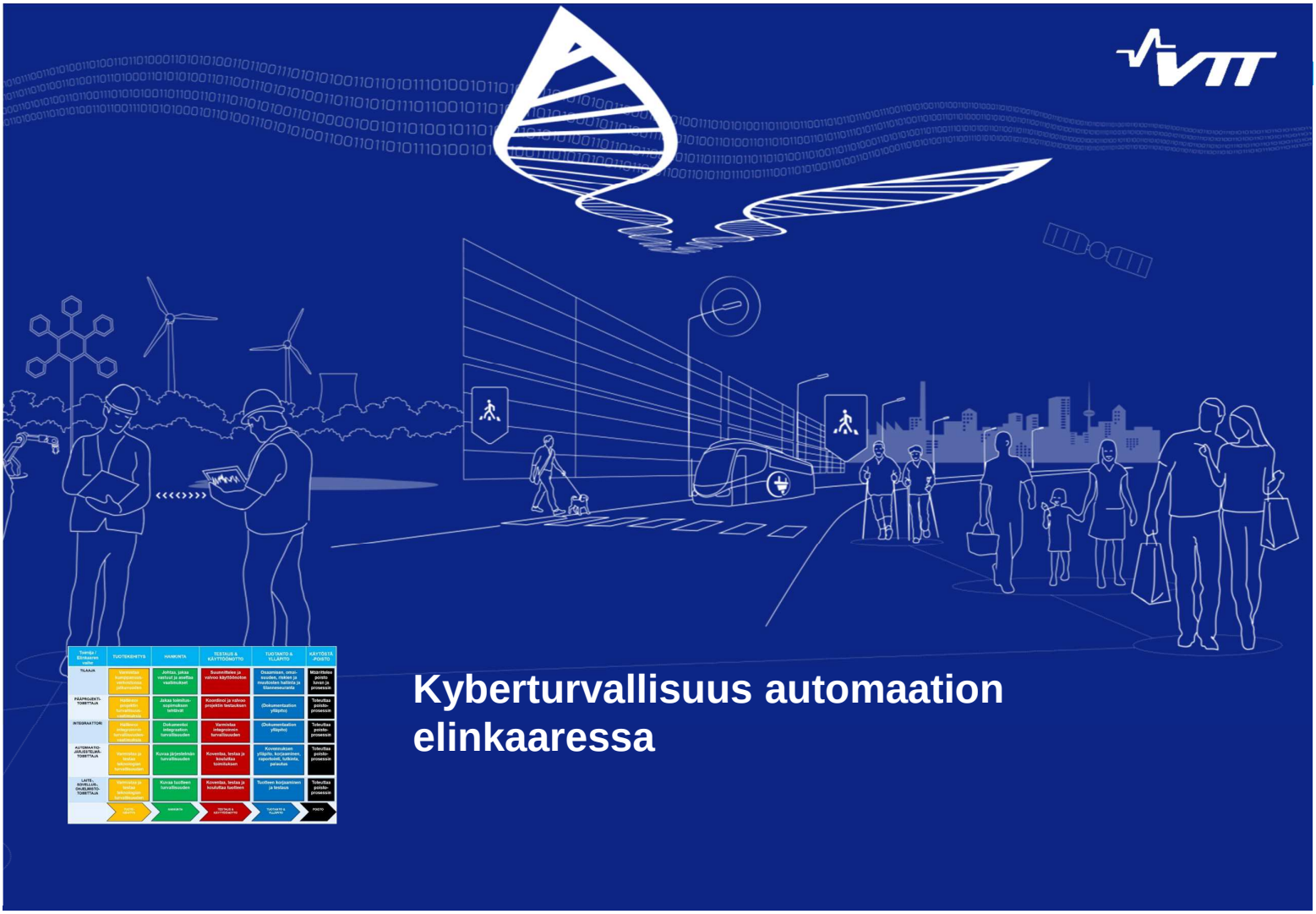
**Teollisuusautomaation kyberturvallisuuden kehittäminen Suomessa vaatii kaikkien toimijoiden osallistamista. Tämä johtuu mm. siitä, että kyberturvallisuuden tason toteuman ratkaisee lopulta ”arvoketjun heikoin toimija” tai ”järjestelmän huomaamaton haavoittuvuus”.**

**Turvallisen toiminnan vastuuta ei voi ulkoistaa, sillä viimekädessä tuotanto vastaa itse kaikkien tarvittavien turvamenettelyjen käyttöönotosta, käytön valvonnasta ja kehittämisestä.**

# 2014 – 2016 JULKAISUN TIIVISTELMÄ (3/3)

**KYBER-TEO projekteissa vuosina 2014 - 2016 kehitettiin yritysten yhteistyötä ja edellytyksiä parantaa monia erilaisia automaation kyberturvallisuuteen vaikuttavia asioita, erityisesti:**

- ✓ **Alan edelläkävijäyrityksissä kehitettiin ja testattiin automaation kyberturvallisuuden kehittämisen palveluja, parhaita käytäntöjä ja ratkaisuja**
- ✓ **Määriteltiin kyberturvallisuuden työnjako ja tehtävät automaation elinkaaressa**
- ✓ **Parannettiin ammattilaisten kyberturvallisuustietoisuutta julkisten tulosten esittelytilaisuuksissa kertomalla uhkista ja seurauksista, sekä varautumiseen kehitetyistä käytännöistä ja koetelluista ratkaisuista**
- ✓ **Kehitettiin ja koestettiin automaation kyberturvatestauksen ympäristöjä**
- ✓ **Kehitettiin ja koestettiin automaation kyberturvaharjoittelun ympäristöjä**
- ✓ **Kehitettiin ja koestettiin automaatioverkkojen kyberturvamonitoroinnin konsepteja ja menetelmiä**
- ✓ **Kehitettiin ja pilotoitiin automaation kyberturvallisuuden sähköistä yhteistyöfoorumia.**



# OPPI: Automaation pitkän elinkaaren hallinta vaatii paljon pohdintaa

**Vaikeinta automaation kyberturvallisuudessa on pitkän elinkaaren hallinta, sillä…**

**…kyberuhkia tulee koko ajan lisää, mutta ongelmat eivät vähene lisäämällä uusia teknologioita ja prosesseja vanhojen päälle, vaan määrittelemällä jatkuvuuden varmistamisen konseptit joissa kyberturvallisuus on aina mukana, sekä sopimalla ymmärrettävät pelisäännöt ja vastuut omalle henkilöstölle ja kumppaneille.**

**Hyvien peruskäytäntöjen ja työkalujen soveltaminen ja yhteistyö ovat toimivia tapoja automaation turvallisuuden ja jatkuvuuden varmistamisessa.**



# Automaation elinkaari - Kyberturvallisuuden päävastuumatriisi

| Toimija / Elinkaaren vaihe | TUOTEKEHITYS | HANKINTA | TESTAUS & KÄYTTÖÖNOTTO | TUOTANTO & YLLÄPITO | KÄYTÖSTÄ -POISTO |
|---|---|---|---|---|---|
| TILAAJA | Varmistaa kumppanuus-verkostonsa jatkuvuuden | Johtaa, jakaa vastuut ja asettaa vaatimukset | Suunnittelee ja valvoo käyttöönoton | Osaamisen, omaisuuden, riskien ja muutosten hallinta ja tilanneseuranta | Määrittelee poisto luvan ja prosessin |
| PÄÄPROJEKTI-TOIMITTAJA | Hallinnoi projektin turvallisuus-vaatimuksia | Jakaa toimitus-sopimuksen tehtävät | Koordinoi ja valvoo projektin testauksen | (Dokumentaation ylläpito) | Toteuttaa poisto-prosessin |
| INTEGRAATTORI | Hallinnoi integroinnin turvallisuuden-vaatimuksia | Dokumentoi integraation turvallisuuden | Varmistaa integroinnin turvallisuuden | (Dokumentaation ylläpito) | Toteuttaa poisto-prosessin |
| AUTOMAATIO-JÄRJESTELMÄ-TOIMITTAJA | Varmistaa ja testaa teknologian turvallisuuden | Kuvaa järjestelmän turvallisuuden | Koventaa, testaa ja kouluttaa toimituksen | Kovennuksen ylläpito, korjaaminen, raportointi, tutkinta, palautus | Toteuttaa poisto-prosessin |
| LAITE-, SOVELLUS-, OHJELMISTO-TOIMITTAJA | Varmistaa ja testaa teknologian turvallisuuden | Kuvaa tuotteen turvallisuuden | Koventaa, testaa ja kouluttaa tuotteen | Tuotteen korjaaminen ja testaus | Toteuttaa poisto-prosessin |
| | TUOTE-KEHITYS | HANKINTA | TESTAUS & KÄYTTÖÖNOTTO | TUOTANTO & YLLÄPITO | POISTO |

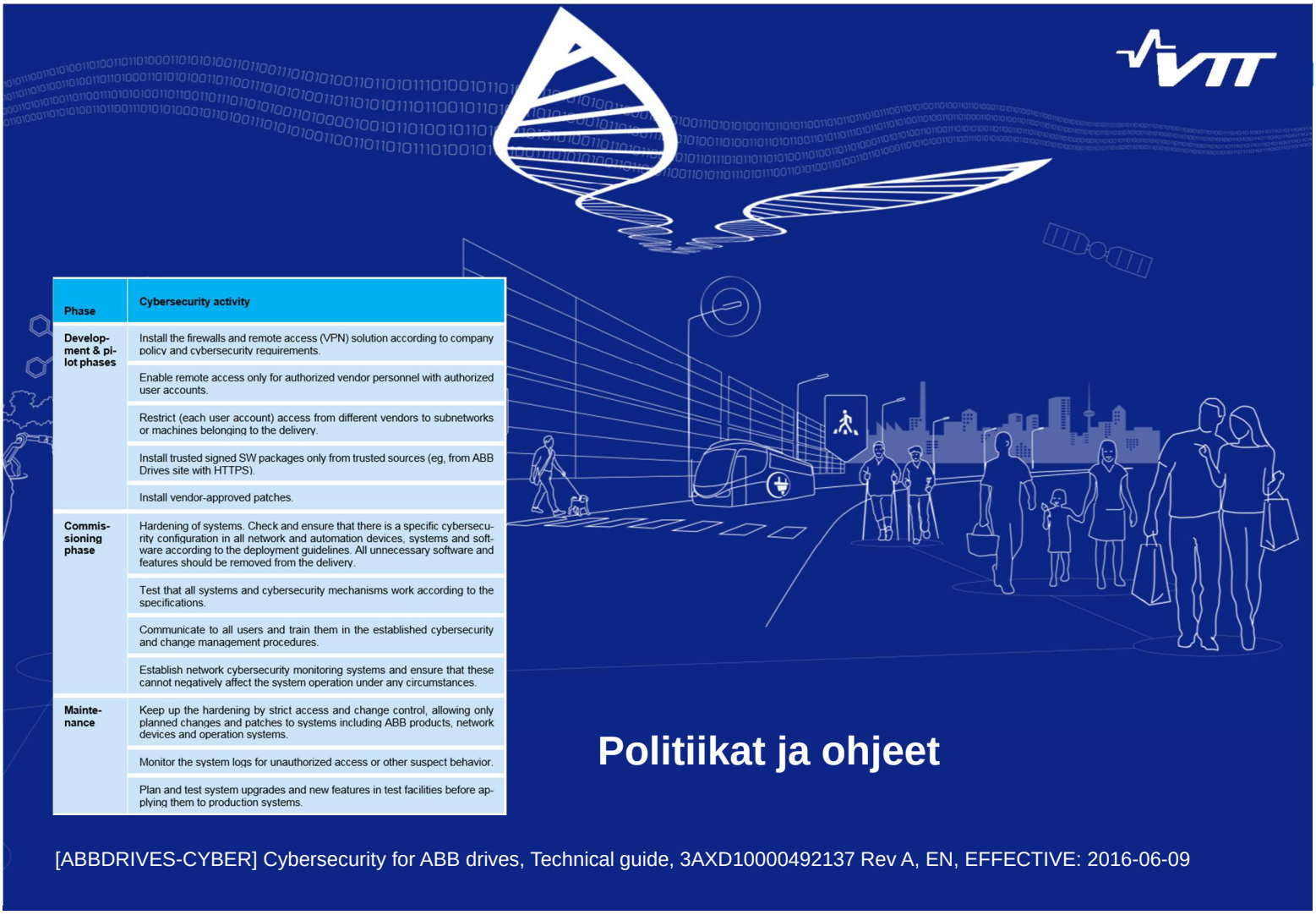
# Automaation elinkaari - Kyberturvallisuuden varmistamiseen ja avustamiseen liittyviä tehtäväkokonaisuuksia toimijoittain (1/2)

| Elinkaaren vaihe \ Toimija | TUOTE-KEHITYS | HANKINTA | TESTAUS & KÄYTTÖÖN-OTTO | TUOTANTO & YLLÄPITO | KÄYTÖS-TÄPOISTO |
|---|---|---|---|---|---|
| TILAAJA | Tilaajan kyberturvallisuuden ja jatkuvuuden vaatimusten ja ohjeiden laadinta ja viestintä. | Määrittelee: yhteiset käytännöt, politiikat, suojavyöhykkeet.<br>Määrittelee: vaatimukset, suojaustasot, etäyhteysmallit.<br>Määrittelee: toimitussisältö ja -raja.<br>Valvoo: koko elinkaari & sopimukset.<br>Jakaa vastuut. Edistää tietoisuutta. | Vastaanoton valvonta ja katselmointi.<br>Validointikatselmointi.<br>Kelpuutuskatselmointi.<br>Jatkuvuussuunnitelmien laadinta.<br>Harjoitussuunnitelmien laadinta. | Omaisuuden hallinta (työluvat) ja jatkuvuus elinkaaressa.<br>Muutosprosessien määrittely ja valvonta. Koulutusjärjestelyt.<br>Varautuminen: kapasiteetti, riskit, katselmoinnit, harjoitukset.<br>Tilanneseurannan & häiriöhallinnan järjestelyt. | Myöntää poistoluvat.<br>Menettelytapojen ja uusiokäytön määrittely & valvonta. |
| PÄÄ-PROJEKTITOIMITTAJA | Projektin turvallisuusvaatimusten laadinta ja noudattamisen valvonta. | Toimituksen sisällön määrittely.<br>Projektin kyberturvallisuussuunnitelman laadinta.<br>Ohjelmisto- ja palvelulisenssien hallinta. | Koordinointi ja valvonta, mm.:<br>-Projektikäytännöt.<br>-Tietoliikenneratkaisut.<br>-Rajapinnat.<br>-Yhdyskäytävät.<br>-Osoitteet. | *(Dokumentaation säilytys ja ylläpito).* | Projektin päättämisen menettelytapojen määrittely & valvonta. |



# Automaation elinkaari - Kyberturvallisuuden varmistamiseen ja avustamiseen liittyviä tehtäväkokonaisuuksia toimijoittain (2/2)

| Elinkaaren vaihe \ Toimija | TUOTE-KEHITYS | HANKINTA | TESTAUS & KÄYTTÖÖN-OTTO | TUOTANTO & YLLÄPITO | KÄYTÖS-TÄPOISTO |
|---|---|---|---|---|---|
| INTEGRAATTORI | Integroinnin turvallisuusvaatimusten määrittely ja noudattaminen. | Vastaa integroinnin arkkitehtuurista ja turvallisuudesta. | Asennus ja konfigurointi.<br>Rajapintojen integrointi.<br>Kovennuksen testaus ja raportointi. | *(Dokumentaation säilytys ja ylläpito).* | Noudattaa hävitysmenettelyä. |
| AUTOMAATIO-JÄRJESTELMÄ-TOIMITTAJA | Turvallisten T&K prosessien ja alustojen määrittely, testaus, katselmointi.<br>Kyberturvallisuustekniikan toteutus ja käyttöönotto järjestelmään.<br>Järjestelmän haavoittuvuuksien seuranta ja vikakorjaukset. | Verkkoarkkitehtuurin ja järjestelmäkuvauksen laadinta.<br>Järjestelmäohjeiden ja prosessien määrittelyt: mm.:<br>-Pääsynvalvonta.<br>-Identiteetinhallinta.<br>Toimitusprosessin turvallisuuden määrittely ja vastuu. | Toimituksen paketointi, asennus, esiasetukset, päivitykset.<br>Kyberturvallisuustestaus ja kovennus.<br>Käyttäjätilien siirto.<br>Varmennus ja palautus.<br>Turvalliset etäyhteydet.<br>Järjestelmäkoulutus. | Kenttäasennusten ylläpito ja dokumentointi.<br>Huoltosopimuksen toimet, korjaukset, riskianalyysit, raportointi.<br>Muutosten testaus.<br>Kovennuksen ylläpito.<br>Lokien seuranta, häiriötutkinta, palautus. | Määrittelee & noudattaa poiston menettelytapoja.<br>Uusiokäyttö. |
| LAITE-, SOVELLUS-, JA OHJELMISTO-TOIMITTAJA | Alustojen kyberturvallisuuden arviointi.<br>Kyberturvallisuuden toteutus, testaus ja ylläpito (ml. vikakorjaukset) | Tuotekuvausten, ohjeiden ja prosessien laadinta.<br>Toimitusprosessin turvallisuuden määrittely ja vastuu. | Alusta, laite-, sovellus-, ja ajurituki.<br>Testaus, paketointi, päivitysten jako.<br>Kovennuksen tuki.<br>Koulutus, käyttäjätiliohjeistus. | Tuotetuki. Huoltosopimuksen toimet, korjausten toimitus.<br>Muutosten testaus.<br>Varalaitteiden toimitus. | Määrittelee & noudattaa menettelytapoja.<br>Uusiokäyttö. |



| Phase | Cybersecurity activity |
|---|---|
| Develop-ment & pi-lot phases | Install the firewalls and remote access (VPN) solution according to company policy and cybersecurity requirements. |
| | Enable remote access only for authorized vendor personnel with authorized user accounts. |
| | Restrict (each user account) access from different vendors to subnetworks or machines belonging to the delivery. |
| | Install trusted signed SW packages only from trusted sources (eg, from ABB Drives site with HTTPS). |
| | Install vendor-approved patches. |
| Commis-sioning phase | Hardening of systems. Check and ensure that there is a specific cybersecu-rity configuration in all network and automation devices, systems and soft-ware according to the deployment guidelines. All unnecessary software and features should be removed from the delivery. |
| | Test that all systems and cybersecurity mechanisms work according to the specifications. |
| | Communicate to all users and train them in the established cybersecurity and change management procedures. |
| | Establish network cybersecurity monitoring systems and ensure that these cannot negatively affect the system operation under any circumstances. |
| Mainte-nance | Keep up the hardening by strict access and change control, allowing only planned changes and patches to systems including ABB products, network devices and operation systems. |
| | Monitor the system logs for unauthorized access or other suspect behavior. |
| | Plan and test system upgrades and new features in test facilities before ap-plying them to production systems. |

# Politiikat ja ohjeet

[ABBDRIVES-CYBER] Cybersecurity for ABB drives, Technical guide, 3AXD10000492137 Rev A, EN, EFFECTIVE: 2016-06-09

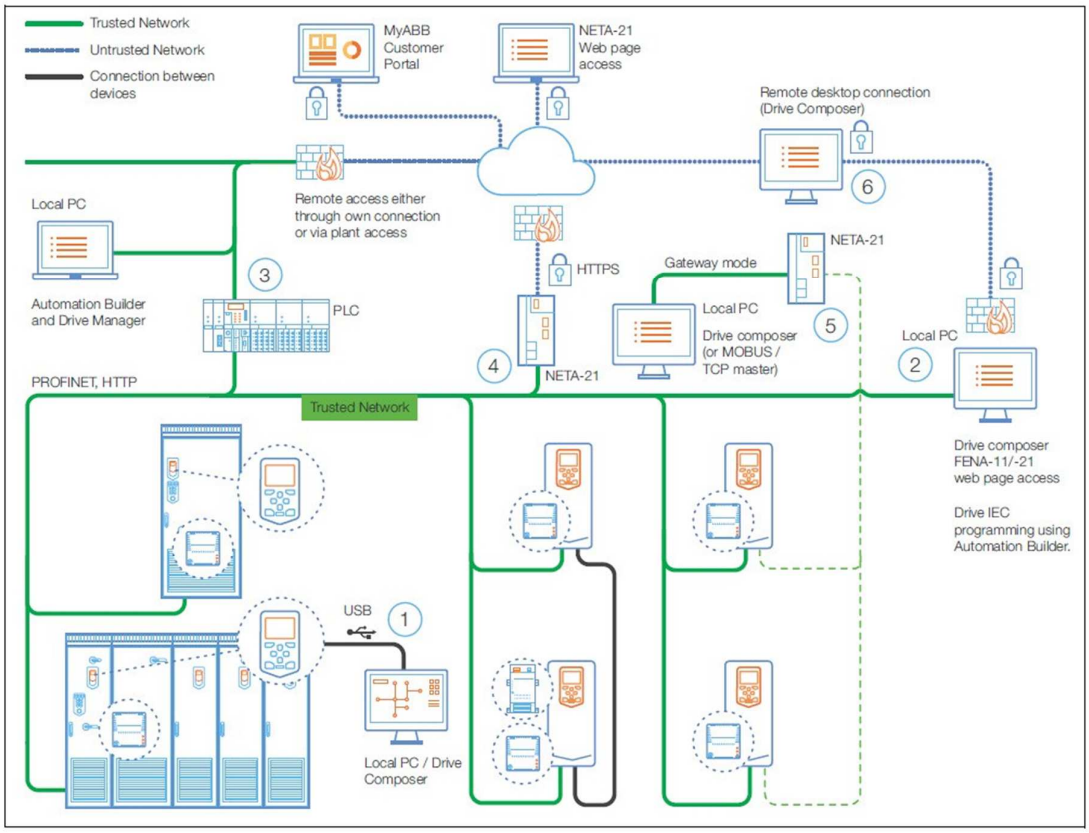


# CASE: Cybersecurity guideline for ABB Drives

## CASE 1: Industrial automation plant:

## Different network possibilities and their secure deployment [ABBDRIVES-CYBER]

**Commissioning of the drives and production line using the Drive composer start-up and maintenance tool and/or Automation Builder suite tool via:**
**1. Local connections (point-to-point serial communication, ie, USB) or**
**2. Shared (with control) upper-level physical fieldbus network (eg, PROFINET) using Ethernet tool communication and/or**
**3. Communicating also through PLC system using Drive Manager device tool or**
**4. NETA-21 remote monitoring tool web interface or**
**5. NETA-21 acting as a gateway between or**
**6. Third-party remote desktop connection**




[ABBDRIVES-CYBER] Cybersecurity for ABB drives, Technical guide, 3AXD10000492137 Rev A, EN, EFFECTIVE: 2016-06-09
https://library.e.abb.com/public/e71305ed2cd747b3b65a2becaf9a58bd/EN_Cybersecurity_guide_A_A4.pdf



# UUSIA UHKIA JA VAATIMUKSIA
## VILKAISTAAN PROJEKTIN ULKOPUOLELLE



## Uudentyyppisiä kyberuhkia lisääviä trendejä

- ❑ **Kiristyshaittaohjelmien levittäminen ja rahastus (esim. Bitcoinin avulla)**
- ❑ **Harhauttaminen valemediaa ja uutisia levittämällä**
- ❑ **IoT-laitteiden laiton haltuunotto ja hyväksikäyttö**
- ❑ **Kaksi-käyttötuotteiden väärinkäyttö, kuten**
  1. **Turvallisuusanalyysiin käytettävien työkalujen käyttö kyberhyökkäyksiin, ja**
  2. **Vahvan salauksen käyttö viranomaisilta pakoiluun.**

# VILKAISU SUOMEN ULKOPUOLELLE!

## Esimerkiksi tietoturvayhtiö Trend Micro tutki viime vuonna Ranskan kyberrikollisuutta

**Trend Micron tutkimuksen tulosesimerkkejä (alamaailmasta ostettavista rikollisista palveluista ja tuotteista):**

- ✓ **Salauspalvelu (Fully undetectable crypting service)**
- ✓ **Varmistettu verkkopalvelu (Bulletproof-hosting service)**
- ✓ **Tietojenkalastelun (phishing) työkalu, web-sivu, web-kehityspalvelu**
- ✓ **Botnettien eli kaapattujen koneiden vuokraus**
- ✓ **Pääsy haltuunotetuille tileille tai verkkoihin**
- ✓ **Väärennetyn kansallisen henkilökortin, identiteetin tai todistuksen myynti**
- ✓ **PDF-tiedostojen editointipalvelu (sis. meta-tiedot)**
- ✓ **Laiton pääsy haavoittuville web-sivustoille (SQL injection-avulla)**
- ✓ **Varastetun datakaappauksen myynti**
- ✓ **Ohjelmistojen haavoittuvuusskannauspalvelu**

Trend Micro, The French Underground, Under a Shroud of Extreme Caution, 2016, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-french-underground.pdf



## Oppi. Kyberturvallisuus vaatii jatkuvaa toimintaympäristön seurantaa ja oman ja ulkoistetun toiminnan kehittämistä

- ✓ **Turvallisuusvaatimusten tulee uusiutua uusia teknologioita, kyberuhkia ja käyttötapauksia vastaaviksi, joten kyberturvallisuus edellyttää jatkuvaa toimintaympäristön seurantaa ja oman ja ulkoistetun toiminnan kehittämistä.**
- ✓ **Relevanttien kyberturvallisuusvaatimusten ymmärtämiseen tarvitaan mm. kyberturvallisuuspäälliköiden, IT-osaston, hankintatoimen, projektipäälliköiden ja ulkoisten kyberturvallisuusasiantuntijoiden vuoropuhelua.**

**VILKAISU SUOMEN ULKOPUOLELLE!**

# Nousevia kyberturvallisuus-vaatimuksia (1/2)

| KONTROLLI-LUOKKA | NOUSEVIA VAATIMUKSIA (esimerkkejä havainnoistamme) |
|---|---|
| CSC 1: Luettelo sallituista ja ei-sallituista laitteista | Käytetään verkkotyökalua, joka etsii ja kirjaa verkon laitteet automaattisesti.<br><br>Käytetään (802.1x:n) verkkotason laitetodennusta.<br>Järjestelmä valtuutetaan sertifikaateilla ennen yksityiseen verkkoon liittämistä. |
| CSC 2: Luettelo sallituista ja ei-sallituista ohjelmistoista | Mikäli on pakottava tarve käyttää korkeamman riskin sovelluksia, joita ei saa asentaa yrityksen verkkoon, tulisi niitä käyttää *air gapped* -järjestelmässä tai erotetulla virtuaalikoneella. |
| CSC 3: Turvalliset asetukset laitteille ja ohjelmistoille | Säilytetään käyttöjärjestelmien levykuvia (*imaget)* ja ohjelmistojen asetuksia turvassa.<br>Päivitetään kaikki levykuvat, joita käytetään järjestelmien uudelleenkäyttöönotossa.<br><br>Tiedostojen *integrity checking* -työkaluilla varmistetaan, ettei kriittisiä tiedostoja ole muokattu.<br><br>Automaattinen monitorointi- ja hallinta asetuksille, jotka voidaan etänä testata ja pakottaa (työkaluineen). |
| CSC 4: Jatkuva haavoittuvuuksien arviointi ja korjaaminen | Automaattiset haavoittuvuusskannaukset viikoittain tai useammin.<br>Haavoittuvuusskannaus myös sisäänkirjautumistilassa erillistä käyttäjätunnusta käyttäen.<br><br>Haavoittuvuustietokanta päivitetään vähintään kuukausittain.<br>Verrataan tapahtumalokeja haavoittuvuusskannausten tuloksiin.<br>Haavoittuvuuksien riskit luokitellaan vaikutuksen mukaan.<br>Automaattiset vikakorjausten- ja päivitystenhallintatyökalut käytössä.<br>Skannausaktiviteettien ja niihin liittyvien ylläpitäjien tunnusten lokiseuranta.<br><br>Testataan että haavoittuvuudet on korjattu ajallaan. |
| CSC 6: Ylläpito, monitorointi ja lokien analysointi | Käytetään vähintään kahta synkronoitua aikalähdettä.<br>Tarkistetaan riittävät valvontalokit kaikille laitteille ja ohjelmistoille.<br>Verkkoliikenne lokitetaan verkon yhdyskäytävissä (*gateways*).<br><br>Lokit arkistoidaan ja allekirjoitetaan digitaalisesti tietyin aikavälein.<br><br>Tunnistetaan poikkeavuuksia mm. järjestelmä- ja tietovuolokeista kahden viikon välein. Käytetään SIEMiä tai lokien analysointityökaluja tiedon yhdistämiseen, korreloin-tiin ja analysointiin. |

Lähde: ETSI TR 103 305 -sarjan tekniset raportit: “Security Assurance by Default; Critical Security Controls for Effective Cyber Defense”



**VILKAISU SUOMEN ULKOPUOLELLE!**

# Nousevia kyberturvallisuus-vaatimuksia (2/2)

| KONTROLLI-LUOKKA | NOUSEVIA VAATIMUKSIA (esimerkkejä havainnoistamme) |
|---|---|
| CSC 15: Langaton pääsynhallinta | Laitteen pääsy sallitaan vain hyväksyttyihin langattomiin verkkoihin. Kaiken langattoman liikenteen tulee käyttää vähintään todennettua AES-kryptausta ja WPA2-suojausta. Peer-to-peer mahdollisuus poistetaan langattomista laitteista. Muut langattomat yhteydet, kuten Bluetooth, poistetaan käytöstä. Jokaisella verkkoon yhdistetyllä langattomalla laitteella tulee olla turvallisuusprofiili, hyväksytyt asetukset, omistaja, sekä tieto miksi tarvitaan työssä.<br><br>Haavoittuvuusskannuksessa testataan myös, ettei langatonta verkkoa ole yhdistetty tuotantoverkkoon. Wireless IDS-palvelua käytetään haitallisten langattomien laitteiden ja hyökkäysyritysten tunnistamiseen. Erilliset VLAN-aliverkot BYOD ja muille ei-luotetuille laitteille. |
| CSC 17: Turvallisuustaitojen arviointi ja koulutus | Järjestetään kybertaitojen mukainen peruskoulutus ja kehityskartta kaikille työntekijöille.<br><br>Toteutetaan turvallisuustietoisuusohjelma, joka:<br>1) keskittyy hyökkäystapoihin jotka voi itse estää.<br>2) hyväksikäyttää verkon kautta jaettavia aineistoja.<br>3) päivitetään säännöllisesti (vähintään vuosittain) sisältäen uusimmat hyökkäystekniikat.<br>4) vaaditaan kaikilta työntekijöiltä vähintään vuosittain.<br>5) valvotaan että kaikki suorittavat loppuun.<br>6) sisältää johtajien viestin ja osallistumisen harjoitukseen.<br><br>Paranna tietoisuustasoja säännöllisten testien kautta, esim. klikkaavatko työntekijät epäilyttävän sähköpostin linkkiä tai luovuttavatko salaista tietoa puhelimessa ilman todennusta. Arvioi turvallisuustaitoja erityisesti kriittisessä roolissa toimivien osalta. |
| CSC 19: Tietoturvahäiriöihin vastaaminen ja hallinta | Kyberhäiriöiden hallintakäytännöt ja kuvaukset henkilöstön rooleista.<br>Määritetään häiriöiden käsittelyprosessin ja päätöksenteon johtohenkilöt.<br><br>Kommunikoidaan henkilöstölle, miten kyberhäiriöistä ja poikkeamista pitää raportoida häiriöhallintatiimille: raportointiviive, sisältö ja käytännöt, ml. CERT -ilmoituskäytännöt ja kolmansien osapuolten yhteystiedot.<br><br>Järjestetään hallintatiimin kanssa säännöllinen häiriöskenaarioiden läpikäynti henkilöstölle, jotta kaikki ymmärtävät nykyiset uhat ja riskit, sekä omat velvollisuutensa. |
| CSC 20: Penetraatiotestit ja Red teamin harjoitukset | Suunnitellaan ja järjestetään säännölliset ulkoiset ja sisäiset penetraatiotestit.<br><br>Toteuta säännölliset Red teamin harjoitukset, joissa testataan yrityksen valmiuksia tunnistaa ja pysäyttää hyökkäyksiä. Dokumentoi ja suunnittele harjoitustulosten pisteytys.<br><br>Kehitä harjoitustestialusta sellaisille harjoituksille ja testeille, joita ei esim. riskien takia kannata toteuttaa todellisessa tuotantoympäristössä. |

Lähde: ETSI TR 103 305 -sarjan tekniset raportit: “Security Assurance by Default; Critical Security Controls for Effective Cyber Defense”




# Arkkitehtuurit liittyvät kaikkeen

**Projekteissa tulee selvittää kenen toimesta ja missä vaiheessa vaihtoehtoiset arkkitehtuurit tulee analysoida ja kiinnittää tilaajan ja toimittajien kesken!**

**Analysoitavia asioita ovat mm.:**

- ✓ **Fyysinen & looginen dataverkkoarkkitehtuuri, tietoliikennearkkitehtuuri**
- ✓ **Automaatiojärjestelmäarkkitehtuuri**
- ✓ **Toimilaitteen toteutusarkkitehtuuri**
- ✓ **Automaatio-ohjelmisto- ja sovellusarkkitehtuuri**
- ✓ **Hallinta- tai ylläpitoarkkitehtuuri**
- ✓ **Tietoturva-arkkitehtuuri**
- ✓ **Seuranta-arkkitehtuuri**
- ✓ **jne.**

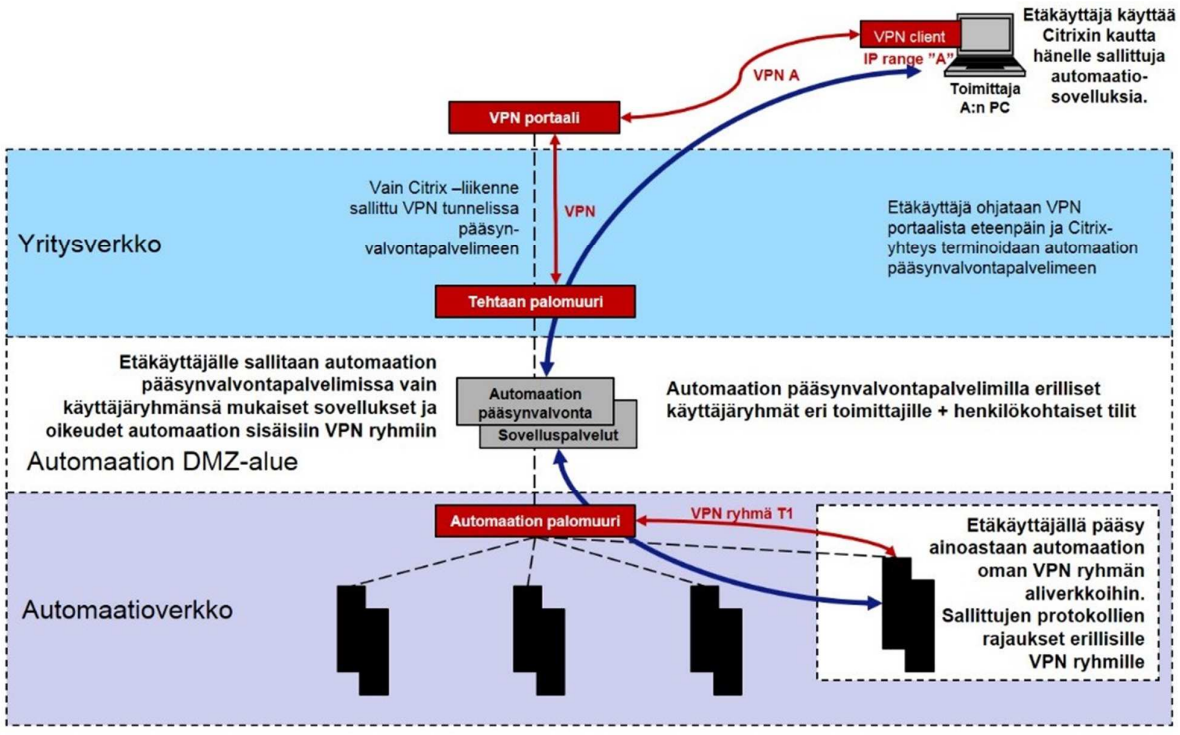
# Turvallisten arkkitehtuurien merkitys

**Tuotantoympäristön tietoliikennettä, dataa ja laskentaa erottelevissa suoja-alueissa, aliverkoissa ja virtuaaliympäristöissä on aukkoja:**

- ✓ **Automaation valvottua verkkoarkkitehtuuria tarvitaan teollisen Internetin ja vapaiden taajuuksien ja mobiiliverkkojen langattoman tiedonsiirron tunkeutuessa tuotantoon!**
- ✓ **Kyberturvallisuuden varmistaminen edellyttää turvallista toteutusta ja ylläpitoa, sekä toteutuneen käyttäytymisen valvontaa! Fokuksessa:**
  - ✓ **yhdyskäytävälaitteet ja –ohjelmistot, sekä**
  - ✓ **langattomat verkot (mm. kiinteistö-automaatio)**



# Automaation etäyhteyksien arkkitehtuurikonsepti - Esimerkki



# Ekosysteemin valinnasta

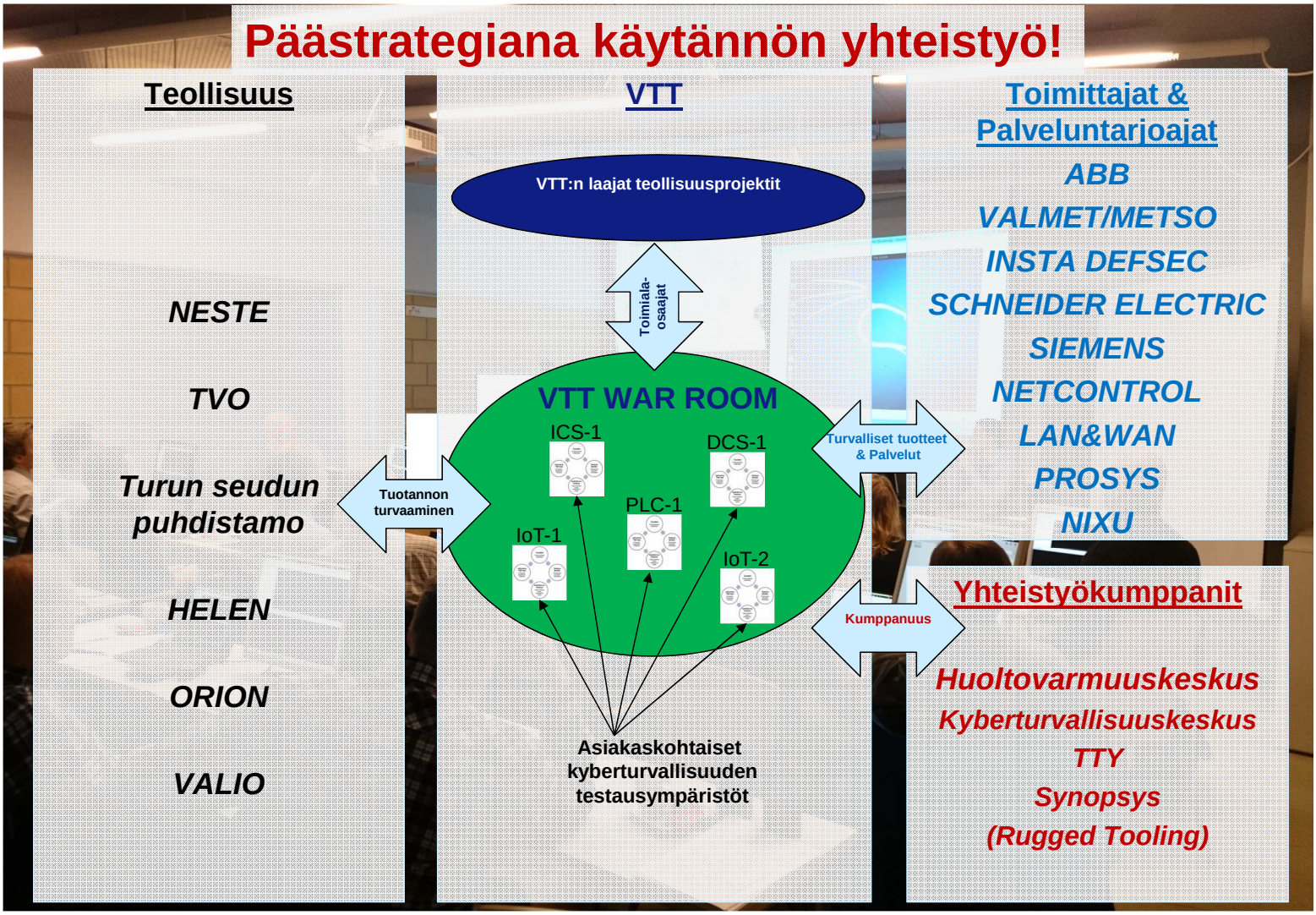
**Mikäli realistisena uhkakuvana pidetään valtiollisten toimijoiden toteuttamaa yritysvakoilua ja soluttautumista, huoltovarmuuskriittisen yrityksen tulee huomioida nämä riskit omissa ekosysteemivalinnoissaan.**

**Tällöin voidaan asettaa tavoitteeksi, että varajärjestelmien tulee olla pääjärjestelmätoimittajasta riippumattomia teknologisesti, maantieteellisesti ja poliittisesti.**

**Esim. tietoliikennejärjestelyt vaativat tyypillisesti erilliset varajärjestelmät päätelaitteineen, verkkoineen ja operaattoreineen.**


## AUTOMAATIOJÄRJESTELMIEN KYBERTURVALLISUUSTESTAUKSEN KEHITTÄMINEN

# Päästrategiana käytännön yhteistyö!




# VTT Cyber Security WAR ROOM

## What is the War Room?

- Includes a mini-Internet environment that is completely isolated from all other telecommunications
- Devices or software can be subjected to highly realistic cyber-attacks in a controlled way
- Wide range of attacks can be tried to test the performance of various systems
- Personnel of over 30 researchers with extensive experience and knowhow on cyber security
- Equipped with cutting edge technologies and devices


## War Room enables

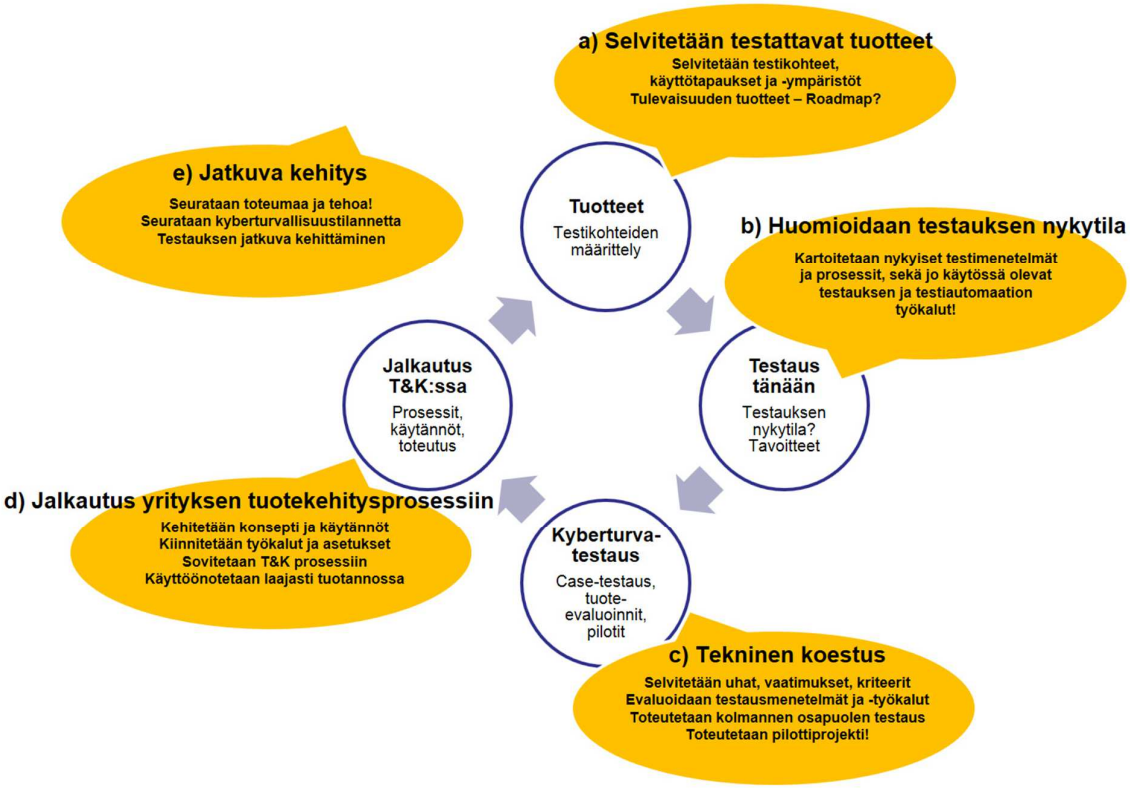
- Conducting of attacks aimed at seizing systems, implementation of typical hacker attack strategies and botnet attacks
- Identification of cyber attacks, threats and vulnerabilities
- Monitoring effective attacks and developing tools for cyber situational awareness
- In-depth cyber analyses from network traffic log information
- Security testing of products and services
- SW security auditing

# VTT Cyber Security WAR ROOM


- Muista verkoista eristetty tietoliikenneympäristö
- Sisältää fyysisen verkon ja virtualisoituja ympäristöjä
- Testattavia laitteita tai järjestelmiä vastaan voidaan tehdä todenmukaisia hyökkäyksiä:
  - Hakkerityökalut, kaupalliset tietoturvatestaustyökalut, bottiverkot
- Tietoturvan monitorointi ja tilannekuva

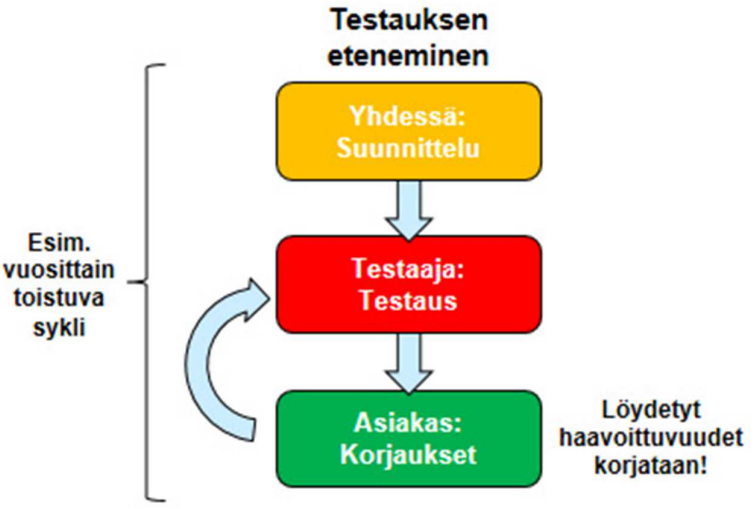


# Tietoturvatestauksen kehittämisen prosessi



# Teknisen koestuksen eteneminen yksinkertaistettuna

1) SUUNNITTELU: Aluksi suunnitellaan yhdessä testattavat **kohteet**, **käyttötapaukset** sekä erityisesti testauksen sisältö: millä menetelmällä ja työkalulla testaus toteutetaan ja **kuinka laaja testaus** tulee olemaan.
2) TESTAUS: Kyberturvallisuustestaaja suorittaa testauksen parhaan osaamisensa mukaan ja kirjoittaa tuloksista testiraportin. **Usein parhaaseen tulokseen päästään, jos mukana on useita testaajia ja asiakasta voidaan konsultoida** esim. testikohteen oikean käyttäytymisen suhteen testauksen alaisena.
3) KORJAUKSET: **Asiakas korjaa tai korjauttaa** tuotteensa testiraportin ilmoittamien löydösten mukaisesti. Tämän jälkeen korjattu tuote kannattaa **uudelleen testata**, jotta varmistutaan että viat on saatu poistettua ja että korjaukset eivät sisällä uusia haavoittuvuuksia.






# Mitä syntyy testauksen tuloksena?

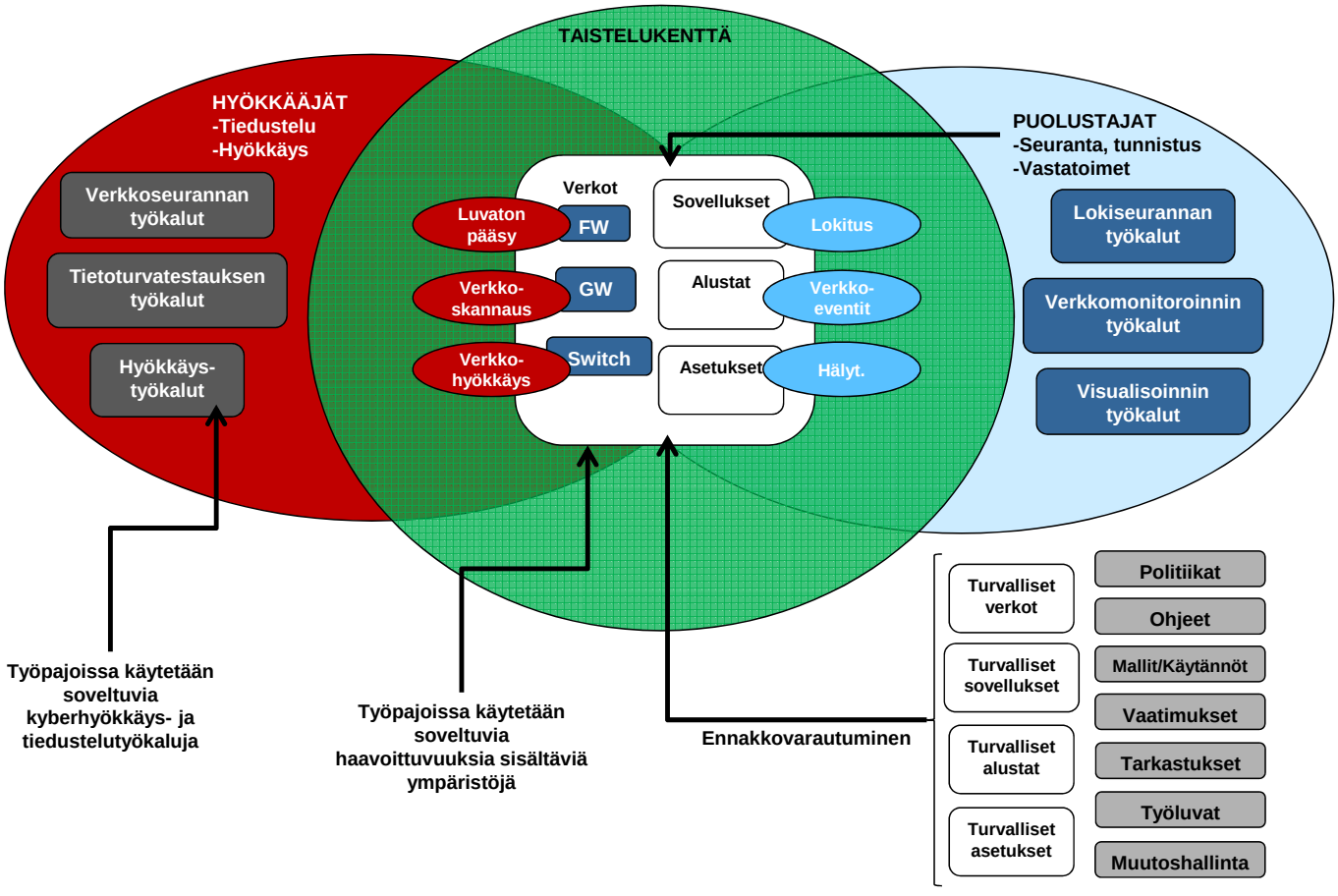
- ✓**Löytyneet viat ja haavoittuvuudet kehittäjälle**
- ✓**Testiraportit tilaajalle**
  - ❖Kuka testasi, miksi (tavoite) ja milloin?
  - ❖Testiympäristön kuvaus
  - ❖Testikohteet (rajapinnat, protokollat…)
  - ❖Käytetyt menetelmät, ala (*scope*), työkalut, työmäärät
  - ❖Löydökset
  - ❖Parannusehdotukset
- ✓**Jatkuva testaus järjestelmäkehityksen tukena**

MITEN KEHITTYÄ ?
Tarvitaan harjoitteluympäristö!
Integroidut järjestelmät kohteeksi
Kokeillaan ja opitaan yhdessä!
Selvitetään mitä on realistista vaatia

# HANDS-ON KYBERHARJOITTELU YRITYKSILLE



# HANDS-ON KYBERHARJOITTELU -konsepti



# HANDS-ON KYBERHARJOITUS JO 2015!

Eristetty siirrettävä ympäristö.
Aitoja ja virtuaalisia komponentteja.
Hyökkäys ja tunnistus tutuksi opastettuna.
Hyökkääjän asenne tutuksi.
Paljon opittavaa!

i. Yritysosallistujien (26 hlö) esittely: 10:00 →

ii. Orientaatio ja osallistujien PC:hen tutustuminen: 10:15 →

1. Murtautuminen toimistoverkkoon: 10:45 →

2. Hiljainen verkkotiedustelu: 11:30 →

*LOUNAS 12:00 – 13.00*

3. Aggressiivinen tiedustelu: 13:00 →

4. Palvelunesto: 13:30 →

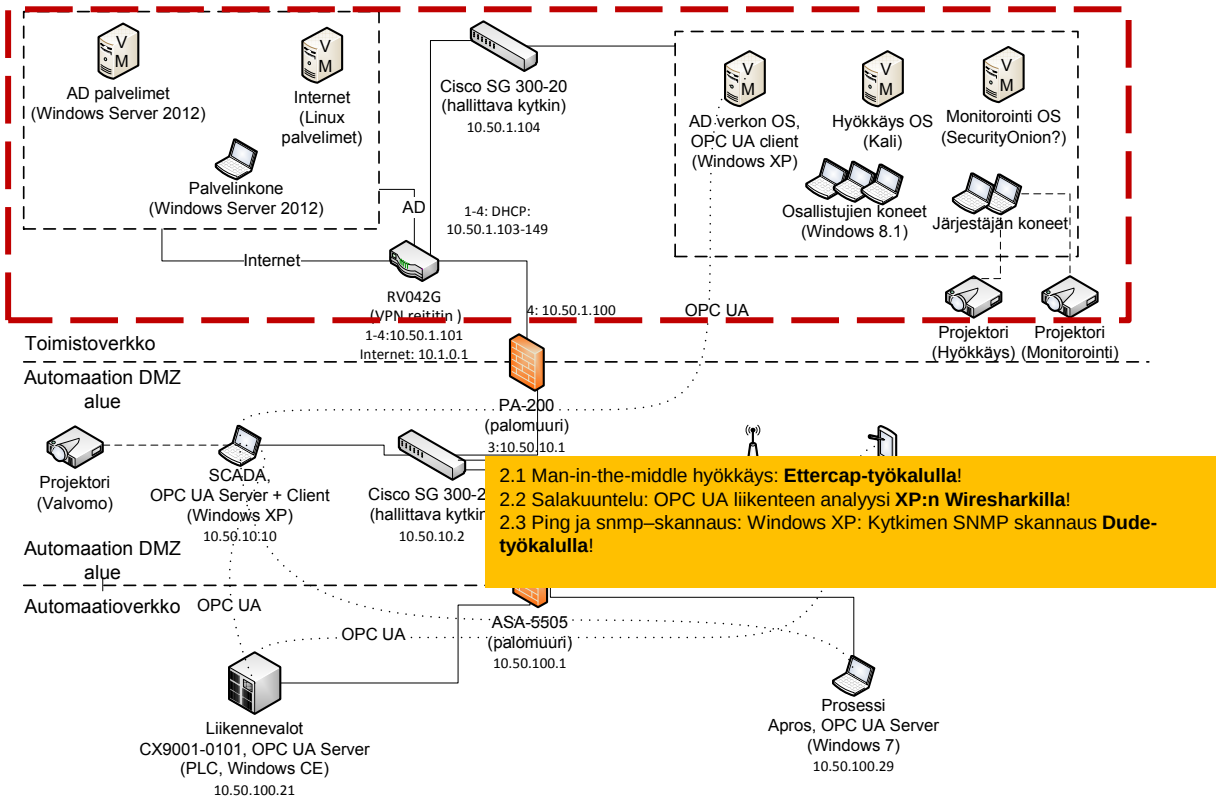
5. Automaatioverkkoon tunkeutuminen: 14:00 →

Työpajan yhteenveto.

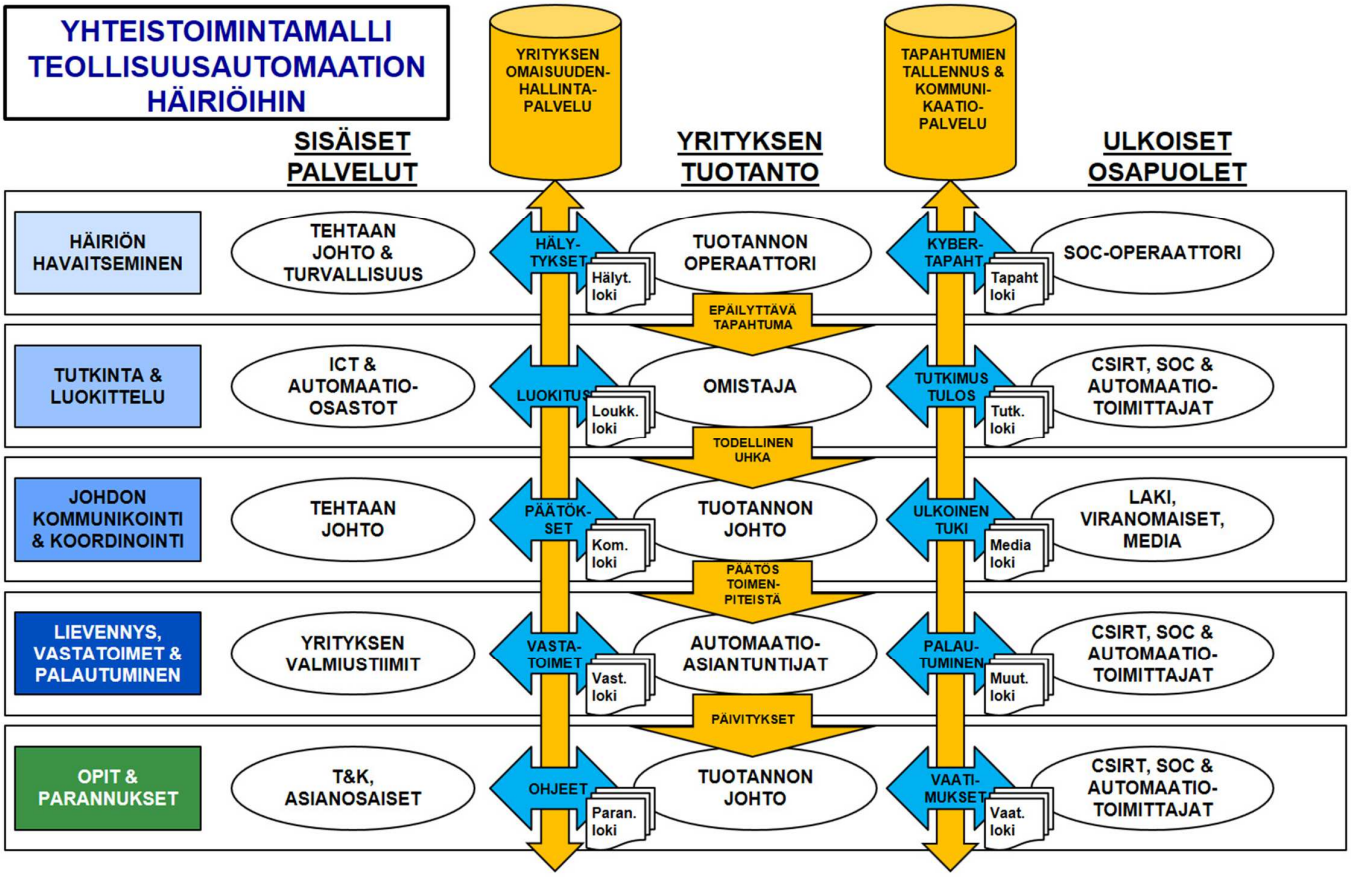
Verkon lokianalyysin alkeet.
Hyökkäyksiä havaittiin ilmaisilla työkaluilla.
Targetin ”kunnonvalvonta”-instrumentointi voidaan tarvittaessa lisätä.



# Hiljainen verkkotiedustelu joulukuun 2015 harjoituksessamme



# Poikkeaman sattuessa - Yhteistoimintamalli






## Hands-on KYBER-harjoituksen SUUNNITTELU JA TOTEUTUS!

**1.Asiakkaan tarve ja koulutussuunnitelmat**
- Asiakkaan tarpeet ja tavoitteet,
- Asiakkaan omat koulutussuunnitelmat,
- Asiakkaan omat tietoturvaohjeistot.

**2.Yhteiset suunnittelukokoukset**
- Harjoituksen tavoitteet,
- Skenaarioiden pohdintaa / määrittelyä,
- Harjoitteluympäristön pohdintaa / määrittelyä,
- Toteutuksen ideointia / suunnittelua,
- Juoksutuksen ideointia / suunnittelua

(opt.) Asiakkaan *target*-ympäristö
- Asiakaskohtaisen *target*-ympäristön määrittely ja kasaus
- Asiakkaan laitteita ja ohjelmistoja
- Asiakkaan työkaluja?

**3.Harjoitusympäristön pystytys VTT:lle**
- Harjoittelukokonaisuuden pystytys
  - VTT:n harjoitteluympäristöjen komponentteja
  - (Asiakkaan laitteita ja ohjelmistoja, työkaluja?)

**Jos asiakkaan oma *target*-kohde**

**4.VTT esianalysoi ja koestaa**
- VTT tutkii harjoitteluympäristön haavoittuvuuksia
- VTT selvittää soveltuvat hyökkäys-, tunnistus- ja puolustustyökalut
- Myös esim. asetusvirhe (joka korjataan livenä)

**5.Harjoitus**
- VTT vetää harjoituksen asiakkaalle, asiakkaan henkilöstö harjoittelee
- Aineiston ja ohjeiden toimitus
- Palautekysely?

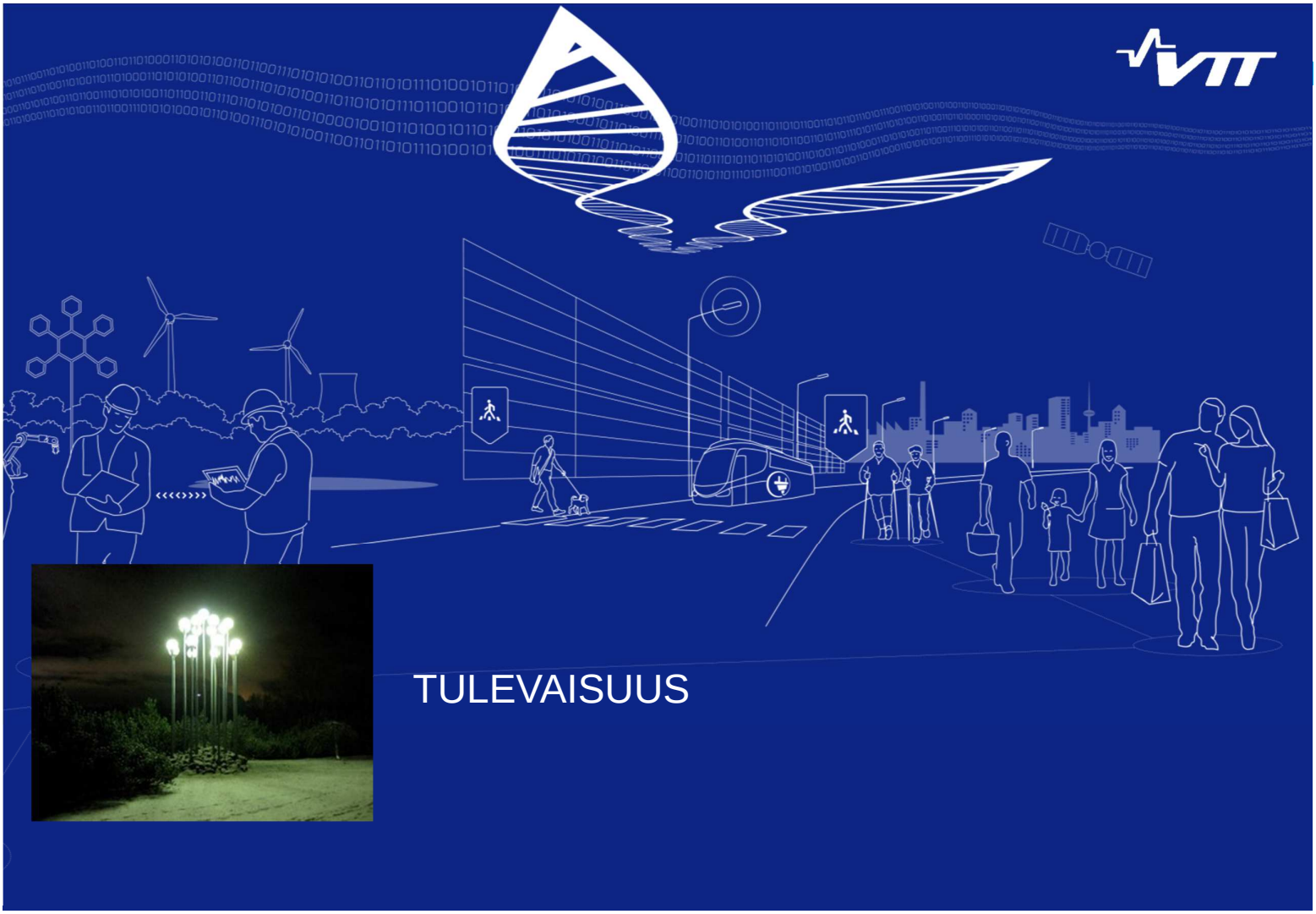
(opt.) *Target* -tulokset
- VTT viimeistelee ja toimittaa *target*-ympäristöön kehitetyt skriptit ja asetukset asiakkaalle

**Otaniemi 14.12.2016:**

# KYBER-TEO 2014 – 2016
# Julkisten tulosten esittely

**YLI 100 AMMATTILAISTA!**

| | | | |
|---|---|---|---|
| **KYBER-TEO 2014-2016 JULKISTEN TULOSTEN JA KYBERHARJOITTELUN ESITTELYTILAISUUS, 14.12.2016** | | | |
| Aika: Keskiviikko 14.12.2016, klo 9.30 – 14.30. Paikka: Geologian tutkimuskeskus, auditorio, Betonimiehenkuja 4, Espoo | | | |
| Kahvitarjoilu alkaa | | 9:00 | |
| **JULKAISU, PALVELUT, TULOKSET -osuus** | **Kuka** | **Aloitus** | **Kesto** |
| 01_Tilaisuuden avaus ja ajankohtaiset asiat | HVK: Sauli Savisalo | 9:30 | 10 min |
| 02_KYBER-TEO 2014- 2016 tulosten kokoomajulkaisu | VTT: Pasi Ahonen | 9:40 | 20 min |
| **KYBER-TEO 2014-2016 yritysten kyberoppeja** | | **10:00** | **(yht. n. 50 min)** |
| 03_Neste-case | Neste: Pasi Lehtinen | 10:00 | 10 min |
| 04_Turun Seudun Puhdistamo-case | TSP: Jyrki Haapasari | 10:10 | 10 min |
| 05_Outotec-case | Outotec: Patrik Granholm | 10:20 | 10 min |
| 06_Netcontrol-case | Netcontrol: Kim Malmberg | 10:30 | 10 min |
| 07_Prosys-case | Prosys: Jouni Aro | 10:40 | 10 min |
| *(lyhyt tauko)* | | *10:50* | *10 min* |
| **08_Kyberturvallisuuskeskuksen palvelut, yhteistyöverkostot** | Kyberturvallisuuskeskus: Erika Suortti-Myyry | 11:00 | 15 min |
| **KYBER-TEO 2014-2016 yritysten kyberoppeja & palveludemonstraatioita** | | **11:15** | **(yht. n. 45 min)** |
| 09_Nixun palvelut | Nixu: Kalle Luukkainen | 11:15 | 10-15 min |
| 10_Orion-case | VTT: Pasi Ahonen | 11:25 | 5 min |
| 11_Valmet-case + demo | Valmet: Markku Tyynelä | 11:30 | 15 min |
| 12_Nordic LAN&WAN Communicationsin palvelut | LAN&WAN: Juha Pasanen | 11:45 | 15 min |
| | | | |
| *LOUNAS 12:00 - 13:00* | | *12:00* | *60 min* |
| | | | |
| **Klo 13:00: KYBERHARJOITTELUN ESITTELY -osuus** | | | |
| 13_Automaation kyberturvallisuuden yhteistyöportaalin suunnittelusta | VTT: Pasi Ahonen | 13:00 | 10 min |
| 14_VTT:n johdanto kyberharjoitteluun | VTT: Pasi Ahonen | 13:10 | 15 min |
| 15_Hyökkäysten havaitseminen ja torjuminen - demonstraatioita | VTT: Sami Noponen (a) ja Juha Pärssinen (b) | 13:25 | 20 min |
| 16_EXTRA Cysec: Tietoliikenteen tallennus | Cysec: Juhani Kallio ja Harri Luuppala | | |
| 17_Automaation tietoturvakoulutus ja harjoittelu | TTY: Jari Seppälä | 13:45 | 20 min |
| 18_MPK:n kyberturvallisuuskurssit | Etelä-Suomen maanpuolustuspiiri Helsingin Koulutus- ja Tukiyksikkö: Kim Malmberg | 14:05 | 15 min |
| 19_Yhteenveto: Automaation kyberongelmat ja -ratkaisut, yhteistyö ja tulevaisuus | VTT: Pasi Ahonen | 14:20 | 10 min |
| **Tilaisuus päättyi klo 14:30** | | | |



## Tavoitetila 2020!

**Tavoitetilassa Suomessa on aina saatavilla riittävästi huoltovarmuuskriittisten yritysten kyberturvallisuutta tehokkaasti edistävää ja tukevaa kotimaista liiketoimintaa.**



## AIKATAULU 2017 – 2020 (syksyllä 2016)

LUOTTAMUKSELLINEN

# TULOSSA: CYBER-POWER 2017-2020

## Sisällysluettelo



**Osallistujiksi kriittisiä energia- tai kiinteistöautomaatio-tuotteita ja -palveluja tuottava elinkeinoelämä, sekä energian tuotantoa, siirtoa ja jakelua ylläpitävät ja varmistavat kriittisen infrastruktuurin toimijat.**



# KIITOKSET!

## Kiinnostuitko? Ota yhteyttä:


**Pasi Ahonen, Johtava tutkija, KYBER-TEO projektipäällikkö.**
**Sähköposti: pasi.ahonen@vtt.fi**
**GSM: 044-730 7152.**