Teemana kyberturvallisuus

ASAF Kahvit 25.3.2022

Pasi Ahonen, https://kyberhallinta.fi/

Alustukseni sisältö

- Alustajan esittely
- Kyberturvallisuus – mitä se on, mihin se liittyy?
- Kyberturvallisuus automaatiossa:
  - Lyhyt oppimäärä
  - Standardit
  - Etäyhteyshaasteet
  - Moderni lähestymistapa

Lopuksi: Kysymykset ja keskustelu!

Kuka puhuu: Pasi Ahonen

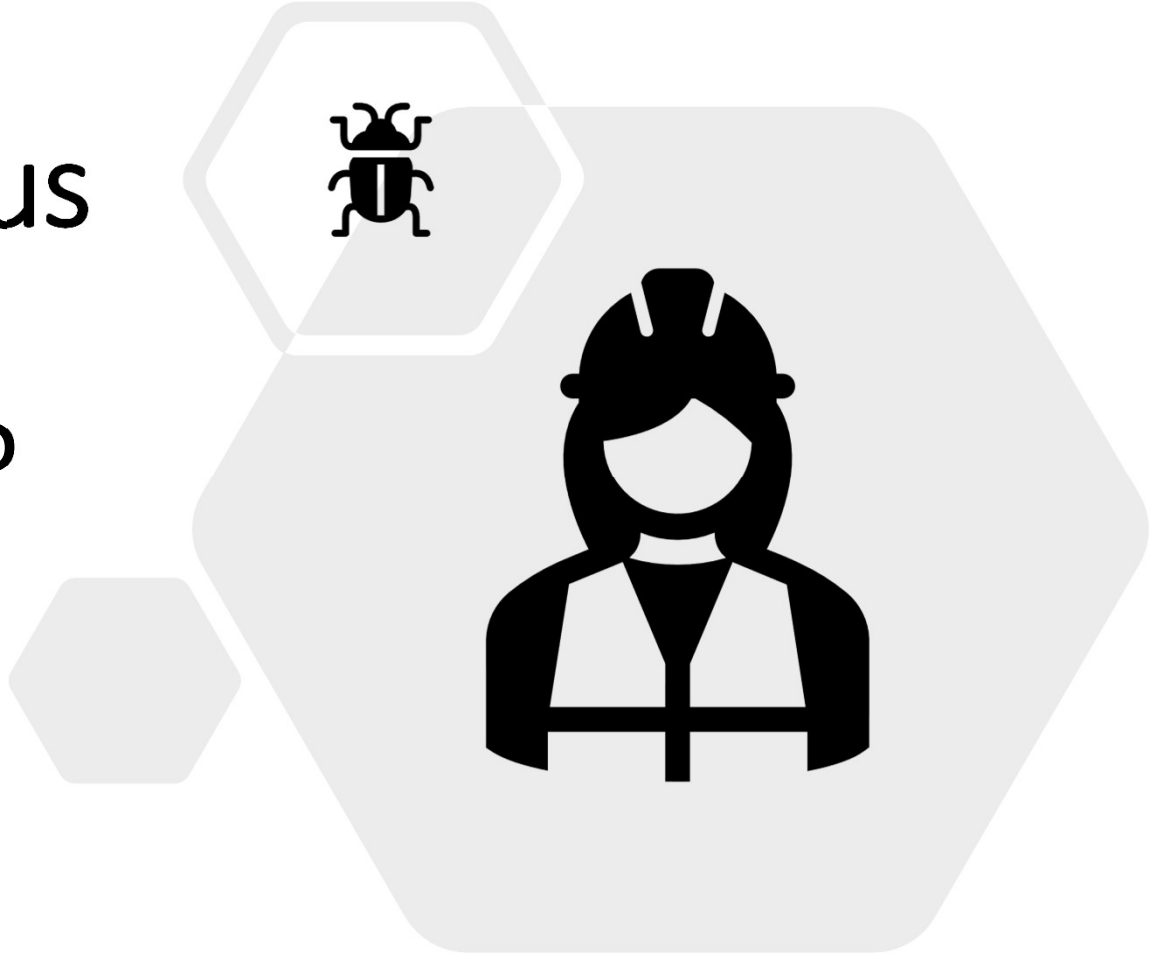
Projektipäällikkö ja pääkirjoittaja:

- ❑ **TITAN-käsikirja** (2008-2010) (VTT)
- ❑ **TEO-TT** (2011-2012) (HVK)
- ❑ **COREQ-VE** (2011-2012) (HVK)
- ❑ **COREQ-ACT** (2012-2013)
- ❑ **Tietoturvaa huoltovarmuuskriittisille yrityksille**, HVK-kirjanen
- ❑ **KYBER-TEO** 2014, HVK-kirjanen
- ❑ **KYBER-TEO** 2014-2016 kirja (VTT)
- ❑ **KYBER-ENE** 1 & 2 kirja (2017-2019)

Kyberhallinta Pasi Ahonen Oy
+358 44 730 7152
pasi.ahonen@kyberhallinta.fi
Kotisivu: www.kyberhallinta.fi

Tarkempi esittely ja mm. palvelutuotteet: https://kyberhallinta.fi/

Kyberturvallisuus – mitä se on, mihin se liittyy?



Tietoturvallisuus on perinteisesti päivityksiä ja vikakorjauksia!

“Konepajakin” myy jo haavoittuvuuksien hallintaa palveluna, ym.!

Ref: https://cdn.wartsila.com/docs/default-source/service-catalogue-files/engine-services---4-stroke/wartsila-ics-vulnerability-management.pdf

Kokonaisvaltainen kyberuhkiin varautuminen on relevanttia ja osa arkipäivää kriittistä infraa ylläpitävissä yrityksissä!

Myös kiristyshyökkäykset kohdistuvat yhä enemmän teollisuusyrityksiin!

Mitä kyberturvallisuus on?

Ref: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Hyvä kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan:

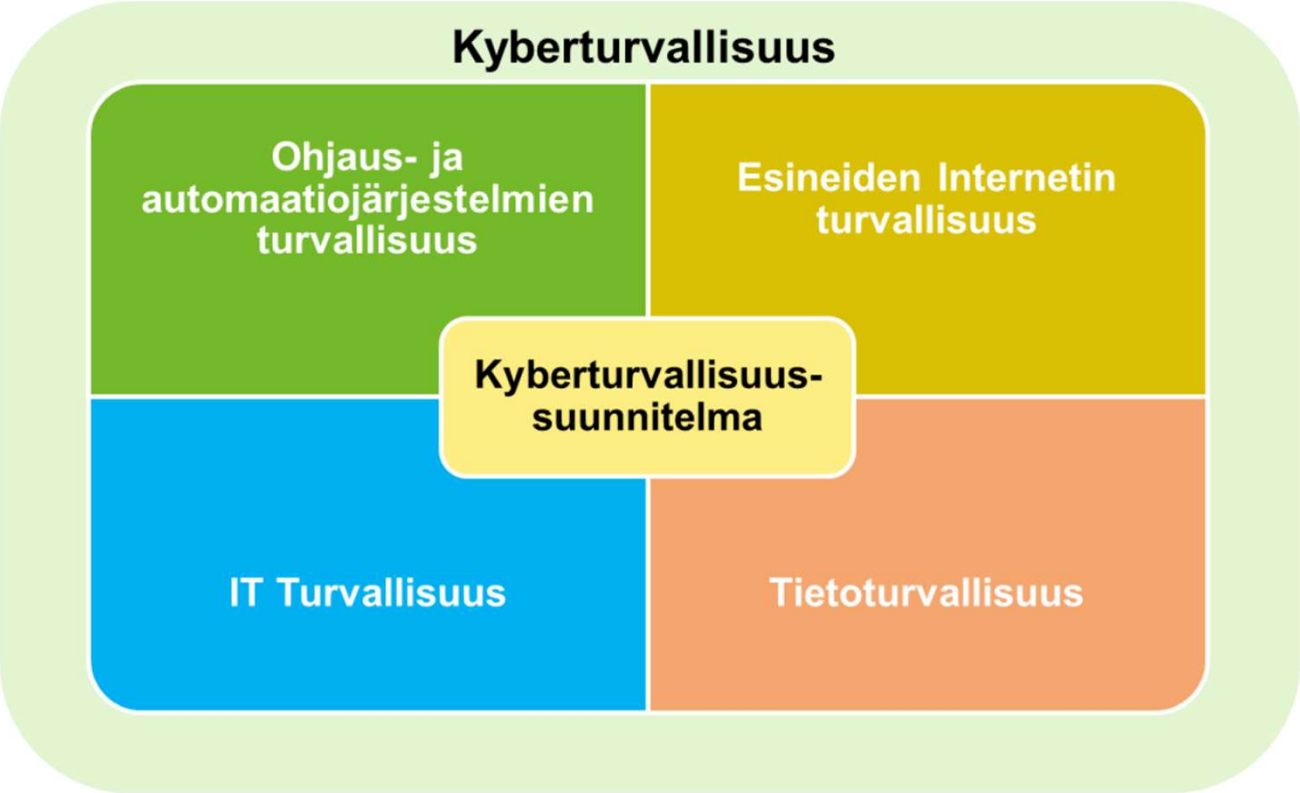
- Toimenpiteitä, joilla hallitaan ja siedetään erilaisia kyberuhkia ja niiden vaikutuksia
- Toimenpiteitä, jotka turvaavat kybertoimintaympäristöstä riippuvaisen fyysisen maailman
- Tietoturvallisuus on kyberturvallisuuden keskeinen osatekijä

Kyberturvallisuus sisältää digitaalisen ja verkottuneen yhteiskunnan turvallisuustilan vaikutuksineen.

➔ Toiminta tulee turvata kokonaisvaltaisen ajattelun ja yhteistyön pohjalta!

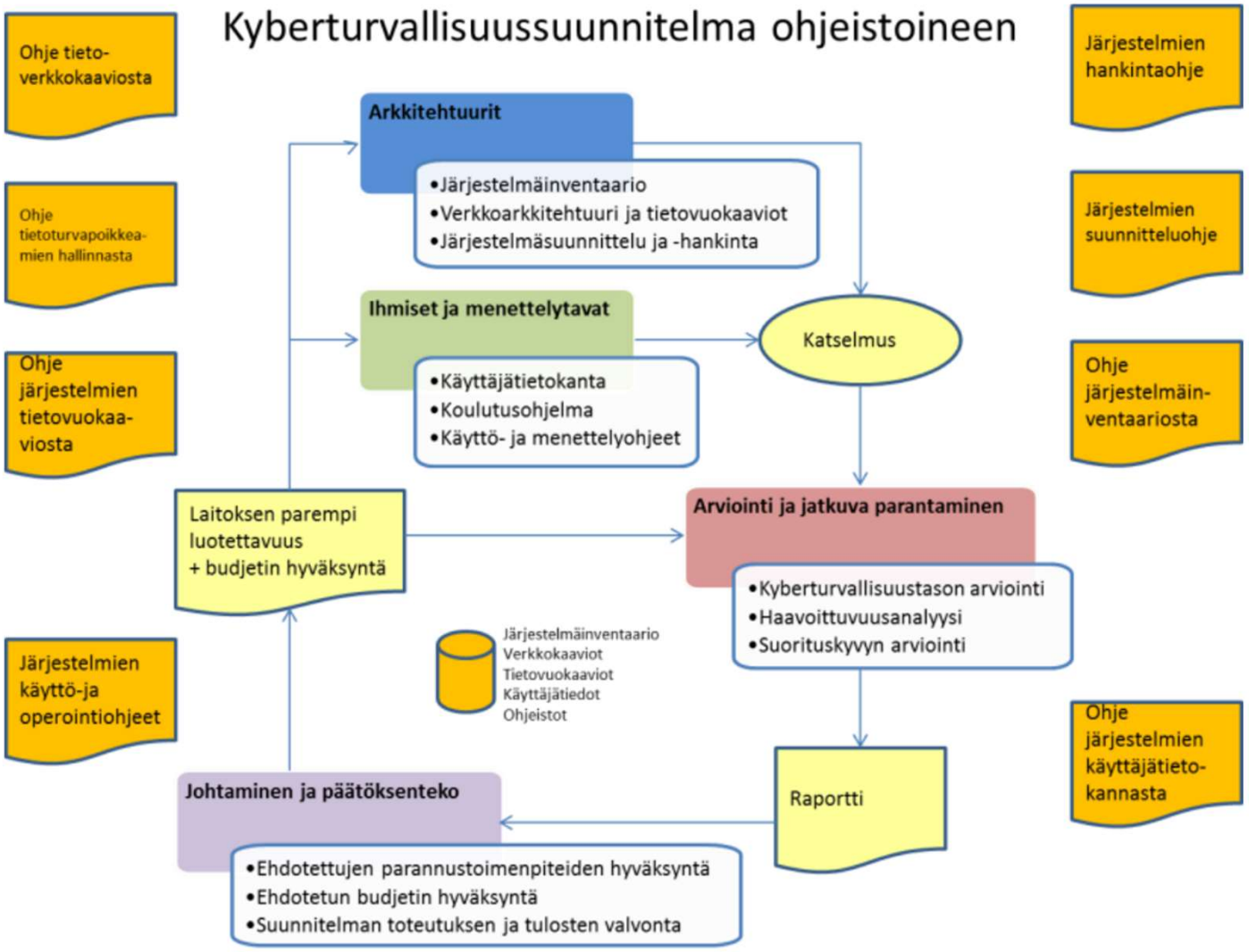
Mihin kyberturvallisuus liittyy?

Kyberturvallisuus vaatii kokonaisvaltaista suunnittelua ja toteutusta!

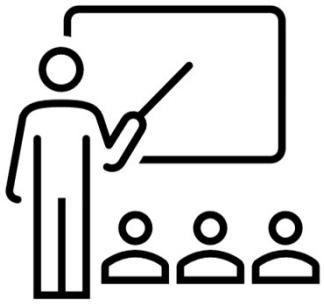


Kuva, Jarmo Huhta: https://www.theseus.fi/bitstream/handle/10024/139741/jarmo_huhta_ONT.pdf

Esimerkki kokonaisvaltaisesta kyberturvallisuus-suunnitelmasta!



Kuva, Jarmo Huhta: https://www.theseus.fi/bitstream/handle/10024/139741/jarmo_huhta_ONT.pdf

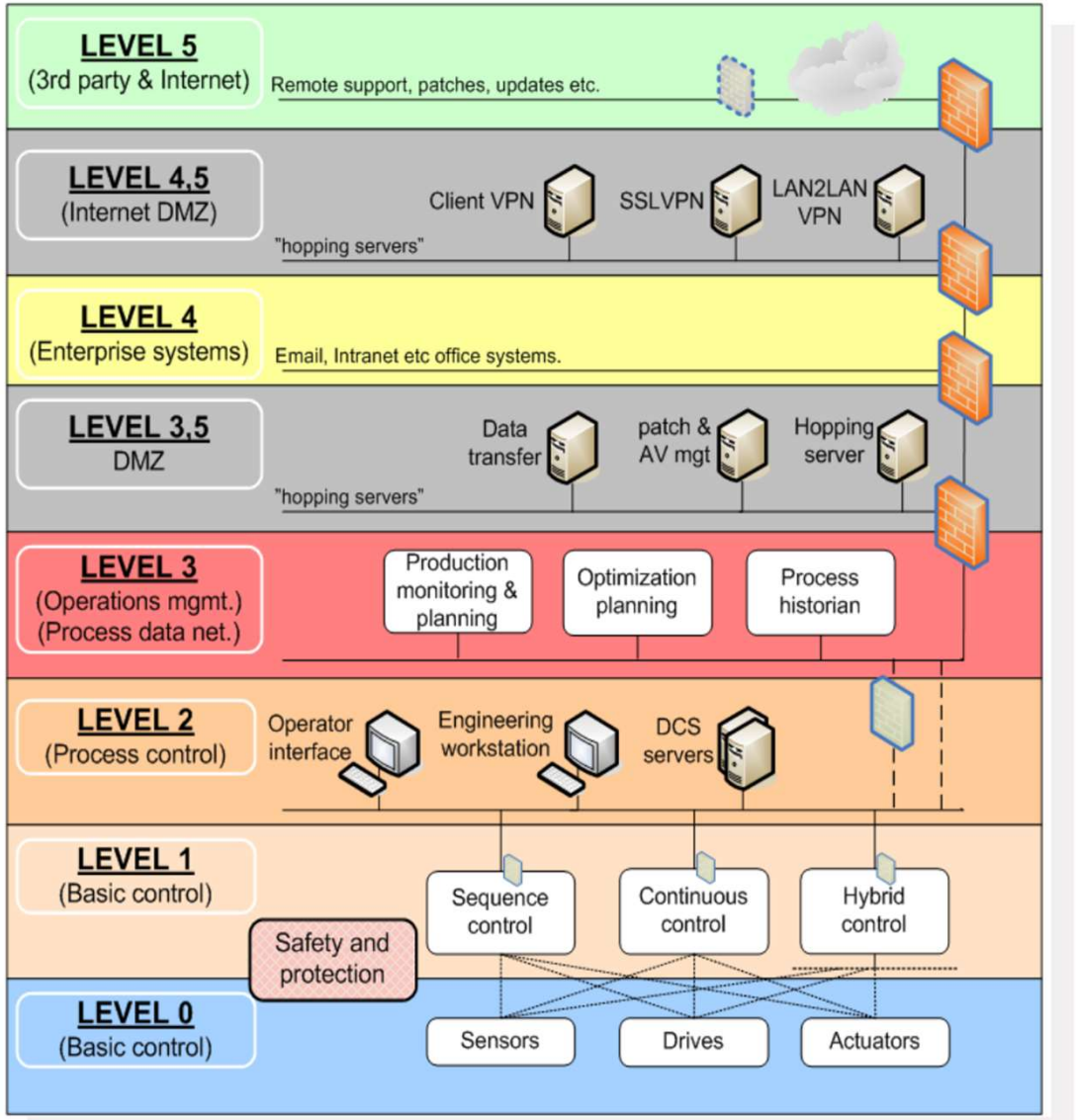


Kyberturvallisuus automaatiossa

- **Lyhyt oppimäärä!**
- Standardit
- Etäyhteyshaasteet
- Moderni lähestymistapa

Teollisuuden ohjaus- ja automaatiojärjestelmien verkkoarkkitehtuuri

Suunnittele yritystasoinen verkkoarkkitehtuuri siten, että se palvelee liiketoiminnan vaatimuksia ja vastaa sen riskeihin!



Kuva, Jarmo Huhta: https://www.theseus.fi/bitstream/handle/10024/139741/jarmo_huhta_ONT.pdf

Automaatioverkon arkkitehtuuri & vyöhykkeet

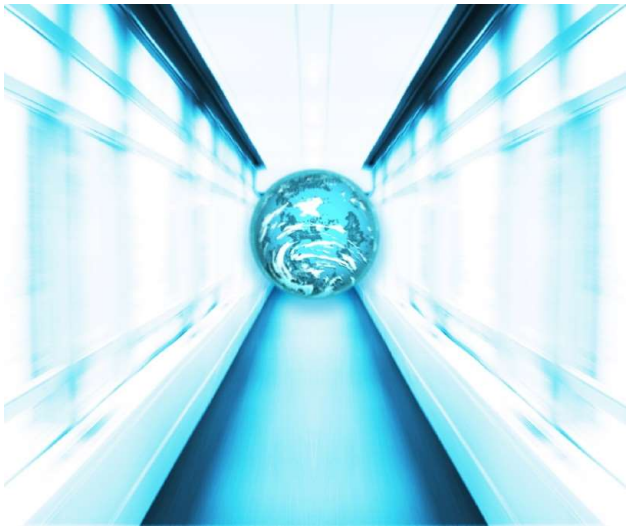
Varmista dataverkon redundanssi & varalaitteet

- **VARALAITTEET: Verkkoelementtien varastokappaleita saatavilla ja konfiguraatio nopeasti asennettavissa (kun lupa asentaa).**
- **KAHDENNUS: Johdotusten kahdennus, väylä, rengas-, tähti-, *mesh*-topologiat.**
- **VIKASIETOISUUS: Industrial Ethernetin välitön palautuminen viasta: HSR (IEC 62439-3). Ethernet: *Rapid Spanning Tree Protocol*.**
- **YHTEYDET: Varasiirtotie *site*-yhteyksille (esim. kaksi teleoperaattoria).**
- **PALAUTUS: Elementtien konfiguraation varmuuskopiointi & palautus.**

Lähde: Tietoturvan aktiiviset teollisuus-caset (COREQ-ACT), 2013

Automaatioverkon arkkitehtuuri & vyöhykkeet

Varmista dataverkkojen riittävä kapasiteetti & palvelutaso



- **SIIRTOKAISTA: Riittävä tiedonsiirtokaistan varaus kriittisissä segmenteissä / *trunk*:ssa (tulevaisuuden tarpeet huomioitu).**
- **ASETUKSET: Tiedonsiirron puskureiden koko ja asetukset jotka toimivat testatusti myös virhetilanteissa.**
- **LOKI: Riittävä lokimuistin määrä ja kyky lokiraportin lähettämiseen tietoturvallisesti.**
- **DATAMYRSKY: Lokidatan päällekirjoitus/pysäytys pakettimyrskyssä (kun DoS-hyökkäys epäily).**
- **IC-PIIRIT: Riittävä CPU- ja muistikapasiteetti kryptografiselle tunnistautumiselle (*VPN authentication*, *Diffie-Hellman* avaimenvaihto, jne.).**

Lähde: Tietoturvan aktiiviset teollisuus-caset (COREQ-ACT), 2013

Automaatioverkon arkkitehtuuri & vyöhykkeet

Jaa dataverkot toiminnallisiin vyöhykkeisiin

VYÖHYKKEITÄ (tai SEGMENTTEJÄ):

- ❑ **YRITYS: Yritysverkko: Runkoverkko / Palvelinkeskukset / Toimistojärjestelmät.**
- ❑ **TEHDAS: Tehdasverkko (tiedonsiirto tehdasalueella).**
- ❑ **VIERAILIJAT: Langaton vierailijaverkko palveluineen (WiFi). (IEEE 802.1X, RADIUS).**
- ❑ **DMZ: DMZ-vyöhykkeet ja sen palvelut.**
- ❑ **VALVONTA: Valvontaverkko: Valvomot, palvelimet, tallennuspalvelut.**
- ❑ **T&K: *Engineering* -työasemat, kehitys-/testiverkko.**
- ❑ **AUTOMAATIO: Automaatioverkko: Kenttäväylät, logiikat, I/O**
- ❑ **TURVA: Turvaväylät (voi olla myös osana kenttäväyläratkaisua).**

Lähde: Tietoturvan aktiiviset teollisuus-caset (COREQ-ACT), 2013

Automaatioverkon arkkitehtuuri & vyöhykkeet

Ja dataverkot itsenäisesti toimiviin segmentteihin

LOOGINEN SEGMENTOINTI:
Estetään oletusarvoisesti vyöhykkeiden välinen liikenne. Rajaa *broadcast* -liikenteen vaikutuksia:

- ❑ **VLAN: Aliverkkoihin jako vyöhykkeiden sisällä**
  - ✓ **Verkkokytkinten tuettava VLAN-ominaisuutta.**
  - ✓ **IP aliverkkoihin jako vyöhykkeiden sisällä IP osoite-skeeman mukaan.**
  - ✓ **Aliverkkojen välinen data *(trunk data)* sallittu vain tarkkaan määriteltyyn tiedonvaihtoon.**
- ❑ **QoS: Kenttäväylän liikenteen QoS: Tuotannon VLAN priorisoitu (esim. Real-time: IEEE 802.1Q)**
- ❑ **VPN: sallitut yhteydet DMZ verkkoihin ja sitä kautta päätteisiin/käyttäjiin.**
  - ✓ **Myös yritysverkon sisällä voi käyttää VPN-suojausta.**

FYYSINEN SEGMENTOINTI:

- ❑ **KYTKIMET ERIYTETTY: Tehdasverkko ja automaatioverkko eriytetään eri kytkimiin**
- ❑ **KAAPELIT: Verkkokaapeloinnit selkeästi eroteltu ja merkitty:**
  - ✓ **Esim. tuotantolinjoittain**
  - ✓ **Toimituksen segmentit, jne.**
    - ○ **Dokumentoiden kaikki, myös varaukset**

Lähde: Tietoturvan aktiiviset teollisuus-caset (COREQ-ACT), 2013

Automaatioverkon arkkitehtuuri & vyöhykkeet

Rajoita ohjelmistojen ja protokollien käyttöä vyöhykkeissä

- **HYVÄ HALLITTAVUUS : Tarkkaan rajatut sovellukset, käyttöjärjestelmät ja ohjelmistot kussakin vyöhykkeessä.**
  - ✓ **Esim. Toimittajan ylläpitämä aliverkko jossa ainoastaan toimittajan hyväksymät ohjelmistot.**
  - ✓ **Muut aliverkot automaation hyväksymillä ohjelmistoilla.**
  - ✓ **Mahdollisimman yhtenevä protokollapino aliverkon laitteissa.**
- **YKSINKERTAISET SÄÄNNÖT: Yksinkertaista palomuurisäännöt yllä rajatuilla sovelluksilla ja järkevillä protokollavalinnoilla.**
  - ✓ **Kiellä kaikki muu data palomuureissa.**
  - ✓ **Suosi OPC UA sovelluksia ja tietoturvaominaisuuksia.**

Lähde: Tietoturvan aktiiviset teollisuus-caset (COREQ-ACT), 2013

Automaatioverkon arkkitehtuuri & vyöhykkeet

Jaa ylläpitovastuut ja tehtävät selkeästi

VERKON hallinnoinnin / ylläpidon VASTUULLISET on määritelty selkeästi:

- ❑ **VYÖHYKE: Aliverkko / Segmentti: vastuullinen!**
  - ✓ Aliverkon jatkuvan itsenäisen toiminnan varmistaminen
  - ✓ Kaapelien standardit, värit ja merkinnät vyöhykkeissä.
  - ✓ Huomioidaan kuitukaapelin edut ja varakaapelien & standardiliitinten säilytyspaikat.
- ❑ **TYÖASEMAT: Automaatioverkossa olevien yleiskäyttöisten työasemien ylläpito:**
  - ✓ Esim. IT-vastaa automaation ennalta asettamien vaatimusten ja ohjeen mukaan.
- ❑ **TYÖLUPA: Luvat verkon muutostöihin:**

  Työlupa oltava esimerkiksi:
  - ✓ Tuotannolta,
  - ✓ Automaatiolta,
  - ✓ (IT-osastolta).

  HUOM!:
  - ✓ Dokumentoi muutokset ja informoi myös ko. tuotantoverkon automaatiotoimittajaa / palvelutoimittajaa.

Lähde: Tietoturvan aktiiviset teollisuus-caset (COREQ-ACT), 2013

Automaatioverkon suojaustehtävät

Verkon kartoitus (nykyiset tehtaan verkot)

- Verkkolaitteet, johdot, yhteydet, käyttöjärjestelmät, sovellukset, jne.

Vyöhykkeet ja verkkojen eriytys

- Automaatiovyöhyke jota *DMZ* alue erottaa
- Automaation palomuuri ylläpitoineen

Rajoitetut sovellukset ja tiedonsiirtoprotokollat

- Vyöhykkeessä sallitut sovellukset ja protokollat kiinnitetty
- *Application whitelisting* ja *AV* tuotteet käytössä määrätyissä kohteissa

Sallitut tietovuot on määritelty

- Lähdeosoite, kohdeosoite, protokolla, portti, liikennemäärä, käyttötarkoitus

Tietovuorajoitukset vyöhykkeiden/segmenttien välillä

- ACL-pääsylistat palomuureissa ja VLAN-määritykset kytkimissä

Monitorointi on järjestetty

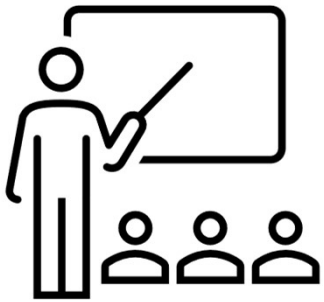
- Palomuurissa ja palvelimissa pääsynvalvonta: s*yslog* tms.
- Verkkoliikenne soveltuvin osin: *IDS* (kriittinen järjestelmä / data)

Etäyhteyskäytännöt on määritelty ja käyttö rajattu

- VPN yhteys terminoitu DMZ:aan toimistoverkon tunnistautumisen kautta

TUOTANNOSSA VAIN YKSI YHTEINEN TOIMINTATAPA AUTOMAATIOVERKON HALLINTAAN JA YLLÄPITOON!

Lähde: Tietoturvan aktiiviset teollisuus-caset (COREQ-ACT), 2013



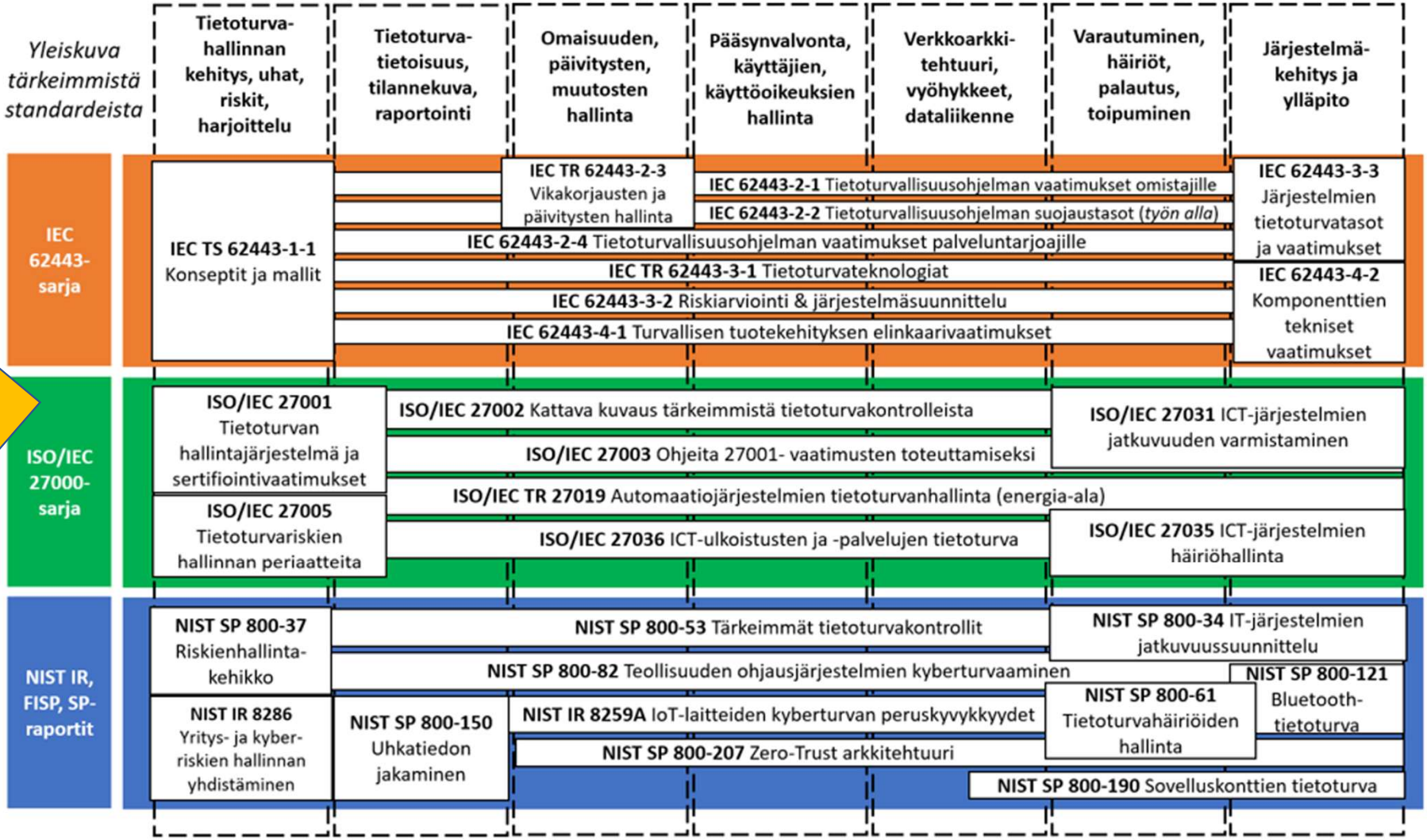
Kyberturvallisuus automaatiossa

- ❑ Lyhyt oppimäärä
- ❑ **Standardit!**
- ❑ Etäyhteyshaasteet
- ❑ Moderni lähestymistapa

Kartta automaatiossa hyödynnettävistä parhaista tietoturva-standardeista!

Useita soveltuvia standardeja!

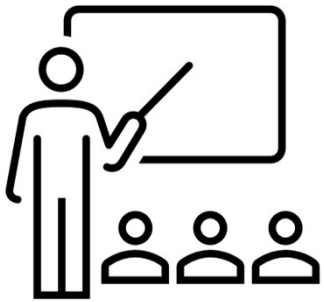
Tieto on hajallaan!



NIST Cyber Security Framework 1.1 (nousussa)

Kuva: Pasi Ahonen

Automaation tietoturva – Kriittisen tuotannon turvaaminen © Suomen Automaatioseura ry (SAS julkaisusarja) www.automaatioseura.fi/AutomaationTietoturva
Päätoimittaja: Pasi Ahonen, Kyberhallinta Pasi Ahonen Oy



Kyberturvallisuus automaatiossa

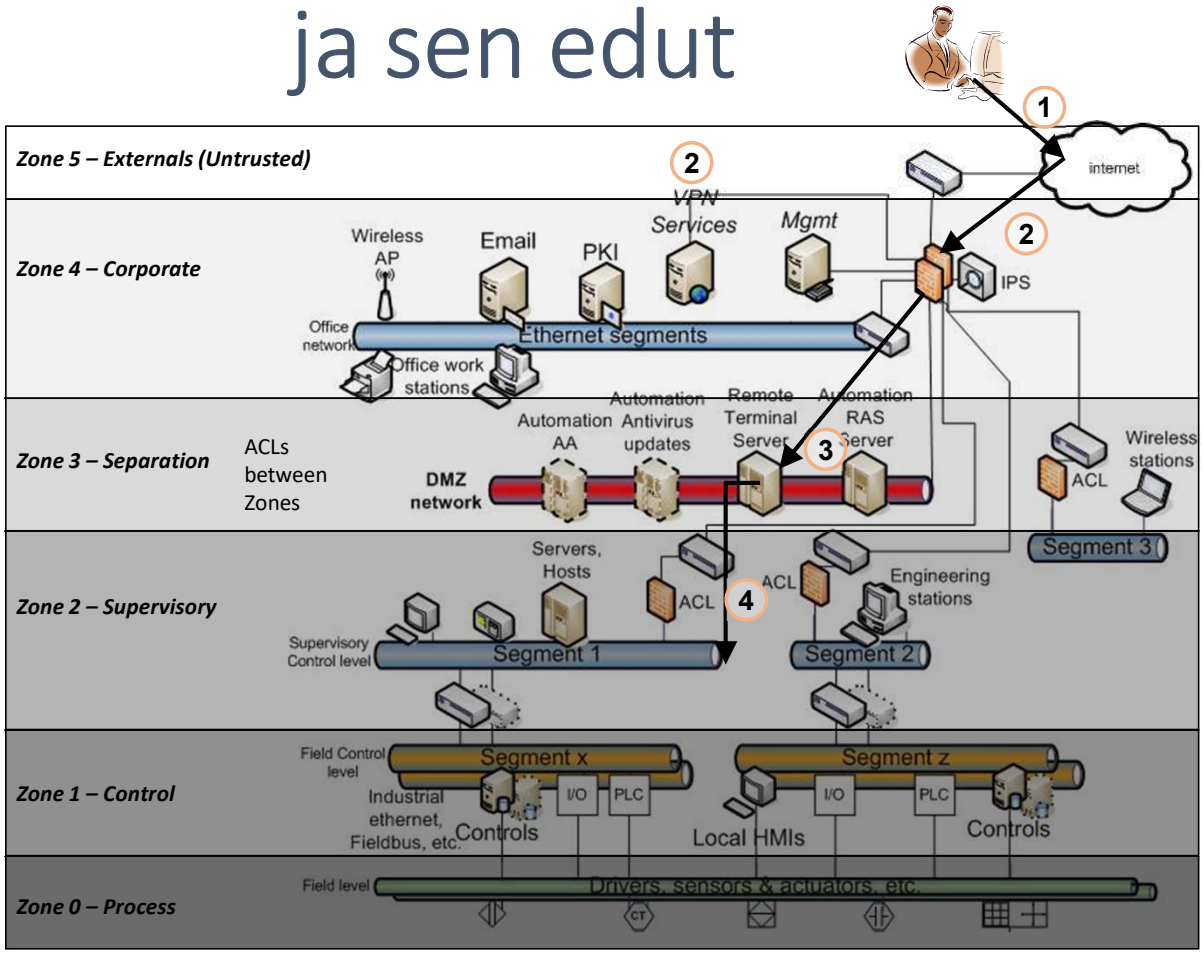
- ❑ Lyhyt oppimäärä
- ❑ Standardit
- ❑ **Etäyhteyshaasteet!**
- ❑ Moderni lähestymistapa

Etäyhteyshaasteista…

Automaation etäyhteydet ovat haasteellisia, kunkin haasteet riippuvat tarpeista, kyvyistä ja prioriteeteista!

Seuraavassa automaation etäyhteyksien lyhyt oppimäärä…

Ideaalimalli (2013) ja sen edut

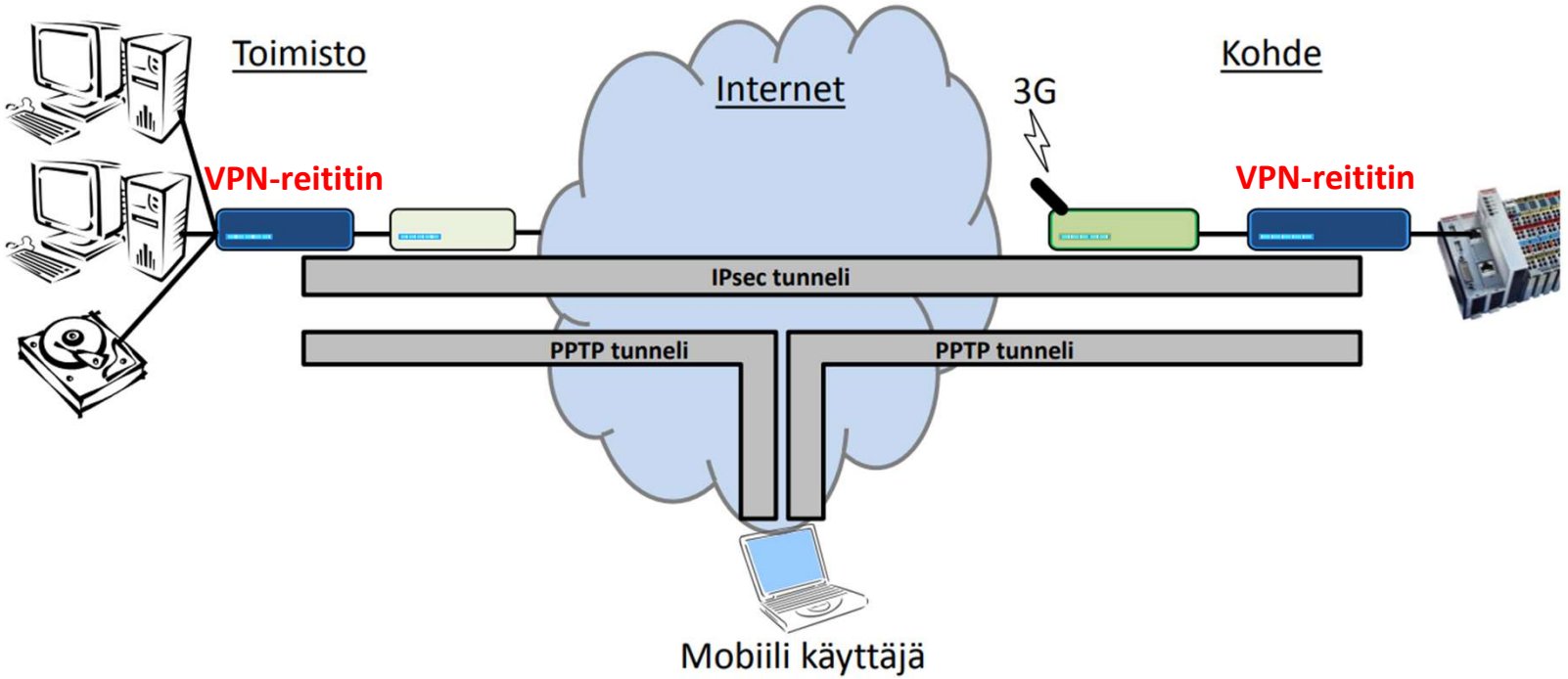


Lähde: Tietoturvan aktiiviset teollisuus-caset (COREQ-ACT), 2013

KRITEERI	+/-	Huom!
VPN YHTEYS	**+**	
Etä-PC ←→ Automaatiolaite (PLC)	+	DMZ kautta
Etä-PC ←→ Automaation DMZ palvelin	+	Kyllä
Etä-PC ←→ Automaation palomuuri	+	Mahdollinen
PALOMUURIT	**+**	
Palomuureja / ACL-kontrolleja eri tasoilla	+	Kaikki tasot
Palomuurin lokiseuranta	+	Kaikki tasot
Protokollien suodatus	+	Kaikki tasot
DMZ-ALUE	**+**	
Väliverkko / aliverkot / VLANit	+	Kaikki tasot
Ei suoria yhteyksiä	+	DMZ kautta
Välipalvelimet	+	Automaatio
Hallintorajoihin jako	+	Hyvä
POIKKEUSTILANTEET	**+**	
Vikasietoisuus	+	Eriytetty
Hyökkäyksen kestävyys	+	Eri tasoja
Ylläpito poikkeustilanteessa	+	Eriytetty
KORVAUS / KORJAUS	**+**	
Laitteen vaihtaminen	+	Eriytetty
Ohjelmiston palautus	+	Eriytetty
Konfiguraation hallinta/palautus	+	Eriytetty
SEURANTA / KEHITTÄMINEN	**+**	
Tiedonkeruu / seuranta	+	Eri tasoja
Testaaminen	+	Eriytetty
Harjoittelu	+	Eriytetty
Päivittäminen	+	Eriytetty

Etäyhteys automaatioon VPN-tunnelina?

Mitä ongelmia näet tässä ratkaisussa?



Kuva: Arttu Simula, Etäkäyttöyhteys automaatiojärjestelmään, Opinnäytetyö, Kesäkuu 2012, Tampereen ammattikorkeakoulu: https://www.theseus.fi/bitstream/handle/10024/45782/Simula_Arttu.pdf

ISA: Klassinen VPN-tunnelointi

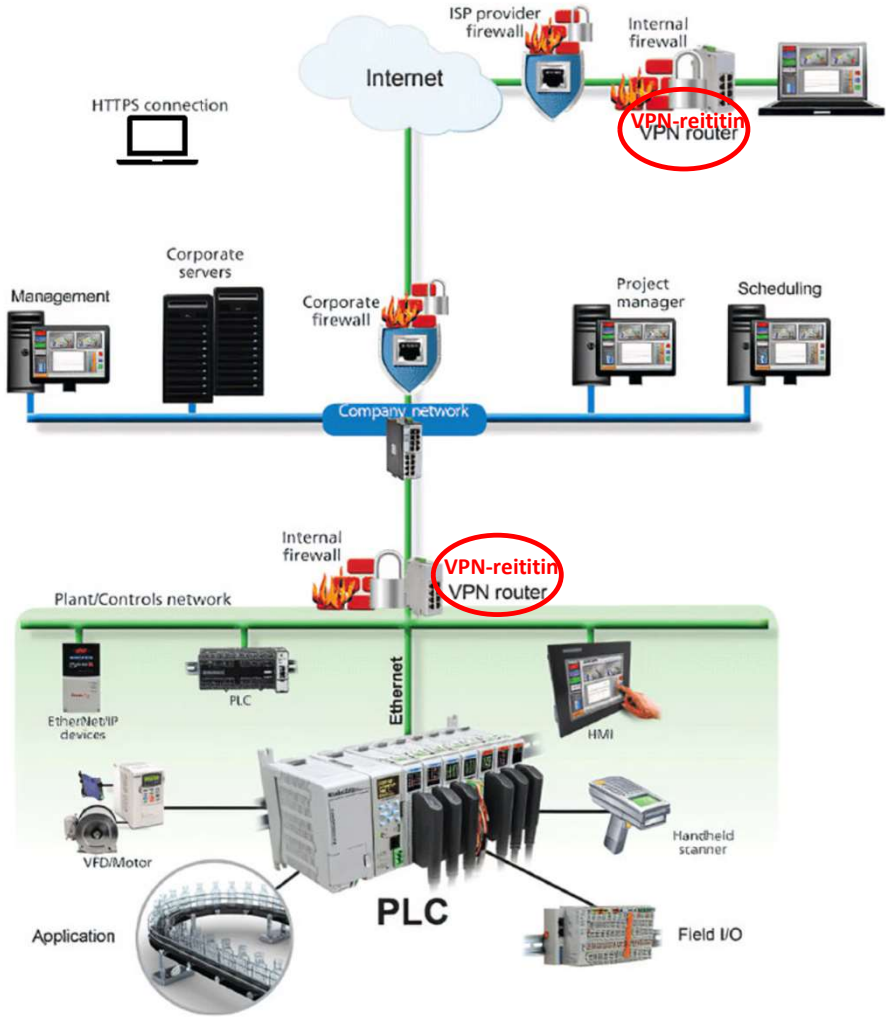
Mitä haasteita klassiseen VPN-ratkaisuun liittyy?

Klassinen VPN-tunneli:

- VPN-reititin tai VPN-ohjelmisto sisäverkkovyöhykkeiden rajalle.
- ➔IT-tuen tarve molemmissa päissä!

Kyetäänkö kaikki etäyhteystarpeet kattamaan “yhdellä” VPN-reititinkonfiguraatiolla?
Onko osaava IT-tuki käytettävissä VPN-ratkaisulle?
Ovatko kaikki tiimit valmiita käyttämään VPN-ratkaisua?

Jos vastaus yhteenkin kysymykseen on ei, niin klassinen tunneli ei oikein sovellu…



Kuva: ISA: How to Implement Secure, Remote Access to an Industrial Automation System
https://blog.isa.org/how-to-implement-secure-remote-access-industrial-automation-system

Entä jos ei ole IT-osaajia/IT-osastoa tukena?

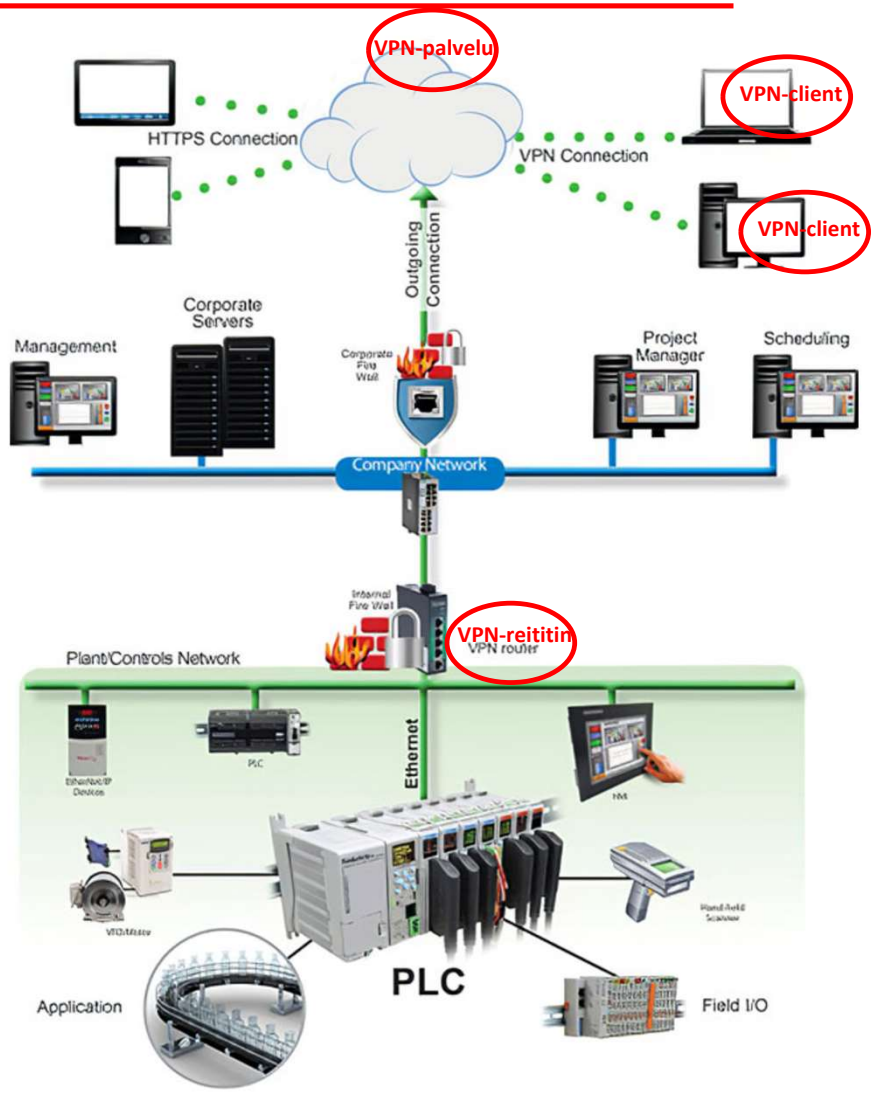
ISA: VPN-palvelu pilvessä = “Hosted VPN”

Mitä haasteita tähän ratkaisuun liittyy?

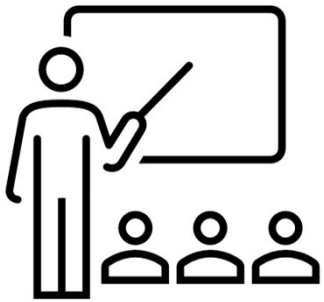
(syntyy riippuvuus pilvipalvelusta…)

”Hosted VPN”-palvelun käyttöönotto on yksinkertaista:

- VPN-reititin ottaa käynnistyessään turvallisen yhteyden VPN-palveluun.
- Käyttäjän ottaessa (VPN-clientilla tai HTTPS:llä) yhteyttä VPN-palveluun hänet tunnistetaan (vahvasti) ja turvallinen yhteys muodostetaan pilveen.
- Lopputuloksena syntyy turvallinen VPN-reititys käyttäjän koneen ja tehtaan VPN-reitittimen välille.



Kuva: ISA: How to Implement Secure, Remote Access to an Industrial Automation System
https://blog.isa.org/how-to-implement-secure-remote-access-industrial-automation-system



Kyberturvallisuus automaatiossa

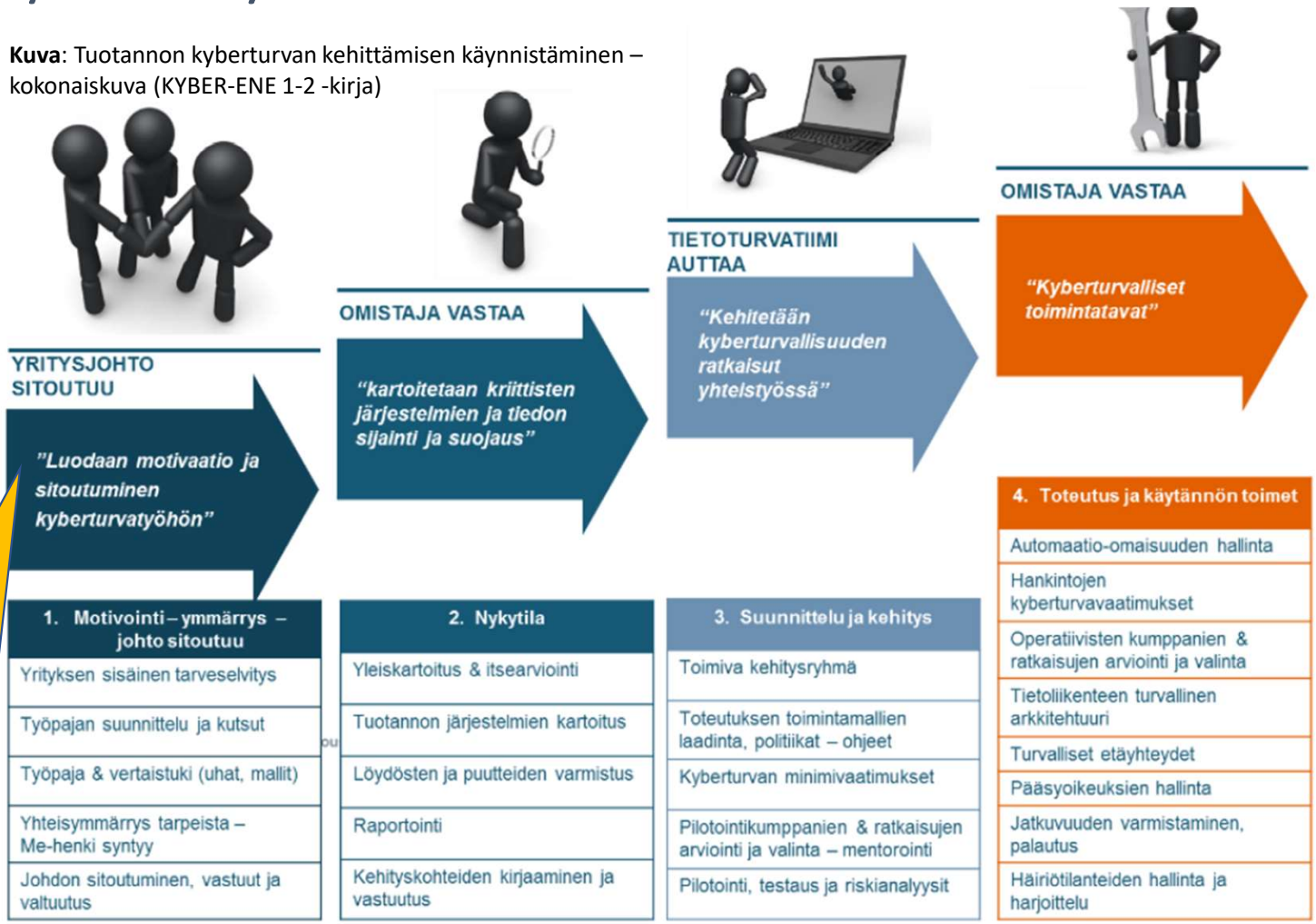
- ❑ Lyhyt oppimäärä
- ❑ Standardit
- ❑ Etäyhteyshaasteet
- ❑ **Moderni lähestymistapa!**

Energiayrityksen kyberturvallisuuden kehittäminen

Yritysjohto:

- Ottaa kyberturvallisuuden **omistajuuden** ja jakaa **vastuut!**
- Sitoutuu organisaation **kulttuurimuutos** prosessiin, lisää kyberturvallisuuden kehittämisen **strategisiin** tavoitteisiin ja nostaa asian **tapetille**!
- Antaa **mandaatin** ja kiinnittää organisaation huomion kyberturvallisuuden **kehittämiseen**!

Kuva: Tuotannon kyberturvan kehittämisen käynnistäminen – kokonaiskuva (KYBER-ENE 1-2 -kirja)



Nämä on kuvattu yksityiskohtaisesti "KYBER-ENE 1-2" kirjan luvussa 2: https://www.vttresearch.com/sites/default/files/pdf/technology/2019/T353.pdf

HARJOITTELE: Tyypillisimmät kyberharjoituksissa havaitut yleisluontoiset opit

Tilannekuvan jatkuva muodostaminen usein vaikeaa:

- ❑ **On vaikeaa saada muilta riittävästi faktoja tilannekuvan muodostamiseksi**
- ❑ **On vaikeaa ylläpitää tilannekuvaa, varsinkin jos tapahtumat etenevät nopeasti**
- ❑ **Tilannekuvan tallentamiseen ja jakamiseen ei osata kiinnittää riittävästi huomiota**

Viestinnän vaikeus tai suunnittelemattomuus:

- ❑ **Kaikki tarvittavat yhteystiedot eivät löydykään helposti**
- ❑ **Toimittajan avainhenkilö(t) ovat varattuja, varsinkin jos häiriö on laaja**
- ❑ **Lehdistölle annetaan koordinoimattomasti haastatteluja**
- ❑ **Asiantuntija vuotaa vahingossa luottamuksellista tietoa**

Nykyaikaisia oppeja tietoturvan parantamisen näkökulmasta

Laajentakaa riskienhallintaa:

- **Ottakaa KYBERRISKIEN analyysi osaksi liiketoimintariskien (jatkuvuuden) hallintaa!**
  - Kyberriskien säännöllinen analyysi mahdollisimman korkealla organisaatiossa, parhaimmillaan johtoryhmässä/hallitustasolla.
  - Säännöllinen riskianalyysi myös kehitystyönne moottorina.
  - Kokeilkaa erilaisia riskianalyysimenetelmiä → valitkaa parhaat menetelmät ja räätälöikää.

Lisätkää harjoittelua:

- **JUURISYYHARJOITUS: Tunnistakaa riskien juurisyyt** → ehditään ajoissa korjata!
- **TYÖPÖYTÄHARJOITUS: "Prosessien toimivuuden testaus"** → Kehittäkää ja testatkaa työpöytäharjoituksessa prosesseja, joilla riskejä voidaan vähentää!
- **TOIMINNALLINEN HARJOITTELU**: → Harjoitelkaa kyberhäiriöhallintaa, varautumista/ palauttamista tai ohjeiden toimivuutta säännöllisesti!

Yhteenveto

- **Koulutus:** Tietoisuuden lisäämistä!
- **Harjoittelu:** Konkretisoi ongelmakohdat!
- **Yrityskulttuuri:** Kokonaisvaltaista kehittämistä!

Muista ainakin seuraavat asiat:

- **UHAT:** Kriittisen infrastruktuurin kyberturvallisuusuhat ja vakavat seuraukset ovat lisääntymässä myös Suomessa!
- **AVUT:** Kannattaa hyödyntää Kyberturvallisuuskeskuksen referenssiaineistoja, ohjeita, soveltuvia kirjoja, sekä tietoturvapalveluiden tarjoajia!
- **HARJOITTELU:** Lisää kyberharjoittelua käytännön osaamisen ja yhteistoiminnan kehittämiseksi!
- **JATKUVA KEHITYS:** Ota kyberriskit haltuun systemaattisella uhkien kartoittamisella ja jatkuvalla kehittämisellä!


Kiitokset mielenkiinnosta
Kysymykset
ja keskustelu!
Kyberhallinta Pasi Ahonen Oy
pasi.ahonen@kyberhallinta.fi
www.kyberhallinta.fi