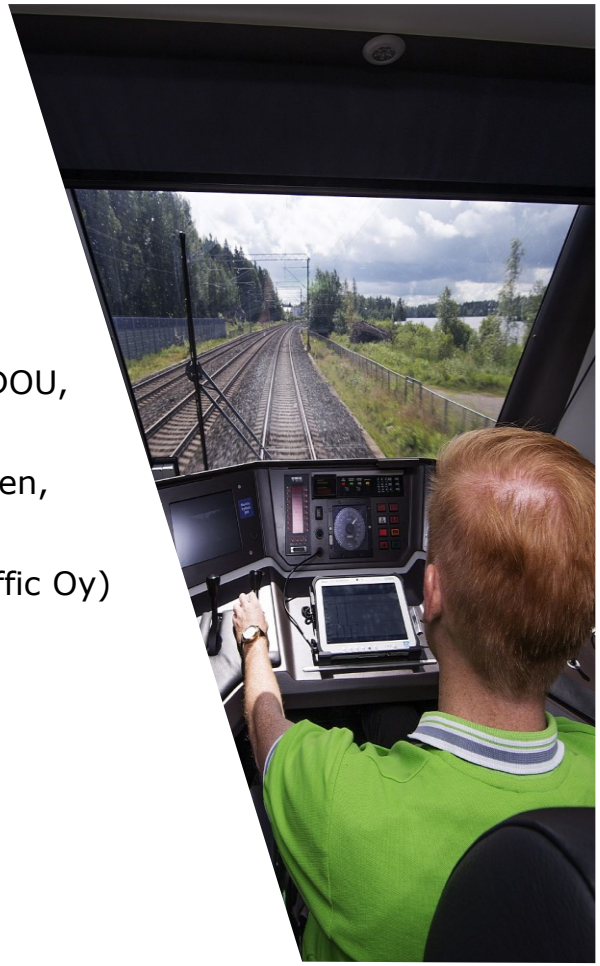
Raideliikenteen kyberturvallisuuden työpajan ohjelma 4.6.2021



- 12.00 Traficomin tervehdys ja käytännönasiat (Ville Lahti, Traficom)
- 12.15 Cybersecurity incidents in railway sector (Dr Marianthi THEOCHARIDOU, European Union Agency for Cybersecurity, ENISA)
- 12.40 Väyläviraston raideliikenteen kyberturvallisuusohjelma (Paul Kinnunen, Väylävirasto)
- 13.15 Maailma on muuttunut, uhkakuvat myös (Anne Hännikäinen, Fintraffic Oy)
- 13.50 Tauko ja vapaata keskustelua
- 14.00 Digiradan kyberturvallisuus (Janne Huhtakallio, Fintraffic Oy)
- 14.35 Kyberturvallisuuskeskuksen kybermittari - Kuinka ilmailusektorin kokemuksia voidaan hyödyntää raiteilla (Tomi Salmenpää, Traficom)
- 15.10 Kyberturvallisuuden merkitys logistiikan huoltovarmuudessa (Jarna Hartikainen, Huoltovarmuuskeskus)
- 15.40 Vapaata keskustelua ja tilaisuuden päättäminen

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY INCIDENTS IN RAILWAY SECTOR

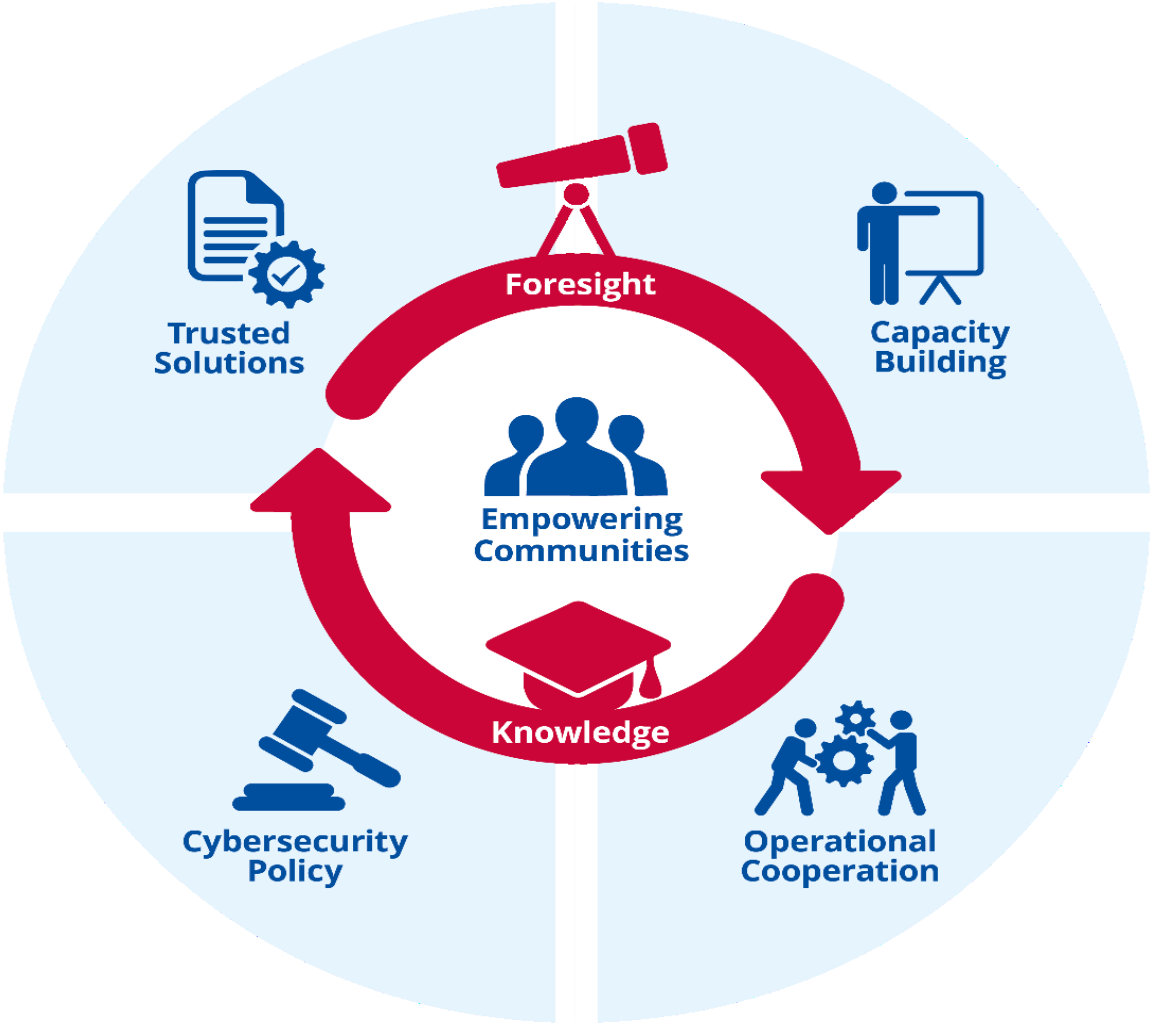
Marianthi Theocharidou, Zoran Stanic
Policy Development and Implementation Unit
Marianthi.Theocharidou@enisa.europa.eu

04 | 06 | 2021

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

A TRUSTED AND CYBER SECURE EUROPE

Our mission is to achieve **a high common level of cybersecurity** across the Union in cooperation with the wider community



ENISA ACTIVITIES ON RAILWAY SECTOR

Support Infrastructure Managers, Railway Undertakings, Competent authorities

- Implementation of the **NIS Directive**
- Partner of the **European Railway ISAC**

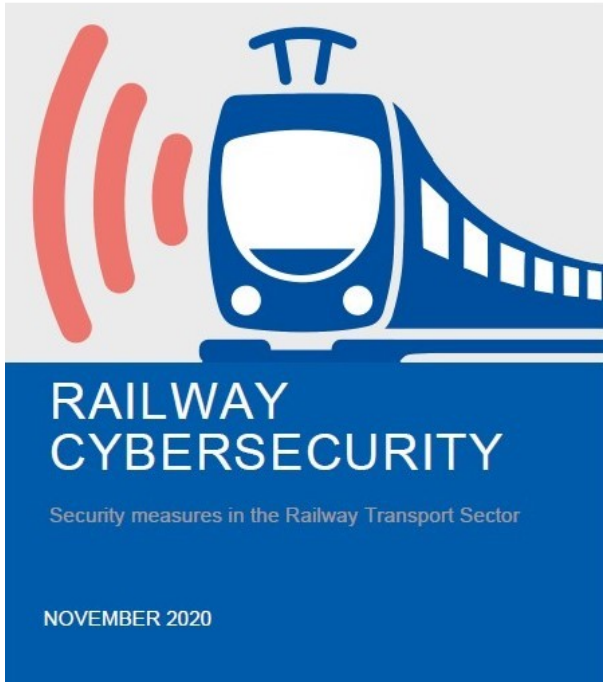
Support standardisation and certification

- Participation in **CEN CENELEC /TC9X/WG26**
- TS **50701 on Railway applications - Cybersecurity**

Collaborate closely with ERA

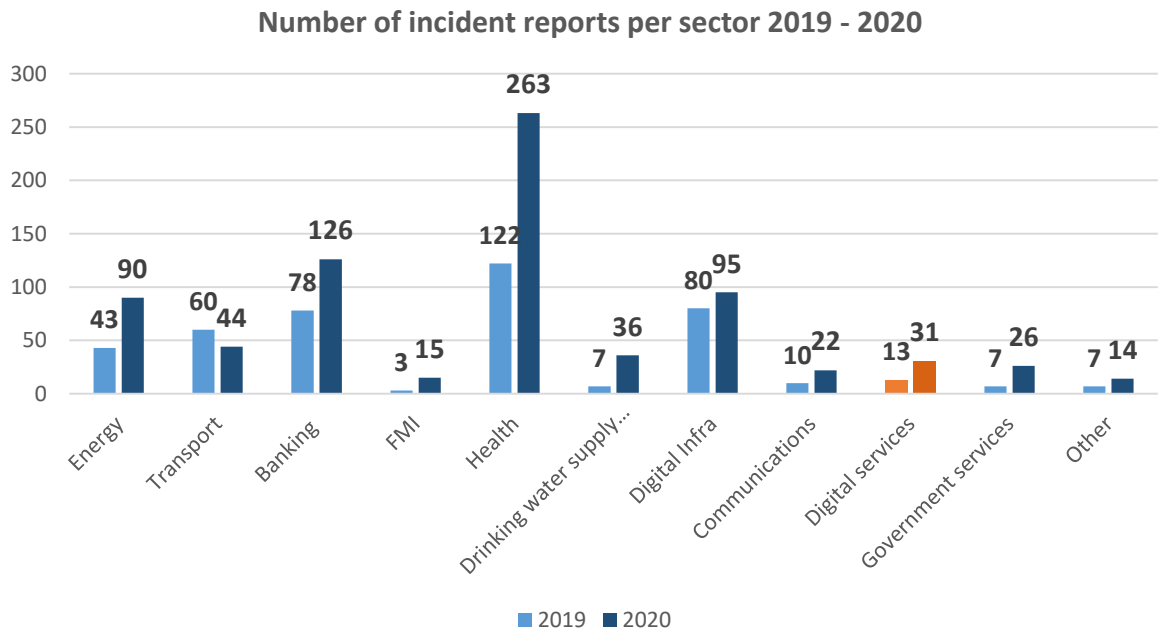
- Cybersecurity for **ERTMS**
- **ENISA ERA conference 2021**

https://www.enisa.europa.eu/events/ENISA-ERA_Conference/



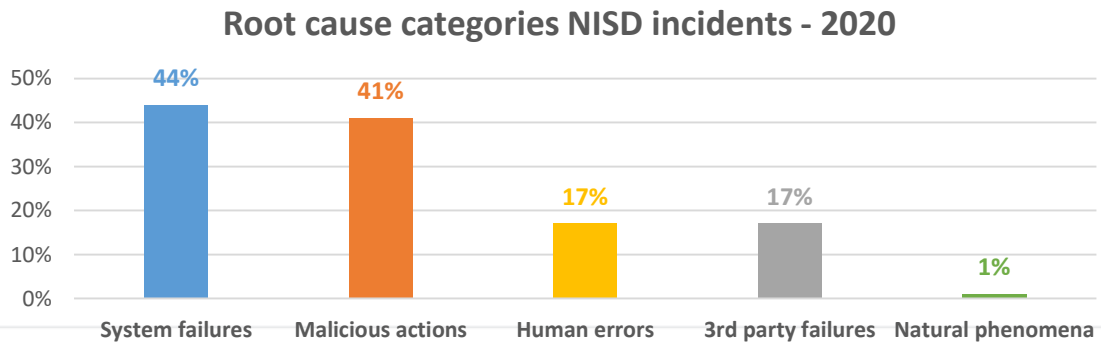
2020 Report on Railway cybersecurity "Security measures in the Railway Transport Sector"

RESULTS OF INCIDENT REPORTING UNDER NIS DIRECTIVE



Very limited railway incidents during 2020.

Railway works caused disruptions to telecom operations in two occasions.



Most common detailed causes: software bugs (53%), malware (51%), DDoS (50%), and faulty software changes/updates (45%).

RECENT INCIDENTS

Period	Country	Incident Summary	Effect
Apr-May 2021	UK	Merseyrail Rail Network: **Ransomware, data theft**	- Staff email hacked, used to sent emails by the director to newspapers and employees - Employee's personal information leaked as proof
Jan 2021	USA	OmniTRAX (Freight company): **Ransomware, data theft**	- Internal OmniTRAX documents leaked - **First attack targeting Freight in the US**
Oct 2020	CA	Montreal's STM public transport system: **Ransomware**	- IT systems, website, and customer support affected
Jul 2020	ES	Spanish state railway company ADIF: **Ransomware**	- Ransom asked, threat of data leak of internal adif documents - Attackers posted data as proof
May 2020	CH	Stadler IT systems: **Malware (possibly ransomware)**	- Ransom asked, threat of data leak - IT systems affected
Feb-Mar 2020	UK	Network Rail and service provider C3UK: **Data breach**	- Email addresses and travel data of customers who used Wi-fi in stations exposed

Information based on press items.

RECENT INCIDENTS

Period	Country	Incident Summary	Effect
Jan 2020	JPN	Mitsubishi Electric Corporation: cyberattack	- Customer Data compromised (projects with Railway Operators) - **Manufacturer**
Jan 2019	CHN	Official online booking platform of the China Railways (CR): **Data breach**	- **Personal data theft** (names, IDs, passwords of 5M customers
May 2088	DK	Danske Statsbaner (DSB): **DDoS** attack	- **Train operations halted** - Blockage of tickets service - Phone and email services
Apr 2018	GB	Great Western Railway (GWR): **Data breach**	- Passenger data and passwords exposed
Nov 2017 - Feb 2018	US	Rail Europe North America (RENA): a 3-month long **data breach**	- Personal data exposed
May 2017	DE	Deutschbahn: **Ransomware** (**Wannacry)** attack	- Passenger information screens affected

Information based on press items.

OBSERVATIONS- PATTERNS

- Not many service disruptions
  - IT systems causing panic or crowding?
- **What about safety?**
  - Not yet, but it remains a concern
  - OT systems vulnerabilities
  - Digitization of modern trains

IT systems are targeted

- Increasing rate
- Ransom as a Service (RaaS)
- Combined with operation disruptions, extortion (double, triple), data theft, and illegal publication

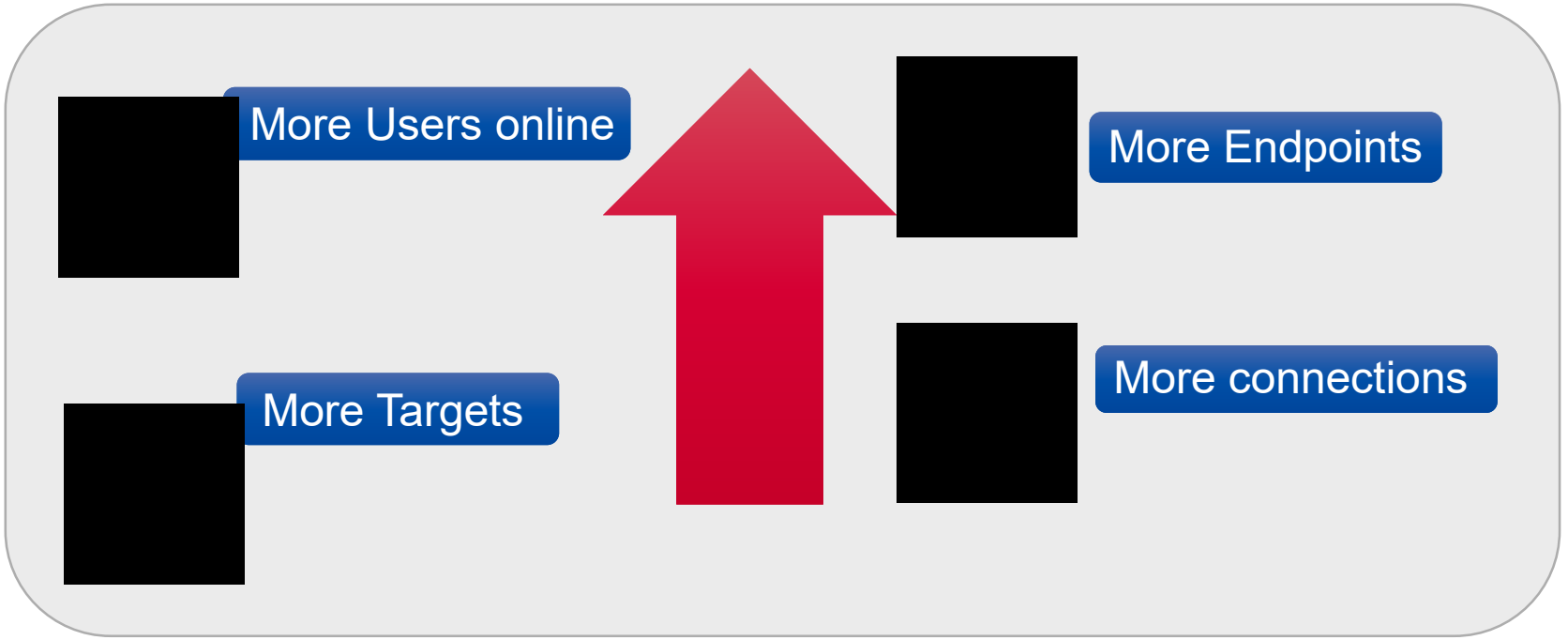
Ransomware

- Software integrity compromise, compromise of aggregated information
- Fewer incidents related to hardware
- Data exfiltration, espionage, hacktivism
- Leverage of last number of clients or target specific ones

Supply Chain attacks

THE THREAT LANDSCAPE DURING THE LAST YEAR

- Attack surface in cybersecurity continues to expand as we are entering a new phase of digital transformation.
- A new social and economic norm caused by COVID-19 pandemic even more dependent on a secure and reliable cyberspace.
- Home is the new perimeter.



SOME FINAL THOUGHTS

- **Actors**
- Ransomware groups (financial gain)
  - In Europe, given the Pandemic, the transport sector is under economic pressure.
- Nation-state threat actors (IP and R&D theft, cyberespionage)
  - Proprietary technology and research developments could be of interest
- **Primary focus appears to not be on railway until now (e.g. aviation).**
- Individual sectors need to be assessed further.

ENISA ACTIVITIES 2021

- Good practises for cyber risk management on the railway sector (Q4 2021)
- ENISA annual threat landscape report (Q4 2021)
- ENISA Supply chain threat landscape (Q3 2021)

ENISA TRANSSEC Expert Group

https://resilience.enisa.europa.eu/transport-security

https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/railway
https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu

Raideliikenteen kyberturvallisuuden työpaja

Rataverkon kyberturvallisuusohjelma

Paul Kinnunen

3.6.2021

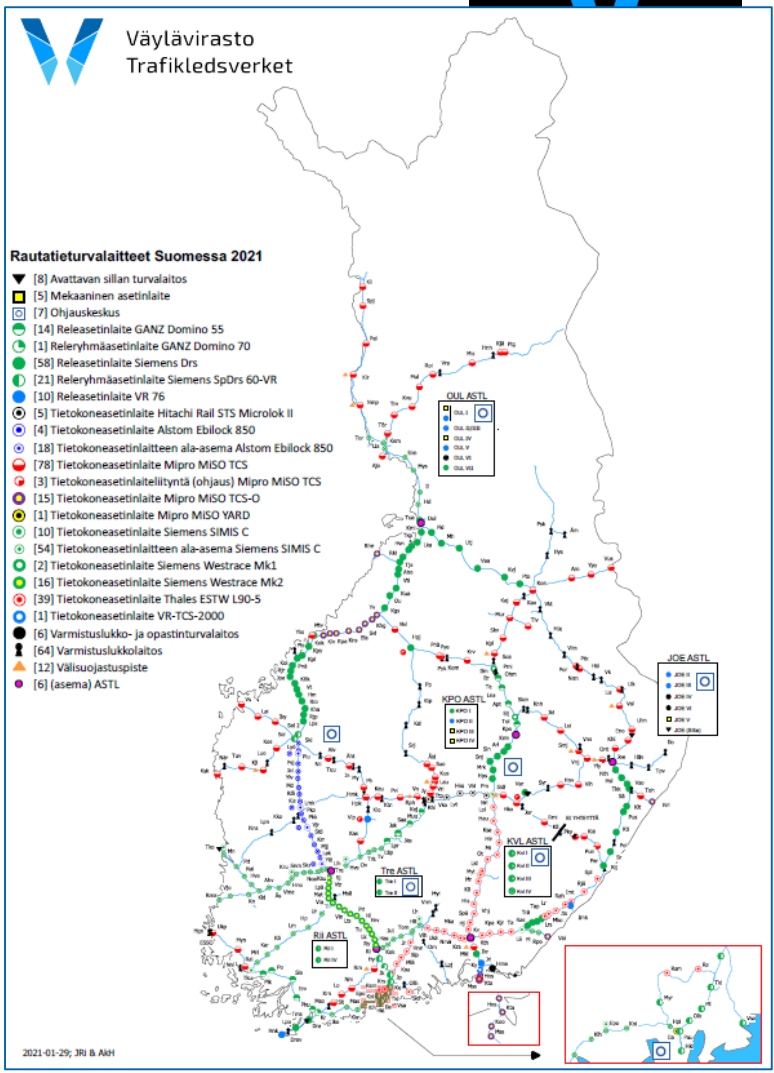
Sisällys

- Hankkeen taustaa
- Tavoitteet
- Hyödyt
- Sidosryhmät
- Rajaukset
- Hankkeen toimenpidekokonaisuudet ja ylätason aikataulu

Hankkeen taustaa

Johdanto

- Tämän hetken palvelutaso rataverkon turvalaitteiden osalta on kohtuullinen. Turvalaitekokonaisuus koostuu useista eri laitteista ja eri aikakausien teknologioista. Vanhimmat käytössä olevat turvalaitejärjestelmät on otettu käyttöön 1960-luvulla ja uusimmat 2020-luvulla.
- Kyberturvallisuuden näkökulmasta turvalaitteiden lisäksi keskeisiä ovat mm. liikenteenhallintajärjestelmät, sähkönsyöttöjärjestelmät ja kaluston valvontalaitteet
- Suomen rataverkolla on useita eri toimijoita, kotimaisia ja kansainvälisiä. Rataverkon turvalaitteiden toimijakenttä muodostuu pääosin seuraavasti:
  - tilaajatoiminnot korvausinvestoinneille (Väylävirasto)
  - rakennuttajakonsultit (palveluntuottajat)
  - laitetoimittajat / korvausinvestointien järjestelmätoimitukset
  - turvalaiteurakoitsijat / projektien turvalaiterakentaminen
  - kunnossapidon tilaajatoiminto (Väylävirasto)
  - alueelliset kunnossapidon valvojat (konsultit)
  - alueelliset kunnossapitourakoitsijat (palveluntuottajat)



Kyberturvallisuusohjelma
Hankkeen taustaa ja tavoitteet

- Väyläviraston vuoden 2021 toiminnan yhdeksi painopisteeksi on nostettu kyberturvallisuuden parantaminen. Työ toteutetaan hankkeen muodossa.
- Hankkeen nimi on **Rataverkon kyberturvallisuusohjelma**
- Hanke ajoittuu vuosille 2021 - 2023 ja sen tavoitteena on tehdä tarvittavat parannustoimenpiteet hallinnollisen, fyysisen ja tietoteknisen turvallisuuden parantamiseksi sekä koko rataverkon turvallisuuden kehittämiseksi
- Hankeen lähtötiedoiksi hankkeen alussa on tuotettu seuraavat turvallisuusarvioinnit ja -selvitykset:
  - Hyvinkää – Karjaa yhteysvälin tietoturva-auditointi
    - Riskianalyysi Hyvinkää - Karjaa välin arvioinnissa havaituille poikkeamille
  - Riihimäki – Tampere yhteysvälin tietoturva-auditointi
  - Kehäradan tietoturva-auditointi
  - Väyläviraston kyberturvallisuuden kypsyysarviointi (CMA)

Hankkeen riippuvuudet muuhun tekemiseen

- Hankkeen alussa toteutettiin esiselvitys päällekkäisten tavoitteiden tunnistamiseksi. Hankkeelle päällekkäisiä tavoitteita tiedetään olevan ainakin
  - Traficomin raideliikennettä kyberturvallisuutta koskevassa suosituksessa
  - Liikenne12-suunnitelmassa
  - Kansallisessa rautatieliikenteen digitalisoimiseen tähtäävässä Digirata-hankkeessa.
- Kyberturvallisuusohjelman rinnalla Väylävirastolla on käynnistetty myös muita turvallisuuden parantamiseen liittyviä projekteja, kuten avaintenhallintaprojekti, jossa uusitaan laitetilojen lukitukset.

Kyberturvallisuusohjelma
Hankkeen taustaa ja tavoitteet

Hankkeen taustalla olevien arviointien perusteella on tunnistettu ainakin seuraavat kehityskohteet:

- Väyläviraston turvalaiteinfrastruktuurin ja niihin liittyvien tietojärjestelmien operatiivisen toiminnan **valvonta, monitorointi sekä muutostilanteiden hallinta** tulee olla yhtenäisempää, laadukkaampaa ja johdetumpaa.
- Erilaisten **kontrollipisteiden tulee olla paremmin tunnistettu** ja asioiden sekä **kokonaisuuksien luokitteluun** tulee kiinnittää enemmän huomiota. Näin toimien Väylävirasto pystyy hallinnoimaan, valvomaan ja puuttumaan ennakoivasti mahdollisiin palvelutuotannon ja operatiivisen toiminnan epäkohtiin sekä huolehtimaan kokonaisuuden laadukkaasta johtamisesta.
- Parannustoimet ja kehittämiskohteet tulee **tunnistaa riskipohjaisesti priorisoimalla** ja **kohdistamalla riittävä panostus** tunnistettuihin toiminnan kriittisiin ja merkityksellisiin kohtiin.
- Eri **toimittajien ja kumppanien hallintaa tiivistämällä** pystytään jatkossa paremmin ylläpitämään riittävä taso palveluiden, järjestelmien ja komponenttien tieto- ja teknisen turvallisuuden osalta.

Hankkeen tavoitteet

Rataverkon kyberturvallisuusohjelma

Hankkeen tavoitteena on varmistaa rataverkon kybertoimintaympäristön luotettavuus.

Väyläviraston rautatieinfrastruktuurin ja niihin liittyvien tietojärjestelmien operatiivisen kybertoimintaympäristön valvonnan ja monitoroinnin sekä muutostilanteiden hallinnan tulee olla yhtenäisempää, laadukkaampaa ja johdetumpaa.

Hankkeessa toteutetaan hallinnollisia, fyysisiä ja teknisiä toimenpiteitä rataverkon digitaalisen turvallisuuden parantamiseksi. Parannustoimenpiteet ja kehityskohteet tunnistetaan ja toteutetaan riskiperusteisesti.

Hyödyt

Rataverkon kyberturvallisuusohjelma

Hankkeella tavoiteltuja hyötyjä ovat

- Raideliikenteen kyberturvallisuuden jatkuvuuden ja sietokyvyn (resilienssi) kasvattaminen
- Prosessien vakiinnuttaminen
  - Turvalaitetilojen vakaus ja suojaaminen
  - Häiriöiden vaikutuksen minimoiminen
  - Rataverkon valvonnan käytäntöjen kattavuus ja yhdenmukaisuus
  - Havainnointi- ja reagointikyvyn varmistaminen
  - Käytäntöjen vaatimustenmukaisuuden varmistaminen
- Varmistetaan nykyisen turvallisuustilanteen säilyminen sekä rataverkon palvelutason ylläpitäminen mm. minimoimalla viivästymiset.

Sidosryhmät

Rataverkon kyberturvallisuusohjelma

Hankkeen keskeiset ulkoiset sidosryhmät:

- Liikenne- ja viestintäministeriö
- Traficom (Liikenne- ja viestintävirasto)
- Fintraffic Raide Oy (Liikenteenohjausyhtiö)
- Palveluntuottajat ja konsultit
  - Rakennuttajakonsultit/palveluntuottajat
  - Laitetoimittajat (korvausinvestointien järjestelmätoimitukset)
  - Turvalaiteurakoitsijat (projektien turvalaiterakentaminen)
  - Alueelliset kunnossapidon valvojat (konsultit)
  - Alueelliset kunnossapitourakoitsijat (palveluntuottajat)

Hankkeen keskeiset sisäiset sidosryhmät:

- Tilaajatoiminnot korvausinvestoinneille (Väylävirasto)
- Kunnossapidon tilaajatoiminto (Väylävirasto)

Hankkeen rajaukset

Rataverkon kyberturvallisuusohjelma

Hankkeen kohteena on

- Väyläviraston hallinnassa oleva valtion rataverkko ja sen liikenteenohjauspalvelu

Hankkeessa ei käsitellä

- Yksityisraiteiden haltijoita
- Rautatieliikenteen harjoittajia

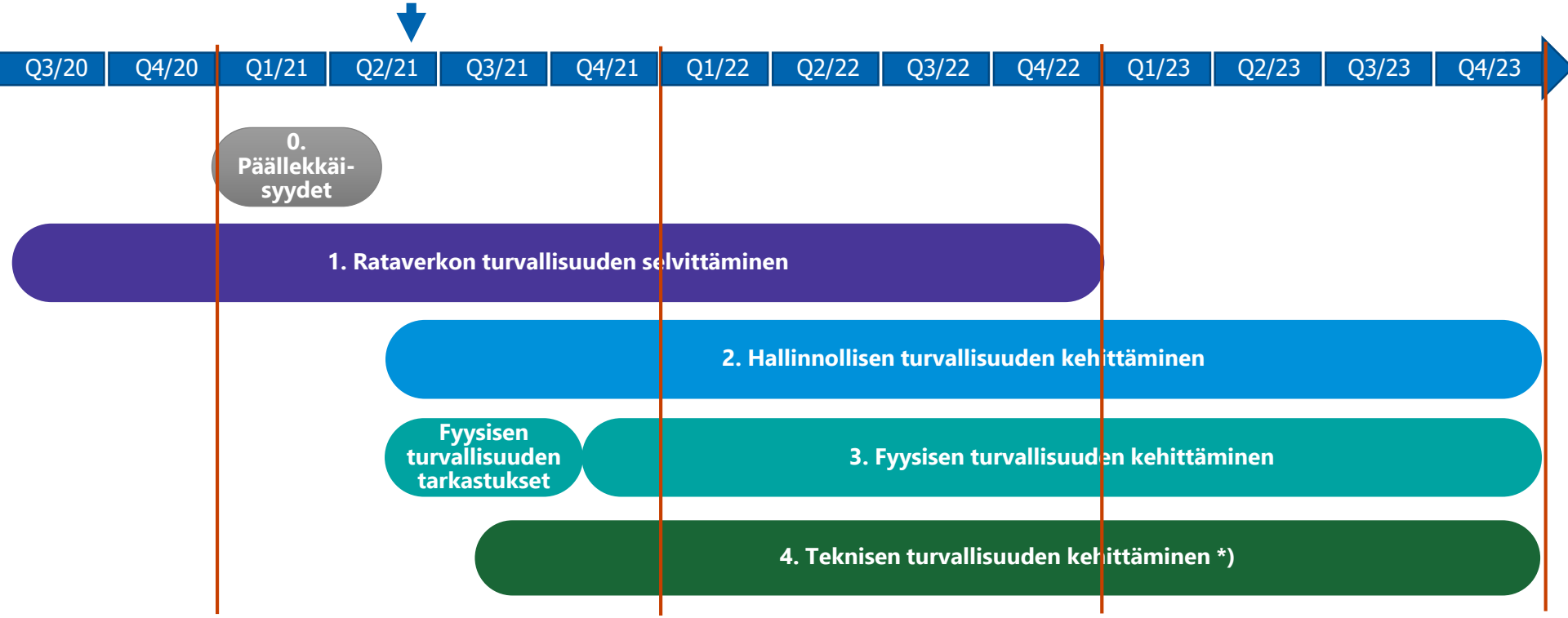
Hankkeen toimenpidekokonaisuudet ja ylätason aikataulu

Hankkeen toimenpidekokonaisuudet

Toimenpiteiden suunnittelussa on huomioitu tietoturvan hallintaan kohdistuvat yleiset vaatimukset, Digirata-selvityksen loppuraportti, Traficomin suositus kyberturvallisuuden edistämisestä raideliikenteessä sekä Valtakunnallisen liikennejärjestelmäsuunnitelman luonnos

0. Esiselvitys - Päällekkäisten tavoitteiden tunnistaminen	• Tunnistetaan päällekkäisyydet Liikenne12-suunnitelman ja Digirata-hankkeen kanssa
1. Rataverkon turvallisuuden selvittäminen	• Toteutetaan rataverkon turvallisuuden selvittäminen
2. Hallinnollisen turvallisuuden kehittäminen	• Määritellään ja selkeytetään digitaalisen turvallisuuden periaatteet Väyläviraston toiminnassa kiinteäksi osaksi johtamisjärjestelmää ja sen hallintamenettelyitä • Varmistetaan kumppaneiden ja palveluntuottajien digitaalisen turvallisuuden systemaattinen hallinta – määritellään ja luodaan menettelyt kiinteäksi osaksi Väyläviraston toimintaa • Kehitetään tiedon luokittelua siten, että oleellisen tiedon suojaaminen varmistetaan entistä paremmin
3. Fyysisen turvallisuuden kehittäminen	• Laitetilojen avaintenhallinta- ja lukitusprojektin (kulunvalvonta) parannustoimenpiteet 2021 – 2023 (alustava) sekä muut rataverkon laitetilojen fyysistä turvallisuutta parantavat toimenpiteet
4. Teknisen turvallisuuden kehittäminen	• Useita teknistä turvallisuutta parantavia toimenpiteitä. Rataverkon teknisen turvallisuuden kehittäminen voi alkaa, kun tietoturva-arviot on tehty riskienhallintatyöjoissa Kehäradan ja Riihimäki-Tampereen osalta ovat valmistuneet ja tuloksia on verrattu aiemmin toteutetun Hyvinkää-Karjaa-välin tietoturva-arvioinnin tuloksiin.

Kyberturvallisuusohjelma
Hankekokonaisuuden aikataulusuunnitelma



*Rataverkon teknisen turvallisuuden kehittäminen voi alkaa, kun tietoturva-arviot riskityöpajojen kautta Kehäradan ja Hyvinkää-Karjaan rataosuuksilta ovat valmistuneet ja tuloksia on verrattu aiemmin toteutetun Hyvinkää-Karjaa-välin tietoturva-arvioinnin tuloksiin

Väylävirasto
Trafikledsverket

Maailma on muuttunut – uhkakuvat myös

Anne Hännikäinen

31.05.2021

Background

Anne Hännikäinen

Security Manager, Nokia

IT Production Manager, Nokia

NOKIA

1999-2013

Information Security Consultant in Nixu, cybersecurity services company.

nixu

2013-2015

CISO in Sanoma, media and learning company.

Service Line Manager, Infrastructure security

sanoma

2015-2019

CISO in Fintraffic, controls and manages traffic on land, air and sea

Fintraffic

2020

Singapore ~2 years

The Netherlands ~1/2 year

Disclaimer: **Opinions** expressed are solely **my own** and do not express **the views** or **opinions** of **my** existing or previous employers.

…the world has changed and continues to change…

‘Cybercrime is worth of billion euros business’

...you are not the only one who is digitalizing, automating and innovating...

Photo by fotografierende on Unsplash; Photo by Abhishek Koli on Unsplash

Cyberattacks can cause more damage than a single warship

MAERSK

HYDRO

COLONIAL PIPELINE CO.

Pixabay.com

Kaikkosen mukaan Suomi ei tunnu oppivan menneistä tapahtumista: ”Miten voimme yllättyä Vastaamon tietomurrosta tai eduskuntaan kohdistetusta kybervakoilusta?”

https://fi.wikipedia.org/wiki/Antti_Kaikkonen

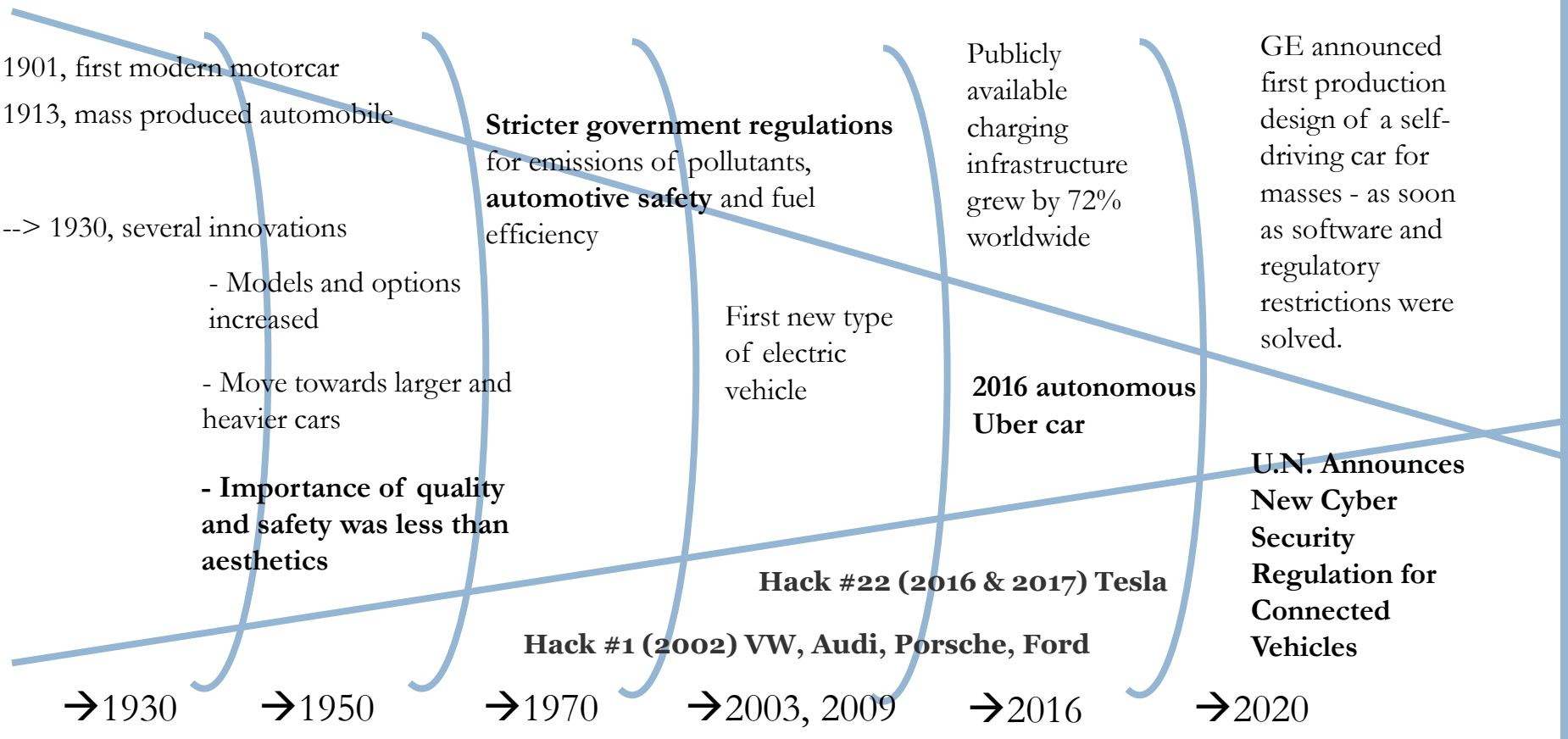
Kaikkonen kertoo ihmettelevänsä sitä, miten vuosi toisensa jälkeen yllätymme siitä, että meille pahaa tahtovat sekä valtiolliset että ei-valtiolliset toimijat onnistuvat vaarantamaan Suomen turvallisuutta tavalla, josta on puhuttu jo vuosia, ellei vuosikymmeniä.

> – Jos jo 20 vuotta sitten olemme todenneet tietoverkkojen kautta leviävien informaatiouhkien lisääntyvän globaalisti, ja jos samaan aikaan totesimme haitallisen kybervaikuttamisen olevan päivittäistä, normaalioloissa tapahtuvaa toimintaa, miten voimme yllättyä Vastaamon tietomurrosta tai eduskuntaan kohdistetusta kybervakoilusta?

Tietoturva ei tapahdu vahingossa eikä pyytämättä.

https://www.anttikaikkonen.fi/category/puheita_ja_kirjoituksia/

History - Automotive



https://en.wikipedia.org/wiki/History_of_the_automobile; https://innovationatwork.ieee.org/un-announces-new-cyber-security-regulation-for-connected-vehicles/

Samples of automotive hacks

'The new Cyber Security Regulation for Connected Vehicles will have major impact how cars will be designed in future.'

- **Hack #1 (2002) VW, Audi, Porsche, Ford:** The hackers were being hired by aftermarket consumers to reprogram powertrain calibrations for more aggressive performance.
- **Hack #5 (2010) General Motors:** a vulnerability where a criminal could have complete control of the car except the steering. They knew about this vulnerability almost 5 years.
- **Hack #14 (2015) Chrysler:** Researchers were able to fully kill the engine and disable the jeep's breaks. Lead to 1,4 million product recall.
- **Hack #17 (2015) VW, Honda, Audi, Hyundai, Kia, Porsche & Volvo:** Millions upon millions of vehicles are vulnerable to theft by a thief recording and reusing the keyfob's communication.
- **Hack #22 (2016 & 2017) Tesla:** Researchers in China demonstrated how they could remotely turn on the windshield wipers, open the trunk and apply the brakes in brand-new Model S sedans. An over-the-air software update was delivered 10 days after Tesla was notified.

Being compliant is not enough in cybersecurity.

https://www.forbes.com/sites/stevetengler/2020/06/30/top-25-auto-cybersecurity-hacks-too-many-glass-houses-to-be-throwing-stones/?sh=7e99e247f65d

…what challenges we face…

Roles and responsibilities

Assumptions

Competent resources

DevOps

Co-operation

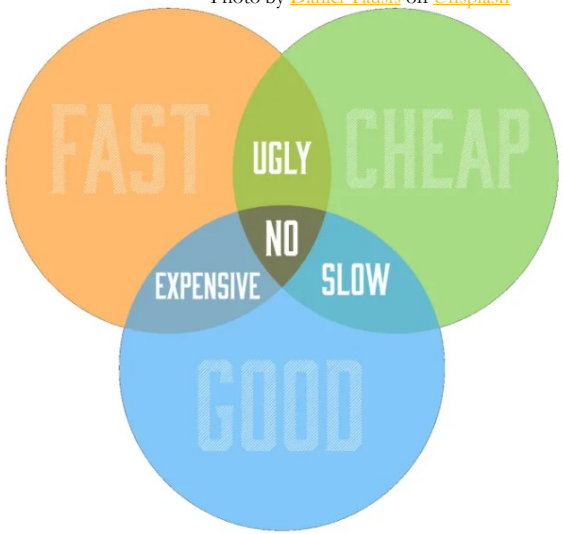
Sec

OT environments

- from closed environment to cloud-

..when you don't know that you don't know..

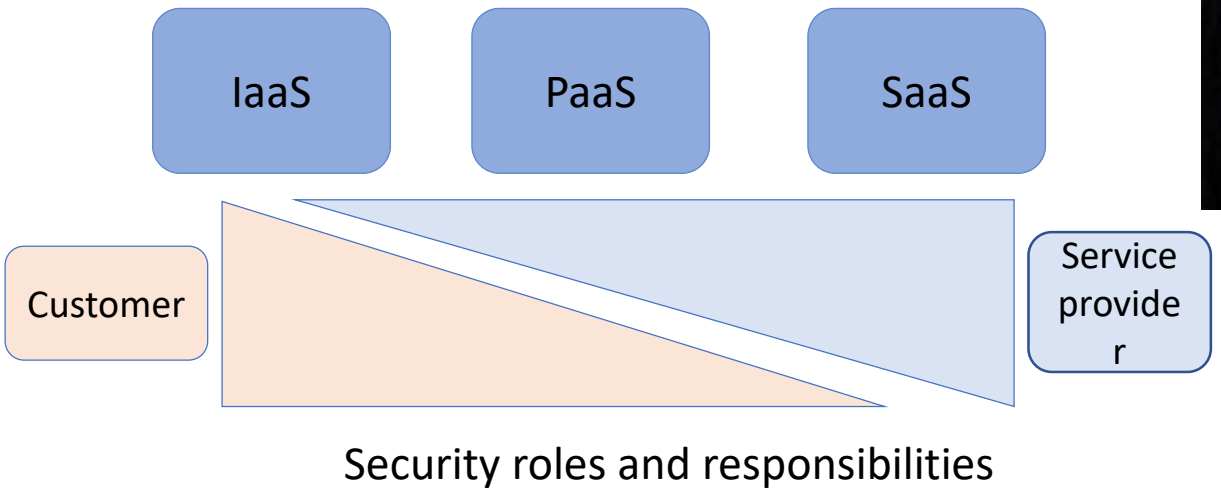
Photo by Daniel Tausis on Unsplash



https://www.blog.greenprojectmanagement.org/index.php/2015/11/01/flaws-with-the-iron-triangle/

Security roles & responsibilities

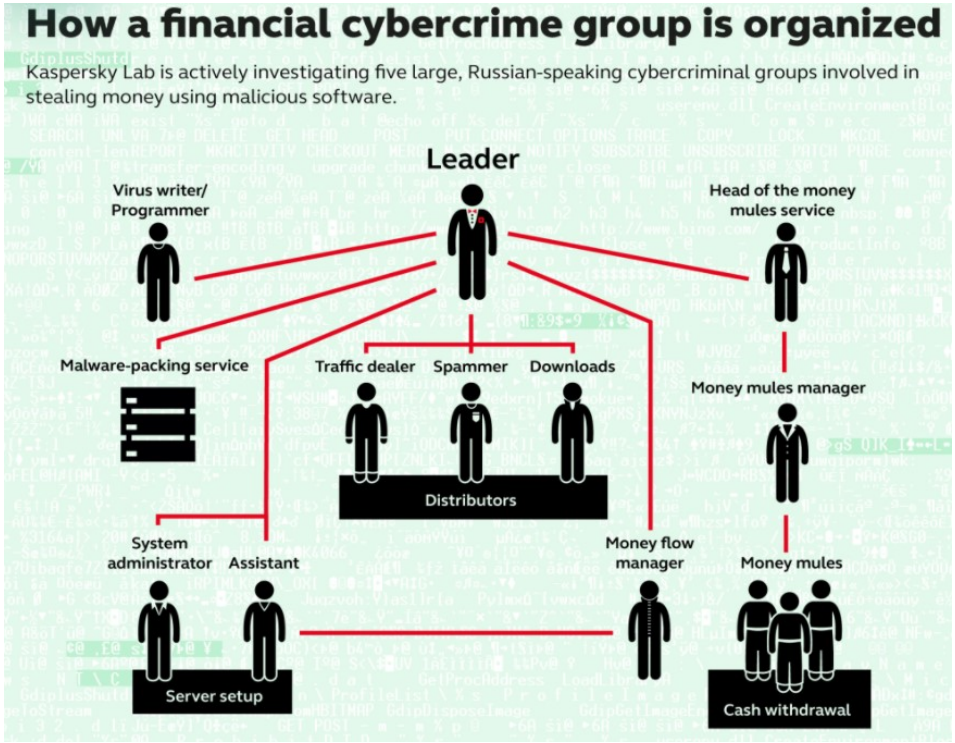
Pixabay.com



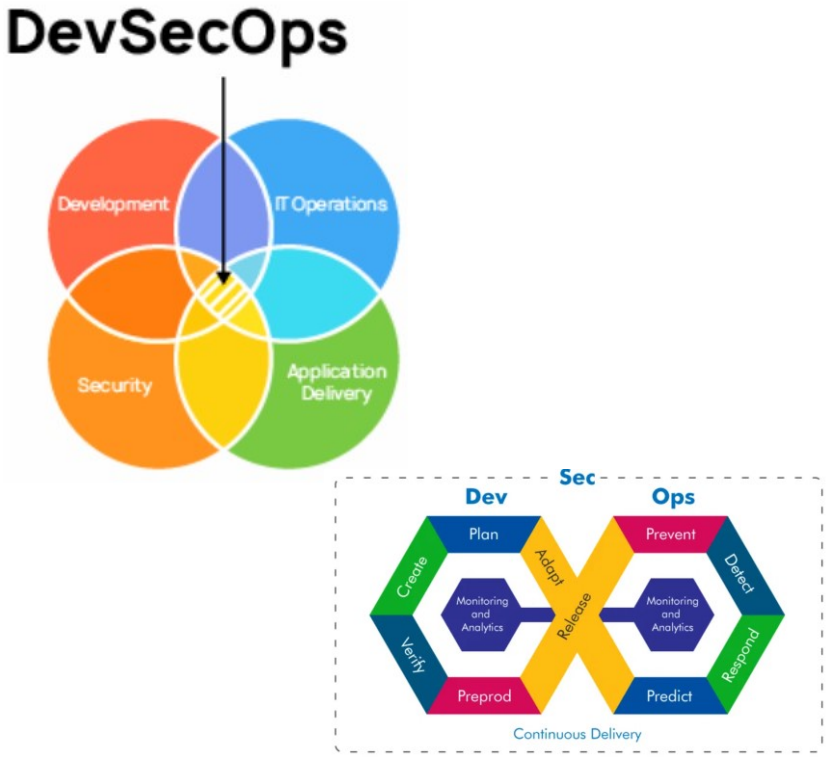
Security roles and responsibilities

You need to manage supplier relationship.

Close co-operation – if they can do it – we can do it



https://securelist.com/russian-financial-cybercrime-how-it-works/72782/



https://www.jasonfranklin.com/evolving-from-devops-to-devsecops-in-an-agile-framework/

Learning is a process

"Tell me and I forget, teach me and I may remember, involve me and I learn." – Benjamin Franklin

Pixabay.com

WE NEED TO FIND BALANCE

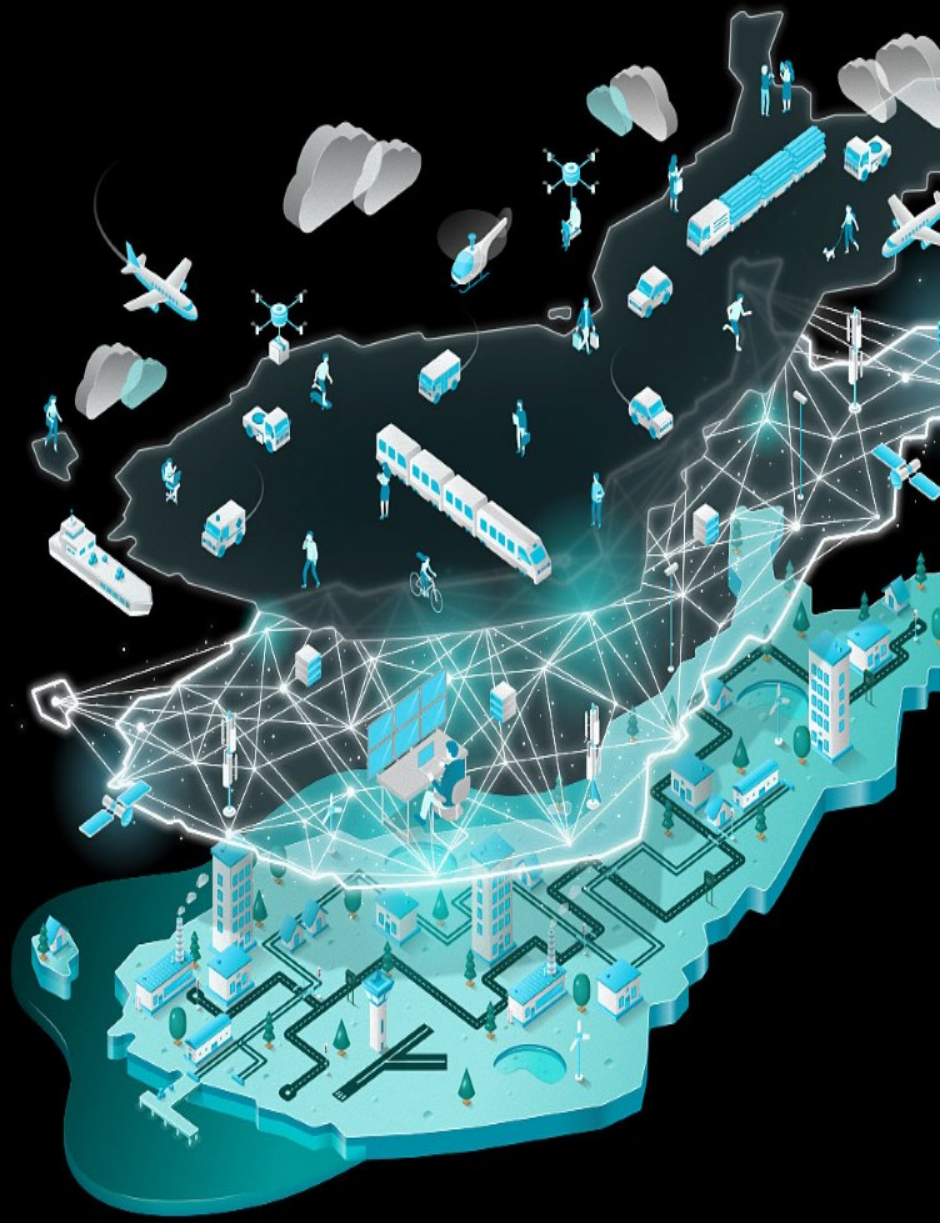
…AND IF THE RISK CANNOT BE MITIGATED…

…BARE MINIMUM IS THAT THE BUSINESS RISKS ARE UNDERSTOOD AND APPROVED IN CORRECT LEVELS.

Fintraffic

Älykkäillä palveluilla maailman turvallisin, sujuvin ja ympäristö-ystävällisin liikenne

Yritysesittely



Meidän tehtävämme

Fintrafficin tehtävänä on varmistaa turvallinen, sujuva ja ympäristöystävällinen liikkuminen Suomen maanteillä, raiteilla, vesillä ja ilmassa. Autamme ihmiset ja tavarat perille turvallisesti, sujuvasti ja ympäristöä huomioiden.

Tässä tehtävässä tärkein välineemme on ajantasainen tieto.

Me tiedämme, millainen Suomen liikennejärjestelmän tila tiettynä ajanhetkenä on ja mitä liikenteessä juuri nyt tapahtuu – ja huolehdimme myös siitä, että tämä tilannekuva on reaaliaikaisesti kaikkien sitä tarvitsevien käytössä.

Luomme Suomeen maailman mittakaavassa ainutlaatuisen liikennetoimijoiden verkoston, liikenteen ekosysteemin.

Fintrafficin palvelut vaikuttavat laajasti

Raideliikenne

- 500 000 junaa vuosittain
- 82 miljoonaa matkustajaa vuosittain
- Rataverkko 6000 km
- 470 ammattilaista

Lennonvarmistus

- Lennonohjausta 22 lentokentällä
- Vuosittain 280 000 operaatiota (Helsinki-Vantaa 190 000)
- 440 ammattilaista

Tieliikenne

- 90 % matkustaja-liikenteestä maanteillä
- Yli 120 miljoonaa km autolla joka päivä
- Tieverkko 78 000 km
- 90 ammattilaista

Meriliikenne

- Viennistä 90 %, tuonnista 80 % meritse
- 30 000 ulkomaan-liikenteen aluskäyntiä / v
- 29 satamaa
- 100 ammattilaista

Lisäksi tuotamme liikenteen ekosysteemin toimijoille ja loppukäyttäjille digipalveluita ja ajantasaista sekä avointa liikennetietoa.

Fintraffic

VISIO: Maailman turvallisin, sujuvin ja ympäristöystävällisin liikenne.

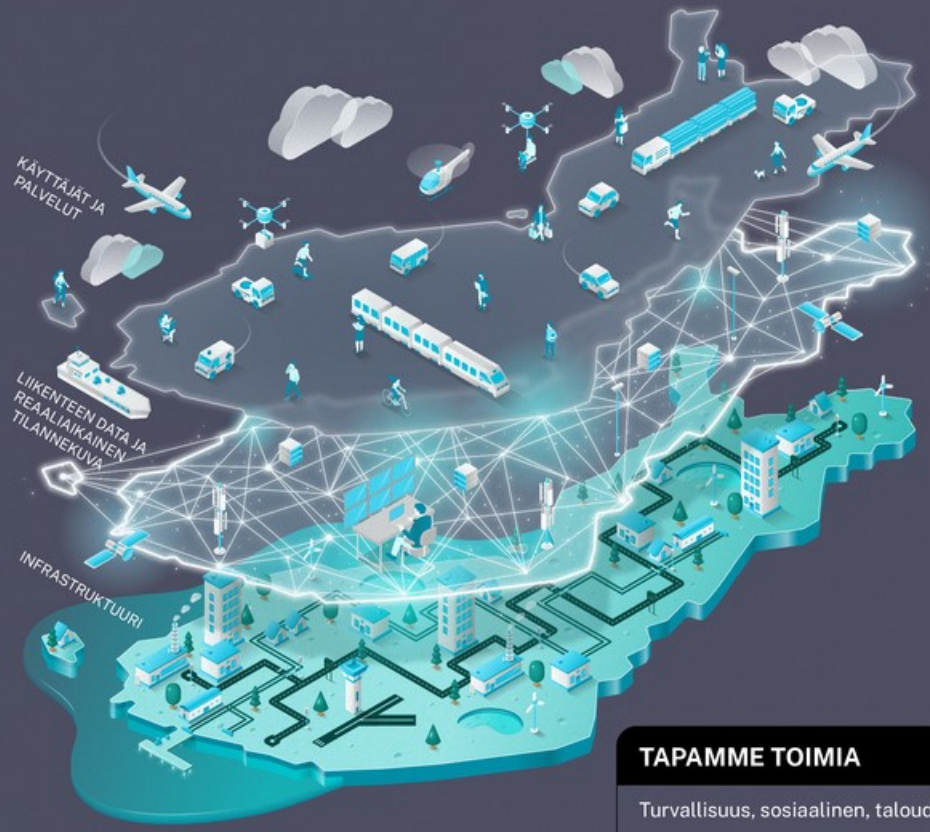
MISSIO: Maailman parasta liikenteenohjausta ja palvelua liikenteen ekosysteemille.

LIIKKUMINEN MUUTTUU

- Digitalisaatio
- Kaupungistuminen
- Ikääntyminen
- Ilmastonmuutos
- Velkaantuminen
- Jakamistalous

TAVOITTEEMME

- Turvallinen, sujuva liikenne & optimoitu liikennejärjestelmä
- Laadukas ja tehokas liikenteenohjaus
- Paremmat palvelut matkustajille ja logistiikalle
- Kasvavaa lisäarvoa asiakkaille ja sidosryhmille
- Erinomainen ja uudistuva työyhteisö



KÄRKIHANKKEEMME

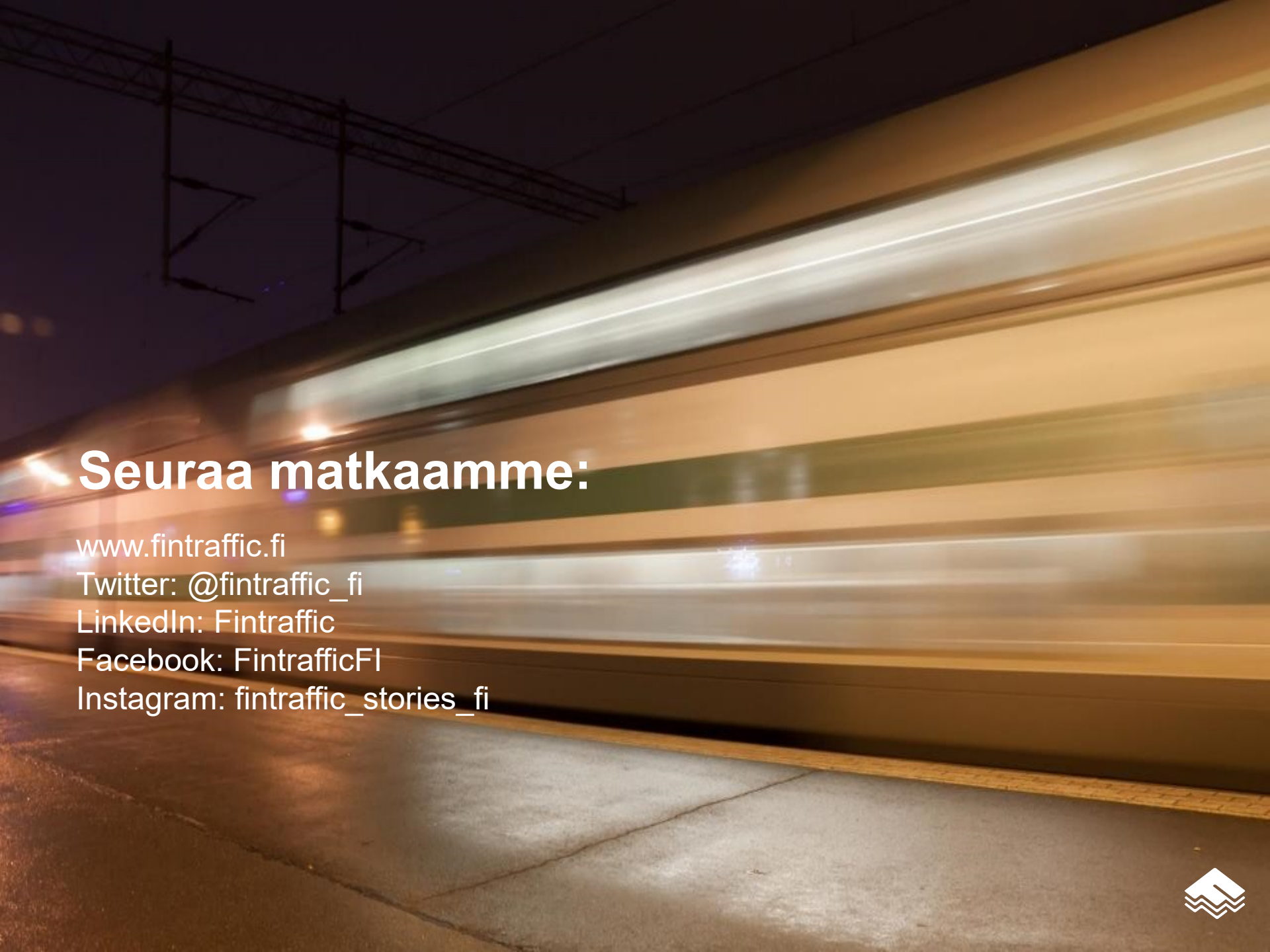
1. Turvallisuuden määrätietoinen parantaminen
2. Oman toimintamme uudistaminen
3. Maailmanluokan liikenteen ekosysteemin luominen
4. Liikenteen reaaliaikainen tilannekuva eli digitaalinen kaksonen
5. Osaaminen, hyvä johtaminen ja uudistuva yrityskulttuuri

KUN ONNISTUMME, SUOMI HYÖTYY

+ Päästöt pienenevät
+ Joukkoliikenne kasvaa
+ Kaikkien kustannukset alenevat
+ Onnettomuudet minimiin
+ Tuloja ja vientimahdollisuuksia liikenteen uusista palveluista
+ Liikenne tukee Suomen kilpailukykyä

TAPAMME TOIMIA

Turvallisuus, sosiaalinen, taloudellinen ja ympäristövastuu, hyvä hallintotapa



Seuraa matkaamme:

www.fintraffic.fi
Twitter: @fintraffic_fi
LinkedIn: Fintraffic
Facebook: FintrafficFI
Instagram: fintraffic_stories_fi

Digiradan Kyberturvallisuus

Fintraffic Oy

Esityksen rakenne

- Johdattelua
- Kyberturvallisuuden tilannekuvaa Digiradan näkökulmasta
- Ohjeistuksia ja hallintajärjestelmän rakentamisesta

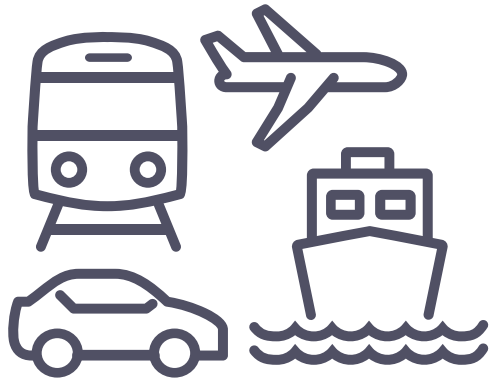
Johdattelua

- Kysykää heti
- Materiaali saatavilla


Fintraffic
Kyberturvallisuuden tilannekuvaa Digiradan näkökulmasta

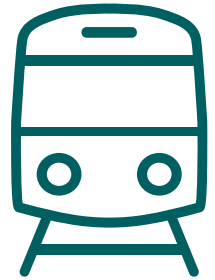
Yleisesti

- Liikenteessä/Logistiikassa
  - Maa
    - Tie
    - Raide
  - Meri
  - Ilma
- Muu infra - riippuvuudet
  - Ruoka ja vesi
  - Sähkö ja lämmitys
  - Tietoliikenne



Tilannekuvaa 1

- Hyvää
  - Raideturvallisuusperusteiset asiat hoidettu hyvin



- Huonoa
  - Digitalisaatioon liittyvät haasteet IT/OT
  - Hyvin erilaiset standardit ja kyvykkyydet toteutukseen
  - Historiallisia laitteita
  - Kyberkulttuurin keskenkasvuisuus
    - Tietoisuus
    - Säätelystä puuttuu kyber

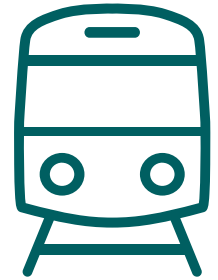
Tilannekuvaa 2

- Haaste – tasapainottaa turvallisuus, toiminnan tehokkuus ja kannattavuus

- Uudessa järjestelmässä erityinen haaste on radiorajapinta/-kantoaalto

Organisoinnista

- NIS(2)-direktiivi
- Joka maassa erilainen hallinnollinen organisointi
- Omat normit
- Erilainen valvonta
- Eri
  - Ohjeet
  - Vaatimukset



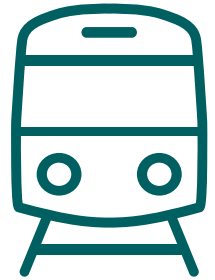
Mitä seuraavaksi?

- Kehitys jatkuu
  - ETCS
  - ERTMS

- ENISA jatkaa harmonisointia ja ohjausta
- TS50701 (luonnos)
- Ei tiukkaa järjestelmällistä ohjausta odotettavissa

Vaikutus digirataan?

- Tehtävä itse, koska olemme kehityksen kärki – ei haittaa vaikka joku muu standardi
- ISO 27001
- ISA 62443
- TS50701



- NIST – hyvää taustatietoa kyberinfran suojaamisesta

Ohjeistuksesta ja kyberturvallisuuden hallintajärjestelmän rakentamisesta

Traficom (Suositus kyberturvallisuuden edistämisestä raideliikenteessä) ja TS 50701(luonnos)

IT- ja OT-tietoturva

- IT – hyvät hallinnolliset menetelmät (esim. tietoturvastandardit)
- OT – hyvä ja luotettava tekniikka (automaatiotekniikka yleisesti tuotannonturvallisuus näkökulmasta)

→Yhdistelmä: huonot hallinnolliset menetelmät ja epäluotettava tekniikka

Ratkaisu:

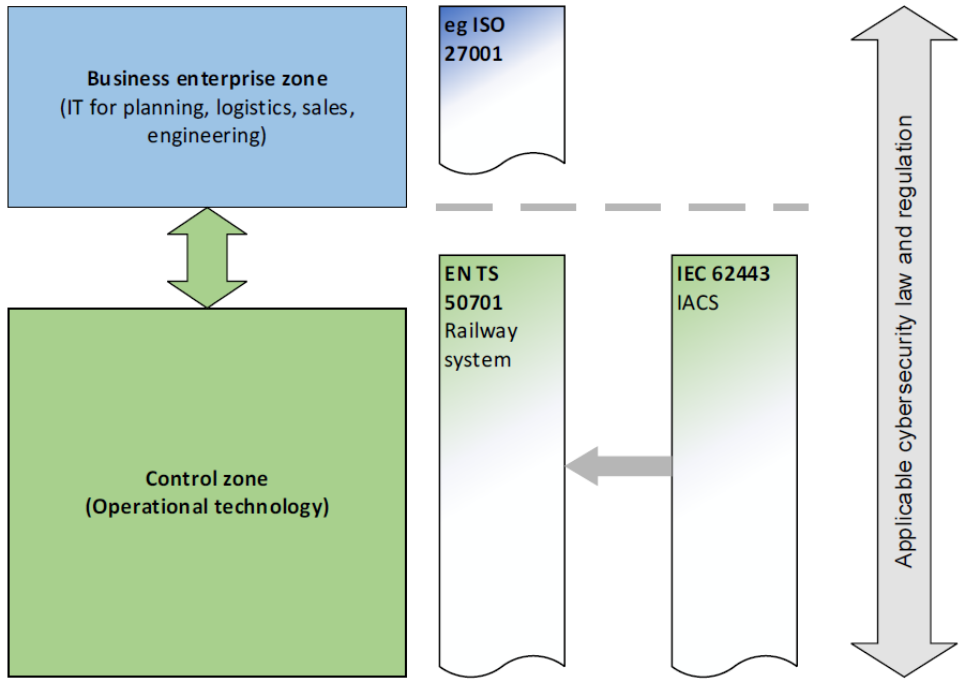
- Noudata hyviä hallinnollisia menetelmiä (IEC 27001 + IEC 62443 ≈ TS 50701)
- Yhdistä järjestelmiä vain, kun olet varma molempien turvallisuudesta
- Eristäminen - edullinen tapa, jos pystyy (jatkamaan automaation fyysistä eristämistä)
- Vanhojen järjestelmien liittäminen tietoverkkoon on suunniteltava hyvin – usein sekään ei auta, vaan uusi järjestelmä tulee halvemmaksi

Kyberympäristön haasteita

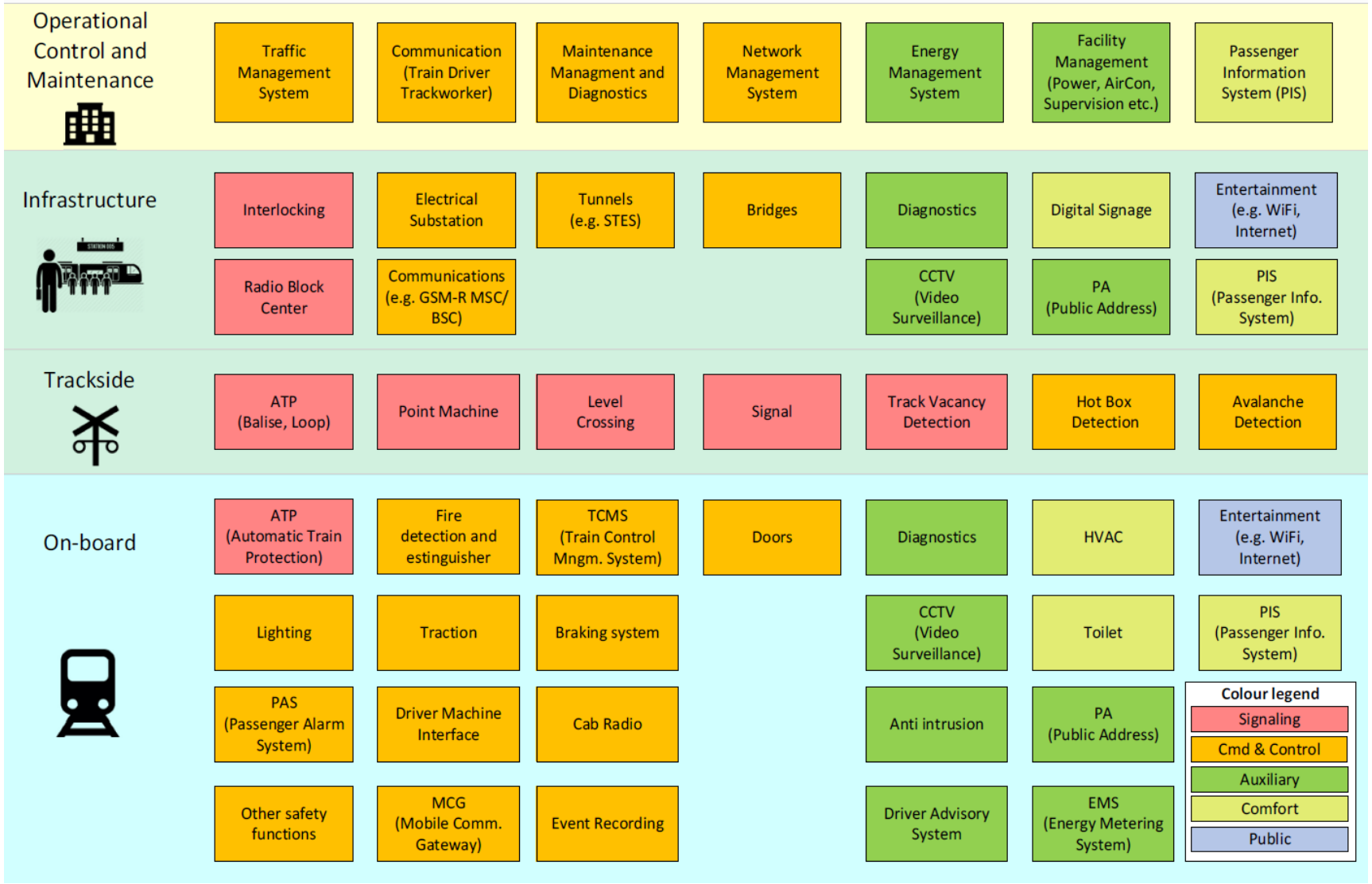
- Päivittämättömät ympäristöt
- Elinkaarensa päässä olevat tuotteet käytössä (tuotetuki ja tietoturvapäivitykset puuttuvat)
- Hybridisodankäynnissä käytetyt 0-päivä-haavoittuvuudet johtavat ympäristöjen saastumiseen
  - Useimmiten käytetään tiedusteluun suorituskyvystä
  - Vasta viime kädessä haitan tekemiseen
- 5G-teknologian myötä mahdollistunut laajempi hyökkäyskaista
- Pilvipalveluiden sabotointi
- Dronejen avulla tehdyt hyökkäykset

TS 50701 (luonnos)

- Secure-by-design – Defence-in-depth
- Turvajärjestelmä
- Periaate suunnittelussa
  - Kaikessa, myös integrointi
  - 27001
  - 62443
- Alueittain/kohteittain (zone)
  - Rautatiejärjestelmän kaikille osa-alueille



TS 50701 (luonnos)



TS 50701 (luonnos)

- Teknisestä rakenteesta
  - Riskipohjainen ajattelu
  - IT ja OT, erottelu ja integrointi
  - Turvajärjestelmäsuunnittelu järjestelmäkohtaisesti
    - Safety
    - Security (Key Management System)
  - Osa kaikkia järjestelmiä
    - Pakollinen prosessi

Kysyttävää?

Kiitos!

TRAFICOM
Finnish Transport and Communications Agency

Kybermittari - Kuinka ilmailusektorin kokemuksia voidaan hyödyntää raiteilla

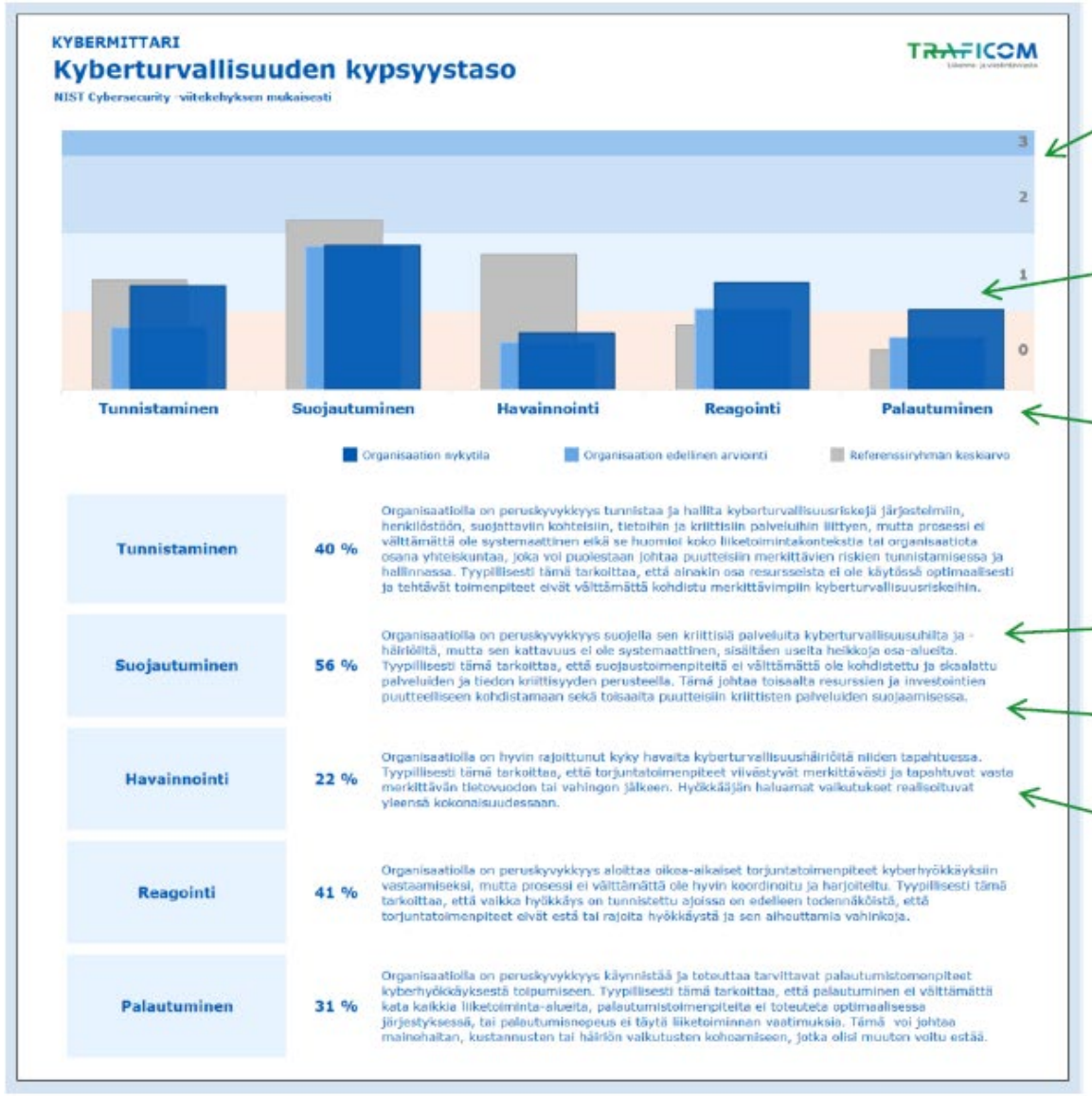
21.4.2021 Raideliikenteen kyberturvallisuuden työpaja

Tomi Salmenpää, Johtava asiantuntija, ilmailun kyberturvallisuus

Kybermittari?

Työkalu organisaatioiden kyberturvallisuuden arviointiin ja kehittämiseen

TRAFICOM



Kypsyysasteikko 0-3

Kolmet arviointitulokset
- Nykyinen
- Edellinen
- Referenssi

NIST CSF 5 osa-aluetta

Osa-alue

Toteutuneiden käytäntöjen osuus (%)

Sanallinen kuvaus kypsyystasosta

NIST CSF Osa-alueet ja tavoitteet

Käytäntöjen määrä ja toteutumisprosentti

(kokonaisuudessaan)

Käytäntöjen määrä ja toteutumisprosentti

(jaettuna kypsyystasojen mukaisesti)

KYBERMITTARI

Yksityiskohtainen NIST Cybersecurity Framework Core -raportti

Perustuen suostuvaan riistinkytkeistä C2M2 ja NIST-mallien välillä

TRAFICOM

NIST Cybersecurity Framework Core						Implementation of C2M2 Practices							
Function	ID	Category	Description	ID	Subcategory	Total implemented	# of controls	Maturity level 1		Maturity level 2		Maturity level 3	
Identify	ID.AM	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1	Physical devices and systems within the organization are inventoried	50 %	4	100 %	1	0 %	1	50 %	2
				ID.AM-2	Software platforms and applications within the organization are inventoried	50 %	4	100 %	1	0 %	1	50 %	2
				ID.AM-3	Organizational communication and data flows are mapped	25 %	4	0 %	0	0 %	1	33 %	3
				ID.AM-4	External information systems are catalogued	20 %	5	100 %	1	0 %	3	0 %	1
				ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	29 %	7	100 %	2	0 %	4	0 %	1
				ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	75 %	4	100 %	2	50 %	2	0 %	0
	ID.BE	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-1	The organization's role in the supply chain is identified and communicated	0 %	5	0 %	1	0 %	3	0 %	1
				ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	17 %	6	0 %	1	25 %	4	0 %	1
				ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	0 %	1	0 %	0	0 %	1	0 %	0
				ID.BE-4	Dependencies and critical functions for delivery of critical services are established	24 %	17	100 %	3	0 %	7	14 %	7
				ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	20 %	5	100 %	1	0 %	4	0 %	0
	ID.GV	Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1	Organizational cybersecurity policy is established and communicated	0 %	3	0 %	0	0 %	1	0 %	2
				ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	67 %	6	100 %	2	100 %	2	0 %	2
				ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	0 %	2	0 %	0	0 %	1	0 %	1
				ID.GV-4	Governance and risk management processes address cybersecurity risks	50 %	6	100 %	2	0 %	1	33 %	3
	ID.RA	Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1	Asset vulnerabilities are identified and documented	67 %	12	100 %	4	40 %	5	67 %	3
				ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources	71 %	7	100 %	5	0 %	1	0 %	1
				ID.RA-3	Threats, both internal and external, are identified and documented	71 %	7	100 %	2	50 %	4	100 %	1
				ID.RA-4	Potential business impacts and likelihoods are identified	25 %	4	0 %	0	25 %	4	0 %	0
				ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	40 %	5	0 %	0	50 %	2	33 %	3
				ID.RA-6	Risk responses are identified and prioritized	50 %	6	0 %	0	50 %	4	50 %	2
	ID.RM	Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	63 %	19	100 %	3	78 %	9	29 %	7
				ID.RM-2	Organizational risk tolerance is determined and clearly expressed	50 %	2	0 %	0	0 %	1	100 %	1
				ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	0 %	1	0 %	0	0 %	1	0 %	0
	ID.SC	Supply Chain Risk Management	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	25 %	4	50 %	2	0 %	1	0 %	1
				ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	13 %	8	50 %	2	0 %	4	0 %	2
				ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	44 %	9	100 %	1	60 %	5	0 %	3
				ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	0 %	3	0 %	0	0 %	1	0 %	2

Taustaa

Mitä tähän mennessä on tehty?

..sitoutuminen, kriittisten järjestelmien tunnistaminen, itsearviointi..

Kokemuksia

- Arvioitavat organisaatiot, edellytykset?
- Yhteinen metodologia kriittisten järjestelmien rajaamiseen (Arvioitava toiminnan osa-alue)
- Visuaalisuus ja konkreettisuus (tunnistaminen, suojaaminen, havaitseminen, reagointi, palautuminen)
  - Johtaa toimenpiteisiin organisaation aloitteesta
- Asioiden herkkyys (avoimuus ja luottamus)
- Perusta uudenlaiselle yhteistyölle

Jatkotyö

Miten ja mitä tästä eteenpäin?

TRAFICOM

Finnish Transport and Communications Agency

tomi.salmenpaa@traficom.fi
www.traficom.fi
@TraficomFinland

Kyberturvallisuuden merkitys logistiikan huoltovarmuudessa

4.6. Raideliikenteen kyberturvallisuuden työpaja

4.6.2021

Jarna Hartikainen

Varautumispäällikkö, kyberturvallisuus

HUOLTOVARMUUSKESKUS

Sisältö

- Mitä on huoltovarmuus?
- Digitaalinen turvallisuus logistiikka alalla ja merkitys huoltovarmuudelle
- Huoltovarmuuskeskuksen ohjelmat tukemassa kehitystä

Mitä on huoltovarmuus?

TOIMIVA YHTEISKUNTA

HUOLTOVARMUUSKESKUS

TURVATAAN YHTEISKUNNAN TOIMINTAKYKY

KESKINÄISRIIPPUVUUDET YTIMESSÄ

- Terrorismi
- Energiapula
- Rikollisuus
- Sään ääri-ilmiöt
- Logistiikan häiriöt
- Verkkohyökkäykset
- Tietojärjestelmä-uhat
- Vaaralliset tartuntataudit

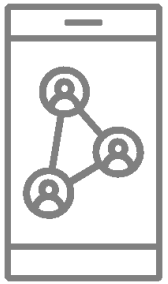
PAINOPISTEET MUUTTUMASSA

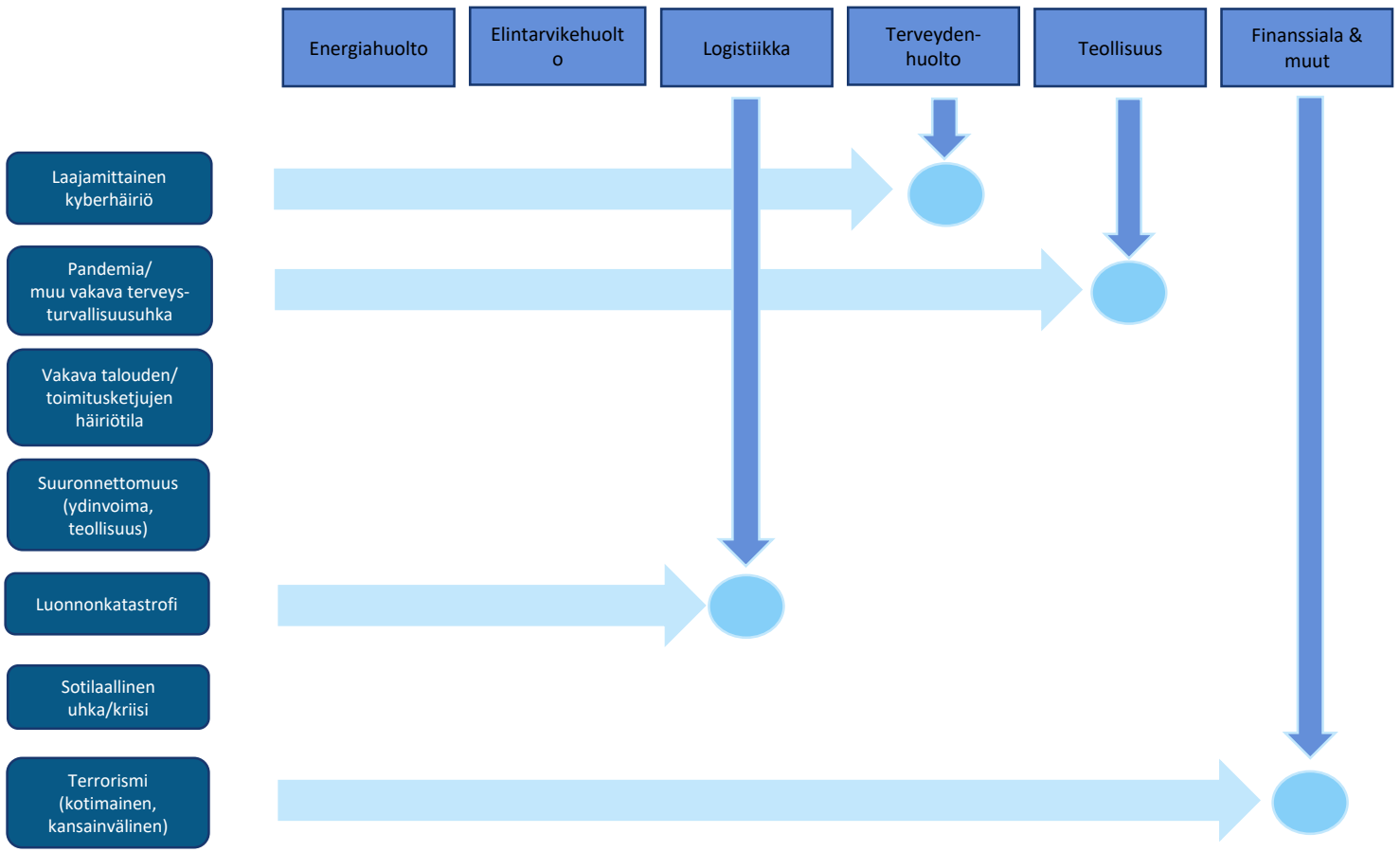
MATERIAALINEN VARAUTUMINEN

- Varastointi
- Tuotantovaraukset
- Investoinnit
- Tekniset järjestelmät

TOIMITUSVARMUUS RESILIENSSI

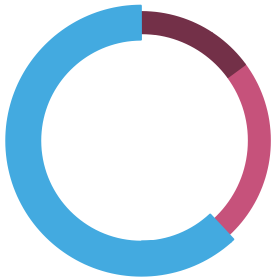
- Jatkuvuudenhallinta
- Häiriönsietokyky
- Yhteistoiminta
- Digitaalisuus





HVK:n ”työkalupakki”: 1. Toimialojen tuntemus, 2. Riskienhallinta, tilannekuva (ml. skenaariointi), 3. Verkostojohtaminen, 4. Johtaminen, 5. Valmiuden kohottaminen, 6. Huoltovarmuuden uudistaminen, 7. Toimintatapojen ja prosessien kehittäminen, 8. Kansainvälinen yhteistyö, 9. Materiaalinen varautuminen, 10. Henkilöstön osaamisen kehittäminen

HUOLTOVARMUUS PERUSTUU LAINSÄÄDÄNTÖÖN



Jokainen viranomainen:

VELVOLLISUUS HUOLEHTIA VARAUTUMISESTA, KEHITTÄMISESTÄ JA VALVONNASTA

(Valmiuslaki 1552/2011 §12 JA §13)

HUOLTOVARMUUSKESKUS TOTEUTTAA ERITYISTOIMENPITEITÄ

(Laki huoltovarmuuden turvaamisesta 1390/1992 ja Huoltovarmuuspäätös)

KRIITTISILTÄ YRITYKSILTÄ ODOTETAAN SITOUTUMISTA JA HYVIN HOIDETTUA JATKUVUUDEN HALLINTAA

HUOLTOVARMUUDEN PERUSTAVOITE

TOIMINNAN TURVAAMINEN VAKAVISSA HÄIRIÖTILANTEISSA JA POIKKEUSOLOISSA

VÄESTÖ – ELINKEINOELÄMÄ - MAANPUOLUSTUS

Jaettu yrityksen ja HVK:n vastuu	**YHTEISKUNNAN TARPEET:** Yhteiskunnan tarpeisiin perustuva kahden- ja monikeskeinen riskienhallinta
Yrityksien vastuulla	**LIIKETOIMINNAN ASETTAMAT VAATIMUKSET:** yrityksen omiin päätöksiin perustuva riskienhallinta (maine, kilpailukyky ja laatu, asiakasvelvoitteet)
	LAIN ASETTAMAT VAATIMUKSET: Regulaatioon ja muuhun ulkoiseen velvoitteeseen perustuva riskienhallinta

Logistiikan merkitys huoltovarmuudelle?

DIGITAALINEN TURVALLISUS LOGISTIIKASSA

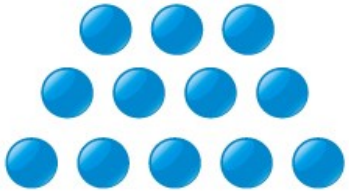
HUOLTOVARMUUSKESKUS

TOIMIALOJEN NYKYTILA KAROITUS – TIETOA KEHITYKSEN TUEKSI

Vaikuttavien kehityskohteiden löytämiseksi tarve tietää
NYKYTILA

KYBERMITTARI
Pohjalta valikoitu liiketoimintanäkökulma
30 kysymystä

Tutkimuksen laajuus



- 100 + organisaatiota
- 12 toimialaa

Arviointiasteikko

5 Kehitetään jatkuvasti riskilähtöisesti
4 Tehdään johdonmukaisesti
3 Määritetty tai suunniteltu
2 Tehdään vaihtelevasti ja/tai osittain
1 Ei tiedä

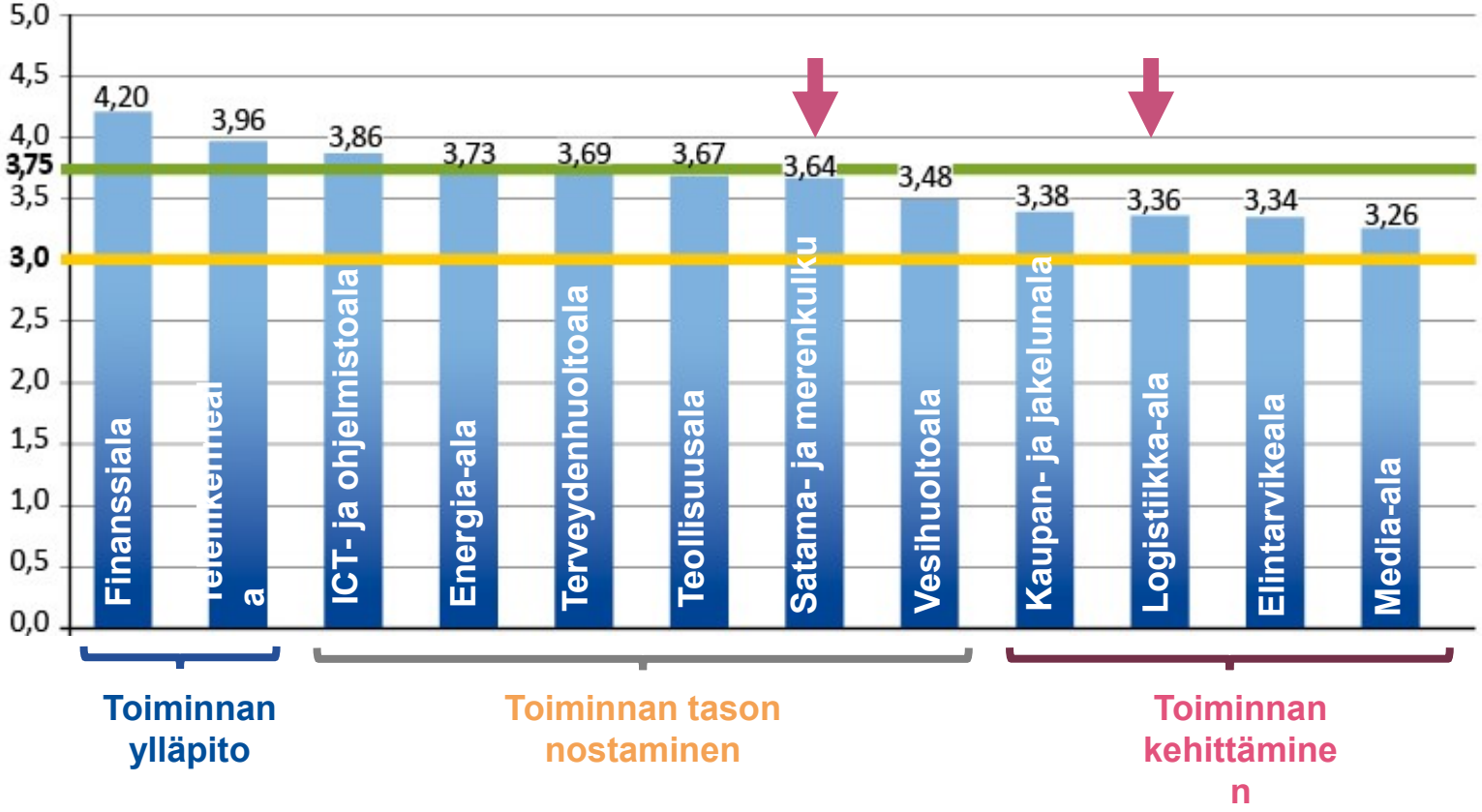
Tavoitteet

4 Organisaation riski laskee

3,75 Toimiala tukee muita

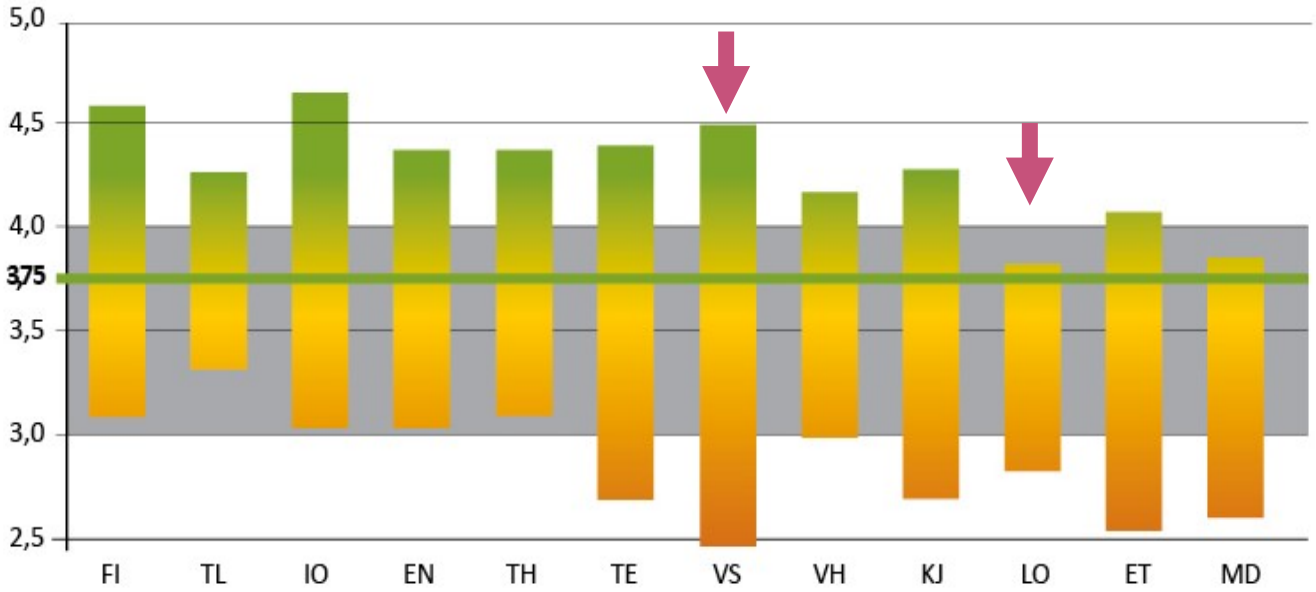
HUOLTOVARMUUSKESKUS

LOGISTIIKKA ALANA KEHITTYVIEN JOUKOSSA



HUOLTOVARMUUSKESKUS

OMAN ALAN EDELLÄKÄVIJÄ VAI SUUNNANETSIJÄ?



FI= finanssiala, TL= teleliikenneala, IO= ICT- ja ohjelmistoala, EN= energia-ala, TH= terveydenhuoltoala, TE= teollisuusala, VS= satama- ja merenkulkualat, VH= vesihuoltoala, KJ= kaupan- ja jakelun ala, LO= logistiikka-ala, ET= elintarvikeala, MD= media-ala

Jokainen yritys on yksilöllinen – hajonta alojen sisällä vaihtelee

HUOLTOVARMUUSKESKUS

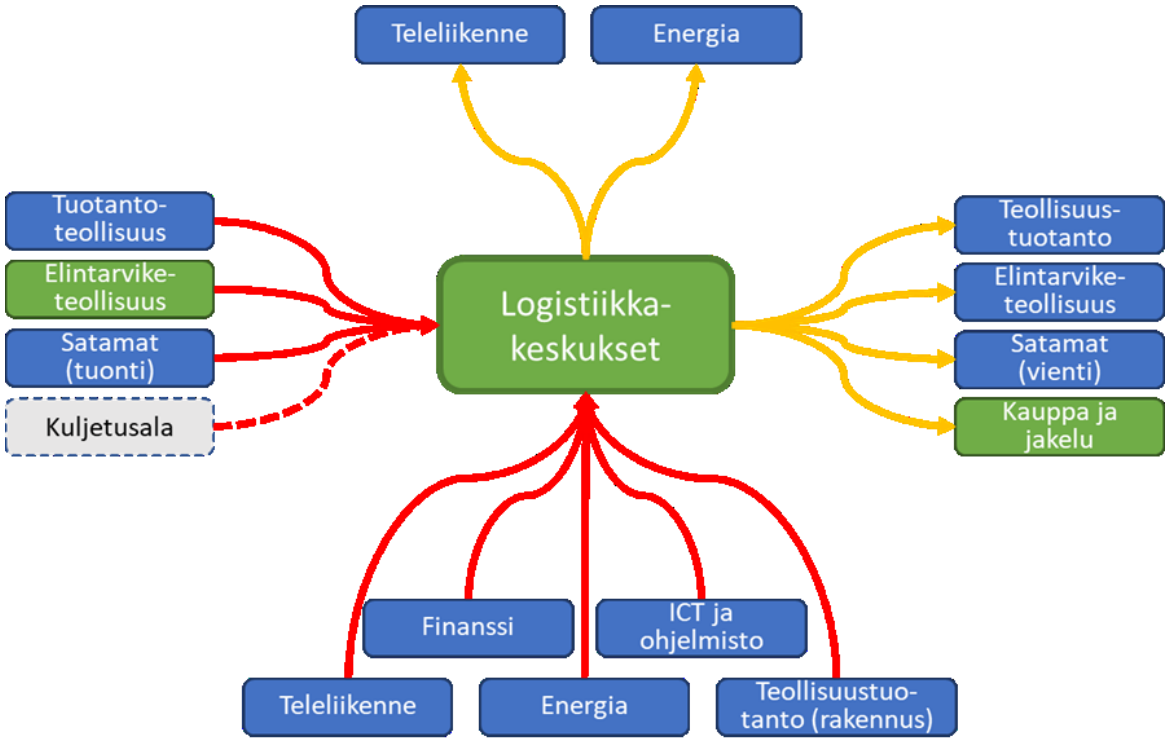
Logistiikka osana riippuvuusverkostoa?

Oman solmun vahvistaminen ja yhteistyön avulla riippuvuuksien huomiointi

= Lähtöpäällä täysi riippuvuus
= Lähtöpäällä merkittävä riippuvuus
= Lähtöpäällä osittainen riippuvuus
= Molemmilla vahva riippuvuus
= Molemmilla osittainen riippuvuus

Logistiikka-alan toimialakohtaiset riippuvuustek…

TLP: AMBER



Merkittävimmät kaikkia aloja koskevat kehityskohteet

YHTEISESTI

huoltovarmuuden näkökulma

1. Yhteinen tilannekuva
2. Turvallinen ohjelmistokehitys
3. Henkilöstön osaaminen

YRITYKSILLE

liiketoiminnan näkökulma

1. Yrityksen kyberturvallisuusstrategia
2. Kyberturvallisuusarkkitehtuuri
3. Tekninen jäljitettävyys

HUOLTOVARMUUSKESKUS

Logistiikka alan päähavainnot

Logistiikka ja raidealan huomioitavia asioita

- Käytettyjen tukijärjestelmien ohjelmistoturvallisuus
- Liikenteenohjaukseen käytettyjen järjestelmien turvallisuus
- Käytettyjen verkkojen turvallisuus
- Varautuminen verkkohäiriöihin ja varayhteydet
- Kyberturvallisuuden johtaminen ja riskienhallinta

Huoltovarmuuskeskuksen ohjelmat kehityksen tukena

HUOLTOVARMUUSKESKUS

TOIMINTAMME PAINOPISTEITÄ 2020-2023

ENERGIA2030	Hiilineutraali Suomi
DIGITAALINEN TURVALLISUUS 2030	Digitaalisen yhteiskunnan turvaaminen
LOGISTIIKKA2030	Logistiikkatoimintojen turvaaminen
ALUE 2030	Alueellinen varautuminen ja yhteistyö

HUOLTOVARMUUSORGANISAATIO

Huoltovarmuusorganisaatio muodostuu n. 1000 osallistujan yhteistoiminta- ja asiantuntijaverkostosta - sekä julkiselta, että yksityiseltä sektorilta.

HUOLTOVARMUUSNEUVOSTO

HUOLTOVARMUUSKESKUS

ELINTARVIKE-HUOLTO

Alkutuotanto

Elintarviketeollisuus

Kauppa ja jakelu

KOVA -toimikunta

ENERGIA-HUOLTO

Voimatalous
- 5 aluetoimikuntaa
- Kaukolämpöjaosto
- Kotimaisten poltto-aineiden jaosto

Öljy
- Maakaasujaosto

LOGISTIIKKA

Ilmakuljetus

Maakuljetus

Vesikuljetus

TERVEYDEN-HUOLTO

Terveydenhuolto

Vesihuolto
Jätealan huolto-varmuustoimikunta

FINANSSIALA

Rahoitushuolto

Vakuutus

TEOLLISUUS

Kemia

Metsä

MIL

Muovi ja kumi

Rakennus
- 6 aluetoimikuntaa

Teknologia

MUUT

Digi

Media

Huoltovarmuuskriittiset yritykset

Alueellisen varautumisen yhteistoiminta

OHJELMAN LÄHTÖKOHDAT

- Logistiikan **toimintaympäristön** muutos
- **Suomen asema** osana globaalia logistiikkaa
- Kokonaisvaltainen varautuminen vaatii **yhteistoimintaa**
- Katse **tulevaan**

LOGISTIIKKA2030

JOTTA YHTEISKUNTAMME KRIITTISET TOIMINNOT KESTÄISIVÄT KYBERHÄIRIÖT

- Yhteiskunnan **digitalisoituminen**
- Kokonaisvaltainen varautuminen vaatii **yhteistyötä**
- Verkostojen ja järjestelmien **kansainvälisyys**
- Tulevaisuuden **ennakointi**

DIGITAALINEN TURVALLISUUS 2030

DIGITAALINEN TURVALLISUUS 2030

OHJELMAN KOKONAISUUS

Toimintaympäristön muutos

- Digitaalisten ekosysteemien hallinta on globaalia
- Riippuvuus automaatiosta, koneoppimisesta ja tekoälystä
- Riskienhallinta kompleksisessa infrastruktuurissa monimutkaistuu
- Häiriöiden leviäminen hallitsemattomasti
- Kriittiset toiminnot ovat kumppaniverkostossa
- Luottamus digitaalisiin palveluihin kyseenalaistuu

VARAUTUMINEN

Kriittisen digitaalisen infrastruktuurin ja palvelujen riippuvuudet ymmärretään niiden toiminnan turvaamiseksi

TOIMINTAKYKY

Tiedonvaihtoa tukee kattava havainnointi- ja analysointikyky, johon riittävät työkalut

YHTEISTYÖVERKOSTOT

Tiedonvaihtoverkostot toimivat aktiivisesti määritetyin tiedonjakomallein ja vastuin

TULEVAISUUS

Huoltovarmuuteen vaikuttavia nousevia ilmiöitä tutkitaan yhteistyössä yritysten, tutkimus- ja oppilaitosten kesken

VISIO

Yhteiskuntamme kriittiset toiminnot kestävät kyberhäiriöt

OHJELMAN KOKONAISUUS

Kiitos!

Jarna Hartikainen
Varautumispäällikkö
Huoltovarmuuskeskus

jarna.hartikainen@nesa.fi
@JarnaHnen

Yhteystiedot

Huoltovarmuuskeskus

Aleksanterinkatu 48A, 7 krs.
FI-00100 HELSINKI
Puh: 02950 51000

- nesa.fi
- huoltovarmuus.fi
- varmuudenvuoksi.fi