Rautateiden kyberturvallisuus Väylävirastossa

Raideliikenteen kyberturvallisuuden seminaari

Tomi Kangas

3.12.2024

Julkinen

Väylävirasto
Trafikledsverket

Sisältö

- Johdanto
- Riskien tunnistamista ja hallintaa
- Menettelyt osana johtamisjärjestelmää
- Mitä on saatu aikaan ja mitä seuraavaksi?

Väylävirasto
Trafikledsverket

Tomi Kangas
turvallisuusjohtaja

tomi.kangas@vayla.fi

Johdanto

- Vuonna 2020 toteutettiin ensimmäinen tietoturva-auditointi rataverkolle – KATAKRI-vaatimukset auditoinnin lähtökohtana
- Tulosten pohjalta päätettiin käynnistää kehittämishanke ”Rataverkon kyberturvallisuusohjelma” – resursseihin lisäpanostusta; vakituinen kyberturvallisuusasiantuntija sekä satojen tuhansien eurojen vuosittainen kehitysrahoitus
- Hankkeen tavoitteena on varmistaa rataverkon kybertoimintaympäristön luotettavuus ja vakiinnuttaa kyberturvallisuuden hallinta osaksi viraston kaikkea toimintaa. Hanke jatkuu ainakin vuoden 2025 loppuun.
- Kohteena on Väyläviraston hallinnassa oleva valtion rataverkko ja sen liikenteenohjauspalvelu, sekä Väyläviraston hallinnassa olevat laitteet, huomioiden nykyinen tilanne ja Digirata.
- Hanketta toteuttaa projektiryhmä, johon osallistuu useita asiantuntijoita Väylävirastosta, Fintraffic Raiteelta ja palveluntuottajilta tarpeen mukaan. Työtä ohjaa ohjausryhmä, joka koostuu Väyläviraston johdosta ja asiantuntijoista.

Väyläviraston tunnuslukuja

Väylävirasto
Trafikledsverket

Väyläomaisuus
20 mrd €

Väyläverkon korjausvelka
4,2 mrd €

Vuosibudjetti **2024** noin
2,1 mrd €

Investointihankkeita rakenteilla
2,9 mrd € arvosta

Henkilöstö, vakinaisia noin
490 asiantuntijaa

Voimassa olevien sopimusten kokonaisarvo
7,5 mrd €

Työllistämme välillisesti
18 000 ihmistä

Voimassa olevia sopimuksia
7 900

Rautatiet lukuina

Rataverkon pituus

5 915 km

Yksiraiteista rataa

88 %

Sähköistetty rata

3 626 km

Henkilöliikenteen matkat

82,4 milj.

Tavaraliikenteen kuljetukset

27,1 milj. tonnia

Tasoristeyksiä pääradalla

2 400

Tunneleita

46

Henkilö- ja tavaraliikenteen liikennepaikkoja

308

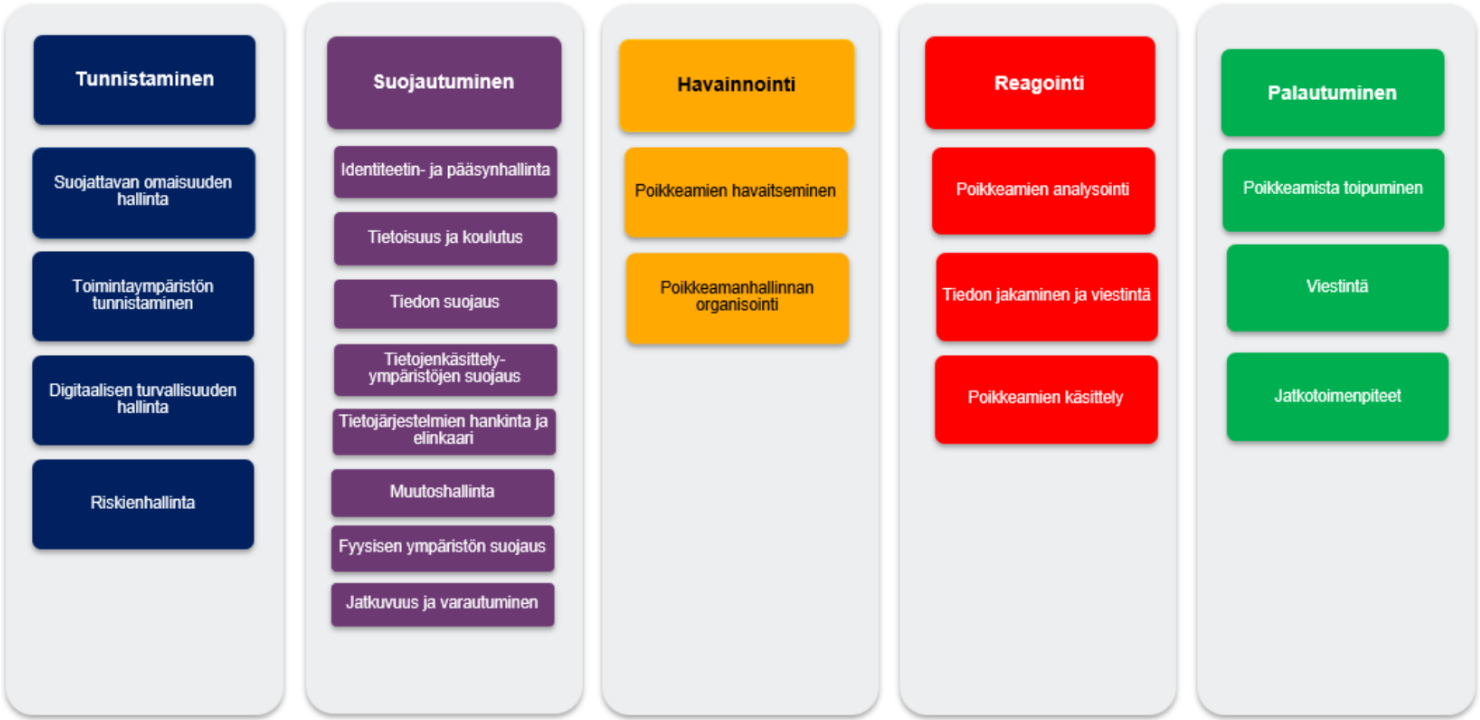
Nopea rataverkko

1 119 km

09/2024

Hankkeen toimenpiteet

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



Toimenpiteiden suunnittelussa on huomioitu tietoturvan hallintaan kohdistuvat yleiset vaatimukset ja hyvät käytännöt, Digitaalisen turvallisuuden arkkitehtuurin julkinen dokumentaatio sekä Traficomin suositus kyberturvallisuuden edistämisestä raideliikenteessä

Kehittämisen suurimmat haasteet

Väylävirasto
Trafikledsverket

Rataverkko on valtava kokonaisuus, jossa on erilaisia ja eri ikäisiä laitteita ja ratkaisuita

- Eri laitekannasta johtuen samat ratkaisut eivät sovellu kaikkialle
- Eri kriittisyysluokasta johtuen ratkaisuita joudutaan priorisoimaan

Asiantuntijaresurssien puute ja useat muut rinnakkaiset tärkeät tehtävät hidastavat etenemistä

- Rautatiejärjestelmän kyberturvallisuuteen liittyvää osaamista ja asiantuntemusta ei juurikaan ole ollut valmiina olemassa – jatkuva oppimisprosessi kaikilla osallistujilla
- Kyberturvallisuuden ymmärryksen lisäksi tarvitaan laajaa ja kokonaisvaltaista rautatiejärjestelmän ja viraston toimintaympäristön tuntemusta
- Kyberturvallisuusohjelman lisäksi muitakin tärkeitä asioita ja kehitystoimenpiteitä meneillään – asiantuntijoilla ei ole mahdollisuutta keskittyä ainoastaan tähän hankkeeseen

Resurssikapeikoista huolimatta haluamme tehdä asioita fiksusti ja riskiperusteisesti

- Konkreettisten toimenpiteiden käynnistäminen vaatii huolellista suunnittelua

Riskien tunnistamista ja hallintaa

Riskiarviointia

Haasteena uhkaskenaarion todennäköisyyden arvioiminen. Pitää ottaa huomioon

- Millaisia taitoja hyökkäyksen tekemiseen tarvitaan
- Kuinka alttiina kohde on hyökkäyksille
- Hyökkääjän tarkoitukset/tavoite

➢ Näiden tarkka arvioiminen voi olla vaikeaa ja vaatii eri asiantuntijoiden yhteistyötä.

Esimerkkiskenaarioita

Väylävirasto
Trafikledsverket

S1 – Opastimien tai JKV:n vaarantaminen -> aiheutuu onnettomuus

- Korkea motivaatio, syvällinen järjestelmien tuntemus -> Matala todennäköisyys
- Vaikutus todella korkea -> "päähuolenaihe" kyberriskejä arvioitaessa
- Tapahtunut 2008 Lodzissa Puolassa, hakkeri päässyt hallinnoimaan raitioteiden liikennevaloja

1 An attacker gathers information (physical trespassing, malicious employee, phishing).

2 The attacker builds a device or software to command-and-control junctions and trains.

3 The attacker takes control of the junctions and trains.

4 False signaling information is injected and leads to a major disruption or a train accident.

Esimerkkiskenaarioita

Väylävirasto
Trafikledsverket

S2 – Liikenteenohjauksen järjestelmien häirintä -> liikenteen pysähtyminen

- Hyökkääjä pääsee järjestelmään sisään verkkoon esim. kalasteluviestin tai USB-tikun kautta
- Haittaohjelma ujuttautuu liikenteenohjausverkkoon
- Hyökkääjä saa etäyhteyden järjestelmään ja katkaisee yhteyden
- Vastaavaa ei ole vielä tapahtunut

1 An ICS malware is introduced into the IS (phishing, removable device).

2 The ICS malware propagates itself to the OT systems.

3 The attacker obtains remote access to traffic supervision systems.

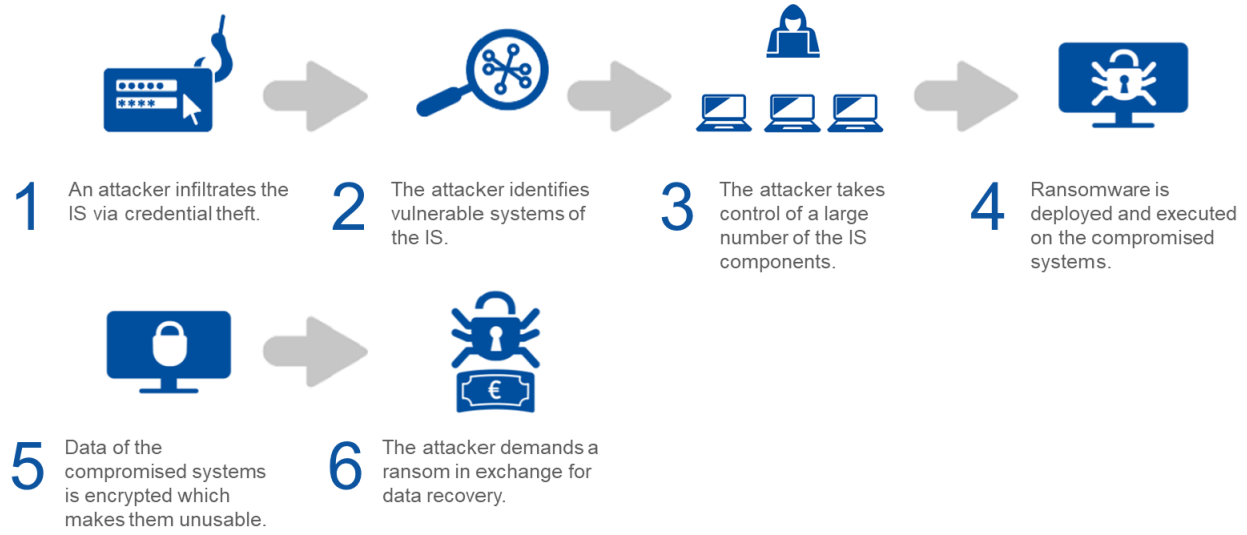
4 The attacker disrupts traffic supervision systems which results in an emergency train traffic interruption.

Esimerkkiskenaarioita

Väylävirasto
Trafikledsverket

S3 – Kiristyshaittaohjelma -> aiheutuu häiriö

- Hyökkääjä pääsee varastetuilla tunnuksilla järjestelmään ja etsii haavoittuvia laitteita
- Asentaa kiristyshaittaohjelman joka kryptaa järjestelmät
- Pidetään mahdollisimpana uhkaskenaariona nykypäivänä
- Esim. 2017 Deutche Bahn'in raideinfra saastui WannaCry kiristyshaittaohjelmasta, jonka seurauksena näytöt asemilla näyttivät tiettyjä viestejä



Esimerkkiskenaarioita

S7 – Datakeskuksen tuhoutuminen -> aiheutuu häiriö IT-palveluihin

- Syy voi olla myös fyysinen, esim. tulipalo, luonnonilmiö
- Vaikutus riippuu paljon siitä, miten järjestelmät on rakennettu (hajautettu maantieteellisesti, pilvi, varmuuskopiot jne.)
- Esim. 2021 OVH:lla tulipalo yhdessä datakeskuksessa, miljoonat nettisivut alhaalla useita päiviä

1 A physical event occurs and affects the datacenter.

2 Permanent physical damage affects the datacenter IT systems and the backups.

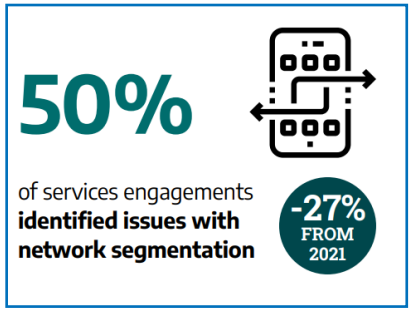
3 IT-related activities are disrupted. Recovery requires more time due to the destruction of backups.

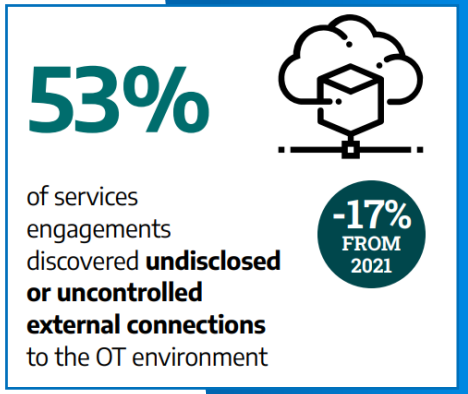
Väylävirasto
Trafikledsverket

Suojaudu

- Miten suojaudumme uhilta?

- Eriytä verkkoympäristöt.
- Kovenna laitteet valmistajan ohjeen mukaisesti.
- Ylläpidä varmuuskopioita ja harjoittele niiden palauttamista.
- Käyttäjätunnusten hallinta: Vaihda oletussalasanat. Vain tarvittavilla henkilöillä käyttäjätunnukset, tarpeellisilla käyttöoikeustasoilla.
  - Eri käyttäjätili & -tunnus IT ja OT ympäristöön! [1]
- Ulkoiset verkkoyhteydet!!! – turvallinen etäkäyttö.
  - Yleisin tapa tunkeutua tuotantoympäristöihin on niihin rakennettujen etäkäyttöyhteyksien väärinkäyttö [1]
- Muista myös fyysinen suojaus.





[1] https://hub.dragos.com/hubfs/312-Year-in-Review/2022/Dragos_Year-In-Review-Report-2022.pdf

Menettelyt osana johtamisjärjestelmää

Väyläviraston johtamis-järjestelmä

Väyläviraston johtamisjärjestelmällä varmistetaan, että viraston toiminta tukee tavoitteiden tehokasta saavuttamista sekä eri lainsäädännöstä tulevien vaatimusten huomiointia.

Jokaisen yksittäisen johtamis- tai hallintajärjestelmän rooli on muodostaa kokonaiskuva kyseisen näkökulman hallinnan menettelyistä ja varmistaa, että ne ovat riittävät ja tarkoituksenmukaiset ko. näkökulman hallintaan.

Väyläviraston johtamisjärjestelmäkokonaisuus

Strategia

Organisaation strategia, arvot, periaatteet, tavoitteet

Hallintamallit

Riskienhallinta, jatkuvuudenhallinta, poikkeamienhallinta, osaamisen hallinta, jatkuva parantaminen, seuranta ja raportointi, muutostenhallinta, tiedonhallinta …

Toimeenpano

Työjärjestys, toimintasuunnitelma, toimintalinjat, tekniset ja turvallisuusohjeet, muut palveluntuottajille suunnatut ohjeet, hankinta- ja muut sopimukset, hankinnan ohjeistuspalvelu ja sisäiset ohjeet, toimintajärjestelmä, vastaavuustaulukot, arkkitehtuurikuvaukset, tiedonohjaussuunnitelma …

Liikennejärjestelmä → Suunnittelu → Rakentaminen → Kunnossapito → Väylien käyttö

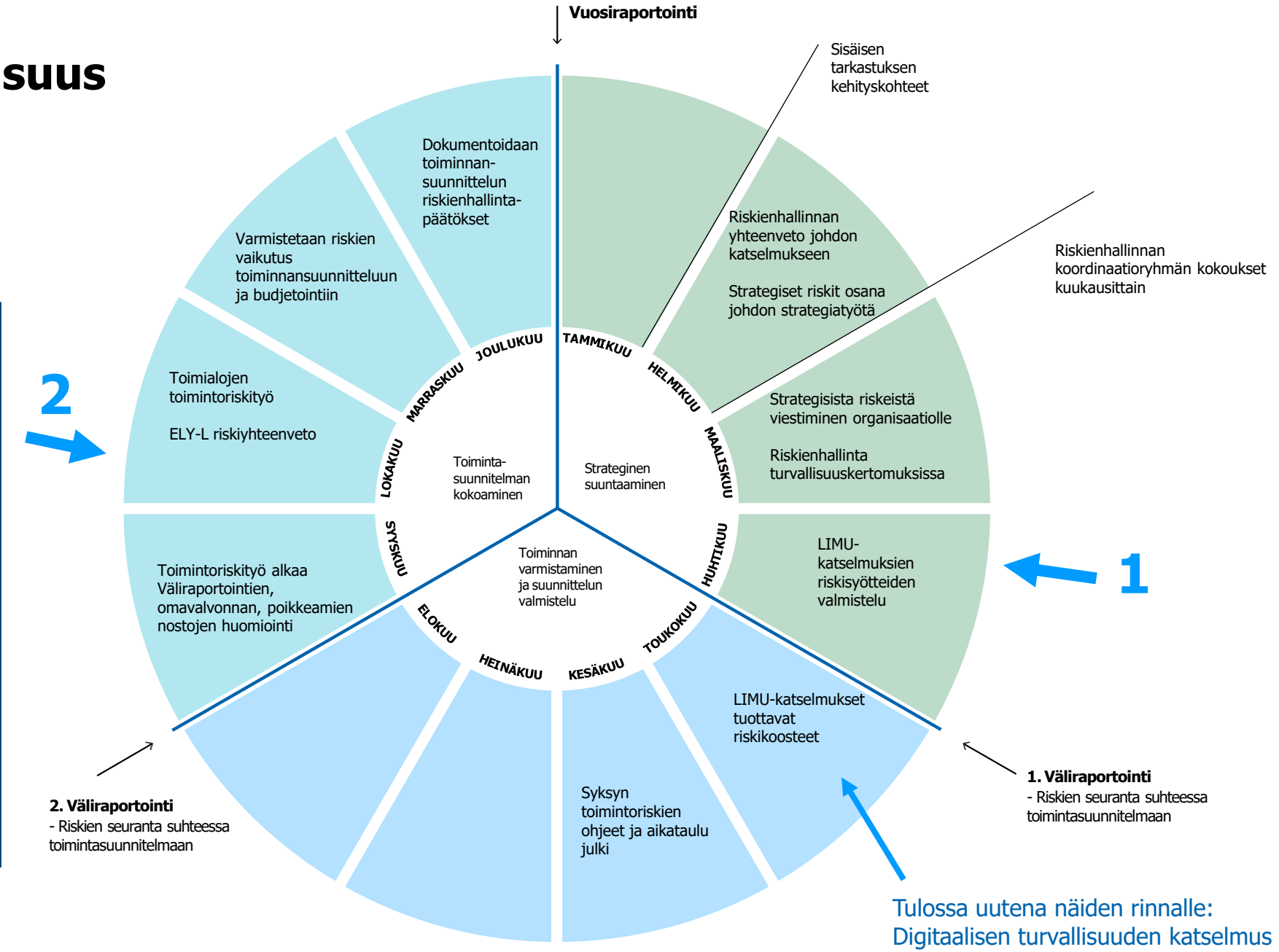
Johtamisjärjestelmät

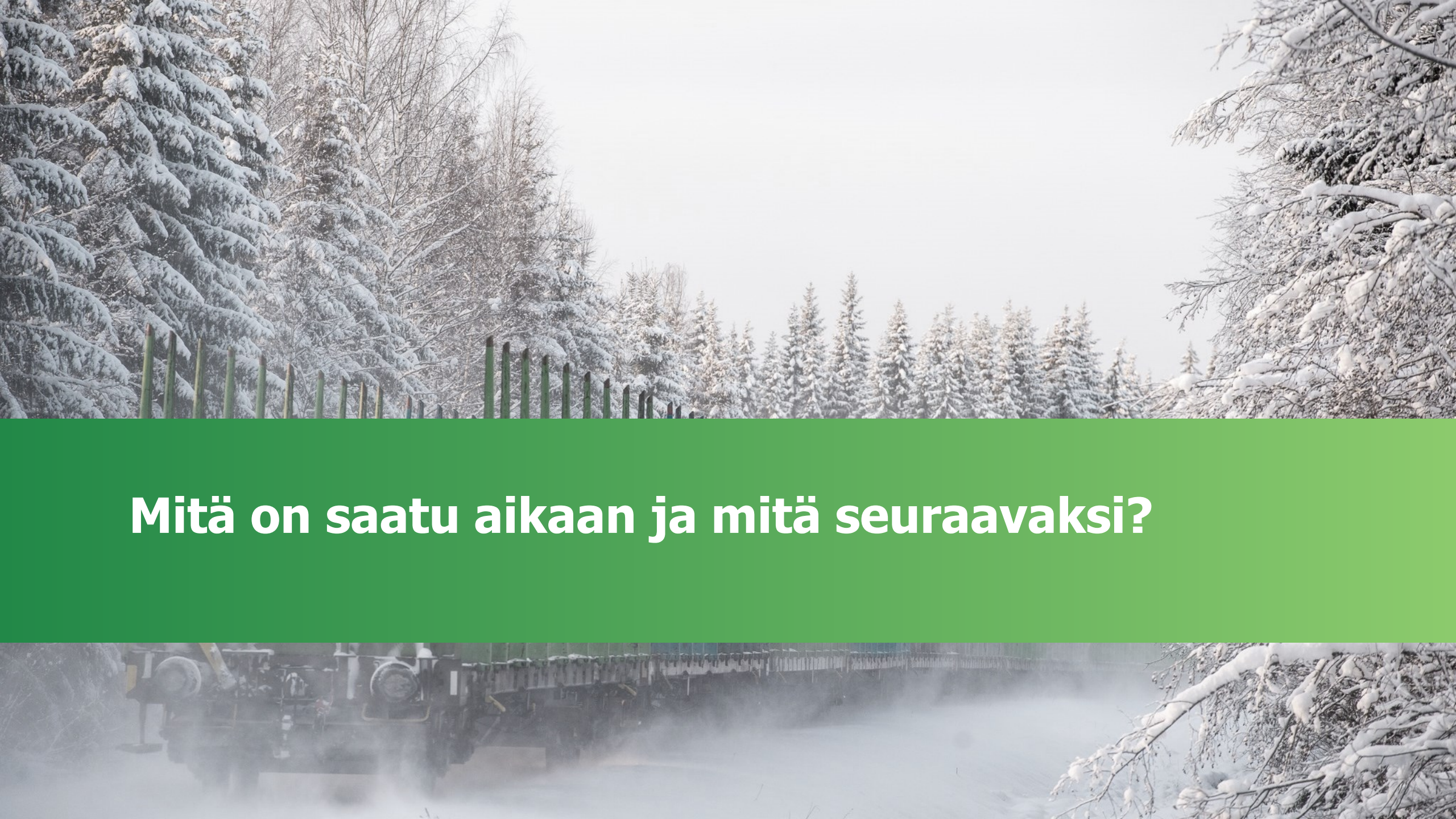
RTJJ	TPJJ	VPJJ	Tietoturva	Ympäristö	OHJ

Tieto- ja kyberturvallisuus riskienhallinnan vuosikellossa

Jatkossa toteutetaan virastotasolla tieto- ja kyberturvallisuusriskien yhteenvedon päivitys kaksi kertaa vuodessa

Rataverkon kyberturvallisuusriskit käsitellään rataverkon kyberturvallisuusohjelman ohjausryhmässä





Mitä on saatu aikaan ja mitä seuraavaksi?

Mitä on saatu aikaan?

Väylävirasto
Trafikledsverket

- Laitetilojen vaatimukset, luokittelut ja riskien arvioinnit sekä fyysisten suojausten riskiperusteinen parantaminen – useita eri tason toimenpiteitä toteutettu: mm. lukitukset ja kulunvalvonta, aitauksia, aukkojen suojauksia, ovia ja murtosuojatappeja, valvontakameroita, murto- ja palohälyttimiä
- Tietoturvavaatimuksia rataverkolle laadittu, käytäntöön vieminen käynnissä
- Järjestelmien havainnointi- ja reagointikyvykkyyden kehittäminen usean eri kokeilun avulla, myös T&K kehitystä käynnissä
- Tiivis yhteistyö Fintraffic Raiteen ja keskeisten palveluntuottajien kanssa – osaaminen kasvanut ja hyvät käytännöt jaetaan
- Riskienhallinnan menettelyt sovittu, käytäntöön vieminen käynnissä
- Digiradassa laadittu mm. kattava Cyber Security Management Plan

2025 tärkeimmät kehitysalueet

Väylävirasto
Trafikledsverket

- Tietoliikenneverkon poikkeamien havainnointi- ja reagointikyvykkyyden edelleen kehittäminen
- Kyberriskienhallinnan menettelyjen vakiinnuttaminen turvalaite- ja tietoliikennemuutosprojekteihin
- BugBounty-ohjelman käynnistäminen
- Omaisuudenhallinnan jatkokehittäminen kyberturvallisuuden kannalta

+ muuta kehittämistä, jota ei voi tässä julkisessa aineistossa kuvata tarkemmin

Väylävirasto
Trafikledsverket