TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Vastuut toimitusketjussa

#DigiSignaali23
30.11.23

Toimitusketju voi muodostaa kyberturvallisuusriskin

- Toimitusketjuhyökkäyksissä yritykseen tai julkiseen organisaatioon yritetään tunkeutua yhteistyökumppanin tai alihankkijan kautta.
- Kohteena ovat varsinaisen kohdeyrityksen yhteistyökumppanit, kuten tavarantoimittajat, huoltoyhtiö tai palveluntuottaja.
- Ensin murtaudutaan yhteistyökumppanin verkkoon, minkä jälkeen voidaan edetä kohdeyrityksen verkkoa kohti.
- Konkreettinen uhka, jossa yrityksen ja toimittajan välistä luottamussuhdetta käytetään hyväksi.
- Riskiä ei voi hoitaa sisäisesti. On tärkeää yhteistyössä varmistaa, että koko ketjun turvallisuus on kunnossa.

”Kyberturvallisuus on harvemmin enää vain yhden organisaation sisäinen asia”

”Suomalaistenkin organisaatioiden kannattaa varautua tähän kasvavaan kyberuhkaan.”

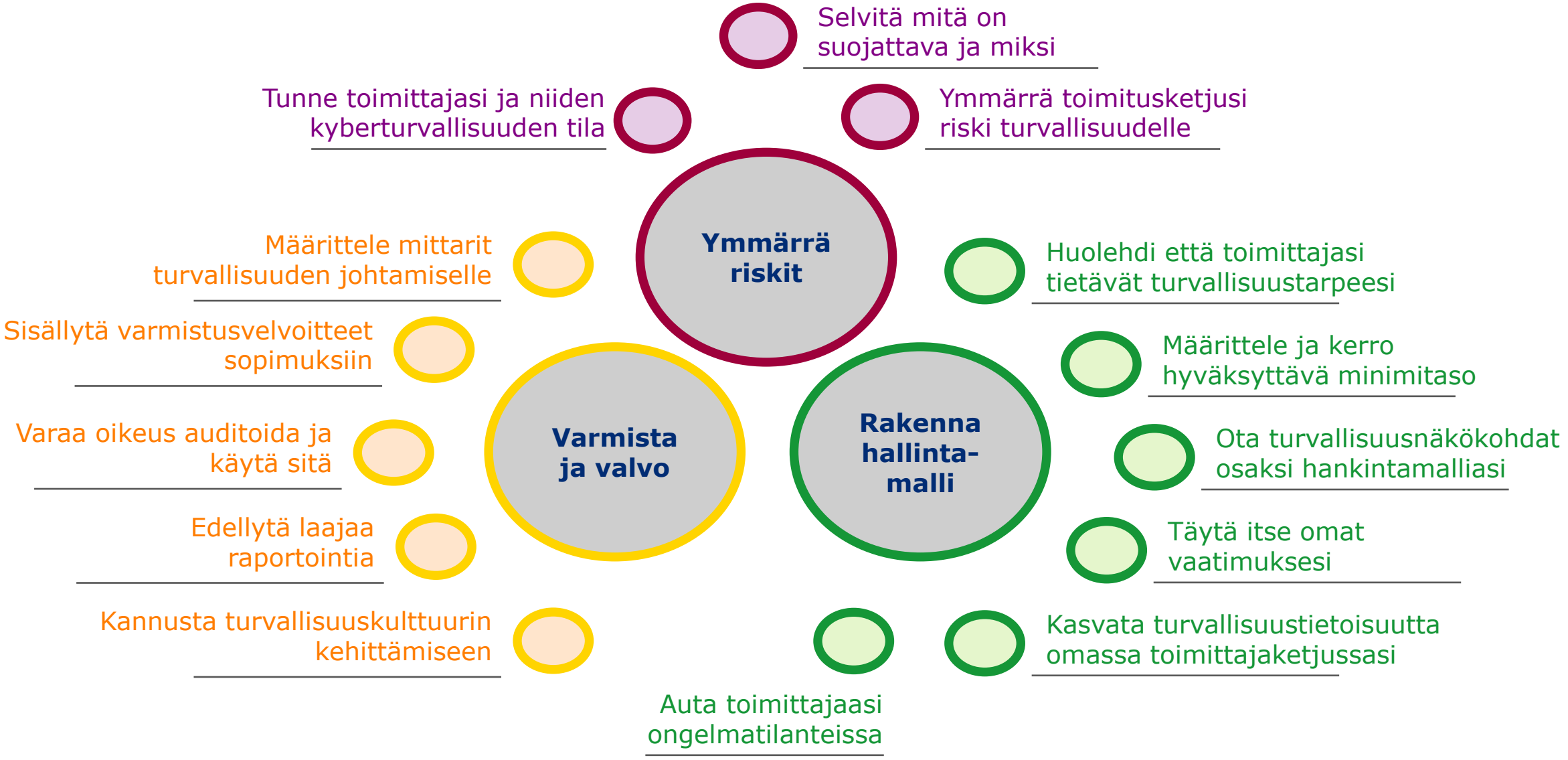
- SUPO (2021)

https://supo.fi/-/kolumni-onko-organisaatiosi-suojautunut-toimitusketjuhyokkaykselta-nailla-vinkeilla-paaset-alkuun

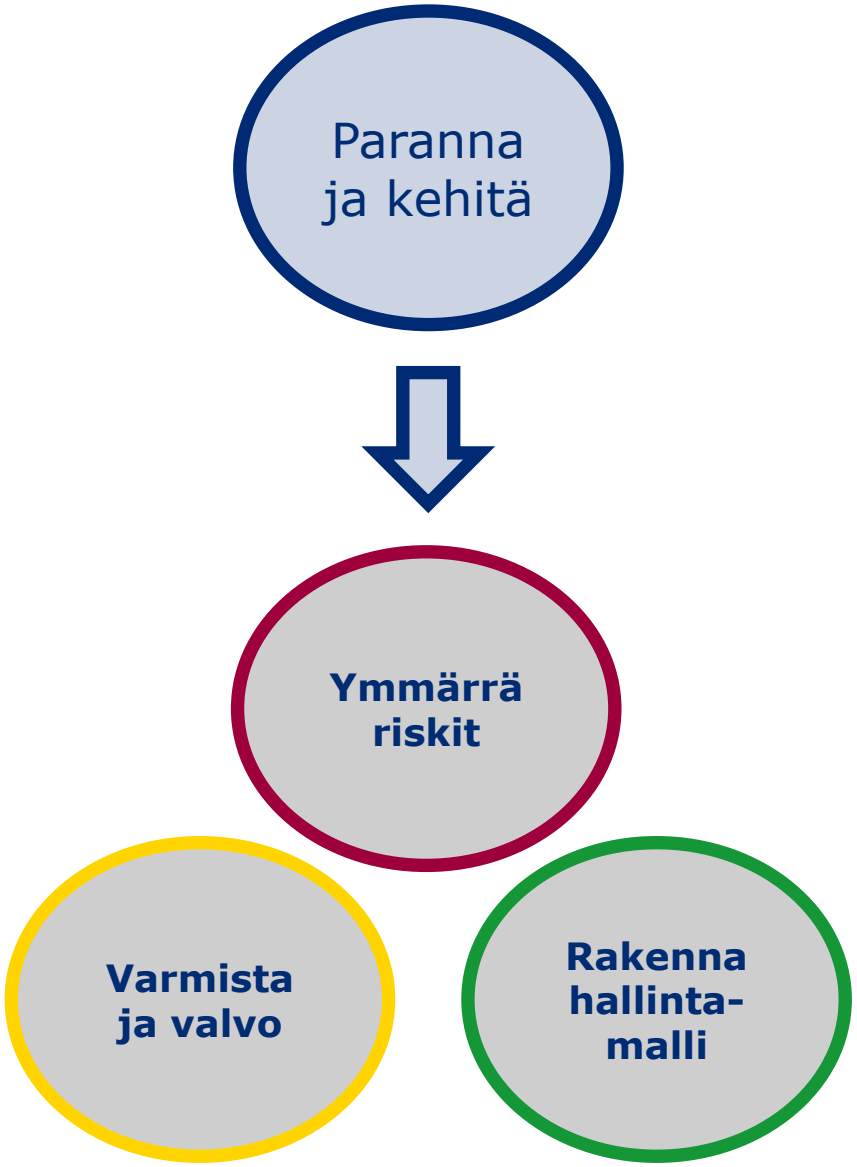
Toimitusketjun turvallisuuden hallinta

https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security

Toimitusketjun turvallisuuden hallinta



https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security



Kerää kokemukset, opi ja reagoi

Kannusta toimittajiasi turvallisuuden ylläpitoon ja kehittämiseen

- Kasvata ja kouli toimittajakuntaa, palkitse toimenpiteistä
- Anna tukea
- Jousta vaatimuksissa, katso tuloksia
- Ole valmis muuttamaan lähestymistapaa jos valittu toimintamalli ei toimi tavoitteiden mukaan.

Rakenna luottamusta

- Hae kumppanuutta
- Ole avoin ja palkitse avoimuudesta
- Huomioi toimittajan tarpeet

https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security

Kriittiset menestystekijät toimitusketjujen riskienhallinnassa:
(NIST C-SCRM mukaan)

1. Toimitusketjujen riskienhallinta osaksi kaikkia hankintatoimenpiteitä
2. Keskeisten suositeltujen riskien hallintakeinojen käyttöönotto organisaatioissa (niiden perustasolla)
3. Vuorovaikutus ja tietojen jako toimitusketjuissa ja verkostoissa
4. Tietoisuuden kasvattaminen, harjoittelu ja koulutus
5. Riskienhallinta on investointi: perusteltava konkreettisilla tavoitteilla, joiden saavuttamista mitataan (sekä itse kyvykkyydet, että kehityshanke)
6. Tarvittavan rahoituksen ja resurssien varmistaminen

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

Kampanja numeroina

150
osallistujaa

2313
toimittajaa tarkastettiin

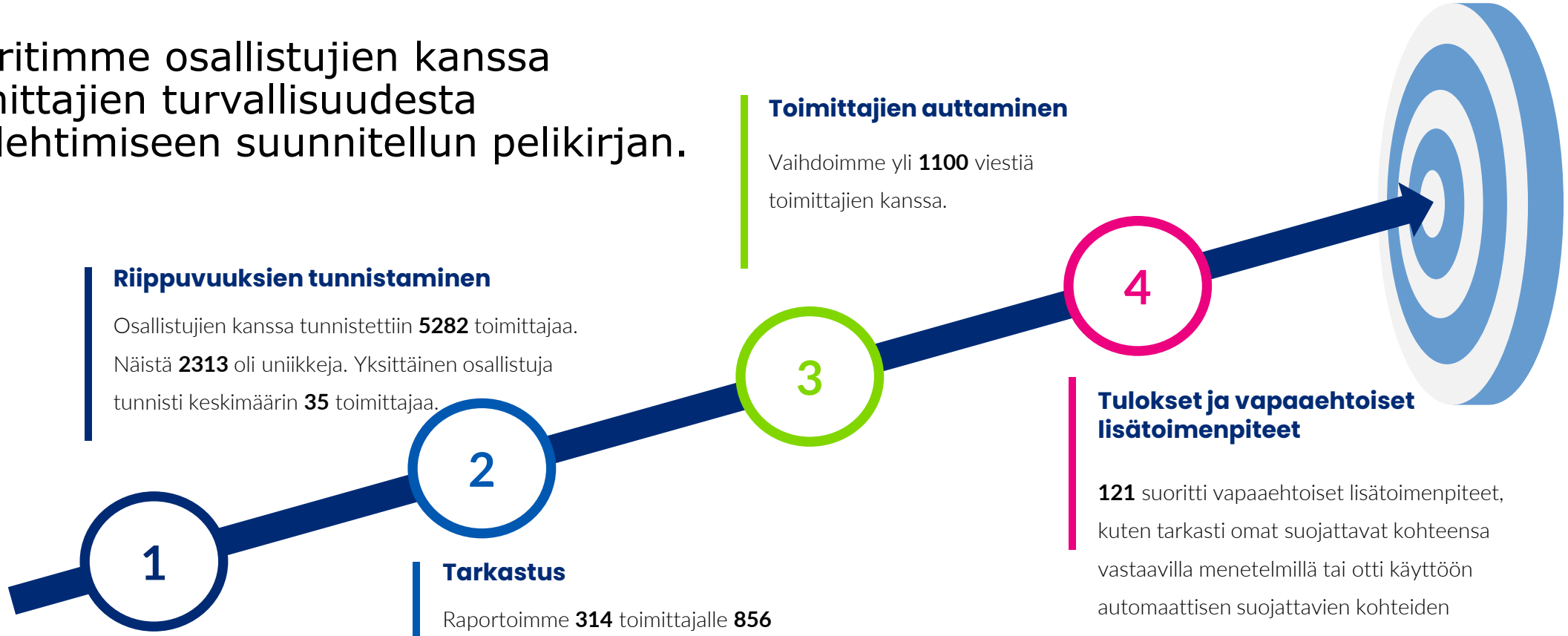
856
havaintoa raportoitiin

Ketjutonttu
–menetelmäkokeilu keskinäisriippuvuuksien kyberturvallisuusriskien vähentämiseksi

- Yhteistyökampanja suomalaisille organisaatioille 2023
- Osallistujat saivat maksuttoman toimitusketjujen tietoturvan tarkastuksen
- Toimittajat saivat raportit haavoittuvuuksista ja apua korjauksiin
- Luokittelimme toimittajat A/B/C-kategorioihin reagoinnin ja vasteen perusteella
- Huoltovarmuuskeskus rahoitti kampanjan

Ketjutontun pelikirja – tilastot eri vaiheista

Suoritimme osallistujien kanssa toimittajien turvallisuudesta huolehtimiseen suunnitellun pelikirjan.



Riippuvuuksien tunnistaminen

Osallistujien kanssa tunnistettiin **5282** toimittajaa. Näistä **2313** oli uniikkeja. Yksittäinen osallistuja tunnisti keskimäärin **35** toimittajaa.

Tarkastus

Raportoimme **314** toimittajalle **856** yksittäistä havaintoa

Toimittajien auttaminen

Vaihdoimme yli **1100** viestiä toimittajien kanssa.

Tulokset ja vapaaehtoiset lisätoimenpiteet

121 suoritti vapaaehtoiset lisätoimenpiteet, kuten tarkasti omat suojattavat kohteensa vastaavilla menetelmillä tai otti käyttöön automaattisen suojattavien kohteiden tiedonjaon Kyberturvallisuuskeskuksen kanssa.

Miten toimittajat suoriutuivat?

https://www.kyberturvallisuuskeskus.fi/fi/tonttu

Yhteenveto

- Vastuullisuus toimitusketjussa on: omasta kyberturvallisuudesta huolehtimista, asiakkaan omaisuuden suojaamista, avointa vuorovaikutusta ja turvallisuuskulttuurin kehittämistä.
- Toimitusketjujen digitaalinen turvallisuus ei ole yksin IT:n ongelma. Tärkeää on huomioida hankintamallit, toimittajahallinta, jatkuvuudenhallinta ja laatu toimitusketjussa.
- Yksinkertaisilla työkaluilla ja etenemällä vaihteittain pääsee alkuun.
- Riskiä ei voi hoitaa sisäisesti. On tärkeää yhteistyössä varmistaa, että koko ketjun turvallisuus on kunnossa.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kiitos