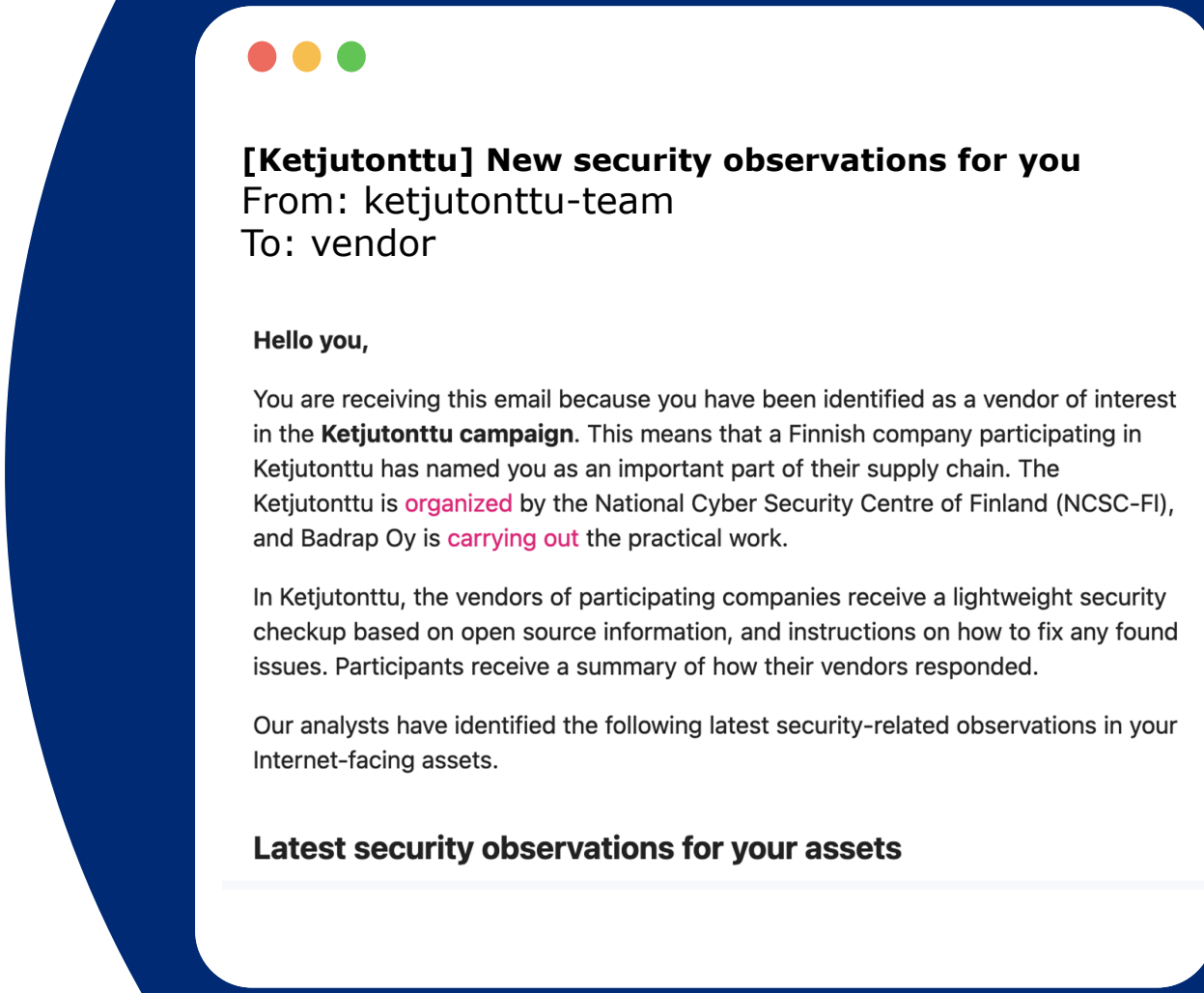
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Ketjutonttu

Näin paransimme yhdessä toimitusketjujen tietoturvaa



Toimitusketjujen auttaminen kannattaa

WithSecure

Jani Kenttälä

("Ketjutonttu" project sponsored by NCSC-FI and National Emergency Supply Agency)

Twitter
LinkedIn

Hall of Fame year 2023

WithSecure would like to thank and recognize the following security researchers who have helped make our products and services safer by reporting valid security vulnerabilities through our public Vulnerability Reward Program.

F5

Support Solution

K75282801: F5 SIRT Security Researcher Acknowledgement

Published Date: May 12, 2020 Updated Date: Aug 18, 2023

SECURITY INCIDENT RESPONSE TEAM

The F5 Security Incident Response Team (**F5 SIRT**) would like to acknowledge Security Researchers who follow responsible disclosure practices when reporting potential vulnerabilities and security-related concerns found in F5 corporate infrastructure.

F5 would like to thank the following people for helping us keep our environments safe and secure.

2023 disclosures

Name	Date
Kasper Kyllonen of Ketjutonttu project sponsored by NCSC-FI and National Emergency Supply Agency of Finland	April 2023

PHILIPS

Philips coordinated vulnerability disclosure Hall of Honors

Philips would like to recognize and thank all the researchers who have submitted a vulnerability report and cooperated with us. For those who want to be listed in our Hall of Honors we will list the first reporter of a new acknowledged vulnerability. Thanks to all for their participation, and have made a disclosure to us to help keep the internet and our customers and patients safe.

2023 HOH

Hall of Honors

- Juho Räsänen (LinkedIn Profile: rjuho)
- Vinit Lakra (LinkedIn Profile: Vinithacker)
- Navreet (Linkedin Profile :- navreet-singh-rnns142500)
- Adarsh S Nair (LinkedIn profile :-@Adarsh S Nair)
- Abhishek Maurya (LinkedIn profile :-abhiishsec, Twitter Profile :-abhiishsec)
- Ahmed Ramzy (LinkedIn Profile: ARamzy05)

BOSCH

Hall of Fame Bosch Websites

2023

Kasper Kyllönen

Subdomain Takeover

Ramkrishna Sawant (Ramkrishna Sawant)

Information Disclosure

Chirag Ketan Prajapati (Chirag Ketan Prajapati)

2x *Cross-Site Scripting*

Dawid Cieśla (Dawid Cieśla)

Cross-Site Scripting

Blakduk (Blakduk)

Information Disclosure

Kampanja numeroina

150
osallistujaa

2313
toimittajaa tarkastettiin

856
havaintoa raportoitiin

Mikä Ketjutonttu?

- Yhteistyökampanja suomalaisille organisaatioille
- Osallistujat saivat maksuttoman toimitusketjujen tietoturvan tarkastuksen
- Toimittajat saivat haavaraportit ja apua korjauksiin
- Luokittelimme toimittajat A/B/C-kategorioihin heidän vasteensa perusteella
- Huoltovarmuuskeskus rahoitti kampanjan
- Käytännön toimenpiteet toteutti yhdessä Liikenne- ja Viestintävirasto Traficomin Kyberturvallisuuskeskus ja Badrap Oy

Mikä Tonttu?

- Menetelmä selvittää, voiko organisaatioiden turvallisuutta parantaa kevyillä menetelmillä
- Tapa tavoittaa myös uutta yleisöä, joka ei ennestään tunne Kyberturvallisuuskeskusta

PASSIIVINEN YHTEISTYÖ

Otamme yhteyttä kun jotain on jo sattunut - jos tunnistamme teidät.

SATUNNAINEN YHTEISTYÖ

Esimerkiksi: osallistut ISAC-toimintaan, kerrot meille mitä suojattavat kohteesi ovat, tai luovutat lokitietoja analysoitavaksi.

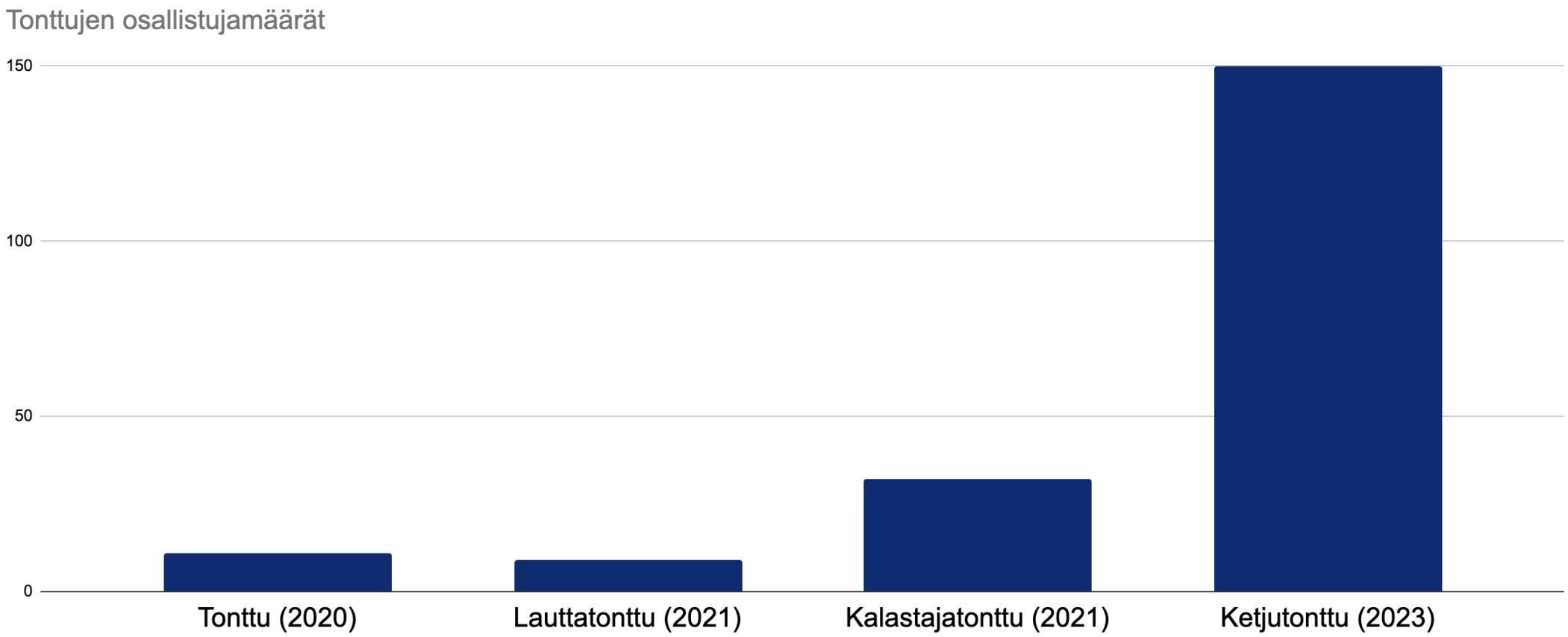
AUTOMATISOITU YHTEISTYÖ

Vähintään yksi yhteistyötä automatisoiva kyvykkyys käytössä.
Esimerkiksi: pilvipalveluiden tunnistaminen tai kevyet yhteistyösensorit.

HAVARO 2

SOC-tilaus, järeät sensorit ja salaiset tunnisteet.

Ketjutonttu harppasi uudelle tasolle tavoitettavuudessa



Yhteistyön skaalaaminen ja uusien osallistujien tavoittaminen – Ketjutontun Suomen kiertue

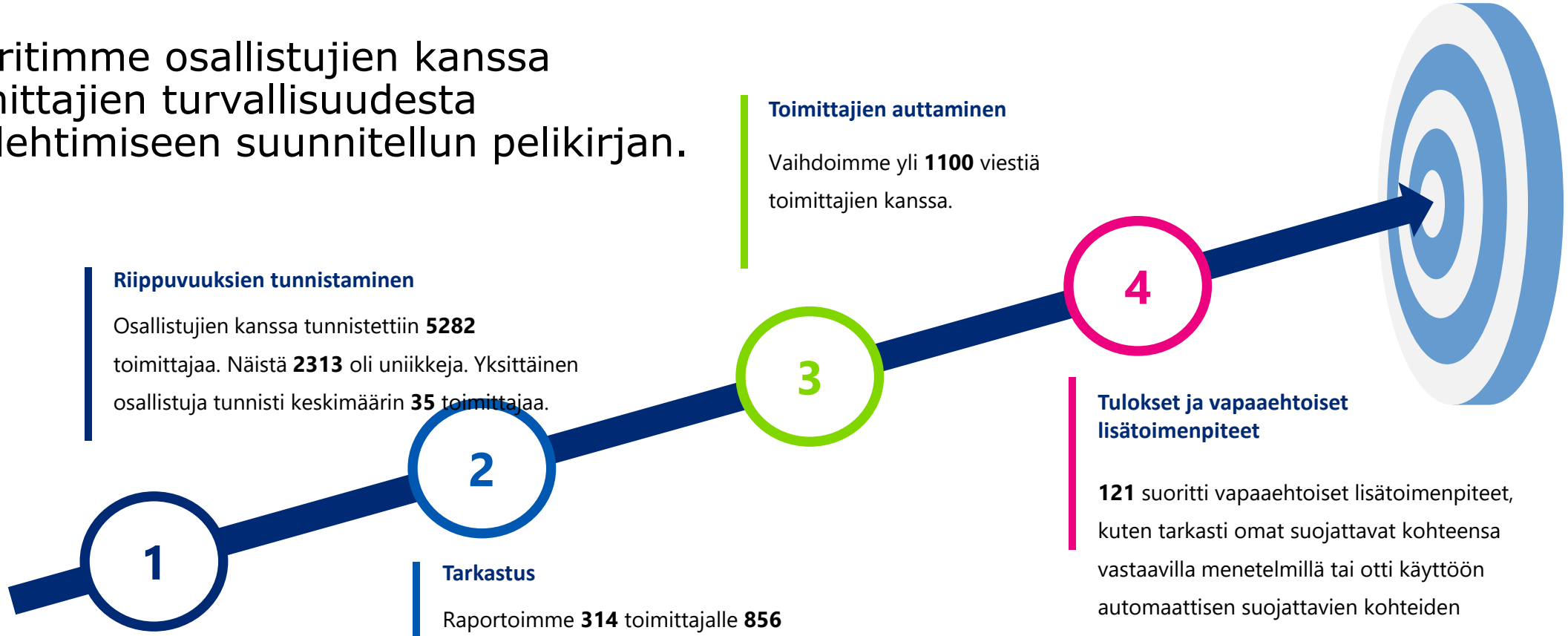
- 21.3. Oulu - Tietoturvamerkki-tapahtuma
- 23.3. Kotka - Kybertuska-tapahtuma sekä Saksalais-Suomalaisen Kauppakamarin jäsenwebinaari
- 24.3. Internet - Viikkokatsaus 12/2023
- 13.4. Internet - Kybersää
- 18.4. Tampere - Tietoturvamerkki-tapahtuma
- 25.4. Jyväskylä - Tietoturvamerkki-tapahtuma
- 3.5. Internet - Verkkokauppojen turvallisuus ja tiedonantovelvoite -webinaari
- 11.5. Internet – Kybersää
- 19.5. Internet - Viikkokatsaus 20/2023
- 23.5. Oulu - Yliopistojen tietoturvapäivät
- 10.8. Internet - Kybersää (heinäkuussa)

Lisäksi:

- Huoltovarmuuskeskuksen tiedotteet organisaatioille
- Kyberturvallisuuskeskuksen ja Badrap Oy:n sosiaalisen median viestintä
- Badrap Oy:n soittokampanja uusien organisaatioiden tavoittamiseksi (⅓ osallistujista)

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.

Toimitusketjujen kartoitukset

- Keskimäärin 35 toimittajaa / osallistuja
- Osalla oli aluksi mielessä muutama toimittaja. Listaa laajennettiin esimerkiksi keskustelemalla, käyden läpi toimittajatyyppejä sekä teknisillä menetelmillä (whois/DNS/TLS-tiedot)
- Toisilla oli valmis toimittajalista joista poimittiin tärkeimmät tarkastuksiin.

50+ riippuvuutta	1 toimittaja
20-50 riippuvuutta	13 toimittajaa
10-19 riippuvuutta	52 toimittajaa
5-9 riippuvuutta	134 toimittajaa

Toimitusketjujen kartoitukset

- Top 10 listalla 8/10 yrityksistä oli kotimaisia. Kaksi ulkomaalaista yritystä olivat ohjelmistoyrityksiä.
- 3 taloushallinnon yritystä
- 3 teleoperaattoria
- 2 ohjelmistoyritystä
- 1 pankki
- 1 terveydenhuolto

Toimittaja 1	78 riippuvuutta	52% osallistujista
Toimittaja 2	49 riippuvuutta	33% osallistujista
Toimittaja 3	49 riippuvuutta	33% osallistujista
Toimittaja 4	39 riippuvuutta	26% osallistujista
Toimittaja 5	33 riippuvuutta	22% osallistujista
Toimittaja 6	31 riippuvuutta	21% osallistujista
Toimittaja 7	30 riippuvuutta	20% osallistujista
Toimittaja 8	29 riippuvuutta	19% osallistujista
Toimittaja 9	29 riippuvuutta	19% osallistujista
Toimittaja 10	29 riippuvuutta	19% osallistujista

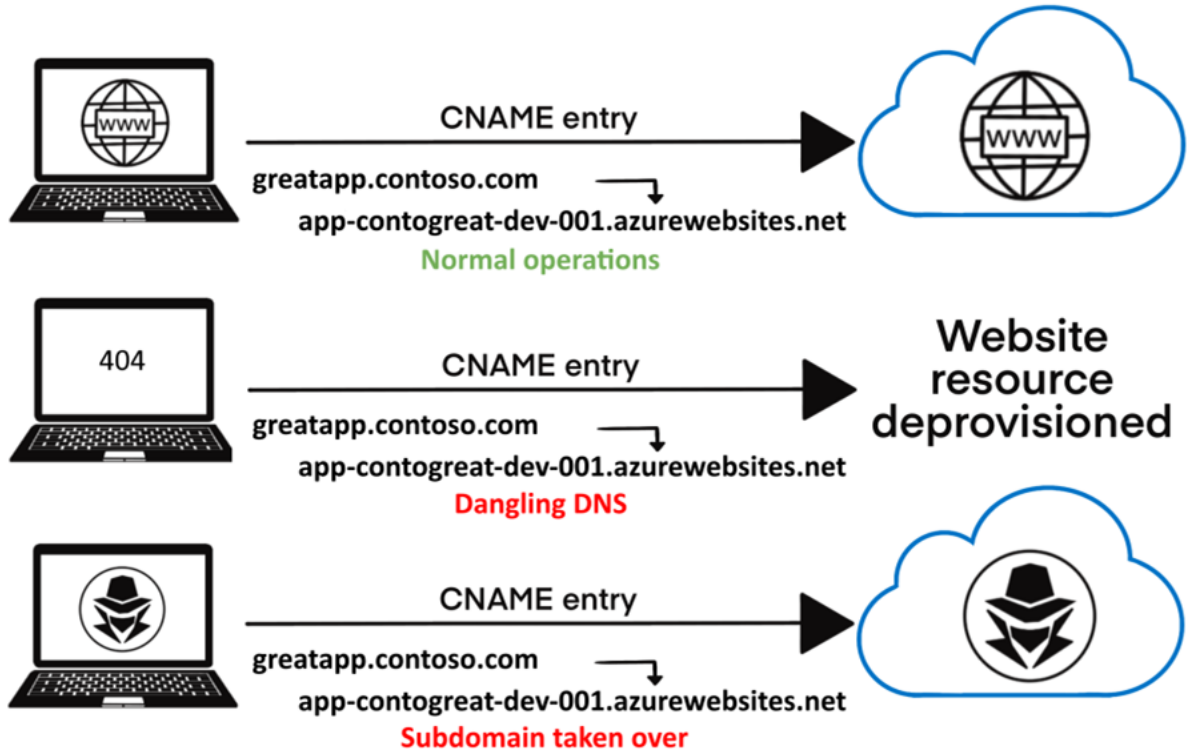
Tarkastusmenetelmät ja havainnot

Joka seitsemännellä toimittajalla oli korjattavaa

Havaintotyyppi	Monellako toimittajalla havaittu
Alidomainin haltuunottoriski (tai vaarattomampi vanhentunut nimipalvelutietue)	114
Vanhentuneet palvelimet ja palvelut	119
Altistuneet verkkopalvelut (tietokannat, etähallinnat, tiedostonjaot)	185

Alidomainin haltuunotto

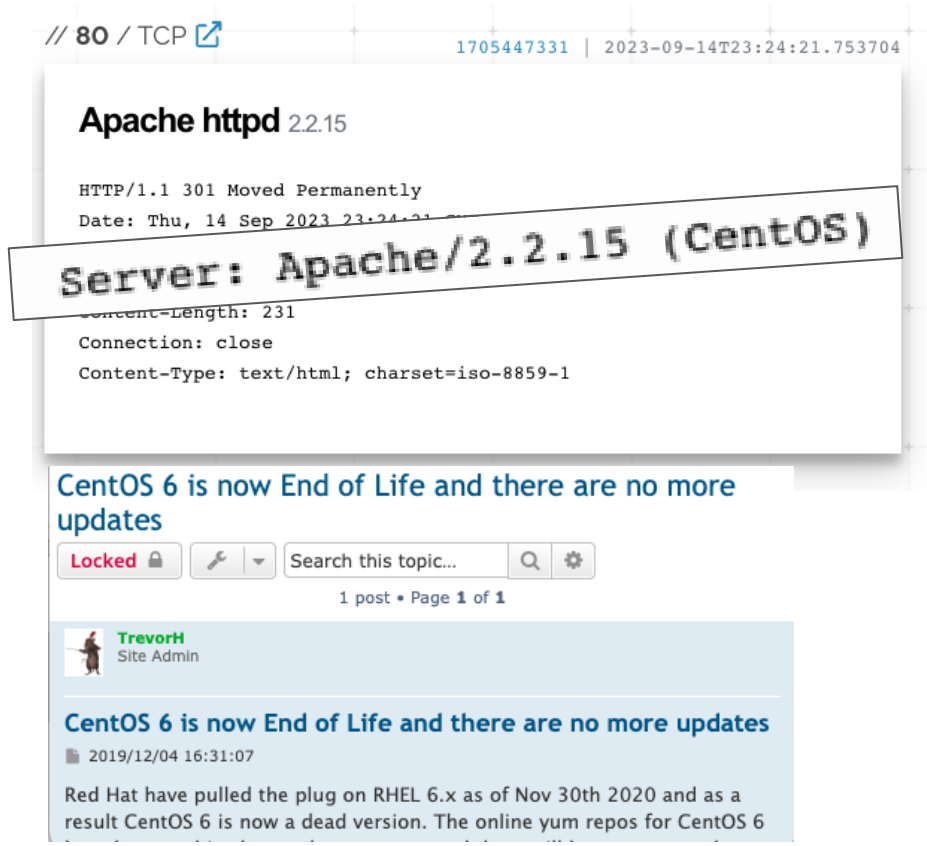
- Yrityksen domain osoittaa pilvipalveluun tai muuhun vuokrattavaan resurssiin
- Nimi, johon domain osoittaa ei ole enää yrityksen käytössä
- Rikollinen ottaa käyttämättömän pilviresurssin haltuunsa
- Rikollinen väärinkäyttää uhrin domainia erilaisissa hyökkäyksissä



https://learn.microsoft.com/en-us/azure/security/fundamentals/subdomain-takeover

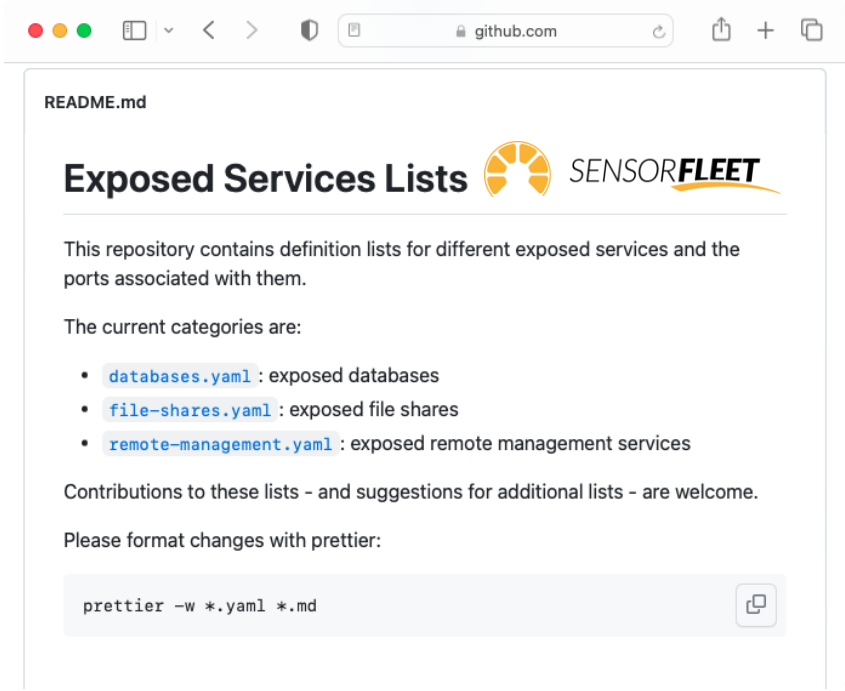
Vanhentuneet palvelimet ja palvelut

- Tarkastimme tiettyjen palveluiden versionumerot
- Päättelimme versionumeroista käytetyn Linux-jakelun tai Windows-version (“alusta”)
- Varoitimme toimittajia, mikäli alusta on niin vanha, että siihen ei saa tietoturvapäivityksiä, tai päivityksien saamiseksi pitää nähdä erityistä vaivaa.



Altistuneet verkkopalvelut

- Skannataan pahimmat ja selkeimmin vahingossa tehdyt altistumiset
- Yhteydenottotesti - emme esimerkiksi tarkastaneet, ovatko altistuneiden tietokantojen tiedot helposti varastettavissa



https://github.com/sensorfleet/exposed-services/tree/main

Palvelu	Yksittäisiä havaintoja
3306 (MySQL/MariaDB)	72
3389 (RDP)	31
5432 (PostgreSQL)	17
…	…
541 (Fortigate Management)	7
Others	58

Raportointi

Vastaanottajan löytäminen

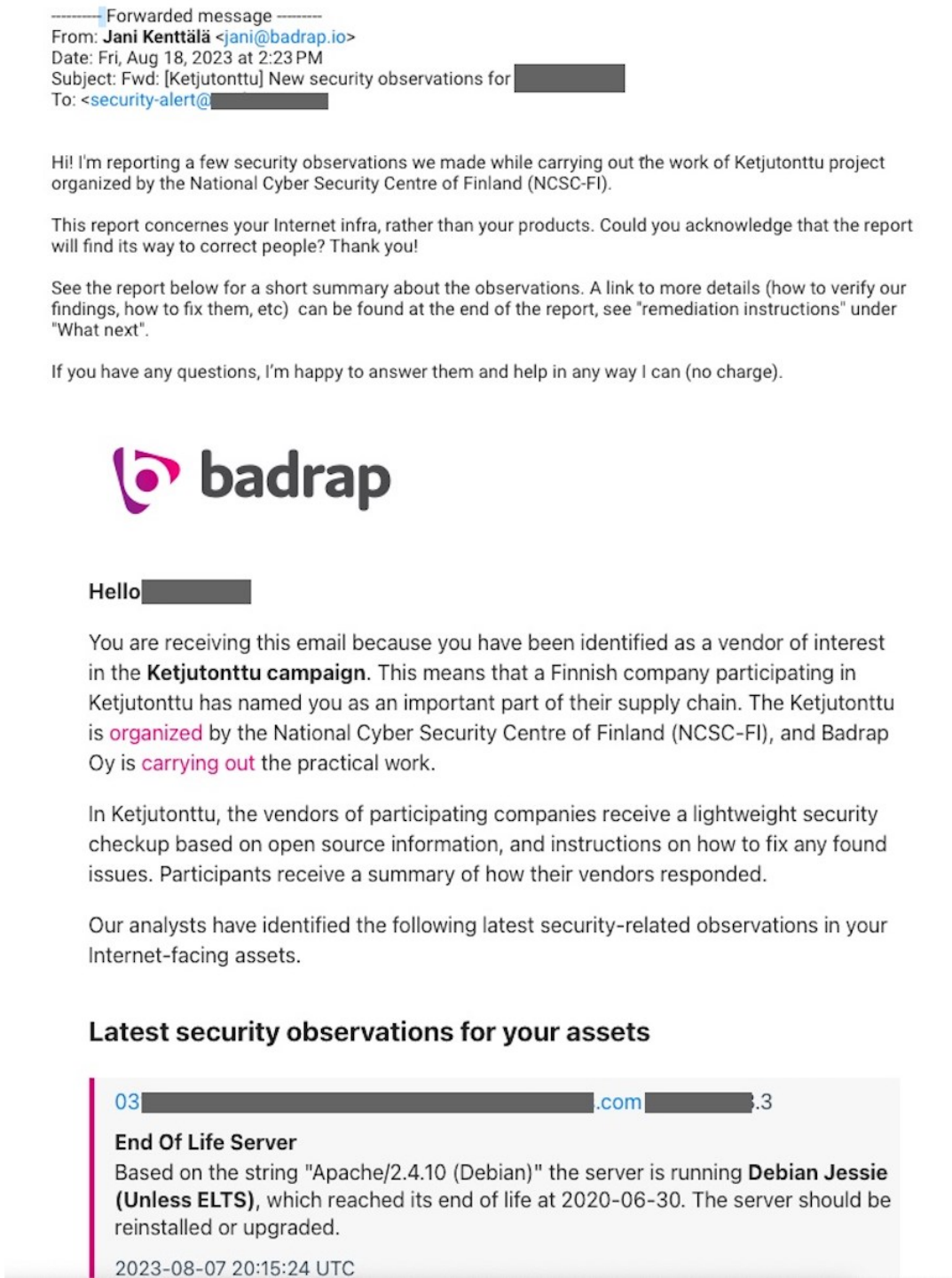
- security.txt - 7% toimittajista
- WWW-sivut
- LinkedIn-roolit
- Yleiset info/contact/support -sähköpostiosoitteet

Vastaanottaja voi pelätä että olet

- “Beg bounty” -metsästäjä
- Myymässä jotain
- Huijari ylipäätään
- Et tärkeä
- Haavapalkkio-ohjelmat ovat oma lukunsa
  - Palkkioon perustuva prosessi vaatii raportoijaa käyttämään enemmän aikaa per tapaus
  - Ketjutonttu keskittyi minimoimaan raportointiin liittyvän ajankäytön (vaarantamatta raportoinnin laatua liikaa)

Raportointi

- Lisää ripaus ihmistä mukaan raportteihin
- Selitä konteksti - miksi raportoija on tehnyt tarkastukset
- Kerro kaikki mitä tiedät
- Ole valmis vastaamaan kysymyksiin
- Seuraa ja tue



---------- Forwarded message ---------
From: **Jani Kenttälä** <jani@badrap.io>
Date: Fri, Aug 18, 2023 at 2:23 PM
Subject: Fwd: [Ketjutonttu] New security observations for [redacted]
To: <security-alert@[redacted]

Hi! I'm reporting a few security observations we made while carrying out the work of Ketjutonttu project organized by the National Cyber Security Centre of Finland (NCSC-FI).

This report concernes your Internet infra, rather than your products. Could you acknowledge that the report will find its way to correct people? Thank you!

See the report below for a short summary about the observations. A link to more details (how to verify our findings, how to fix them, etc) can be found at the end of the report, see "remediation instructions" under "What next".

If you have any questions, I'm happy to answer them and help in any way I can (no charge).

badrap

Hello [redacted]

You are receiving this email because you have been identified as a vendor of interest in the **Ketjutonttu campaign**. This means that a Finnish company participating in Ketjutonttu has named you as an important part of their supply chain. The Ketjutonttu is organized by the National Cyber Security Centre of Finland (NCSC-FI), and Badrap Oy is carrying out the practical work.

In Ketjutonttu, the vendors of participating companies receive a lightweight security checkup based on open source information, and instructions on how to fix any found issues. Participants receive a summary of how their vendors responded.

Our analysts have identified the following latest security-related observations in your Internet-facing assets.

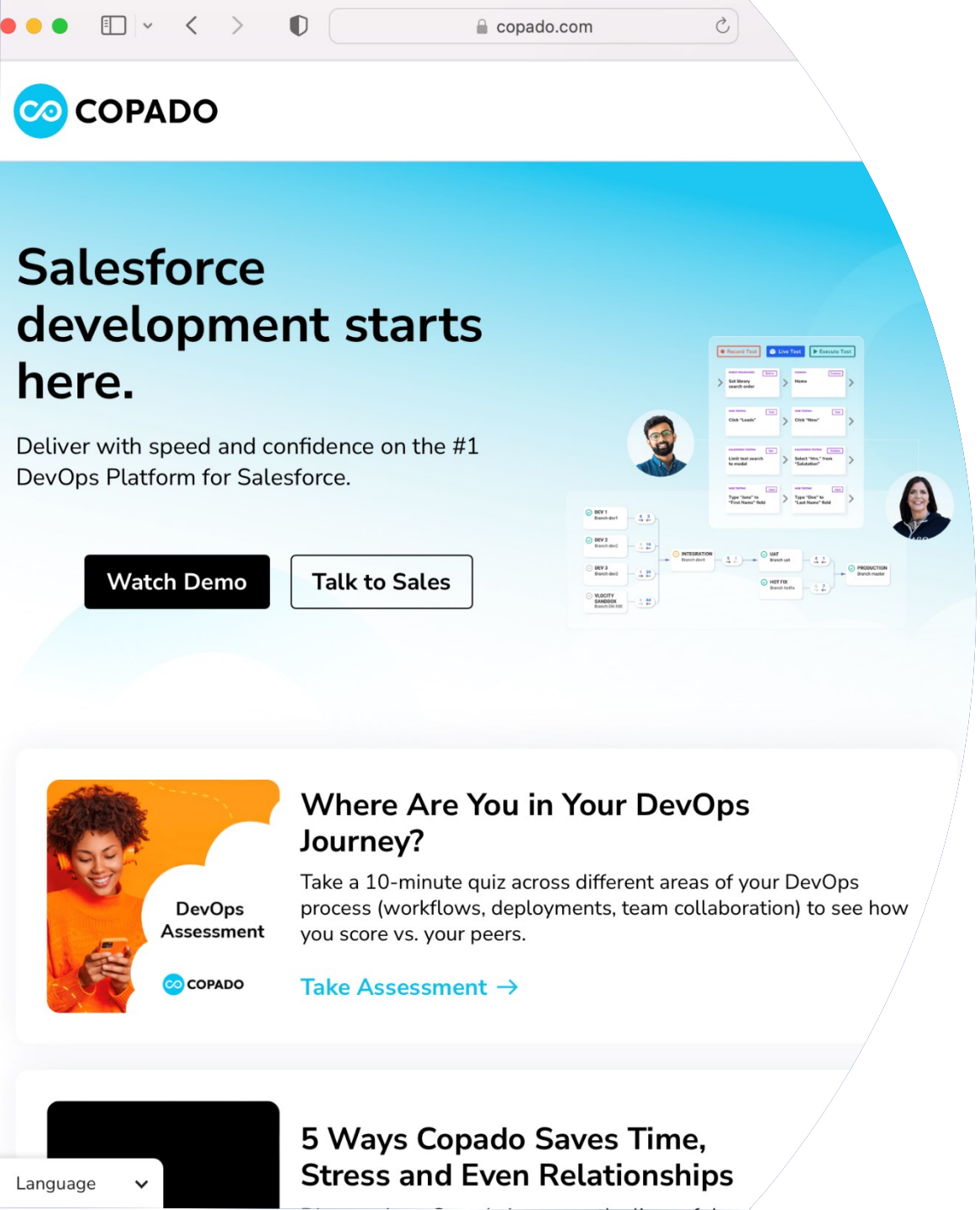
Latest security observations for your assets

03[redacted].com[redacted].3

End Of Life Server
Based on the string "Apache/2.4.10 (Debian)" the server is running **Debian Jessie (Unless ELTS)**, which reached its end of life at 2020-06-30. The server should be reinstalled or upgraded.

2023-08-07 20:15:24 UTC

TRAFICOM



Thank you for reporting this, our team has looked into it and resolved the issue.

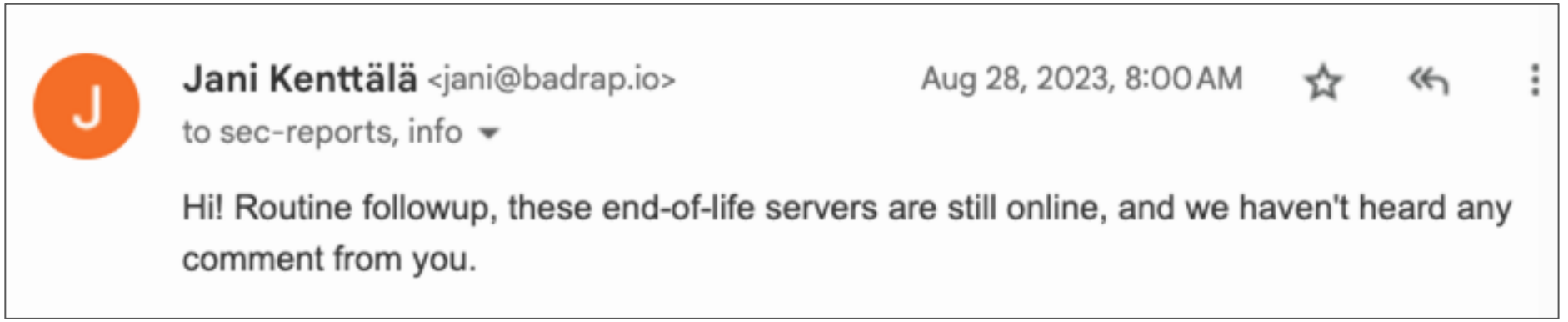
Also - our team thoroughly appreciated how well-written and polite your report was!

Thanks and please pass our regards to the chain elf,

The Copado Security Team

Auttaminen

- 95% ajasta sinnikästä seurantaa - ole toimittajan tiketöinti- ja muistutusjärjestelmä
- Auta toimittajaa selvittämään ongelma heidän toimittajalleen
- Keskustele toimittajan kanssa heidän omasta riskiarviostaan - arvio on saattanut perustua väärään tietoon



Miten toimittajat suoriutuivat?

- A - Korjaa ongelmat nopeasti ja viestii selkeästi
- B - Ottaa ongelmat vakavasti, mutta korjaukset vievät aikaa
- C - Ei vastaa eikä korjaa - tai vastaa, mutta vastaus ei käy järkeen
- OK - Ei havaintoja, ei vasteen mittausta -> ei luokitella
- Toimittajien luokitukset jakautuivat seuraavasti:

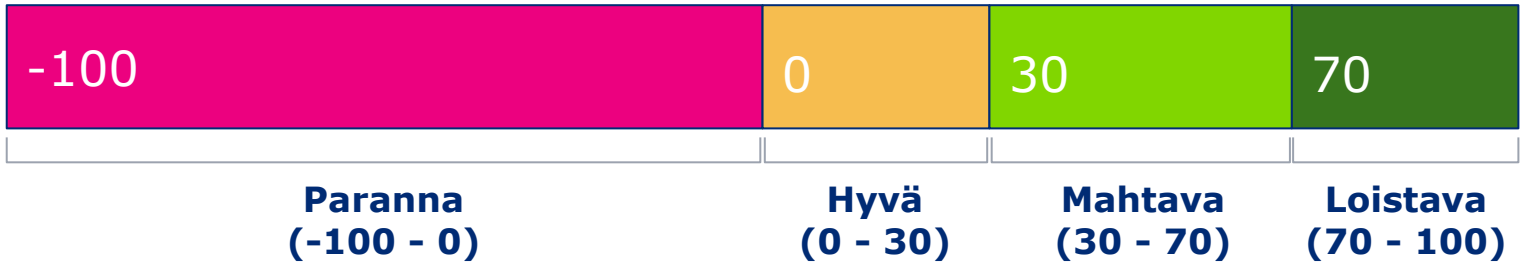
A	B	C	OK
98	95	121	1999

Toimittajien stereotyypit

- A: Ammattilainen - kertoo korjaavansa, korjaa, kertoi että korjasi (sisältää myös hyvin toimivat haavapalkkio-ohjelmat)
- A: Sinnikäs metsästäjä - ei lepää ennen kuin ongelma on ratkaistu
- B: Hitaanpuoleinen organisaation koon vuoksi
- B: Hitaanpuoleinen, koska elinkaarisuunnittelu puuttuu
- B: Hitaanpuoleinen haavapalkkio-ohjelman takia
- C: Hiljainen toimittaja
- C: “Ongelmaa ei ole” -selitys ei käy järkeen
- C: Ongelma jumittaa haavapalkkio-ohjelman prosessiin koska emme demonstroi haavoittuvuuden hyödyntämistä

Miten osallistujat suhtautuivat Ketjutonttuun?

- Keräsimme palautetta kyselylomakkeen avulla syyskuun 2023 aikana
- 30.9.2023 mennessä kyselyyn vastasi 18% osallistujista
- Tonttu-kampanjat pyrkivät löytämään uusia yhteistyöorganisaatioita. Organisaatioiden suositukset toisilleen auttavat tässä tavoitteessa.
- Kysyimme osallistujien halukkuutta suositella Ketjutonttua muille ja laskimme palautteesta ns. Net Promoter –pisteet (NPS).



Osallistujat antoivat loistavaa palautetta

- Net Promoter Score (NPS) = 81.
- Palautekysymykseen “Suosittelisitko Tonttu-kampanjoita tuttavillesi?” 85% vastanneista antoi asteikolla 0-10 arvosanan 9 tai 10.
- Vastaavia lukuja saavat vain maailman huippubrändit esimerkiksi B2B-ohjelmistopalveluiden kategoriassa.
- Kysyimme myös asteikolla 1-10, kuinka mielekästä toimitusketjujen kartoittaminen oli. Osallistujien vastausten keskiarvoksi muodostui 9, erinomainen.

Erinomainen

81

Osallistujien palautetta

- *Hats off! Ketjutonttu oli loistava panostus. Organisaatioiden keskinäinen riippuvuus kasvaa jatkuvasti lisääntyvien integraatioiden ja tiedonjaon myötä. Sen seurauksena myös hyökkäyspinta-ala kasvaa. Toiminta taas monesti pohjautuu pitkälle yhteistyölle ja luottamukselle joka taas ei välttämättä aina tarkoita että toimijan kyberhygienia on yhtä hyvällä mallilla kuin itse toiminta/palvelu jonka vuoksi yhteistyötä tehdään. Supply chain riskin kartoitus ja arviointi on monesti hankalaa. Toivottavasti Ketjutonttu projekti saa jatkoa joskus toiste.*
- *Kiitos oli hyvä kampanja. Mielellään otetaan vastaan kaikki etenkin ilmainen apu mitä saadaan tietoturvaan liittyen. Hyvä jos Kyberturvallisuuskeskus auttaisi jatkossakin etenkin verkon suojaamisessa. Yrityksen rahat, resurssit ja oma osaaminen ei riitä kuin tavanomaisiin tietoturva toteutuksiin.*
- *Todella hyödyllinen ja yritykselle helppo kampanja.*

Yhteenveto

- Ketjutonttu paransi toimitusketjujen tietoturvaa merkittävästi
- Toimittajat maailmanlaajuisesti saivat korjattua haavoittuvuuksiaan
- Toimittajien tunnistaminen ja riskien selvittäminen auttaa organisaatioita varautumaan poikkeuksiin toimitusketjuissaan
- Kampanja osoitti, että kyberturvallisuutta voidaan parantaa keveillä menetelmillä - myös pk-yritysten osalta

150
suoritti Ketjutontun

2313
toimittajaa tarkastettiin

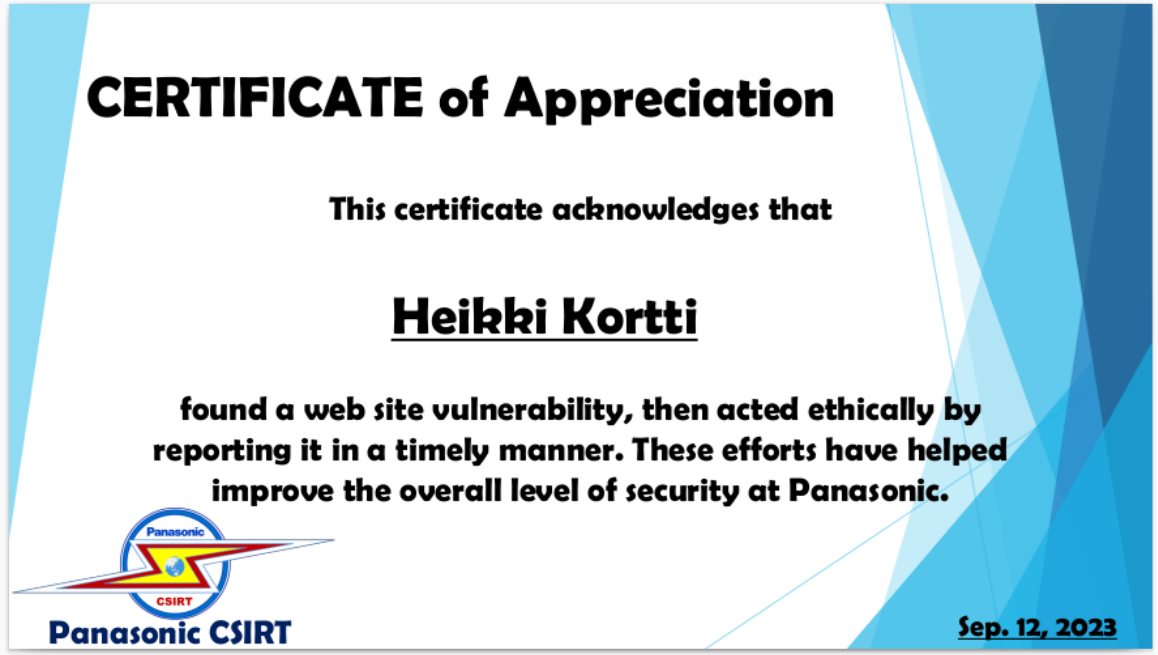
856
havaintoa raportoitiin

NPS:81
erinomainen palaute osallistujilta

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Ketjutonttu

Parannetaan toimittajien turvallisuutta yhdessä



Toimittajat kiittävät!