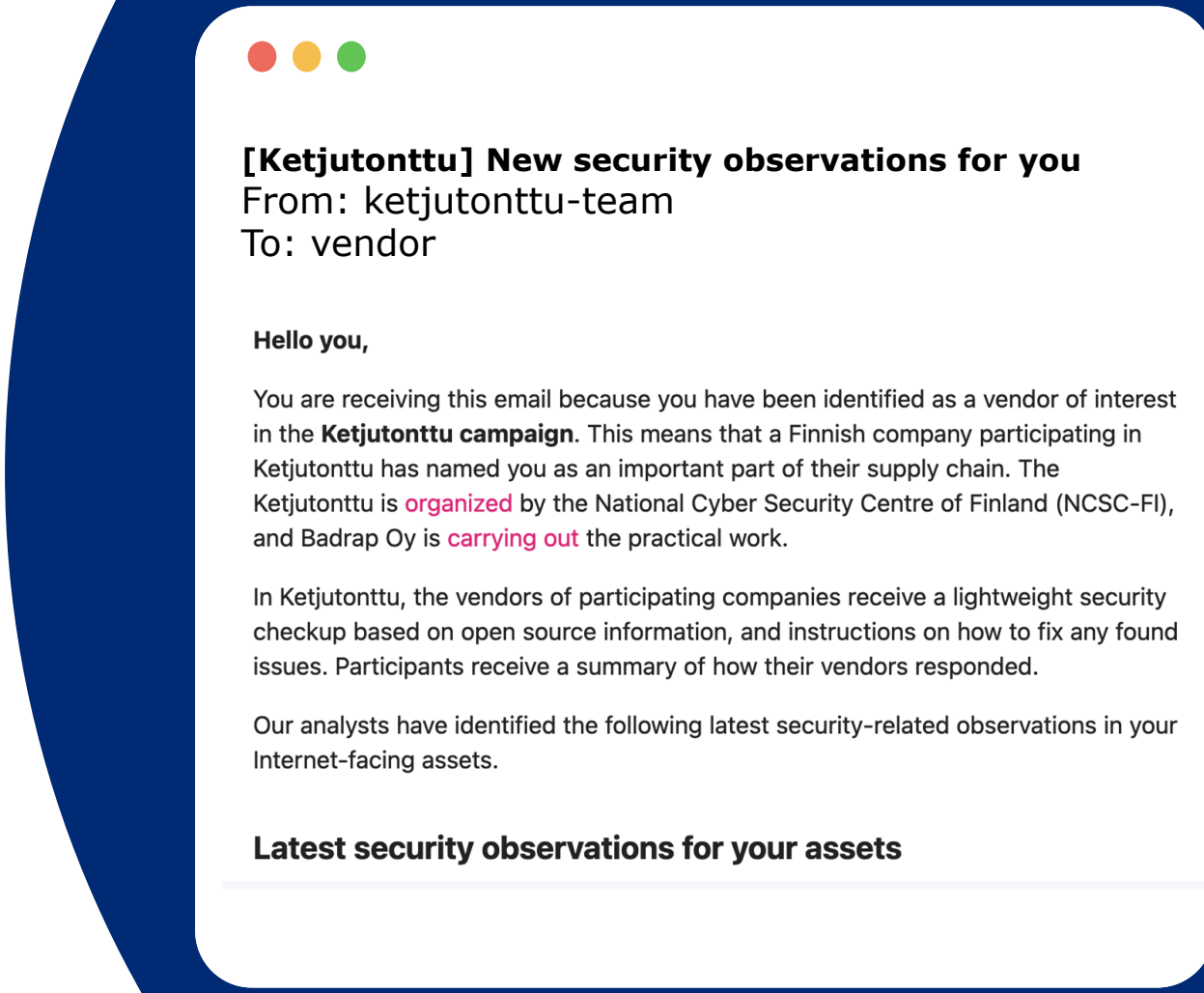
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Ketjutonttu

How we improved together the security of your supply chains



Improving supply chains has value

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

Campaign in figures

150
participants

2313
vendors checked

856
findings reported

What is Ketjutonttu?

- A collaborative campaign for Finnish organisations
- Participants received a free checkup for the cyber security of their supply chains
- Vendors received vulnerability reports and help with fixes
- We classified vendors into A/B/C categories based on their response
- National Emergency Supply Authority funded the campaign
- Practical measures were done in collaboration with Traficom’s NCSC-FI and Badrap Oy

What is Tonttu?

- Campaigns that find out whether the cyber security of organisations can be improved with lightweight methods
- A way to reach new audiences, who might not be familiar with the National Cyber Security Centre of Finland (NCSC-FI)

PASSIVE COLLABORATION

We'll contact you after an incident has occurred - if we can identify you.

OCCASIONAL COLLABORATION

For instance: You take part in our ISAC functions, provide us with details about your assets, or deliver log information for analysis.

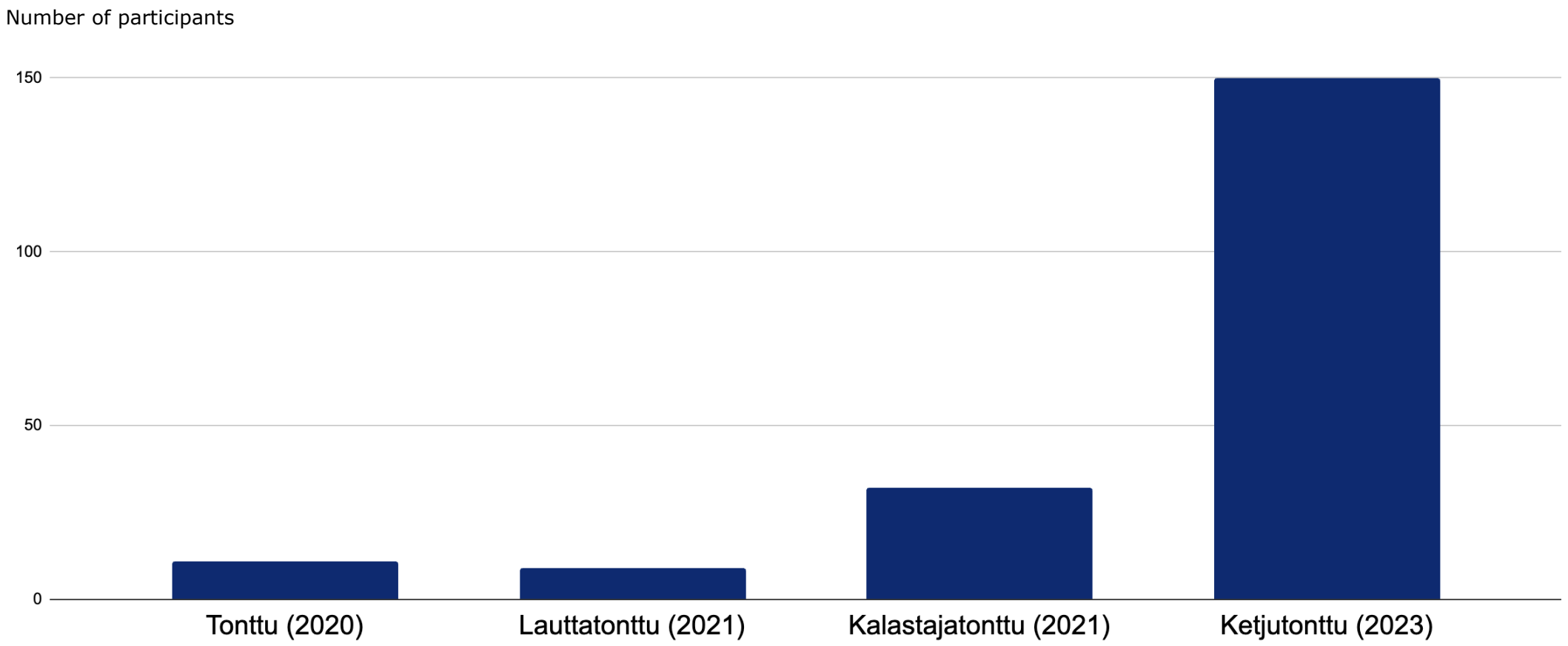
AUTOMATED COLLABORATION

You are using at least one collaborative automation capability. For instance: identifying your cloud assets, or using lightweight collaborative sensors.

HAVARO 2

SOC subscription, heavy-duty sensors, private identifiers.

Ketjutonttu jumped to a whole new level of reach



Scaling collaboration and reaching new participants - Ketjutonttu Tour of Finland

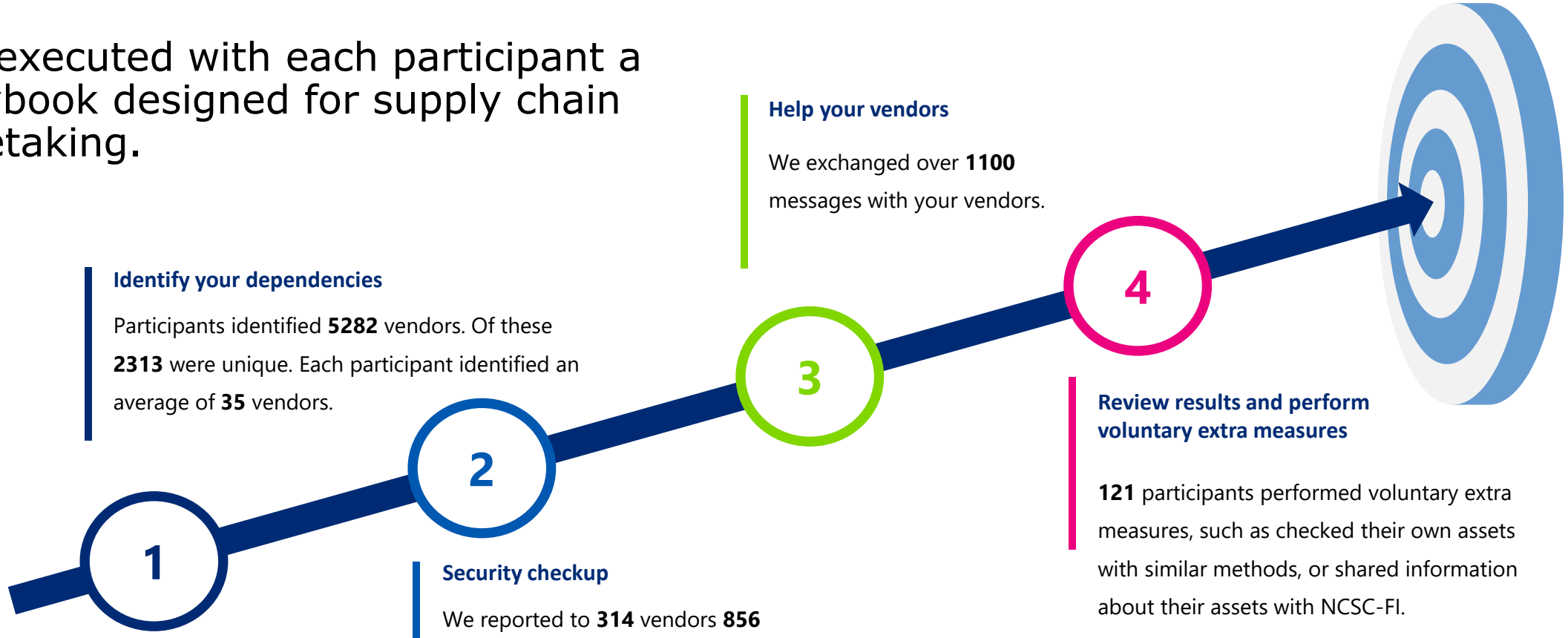
- 21.3. Oulu - Finnish Cyber Security Label event
- 23.3. Kotka - Kybertuska event, Internet - Member webinar of the German-Finnish Chamber of Commerce
- 24.3. Internet - NCSC-FI Weekly Review 12/2023
- 13.4. Internet - NCSC-FI Cyber Weather Report
- 18.4. Tampere - Cyber Security Label event
- 25.4. Jyväskylä - Cyber Security Label event
- 3.5. Internet - “Security of web stores and the obligation to provide information” webinar
- 11.5. Internet – NCSC-FI Cyber Weather Report
- 19.5. Internet - NCSC-FI Weekly Review 20/2023
- 23.5. Oulu - Presentation at Finnish universities security day
- 10.8. Internet - NCSC-FI Cyber Weather Report

Additionally:

- National Emergency Supply Authority’s communications for organisations
- Social media communications from NCSC-FI and Badrap Oy
- Phone campaign to reach new organisations by Badrap Oy (⅓ of participants)

Ketjutonttu playbook – statistics on each phase

We executed with each participant a playbook designed for supply chain caretaking.



Identify your dependencies

Participants identified **5282** vendors. Of these **2313** were unique. Each participant identified an average of **35** vendors.

Security checkup

We reported to **314** vendors **856** individual findings.

Help your vendors

We exchanged over **1100** messages with your vendors.

Review results and perform voluntary extra measures

121 participants performed voluntary extra measures, such as checked their own assets with similar methods, or shared information about their assets with NCSC-FI.

Supply chain discovery

- Average 35 vendors / participant
- Some participants initially had only a few vendors in mind. The list was expanded e.g. by discussion, going through different types of vendors, and with technical discovery (whois/DNS/TLS records).
- Other participants had a ready vendor listing, from which the most critical ones were selected for review.

50+ dependents	1 vendor
20-50 dependents	13 vendors
10-19 dependents	52 vendors
5-9 dependents	134 vendors

Supply chain discovery

- Top 10 list contained 8 Finnish companies and 2 multinational software companies.
- 3 financial administration
- 3 teleoperators
- 2 software companies
- 1 bank
- 1 healthcare

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

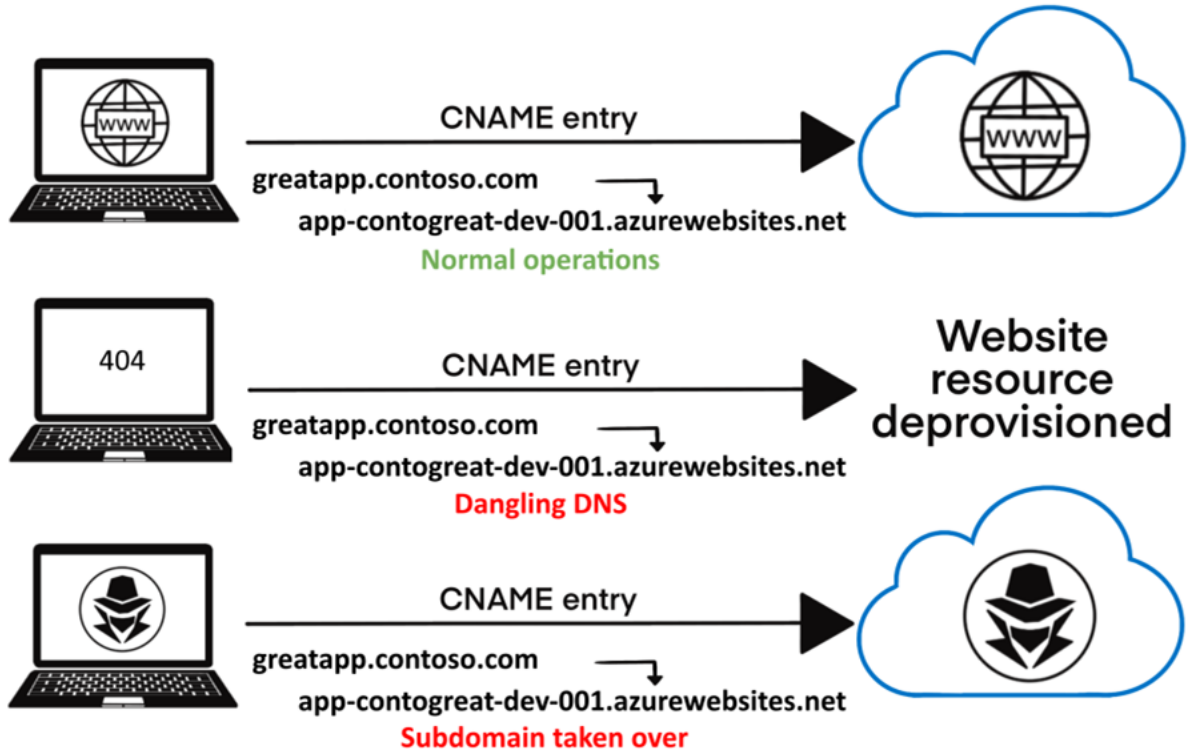
Security checkups and findings

One out of every seven vendors had issues

Type of finding	How many vendors had this
DNS subdomain takeover risk (or a less critical dangling DNS record)	114
End-of-life servers and services	119
Exposed services (databases, remote management, file sharing)	185

Subdomain takeover risk

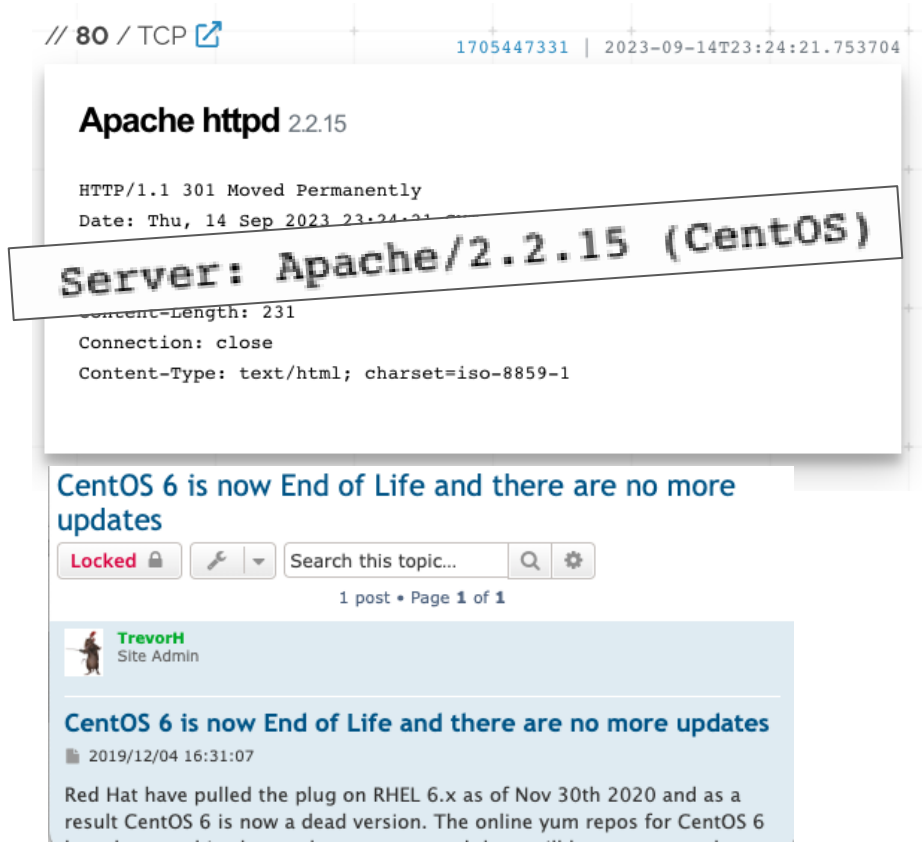
- A domain name record at the company points to a cloud provider or another leased resource
- The name to which the record points is no longer used by the company
- A criminal assumes control of the unused cloud resource
- The criminal abuses the victim's domain for various attacks



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

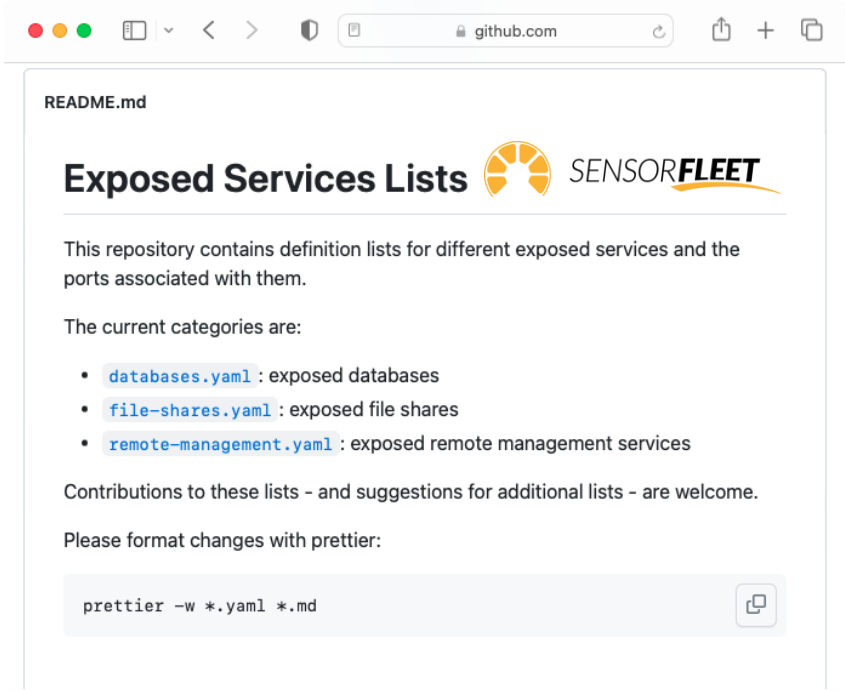
End-of-life servers and services

- We inspected the version numbers of certain services
- We deduced the Linux distribution or Windows version based on the version numbers (“platform”)
- We warned your vendors if the platform was so old that it no longer receives security updates, or updates require extra effort.



Exposed services

- Scan for the worst and most clearly accidental exposures
- Connection test - we did not check e.g. if the contents of an exposed database were easily accessible



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

Service port	Individual findings
3306 (MySQL/MariaDB)	72
3389 (RDP)	31
5432 (PostgreSQL)	17
…	…
541 (Fortigate Management)	7
Others	58

Reporting

Finding the right contact

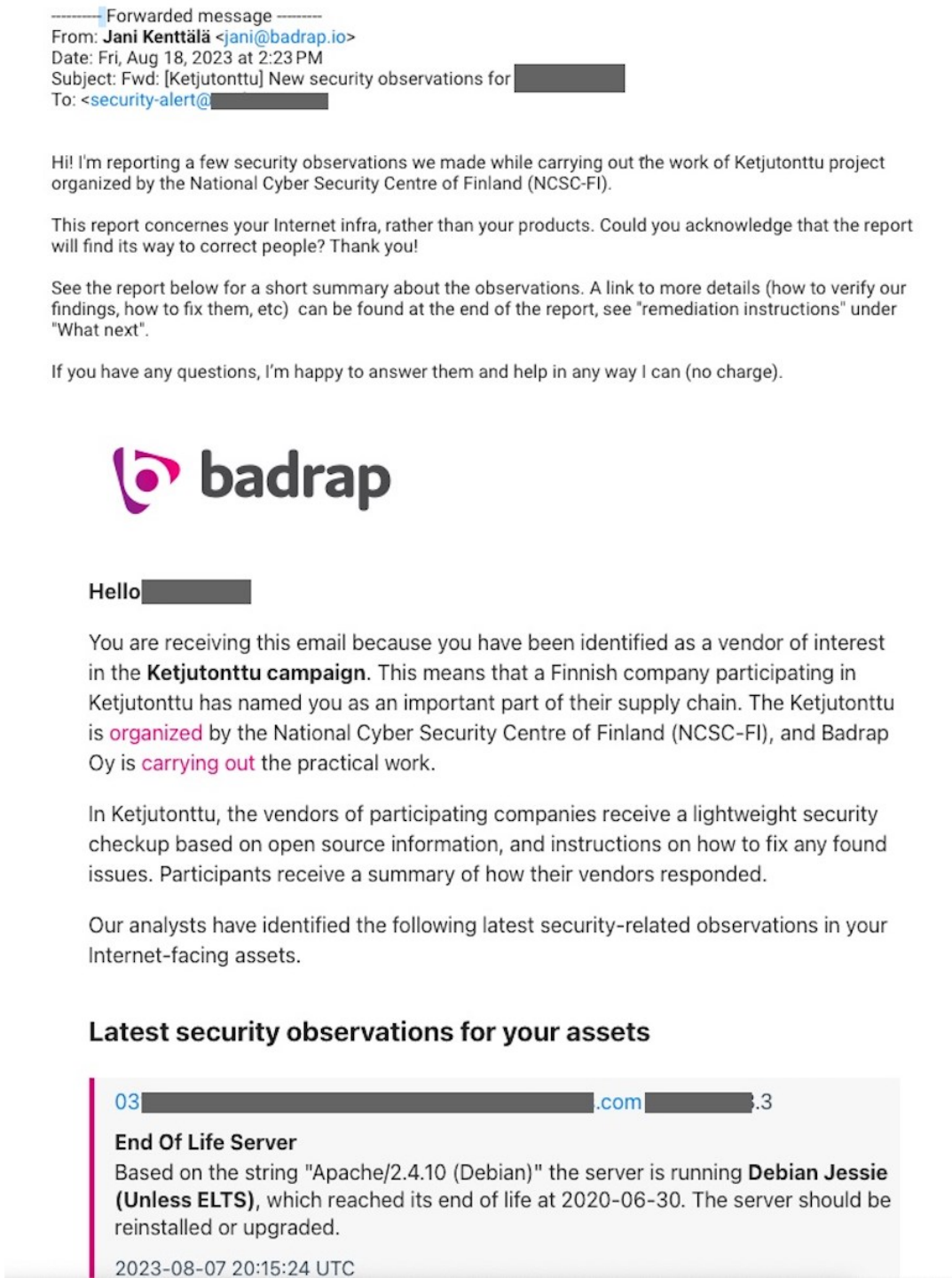
- security.txt - 7% of vendors
- Web pages
- LinkedIn roles
- Generic info/contact/support email addresses

The recipient may think you are:

- A “Beg bounty” hunter
- Selling something
- Some kind of fraud
- Not important
- Bug bounty programs are a category of their own
  - A reward-based process requires a reporter to use more time per case
  - Focus in Ketjutonttu was to minimise time spent on reporting (without compromising report quality)

Reporting

- Add a pinch of human into your reports
- Explain the context - why has the reporter made these checks
- Tell all that you know about the finding
- Be prepared to answer questions
- Track and support



---------- 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.

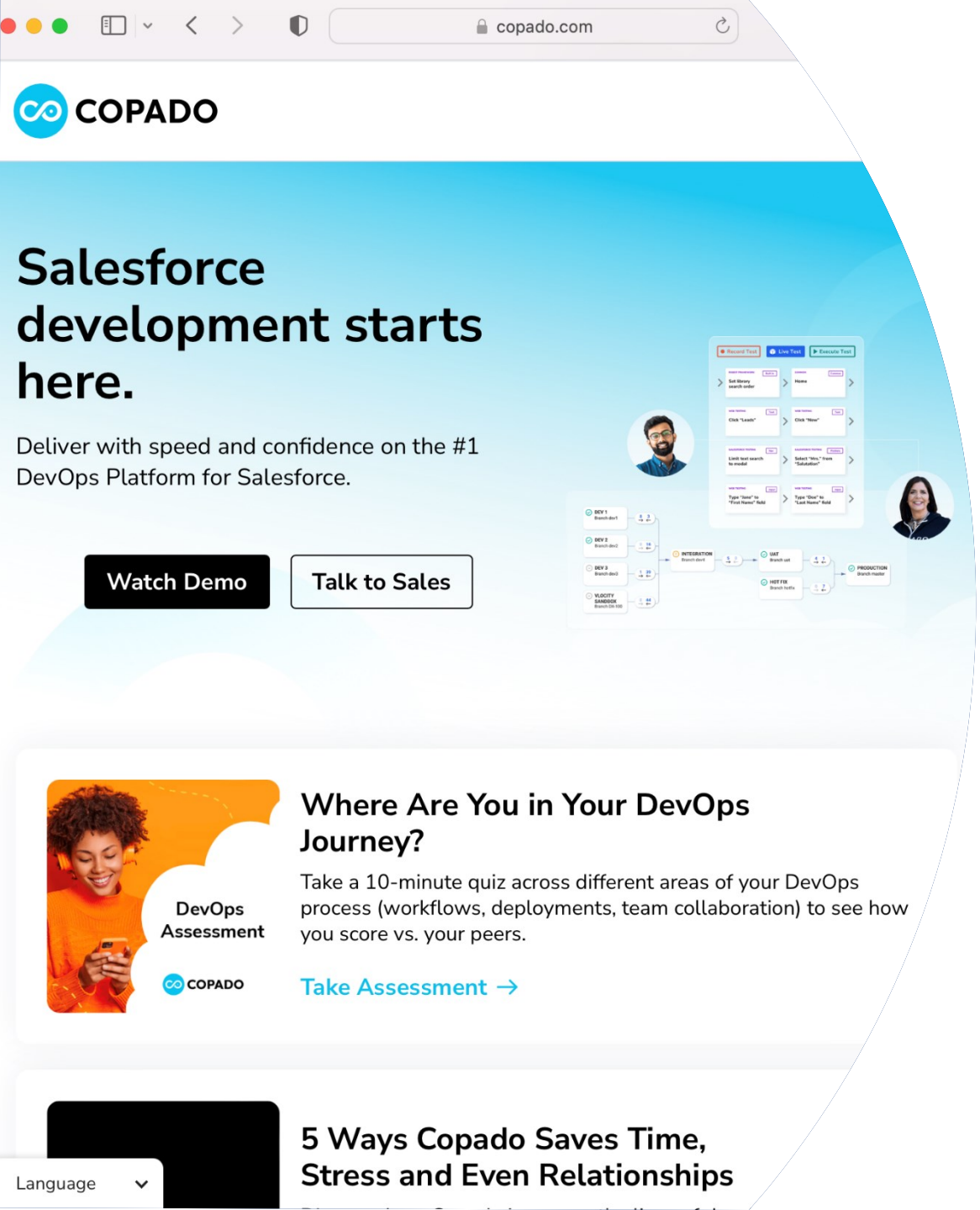
Our analysts have identified the following latest security-related observations in your Internet-facing assets.

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



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

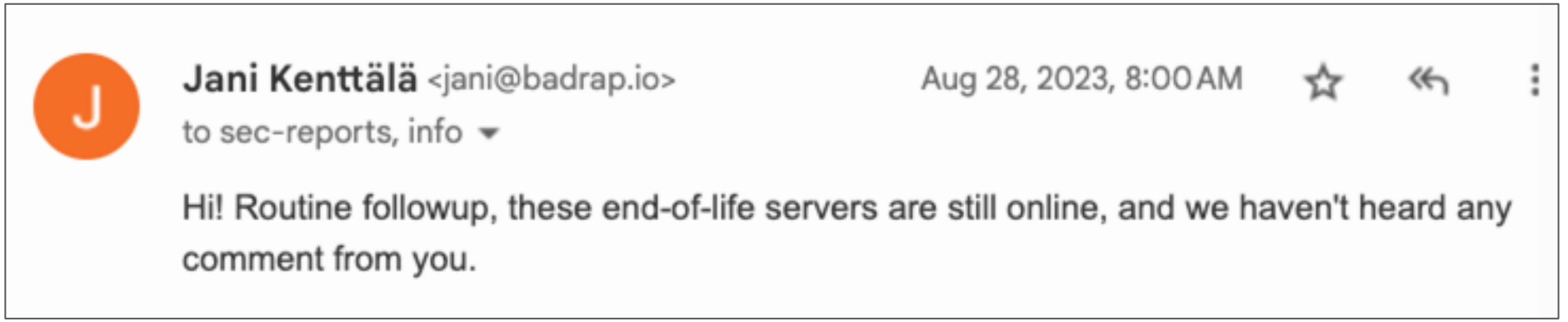
Also - our team thoroughly appreciated how well-written and polite your report was!

Thanks and please pass our regards to the chain elf,

The Copado Security Team

Helping the vendors

- 95% of the time goes to persistent tracking - be the vendor’s ticketing system with reminders
- Help the vendor explain the issue to their own vendor
- Discuss with the vendor about their risk assessments - the assessment may have been based on wrong information



How did the vendors perform?

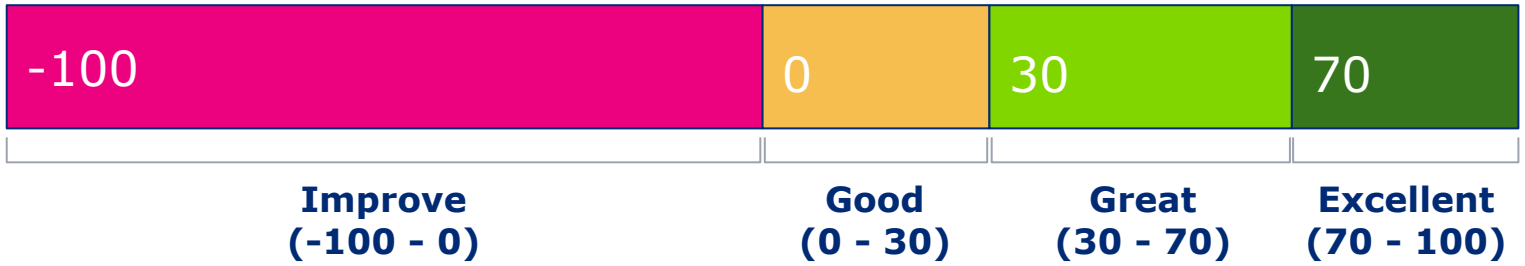
- A - Fixes issues quickly and communicates clearly
- B - Takes issues seriously, but fixing takes time
- C - Does not respond or fix - or responds, but it does not make any sense
- OK - No findings, no responses measured -> no rating
- These ratings were given to vendors:

Vendor stereotypes

- A: Professional - communicates about fixes, does the fixes, explains that the fixes have been made (this includes also well-working bug bounty programs)
- A: Relentless hunter - does not rest until the issue has been resolved
- B: Slow due to the size of their organization
- B: Slow due to a lack of lifecycle planning
- B: Slow due to a bug bounty program
- C: Silent vendor
- C: “There is no problem” explanation does not make any sense
- C: The issue is stuck at a bug bounty program since we do not demonstrate exploitation

How did the participants see Ketjutonttu?

- We gathered feedback with a questionnaire during September 2023
- By 30th of Sep, 18% of the participants responded
- Tonttu campaigns aim to find new organisations for collaboration. Recommending campaigns to another organisation helps reach this goal.
- We asked how likely participants are to recommend Tonttu campaigns to others, and calculated a Net Promoter Score (NPS) based on the responses.



Feedback from participants was excellent

- For the question “Would you recommend Tonttu campaigns to your acquaintances?” 85% of the respondents gave a 9 or 10 on a scale of 0-10.
- Net Promoter Score (NPS) = 81.
- Only the top brands globally can reach similar ratings e.g. on the category of B2B software.
- We also asked on a scale of 1-10, how meaningful it was to map the organisations’ supply chains. The average for these responses was 9 - very meaningful.

Feedback from participants

- *Hats off! Ketjutonttu was an excellent effort. The interdependency of organisations continues to increase due to new integrations and information sharing. Attack surface is also increasing as a result of this. Activities on the other hand are often based on a long relationship and trust, which does not necessarily mean that the other actor's cyber hygiene is as good as the activity/service which is provided. Auditing and assessing the risks of supply chains is often hard. I hope the Ketjutonttu project will be continued at another time.*
- *Thanks this was a good campaign. We gladly accept especially any free help we can get for cyber security. It would be great if NCSC-FI would help going forward especially in protecting our network. Our organisation's money, resources and knowhow are enough only for usual security implementations.*
- *A really useful and easy campaign for our organisation.*

Summary

- Ketjutonttu improved the security of supply chains significantly
- Vendors around the world managed to fix their vulnerabilities
- Identifying your vendors and assessing their risks helps organisations prepare for incidents in their supply chains
- This campaign proved that cyber security can be improved with lightweight methods - also for small and medium businesses

150
participants went through Ketjutonttu

2313
vendors checked

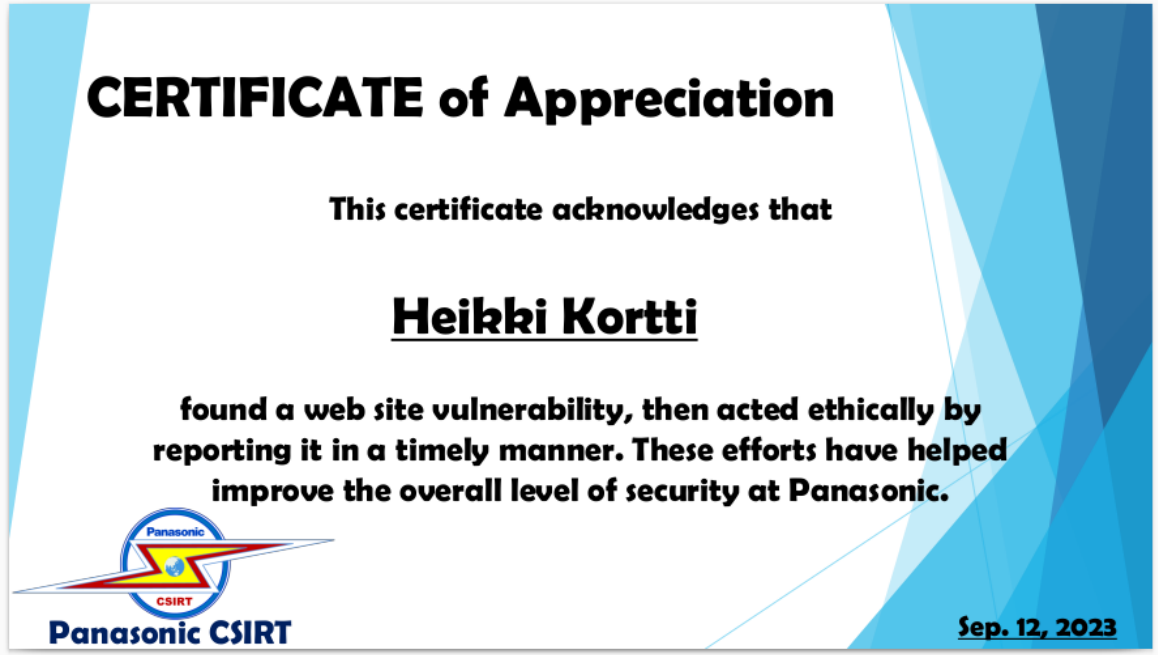
856
findings reported

NPS:81
excellent feedback from participants

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Ketjutonttu

Let’s improve together the security of your vendors



Thanks from your vendors!