SUNET security center

David Heed, Coordinator Sunet security center

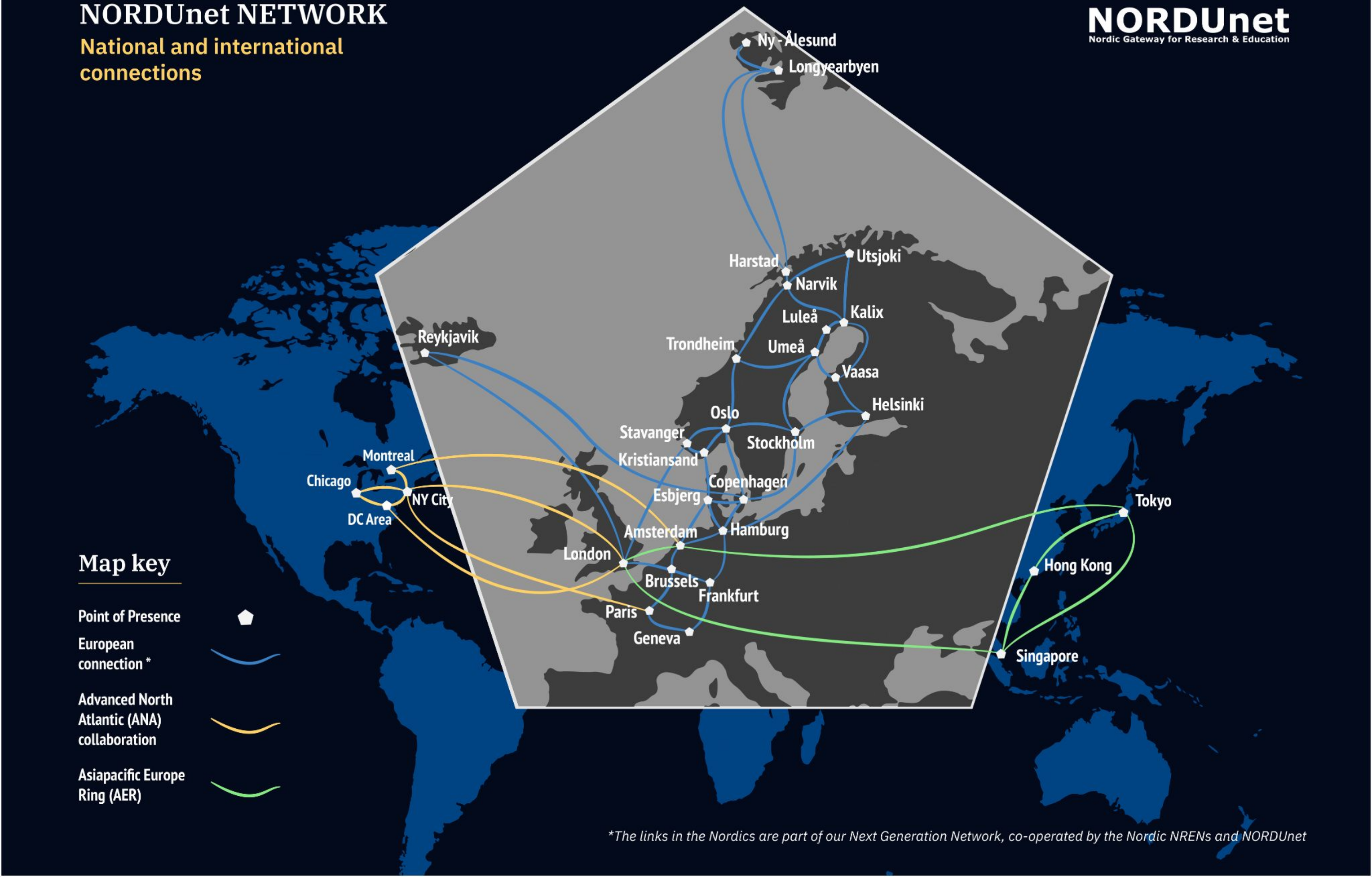
Vetenskapsrådet

SUNET

NORDUnet NETWORK

National and international connections

NORDUnet
Nordic Gateway for Research & Education



Map key

Point of Presence ⬟

European connection *

Advanced North Atlantic (ANA) collaboration

Asiapacific Europe Ring (AER)

*The links in the Nordics are part of our Next Generation Network, co-operated by the Nordic NRENs and NORDUnet

Vetenskapsrådet

SUNET

Continued establishment of our security center

- Need for efficient information exchange
- Large amounts of attacks and events
- Increased expectations for teleworking / digitization
- Encourage, develop and retain skills in the sector
- It is difficult for small and large organizations to monitor and manage risks in a global context
- Cooperation is a key factor

Vetenskapsrådet

SUNET

Parts of work

Proactive work - community building, recommendations, intelligence

Real-time / Detect - monitor C2, 0day Vulnerability mapping

Respond & Coordinate - ticket initialisation and relaying

Keeping our own infrastructure and tools up to date

Basic operational activities - Security center

❑ Monitor the world around us and notify about critical vulnerabilities

❑ Coordinate incident management between organizations and within SUNET's own services

❑ Facilitate and encourage networking, knowledge dissemination and competence sharing

❑ Advice and information sharing - in collaboration with organizations

❑ Establish and maintain relationships with other incident management organizations

❑ Manage and further develop contact registers for all affiliated organizations

Technology support that all affiliated organizations have access to:

- MISP and general information sharing from other tools / sources
- SUNET DNS Resolver with policy-based blocking
- Vulnerability scanner

Everything above is included in the SUNET connection

Challenges ahead

Reduce detection speed for attacks

Upgrade to 400Gb core network. Sensors and tapping.

Increased legal requirements for information security

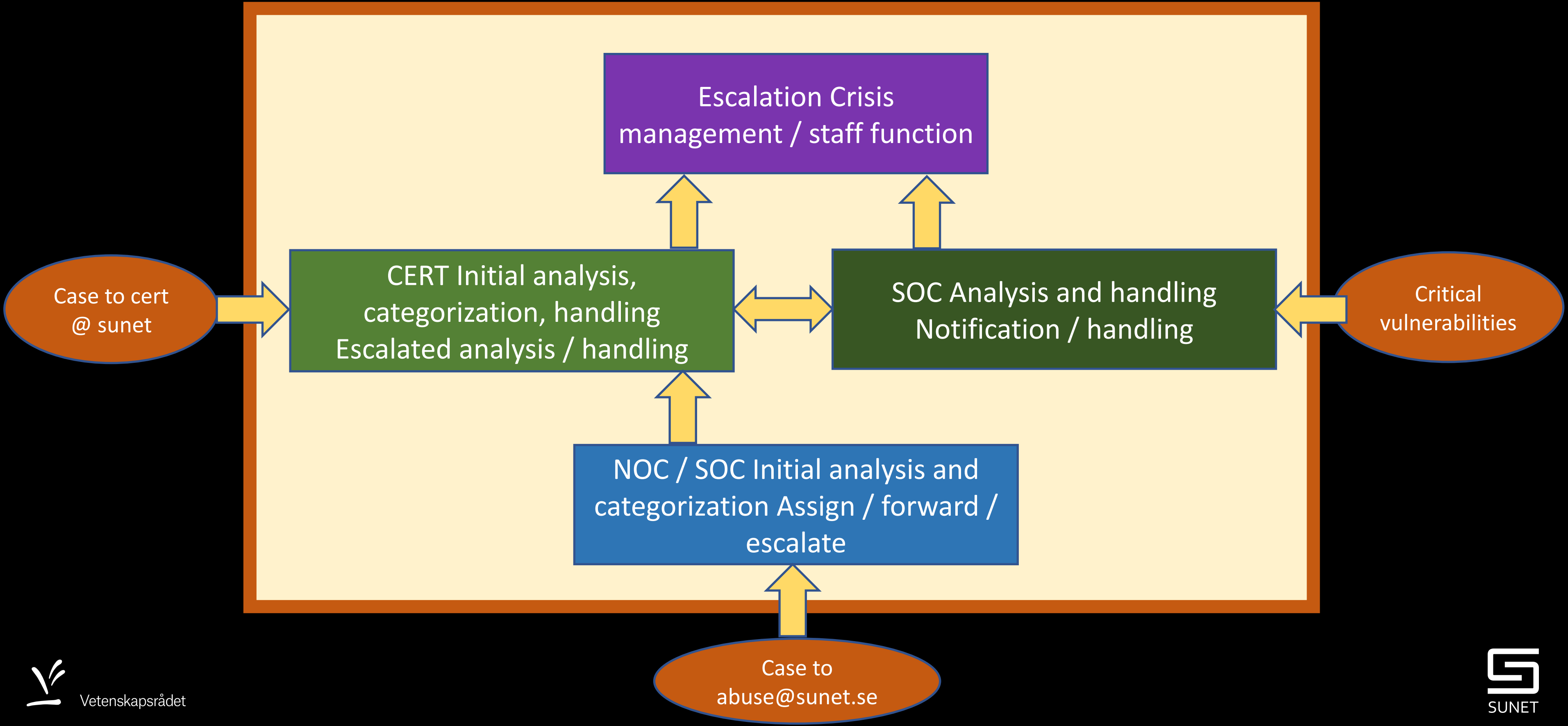
Possibilities ahead (new services)

Penetration testing as addition to automated checks

Larger sector wide crisis exercises

Common training materials for security awareness

Case management



Escalation Crisis management / staff function

CERT Initial analysis, categorization, handling Escalated analysis / handling

SOC Analysis and handling Notification / handling

NOC / SOC Initial analysis and categorization Assign / forward / escalate

Case to cert @ sunet

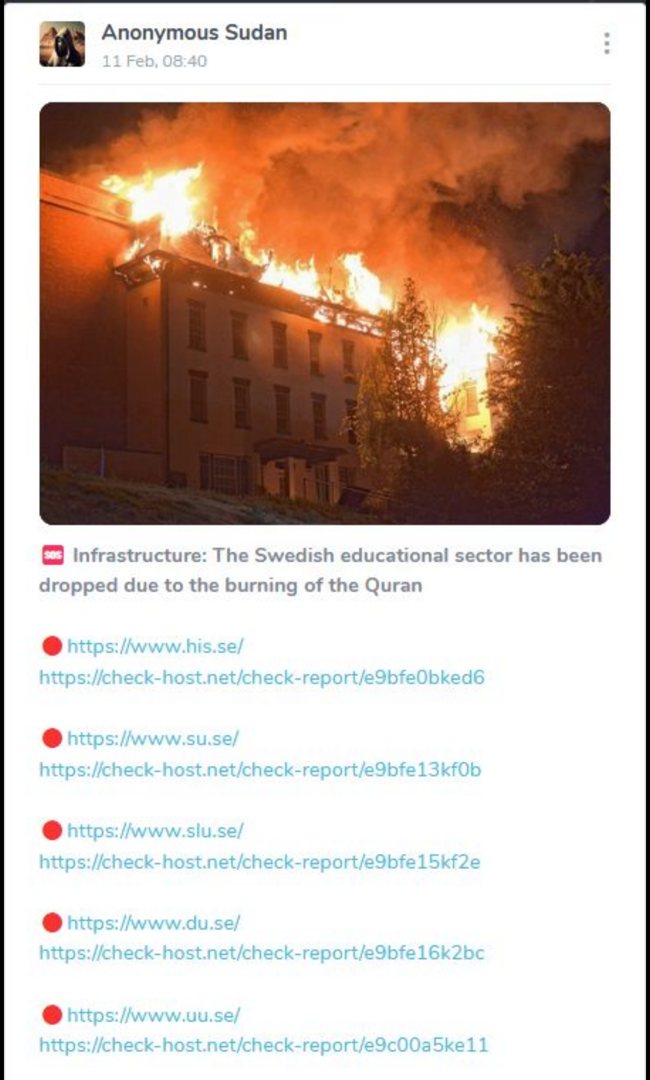
Critical vulnerabilities

Case to abuse@sunet.se

Targeted attacks

Big attacks during february

(saturday...)



Anonymous Sudan

11 Feb, 08:40

🆘 Infrastructure: The Swedish educational sector has been dropped due to the burning of the Quran

● https://www.his.se/
https://check-host.net/check-report/e9bfe0bked6

● https://www.su.se/
https://check-host.net/check-report/e9bfe13kf0b

● https://www.slu.se/
https://check-host.net/check-report/e9bfe15kf2e

● https://www.du.se/
https://check-host.net/check-report/e9bfe16k2bc

● https://www.uu.se/
https://check-host.net/check-report/e9c00a5ke11

Information channels and cooperation

Channels

- Webforum
- Slack-channel
- Mailinglist
- Signal-group
- Wiki-pages

Conferences, CSIRT-forum, workshops

- At least three-four times per year

Open-house! Every other week

Exercises and workshops

Perform crisis exercises locally at connected organizations

- Usually a 4-hour tabletop exercise with report and feedback

Show and tells of tools and best practise from community is encouraged

Open-house every other week

Open collaboration meeting

- Open discussion on any topic around IT, Infosec & general-security
- Current events including regulations and risk management
- Recent attacks and 0day vulnerabilities
- Demos from potential vendors

MISP - Threat sharing platform

https://misp.cert.sunet.se

(See https://wiki.sunet.se/display/SUNETCERT/MISP)

Has general Threat feeds + "manually" reported data

Simplified "Frontend" to MISP: https://IOC-lookup.sunet.se for quick search of the most common attributes, including simplified reporting, and "sightings" reporting.

SUNET DNS resolver

89.32.32.32 / 2001:6b0:89::32:32:32

Started 2019

“Public”

“Internet hardened” / DDoS-mitigation

RPZ (via MISP) with SWITCH & SURBL and other feeds

What we do to counter these threats

Focused on what can have a greater impact and is already being used or is likely to be used.

Develop tools and scan majority of all vulnerabilities of high impact

Track and act (block) the infrastructure deployed by a majority of these actors.

Principles for tickets on intelligence forwarded from SUNET security center

- Focused on what can have a greater impact and is already being used or is likely to be used.
- High accuracy.
- Only in exceptional cases should the level of factuality be lowered and it must then be clearly stated why the recipient should still act on the basis.
- Prepared quickly, preferably before threat actors have time to act, with an understanding of when the recipient can act on it.

Analysis and prioritization

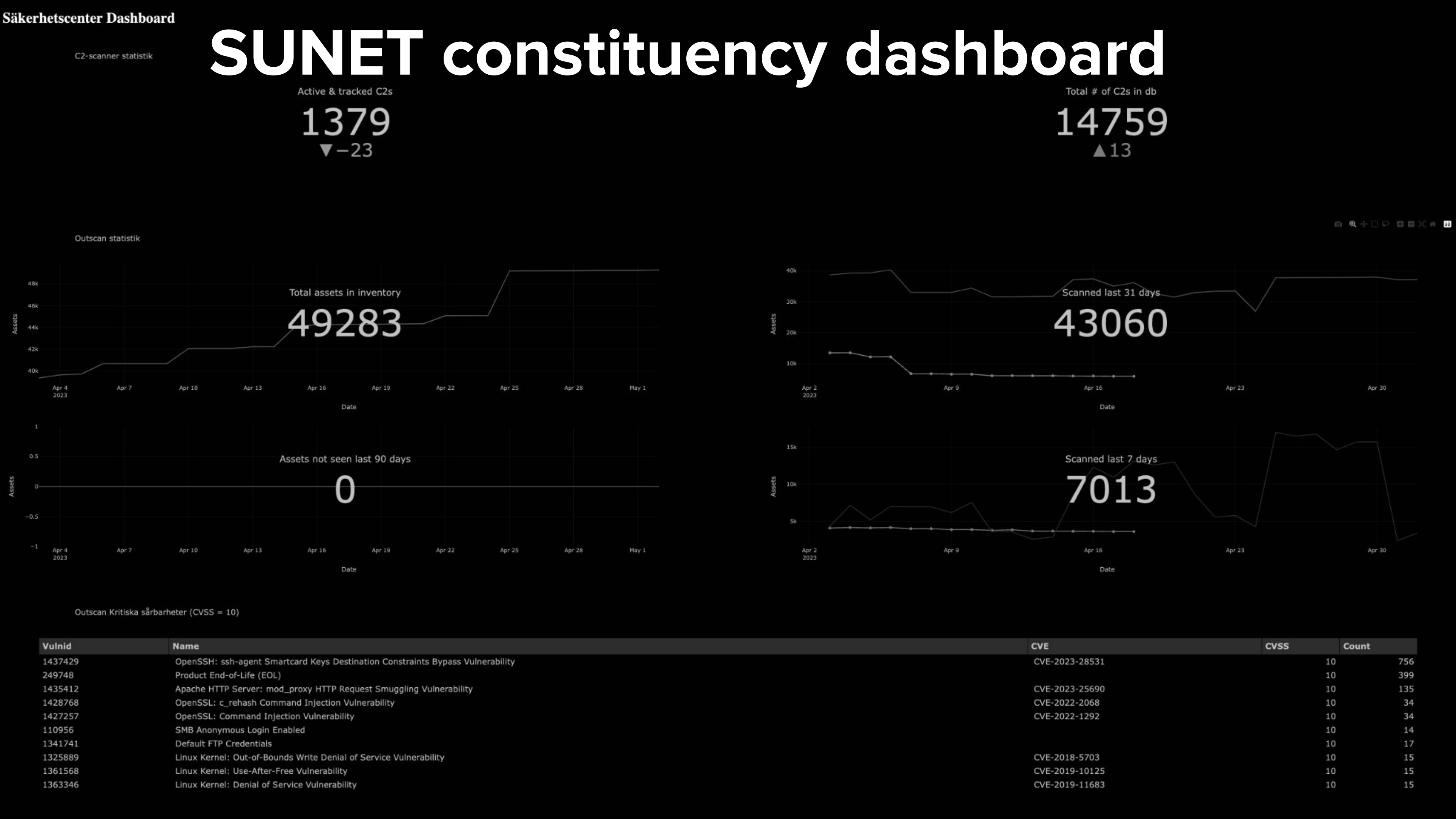
- Is the vulnerable product easy to access, eg is it directly accessible from the internet or not?
- Is the vulnerability easy to exploit, eg is it a logical bug in a common configuration or is there already a well-functioning exploit?
- How important are the systems with the vulnerability, e.g. does it affect central parts of important systems?
- What do you get access to and what can you do if you exploit the vulnerability?
- Is it likely that actors will exploit the vulnerability and, if so, within what time frame?

The result so far

18491 Cobalt Strike C2:or identified since end of Jan 2022.

- Identified C2s for the majority of ransomware groups.
- Identified Russian state actors that e.g. were targeting critical infrastructure in Ukraine in the ongoing war.
- Identified Chinese state actors targeting countries in Asia as well as possibly in Sweden.
- Identified new C2s for advanced actors in Sweden that in several cases could be taken down the same day as it was set up by the actor.

SUNET constituency dashboard



Säkerhetscenter Dashboard

C2-scanner statistik

Active & tracked C2s

1379

▼−23

Total # of C2s in db

14759

▲13

Outscan statistik

Total assets in inventory

49283

Scanned last 31 days

43060

Assets not seen last 90 days

0

Scanned last 7 days

7013

Outscan Kritiska sårbarheter (CVSS = 10)

Vulnid	Name	CVE	CVSS	Count
1437429	OpenSSH: ssh-agent Smartcard Keys Destination Constraints Bypass Vulnerability	CVE-2023-28531	10	756
249748	Product End-of-Life (EOL)		10	399
1435412	Apache HTTP Server: mod_proxy HTTP Request Smuggling Vulnerability	CVE-2023-25690	10	135
1428768	OpenSSL: c_rehash Command Injection Vulnerability	CVE-2022-2068	10	34
1427257	OpenSSL: Command Injection Vulnerability	CVE-2022-1292	10	34
110956	SMB Anonymous Login Enabled		10	14
1341741	Default FTP Credentials		10	17
1325889	Linux Kernel: Out-of-Bounds Write Denial of Service Vulnerability	CVE-2018-5703	10	15
1361568	Linux Kernel: Use-After-Free Vulnerability	CVE-2019-10125	10	15
1363346	Linux Kernel: Denial of Service Vulnerability	CVE-2019-11683	10	15

Cyber threat intelligence history archive

Website: orkl.eu

Focus on TLP:Clear Search functionality and some indexing

There is an API for full-text searches

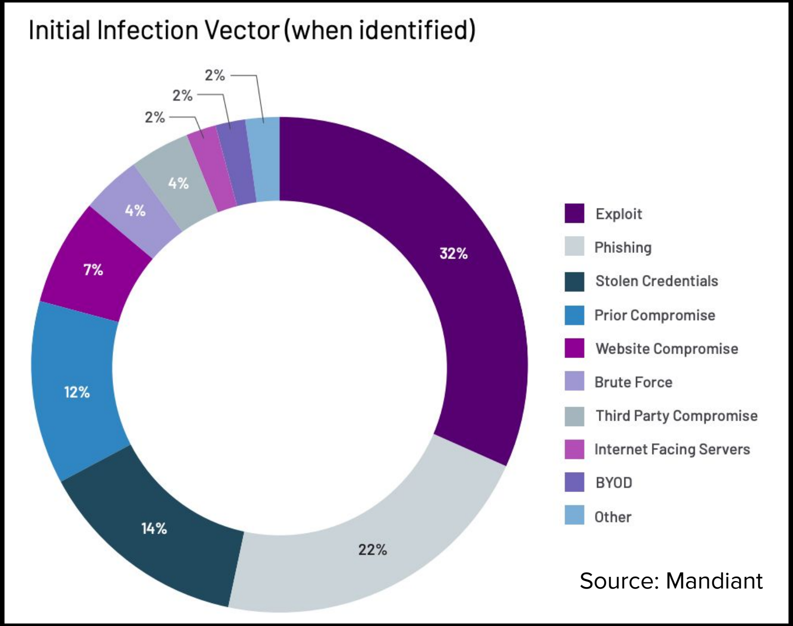
Cirka: 2700 documents in English today

Hosted by Sunet security center to
offload cloud infrastructure for the community effort.

Can we reduce the threats?

60+% can be “fixed” with

- Vulnerability management
- Security awareness
- (VPN MFA)



Source: Mandiant

Questions & Comments?