Synergie fyzické a kybernetické bezpečnosti v moderním datacentru

Konference CRA security

Michal Polívka | Architekt kybernetické bezpečnosti

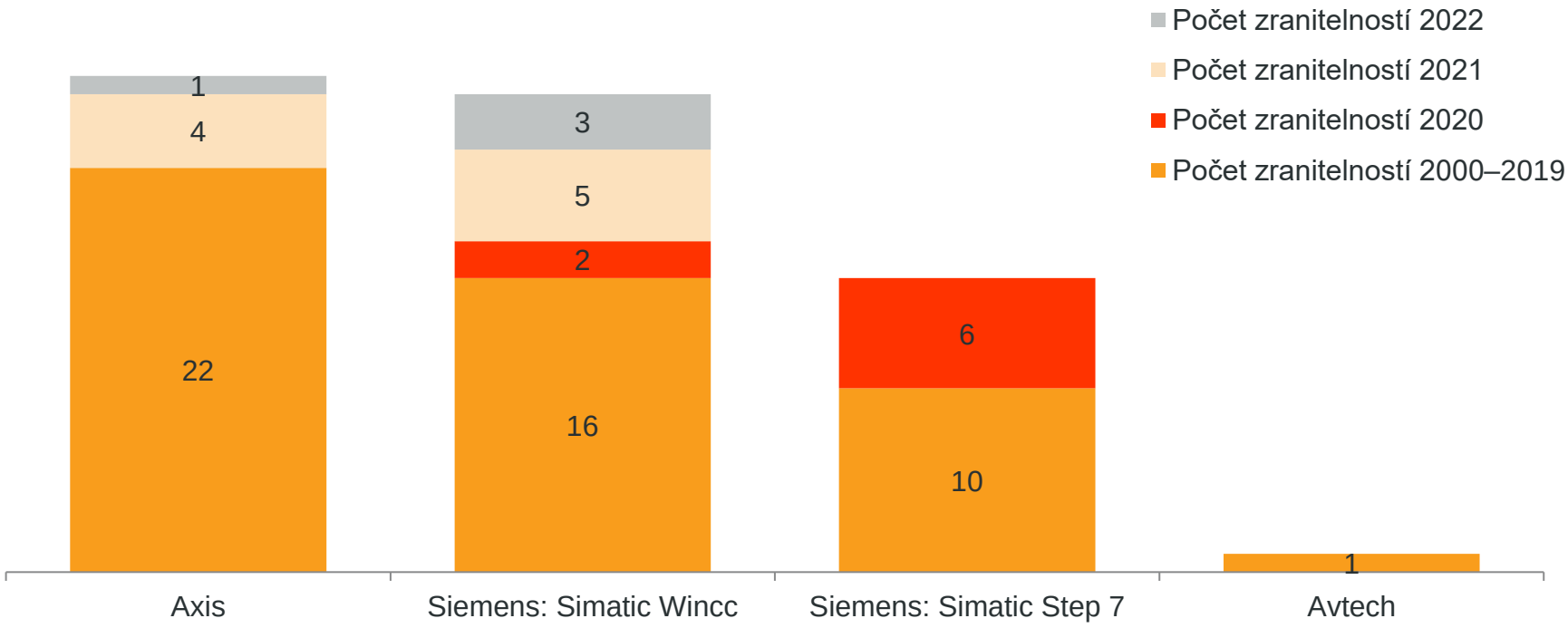
18. října 2022 | Žižkovská televizní věž

TLP CRA: GREEN (ZELENÁ)

https://www.lupa.cz/clanky/foto-ceske-radiokomunikace-rozsirily-datacentrum-dc-tower/

Vybrané produkty a počet evidovaných chyb

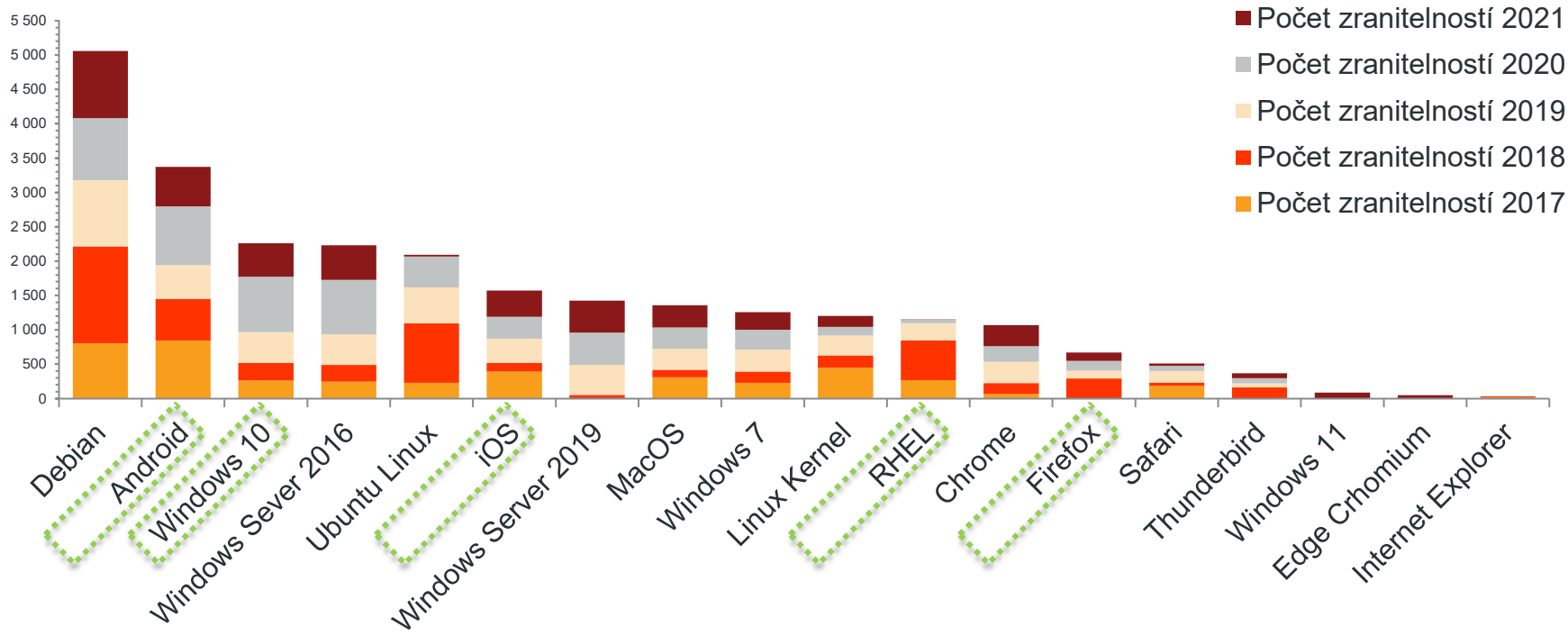
Srovnání počtu CVE 2017–2021



https://www.cvedetails.com/

TOP produkty v počtu evidovaných chyb

Srovnání počtu CVE 2017–2021



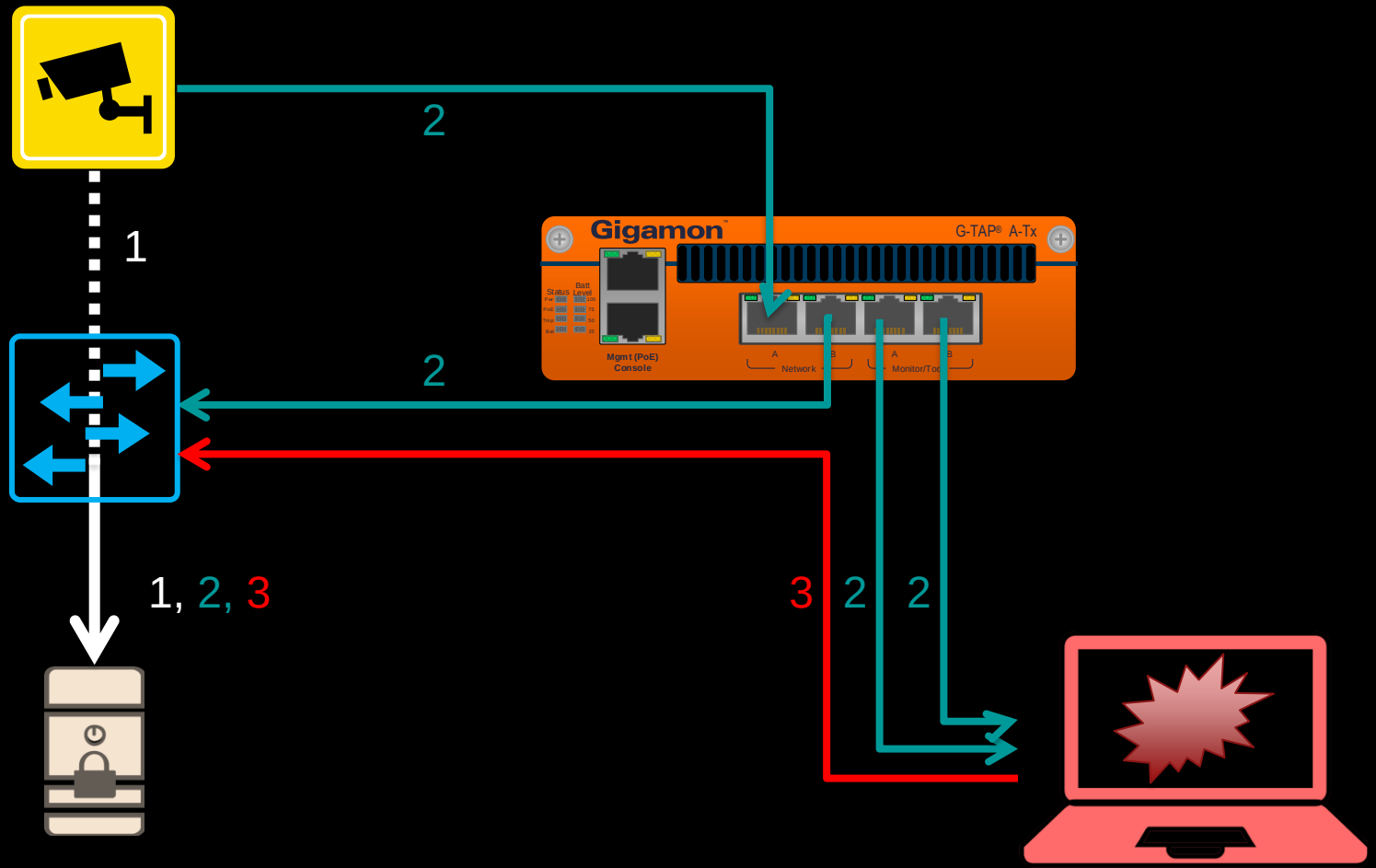
https://www.cvedetails.com/top-50-products.php

https://www.cvedetails.com/

https://www.exploit-db.com/


CRA
VÍTÁME VÁS

https://www.ceskatelevize.cz/porady/1097181328-udalosti/207411000100617/cast/34910/


2
1
Gigamon
G-TAP® A-Tx
Mgmt (PoE)
Console
Network
2
1, 2, 3
3
2
2

Bezpečnostní testy technologií

uz01@RHEL-v

```
uz01@RHEL-v:~# hping3 -c 10000 -d 120 -S -w 64 -p 443
--flood [redacted]
HPING [redacted] (eth1 [redacted]): S set, 40
headers + 0 data bytes

--- [redacted] hping statistic ---
3 packets transmitted, 0 packets received, 100% packet
loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

The following is an automated response sent to you by the QRadar event custom rules engine:

Start Time:
Oct 3, 2022 9:11:14 AM CEST

Rule Name:
Monitoring switch ██-SW-30 - ██ | CRA

Event Name:
Link Up

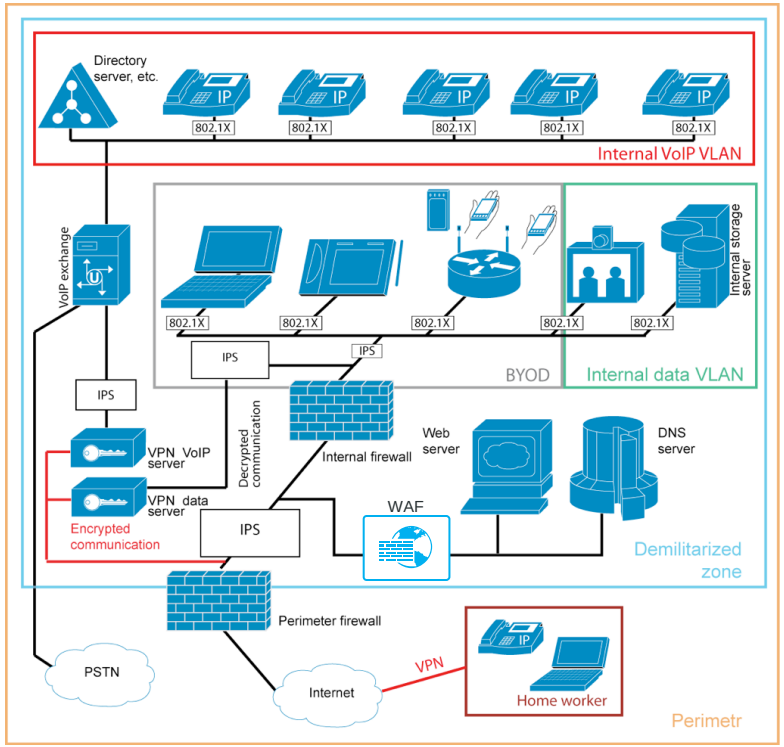
Event Description:

Category:
Information

Payload:
<190>%LINK-I-Up: gi1/14

Síťová infrastruktura datacentra

DC core vs. podpůrná infrastruktura



NetFlow

IDS

ARP Cache poisoning

Port steeling

switch spoofing

VLAN hopping

MAC flooding

double tagging

ČSN EN 50600	https://csnonline.agentura-cas.cz/
ANSI/TIA-942-B	https://tiaonline.org/wp-content/uploads/dlm_uploads/2021/01/TIA-942-Standard_OnePager-110220.pdf
Tier Classification System (Uptime Institute)	https://uptimeinstitute.com/tiers

DISA STIG	https://public.cyber.mil/stigs/
CIS	https://downloads.cisecurity.org/
PCI DSS	https://www.pcistandard.cz/pcidss/
NIST 800-171	https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
ACSC Essential Eight	https://www.cyber.gov.au/acsc/view-all-content/essential-eight https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Essential%20Eight%20in%20Linux%20Environments%20%28June%202020%29.pdf
NIST HIPAA Security Rule Toolkit	https://csrc.nist.gov/projects/security-content-automation-protocol/hipaa


CRA
ČESKÉ RADIOKOMUNIKACE