REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

KONFERENCA ZInfV-1
ZAKON ZA KIBERNETSKO VARNO PRIHODNOST SLOVENIJE

URSIV

13. oktober 2025
Brdo pri Kranju

POSTOPEK NADZORA PO ZInfV-1

Matjaž Mravljak
direktor Inšpekcije za informacijsko varnost, URSIV

NAČRTOVANJE IN IZVAJANJE INŠPEKCIJSKIH NADZOROV

- **Strateške usmeritve in prioritete inšpekcijskega nadzora** Urada Vlade RS za informacijsko varnost (za posamezno leto – pogoji za izvajanje rednih in izrednih nadzorov)
- **Načrt inšpekcijskih nadzorov** Inšpekcije za informacijsko varnost (za posamezno leto)

URSIV

KOMPETENCE INŠPEKTORJEV ZA INFORMACIJSKO VARNOST

- **Opravljen strokovni izpit za inšpektorja** (ZIN, ZUP, ZP-1)
- **Manager SUVI** ISO 27001 (certifikat CIS-M)
- **Vodilni presojevalec** ISO 27001 (certifikat CIS-A)
- **Notranji presojevalec za sistem neprekinjenega poslovanja** (certifikat ISO 22301)
- **CCNA-1: osnove omrežij in tehnologije** (certifikat CCNA-1)
- **CCNA CyberOps: izvajanje kibernetskih operacij** (certifikat CCNA Cyber Operations)
- **Varnost ICS/OT/IoT okolij** (certifikat ali potrdilo za OT sisteme)
- **Preizkušeni revizor informacijskih sistemov** (certifikat PRIS)

URSIV

POOBLASTILA INŠPEKTORJEV ZA INFORMACIJSKO VARNOST

- **Inšpekcijski pregled na kraju ali nadzor na daljavo** (eksperti)**.**
- **Inšpekcijski varnostni pregled** (testiranja varnostnih ukrepov).
- **Neposreden vpogled** v podatke, dokumentacijo ter v omrežne in informacijske sisteme.
- **Preverjanje pogojev in načina izvajanja varnostnih ukrepov.**
- **Pregled območij, objektov in prostorov zavezancev,** kjer so ključni sistemi ni podatki.
- **Pregled dokumentacije o izvajanju obveščanja o incidentih.**
- **Pregled poročil o izvedbi revizije IS in izvedbi varnostnih pregledov.**

URSIV

IZVAJANJE INŠPEKCIJSKIH NADZOROV 1/3

FAZA PRIPRAVE:

- **Pisna najava** izvedbe inšpekcijskega nadzora in **posredovanje vprašalnika** za preliminarno oceno skladnosti.
- **Pridobitev relevantnih podatkov o zavezancu** od drugih organov in organizacij (SIKV, SIGOV-CERT, SI-CERT, VOC, ipd.) in analiza pridobljenih podatkov.
- **Pridobivanje podatkov iz „odprtih“ in namenskih orodij** (Shodan, Censys, SSLServerTest, DNSviz, ipd.) ter analiza podatkov.
- **Priprava internega načrta in opomnika** za izvedbo nadzora.

URSIV

IZVAJANJE INŠPEKCIJSKIH NADZOROV 2/3

FAZA IZVEDBE:

- **Zbiranje, pregled in presoja internih dokumentov** (in pogodb), katere predpisuje ZInfV-1 oziroma drug predpis.
- **Razgovori s pristojnimi predstavniki zavezanca** in (po potrebi) z drugimi zaposlenimi.
- **Pregledi lokacij,** kjer se izvajajo (IT) procesi v povezavi z izvajanjem dejavnosti.
- Posredovanje **pisnih vprašanj** zavezancu.
- **Pridobitev in presoja dokazil** o izvajanju predpisanih ukrepov.
- **Izvedba različnh testiranj** izvajanja predpisanih ukrepov.

URSIV

IZVAJANJE INŠPEKCIJSKIH NADZOROV 3/3

FAZA ZAKLJUČKA:

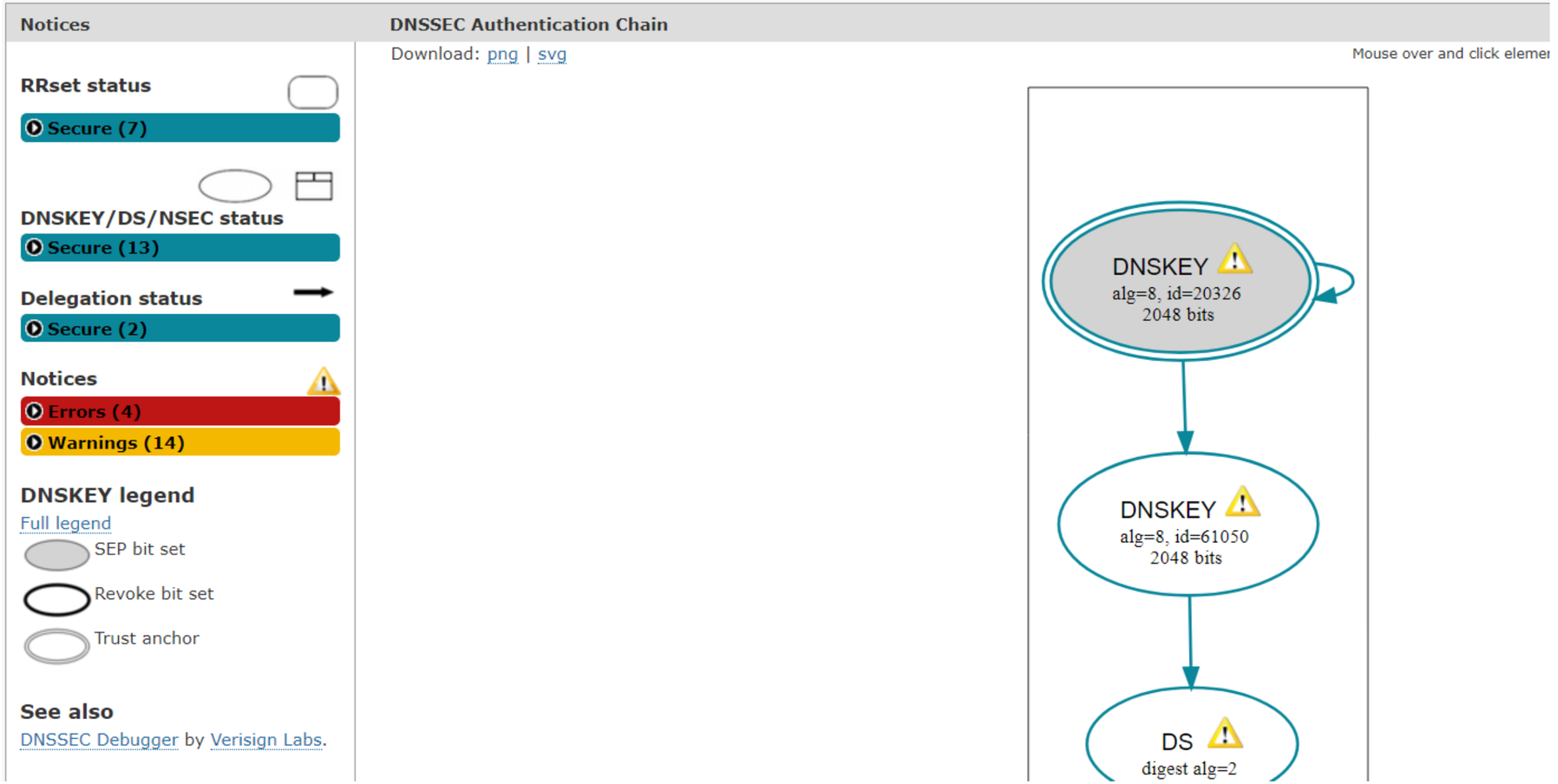
- **Zapis ugotovitev nadzora,** ukrepov za odpravo nepravilnosti in priporočil v zapisnik o inšpekcijskem pregledu.
- **Izvedba usklajevalnega sestanka** s predstavniki zavezanca s predstavitvijo ugotovitev in dogovor o rokih za izvedbo ukrepov.
- **Izvedba notranjega kolegijskega pregleda zapisnika** o inšpekcijskem nadzoru.
- **Podpis in vročitev zapisnika** o inšpekcijskem nadzoru zavezancu.
- **Izdaja ureditvene odločbe** zavezancu in **prekrškovni postopek**.

URSIV

PRAKTIČEN PRISTOP PRI ZVAJANJU NADZOROV

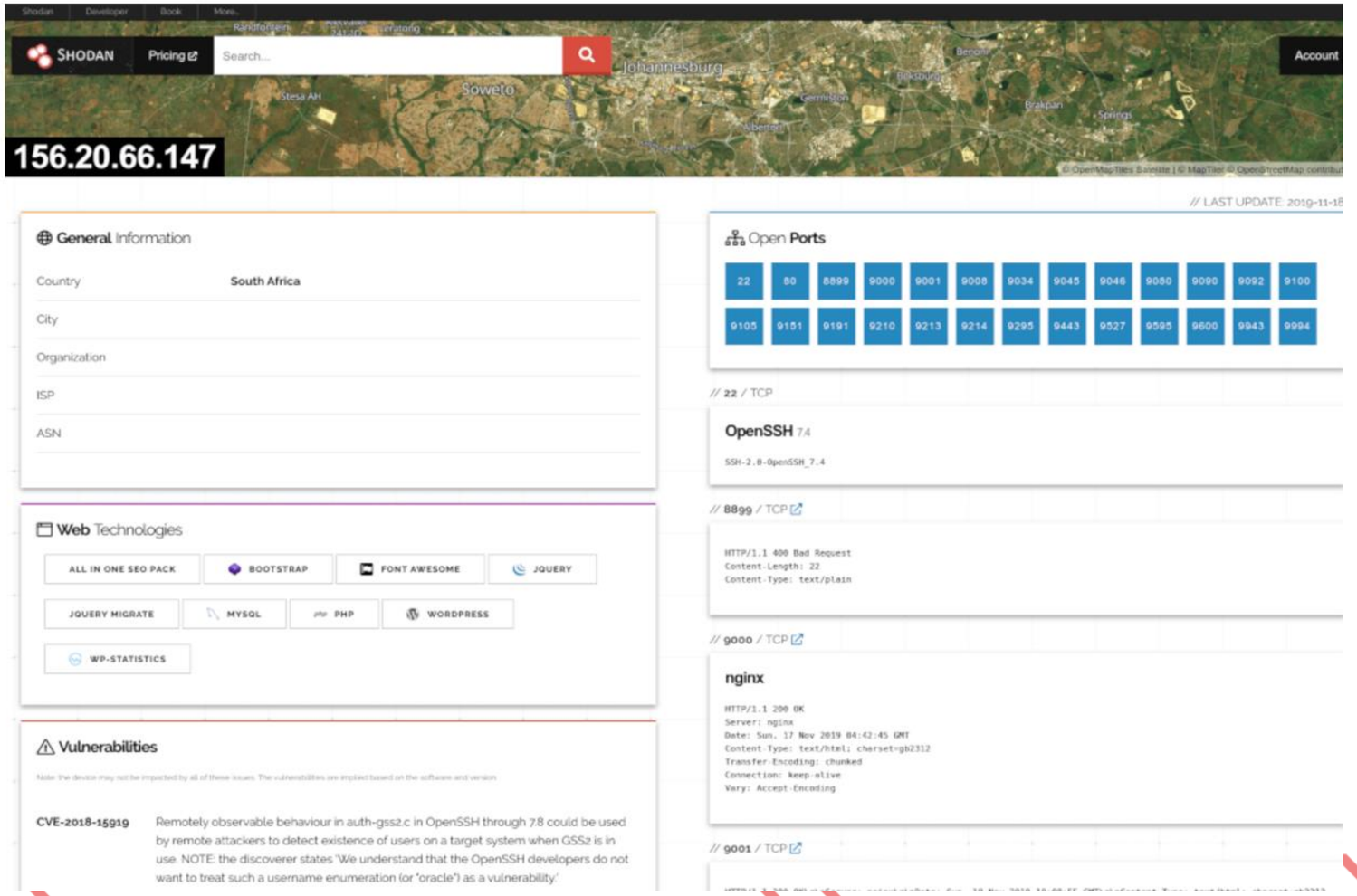
- Pregled **seznama poslovnih procesov**.
- Pregled **popisa informacijskih sredstev**.
- Pregled **ocene vpliva na poslovanje**.
- Pregled **politike o varnosti omrežij in informacijskih sistemov**.
- Prelged **analize obvladovanja tveganj (ocena tveganj)**.
- Pregled **politike neprekinjenega poslovanja**.
- Pregled **načrta neprekinjenega poslovanja**.
- Pregled **načrta varnostnih ukrepov** (pogodbe-*outsourcing*).
- Prelged **načrta obnovitve in ponovne vzpostavitve sistemov.**
- Pregled **načrta odzivanja na incidente in obveščanja CSIRT**.
- Pregled **politike s postopki za presojo učinkovitosti ukrepov**.

UPORABA NAMENSKIH ORODIJ V NADZORIH 1/10



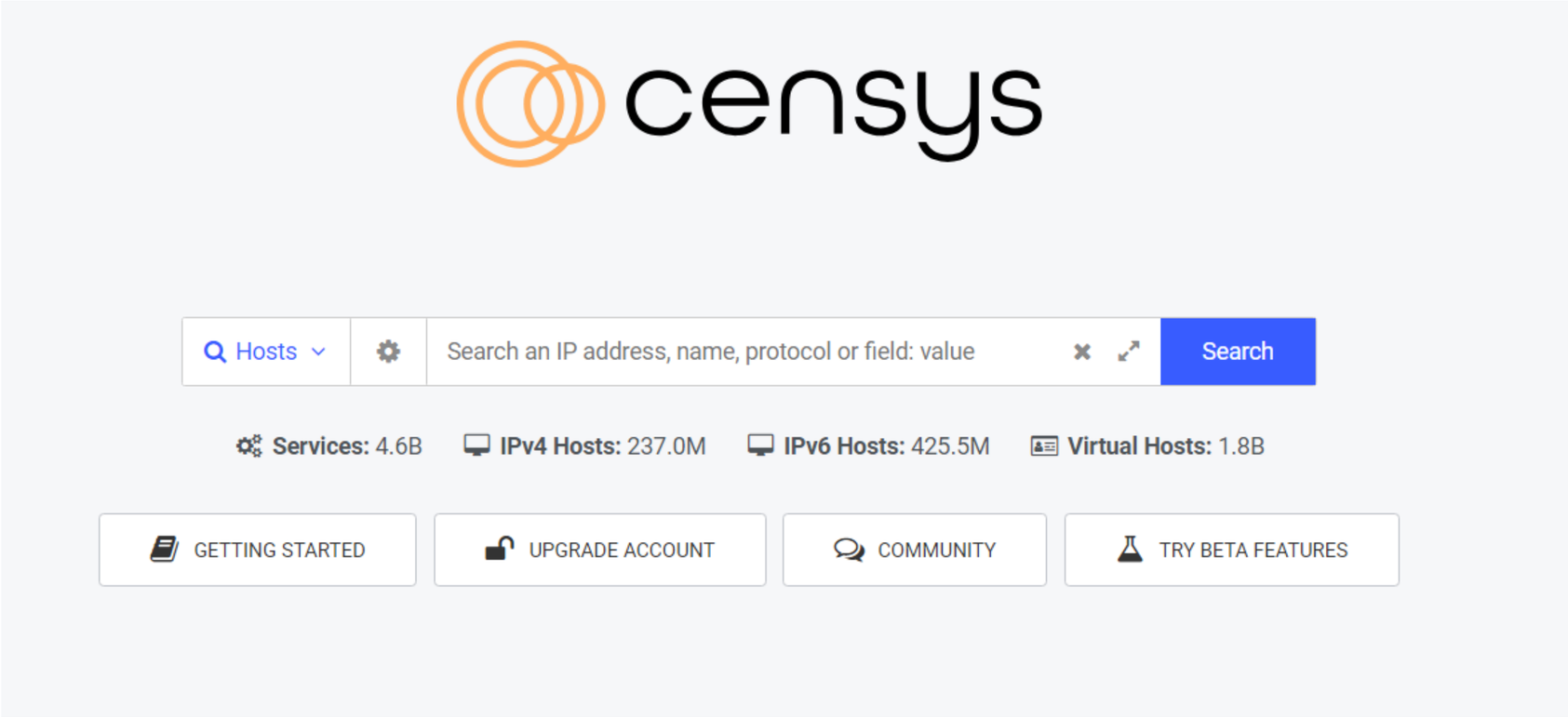
URSIV

UPORABA NAMENSKIH ORODIJ V NADZORIH 2/10



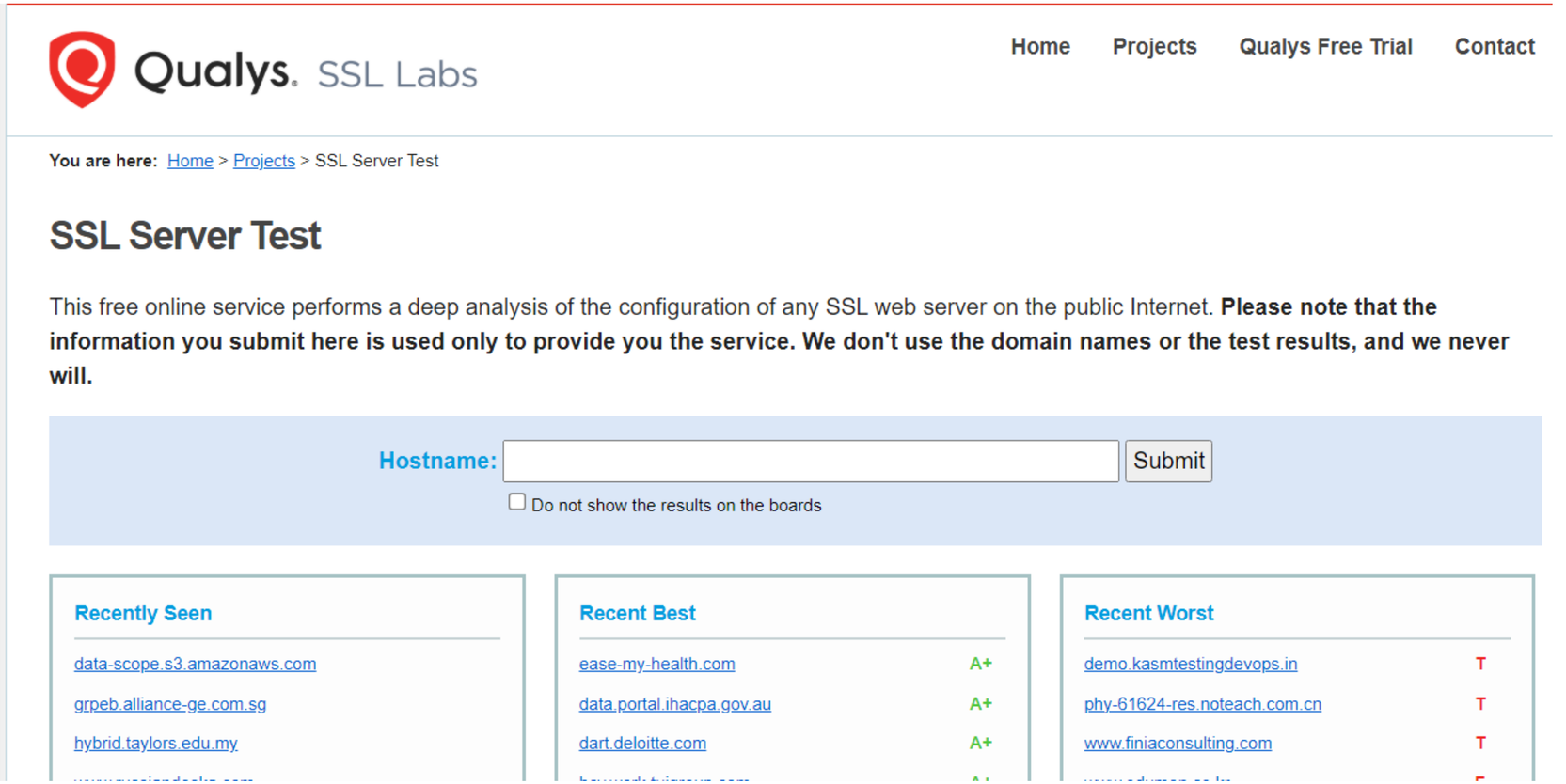
URSIV

UPORABA NAMENSKIH ORODIJ V NADZORIH 3/10



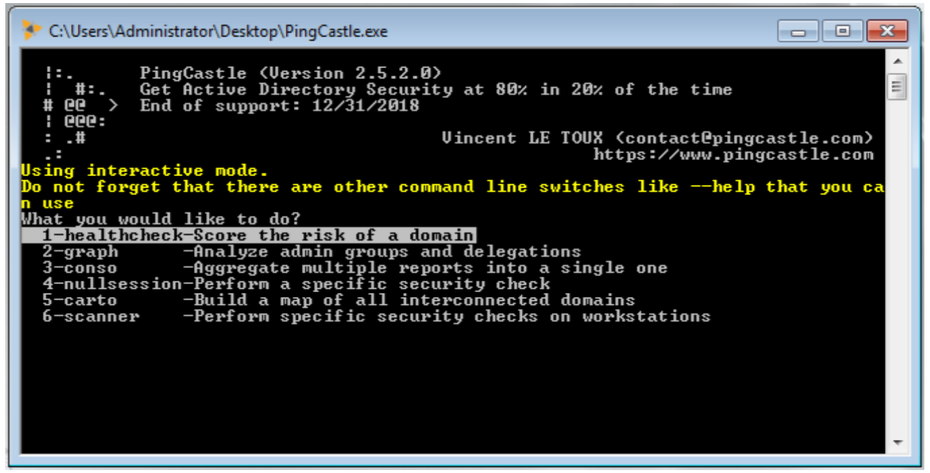
URSIV

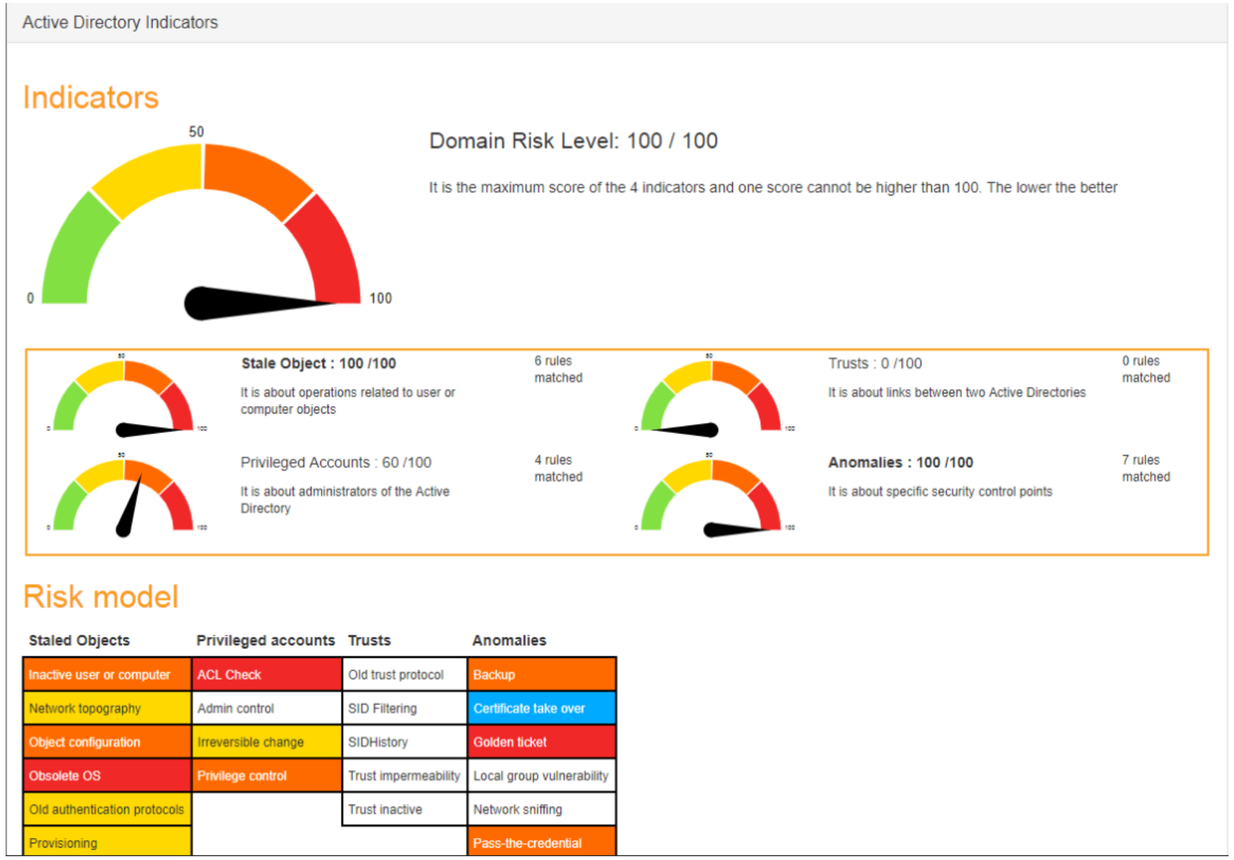
UPORABA NAMENSKIH ORODIJ V NADZORIH 4/10



URSIV

UPORABA NAMENSKIH ORODIJ V NADZORIH 5/10





URSIV

UPORABA NAMENSKIH ORODIJ V NADZORIH 6/10

Ukaz	Razlaga
nmap	Defaultni ukaz za skeniranje omrežij
-sU	Izvede UDP sken
-v	Verbose način (prikaže dodatne podatke)
-p-	Izvede sken vseh **65,535 UDP portov**
-n	ne razrešuj domenskih imen (pospeši hitrost skena)
-T4	Nastavi agresivnost skeniranja, uporabljamo načine od -T0 (tihi način) do -T5 (t.i. božično drevo)
--max-parallelism 256	Nastavitev števila dovoljenih sočasnih preiskav (poveča hitrost skeniranja)
`--min-rate 1000`	Nastavitev minimalnega števila paketov na sekundo (poveča hitro skeniranja)
`-oN Udp_port_scan.txt`	Zapiše razultate v datoteko
`$(cat {ip_list_file})`	Izvorna datoteka z IP, ki jo izbere uporabnik

```
Nmap scan report for [redacted]
Host is up (0.051s latency).
Not shown: 52744 open|filtered udp ports (no-response), 12789 filtered udp ports (port-unreach)
PORT    STATE SERVICE
123/udp open  ntp
161/udp open  snmp
```

```
Nmap scan report for [redacted]
Host is up (0.017s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

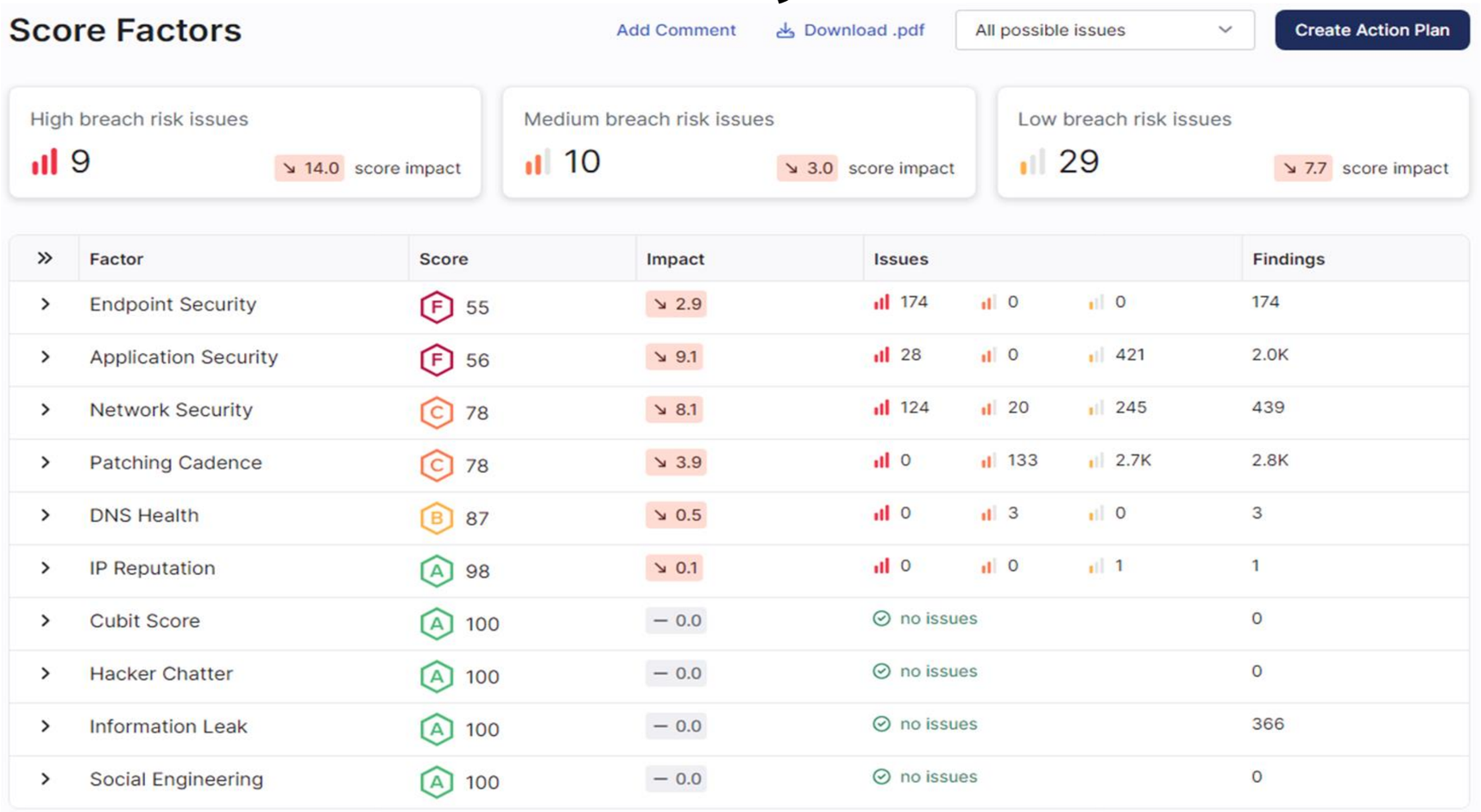
```
Nmap scan report for [redacted]
Host is up (0.017s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

podroben opis ugotovitev

- 123/udp je pokazal različico NTP v4.2.0, ki teče na Juniper napravi z JUNOS15.1X49-D150.2 OS;
- različica NTP v4.2.0 je zastarela (2003), brez posodobitve gre za ranljivo različico (seznam točnih ranljivosti, ugotovljenih z nmap --script=vuln ukazom je dostopen v datoteki Udp_full_scan.txt;
- posodobljena različica NTP je 4.2.8p18 (maj 2024)
- različica OS JUNOS15.1X49-D150.2 je zastarela (2015, end-of-support 2021), brez posodobitve gre za ranljivo različico (seznam ranljivosti je dostopen na spletni strani CVEdetails)
- potencialni vektorji napada so: ponarejanje časa (time spoofing), DDOS skozi NTP ojačitev (amplification), izvršitev oddaljene kode (RCE) preko ranljivosti prekoračitve medpomnilnika (buffer overflow) in razkritje informacij preko neoverjenih poizvedb
- gre za Stratum 3 strežnik, ki se sinhronizira preko [redacted]

URSIV

UPORABA NAMENSKIH ORODIJ V NADZORIH 7/10



Score Factors

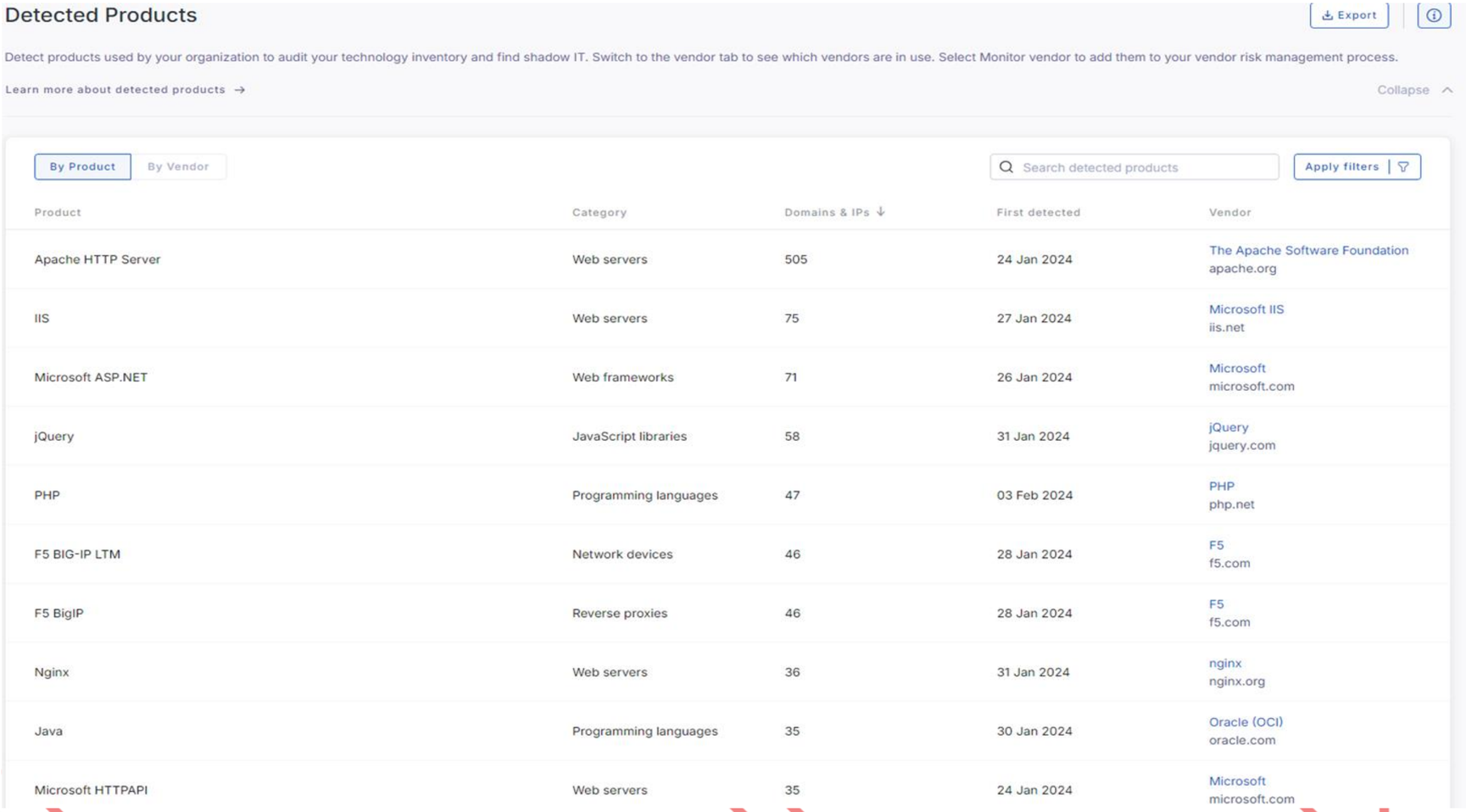
Add Comment | Download .pdf | All possible issues | Create Action Plan

High breach risk issues	Medium breach risk issues	Low breach risk issues
9 — ↘ 14.0 score impact	10 — ↘ 3.0 score impact	29 — ↘ 7.7 score impact

Factor	Score	Impact	Issues			Findings
Endpoint Security	F 55	↘ 2.9	174	0	0	174
Application Security	F 56	↘ 9.1	28	0	421	2.0K
Network Security	C 78	↘ 8.1	124	20	245	439
Patching Cadence	C 78	↘ 3.9	0	133	2.7K	2.8K
DNS Health	B 87	↘ 0.5	0	3	0	3
IP Reputation	A 98	↘ 0.1	0	0	1	1
Cubit Score	A 100	— 0.0	no issues			0
Hacker Chatter	A 100	— 0.0	no issues			0
Information Leak	A 100	— 0.0	no issues			366
Social Engineering	A 100	— 0.0	no issues			0

URSIV

UPORABA NAMENSKIH ORODIJ V NADZORIH 8/10



Detected Products

Export

Detect products used by your organization to audit your technology inventory and find shadow IT. Switch to the vendor tab to see which vendors are in use. Select Monitor vendor to add them to your vendor risk management process.

Learn more about detected products →

Collapse

By Product | By Vendor

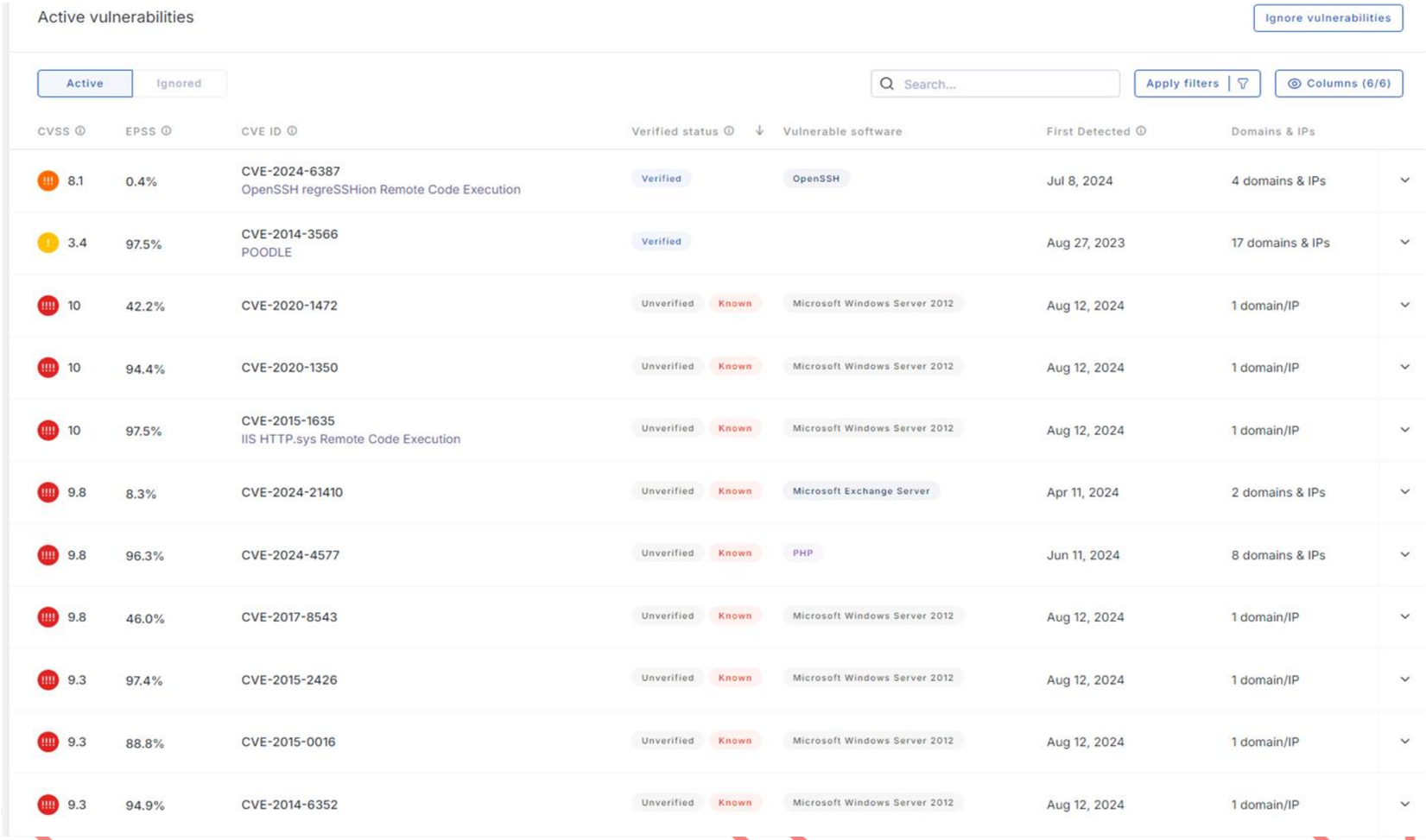
Search detected products

Apply filters

Product	Category	Domains & IPs ↓	First detected	Vendor
Apache HTTP Server	Web servers	505	24 Jan 2024	The Apache Software Foundation apache.org
IIS	Web servers	75	27 Jan 2024	Microsoft IIS iis.net
Microsoft ASP.NET	Web frameworks	71	26 Jan 2024	Microsoft microsoft.com
jQuery	JavaScript libraries	58	31 Jan 2024	jQuery jquery.com
PHP	Programming languages	47	03 Feb 2024	PHP php.net
F5 BIG-IP LTM	Network devices	46	28 Jan 2024	F5 f5.com
F5 BigIP	Reverse proxies	46	28 Jan 2024	F5 f5.com
Nginx	Web servers	36	31 Jan 2024	nginx nginx.org
Java	Programming languages	35	30 Jan 2024	Oracle (OCI) oracle.com
Microsoft HTTPAPI	Web servers	35	24 Jan 2024	Microsoft microsoft.com

URSIV

UPORABA NAMENSKIH ORODIJ V NADZORIH 9/10



Active vulnerabilities

Ignore vulnerabilities

Active | Ignored

Search...

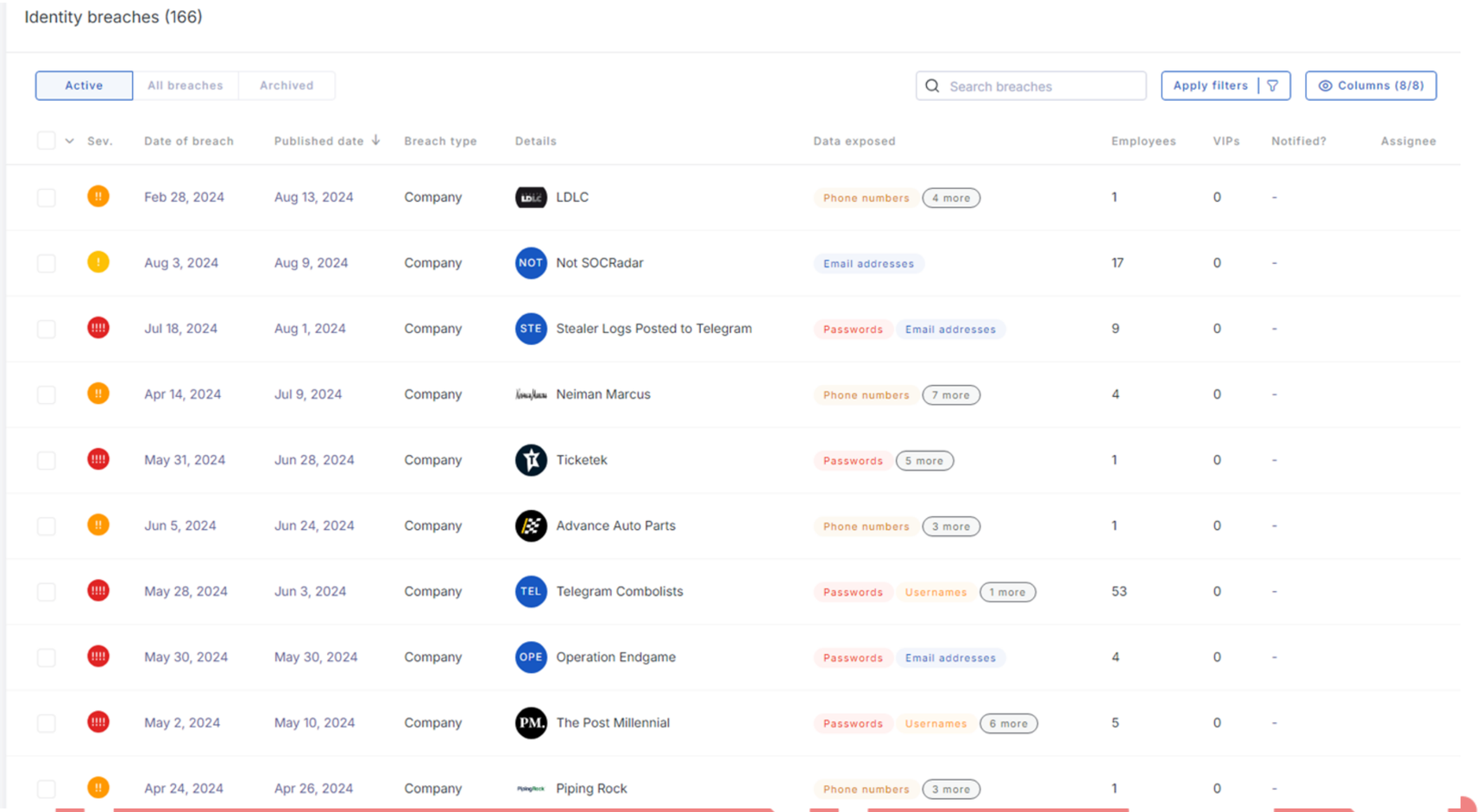
Apply filters

Columns (6/6)

CVSS	EPSS	CVE ID	Verified status	Vulnerable software	First Detected	Domains & IPs
8.1	0.4%	CVE-2024-6387 OpenSSH regreSSHion Remote Code Execution	Verified	OpenSSH	Jul 8, 2024	4 domains & IPs
3.4	97.5%	CVE-2014-3566 POODLE	Verified		Aug 27, 2023	17 domains & IPs
10	42.2%	CVE-2020-1472	Unverified Known	Microsoft Windows Server 2012	Aug 12, 2024	1 domain/IP
10	94.4%	CVE-2020-1350	Unverified Known	Microsoft Windows Server 2012	Aug 12, 2024	1 domain/IP
10	97.5%	CVE-2015-1635 IIS HTTP.sys Remote Code Execution	Unverified Known	Microsoft Windows Server 2012	Aug 12, 2024	1 domain/IP
9.8	8.3%	CVE-2024-21410	Unverified Known	Microsoft Exchange Server	Apr 11, 2024	2 domains & IPs
9.8	96.3%	CVE-2024-4577	Unverified Known	PHP	Jun 11, 2024	8 domains & IPs
9.8	46.0%	CVE-2017-8543	Unverified Known	Microsoft Windows Server 2012	Aug 12, 2024	1 domain/IP
9.3	97.4%	CVE-2015-2426	Unverified Known	Microsoft Windows Server 2012	Aug 12, 2024	1 domain/IP
9.3	88.8%	CVE-2015-0016	Unverified Known	Microsoft Windows Server 2012	Aug 12, 2024	1 domain/IP
9.3	94.9%	CVE-2014-6352	Unverified Known	Microsoft Windows Server 2012	Aug 12, 2024	1 domain/IP

URSIV

UPORABA NAMENSKIH ORODIJ V NADZORIH 10/10



Identity breaches (166)

Active | All breaches | Archived

Search breaches | Apply filters | Columns (8/8)

Sev.	Date of breach	Published date	Breach type	Details	Data exposed	Employees	VIPs	Notified?	Assignee
!!	Feb 28, 2024	Aug 13, 2024	Company	LDLC	Phone numbers, 4 more	1	0	-	
!	Aug 3, 2024	Aug 9, 2024	Company	Not SOCRadar	Email addresses	17	0	-	
!!!!	Jul 18, 2024	Aug 1, 2024	Company	Stealer Logs Posted to Telegram	Passwords, Email addresses	9	0	-	
!!	Apr 14, 2024	Jul 9, 2024	Company	Neiman Marcus	Phone numbers, 7 more	4	0	-	
!!!!	May 31, 2024	Jun 28, 2024	Company	Ticketek	Passwords, 5 more	1	0	-	
!!	Jun 5, 2024	Jun 24, 2024	Company	Advance Auto Parts	Phone numbers, 3 more	1	0	-	
!!!!	May 28, 2024	Jun 3, 2024	Company	Telegram Combolists	Passwords, Usernames, 1 more	53	0	-	
!!!!	May 30, 2024	May 30, 2024	Company	Operation Endgame	Passwords, Email addresses	4	0	-	
!!!!	May 2, 2024	May 10, 2024	Company	The Post Millennial	Passwords, Usernames, 6 more	5	0	-	
!!	Apr 24, 2024	Apr 26, 2024	Company	Piping Rock	Phone numbers, 3 more	1	0	-	

URSIV

UKREPI INŠPEKTORJA – BISTVENI SUBJEKTI

- Odreditev **izvedbe redne ali ciljno usmerjene revizije skladnosti** s predpisi, ki jo izvede PRIS.
- Odreditev **izvedbe izredne revizije skladnosti** s predpisi, ki jo izvede PRIS (pomemben incident ali očitne kršitve).
- Odreditev **obveščanja subjektov**, za katere opravlja storitve ali dejavnost, **o vplivu grožnje in sprejemu o zaščitnih ali popravnih ukrepov**.
- Odreditev **izvedbe priporočil izvedene revizije skladnosti**.
- **Imenovanje pooblaščene osebe**, ki spremlja sklanost z ZInfV-1.
- Odreditev (javne) **objave kršitve ZInfV-1**.

URSIV

UKREPI INŠPEKTORJA – POMEMBNI SUBJEKTI

- Odreditev **izvedbe ciljno usmerjene revizije skladnosti** s predpisi, ki jo izvede PRIS.
- Odreditev **obveščanja subjektov**, za katere opravlja storitve ali dejavnost, **o vplivu grožnje in sprejemu o zaščitnih ali popravnih ukrepov**.
- Odreditev **izvedbe priporočil izvedene ciljno usmerjene revizije skladnosti**.
- Odreditev (javne) **objave kršitve ZInfV-1**.

GLOBE V PREKRŠKOVNEM POSTOPKU PO ZInfV-1 1/2

BISTVENI SUBJEKTI:

- **Od 0,5 % do 2 % skupnega letnega prometa pravne osebe**, doseženega v preteklem poslovnem letu, vendar **ne manj kot 10.000 eurov in ne več kot 10.000.000 eurov**, odvisno od tega, kateri znesek je višji.
- **Od 1.000 eurov do 10.000 eurov za odgovorno osebo pravne osebe** (odgovorna oseba samostojnega podjetnika posameznika, odgovorna oseba posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu).

URSIV

GLOBE V PREKRŠKOVNEM POSTOPKU PO ZInfV-1 2/2

POMEMBNI SUBJEKTI:

- **Od 0,3 odstotka do 1,4 odstotka skupnega letnega prometa pravne osebe**, doseženega v preteklem poslovnem letu, vendar ne manj kot 7.000 eurov in ne več kot 7.000.000 eurov, odvisno od tega, kateri znesek je višji.
- **Od 1.000 eurov do 7.000 eurov se kaznuje odgovorna oseba pravne osebe** (odgovorna oseba samostojnega podjetnika posameznika, odgovorna oseba posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu, samoupravni lokalni skupnosti).

URSIV

ODGOVORNOST ZA KRŠITVE ZAKONA

ENOTIRNI SISTEM UPRAVLJANJA PO ZGD-1:

- **Poslovodstvo** (**upravitelji, direktorji, člani uprave/upravnega odbora**) je po ZGD-1 primarno odgovorno za zakonito poslovanje in sprejemanje potrebnih ukrepov.

DVOTIRNI SISTEM UPRAVLJANJA PO ZGD-1:

- **Poslovodstvo** (**upravitelji, direktorji, člani uprave/upravnega odbora**) **IN**
- **Nadzorni svet,** ki je odgovoren za nadzor in mora spremljati, ali poslovodstvo ravna v skladu z zakonom in akti družbe.

URSIV

RAZBREMENITEV ODOGOVORNOSTI POSLOVODSTVA ZA KRŠITVE ZAKONA V PREKRŠKOVNEM POSTOPKU

Odgovorna oseba pravne osebe je član poslovodstva, drug zastopnik ali oseba, ki je pri pravni osebi zadolžena za nadzor, vodenje ali izvajanje nalog (**14. člen ZP-1**).

Poslovodstvo odgovarja za prekršek, **razen če dokaže**, da je:

- z **aktom pravne osebe ali s pisnim pooblastilom določilo drugo osebo** za izvajanje nadzora in **določenih nalog**;
- pri tem **ravnalo s potrebno skrbnostjo** in
- ima odgovorna oseba, na katero so bile naloge prenesene, **ustrezna pooblastila, pogoje in sredstva za njihovo izvedbo**.

URSIV

PRIMER RAZBREMENITVE ODOGOVORNOSTI POSLOVODSTVA ZA KRŠITVE ZAKONA - ZInfV-1

Poslovodstvo z aktom ali pisnim pooblastilom imenuje odgovorno osebo za informacijsko varnost (CISO), **se odgovornost za prekrške s tega področja prenese nanj**, pod pogojem, da:

- je CISO **dejansko zadolžen za izvajanje teh nalog** in za nadzor varnostnih ukrepov, **ima potrebna pooblastila, ustrezne kompetence in znanje** (dostop do potrebnih virov in odločanja)**;**
- poslovodstvo **pri imenovanju ravna s potrebno skrbnostjo** (**izbira osebe, določitev nalog** in **zagotovitev pogojev za delo**) in
- Poslovodstvo **izvaja dolžno nadzorstvo** nad delom CISO.

URSIV

ODGOVORNOST PRI NAJEMANJU (IT) STORITEV

Za informacijsko varnost je vselej odgovoren zavezanec:

- Da z zunanjim ponudnikom storitev sklene ustrezno pogodbo (ustrezen sporazumom o ravni storitev - SLA) s katero **prenese določene zahteve informacijske / kibernetske varnosti na pogodbenika-dobavitelja**.
- Da **izvaja dolžno nadzorstvo nad izvajanjem storitev in varnostnih zahtev** iz pogodbe.

URSIV

POGOSTA UGOTOVLJENA NESKLADJA / KRŠITVE 1/2

- **Ni izvedenega ustreznega popisa sredstev** (pogosto samo delno, nepopolno ali neažurno).
- **Ni izvedenih popisov poslovnih procesov** (ali so izvedeni samo delno), posledično ni izvedene BIA ali je BIA izvedena neustrezno.
- **Neobvladovanje izvajanja informacijskih storitev pogodbenih izvajalcev** / neučinkovito izvajanje dolžnega nadzorstva nad pogodbeniki.
- **Nedosledno izvajanje postopkov dodelitve in odvzema pravic** pri spremembah ali prekinitvah zaposlitve.

URSIV

POGOSTA UGOTOVLJENA NESKLADJA / KRŠITVE 2/2

- **Neustrezna segmentacija omrežja** (ali je sploh ni).
- **Ni določene minimalne ravni poslovanja.**
- **Ne izvaja se rednega izobraževanja / ozaveščanja zaposlenih** na področju informacijske varnosti.
- **Ne zagotavlja se ustreznih usposabljanj in izpopolnjevanj ključnega IT kadra** (skrbniki IS).
- **Ni preverjanja kakovosti izdelave varnostnih kopij**.
- **Ne zagotavlja se ohranjanja dnevniških zapisov** o delovanju vseh ključnih informacijskih sistemov in delov omrežja.

URSIV

REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

KONFERENCA ZInfV-1
Zakon za kibernetsko varno prihodnost Slovenije

HVALA ZA POZORNOST

Matjaž Mravljak
gp.uiv@gov.si

URSIV
KIBERNETSKO VARNI