REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

URSIV

Praktični vidiki prenosa direktive NIS 2 v novi Zakon o informacijski varnosti

Matjaž Mravljak, direktor Inšpekcije za informacijsko varnost
Urad Vlade Republike Slovenije za informacijsko varnost

Ljubljana, marec 2025

Prenos direktive NIS 2 z novim ZInfV-1

DIREKTIVA (EU) 2022/2555 EVROPSKEGA PARLAMENTA IN SVETA z dne 14. decembra **2022**

o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148

DIREKTIVA (EU) 2016/1148 EVROPSKEGA PARLAMENTA IN SVETA z dne 6. julija 2016

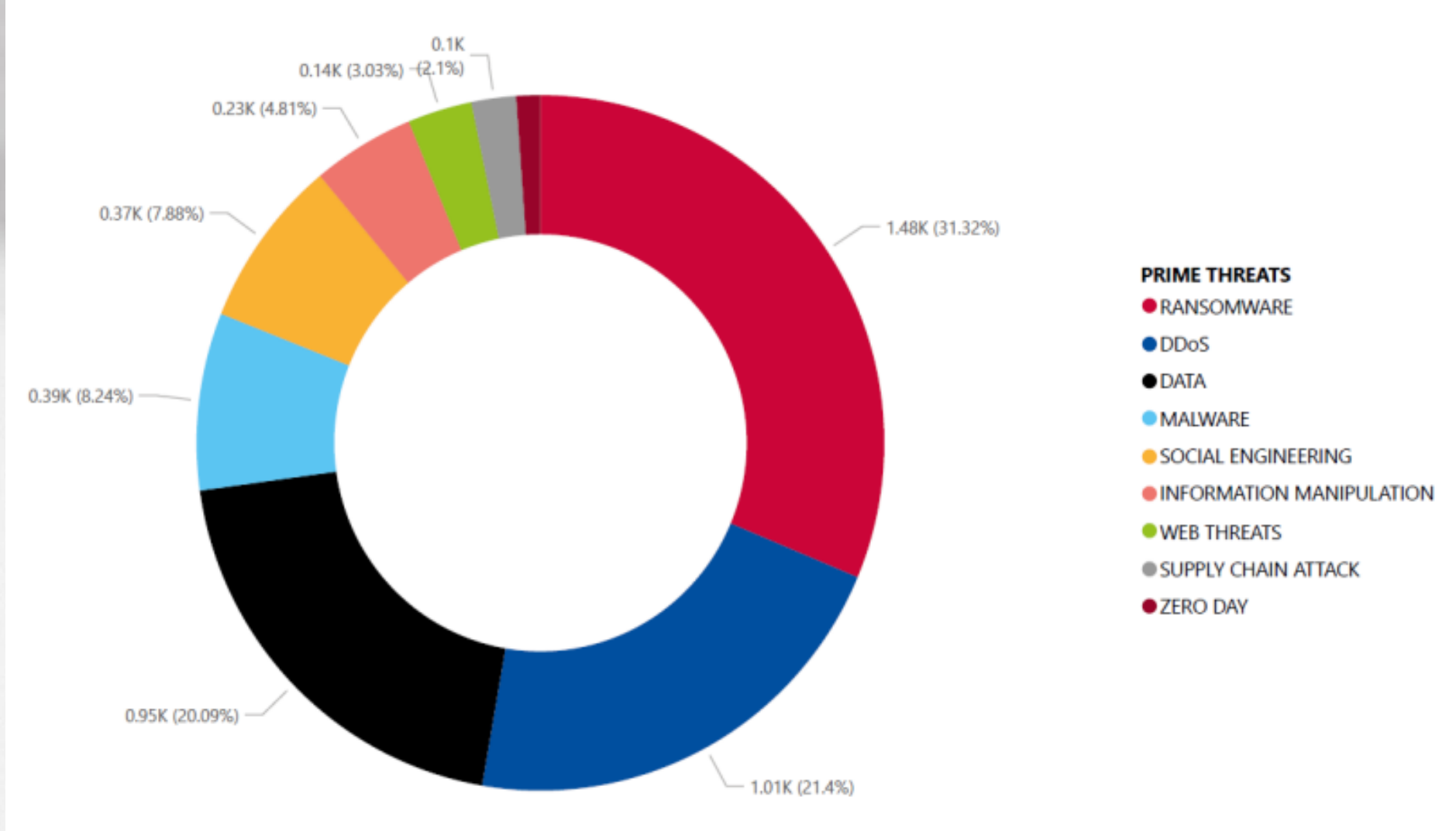
o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji

Uvod v NIS 2

- V Evropski uniji je bilo v 2022 **izvedenih 43 % kibernetskih napadov na mala in srednje velika podjetja**, ki niso imela vzpostavljenih ustreznih varnostnih mehanizmov.
- Od tega **83 % napadenih malih in srednjih podjetij ni bilo pripravljenih na okrevanje po kibernetskem napadu**.
- Vsak dan v 2022 je bilo **v EU poslanih 3,1 milijarde lažnih e-poštnih sporočil**, del teh lažnih sporočil je kljub varnostnim ukrepom pristal v e-poštnih predalih ljudi.
- V Evropski uniji je v 2022 znašala **skupna materialna škoda (posredna in neposredna) zaradi kibernetskih incidentov in napadov približno 150 milijard evrov**.

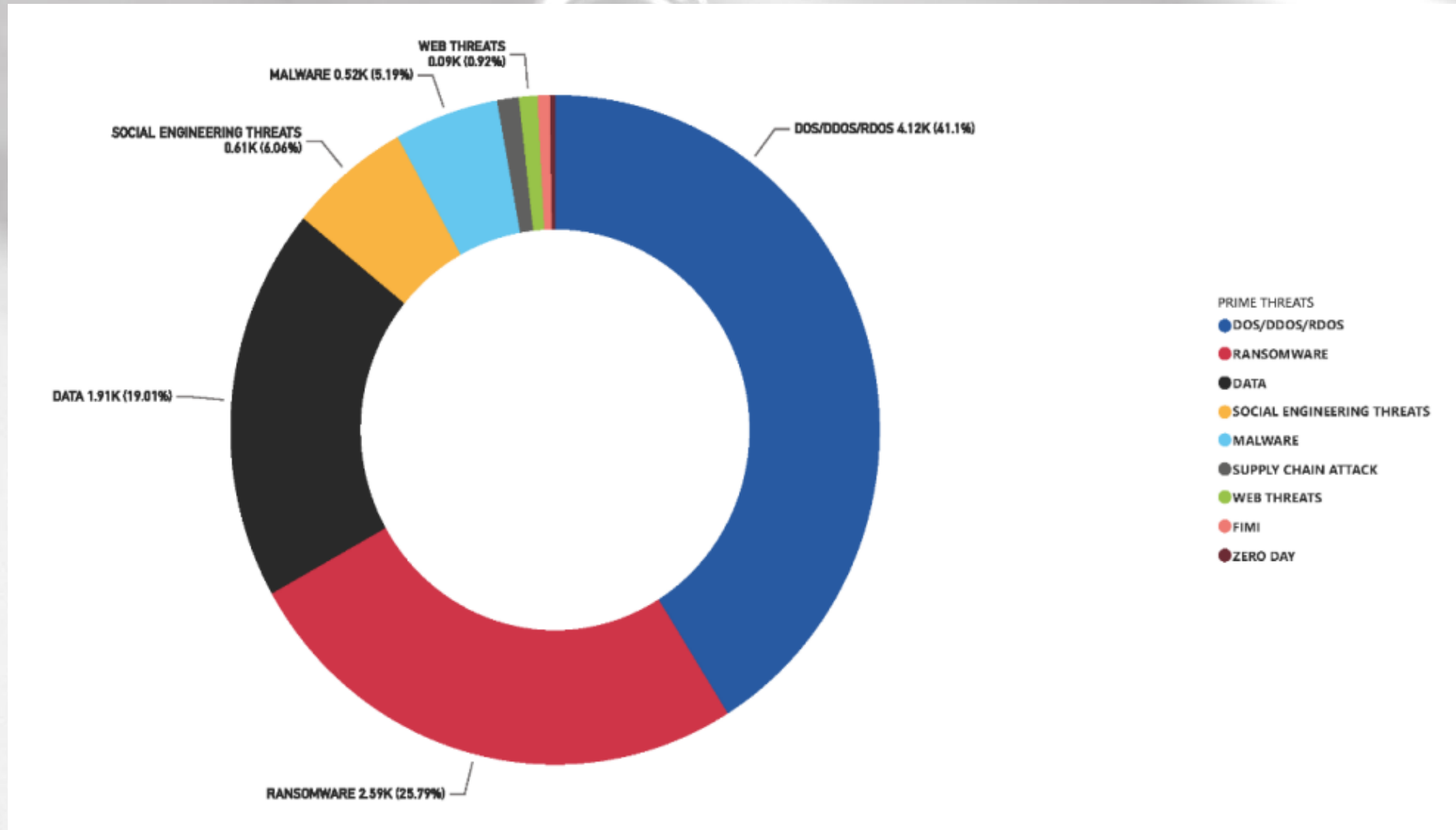
Uvod v NIS 2

Kibernetski incidenti v EU **julij 2022 – julij 2023** (ENISA)



Uvod v NIS 2

Kibernetski incidenti v EU **julij 2023 – julij 2024** (ENISA)



BISTVENI SUBJKEKTI (visoko kritični sektorji)

PRILOGA I: **VISOKO KRITIČNI SEKTORJI**:

1. **energija** (elektrika, daljinsko ogrevanje in hlajenje, nafta, vodik);
2. **promet** (zračni, železniški, vodni, cestni);
3. **bančništvo** (kreditne institucije);
4. **infrastruktura finančnega trga** (upravljalci mest trgovanja, centralne nasprotne stranke);
5. **zdravje** (izvajalci zdravstvenega varstva, referenčni laboratoriji, medicinski pripomočki);
6. **pitna voda** (dobavitelji in distributerji pitne vode – glavna dejavnost);
7. **odpadna voda** (zbiranje, odvajanje in čiščenje odpadne vode – glavna dejavnost);
8. **digitalna infrastruktura** (DNS, TLD, storitve zaupanja, operaterji javnih elektronski komunikacijskih omrežij ali storitev, podatkovni centri, storitve oblaka);
9. **upravljanje storitev IKT** (ponudniki upravljanih varnostnih storitev);
10. **javna uprava** (subjekti javne uprave na državni ravni, druge osebe javnega prava);
11. **vesolje** (upravljalci talne infrastrukture, podpora opravljanja vesoljskih storitev).

POMEMBNI SUBJKEKTI (drugi kritični sektorji)

PRILOGA II - **DRUGI KRITIČNI SEKTORJI**:

1. **poštne in kurirske storitve** (izvajalci določenih poštnih in kurirskih storitev);
2. **ravnanje z odpadki** (izvajalci – glavna dejavnost);
3. **izdelava, proizvodnja in distribucija kemikalij** (proizvodnja in distribucija določenih snovi);
4. **pridelava, predelava in distribucija živil** (prodaja na debelo, industrijska pri(e)delava);
5. **proizvodnja določenih vrst izdelkov** (medicinski pripomočki; računalniki, elektronski in optični izdelki, proizvodnja električnih naprav, proizvodnja drugih strojev in naprav, proizvodnja motornih vozil, prikolic, polprikolic, proizvodnja drugih vozil in plovil);
6. **digitalni ponudniki** (spletne tržnice, spletni iskalniki, platforme storitev družbenega mreženja);
7. **raziskave** (raziskovalne organizacije)
8. **javna uprava** (lokalna samouprava – mestne občine).

ZAVEZANCI (drugi subjekti javne uprave-državna raven)

PRILOGA III - **DRUGI SUBJEKTI JAVNE UPRAVE NA DRŽAVNI RAVNI (bistveni subjekti)**:

1. **javne agencije** (Javna agencija za civilno letalstvo, Agencija za energijo, ipd. - 14);
2. **javni skladi** (Eko sklad, Stanovanjski sklad RS, ipd. - 7);
3. **javni zavodi** (RTV, Državni izpitni center, Slovenska akreditacija, ipd. - 13);
4. **druge osebe javnega prava oziroma neodvisni državni organi** (DVK, KPK, Informacijski pooblaščenec, ipd. - 5);

ZAVEZANCI po ZInfV-1

SUBJEKTI (so zavezanci iz predloga ZInfV-1)**, ki:**

- spadajo med vrste subjektov iz Prilog 1 ali 2, **če imajo vsaj 50 zaposlenih in letni promet** (ali letno bilančno vsoto) **vsaj 10 milijonov eurov**.
- spadajo med vrste subjektov iz Prilog 1 ali 2, **ne glede na število zaposlenih ali letni promet**, **če so**: ponudniki javnih elektronskih komunikacijskih omrežij ali storitev; ponudniki storitev zaupanja; registri vrhnjih domenskih imen; ponudniki storitev sistema domenskih imen; subjekti javne uprave na državni ravni; je subjekt edini ponudnik storitve, ki je bistvena za ohranjanje kritičnih družbenih ali gospodarskih dejavnosti v Republiki Sloveniji; bi motnja pri opravljanju storitve subjekta lahko pomembno vplivala na javni red, javno varnost ali javno zdravje; je subjekt kritičen zaradi njegovega posebnega pomena na državni, pokrajinski/lokalni ravni za določen sektor ali vrsto storitve ali za druge medsebojno odvisne sektorje v Republiki Sloveniji ali **je subjekt javne uprave na državni ravni**.

ZAVEZANCI po ZInfV-1

BISTVENI SUBJEKTI:

- Vsi subjekti, iz Priloge Direktive 2022/2555 **I**, ki imajo **vsaj 250 zaposlenih** in **letni promet vsaj 50 milijonov EUR** oziroma letno bilančno vsoto vsaj 42 milijonov EUR.
- **Ponudniki** kvalificiranih storitev zaupanja in registri vrhnjih domenskih imen ter ponudniki storitev DNS, **ne glede na njihovo velikost**.
- Ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, ki imajo **vsaj 50 zaposlenih** in letni promet oziroma **letno bilančno vsoto vsaj 10 milijonov EUR**.
- **Subjekti javne uprave na državni ravni** (izrecno navedeni in iz Priloge 3).
- Subjekti, ki so določeni kot kritični na podlagi zakona, ki ureja kritično infrastrukturo.
- Vsi drugi subjekti vrste iz Prilog Direktive 2022/2555 I ali II, ki jih na predlog pristojnega nacionalnega organa **določi vlada z odločbo**.

ZAVEZANCI po ZInfV-1

POMEMBNI SUBJEKTI:

- Vsi subjekti, ki izvajajo vrste dejavnosti iz **Prilog I in II**, in niso določeni kot bistveni subjekti, imajo pa **vsaj 50 zaposlenih** in letni promet oziroma **letno bilančno vsoto vsaj 10 milijonov EUR**.
- Ponudniki nekvalificiranih storitev zaupanja (ne glede na velikost).
- Subjekti, ki so v državnih načrtih zaščite in reševanja opredeljeni kot **službe državnega pomena**, če bi nedelovanje njihovih omrežnih in informacijskih sistemov ogrozilo izvajanje nalog zaščite in reševanja.
- **Mestne občine**.
- Subjekti iz Prilog I in II Direktive, ki jih na podlagi zakonskih kriterijev **določi vlada z odločbo.**

OBVEZNOSTI ZAVEZANCEV

OBVEZNOSTI BISTVENIH IN POMEMBNIH SUBJEKTOV:

- **izvedba samo-registracije** v aplikaciji pri PNO (register ENISA za sektor digitalne infrastrukture)
- **obvezno usposabljanje članov poslovodnih organov** na področju obvladovanja tveganj kibernetske varnosti (vsake 4 leta)
- **priprava in vzdrževanje predpisane varnostne dokumentacije**
- **implementacija (varnostnih) ukrepov** za obvladovanje tveganj za kibernetsko varnost
- **priglašanje kibernetskih incidentov** pristojnemu CSIRT
- **uporaba evropskih in mednarodnih standardov** ter tehničnih specifikacij in kvalificiranih storitev zaupanja (v čim večji meri, **kjer to ne bo obvezno**)
- upoštevanje izvedbenih aktov Evropske komisije

RAZLIKE MED ZAVEZANCI

RAZLIKE PRI BISTVENIH IN POMEMBNIH SUBJEKTIH:

- izvajanje **periodične revizije skladnosti** sprejetih ukrepov in izvajanje **periodične samoocene skladnosti** sprejetih ukrepov (na dve leti),
- **izvajanje nadzora nad zavezanci**: *ex-ante* in *ex-post* nadzori – pogoji za uvedbo nadzora in ukrepi inšpektorja in
- **višina predpisanih glob** zaradi kršitve zakona.

VARNOSTNA DOKUMENTACIJA

PREDPISANA VARNOSTNA DOKUMENTACIJA ZAVEZANCEV:

1. ***politika oziroma področne politike*** *o varnosti omrežnih in informacijskih sistemov;*

2. natančen in posodobljen **popis informacijskih in drugih sredstev ter podatkov**, potrebnih za nemoteno delovanje omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev ter določitev njihovih upravljavcev;

3. **analiza obvladovanja tveganj**, vključno z določitvijo sprejemljive ravni tveganja in opisano uporabljeno metodologijo;

4. **politika in načrt neprekinjenega poslovanja**, vključno z **oceno vpliva na poslovanje**, navedbo postopkov zagotavljanja neprekinjenega poslovanja, določitvijo minimalne ravni poslovanja, upravljanjem varnostnih kopij in določitvijo vlog ter odgovornosti;

VARNOSTNA DOKUMENTACIJA

PREDPISANA VARNOSTNA DOKUMENTACIJA ZAVEZANCEV:

5. **načrt obnovitve in ponovne vzpostavitve delovanja omrežnih in informacijskih sistemov**, ki jih potrebujejo za svoje delovanje ali opravljanje storitev, vključno z opisom odgovornosti in postopkov za obnovitev delovanja teh sistemov po dogodku, ki povzroči prekinitev njihovega delovanja;

6. **načrt odzivanja na incidente** s protokolom obveščanja pristojnega CSIRT, vključno z opisom sistema za zaznavo in odziv na incidente informacijske varnosti ter opisom vlog in odgovornosti za odzivanje na incidente;

VARNOSTNA DOKUMENTACIJA

PREDPISANA VARNOSTNA DOKUMENTACIJA ZAVEZANCEV:

7. **načrt varnostnih ukrepov** za zagotavljanje celovitosti, avtentičnosti, zaupnosti in razpoložljivosti omrežnih in informacijskih sistemov oziroma za obvladovanje tveganj za kibernetsko varnost, ki upošteva in področne posebnosti bistvenega ali pomembnega subjekta.

8. **politika s postopki za oceno učinkovitosti varnostnih ukrepov** za obvladovanje tveganj za informacijsko in kibernetsko varnost, vključno z določitvijo kazalnikov učinkovitosti in izvedeno analizo zbranih podatkov.

MINIMALNI VARNOSTNI UKREPI

UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ:

- Zavezanci morajo pri izbiri varnostnih ukrepov **upoštevati najsodobnejše in ustrezne evropske ter mednarodne standarde**.
- Varnostni ukrepi **morajo zagotavljati raven varnosti** omrežnih in informacijskih sistemov, **ki ustreza obstoječim oziroma prepoznanim tveganjem**.
- Zavezanci morajo pri **ocenjevanju sorazmernosti varnostnih ukrepov** ustrezno upoštevati:

- stopnjo izpostavljenosti tveganjem (inherentna vs. rezidualna tveganja),

- velikost subjekta (lokacijska razpršenost),

- verjetnost pojava incidentov (predhodni podatki) in

- resnost morebitnih incidentov, vključno z njihovim družbenim ter gospodarskim (tudi čezmejnim) vplivom (potencialni učinek).

MINIMALNI VARNOSTNI UKREPI

UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ:

Varnostni ukrepi morajo temeljiti na pristopu **upoštevanja vseh nevarnosti**, in morajo obsegati **najmanj**:

1. **podporo vodstva subjekta** pri zagotavljanju informacijske in kibernetske varnosti in vključitvijo področja informacijske in kibernetske varnosti v letni načrt poslovanja oziroma letni program dela;
2. **zagotavljanje integritete kadrov** v povezavi z informacijsko varnostjo pred zaposlitvijo, med zaposlitvijo in ob prenehanju ali spremembi zaposlitve (*preverjanje preteklosti za ključen kader - alternativno*);
3. ***osnovne prakse kibernetske higiene in usposabljanje*** na področju informacijske in kibernetske varnosti;

MINIMALNI VARNOSTNI UKREPI

UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ:

4. **varnost človeških virov**, preverjanje identitete uporabnikov, zagotavljanje ravni dostopnosti informacij in upravljanje pooblastil za dostop;
5. **izvajanje in upravljanje varnostnih kopij podatkov**;
6. **zagotavljanje in ohranjanje dnevniških zapisov** o delovanju omrežnih in informacijskih sistemov;
7. **upravljanje omrežnih in informacijskih sistemov**, ki jih uporabljajo za svoje delovanje ali opravljanje storitev z **določitvijo odgovornosti za njihovo zaščito**;
8. politike in postopke v zvezi z **uporabo kriptografije** in po potrebi s šifriranjem;

MINIMALNI VARNOSTNI UKREPI

UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ:

9. **upravljanje prometa in komunikacij**;

10. **varnost dobavne verige** z določitvijo ustreznih minimalnih zahtev povezanih s kibernetsko varnostjo za ključne dobavitelje ali ponudnike storitev;

11. **fizično in tehnično varovanje** prostorov in dostopov do prostorov, kjer so ključni deli omrežnih in informacijskih sistemov, ki jih uporabljajo za svoje delovanje ali opravljanje storitev;

12. **varnostne mehanizme v aplikativni programski opremi** za izvajanje dejavnosti, vključno z varnostjo pri pridobivanju, razvoju in vzdrževanju omrežnih in informacijskih sistemov ter ***obravnavanjem in razkrivanjem ranljivosti;***

MINIMALNI VARNOSTNI UKREPI

UKREPI ZA OBVLADOVANJE KIBERNETSKIH TVEGANJ:

13. **upravljanje in preprečevanje izrab tehničnih ranljivosti**;
14. **zaščito pred zlonamerno programsko kodo, zaznavanje poskusov vdorov in preprečevanje incidentov**;
15. **uporabo večfaktorske avtentikacije** ali rešitev neprekinjene avtentikacije, kadar je to potrebno zaradi obvladovanja tveganj za kibernetsko varnost;
16. **uporabo varovanih glasovnih, video in besedilnih komunikacij in varnih sistemov za komunikacije v sili znotraj subjekta,** kadar je glede na dejavnost subjekta to primerno;
17. **politike in postopke v zvezi z uporabo oblačnih storitev**, ki jih uporabljajo za svoje delovanje ali opravljanje storitev.

POOBLASTILA INŠPEKTORJA (ZInfV-1)

- opraviti inšpekcijski pregled na kraju samem in nadzor na daljavo, ki ju lahko izvede skupaj z usposobljenimi strokovnjaki;
- opraviti inšpekcijski varnostni pregled, ki temelji na objektivnih, nediskriminatornih, poštenih in preglednih merilih za oceno tveganj;
- opraviti neposreden vpogled v podatke, dokumentacijo ter v omrežne in informacijske sisteme;
- preveriti pogoje in način izvajanja ukrepov za obvladovanje tveganj kibernetske varnosti;

POOBLASTILA INŠPEKTORJA (ZInfV-1)

- pregledati območja, objekte in prostore zavezancev, kjer se nahajajo ključni, krmilni in nadzorni informacijski sistemi ter podatki;
- pregledati dokumentacijo o izvrševanju predpisanih obveznosti obveščanja o kibernetskih incidentih ter drugih obveznostih na podlagi zahtev pristojnih organov;
- pregledati poročila o izvedbi revizije informacijskih sistemov in varnostnih pregledov omrežja ter informacijskih sistemov;
- pregledati drugo dokumentacijo, potrebno za izvedbo nadzora.

UKREPI INŠPEKTORJA - BISTVENI SUBJEKTI (ZInfV-1)

- lahko **odredi izvedbo redne in ciljno usmerjene revizije skladnosti** s predpisi s področja informacijske in kibernetske varnosti, ki jo **izvede revizor informacijskih sistemov;**
- lahko **odredi**, da zavezanec v razumnem roku **izvede priporočila, dana na podlagi izvedene revizije skladnosti;**
- lahko **odredi** zavezancu, **da obvesti fizične ali pravne osebe, v zvezi s katerimi opravlja storitve ali izvaja dejavnost**, na katere bi lahko vplivala pomembna kibernetska grožnja, o naravi grožnje, pa tudi o zaščitnih ali popravnih ukrepih, ki jih lahko te fizične ali pravne osebe sprejmejo v odziv na to grožnjo;
- lahko **imenuje pooblaščeno osebo** z natančno opredeljenimi nalogami v določenem obdobju, ki **spremlja izpolnjevanje določenih določb zakona;**
- lahko odredi, da **zavezanec na določen način objavi kršitve zakona.**

UKREPI INŠPEKTORJA - POMEMBNI SUBJEKTI (ZInfV-1)

- lahko **odredi izvedbo ciljno usmerjene revizije skladnosti** s predpisi s področja informacijske in kibernetske varnosti, ki jo **izvede revizor informacijskih sistemov;**
- lahko odredi, da zavezanec v razumnem roku **izvede priporočila,** dana **na podlagi ciljno usmerjene revizije skladnosti;**
- lahko **odredi, da zavezanec obvesti fizične ali pravne osebe, v zvezi s katerimi opravlja storitve ali izvaja dejavnost**, na katere bi lahko vplivala pomembna kibernetska grožnja, o naravi grožnje, pa tudi o zaščitnih ali popravnih ukrepih, ki jih lahko te fizične ali pravne osebe sprejmejo v odziv na to grožnjo;
- lahko odredi, da **zavezanec na določen način objavi kršitve zakona.**

Potek izvedbe inšpekcijskega nadzora

- **Pisna najava inšpekcijskega nadzora.**
- **Predhodno pridobivanje podatkov od drugih organov,** iz **odprtih virov** in **orodij**.
- **Zbiranje, pregled in presoja interne dokumentacije**, katero predpisujeta ZInfV oziroma podzakonski predpis.
- **Razgovori s pristojnimi predstavniki zavezanca** in drugimi zaposlenimi.
- **Pregledi lokacij**, kjer se izvajajo aktivnosti, povezane z izvajanjem bistvenih storitev.
- **Posredovanje pisnih vprašanj** zavezancu.
- **Pridobivanje in presoja dokazil** o izvajanju predpisanih ukrepov.
- **Izvedba testiranj izvajanja minimalnih varnostnih ukrepov**.

Zakonsko predpisana dokumentacija zavezancev

- **Seznam ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov**, ki so bistvenega pomena za delovanje bistvenih storitev
- **Načrt obnovitve in ponovne vzpostavitve delovanja informacijskih sistemov** iz prejšnje alineje
- **Analiza obvladovanja tveganj** z **oceno sprejemljive ravni tveganj**
- **Politika neprekinjenega poslovanja z Načrtom neprekinjenega poslovanja**
- **Načrt odzivanja na incidente s protokolom obveščanja CSIRT**
- **Načrt varnostnih ukrepov** za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov.

Upoštevanje Uredbe o varnostni dokumentaciji in varnostnih ukrepih...

Faze izvedbe inšpekcijskega nadzora

FAZA PRIPRAVE:

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

Faze izvedbe inšpekcijskega nadzora

FAZA IZVEDBE:

- **Zbiranje, pregled in presoja internih dokumentov** (pogodb), katere predpisujeta ZInfV oziroma podzakonski predpis.
- **Razgovori s pristojnimi predstavniki zavezanca** in (po potrebi) z drugimi zaposlenimi.
- **Pregledi lokacij**, kjer se izvajajo aktivnosti, povezane z izvajanjem bistvenih storitev.
- **Pridobitev in presoja dokazil** o izvajanju predpisanih ukrepov.
- **Pisna vprašanja** zavezancu.
- **Izvedba različnh testiranj izvajanja minimalnih varnostnih ukrepov**.

Faze izvedbe inšpekcijskega nadzora

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, ukrepov in dogovor o predlaganih rokih za izvedbo ukrepov.
- **Izvedba notranjega kolegijskega pregleda** zapisnika o inšpekcijskem nadzoru.
- **Podpis in vročitev zapisnika** o inšpekcijskem nadzoru zavezancu.

Uporaba dostopnih orodij v inšpekcijskem nadzoru

DNSViz is a tool for visualizing the status of a DNS zone. It was designed as a resource for understanding and troubleshooting deployment of the DNS Security Extensions (DNSSEC). It provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace, and it lists configuration errors detected by the tool. Your feedback is appreciated.

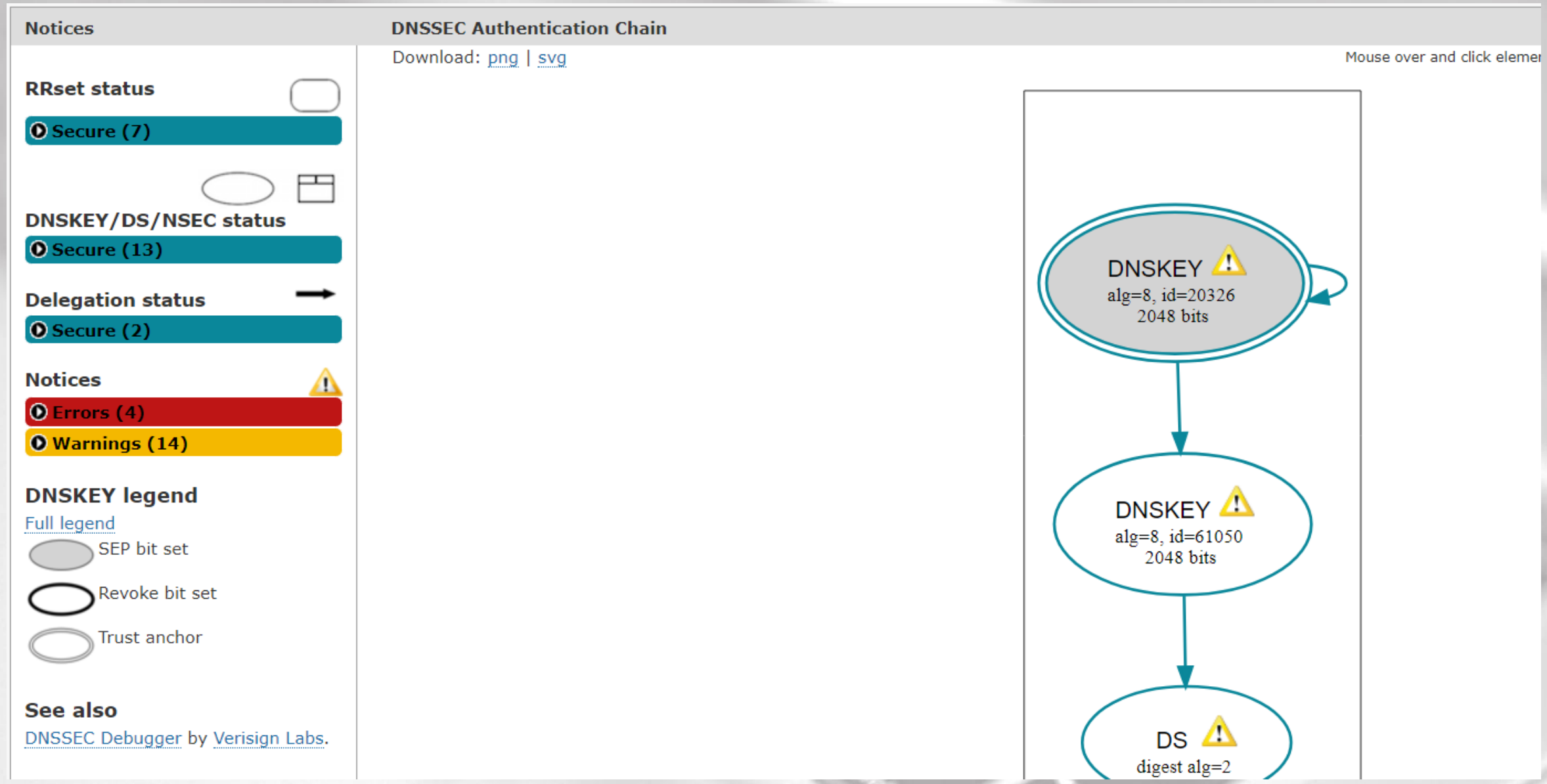
Post

Enter a domain name

Go »

e.g., www.example.com

Uporaba dostopnih orodij v inšpekcijskem nadzoru

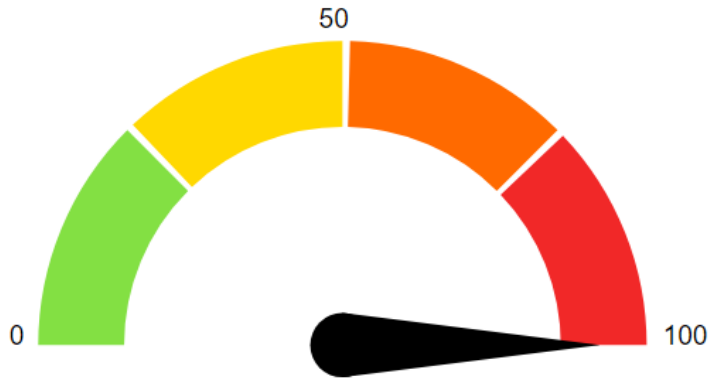


Uporaba dostopnih orodij v inšpekcijskem nadzoru

Active Directory Indicators

This section focuses on the core security indicators.
Locate the sub-process determining the score and fix some rules in that area to get a score improvement.

Indicators

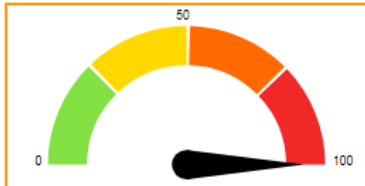


Domain Risk Level: 100 / 100

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

Compare with statistics

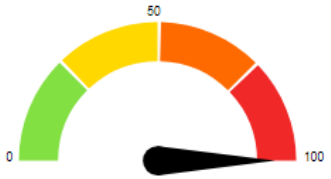
Privacy notice



Stale Object : 100 /100

It is about operations related to user or computer objects

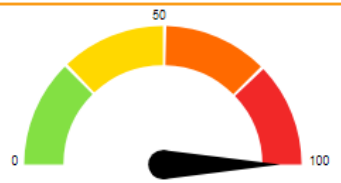
16 rules matched



Privileged Accounts : 100 /100

It is about administrators of the Active Directory

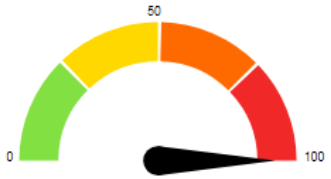
21 rules matched



Trusts : 100 /100

It is about links between two Active Directories

6 rules matched

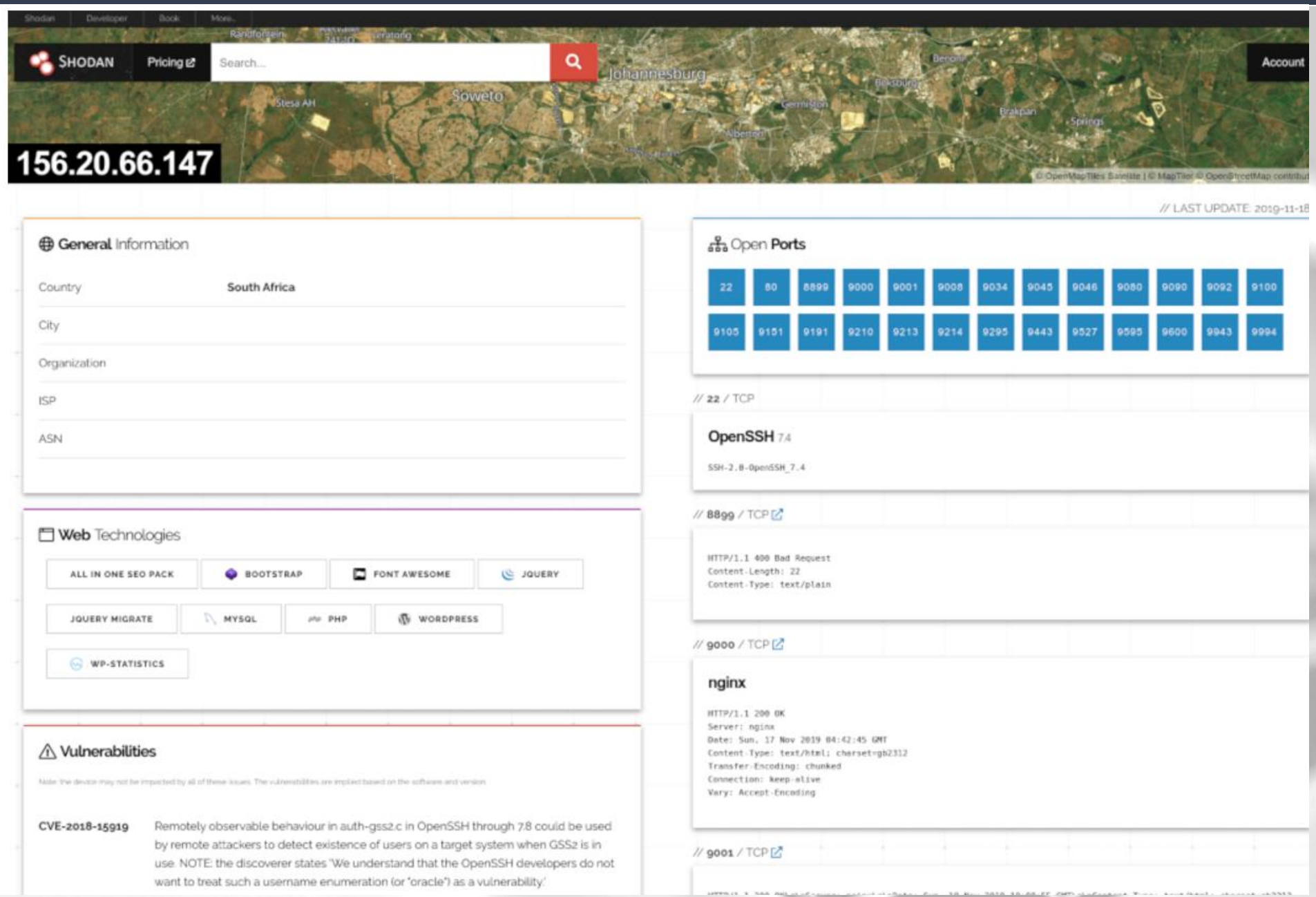


Anomalies : 100 /100

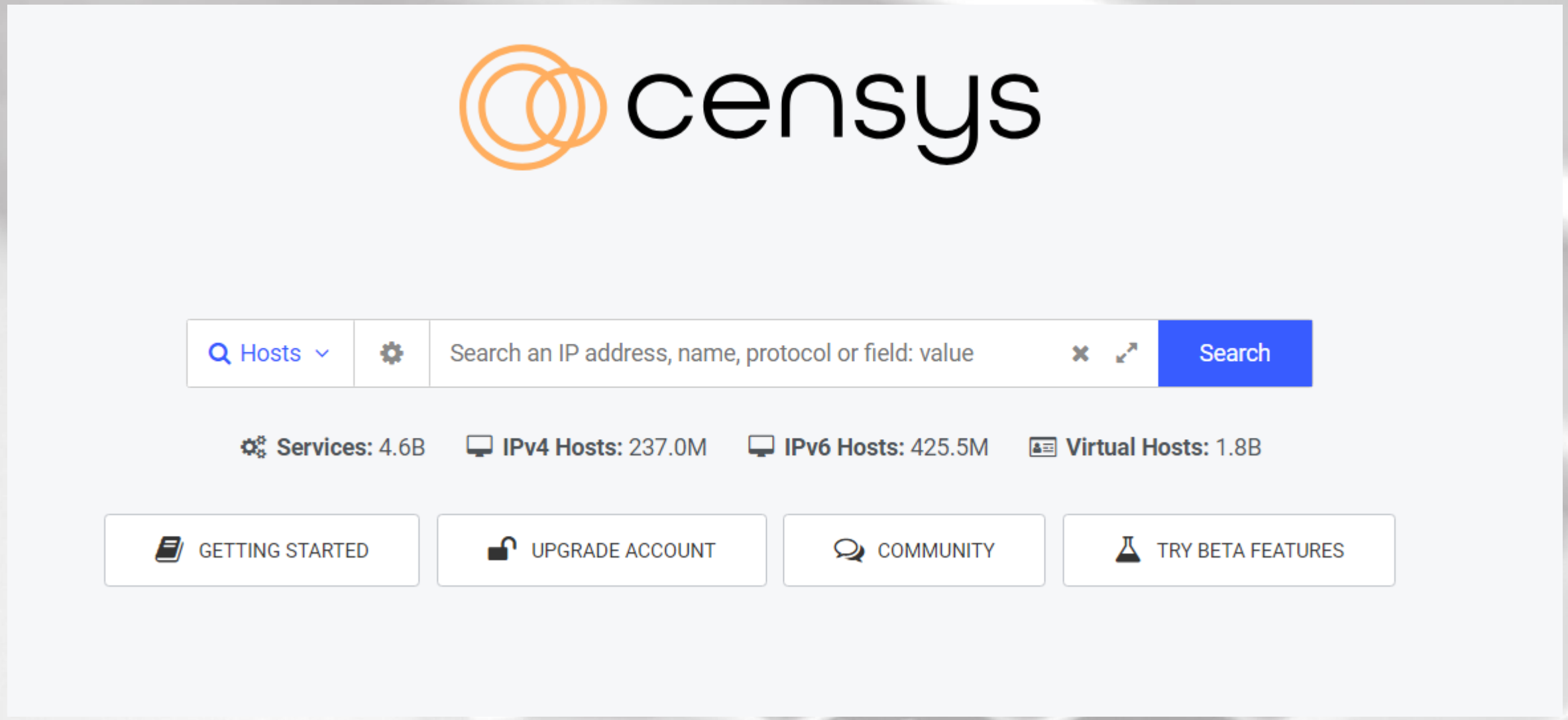
It is about specific security control points

35 rules matched

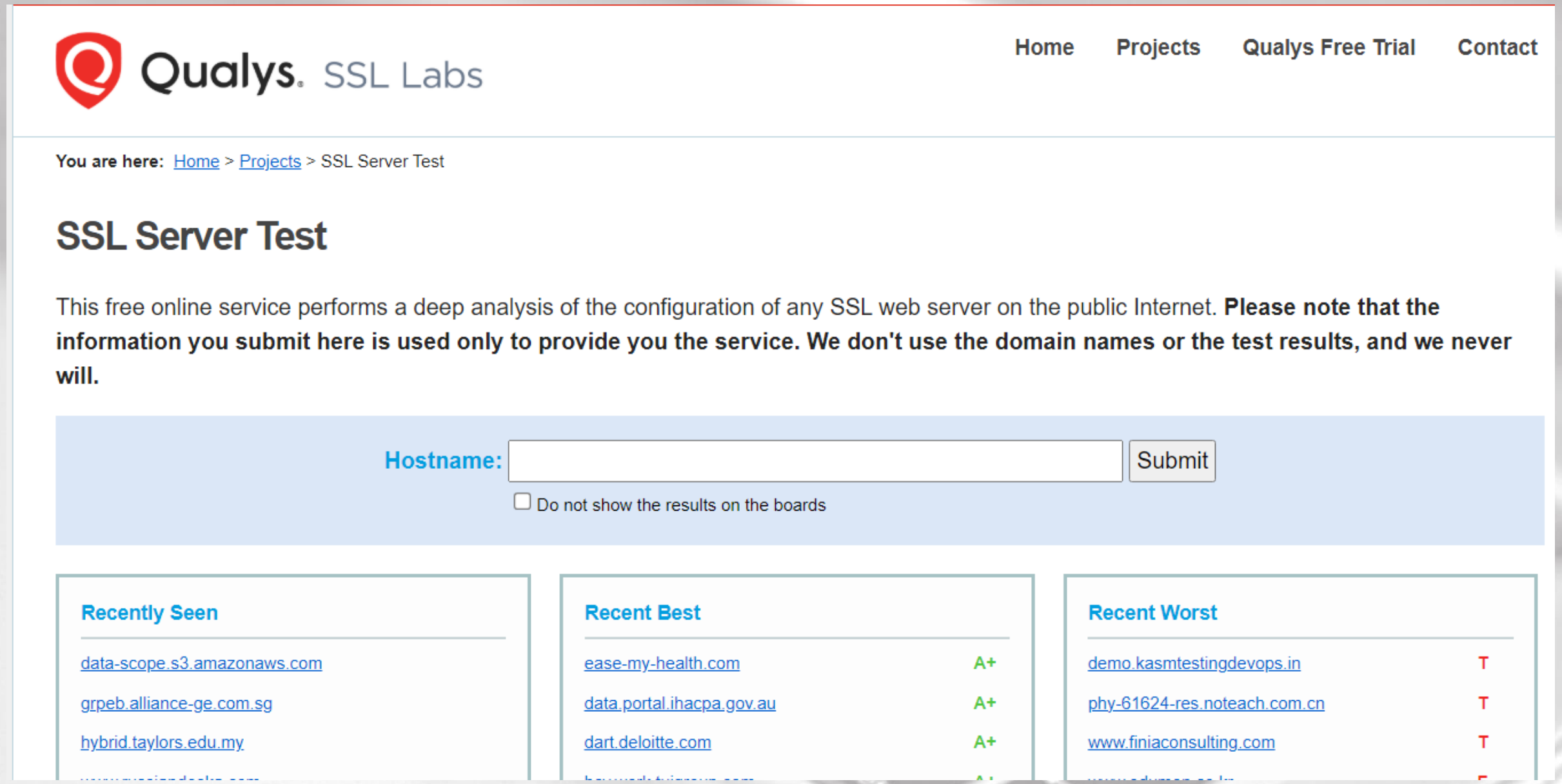
Uporaba dostopnih orodij v inšpekcijskem nadzoru



Uporaba dostopnih orodij v inšpekcijskem nadzoru



Uporaba dostopnih orodij v inšpekcijskem nadzoru



Uporaba namenskih orodij v inšpekcijskem nadzoru

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

Uporaba namenskih orodij v inšpekcijskem nadzoru

Factor	Score	Impact	Issues			Findings
Endpoint Security	F 55	↘ 2.9	174	0	0	174

Detecting unprotected endpoints or entry points of user tools, such as desktops, laptops, mobile devices, and virtual desktops

High breach risk 174 findings

- Outdated Operating System Observed 10
- Outdated Web Browser Observed 164

Medium breach risk

No medium risk issues to detect for this factor

Low breach risk

Browser Average Age Indicates Older Versions 0

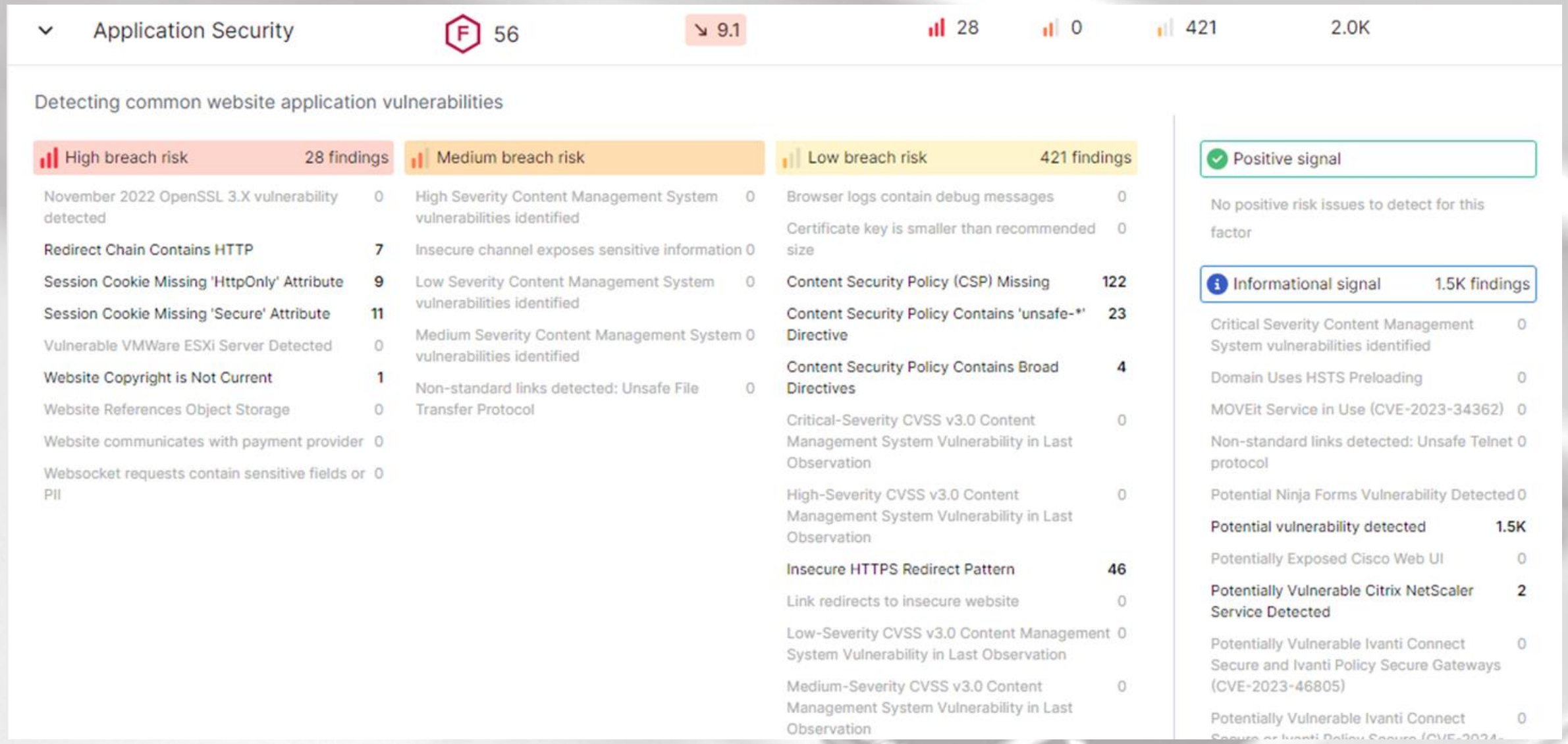
Positive signal

No positive risk issues to detect for this factor

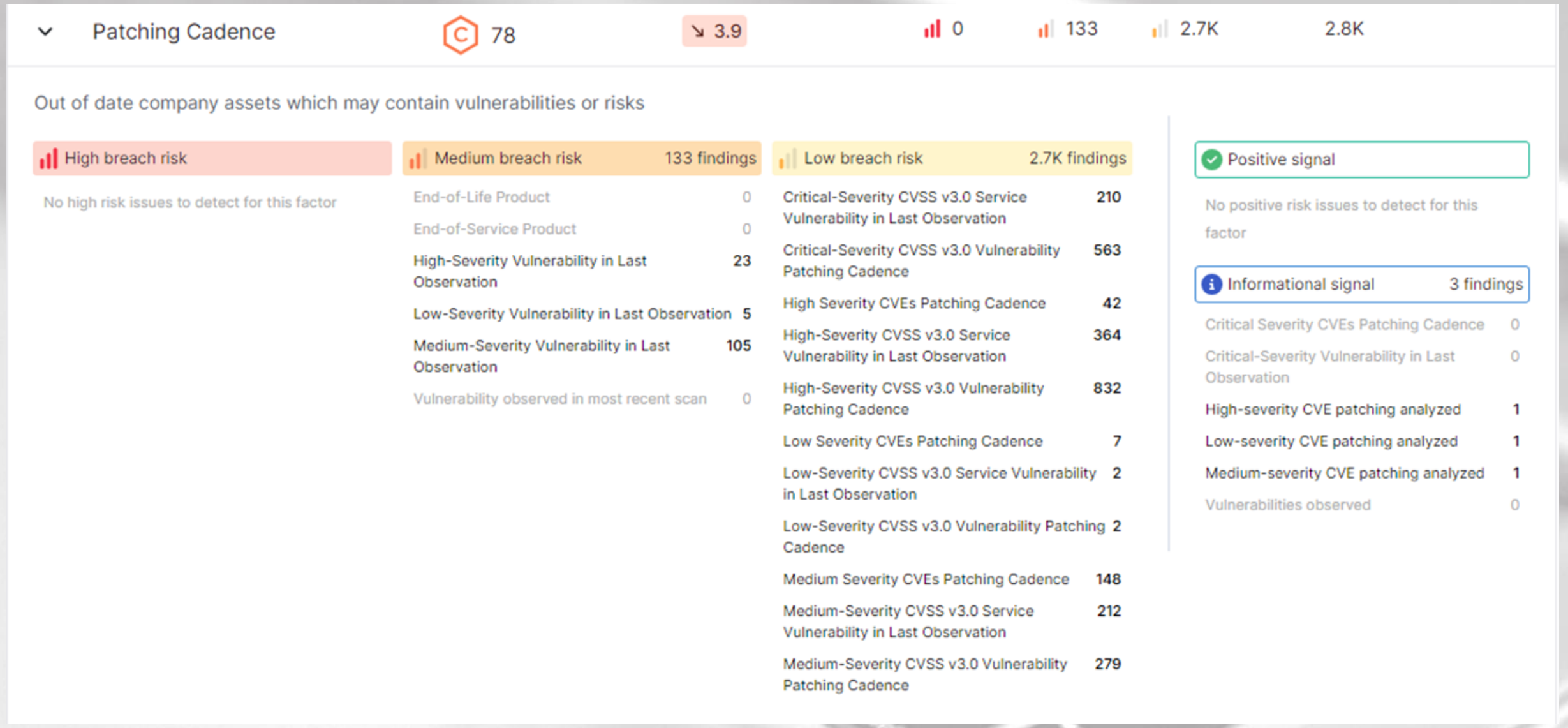
Informational signal

No info risk issues to detect for this factor

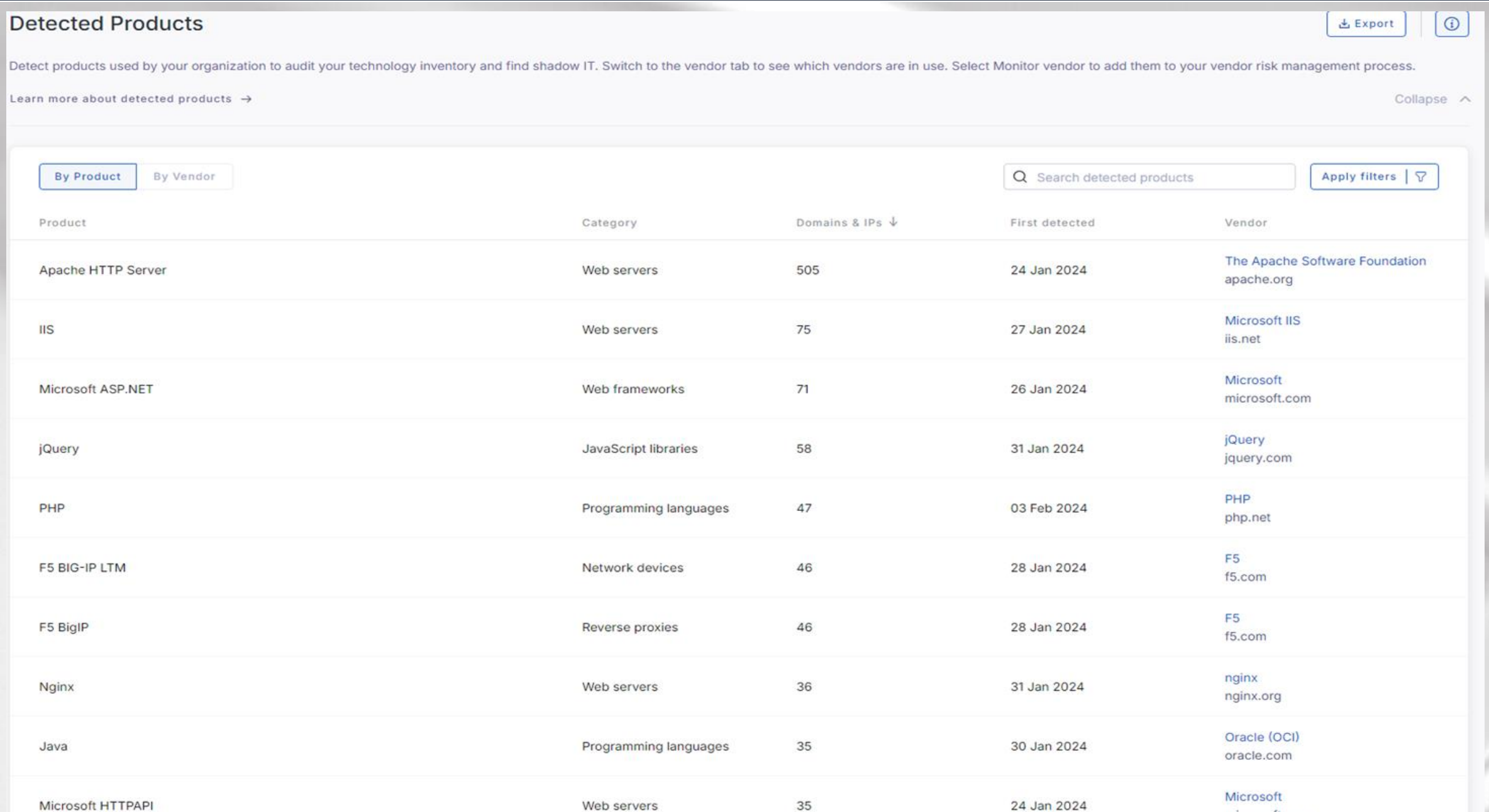
Uporaba namenskih orodij v inšpekcijskem nadzoru



Uporaba namenskih orodij v inšpekcijskem nadzoru



Uporaba namenskih orodij v inšpekcijskem nadzoru



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

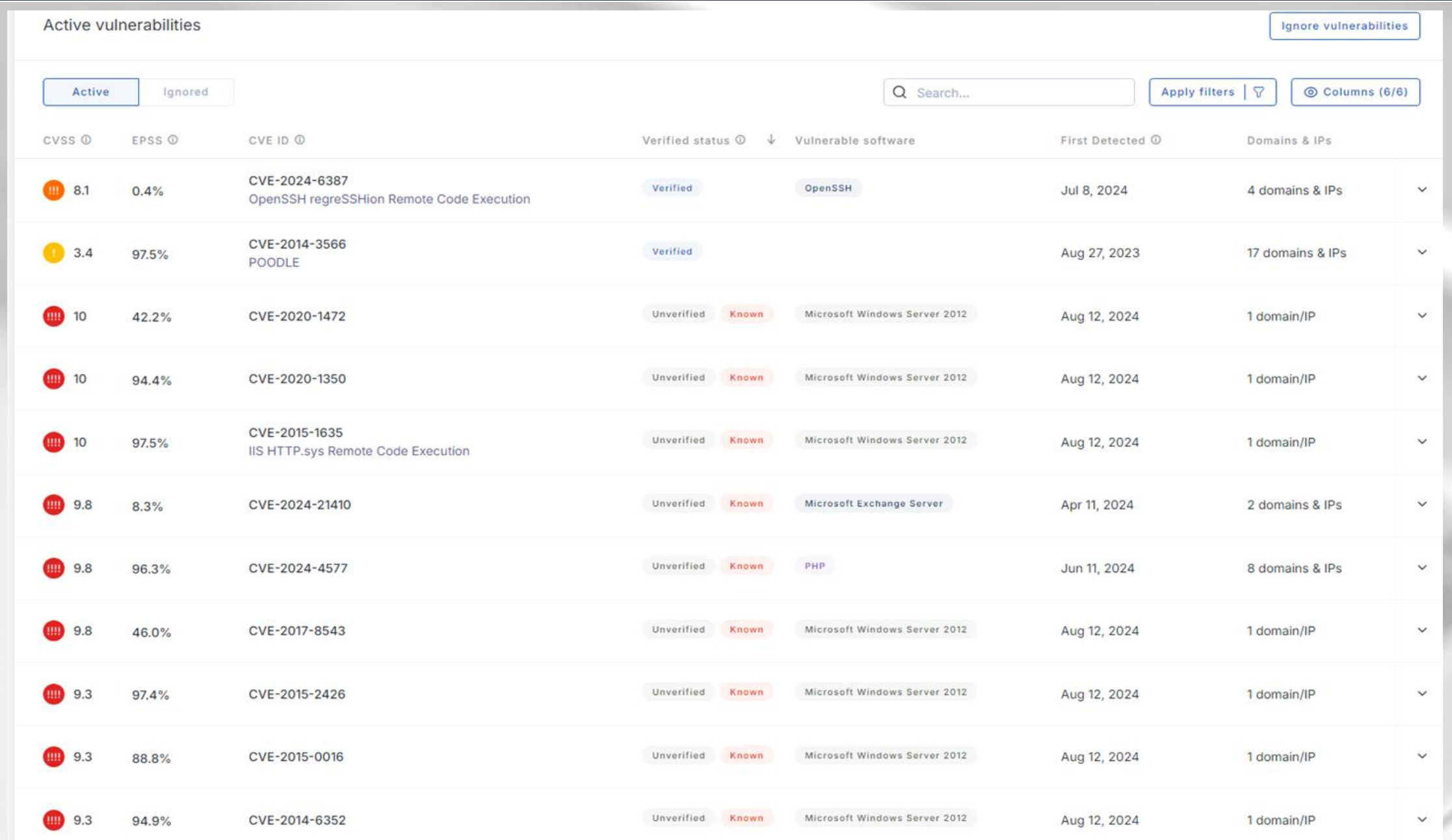
Apply filters

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

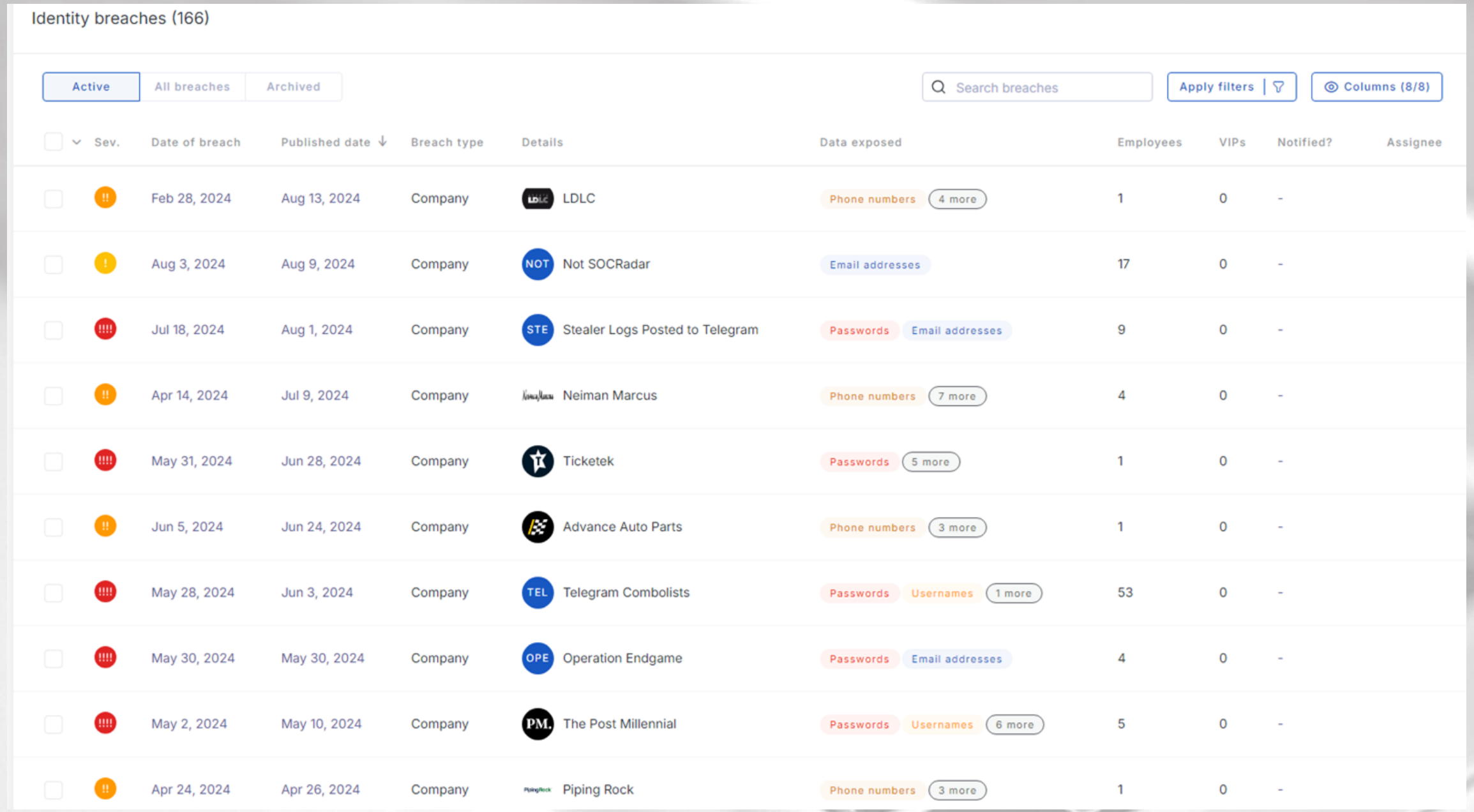
Uporaba namenskih orodij v inšpekcijskem nadzoru

Sev. ↓	Finding / Risk	Category	First detected	Assets affected	Status	
	'FTP' port open Unnecessary open ports	Network	18 Apr, 2021	17		›
	'MySQL' port open Unnecessary open ports	Network	10 Sep, 2023	10		›
	'SIP' port open Unnecessary open ports	Network	2 Jul, 2022	7		›
	SSL not available Susceptible to man-in-the-middle attacks	Encryption	22 Mar, 2019	4		›
	'Remote Desktop' port open Unnecessary open ports	Network	12 Aug, 2024	2		›
	'FTP (Anonymous)' port open Unnecessary open ports	Network	29 Aug, 2024	1		›
	'Microsoft Windows RPC' port open Unnecessary open ports	Network	12 Aug, 2024	1		›
	HTTP does not redirect to HTTPS Susceptible to man-in-the-middle attacks	Encryption	17 Oct, 2018	346		›

Uporaba namenskih orodij v inšpekcijskem nadzoru



Uporaba namenskih orodij v inšpekcijskem nadzoru



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	-	

Pogoste (sistemske) ugotovitve v inšpekcijskih nadzorih

- **Dolgoletno zanemarjanje področja informacijske in kibernetske varnosti,** ko se ne namenja dovolj (kadrovskih in finančnih) virov za to področje.
- **Ne-zavedanje poslovodstva zavezancev, da manko dokumentiranja procesov** (ko niso izvedene celovite analize tveganj ter ocene vplivov na poslovanje), posledično **vodi do neobvladovanja (tveganj) ključnih informacijskih sredstev.**
- **Neobvladovanje izvajanja informacijskih storitev pogodbenih izvajalcev** (ang. *outsourcing*) oziroma neučinkovito izvajanje dolžnega nadzorstva nad izvajalci.

Pogoste (tehnične) ugotovitve v inšpekcijskih nadzorih

- **Ni izvedenega ustreznega popisa sredstev** (pogosto samo delno, za ozke segmente poslovanja).
- **Ni** (ali so samo delno) **izvedenih popisov poslovnih procesov**, posledično ni izvedene BIA analize ali pa je BIA analiza izvedena brez ustreznega temelja.
- **Nedosledno izvajanje postopkov dodelitve in odvzema pravic** pri spremembah ali prekinitvah zaposlitve.
- Odgovorne osebe za **neprekinjeno poslovanje** so sicer prepoznane, **niso pa ti ključni kadri prepoznani v podpornih procesih** (ni zagotovljene dosegljivosti izven delovnega časa).
- **Ni določene minimalne ravni poslovanja**.

Pogoste (tehnične) ugotovitve v inšpekcijskih nadzorih

- **Ne izvaja se rednega izobraževanja zaposlenih na področju informacijske varnosti** in ne zagotavljajo zadostnega usposabljanja in izpopolnjevanja za ključen IT kader.
- **Omrežje** (sploh ni) **ni ustrezno segmentirano.**
- **Upravljanje in preprečevanje izrab tehničnih ranljivosti je zelo oteženo** (kot posledica neustrezno izvedenega ali ne ažuriranega popisa sredstev).
- **Varnostnih zahtev za ključne zunanje ponudnike storitev ni opredeljenih v internih aktih niti vključenih v pogodbe**.
- **Datumi pregleda in ažuriranja dokumentacije** dostikrat sovpadajo z najavo inšpekcijskega nadzora.

Pogoste (tehnične) ugotovitve v inšpekcijskih nadzorih

- **Ni potrebnega/usposobljenega kadra za izvajanja dolžnega nadzorstva** nad izvajanjem storitev zunanjih ponudnikov (ni mogoče obvladovanje tveganj dobavne verige).
- **Ni predpisanih in izvedenih testov postopkov upravljanja izrednih dogodkov** (ki imajo negativen vpliv na izvajanje bistvenih storitev).
- **Ni** (rednega) **preverjanja kakovosti izdelave varnostnih kopij**.
- **Ne zagotavlja se ohranjanje dnevniških zapisov** o delovanju vseh ključnih informacijskih sistemov in delov omrežja (ki so bistvenega pomena za delovanje bistvenih storitev**), za obdobje najmanj 6 mesecev.**
- **Neustrezne politike v AD** (neaktivni računi, geslo nikoli ne poteče…)

Ugotovljene dobre prakse v inšpekcijskih nadzorih

- **Umestitev vodje informacijske varnosti (*CISO*)** v hierarhiji organizacije - neposredno odgovoren poslovodnemu organu.
- **Redno izvajanje notranjih revizij** tudi na področju informacijske varnosti, kjer notranjemu revizorju asistira veščak s področja informacijskih tehnologij (npr. *CISA*).
- **Implementacija strogih politik v AD** (redno pregledovanje ustreznosti politik, minimalno število administratorskih računov, brisanje neaktivnih računov, dolžina in kompleksnost gesel, ipd.).
- **Implementacija mehanizma „omrežnih pasti“** (ang. *Honeypot*) v določenih (kritičnih) segmentih notranjega omrežja.
- **Certifikacija po mednarodnih standardih** (ISO 27001, ISO 22301).

Ugotovljene dobre prakse v inšpekcijskih nadzorih

- **V pogodbah s ključnimi dobavitelji ali zunanjimi ponudniki storitev** so varnostne zahteve zelo dobro definirane in vključene določbe o informacijski varnosti.
- **Implementirana rešitev PAM** (ang. *Privileged Access Management*), ki omogoča dober nadzor tudi nad dostopi v omrežje in aktivnostjo zunanjih ponudnikov storitev.
- **Izvajanje rednih testiranj** (agregatov pod obremenitvijo, kakovosti varnostnih kopij, dosegljivost ključnega kadra, izrednih postopkov).
- **Ustrezna segmentacija omrežja** (fizično, VLAN, VRF, DMZ).
- **Izvedba varnostnega kopiranja podatkov** z uporabo sistema 3-2-1.
- **Redno izvajanje *anti-phishing* kampanj** in poročanje poslovodstvu.

Vprašanja?

REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST

URSIV

gp.uiv@gov.si
www.uiv.gov.si
Twitter: @URSIV_Slovenia