FREEDIVISION

4. 11. 2026 · Enforum, Praha-Karlín

FREEDIVISION SECURITY DAY 2026 · 11:20

FD.io VulnerAbility



Od objevení zranitelnosti k řízené, ověřené nápravě.

powered by targetfive

Ladislav Šolc
CEO, Target Five s.r.o.

11:00 PhishingGym | **11:20 FD.io VulnerAbility** | 11:50 FD.io Data | 12:30 FD.io Risk

JAK ZAČÍT

Tři kroky od prvního assessmentu k průběžné službě

01

Kombinovaný assessment

AD audit, PWD audit a sken zranitelností. Výchozí stav a plán nápravy.

02

Interní sonda a EDR

Pravidelné skeny ve vaší síti a napojení inventáře z EDR.

03

Průběžná služba

Black Radar: vlastníci, termíny, ověření a reporty v Logsign.

Assessment je první krok k platformě. Navazující služba se sjednává samostatně.



PROČ TEĎ

Zranitelností je rekordně mnoho

48 185

nových CVE zveřejněných v roce 2025, nový rekord

131

nových zranitelností každý den

+21 %

meziročně oproti roku 2024

Regulace to chce doložit

- ✓ ZKB 264/2025 Sb.: zvládání zranitelností
- ✓ NIS2, čl. 21 odst. 2 písm. e)
- ✓ ISO/IEC 27001:2022, A.8.8

Zneužije se jen malá část z nich. Rozhodující je vědět, která se týká právě vás.



FREEDIVISION

Zdroj: J. Gamblin, 2025 CVE Data Review (bez odmítnutých CVE)

VÝCHOZÍ STAV

Problém není najít CVE. Problém je řídit riziko

Sken jednou ročně

Mezi dvěma skeny vyjdou tisíce nových zranitelností. Report stárne od prvního dne.

Šum místo priorit

Externí sken, sondy a endpointy hlásí totéž několikrát. Všechno vypadá důležitě.

Nález bez uzavření

Chybí vlastník, termín, důkaz nápravy a opakovaná kontrola. Končí v e-mailu.

Víte, které tři zranitelnosti máte opravit tento týden?



JAK TO FUNGUJE

Celý životní cyklus zranitelnosti v jedné službě



01

Objevit

Externí a interní sken, inventář z EDR

02

Obohatit

Komerční databáze, exploity, kontext aktiva

03

Prioritizovat

Kritické, zneužitelné a exponované

04

Předat

Vlastník, termín a upozornění

05

Ověřit

Opakovaný sken potvrdí opravu

06

Doložit

Trend, SLA a report pro vedení

Dokola, ne jednou za rok. Celý cyklus drží platforma Black Radar.

ARCHITEKTURA

Jeden proces, více nezávislých zdrojů



Bez závislosti na jediném výrobci skeneru.

ČÁST 2 · DATA A PLATFORMA

Vidíme vaše prostředí zvenku i zevnitř

Externí assessment, interní sondy, inventář z EDR a komerční zdroje



EXTERNÍ A INTERNÍ ASSESSMENT

Dva pohledy, jedna platforma

Externí assessment

Jak vás vidí útočník z internetu

- Veřejné IP adresy, domény a služby
- Nově objevená a zapomenutá aktiva
- Bez instalace u vás, start během dnů
- Ideální první krok

Interní assessment

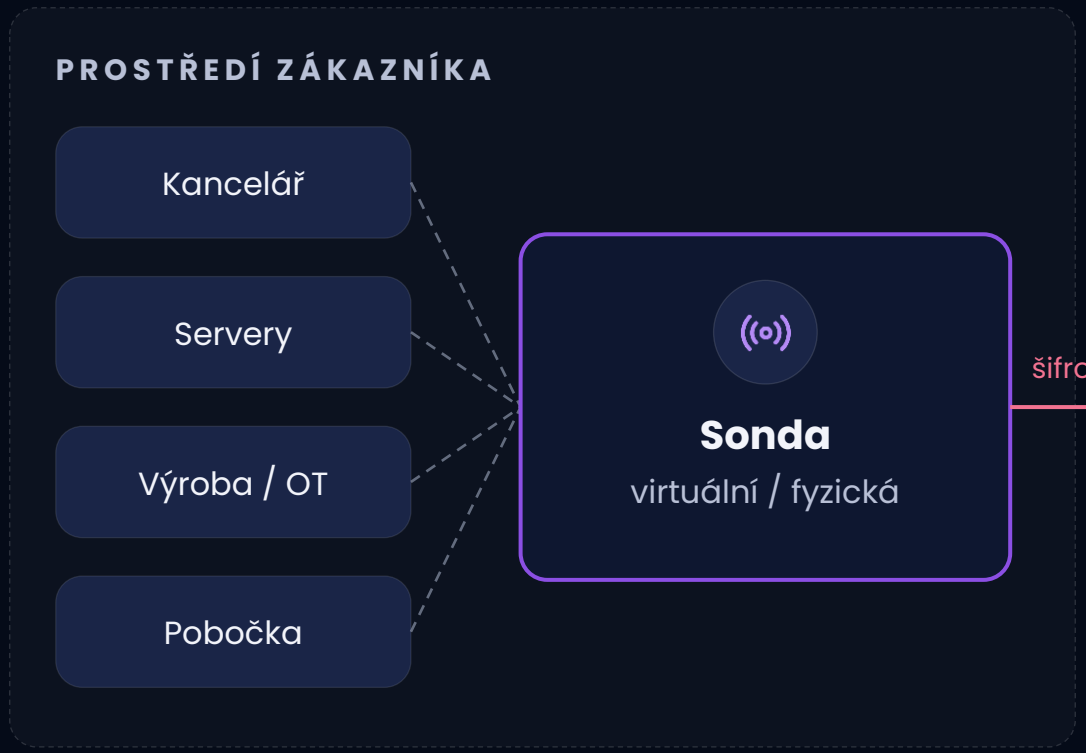
Co je za firewallem

- Sonda ve vaší síti, všechny segmenty
- Servery, stanice, síťové prvky, OT
- Autentizovaný sken vidí verze softwaru
- Pravidelně podle plánu

Bez licenčního stropu počtu IP adres. Rozsah a frekvence skenů se sjednávají.

SONDY

Sondy skenují pravidelně, řízení je centrální



- **Bez licenčního stropu IP**
- **Plánované pravidelné skeny**
- **Autentizovaný i neautentizovaný**
- **Řízeno centrálně, bez práce pro vás**

INTERNÍ SONDA

Interní sonda: jeden malý box, celá síť



- Fyzický box, nebo virtuální appliance
- Jedno připojení, může mít dosah do všech segmentů
- Autentizovaný i neautentizovaný sken
- Šifrovaně do Black Radar (SaaS)

EDR ENRICHMENT

Inventář z EDR doplní, co sken nevidí

Inventář z EDR
agent, aplikace, výrobce, verze

→

Normalizace
sjednocení názvů a verzí

→

Párování
CVE, KEV a EPSS na konkrétní aktivum

→

Jeden nález
dva důkazy: sken a EDR

Příklad: HarfangLab EDR

Inventář aplikací z agentů přidáme k nálezům, bez dalšího agenta. Aktivum párujeme podle ID agenta, názvu a IP, změna IP nevytvoří duplicitu.

Nejen HarfangLab, ale i M365/Office 365 E3

- ✓ Další EDR přes export inventáře (CSV/XLSX) nebo API
- ✓ EDR vidí notebooky mimo síť, sonda servery a OT
- ✓ Uzavření potvrdí nový sken nebo inventář z EDR

ZDROJE INFORMACÍ

Komerční databáze a kontext, ne jen seznam CVE



Komerční databáze

Denně aktualizované kontroly zranitelností, rychleji než veřejné zdroje

CVE a CVSS

Jednotná identifikace a základní závažnost

Aktivně zneužívané

Katalog zranitelností, které útočníci už zneužívají

Pravděpodobnost zneužití

Predikce, zda se zranitelnost zneužije v příštích 30 dnech

Bulletiny výrobců

Opravy a doporučení přímo od výrobců

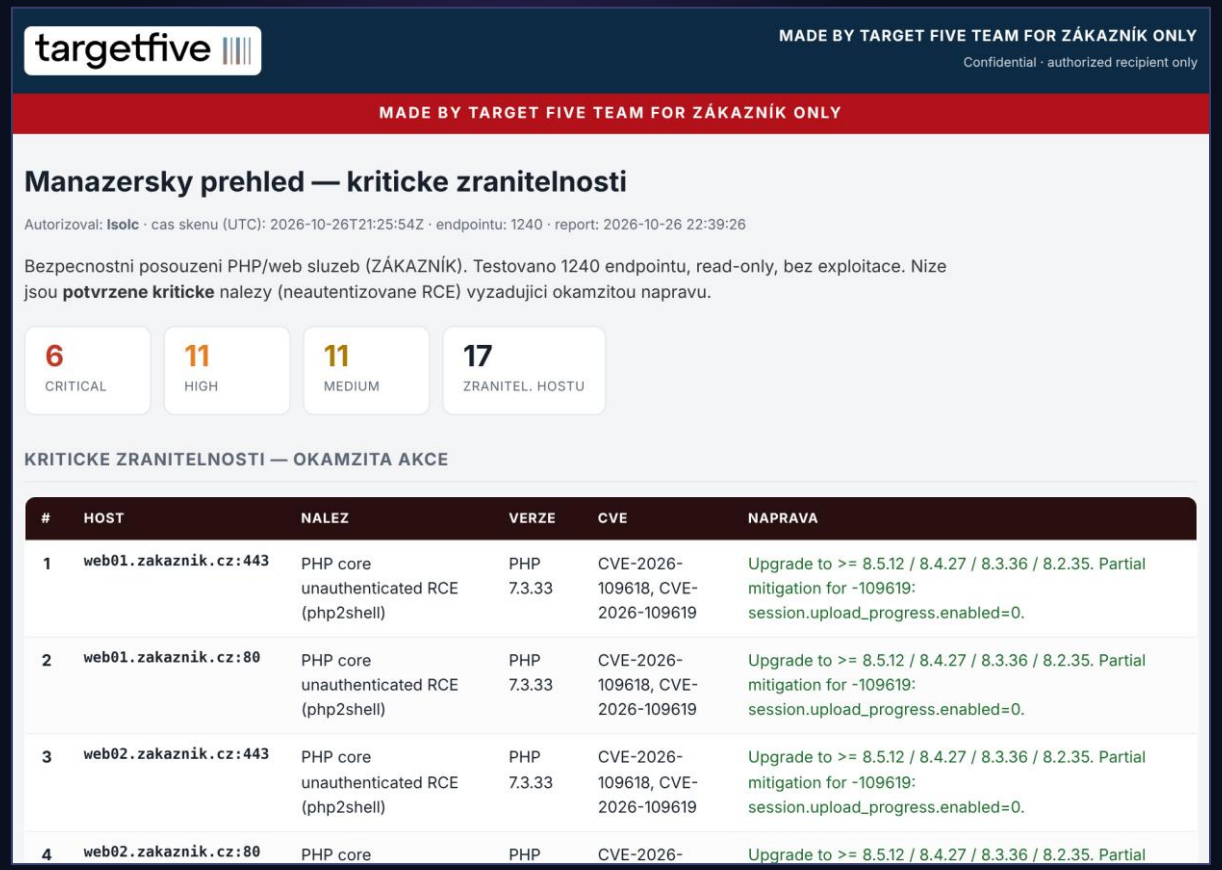
Dostupnost exploitu

Existuje veřejný exploit nebo nástroj?

O prioritě rozhoduje hlavně to, jestli se zranitelnost zneužívá a jak pravděpodobně.

UKÁZKA REPORTU · RYCHLÁ REAKCE NA KRITICKOU CVE

Nová kritická CVE: odpověď do hodin



targetfive

MADE BY TARGET FIVE TEAM FOR ZÁKAZNÍK ONLY
Confidential · authorized recipient only

MADE BY TARGET FIVE TEAM FOR ZÁKAZNÍK ONLY

Manazersky prehled — kriticke zranitelnosti

Autorizoval: **lsolc** · cas skenu (UTC): 2026-10-26T21:25:54Z · endpointu: 1240 · report: 2026-10-26 22:39:26

Bezpecnostni posouzeni PHP/web sluzeb (ZÁKAZNÍK). Testovano 1240 endpointu, read-only, bez exploitace. Nize jsou **potvrzene kriticke** nalezy (neautentizovane RCE) vyzadujici okamzitou napravu.

6	11	11	17
CRITICAL	HIGH	MEDIUM	ZRANITEL. HOSTU

KRITICKE ZRANITELNOSTI — OKAMZITA AKCE

#	HOST	NALEZ	VERZE	CVE	NAPRAVA
1	web01.zakaznik.cz:443	PHP core unauthenticated RCE (php2shell)	PHP 7.3.33	CVE-2026-109618, CVE-2026-109619	Upgrade to >= 8.5.12 / 8.4.27 / 8.3.36 / 8.2.35. Partial mitigation for -109619: session.upload_progress.enabled=0.
2	web01.zakaznik.cz:80	PHP core unauthenticated RCE (php2shell)	PHP 7.3.33	CVE-2026-109618, CVE-2026-109619	Upgrade to >= 8.5.12 / 8.4.27 / 8.3.36 / 8.2.35. Partial mitigation for -109619: session.upload_progress.enabled=0.
3	web02.zakaznik.cz:443	PHP core unauthenticated RCE (php2shell)	PHP 7.3.33	CVE-2026-109618, CVE-2026-109619	Upgrade to >= 8.5.12 / 8.4.27 / 8.3.36 / 8.2.35. Partial mitigation for -109619: session.upload_progress.enabled=0.
4	web02.zakaznik.cz:80	PHP core	PHP	CVE-2026-	Upgrade to >= 8.5.12 / 8.4.27 / 8.3.36 / 8.2.35. Partial

1 240 endpointů
zkontrolováno cíleně na php2shell, read-only, bez exploitace

6 kritických nálezů
neautentizované RCE na webech z internetu, oprava ihned

17 zranitelných hostů
manažerský přehled a akční GO list pro IT

EDR doplní, co sken bez agenta nevidí
inventář z EDR nebo lokální kontrola dá jistotu o zranitelnostech lokálních apliakcí

JAK URČUJEME PRIORITU

Priorita je víc než skóre CVSS

Závažnost — technický dopad a základní hodnocení

+

Exploit intelligence — známé zneužívání a pravděpodobnost exploitace

+

Expozice — internet, síťový dosah, kompenzační opatření

+

Kritičnost aktiva — business služby, citlivá data, role systému

→

VÝSLEDEK

Backlog podle rizika

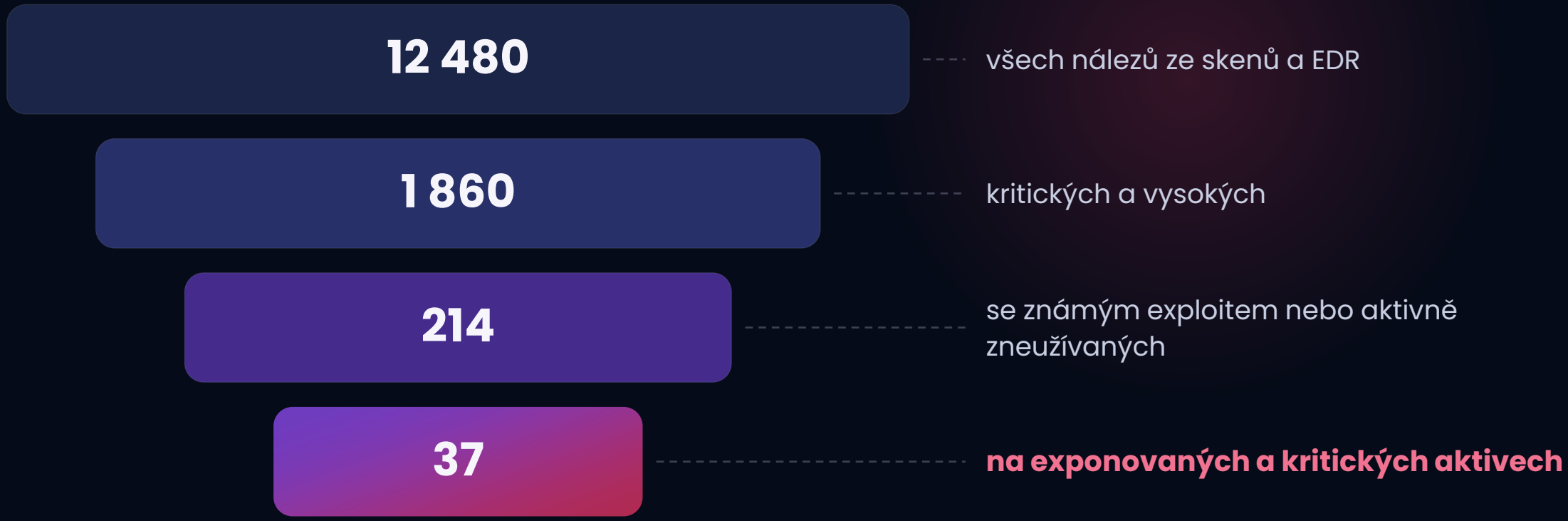
kritické → **vysoké** → **běžné**

Zneužitelné a exponované jdou první.

Cílem není opravit vše najednou. Cílem je efektivně snižovat riziko.

PRIORITIZACE

Opravte nejdřív to, co útočník opravdu použije



Ze dvanácti a půl tisíce nálezů zbude seznam, se kterým jde tento týden pracovat.

PLATFORMA BLACK RADAR

Jedno místo pro zranitelnosti z jakéhokoli zdroje

Agnostický lifecycle

Nezáleží na tom, odkud nález přišel: sondy, externí sken, EDR nebo import CSV/XLSX a API. Black Radar ho vede až do ověřeného uzavření a každou akci zapíše do historie.

Sjednocení a deduplikace

Stejné CVE ze sondy i EDR je jeden nález

Kontext aktiva

Vlastník podle útvaru, kritičnost, expozice

Prioritizace P1 až P4

KEV, CVSS, EPSS a kritičnost aktiva

SLA a eskalace

Eskalace při 75, 100 a 150 % lhůty

Výjimky a audit

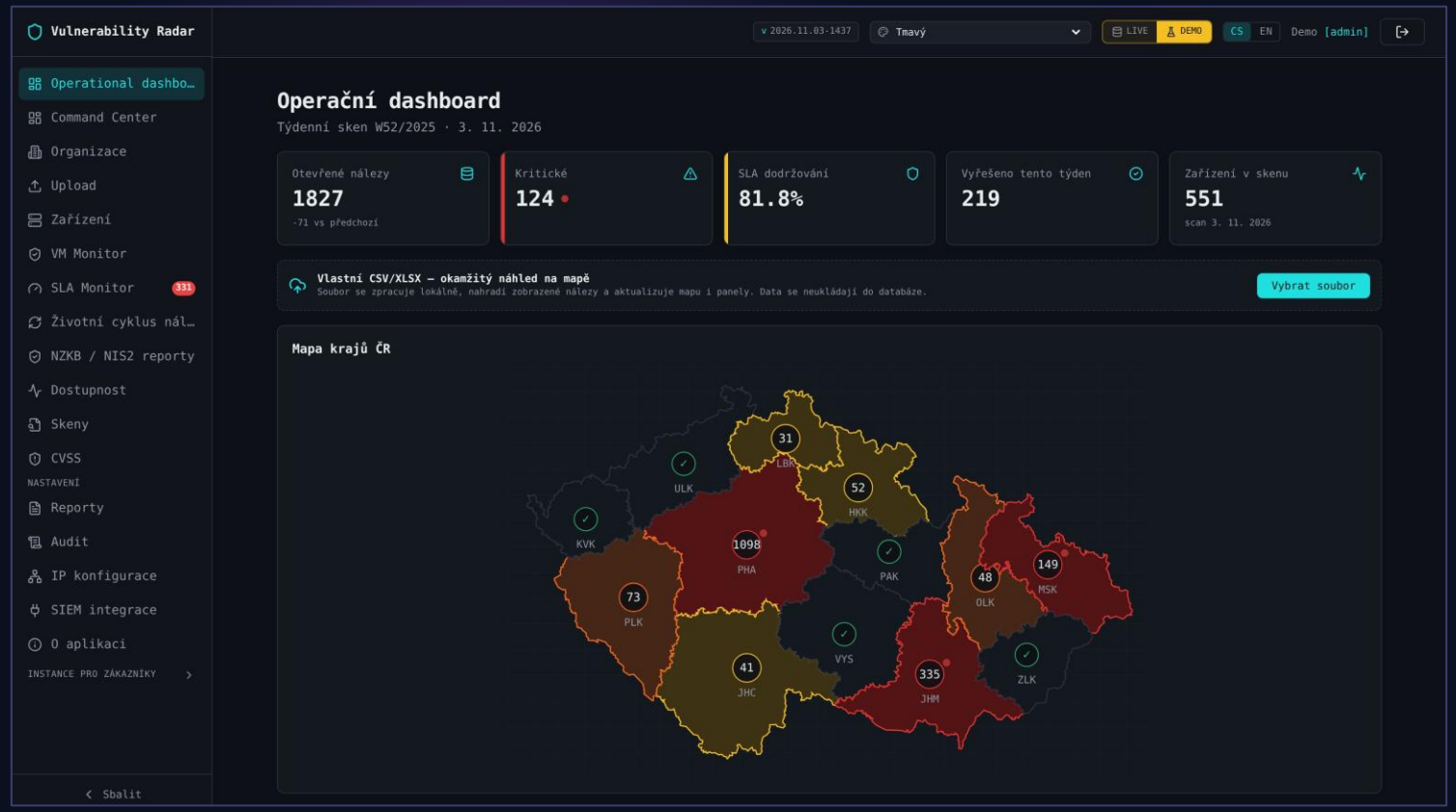
Schválené odklady, registr výjimek, audit log

Přehled pro vedení

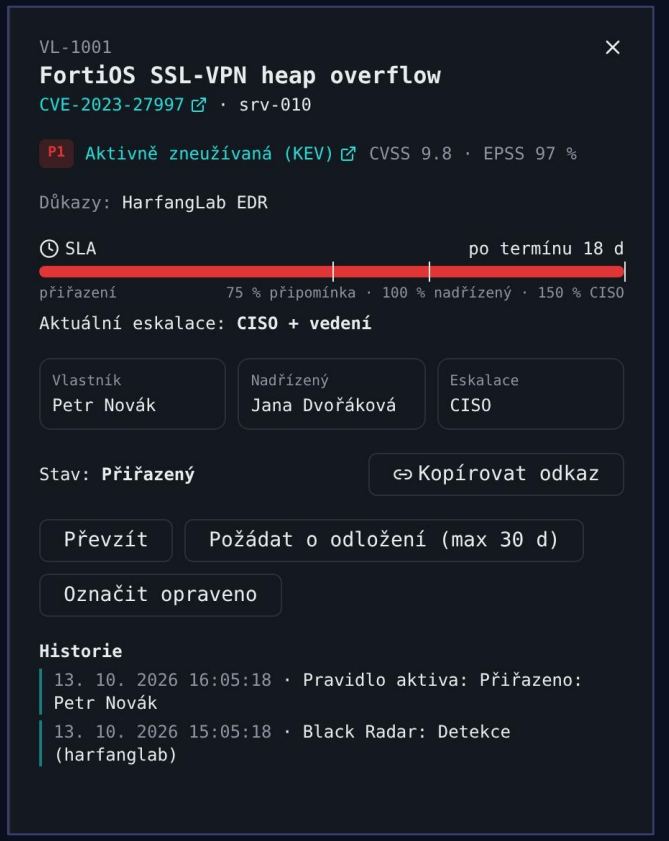
Dashboard, mapa krajů a PDF reporty

BLACK RADAR V PRAXI

Od přehledu po detail jednoho nálezu



Operační dashboard: otevřené a kritické nálezy, plnění SLA a mapa krajů



Detail nálezu: priorita, KEV, SLA s eskalací, důkaz z EDR

ŽIVOTNÍ CYKLUS NÁLEZU

Každý nález má stav, vlastníka a termín



Nový › Posouzení › Přidělený › V řešení › Čeká na retest › **Uzavřený**

Odložení jen se schválenou výjimkou, SLA se pozastaví. Uzavřeno = oprava potvrzená novým skenem nebo EDR.

BR-1024 · ukázka záznamu

Nález	**Kritická expozice webové služby**
Aktivum	**WEB-PROD-02, dostupné z internetu**
Vlastník	**IT Operations**
Stav	**V řešení**
Kontrola	**Opakovaný sken nebo nový inventář z EDR**

SLA podle priority (výchozí pravidla)

P1 dostupné z internetu	**72 h**
P1 · KEV nebo exploit	**7 dní**
P2	**15 dní**
P3 / P4	**30 / 90 dní**

ŽIVÁ UKÁZKA · BLACK RADAR

Od přehledu k ověřené opravě

Krátce naživo, zhruba tři minuty



1 · Prioritní nález

2 · Vlastník a termín

3 · Ověření a report

NAPOJENÍ NA LOGSIGN

Zranitelnosti tam, kde se řeší incidenty



Korelace s útoky

Pokus o útok na aktivum se známou zranitelností dostane v SOC vyšší prioritu.

Okamžité upozornění

Nová kritická zneužitelná zranitelnost? Upozornění hned, ne až v měsíčním reportu.

Průběžné reporty

Trend zranitelností, plnění termínů a stav podle oddělení a lokalit.

Do Logsign posíláme: nové kritické nálezy · změny priorit a stavů · aktiva a vlastníky · výsledky ověření

Black Radar řídí zranitelnosti, Logsign je promítá do provozního obrazu FD.io Advanced .

VÝSLEDEK

Stejná data, tři pohledy: IT, CISO a vedení

IT PROVOZ

Co máme opravit?

Jeden backlog, přidělení správcům, opakovaná kontrola a doložené uzavření.

CISO A SOC

Co nás ohrožuje?

Zranitelnosti propojené s expozicí a exploit intelligence, kontext v Logsign.

VEDENÍ

Snižujeme riziko?

Trend, prioritní rizika, nedodržené termíny a stav nápravy bez technických detailů.

Měříme: čas do přidělení · čas do nápravy · podíl kritických po termínu · znovuotevřené nálezy



REGULACE

Doklady pro ZKB, NIS2 a ISO 27001

Co chtějí předpisy

- ZKB 264/2025 Sb. a vyhlášky: zvládání zranitelností
- NIS2, čl. 21 odst. 2 písm. e): řešení a zveřejňování zranitelností
- ISO/IEC 27001:2022, A.8.8: řízení technických zranitelností

Co dodá FD.io VulnerAbility

- Pravidelné skeny s historií a datem
- Prioritizace s doloženým zdůvodněním
- Vlastník, termín a ověření opravy u každého nálezu
- Záznam akceptovaných rizik
- Report pro vedení a auditora

Posouzení souladu zůstává na vás a vašem auditorovi.

ČÁST 3 · JAK ZAČÍT

Doporučený start: tři assessmenty

AD audit, PWD audit a sken zranitelností. První krok k platformě.



AD AUDIT

AD audit: kdo může získat kontrolu nad doménou



AD audit

Read-only export z AD v dohodnutém rozsahu, automatizované kontroly a posouzení konzultantem. Výsledkem jsou nálezy s důkazy, dopadem a doporučením.

Privilegované účty

Domain Admins, servisní účty, oddělení od běžné práce

Delegace a oprávnění

Delegovaná práva a oprávnění na chráněných objektech

Riziková konfigurace

Zastaralé ověřování, LDAP signing, Print Spooler, LAPS

Možné útočné cesty

Které vazby mohou vést k převzetí domény

Zastaralé objekty

Neaktivní účty, nepodporované OS, výjimky z politik

Dohodnutý režim

Kontroly v předem dohodnutém rozsahu a režimu

PWD AUDIT

PWD audit: která hesla představují riziko



PWD audit

Kontrola kvality hesel proti databázi 130 mil. uniklých hesel, v dohodnutém rozsahu. Report ukazuje agregované výsledky a identifikátory účtů, nikdy hesla ani hashe.

Kvalita hesel

Hesla, která nesplňují dohodnutá kritéria

Sdílená hesla

Stejné heslo u více účtů

Kompromitovaná hesla

Shoda s databází 130 mil. uniklých hesel

Privilegované účty

Zvláštní pozornost účtům s nejvyšším dopadem

Politiky hesel

Výjimky, expirace a nastavení politik

Řízená náprava

Změna dotčených hesel a doplňující opatření

SKEN ZRANITELNOSTÍ

Sken zranitelností: co je zranitelné zvenku i uvnitř

Externí sken

Jak vás vidí útočník z internetu

- Veřejné IP adresy, domény a služby
- Nově objevená a zapomenutá aktiva
- Verze softwaru proti známým zranitelnostem
- Bez instalace u vás

Interní sken

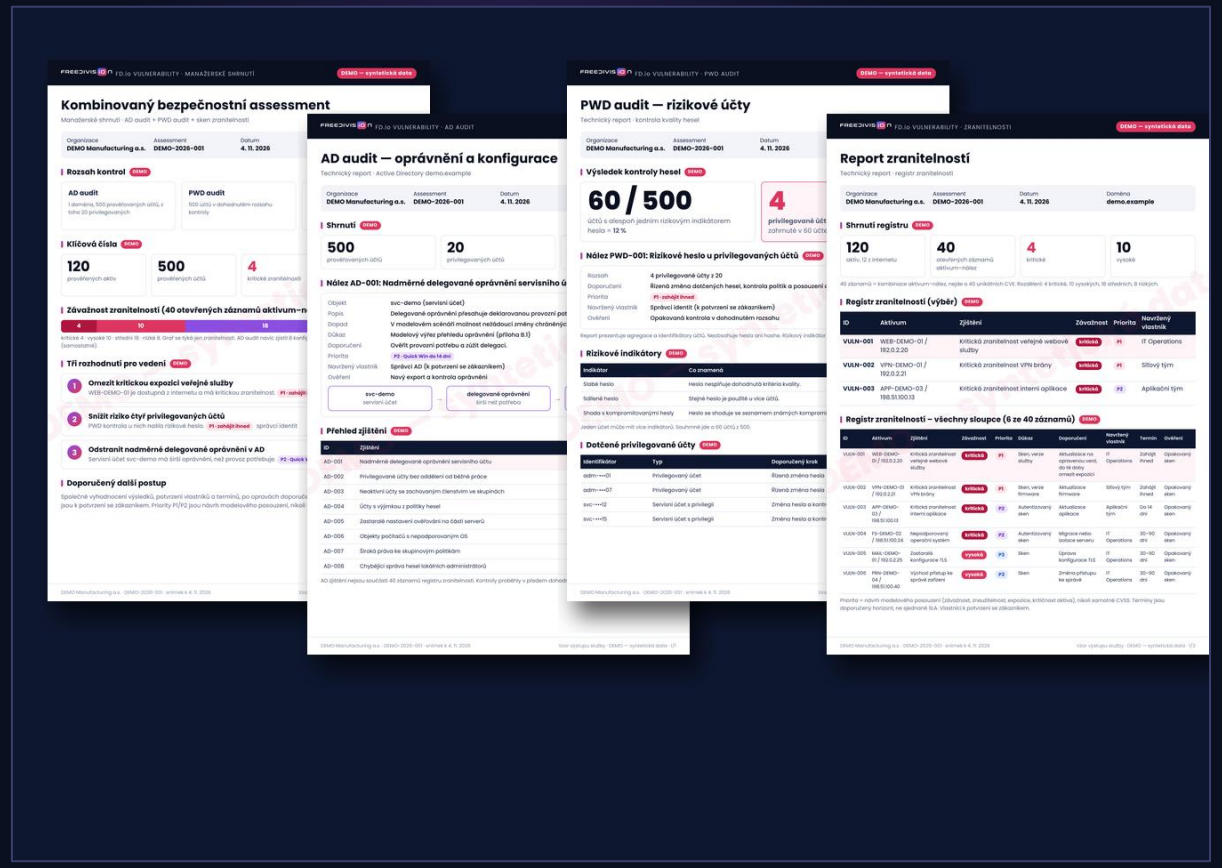
Co je za firewallem

- Servery, stanice a síťové prvky
- Autentizovaný sken vidí verze softwaru
- Sonda v dohodnutých segmentech
- Read-only kontroly bez exploitace

Každý nález: aktivum → nález → doporučená oprava. Interně a/nebo externě podle rozsahu.

CO SI ODNESETE

Výstupy, se kterými se dá hned pracovat



Manažerské shrnutí
Rizika, dopad a tři první kroky pro vedení

Tři odborné reporty
AD audit, PWD audit a zranitelnosti s důkazy

Společný akční plán
Priorita, důvod, navržený vlastník, termín, ověření

Společné vyhodnocení
Výsledky projdeme a domluvíme pořadí kroků

Tři rozhodnutí pro vedení

Klíčová čísla DEMO

120	500	4	60
prověřených aktiv	prověřených účtů	kritické zranitelnosti	účtů s rizikovým indikátorem hesla (12 %)

Závažnost zranitelností (40 otevřených záznamů aktivum–nález) DEMO



kritické 4 · vysoké 10 · střední 18 · nízké 8. Graf se týká jen zranitelností. AD audit navíc zjistil 8 konfiguračních a oprávňových zjištění (samostatně).

Tři rozhodnutí pro vedení DEMO

1. **Omezit kritickou expozici veřejné služby**
   WEB-DEMO-01 je dostupná z internetu a má kritickou zranitelnost. P1 · zahájit ihned IT Operations
2. **Snížit riziko čtyř privilegovaných účtů**
   PWD kontrola u nich našla rizikové heslo. P1 · zahájit ihned správci identit
3. **Odstranit nadměrné delegované oprávnění v AD**
   Servisní účet svc-demo má širší oprávnění, než provoz potřebuje. P2 · Quick Win do 14 dní správci AD

DEMO — syntetická data



celá strana · DEMO

1 · Omezit kritickou expozici
Veřejná služba WEB-DEMO-01 s kritickou zranitelností. P1, IT Operations.

2 · Snížit riziko 4 privilegovaných účtů
PWD kontrola u nich našla rizikové heslo. P1, správci identit.

3 · Odstranit nadměrnou delegaci v AD
Servisní účet svc-demo. P2, quick win do 14 dní, správci AD.

Vedení dostane pořadí rozhodnutí
IT dostane konkrétní práci. DEMO — syntetická data.

AD audit a PWD audit: nález a doporučení

Nález AD-001: Nadměrné delegované oprávnění servisního účtu

DEMO

Objekt	svc-demo (servisní účet)
Popis	Delegované oprávnění přesahuje deklarovanou provozní potřebu.
Dopad	V modelovém scénáři možnost nežádoucí změny chráněných objektů.
Důkaz	Modelový výřez přehledu oprávnění (příloha B.1)
Doporučení	Ověřit provozní potřebu a zúžit delegaci.
Priorita	P2 · Quick Win do 14 dní
Navržený vlastník	Správci AD (k potvrzení se zákazníkem)
Ověření	Nový export a kontrola oprávnění

svc-demo servisní účet → **delegované oprávnění** širší než potřeba → **chráněný objekt** modelový scénář

DEMO — syntetická data

AD-001 · nadměrná delegace u svc-demo · P2

Výsledek kontroly hesel

DEMO

60 / 500

účtů s alespoň jedním rizikovým indikátorem hesla = **12 %**

4

privilegované účty s rizikovým heslem (jsou zahrnuté v 60 účtech)

Nález PWD-001: Rizikové heslo u privilegovaných účtů

DEMO

Rozsah	4 privilegované účty z 20
Doporučení	Řízená změna dotčených hesel, kontrola politik a posouzení doplňujících opatření.
Priorita	P1 · zahájit ihned
Navržený vlastník	Správci identit (k potvrzení se zákazníkem)
Ověření	Opakovaná kontrola v dohodnutém rozsahu

Report prezentuje agregace a identifikátory účtů. Neobsahuje hesla ani hashe. Rizikový indikátor není důkazem převzetí účtu.

DEMO — syntetická data

PWD-001 · rizikové heslo u 4 privilegovaných účtů · P1

Co má IT opravit

Registr zranitelností (výběr) DEMO

ID	Aktivum	Zjištění	Závažnost	Priorita	Navržený vlastník
VULN-001	WEB-DEMO-01 / 192.0.2.20	Kritická zranitelnost veřejné webové služby	kritická	P1	IT Operations
VULN-002	VPN-DEMO-01 / 192.0.2.21	Kritická zranitelnost VPN brány	kritická	P1	Síťový tým
VULN-003	APP-DEMO-03 / 198.51.100.13	Kritická zranitelnost interní aplikace	kritická	P2	Aplikační tým

DEMO — syntetická data

Registr: aktivum, zjištění, závažnost, priorita a navržený vlastník

Detail VULN-001 DEMO

Aktivum	WEB-DEMO-01 · 192.0.2.20 · dostupné z internetu
Zjištění	Kritická zranitelnost veřejné webové služby (modelová zranitelnost, bez identifikátoru CVE)
Závažnost	kritická
Proč P1	Kritická závažnost, služba je dostupná z internetu, aktivum podporuje obchodní web
Důkaz	Výstup skenu: zjištěná verze služby a odpověď na kontrolní požadavek (příloha D.1)
Doporučení	Aktualizace na opravenou verzi, do té doby omezit expozici služby
Navržený vlastník	IT Operations (k potvrzení se zákazníkem)
Horizont	Zahájit ihned
Ověření	Opakovaný sken po opravě

DEMO — syntetická data

Detail VULN-001: důkaz, doporučení, ověření

KONFERENČNÍ NABÍDKA

První kombinovaný assessment se slevou 50 %



01 · IDENTITY

AD audit

Riziková oprávnění, konfigurace a cesty ke kompromitaci domény.

02 · HESLA

PWD audit

Slabá, sdílená nebo kompromitovaná hesla v dohodnutém rozsahu.

03 · SYSTÉMY

Sken zranitelností

Zranitelné systémy a služby, závažnost a priorita nápravy.

Výstup: manažerské shrnutí · technické reporty · prioritizovaný plán nápravy · společné vyhodnocení

Zjistěte slabá místa identit, hesel a systémů. Získáte přehled rizik a plán, co opravit jako první.

Sleva 50 % na první kombinovaný assessment. Konkrétní rozsah a výchozí cenu stanovíme v individuální nabídce.

-50 %

PRVNÍ ASSESSMENT



03

Zastavte se za námi o přestávce nebo po akci · sales@freedivision.com

powered by targetfive

Ladislav Šolc
CEO, Target Five s.r.o.