FREEDIVISION

4. 11. 2026 · Enforum, Praha-Karlín

FREEDIVISION SECURITY DAY 2026 · KEYNOTE

FreeDivision 2.0

Bezpečnost, která dává smysl



Jakub Karvánek
CSO, FreeDivision

Marek Szotkowski
Marketing Manager, FreeDivision

Martin Kratochvil
CTO, FreeDivision

01 Keynote | 02 FreeDivision 2.0 | 03 FD.io Advanced | 04 FD.io Essential

PROGRAM DNE

Od srdce ekosystému až po rizika

09:00	**Welcome keynote** Jakub Karvánek, Martin Kratochvil, Marek Szotkowski	
09:15	**FreeDivision 2.0: ekosystém, portál a PoC box** Jakub Karvánek, Martin Kratochvil	
09:40	**FD.io Advanced: srdce ekosystému naživo** Jakub Karvánek, Martin Kratochvil	
10:10	**FD.io Essential: HarfangLab a IKARUS** Miroslav Mašek, Jakub Karvánek	
10:40	Coffee break	
		11:00 **FD.io PhishingGym** Ladislav Šolc
		11:20 **FD.io VulnerAbility** Ladislav Šolc
		11:50 **FD.io Data a compliance** Jakub Karvánek
		12:30 **FD.io Risk a NIS2** Petr Sobotka, Daniel Fleišer
		13:10 Dotazy a diskuse
		13:30 **Oběd, barmanská show a volná zábava** Kvůli počasí uvnitř · oficiální konec v 15:30

JAK DEN POBĚŽÍ

Čtyři věci, které se vám dnes budou hodit

Ptejte se kdykoli

Klidně i uprostřed prezentace. Ve 13:10 je navíc prostor na diskusi

Dema všech řešení

Ukážeme vám je v pauzách nebo po skončení akce

Sken nebo PoC zdarma

CTI sken vaší firmy nebo PoC risk assessment z kteréhokoli řešení

Zůstaňte na oběd

Od 13:30 oběd, barmanská show a koktejly. Kvůli počasí uvnitř, ne na terase

JEDNA NOC U NAŠICH ZÁKAZNÍKŮ

Zatímco jsme spali…

800+ mil.
logů zpracovaných napříč zákazníky

→

650+
alertů, které ráno čekají na naše analytiky

→

~10 %
z nich vyřešil SOAR automaticky

⚠ Proč jen 10 %? Systémy spolu nemluví, a tak se automatickou reakci nikdo neodváží zapnout.

BLOK 2 · 09:15–09:40

02

FreeDivision 2.0

Ekosystém FreeDivision.io a kam jsme se za rok posunuli

Jakub Karvánek
CSO, FreeDivision

Martin Kratochvíl
CTO, FreeDivision

FREEDIVISION V KOSTCE

Přes 20 let jen kybernetická bezpečnost

Česká firma, od roku 2005. Vybíráme nejlepší technologie na trhu a stavíme kolem nich vlastní služby: dohled, automatizaci a tým specialistů pod jednou střechou.

20+	**250 000+**	**24/7**	**ISO**
let na trhu	spravovaných licencí	detekce a reakce	27001 a 9001

2005	2021	2022	2024	2026
Založení	ISO 27001 a 9001	FD.io Essential	FD.io Advanced	FreeDivision 2.0



ROK V ČÍSLECH · 2025 → 2026

Kam jsme se za jediný rok posunuli

+7
nových kolegů v týmu

+14
nových zákazníků

10 000+
chráněných endpointů, desítky tisíc

100 000+
chráněných identit

1 600
napojených konektorů

8+
workshopů v krajích ČR

Co je letos nového

- FD.io Essential na HarfangLab a IKARUS
- PoC box: celý ekosystém v jednom HW
- Nový web FreeDivision.io
- Corporate Identity
- Zákaznický portál · rozběhnuto, finále 2027

PROČ FREEDIVISION 2.0

Víc opatření, víc systémů, stejně lidí

Regulace chce opatření

NIS2 a nový zákon o kybernetické bezpečnosti chtějí po tisících organizací konkrétní opatření.

Každé opatření je další systém

Další nástroj, další konzole, další samostatná správa. A spolu si nepovídají.

Chybí lidé

Kdo to všechno bude spravovat? Specialistů je málo a nepřetržitý provoz si dovolí málokdo.

Odpověď je jeden propojený ekosystém, ne další samostatné opatření.

TRANSFORMACE

Z FreeDivision 1.0 na FreeDivision 2.0

DŘÍVE	DNES
Prodej licencí	**Jen předplatné s kompletní péčí, které přináší hodnotu od prvního dne**
Samostatné technologie	**Propojený ekosystém s jedním mozkem: FD.io Advanced**
Reakce po incidentu	**Varování předem (CTI) a automatická reakce (SOAR)**
Reporty e-mailem	**Zákaznický portál: vše přehledně na jednom místě**
Ozveme se při obnově	**Customer Care: člověk, který hlídá vaši spokojenost**
Časově náročné PoC	**PoC box u vás, připravený k okamžitému spuštění**

Vlastní vývoj: nechceme jen prodávat boxy

Naše hodnota je know-how. Bezpečnostních systémů už máte spoustu. My z nich uděláme jeden funkční celek, a proto s FreeDivision 2.0 zahajujeme vlastní vývoj.

01
Propojíme
systémy, které už máte, od jakéhokoli výrobce

→

02
Odfiltrujeme šum
balast pryč, zůstane jen to podstatné

→

03
Ukážeme, co řešit
jasné priority místo tisíců alertů

→

04
Nastavíme lifecycle a automatizace
aby to fungovalo dlouhodobě

Začínáme: Zákaznický portál | FD.io Essential Vulnerability ✓ hotovo | Coming soon…

ZÁKAZNICKÁ INFRASTRUKTURA – VYUŽIJEME MAXIMUM Z TOHO, CO UŽ MÁTE

Počítače & notebooky · Cloud & SaaS · Servery · Virtuální servery · Firewall VPN · Network zařízení · IoT / OT zařízení · Switches · Tiskárny · Úložiště & zálohy · Databáze · Identity & users · Active Directory · Aplikace · E-mail · Endpoint protection · Monitoring nástroje · DNS Proxy · Ostatní systémy

FREEDIVISION

Ecosystem

ROZŠIŘITELNÁ OCHRANA

Advanced

PLATFORMA PRO POKROČILOU DETEKCI A REAKCI

- **LOG MANAGEMENT** – Centralizovaný sběr a správa logů
- **DETECTION – SIEM** – Korelace, detekce a analýza hrozeb
- **REACTION – SOAR** – Automatizace reakce a orchestrace
- **SECURITY ANALYSES** – Hloubková analýza a threat hunting

Essential

NEJLEPŠÍ ÚČINNOST BEZPEČNOSTI ZA SKVĚLÉ PENÍZE

- **WHITE BOX EDR/XDR/MDR** – Hloubková ochrana a detekce v reálném čase
- **ANTIMALWARE** – Vícevrstvá ochrana proti malwaru
- **DEVICE CONTROL** – Kontrola zařízení a přístupů
- **FIREWALL** – Síťová ochrana na endpointu
- **AUTOMATIC POLICIES** – Automatické politiky podle kontextu

Data
Identifikace, řízení a ochrana dat

Endpoint
Správa a ochrana koncových zařízení

Risk
Evidence aktiv, plán & řízení rizik

PhishingGym
Cílené kampaně a systematické vzdělávání

AuDit
Rychlý přehled rizik identit, oprávnění a kvality hesel

CTI
Zpravodajství o hrozbách a prediktivní monitoring

PAM
Privilegovaný přístup pod kontrolou

Vulnerability
Skenování zranitelností a řízení nápravných opatření

SERVICES

TECHNICKÁ PODPORA
10/5

LIFECYCLE MANAGEMENT
Plánování, implementace, provoz a rozvoj

SOC MONITORING & RESPONSE
24/7 detekce & automatická reakce
10/5 analytický tým L1–L3

ZÁKAZNICKÝ PORTÁL
Vše přehledně na jednom místě.

1. **JEDEN PARTNER** – Technologie, služby a experti pod jednou střechou
2. **PoC & PoV** – HW FreeDivision, ALL-in-ONE, Ready to GO
3. **KOMPLEXNÍ OCHRANA** – Od koncových bodů až po data a privilegované účty
4. **MĚŘITELNÉ VÝSLEDKY** – Snížení rizik, detekce, reakce, TCO
5. **LEGISLATIVA** – NIS2, ZoKB, DORA, ISO27000, GDPR...

NA JEDNOM PŘÍBĚHU

Jeden útok, celý ekosystém

1 · FD.io CTI

Na dark webu se objeví přihlašovací údaje vašeho zaměstnance.

2 · FD.io Advanced

Účet se v noci přihlásí z neobvyklé země. Advanced to spojí s únikem.

3 · FD.io Vulnerability

Útočník míří na server s neopravenou kritickou zranitelností.

4 · FD.io Data

Víme přesně, k jakým citlivým datům měl účet přístup.

5 · SOAR + Essential

Stanice izolována, účet zamčen, IP zablokována. Automaticky.

6 · FD.io Risk + portál

Incident se propíše do rizik a podkladů pro NIS2. Vy ho vidíte v portálu.

Když systémy vidí celý obraz, automatické reakci se dá věřit.

SLUŽBY

Za každou technologií stojí naši lidé

SOC monitoring a reakce

Detekce a automatická reakce 24/7, analytici L1–L3 10/5

Technická podpora

10/5 se SLA a vlastním Service Deskem

Lifecycle management

Plánování, implementace, provoz a rozvoj

PhishingGym

Cílené phishingové kampaně a vzdělávání uživatelů

AuDit

Rizika identit, oprávnění a hesel v AD a Entra ID

VulnerAbility

Pravidelné skeny zranitelností a plán nápravy

CERTIFIKACE A ZASTOUPENÍ

Důvěra, kterou si necháváme ověřit

Máme

ISO/IEC 27001
Řízení bezpečnosti informací · od 2021

ISO 9001
Řízení kvality · od 2021

Exkluzivita
Zastupujeme většinu vendorů pro ČR a SK

Míříme

ISO 31000
Řízení rizik

NBÚ: firma, stupeň Důvěrné
Prověrka podnikatele pro práci s utajovanými informacemi

NBÚ: produkt HarfangLab
Certifikace EDR ve FD.io Essential, navazujeme na certifikaci od BSI

FREEDIVISION 2.0 · DALŠÍ ČÁST

Zákaznický portál

Celá vaše bezpečnost na jednom místě. Vývoj je rozběhnutý, finální verze v roce 2027.

Customer Care | **Co v portálu uvidíte** | **Ukázkový výstup**

NOVĚ V TÝMU · CUSTOMER CARE

Přiznáváme barvu: bez vaší spokojenosti není obnova

Prodáváme předplatné. Když neuvidíte přidanou hodnotu, neobnovíte. Proto máme Radka.



Radek Vostřez

Customer Care

- **Nic nezapadne ve skladu**: hlídá nasazení i reálné využití
- **Pravidelné reporty**: co se dělalo a proč
- **Pravidelné QBR**: co vám technologie přinesla a co dál
- **Posouvá vás dál**: další krok, který má smysl
- **Váš hlas uvnitř firmy**: eskalace, když něco nejde

Nemá obchodní ani technické KPI. Měří se jen tím, jak jste spokojení vy.

NOVINKA · ZÁKAZNICKÝ PORTÁL

Celá vaše bezpečnost na jednom místě

Přehled
Health score, kritické nálezy, incidenty, EDR pokrytí

Akční centrum
Co čeká na vaši reakci; kritické případy i SMS

Bezpečnost podle technologií
Endpoint, SIEM, zranitelnosti, CTI, awareness

Služby a licence
Využití, expirace a čerpání MD

Service Desk a SOC reporty
Tickety, SLA a pravidelné reporty

Lidé a přístupy
Kontakty, role a jejich pravidelné ověření



Beta verze

konec Q4/2026

Na dalších slidech náhledy, jak bude portál vypadat

UKÁZKOVÝ VÝSTUP PORTÁLU · FIKTIVNÍ DATA

Portál neukazuje data. Ukazuje rozhodnutí.



5 akcí
čeká na vaše rozhodnutí, jedna má lhůtu dnes do 18:00

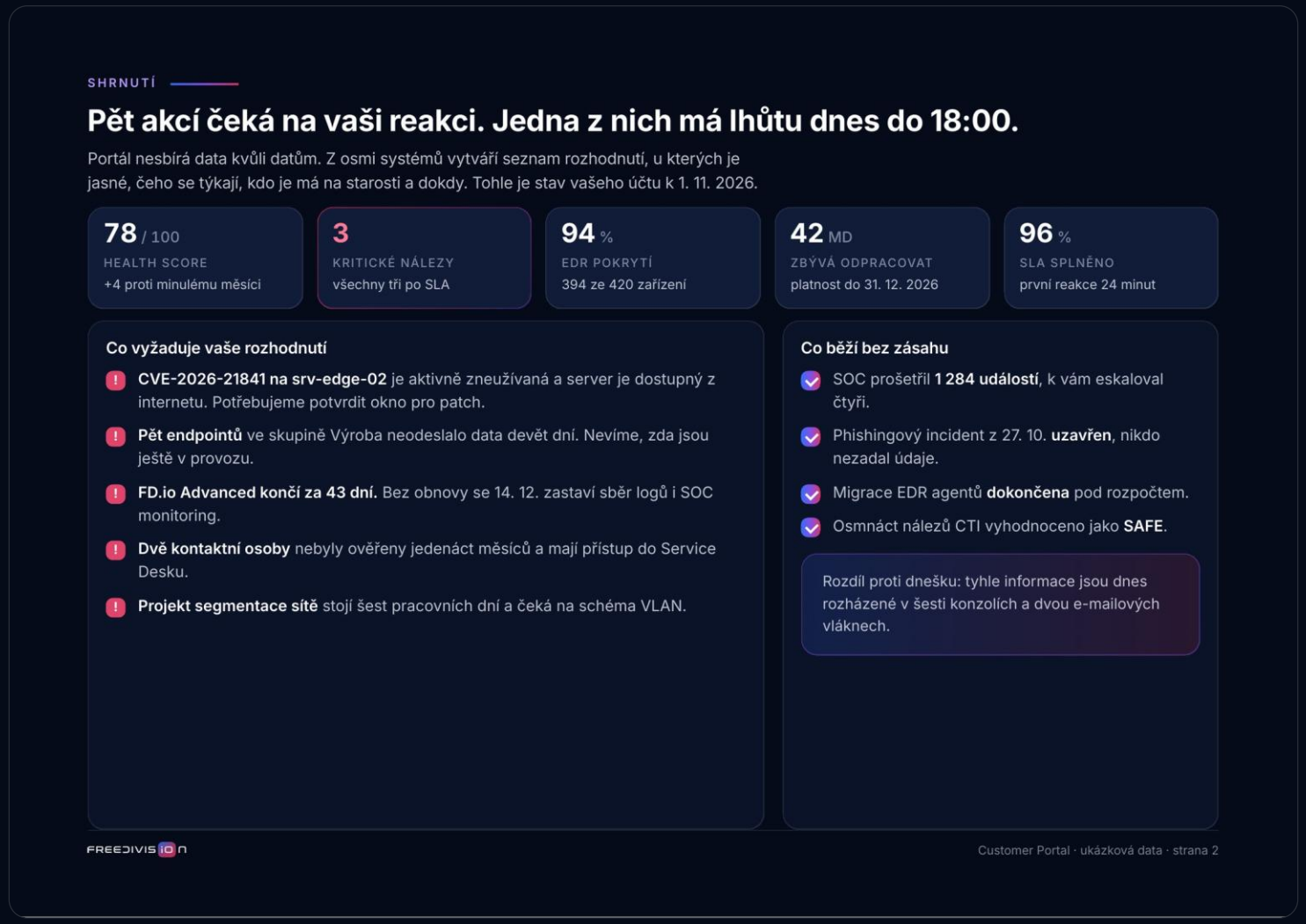
1 284 → 4
událostí prošetřil SOC, k vám se dostaly čtyři

1 obrazovka
místo šesti konzolí a hromady e-mailů

21 strojů
s Windows 10 bez agenta, přitom licence jsou volné

42 MD
zbývá vyčerpat, portál řekne dřív, než propadnou

5 kroků
doporučení v pořadí, první dva nestojí nic navíc



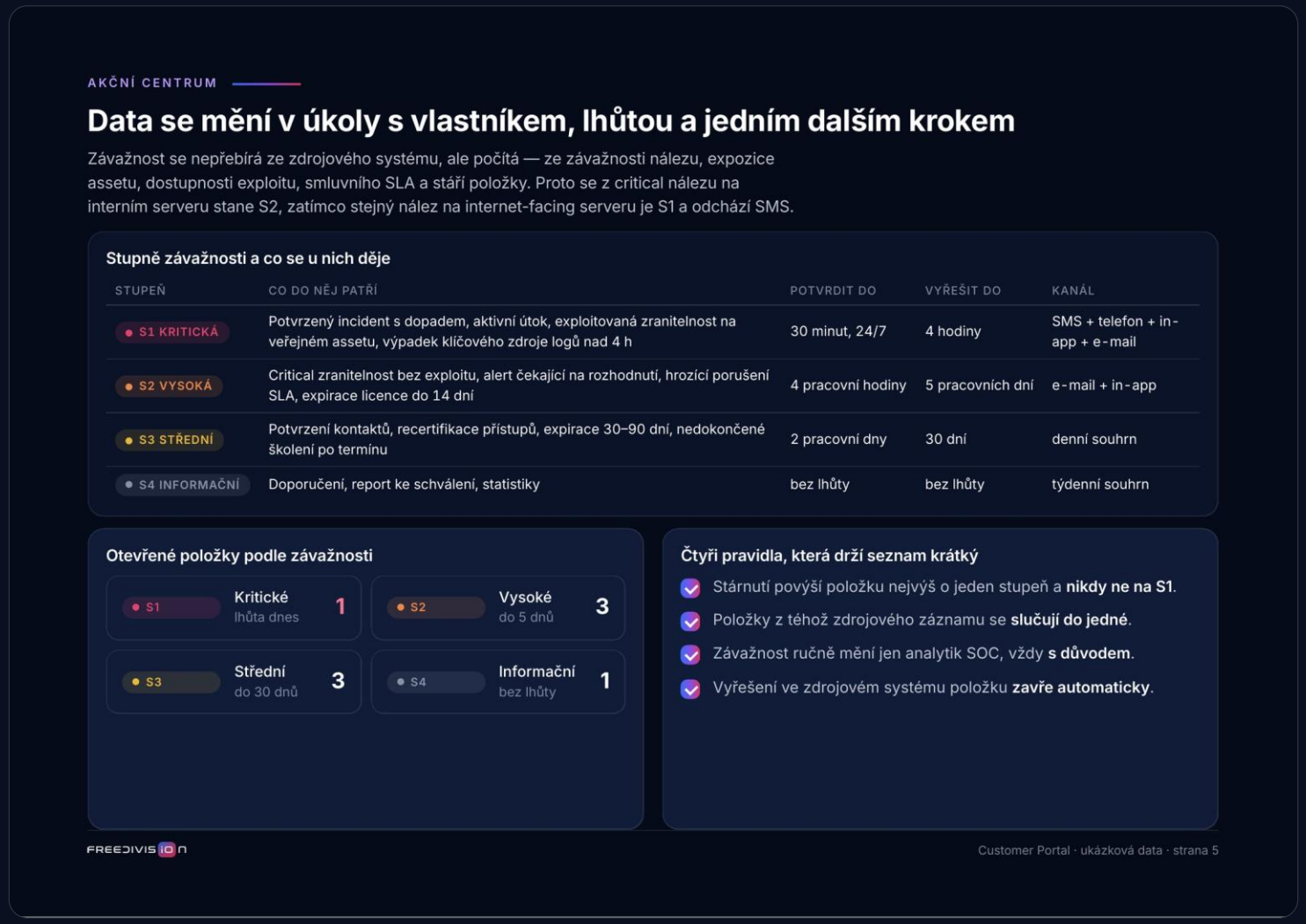
PORTÁL · SHRNUTÍ

Ráno víte, co je na vás

5 akcí
čeká na vaše rozhodnutí, každá s vlastníkem a lhůtou

78 / 100
health score účtu, +4 proti minulému měsíci

6 konzolí
a dvě e-mailová vlákna nahradí jedna obrazovka



PORTÁL · AKČNÍ CENTRUM

Závažnost se počítá, ne přebírá

S1 do 30 min

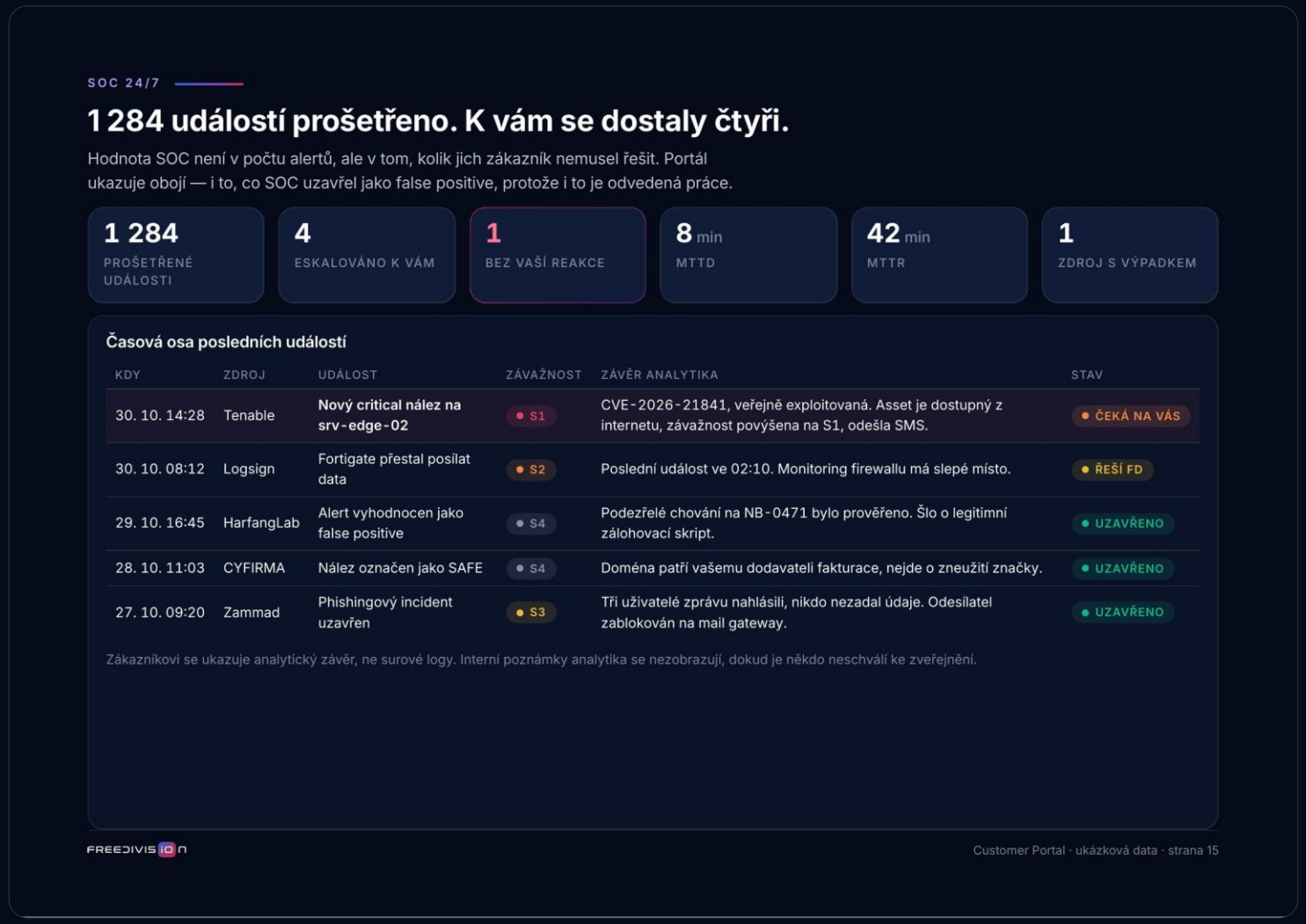
potvrzení 24/7, upozornění SMS, telefonem, v portálu i e-mailem

Interní S2, z internetu S1

stejný nález, jiná priorita podle toho, kde leží

4 pravidla

drží seznam krátký: slučování duplicit a automatické uzavření



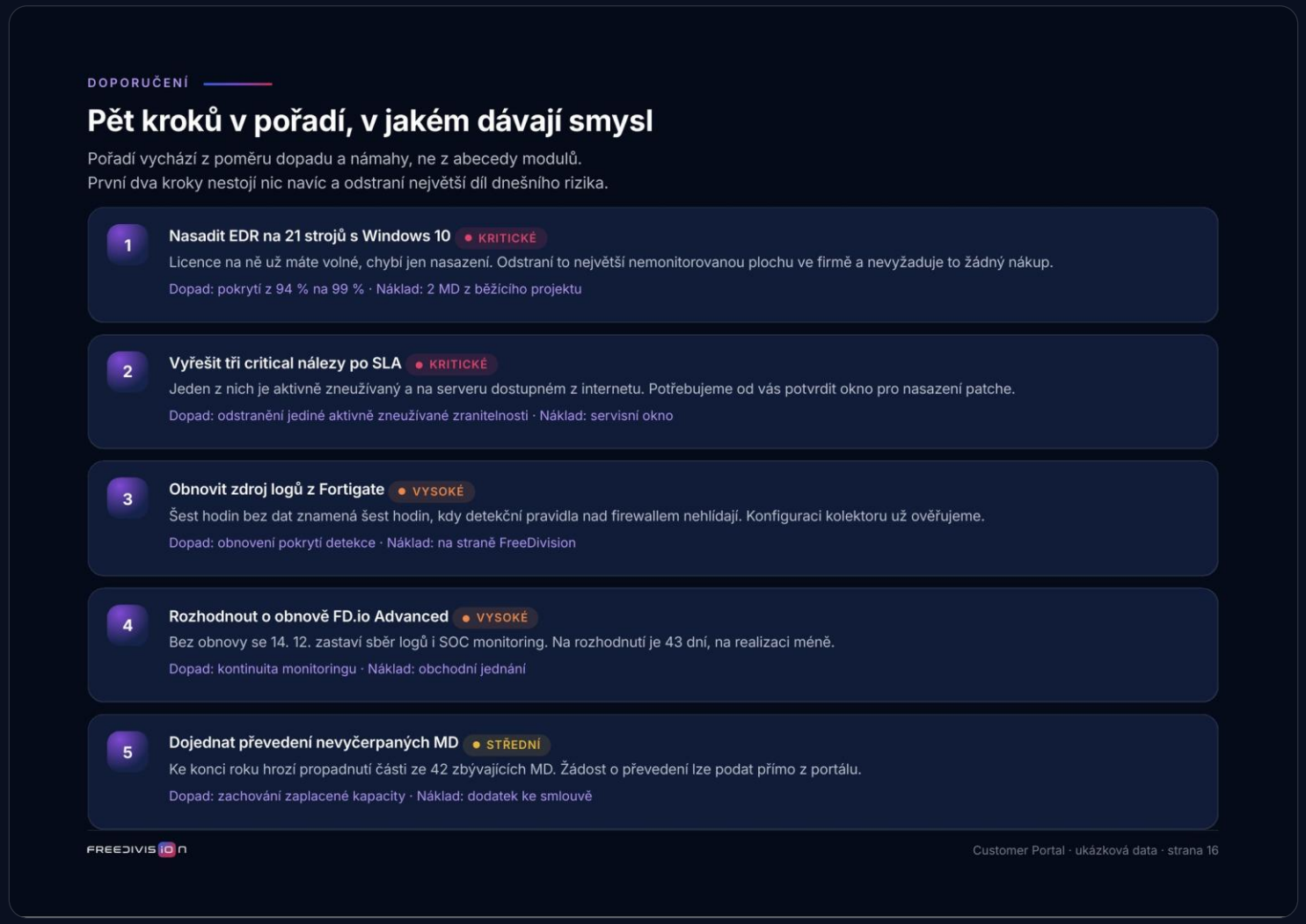
PORTÁL · SOC 24/7

1 284 událostí. K vám se dostaly čtyři.

1 284
událostí prošetřil SOC, i ty uzavřené jako false positive

8 / 42 min
průměrný čas detekce a čas vyřešení

Závěr, ne log
u každé události, co se stalo a co s tím uděláme



PORTÁL · DOPORUČENÍ

Na konci vždy jasný další krok

5 kroků
seřazených podle dopadu a námahy, ne podle modulů

94 → 99 %
pokrytí EDR jediným krokem, licence už máte

Na pravidelné schůzce z toho uděláme plán.

FREEDIVISION 2.0 · POSLEDNÍ ČÁST

FreeDivision.io PoC Box

Celý ekosystém v jednom hardwaru. Postavený na technologiích, kterým věříme.

Technologie v boxu | **Co box umí** | **60 dní a 8 lidí**

PARTNEŘI AKCE

Děkujeme technologiím, na kterých stavíme

Absolute (SyxSense)
- FD.io Endpoint

flexiiGuard
- FD.io Risk

IKARUS · HarfangLab
- FD.io Essential

Logsign
- FD.io Advanced

TargetFive
- FD.io PhishingGym
- FD.io AuDit
- FD.io Vulnerability

Varonis
- FD.io Data

CYFIRMA
- FD.io CTI

Everfox (DEEP SECURE)
- IEG
- Datové diody

Připravujeme
- AI Triage a vyhodnocování

Připravujeme
- Shadow AI Security

Většina z nich běží i v PoC boxu. Každou technologii známe do hloubky a garantujeme ji vlastními lidmi.

POC BOX

Celý ekosystém v jednom hardwaru

Všechny technologie předinstalované a propojené, včetně PoC portálu. Přivezeme ho, zapojíme a ukazuje výsledky na vašich datech.

Uvnitř boxu

- **FD.io Advanced**
- Essential
- Data
- Risk
- Vulnerability
- CTI
- AuDit: MS AD a Entra ID
- PoC portál

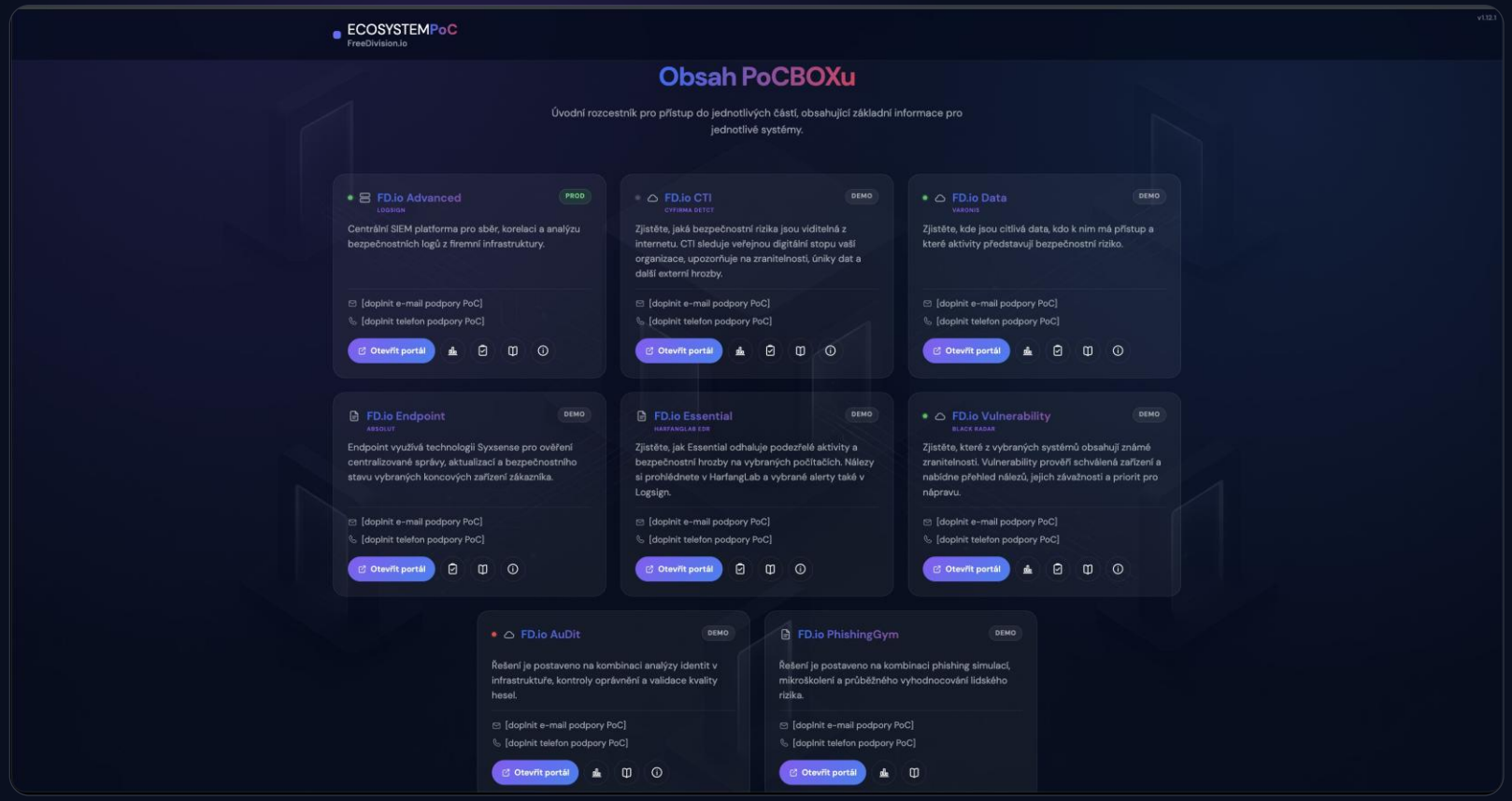
Připraveno k okamžitému spuštění

Předintegrované, bez týdnů nastavování



POC BOX · INTERNÍ POC PORTÁL

Jeden rozcestník ke všem technologiím v boxu



8 modulů

Advanced, CTI, Data, Endpoint, Essential, Vulnerability, AuDit, PhishingGym

Na jeden klik

Portál, reporty, dokumentace a podpora ke každému modulu

Stav na první pohled

U každého modulu PROD nebo DEMO

Kontakty doplníme podle týmu přiděleného na vaše PoC, ještě než box odešleme.

JAK PROBÍHÁ POC · 60 DNÍ

PoC není jen krabice. U vás se protočí 8 našich lidí.

1 Ambasador FD.io PoC **Michal Hrinda**	2 Projektový manažer **Bohdan Keil**	3 SIEM a SOAR **Jakub Šlampa**	4 Specialista EDR **Václav Hurt**
5 Specialista Data **Viktor Jahna**	6 Konzultant Risk **Josef Kazík**	7 Ambasador CTI **Sandro Huber**	8 SOC analytici **L1–L3**

Den 1

Box dorazí, zapojíme a připojíme zdroje

Dny 1–60

Plné nasazení a pravidelné reporty z každé technologie

Den 60

Závěrečné vyhodnocení, sada reportů a další kroky

DALŠÍ KROK

Chcete PoC u sebe?

Řekněte si o CTI sken nebo PoC risk assessment zdarma. V pauze, po akci, nebo na sales@freedivision.com.

09:40 FD.io Advanced: srdce ekosystému naživo



BLOK 3 · 09:40–10:10

FD.io Advanced

03

Vrchol ekosystému a pokročilá platforma. Naživo.

powered by Logsign

Jakub Karvánek
CSO, FreeDivision

KDO STOJÍ ZA FD.IO ADVANCED

Logsign: 15 let vývoje jedné platformy

2010
založení firmy

600+
organizací a státních institucí

100+
partnerů a MSSP, 15+ distributorů

4
kanceláře: Haag, San Francisco, Istanbul, Johannesburg

2010	2013	2015	2017	2018	2021	2022	2023	2024
Založení	Log management	Big data v SIEM	Threat Intel	SOAR	Next-gen SIEM	UEBA	Unified SecOps	Cloud

FreeDivision je výhradním zastoupením Logsignu pro Česko a Slovensko od roku 2023.

OCENĚNÍ A RECENZE

Co o Logsignu říkají uživatelé a analytici

4,7 **G2**
z 5 · 54 recenzí

4,7 **Gartner Peer Insights**
z 5 · 100 % hodnocení 4–5 hvězd

4,9 **Capterra**
z 5 · snadnost použití 4,9

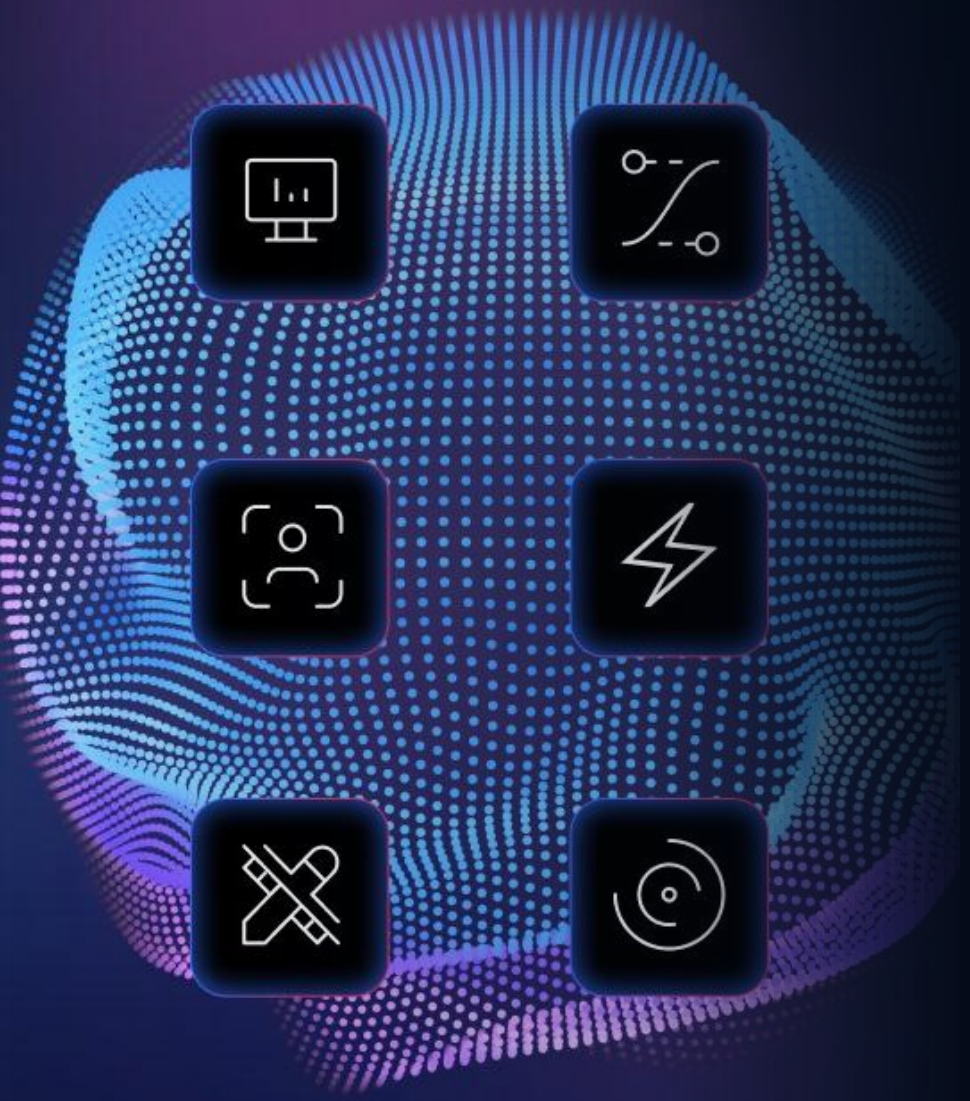
Gartner MQ for SIEM
zmíněn dva roky po sobě (2022)

G2: #1 v použitelnosti
Usability Index pro SIEM, léto 2023

G2 odznaky
High Performer, Easiest to Use, Easiest Setup

Cybersecurity Excellence
SIEM Gold, SOAR Bronze (2021)

„In Logsign SIEM we can easily integrate responses and it's very easy to add data collection devices."
SOC analytik, firma 51–1000 zaměstnanců, G2



CO JE UVNITŘ

Šest nástrojů v jedné konzoli

Log management | SIEM | SOAR | UEBA | Threat Intelligence | Incident case management

550+ integrací pro sběr logů

125+ integrací pro reakci

600+ korelačních pravidel

40+ zdrojů Threat Intelligence

- Neznámý zdroj? **FreeDivision napíše vlastní plugin**, případně ho předáme výrobci jako nativní konektor.
- Chybí response konektor? Výrobce ho vytvoří **zdarma**.
- On-premise, SaaS z datového centra FreeDivision, nebo Blackbox

KONCEPT

Advanced je srdce celého ekosystému

Vidí: všechno připojené

- Infrastruktura, AD, cloud
- Essential: EDR/XDR
- Endpoint · Data · PAM
- Vulnerability · Risk
- CTI: pohled zvenku

ROZHODUJE

FD.io Advanced

Log management · SIEM · UEBA · Threat Intelligence · SOAR · Case management

Jeden pohled, jeden případ, jedna reakce

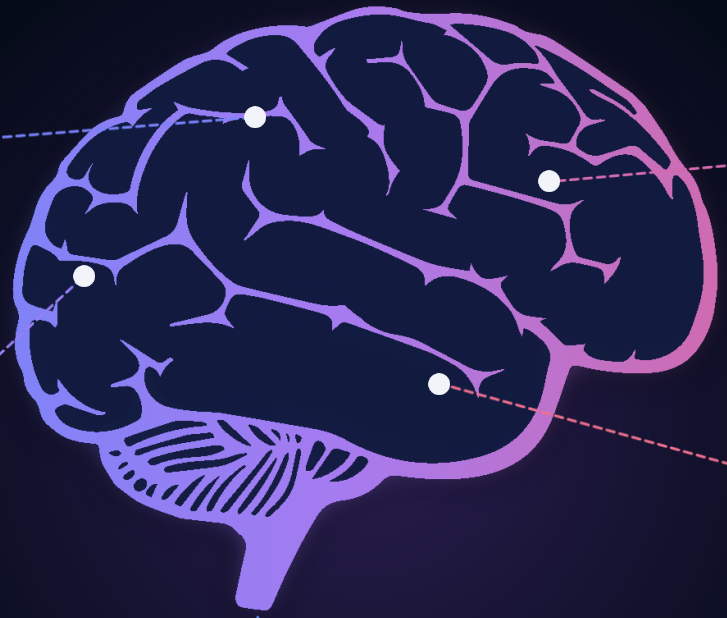
Jedná: automaticky

- Izoluje stanici přes EDR
- Zamkne účet v AD a Entra ID
- Zablokuje IP na firewallu
- Upozorní přes SMS a Teams
- Zapíše vše do portálu

JAK TO FUNGUJE

Nervový systém vaší bezpečnosti

Jako mozek sbírá signály z celého těla, Advanced sbírá data ze všech vašich nástrojů, dává je do souvislostí a včas reaguje.



UEBA

Chování uživatelů a zařízení. Pozná, když se účet chová jinak než obvykle.

Next-gen SIEM

Sběr, obohacení a korelace logů z celého prostředí.

Threat Intelligence

40+ zdrojů o hrozbách. Útočníka pozná už při prvním pokusu.

Detekce a reakce

Vyšetřování a automatická reakce (SOAR) v řádu sekund.

Logy událostí

Surová data ze všech zdrojů. Z nich mozek čerpá.

PROČ JEDEN NÁSTROJ VLÁDNE VŠEM

Slepit pět nástrojů dohromady dnes nestačí

Jedna platforma

Logy, SIEM, SOAR, UEBA a TI v jedné konzoli

Snadné ovládání

#1 v použitelnosti SIEM podle uživatelů G2

Rychlé nasazení

On-premise, SaaS i Blackbox, hybridní prostředí

Rychlost

Odpověď na dotaz v milisekundách, reakce v sekundách

Žádné skryté náklady

Licence na zdroje, ne na objem dat

No stress cost.

LICENCOVÁNÍ

Platíte za zdroje, ne za objem dat

Licence na zdroj

Zdroj je to, co nám logy reálně posílá. Ne každé zařízení zvlášť.

Předvídatelná cena

Víc logů neznamená vyšší účet. Žádné počítání GB ani EPS.

Celá platforma

Log management, SIEM, SOAR, UEBA a Threat Intelligence v jedné licenci.

A kolik zdrojů to u vás bude? Díky agregaci obvykle mnohem méně, než čekáte.

LICENCOVÁNÍ · AGREGACE

Jak počítáme zdroje

1 zdroj

Centrální management / API

EDR, antivir, MDM, vCenter, Microsoft 365, stanice přes WEF/WEC. Celé řešení je jeden zdroj.

1:50 · 1:25

Agregace přes kolektor

Síťová zařízení až 50 na jeden zdroj, servery přes WEF/WEC až 25.

1:1

Přímé připojení

Firewally, řadiče domény, databáze a vše, kde má probíhat automatická reakce.

⚠ Kde chcete automatickou reakci, připojujeme napřímo. Výjimkou jsou EDR a Microsoft 365, kde reakce jde přes API.

☆ **Potřebujete vyšší agregaci? Umíme vyjednat výjimku.**

FD.IO ADVANCED · ŽIVÁ UKÁZKA

Srdce ekosystému naživo

≈ 20 minut

Osm zastávek, jedna platforma. Od prvního konektoru až po náš SOC.

1
Konektory
550+ výrobců, nový konektor se přidá na pár kliků

2
Sběr dat
Logy ze všech systémů na jednom místě

3
Incidenty a alerty
Z milionů událostí pár hotových incidentů

4
Reakce
Izolace stanice nebo blokace účtu

5
Automatizace
Playbooky SOAR, které zasáhnou samy

6
Dashboardy
Přehled pro SOC i pro vedení

7
Integrace
EDR, identity, firewall i ticketing

8
Napojení na náš SOC
A celé to převezme náš tým

BLOK 4 · 10:10–10:40

04

FD.io Essential

Evropské EDR, které mění český trh

powered by HarfangLab + IKARUS security software

Miroslav Mašek
KAM, FreeDivision

Jakub Karvánek
CSO, FreeDivision

PROČ JSME SE ROZHODLI

Nehledali jsme náhradu. Hledali jsme nejsilnější technologii na další roky.

Hrozby řízené AI

Útočníci automatizují průzkum a obcházejí detekci

Antivir nestačí

Trh chce transparentní detekci a otevřené API

Konec QRadar EDR

IBM prodal QRadar SaaS Palo Altu, EDR skončil 31. 8. 2026

Digitální suverenita

Evropský původ, data pod vaší kontrolou

Vlastní evaluace

Podle technických kritérií, ne podle marketingu

Výsledek: evropské EDR, které mění český trh.

JAK JSME HODNOTILI

Devět kritérií velkých firem s vysokými nároky

Kvalita detekce
Chování, MITRE ATT&CK, málo falešných poplachů

Threat hunting
Surová telemetrie a editovatelná pravidla

Incident response
Izolace, forenzní sběr a náprava z konzole

Výkon endpointu
Minimální zátěž CPU a paměti v produkci

Integrace se SIEM
Nativní konektory, napojení na FD.io Advanced

Otevřené API
Plně dokumentované REST API pro automatizaci

Transparentnost
Viditelná detekční logika, žádné černé skříňky

Flexibilní nasazení
Stejná platforma v SaaS, on-premise i air-gapped

Digitální suverenita
Evropský původ, data a soulad s právem EU

Rozhodla technická evaluace, ne marketing dodavatele.

VÝSLEDEK EVALUACE

Dvě evropské technologie, jeden agent

EDR · FRANCIE · OD 2018

HarfangLab

Behaviorální detekce podle MITRE ATT&CK, threat hunting a reakce. Whitebox: editovatelná pravidla a surová telemetrie.

Zakladatelé z francouzského námořnictva, ministerstva obrany a ANSSI

+

EPP · RAKOUSKO · OD 1986

IKARUS

Vlastní engine na analýzu malwaru a blokace ještě před spuštěním. Device control a firewall.

Téměř 40 let zkušeností, hluboká znalost střední Evropy

EDR
detekce a reakce

EPP
antimalware, device control, firewall

ASM a zranitelnosti
integrovaně

1 agent
pro všechny funkce

HarfangLab Guard feat. IKARUS · EU cloud, on-premise nebo air-gapped · vyvinuto a hostováno 100% v Evropě

HARFANGLAB V ČÍSLECH

Čísla z reálného provozu, ne z marketingu

1400+
organizací napříč Evropou

3M+
chráněných endpointů v produkci

16/16
kroků útoku zachyceno, MITRE ATT&CK 2024

4,9
z 5 na Gartner Peer Insights

V MITRE 2024 navíc správně rozlišil 19 z 20 neškodných aktivit schovaných mezi 80 útočnými. Málo falešných poplachů znamená méně práce pro váš tým.

CERTIFIKACE

První EDR, které prošlo francouzskou i německou certifikací

ANSSI · Francie

První EDR s certifikací CSPN (2020, rozšířeno 2024) a kvalifikace ANSSI (12/2024)

BSI · Německo

První EDR s certifikací BSZ (2025), testováno TÜV podle EN 17640

Evropská suverenita

Vývoj, vlastnictví i data v EU. Soulad s GDPR a NIS2.

Cíl: certifikace NBÚ

Chceme, aby HarfangLab získal certifikaci NBÚ jako produkt a navázal na BSI

Certifikace neměří marketing, ale bezpečnost a odolnost samotného produktu.

NEZÁVISLÉ POTVRZENÍ · NATO

Locked Shields 2026

Největší živé cvičení kybernetické obrany na světě, pořádané NATO CCDCOE. Německá armáda vybrala HarfangLab jako technologického partnera a jeho EDR chránilo tým DACHL. Ten vyhrál kategorii technické kybernetické obrany a celkově skončil druhý ze 16 týmů.

Německo **Rakousko** **Švýcarsko** **Lucembursko**

Zdroje: Orange Cyberdefense, člen týmu DACHL (infopoint-security.de, 9. 6. 2026) · Švýcarská armáda (vtg.admin.ch, 24. 4. 2026)



41
zemí

1. místo
technická kybernetická obrana

2. místo
celkově ze 16 týmů

TECHNOLOGIE

Co přesvědčilo nás?

Whitebox detekce	Čitelná a transparentní pravidla: vidíte, proč detekce vznikla, a můžete je upravit.
Množství telemetrie	Nejvíc surových dat bez filtrování. Plný přístup přes API.
Integrace s FD.io Essential Vulnerability	Skeny zranitelností napojené přímo na agenta. Naše vlastní řešení.
Jeden agent	EDR, EPP a ASM v jednom. Žádné konflikty produktů ani dvojitá zátěž.
Nízký dopad na výkon	Minimální zátěž CPU. Chrání i offline, bez závislosti na cloudu.
Stejné v SaaS i on-premise	Máme air-gapped instalace. Stejná platforma v SaaS i on-premise.
Otevřený ekosystém	Nativně napojené na FD.io Advanced: SIEM, SOAR i automatická reakce.

Platforma v akci

≈ 25 minut

Šest zastávek. Žádná simulace, reálné prostředí v reálném čase.

1
Architektura a nasazení
Jeden lehký agent, EU cloud i on-premise

2
Detekce útoku
Viditelná logika: vidíte, proč detekce vznikla

3
Threat hunting
Hledání nad surovou telemetrií, ne nad souhrnem

4
Vyšetřování
Celý útočný řetězec na jedné obrazovce

5
Izolace a náprava
Zásah na stanici z jedné konzole

6
Napojení na FD.io Advanced
Reakce napříč ekosystémem, sama