FREEDIVISION

SOLUTION GUIDE



FreeDivision.io Vulnerability

Řízení zranitelností

Řízené skeny zranitelností formou služby. Pravidelné skenování, prioritizace podle závažnosti a kontextu a jasný plán nápravy – bez vlastní skenovací infrastruktury.

Proč nestačí skenovat jednou za čas

Neaktualizované systémy, zranitelné internetové služby, chybné konfigurace a zastaralé komponenty patří k nejčastějším vstupním bodům útoků. Nové zranitelnosti přitom přibývají každý den a útočníci je začnou zneužívat často jen několik dní po zveřejnění.

Jednorázový sken nebo penetrační test ukáže stav v jednom okamžiku. Za několik týdnů je ale infrastruktura jiná – přibydou nové servery a služby, změní se konfigurace a objeví se nové CVE. Bez pravidelného skenování roste technický dluh, o kterém nikdo nemá přehled.

Vlastní vulnerability management přitom znamená skenovací infrastrukturu, licence, pravidelnou údržbu a hlavně lidi, kteří nálezy vyhodnotí a určí, co opravit jako první. Na to interní IT často nemá kapacitu.

FreeDivision.io Vulnerability přináší vulnerability management jako službu. Infrastrukturu pravidelně skenujeme, nálezy prioritizujeme podle závažnosti a kontextu zařízení a výsledky předáváme v podobě, se kterou lze okamžitě pracovat.

Executive Summary

FreeDivision.io Vulnerability je řízená služba skenování zranitelností. Spojuje lokální skenovací appliance v síti zákazníka, aktuální databázi zranitelností a manažerský reporting do jednoho celku – bez nutnosti budovat vlastní tým nebo skenovací infrastrukturu.

Služba automatizovaně skenuje infrastrukturu bez omezení počtu koncových zařízení, identifikuje známé zranitelnosti a CVE, hodnotí jejich závažnost podle CVSS a kontextu zařízení a uchovává auditovatelnou historii nálezů. Výsledky jsou dostupné v dashboardu 24/7 i v pravidelných PDF reportech a lze je předávat do FreeDivision.io Advanced a FreeDivision.io SOC.

Organizace si volí mezi variantou Starter, kdy s výsledky pracuje interní tým, a variantou Coach, kdy celý vulnerability management průběžně řídíme za ni. V obou případech získává přehled o rizicích, prioritizovaný plán nápravy a podklady pro NIS2, ZoKB a ISO 27001.



Najděte slabá místa dřív než útočník.
Bez provozní zátěže pro vaše IT.

Jak řešení funguje

FreeDivision.io Vulnerability pracuje ve třech na sebe navazujících krocích. Výsledkem není dlouhý seznam nálezů, ale jasné priority oprav.

1 · Skenovat

Lokální appliance nebo virtuální skener v síti zákazníka pravidelně prověřuje:

- servery
- pracovní stanice a endpointy
- síťová zařízení a služby
- externě dostupné služby

Bez omezení počtu koncových zařízení.do vaší sítě.

2 · Vyhodnotit

Nálezy porovnáme s databází známých zranitelností a CVE.

Závažnost hodnotíme podle CVSS i podle kontextu zařízení – stejná zranitelnost má jinou prioritu na serveru dostupném z internetu a na izolované testovací stanici.

3 · Řídit nápravu

IT dostane prioritizovaný seznam oprav, vedení srozumitelný manažerský přehled.

Opakované skeny ověří, že opravy proběhly, a historie nálezů doloží práci se zranitelnostmi při auditu.

Vulnerability management je cyklus, ne jednorázová akce. Každý sken navazuje na předchozí a ukazuje, jak se bezpečnostní stav infrastruktury vyvíjí.

01 **Sken** › 02 **Identifikace CVE** › 03 **Prioritizace** › 04 **Akční plán** › 05 **Oprava** › 06 **Ověření**

Skenovací appliance

Dodáme fyzickou appliance nebo virtuální skener, který běží přímo v síti zákazníka. Implementaci a konfiguraci zajistíme my.

Organizace nemusí provozovat vlastní skenovací řešení ani spravovat licence.

Reporting pro IT i vedení

Dashboard dostupný 24/7 ukazuje aktuální stav a nejzávažnější nálezy. Pravidelné PDF reporty shrnují vývoj pro management.

Auditovatelná historie nálezů doloží, kdy byla zranitelnost nalezena a kdy opravena.

Klíčové schopnosti řešení

Kompletní vulnerability management v jedné službě – od skenování přes prioritizaci až po reporting a audit.

Automatizované skenování

Lokální i externí skeny infrastruktury bez omezení počtu koncových zařízení. Detekce známých zranitelností a CVE na serverech, endpointech a síťových službách. Skeny běží pravidelně a automaticky.

Prioritizace rizik

Hodnocení závažnosti pomocí CVSS doplněné o kontext zařízení. Identifikace kritických aktiv a doporučení, které opravy mají přednost. IT tak neřeší stovky nálezů najednou, ale ty, které skutečně ohrožují provoz.

Manažerský reporting

Přehled nejzávažnějších nálezů, pravidelné PDF reporty a dashboard dostupný 24/7. Vedení vidí stav bezpečnosti infrastruktury a jeho vývoj v čase bez technických detailů.

Integrace a audit

Výsledky lze předávat do FreeDivision.io Advanced a FreeDivision.io SOC. Auditovatelná historie zranitelností a evidence práce s nimi slouží jako podklad pro NIS2, ZoKB a ISO 27001.

Varianty řešení

FreeDivision.io Vulnerability lze nasadit ve dvou variantách – podle toho, kolik práce s nálezy chce organizace převzít sama.

[STARTER]

Starter

Pro organizace, které chtějí kvalitní skenování a s výsledky pracují samy.

- dodávka appliance nebo virtuálního skeneru
- implementace a konfigurace
- pravidelné skeny zranitelností
- základní reporting a dashboard
- onboarding administrátorů

S výsledky pracuje interní tým zákazníka.

[PROVOZ]

Coach

Pro organizace, které chtějí vulnerability management předat do řízené péče.

- všechny služby varianty Starter
- kontinuální správa vulnerability managementu
- pravidelné vyhodnocování nálezů
- prioritizovaný akční plán
- manažerský reporting
- integrace do FreeDivision.io Advanced a napojení do FreeDivision.io SOC

Typické scénáře využití

FreeDivision.io Vulnerability pomáhá organizaci najít slabá místa infrastruktury a opravit je ve správném pořadí.

Pravidelný vulnerability management

Interní IT nemá kapacitu ani nástroje na pravidelné skenování a vyhodnocování nálezů.

Služba skenuje infrastrukturu automaticky, výsledky prioritizuje a ve variantě Coach připravuje akční plán. IT se soustředí na opravy, ne na provoz skeneru.

Nová kritická zranitelnost

Je zveřejněna kritická CVE a vedení se ptá, zda se organizace týká.

Díky pravidelným skenům a historii nálezů je rychle jasné, která zařízení jsou zasažená a jak naléhavá je oprava. Opakovaný sken pak ověří, že náprava proběhla.

Externě dostupné služby

Webové aplikace, VPN brány, poštovní servery nebo vzdálený přístup jsou vidět z internetu – a útočníci je skenují také.

Externí skeny průběžně hlídají zranitelné internetové služby a chybné konfigurace dřív, než je někdo zneužije.

Audit a compliance

Auditor chce doložit, jak organizace řídí technické zranitelnosti.

Auditovatelná historie nálezů, pravidelné reporty a evidence práce se zranitelnostmi slouží jako podklad pro bezpečnostní audit infrastruktury i pro NIS2, ZoKB a ISO 27001.

Přínosy pro organizaci

Hodnotou FreeDivision.io Vulnerability není další report, ale jasné priority oprav a doložitelný bezpečnostní stav.

Lepší přehled o rizicích

Kritické zranitelnosti, priority oprav podle dopadu a pravidelný bezpečnostní přehled infrastruktury.

Méně zátěže pro interní IT

Bez provozu vlastního řešení, bez správy licencí a skenovací infrastruktury, s automatizovaným reportingem.

Rychlejší reakce na rizika

Rychlé odhalení kritických slabin, jasné priority a jednodušší plánování nápravných opatření.

Podpora compliance

Podklady pro NIS2, ZoKB a ISO 27001, auditovatelná historie nálezů a evidence práce se zranitelnostmi.

Co ve vaší infrastruktuře najdeme

FreeDivision.io Vulnerability odhaluje slabá místa, kterými útočníci nejčastěji vstupují do organizace.

Neaktualizované systémy

Chybějící bezpečnostní aktualizace operačních systémů a aplikací

Zranitelné internetové služby

Webové servery, VPN, pošta a vzdálený přístup dostupné z internetu

Chybné konfigurace

Výchozí nastavení, zbytečně otevřené porty a slabé šifrování

Zastaralé komponenty

Software, knihovny a firmware bez podpory výrobce

Známé zranitelnosti a CVE

Podezřelé a podvržené mobilní aplikace s vaší značkou

Technický dluh

Neřízený růst starých systémů a nálezů, které nikdo neopravuje

Priorita podle závažnosti i kontextu

CVSS říká, jak závažná zranitelnost je. Kontext zařízení říká, jak velké riziko představuje právě pro vás. Teprve obojí dohromady určuje, co opravit jako první.

Critical

CVSS 9,0–10,0
Oprava okamžitě, zejména na zařízeních dostupných z internetu

High

CVSS 7,0–8,9
Oprava v nejbližším plánovaném okně

Medium

CVSS 4,0–6,9
Oprava podle kontextu a kritičnosti aktiva

Low

CVSS 0,1–3,9
Evidence a oprava v rámci běžné údržby

Stejná zranitelnost, jiná priorita

Server dostupný z internetu s citlivými daty má přednost před izolovanou testovací stanicí, i když mají stejné CVSS skóre.

Důkazy, které chtějí auditoři

Jaké zranitelnosti organizace má, jak rychle je opravuje a jak to doloží – přehledně, pravidelně a s historií.

NIS2

Směrnice EU o kybernetické

ZoKB

Zákon o kybernetické bezpečnosti

ISO 27001

Opatření 8.8 Řízení technických

AUDIT

Auditovatelná historie nálezů

Pro každého v organizaci

FreeDivision.io Vulnerability není jen pro administrátory. Vedení dostane manažerský přehled, IT priority oprav a auditoři doložitelnou historii.

Vedení a majitelé

Srozumitelný přehled bezpečnostního stavu infrastruktury a jeho vývoje.

Security / CISO

Priority podle závažnosti a kontextu a měřitelné snižování rizika.

IT administrátoři

Prioritizovaný seznam oprav místo stovek nálezů bez pořadí.

SOC

Nálezy předané do FreeDivision.io Advanced a FreeDivision.io SOC.

Risk a compliance

Evidence práce se zranitelnostmi pro NIS2, ZoKB a ISO 27001.

Interní audit

Auditovatelná historie nálezů a pravidelné PDF reporty.

Vlastníci aplikací

Přehled zranitelností systémů, za které odpovídají.

Externí dodavatelé IT

Jasné zadání, co a v jakém pořadí opravit.



Proč FreeDivision

Úspěšná kybernetická bezpečnost nestojí pouze na moderních technologiích. Stejně důležití jsou lidé, správně nastavené procesy a schopnost dlouhodobě udržet zranitelnosti pod kontrolou.

Proto stavíme všechna řešení platformy FreeDivision.io na třech vzájemně propojených pilířích.

Technologie

FreeDivision.io Vulnerability využívá lokální skenovací appliance v síti zákazníka a aktuální databázi zranitelností. Skeny běží automaticky a bez omezení počtu koncových zařízení.

Dashboard dostupný 24/7, pravidelné PDF reporty a integrace do FreeDivision.io Advanced.

Experti

Za vulnerability managementem nestojí jen skener, ale především lidé, kteří nálezům rozumějí a dokážou je převést do konkrétních kroků.

Ve variantě Coach naši specialisté pravidelně vyhodnocují nálezy, připravují prioritizovaný akční plán a manažerský reporting.

Procesy

Řízení zranitelností přináší výsledky pouze tehdy, pokud je součástí pravidelného a systematického procesu. FreeDivision.io Vulnerability propojuje skenování, identifikaci CVE, prioritizaci, akční plán a ověření oprav do jednoho opakovatelného cyklu. Auditovatelná historie nálezů zajistí, že práci se zranitelnostmi lze kdykoli doložit.

FreeDivision.io jako platforma pro komplexní kybernetickou bezpečnost

FreeDivision.io Vulnerability je součástí platformy FreeDivision.io, která propojuje technologie, odborné služby a řízení bezpečnosti do jednoho ekosystému.

Podle potřeb organizace ji lze rozšířit například o automatickou opravu zranitelností, ochranu endpointů, řízení bezpečnostních operací, kybernetické zpravodajství, ochranu dat, bezpečnostní osvětu nebo řízení rizik.

Co nejlépe doplňuje FreeDivision.io Vulnerability

Automatická oprava zranitelností

FreeDivision.io Endpoint jde o krok dál: zranitelnosti na zařízeních nejen najde, ale sám je opraví – automatickým patchováním operačních systémů i aplikací třetích stran, včetně zařízení mimo firemní síť.

Řízení bezpečnostních operací

FreeDivision.io Advanced poskytuje centralizované prostředí pro monitoring, korelaci bezpečnostních událostí a řízení bezpečnostních operací. Nálezy z FreeDivision.io Vulnerability v něm dávají kontext bezpečnostním událostem.

Threat Intelligence

FreeDivision.io CTI přidává pohled zvenčí: které zranitelnosti útočníci právě aktivně zneužívají a co je o organizaci vidět z internetu. Opravujete to, co vás skutečně ohrožuje.

Řízení rizik

FreeDivision.io Risk propojuje aktiva, hrozby, zranitelnosti a opatření do jednoho systému řízení rizik.
Nálezy z FreeDivision.io Vulnerability do něj přinášejí aktuální obraz technických zranitelností.



For Safety Reasons.
Be Best. Not First.

Závěr

Zranitelnosti přibývají každý den a jednorázový sken nestačí. FreeDivision.io Vulnerability proto přináší pravidelné skenování, prioritizaci podle závažnosti a kontextu a jasný plán nápravy jako službu.
Organizace získává profesionální vulnerability management bez provozní zátěže, rychlou identifikaci kritických zranitelností, prioritizovaný plán nápravy a auditovatelný přehled bezpečnostního stavu infrastruktury.
Ve spojení s dalšími řešeními FreeDivision.io se výsledky propojují s FreeDivision.io Advanced a stávají se součástí ucelené bezpečnostní architektury.

Chcete vědět, jaké zranitelnosti ve vaší síti jsou?

Domluvte si živou ukázku nebo si službu otestujte ve vlastním prostředí. Ukážeme vám, co skeny najdou a jak vypadají priority oprav a reporting.

ADRESA

FreeDivision s.r.o.
Rektorská 50/52
108 00 Praha 10 – Malešice
Česká republika

KONTAKT

sales@freedivision.com
+420 220 972 426

www.freedivision.io