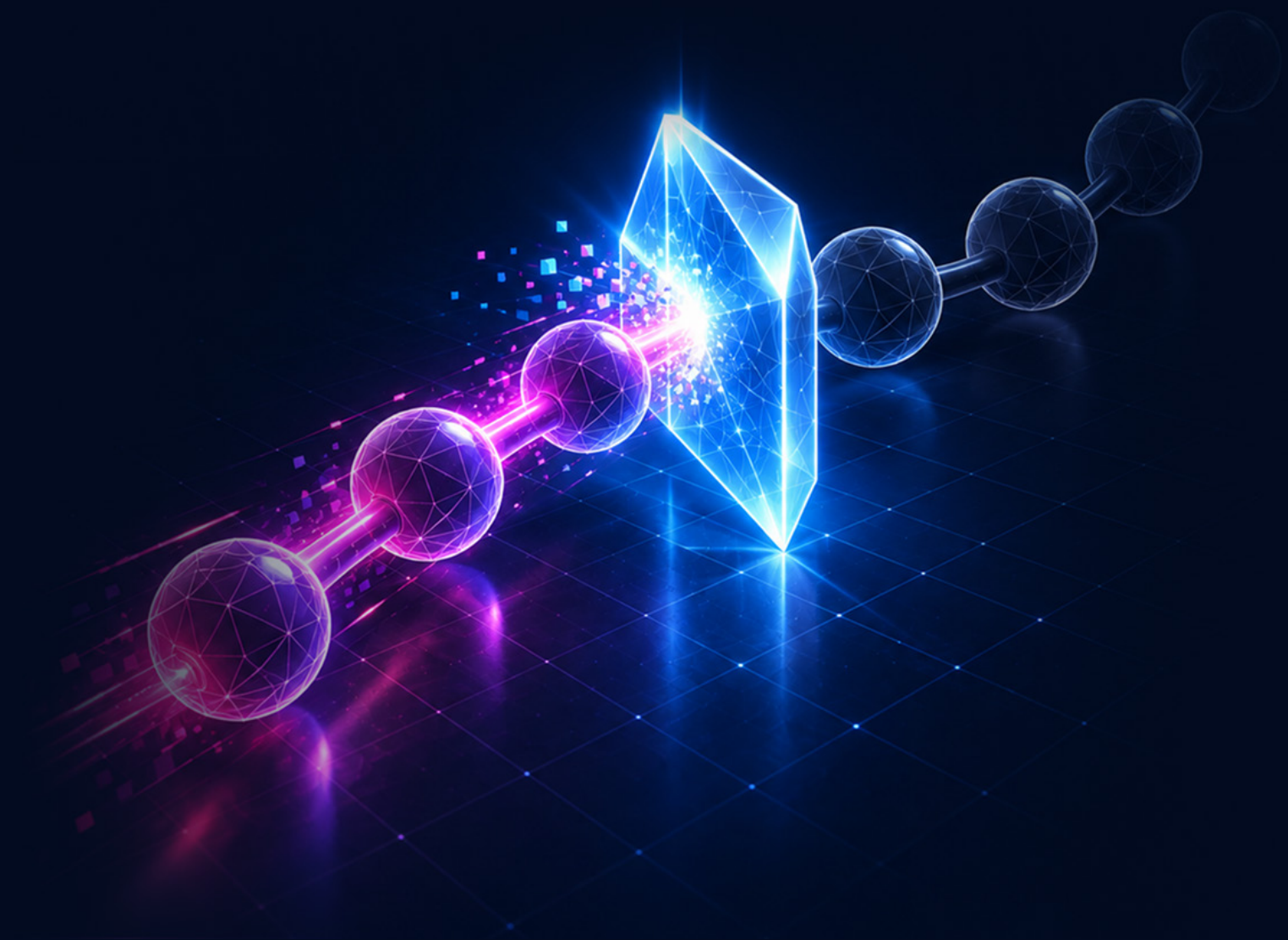
FREEDIVISION

SOLUTION GUIDE



FreeDivision.io CTI

Cyber Threat Intelligence

Pohled útočníka na vaši organizaci. Vnější útočná plocha, ochrana značky, prediktivní zpravodajství a hodnocení dodavatelů – dřív, než útok začne.

Proč nestačí hlídat jen vlastní síť

Firewall, EDR i SIEM jsou důležité – ale všechny sledují, co se děje uvnitř vaší sítě. Útok přitom začíná venku: na fórech, v nabídkách na dark webu, na falešných doménách nebo v zapomenutém serveru, o kterém nikdo neví.

Útočník si cíl vybírá a připravuje týdny. Nejdřív provede průzkum, pak připraví nástroje, phishing a falešné domény a teprve potom útok nasadí. Většina běžných nástrojů reaguje až ve chvíli, kdy útočník zneužije zranitelnost nebo účet – tedy když už je uvnitř a čas hraje proti vám.

Útočníci navíc cílí podle oboru, regionu i geopolitické situace a stále častěji vstupují přes dodavatele a partnery. Obecný přehled hrozeb proto nestačí.

FreeDivision.io CTI se dívá ven – na vaši organizaci očima útočníka. Odhalí zranitelná místa na internetu, zneužití vaší značky, uniklé přihlašovací údaje i kampaně, které se proti vám připravují, a umožní vám zasáhnout dřív, než útok začne.

Executive Summary

FreeDivision.io CTI je cloudová služba kybernetického zpravodajství bez agentů a bez zásahu do vaší sítě. Pokrývá čtyři oblasti: vnější útočnou plochu a zranitelnosti, ochranu značky a digitální stopy, prediktivní zpravodajství o útočnících a hodnocení dodavatelů a třetích stran.

Řešení stojí na principu Odhalit · Předvídat · Zasáhnout. Umělá inteligence zpracovává miliony událostí denně a zkušení analytici z nich vybírají to, co je relevantní pro vaši organizaci, obor a region. Výstupy jsou připravené pro majitele a vedení, management i SOC a volitelně je doplňují žádosti o odstranění falešných domén, profilů a aplikací.

Organizace tak získává pohled útočníka na vlastní organizaci, varování dřív, než útok začne, minimální vnější útočnou plochu, chráněnou značku, bezpečnější dodavatele a podklady pro NIS2, DORA, ISO 27001 i GDPR.



Ostatní hlídají dovnitř.
FreeDivision.io CTI se dívá ven.

Jak řešení funguje

FreeDivision.io CTI pracuje ve třech na sebe navazujících krocích. Řešení nekončí u reportu – každé zjištění vede ke konkrétnímu kroku.

1 · Odhalit

Co je o vaší organizaci vidět zvenčí:
- zapomenuté systémy
- zranitelnosti
- uniklé údaje
- falešné domény
- zneužití značky

Stejný průzkum jako útočník – průběžně, bez agentů a bez přístupu do vaší sítě.

2 · Předvídat

Kdo se o vás zajímá, jaké má motivy a nástroje a kdy, kde, jak a proč může zaútočit.

Zpravodajství zohledňuje obor, region i geopolitickou situaci a odhaluje kampaně už ve fázi přípravy.

3 · Zasáhnout

IT a bezpečnostní tým dostane prioritizovaná doporučení. Zjištění předáme do SIEM, SOAR a ticketovacích systémů.

Na základě vašeho pověření podáme žádosti o odstranění falešných domén, profilů a aplikací.

Zranitelné místo zavřete a účet zablokujete dřív, než je útočník zneužije.

Útok probíhá v sedmi na sebe navazujících fázích. FreeDivision.io CTI zasahuje už v prvotní fázi přípravy útoku – při průzkumu, zbrojení a nasazení, kdy je ještě čas útok zastavit.

01 **Průzkum** › 02 **Zbrojení** › 03 **Nasazení** › 04 **Zneužití** › 05 **Instalace** › 06 **Ovládání** › 07 **Akce v cíli**

Tři úrovně pohledu

Strategický pro majitele a vedení – rizika podle oboru a geopolitiky.
Manažerský – priority a řízení bezpečnosti.
Taktický pro SOC – indikátory a konkrétní opatření.

Každý dostane informace v podobě, se kterou může pracovat.

AI a zkušení analytici

AI zpracovává miliony událostí denně z dark webu, sociálních sítí, internetu, databází zranitelností a obchodů s aplikacemi. Analytici z nich vybírají to, co je relevantní pro vaši organizaci.

Vnější prostředí sledujeme 24/7, klamné cíle zaměřené na váš obor dávají včasné varování. Cloudová služba bez agentů s otevřeným API.

Klíčové schopnosti řešení

Jedna platforma, čtyři oblasti. Všechny sdílejí stejný pohled zvenčí – na vaši organizaci, značku, dodavatele i útočníky.

Vnější útočná plocha

Hlavní oblast: domény, subdomény, IP adresy a cloudové služby, shadow IT a zapomenuté systémy, otevřené porty, chybné konfigurace a prošlé certifikáty. Zpravodajství o zranitelnostech ukáže, které z nich útočníci skutečně zneužívají – priorita podle reálné hrozby, ne jen podle CVSS skóre. Souhrnné skóre napadnutelnosti ukáže, jak snadno se dá organizace napadnout zvenčí.

Značka a digitální stopa

Falešné domény a weby, podvržené profily, deepfaky, podezřelé aplikace, porušení ochranné známky a změny vzhledu webu. Uniklé přihlašovací údaje a data na dark webu. Volitelně za příplatek podáme na základě vašeho pověření žádosti o jejich odstranění u registrátorů, hostingů a platforem.

Prediktivní zpravodajství

Monitorujeme nepřetržitě skupiny útočníků, jejich motivy, nástroje a kampaně. Z milionů událostí denně vybereme ty, které se týkají vašeho oboru, regionu a organizace, a varujeme vás s kontextem: kdo, proč, jakými nástroji a na které systémy cílí.

Dodavatelé a třetí strany

Vnější útočná plocha, zranitelnosti a uniklé údaje dodavatelů a partnerů – bez dotazníků a bez jejich součinnosti. Přehledné hodnocení rizika, průběžné sledování a prověrka firmy před akvizicí.

Varianty řešení

S FreeDivision.io CTI lze začít bezplatnou analýzou vnějších hrozeb a navázat průběžnou službou s důrazem na útočnou plochu, značku nebo dodavatele.

[ANALÝZA]

Analýza vnějších hrozeb zdarma

Stačí nám vaše domény a název organizace – bez agentů a bez závazků.

Analýza ukáže skóre napadnutelnosti – souhrnné hodnocení, jak snadno se dá organizace napadnout zvenčí – a dále vnější útočnou plochu, zranitelnosti, které útočníci aktivně zneužívají, uniklé přihlašovací údaje a data na dark webu, zneužití značky a hrozby pro váš obor a region.

Report vám zůstane. Obdobně lze prověřit dodavatele nebo firmu před akvizicí.

[PROVOZ]

Průběžné zpravodajství pro vaši organizaci

Cloudová služba s průběžným sledováním vnějšího prostředí 24/7.

Organizace získává mapování útočné plochy v reálném čase, ochranu značky s volitelným podáváním žádostí o odstranění podvodného obsahu, prediktivní zpravodajství na třech úrovních a průběžné hodnocení dodavatelů.

Výstupy lze předávat do SIEM, SOAR a ITSM nástrojů i do prostředí FreeDivision.io Advanced.

Typické scénáře využití

FreeDivision.io CTI pomáhá organizaci vidět se očima útočníka a zastavit útok ve fázi přípravy.

Kampaň odhalená ve fázi přípravy

Hacktivistická skupina na uzavřeném fóru plánuje útoky na firmy ve vašem oboru a registruje domény podobné té vaší.

FreeDivision.io CTI zachytí přípravu a pošle varování s kontextem. Žádosti o odstranění falešných domén jsou podané, zranitelná místa zavřená a zaměstnanci varovaní dřív, než kampaň začne.

Zapomenutá aktiva

Testovací server z minulého projektu, stará kampaňová doména nebo zapomenutá služba v cloudu. Útočník je najde během hodin.

Naše řešení je najde dřív než on, ohodnotí jejich riziko a předá seznam priorit pro opravu. Skóre napadnutelnosti pak ukazuje, jak se odolnost organizace zlepšuje.

Ochrana značky

Falešný web, profil ředitele na sociálních sítích nebo aplikace s vaším logem zneužívají důvěru zákazníků i zaměstnanců.

Řešení FreeDivision.io CTI podvodný obsah odhalí. Na základě vašeho pověření podáme žádosti o jeho odstranění u registrátorů, hostingů a platforem a dohlédneme na jejich vyřízení. Pro případné právní kroky dodáme podklady. Uniklé přihlašovací údaje zaměstnanců můžete zablokovat dřív, než je útočník použije.

Dodavatelé a akvizice

Místo dotazníku vyplňovaného jednou ročně získáte nezávislý pohled útočníka na vaše dodavatele a jejich průběžné sledování. O úniku u dodavatele se tak dozvíte hned po zjištění, a ne až z médií.

Před akvizicí prověříme útočnou plochu, uniklá data a historii incidentů kupované firmy. Výsledek je velmi užitečný jako podklad pro vyjednávání o ceně.

Přínosy pro organizaci

Hodnotou FreeDivision.io CTI není další zpráva o hrozbách, ale čas zasáhnout dřív, než útok začne.



Pohled útočníka na vlastní organizaci

Organizace ví, co je o ní vidět zvenčí – zapomenuté systémy, zranitelnosti, uniklé údaje i zneužití značky.



Varování dřív, než útok začne

Kampaně odhalené ve fázi přípravy a zpravodajství šité na míru oboru, regionu a organizaci.



Minimální útočná plocha a bezpečnější dodavatelé

Méně slabých míst u vás i u dodavatelů, chráněná značka a doložitelné podklady pro audit.

Sledujeme místa, kde se útoky připravují

FreeDivision.io CTI běží jako cloudová služba bez agentů a pracuje s veřejně dostupnými a zpravodajskými zdroji.

Dark web a deep web

Uzavřená fóra, tržiště, úniky dat a nabídky přístupů do firem

Sociální sítě a fóra

Hacktivistické skupiny, komunikační kanály útočníků a falešné profily

Internet a DNS

Domény, subdomény, certifikáty, IP adresy a cloudové služby

Zranitelnosti a exploity

Nové zranitelnosti, dostupné exploity a jejich aktivní zneužívání

Obchody s aplikacemi

Podezřelé a podvržené mobilní aplikace s vaší značkou

Integrace

Otevřené a dokumentované API pro integraci SIEM, SOAR a nástrojů ITSM

Zasahujeme už ve fázi přípravy útoku

Většina bezpečnostních nástrojů reaguje, až když je útočník uvnitř. FreeDivision.io CTI zachytí útok v prvních třech fázích, kdy se teprve připravuje.

01 **Průzkum** Mapuje domény, servery a zaměst-nance

02 **Zbrojení** Připravuje nástroje a falešné domény

03 **Nasazení** Rozesílá phishing, zkouší hesla

04 **Zneužití** Zneužije zranitelnost nebo účet

05 **Instalace** Usadí se v systému

06 **Ovládání** Spojení s řídicím serverem

07 **Akce v cíli** Krade či šifruje data

Tady zasahuje FreeDivision.io CTI
útok se teprve připravuje – je čas ho zastavit

Tady reaguje většina běžných nástrojů
útočník už je uvnitř - je pozdě, už škodí

Důkazy, které chtějí auditoři

Jaké hrozby organizaci reálně ohrožují, jak je sledujete a jak hodnotíte své dodavatele – doložitelně a průběžně.

NIS2

Zákon o kybernetické bezpečnosti

DORA

Odolnost finančních institucí

ISO 27001

Opatření 5.7 Threat Intelligence

GDPR

Únik osobních údajů

Pro každého v organizaci

FreeDivision.io CTI není jen pro analytiky. Majitelé a vedení dostanou strategický přehled, management priority a SOC konkrétní opatření.

Vedení a majitelé

Srozumitelný přehled hrozeb pro obor a region a podklady pro rozhodování.

Security / CISO

Priority podle reálných hrozeb a měřitelné snížení vnější útočné plochy.

SOC

Indikátory kompromitace a kontext útoků přímo do SIEM a SOAR.

IT

Seznam zapomenutých systémů a zranitelností, které je třeba opravit jako první.

Risk a compliance

Doložitelné sledování hrozeb a hodnocení dodavatelů pro NIS2 a DORA.

Nákup a dodavatelé

Nezávislé hodnocení rizika dodavatelů a partnerů.

Marketing a PR

Ochrana značky před falešnými weby, profily a deepfaky.

M&A a právní

Prověrka kybernetických rizik firmy před akvizicí.



Proč FreeDivision

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

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

Technologie

FreeDivision.io CTI je cloudová platforma bez agentů a bez instalace. Umělá inteligence zpracovává miliony událostí denně z dark webu, sociálních sítí, internetu a dalších zdrojů a všechny oblasti sdílejí stejný pohled zvenčí.

Otevřené a dokumentované API předává zjištění do SIEM, SOAR a ITSM nástrojů.

Experti

Za kybernetickým zpravodajstvím nestojí jen technologie, ale především analytici, kteří rozumí útočníkům, jejich motivům i fungování organizací.

Z obrovského množství dat vybírají to, co je relevantní pro vaši organizaci, a převádějí to do srozumitelných doporučení pro vedení, management i SOC.

Procesy

Kybernetické zpravodajství přináší dlouhodobé výsledky pouze tehdy, pokud je součástí pravidelného a systematického procesu. FreeDivision.io CTI propojuje průběžné mapování útočné plochy, ochranu značky s volitelným podáváním žádostí o odstranění podvodného obsahu, sledování útočníků a hodnocení dodavatelů do jednoho opakovatelného modelu. Výstupy na třech úrovních zajistí, že se zjištění dostanou k těm, kdo podle nich mají jednat.

FreeDivision.io jako platforma pro komplexní kybernetickou bezpečnost

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

Podle potřeb organizace jej lze rozšířit například o ochranu endpointů, řízení bezpečnostních operací, ochranu dat, správu zranitelností, správu identit a přístupů, bezpečnostní osvětu nebo řízení rizik.

Co nejlépe doplňuje FreeDivision.io CTI



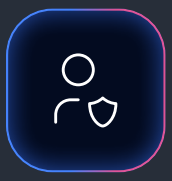
Řízení bezpečnostních operací

FreeDivision.io Advanced poskytuje centralizované prostředí pro monitoring, korelaci bezpečnostních událostí, automatizaci reakcí a řízení bezpečnostních operací. Zpravodajství z FreeDivision.io CTI v něm dává kontext událostem uvnitř sítě.



Správa zranitelností

FreeDivision.io Endpoint najde zranitelnosti na zařízeních a sám je opraví. FreeDivision.io CTI k tomu přidává informaci, které z nich útočníci právě zneužívají – opravujete to, co vás skutečně ohrožuje.



Lidský faktor

FreeDivision.io PhishingGym systematicky snižuje lidské riziko prostřednictvím phishingových simulací a vzdělávání. Zaměstnanci tak rozpoznají i kampaně, které FreeDivision.io CTI odhalí ve fázi přípravy.



Řízení rizik

FreeDivision.io Risk propojuje aktiva, hrozby, zranitelnosti, opatření a dodavatele do jednoho systému řízení rizik. Zjištění z FreeDivision.io CTI do něj přinášejí reálný obraz hrozeb a hodnocení dodavatelů.



For Safety Reasons. Be Best. Not First.

Závěr

Útok se připravuje týdny předem. FreeDivision.io CTI proto doplňuje nástroje, které hlídají dění uvnitř sítě, o pohled zvenčí – na vaši organizaci očima útočníka.

Díky principu Odhalit · Předvídat · Zasáhnout získává organizace varování dřív, než útok začne, minimální vnější útočnou plochu, chráněnou značku a bezpečnější dodavatele.

Ve spojení s dalšími řešeními FreeDivision.io představuje FreeDivision.io CTI přirozenou součást bezpečnostní architektury, která organizaci udrží o krok napřed.

Připraveni podívat se na svou organizaci očima útočníka?

Začněte bezplatnou analýzou vnějších hrozeb. Stačí nám vaše domény a název organizace – bez agentů, bez přístupu do vaší sítě a bez závazků. Report vám zůstane.

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