FREEDIVISION

SOLUTION GUIDE

FreeDivision.io Advanced

Security Operations

Jednotné řízení bezpečnostních operací pro moderní organizace.

Úvod

Digitalizace podnikových procesů, rozvoj cloudových služeb a rostoucí počet propojených informačních systémů zásadně mění způsob, jakým organizace přistupují ke kybernetické bezpečnosti. Zatímco rozsah spravované infrastruktury neustále roste, bezpečnostní týmy jsou nuceny pracovat s omezenými personálními kapacitami a současně čelit stále sofistikovanějším kybernetickým hrozbám.

Ve většině organizací dnes vzniká velké množství bezpečnostních dat. Logy z firewallů, endpointů, serverů, cloudových služeb, identit, síťových zařízení i podnikových aplikací přinášejí cenné informace o dění v prostředí. Jejich hodnota však závisí na schopnosti tato data správně zpracovat a zasadit do souvislostí.

Výzvou je schopnost tato data shromažďovat, propojovat, správně interpretovat a využít při rozhodování.
Bez centralizovaného řízení bezpečnostních operací mohou jednotlivé nástroje fungovat izolovaně. Analytici pak musí přepínat mezi různými konzolemi, ručně ověřovat souvislosti a provádět rutinní činnosti, které prodlužují dobu reakce a zvyšují nároky na bezpečnostní tým.

FreeDivision.io Advanced představuje platformu pro řízení bezpečnostních operací, která propojuje klíčové bezpečnostní disciplíny do jednoho operačního prostředí.

Řešení podporuje současné požadavky na řízení kybernetické bezpečnosti a vytváří základ pro další rozvoj bezpečnostní architektury organizace.

Propojte data. Získejte kontext.
Jednejte rychleji.

Executive Summary

FreeDivision.io Advanced je řešení pro centralizované řízení bezpečnostních operací, které propojuje technologie, data a procesy do jednoho operačního prostředí.

Řešení sjednocuje sběr bezpečnostních dat, jejich korelaci, behaviorální analýzu uživatelů a zařízení, automatizaci reakcí, správu incidentů a využití Threat Intelligence.

Získaná data jsou zpracována v jednotném kontextu, který bezpečnostním týmům usnadňuje analýzu událostí, jejich prioritizaci a následnou reakci.

FreeDivision.io Advanced vychází z konceptu **Unified Security Operations**, ve kterém jednotlivé bezpečnostní technologie spolupracují jako součást jednoho procesu. Nejde proto pouze o SIEM nebo SOAR, ale o prostředí, které propojuje bezpečnostní technologie s procesy a odbornými znalostmi.

V rámci ekosystému FreeDivision.io reprezentuje Advanced strategickou vrstvu pro řízení bezpečnostních operací. Navazuje na ochranu endpointů zajišťovanou řešením FreeDivision.io Essential a vytváří základ pro zapojení dalších specializovaných řešení ekosystému.

Proč centralizovat bezpečnostní operace

Kybernetická bezpečnost dnes není pouze otázkou jednotlivých technologií. Významnou roli hraje také jejich schopnost vzájemného propojení.

Organizace běžně využívají řadu bezpečnostních nástrojů – od firewallů a ochrany endpointů přes cloudové služby a systémy správy identit až po síťovou infrastrukturu a podnikové aplikace. Každý z nich vytváří bezpečnostní události a poskytuje vlastní pohled na prostředí.

Bez vzájemného propojení tak bezpečnostní informace zůstávají rozdělené mezi jednotlivé systémy. Správci IT bezpečnosti často v takových situacích přirozeně selhávají, jelikož jim chybí širší kontext událostí potřebný pro jejich správné vyhodnocení.

Analytik může například potřebovat ověřit, zda upozornění z endpointu souvisí s aktivitou na firewallu, přihlášením uživatele nebo událostí v cloudové službě. Každé další ověření prodlužuje analýzu a zvyšuje riziko, že důležitá souvislost zůstane přehlédnuta.

Rostoucí objem událostí navíc zvyšuje nároky na jejich třídění a vyhodnocování. Závažné incidenty se mohou ztrácet mezi velkým množstvím méně významných upozornění.

Efektivní Security Operations proto stojí na třech základních principech:

01 / Viditelnost

Mít přehled o bezpečnostním dění napříč celou infrastrukturou – od endpointů a serverů až po cloudové služby a podnikové aplikace.

02 / Kontext

Propojovat jednotlivé události tak, aby bylo možné určit jejich význam, souvislosti a potenciální dopad.

03 / Automatizace

Automatizace má omezit množství rutinní práce, snížit chybovost a zkrátit dobu potřebnou pro reakci.

FreeDivision.io Advanced tyto principy propojuje do jednoho prostředí a vytváří společný základ pro řízení bezpečnostních operací.

Jak řešení funguje

FreeDivision.io Advanced představuje centrální vrstvu bezpečnostních operací organizace. Nenahrazuje jednotlivé bezpečnostní technologie, ale propojuje jejich výstupy a využívá je v rámci společných procesů.

Architektura řešení vychází z konceptu Unified Security Operations, ve kterém jednotlivé bezpečnostní disciplíny spolupracují jako součást jednoho procesu.

Sběr a normalizace dat

Řešení centralizuje bezpečnostní události z celé infrastruktury. Přijímá data z endpointů, firewallů, serverů, síťových zařízení, cloudových služeb, systémů správy identit i dalších bezpečnostních technologií.

Události z různých zdrojů jsou převedeny do společného datového modelu, který umožňuje jejich další zpracování a analýzu.

FreeDivision.io Advanced podporuje více než 500 výrobců bezpečnostních nástrojů prostřednictvím nativních integrací a konektorů.

Korelace bezpečnostních událostí

Události z jednotlivých zdrojů jsou v rámci platformy vzájemně propojeny a vyhodnocovány v kontextu dalších relevantních informací.

Behaviorální analýza

Řešení vedle klasických detekčních mechanismů disponuje také behaviorální analýzou uživatelů a zařízení.

Sleduje běžné chování jednotlivých entit a detekuje odchylky, které mohou signalizovat kompromitaci účtu, zneužití oprávnění nebo nestandardní aktivitu.

Tento přístup umožňuje identifikovat také situace, kdy útočník využívá legitimní přístupové údaje nebo běžné administrátorské nástroje.

Automatizace bezpečnostních procesů

Opakující se bezpečnostní činnosti lze automatizovat prostřednictvím předem definovaných pracovních postupů.

Automatizace může zahrnovat ověřování událostí, získávání doplňujících informací, eskalaci incidentů nebo spuštění předem schválených reakcí.

Incidenty lze současně předávat mezi analytiky v úrovních L1 až L3.

Řízení bezpečnostních incidentů

Řešení podporuje evidenci incidentů jako samostatných případů v rámci jednotného procesu.

Podporuje přiřazení odpovědností, dokumentaci jednotlivých kroků, evidenci provedených opatření a vyhodnocení průběhu řešení.

Organizace tak získává přehled o životním cyklu incidentu od jeho detekce až po uzavření.

Threat Intelligence

Threat Intelligence doplňuje interní bezpečnostní data o informace o aktuálních hrozbách a aktivitách útočníků.

Tyto informace lze využít při zpřesňování detekčních scénářů, prioritizaci událostí a vyhodnocování nových typů hrozeb.

Klíčové schopnosti řešení

FreeDivision.io Advanced propojuje jednotlivé funkce do společného procesu Security Operations. Níže uvedené schopnosti představují hlavní funkční oblasti řešení.

Centralizovaný sběr a správa logů

Řešení centralizuje logy z různorodých zdrojů a poskytuje společné úložiště bezpečnostních informací.

Podporuje integraci s endpointy, síťovou infrastrukturou, servery, cloudovými službami, systémy správy identit i podnikovými aplikacemi.

Centralizovaný sběr vytváří základ pro další analýzu, korelaci a reporting a současně podporuje auditní požadavky.

Inteligentní korelace událostí

Řešení propojuje informace z různých technologií a vytváří kontext pro vyhodnocení vznikajícího incidentu.

Analytik tak nepracuje pouze s jednotlivým alertem, ale s informacemi o souvisejících událostech, systémech a uživatelích. To usnadňuje stanovení priority a volbu odpovídající reakce.

Orchestrace bezpečnostních operací

FreeDivision.io Advanced umožňuje vytvářet předdefinované pracovní postupy pro opakující se činnosti.

Automatizovat lze například ověřování událostí, získávání doplňujících informací, eskalaci incidentů, vytváření úloh nebo spuštění předem schválených reakcí.

Behaviorální analýza uživatelů a zařízení – UEBA

UEBA sleduje běžné chování uživatelů a zařízení a identifikuje odchylky od očekávaného provozu.

Pomáhá odhalovat rizikové účty, zneužití oprávnění nebo aktivity, které nemusí vykazovat klasické známky škodlivého chování.

Řízení bezpečnostních incidentů

Řešení podporuje celý proces řízení incidentu – od evidence a přiřazení odpovědností přes dokumentaci jednotlivých kroků až po uzavření případu.

Jednotný proces usnadňuje předávání incidentů mezi členy týmu a vytváří dohledatelnou historii řešení.

Threat Intelligence

FreeDivision.io Advanced umožňuje využívat informace z více než 40 externích zdrojů o známých indikátorech kompromitace, aktivních útočných kampaních, nově publikovaných zranitelnostech a používaných technikách útočníků.

Tyto informace lze využít pro zpřesnění detekčních pravidel, prioritizaci incidentů a vyhodnocení aktuálních hrozeb.

Řešení umožňuje také připojení vlastních zdrojů, například MISP databází Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

Reporting a podpora rozhodování

FreeDivision.io Advanced poskytuje reporting a dashboardy přizpůsobené potřebám jednotlivých úrovní řízení – od provozu a infrastruktury přes bezpečnostní specialisty až po management.
Lze sledovat například vývoj incidentů, vytížení bezpečnostních týmů, úroveň rizik a dlouhodobé trendy.

Architektura řešení

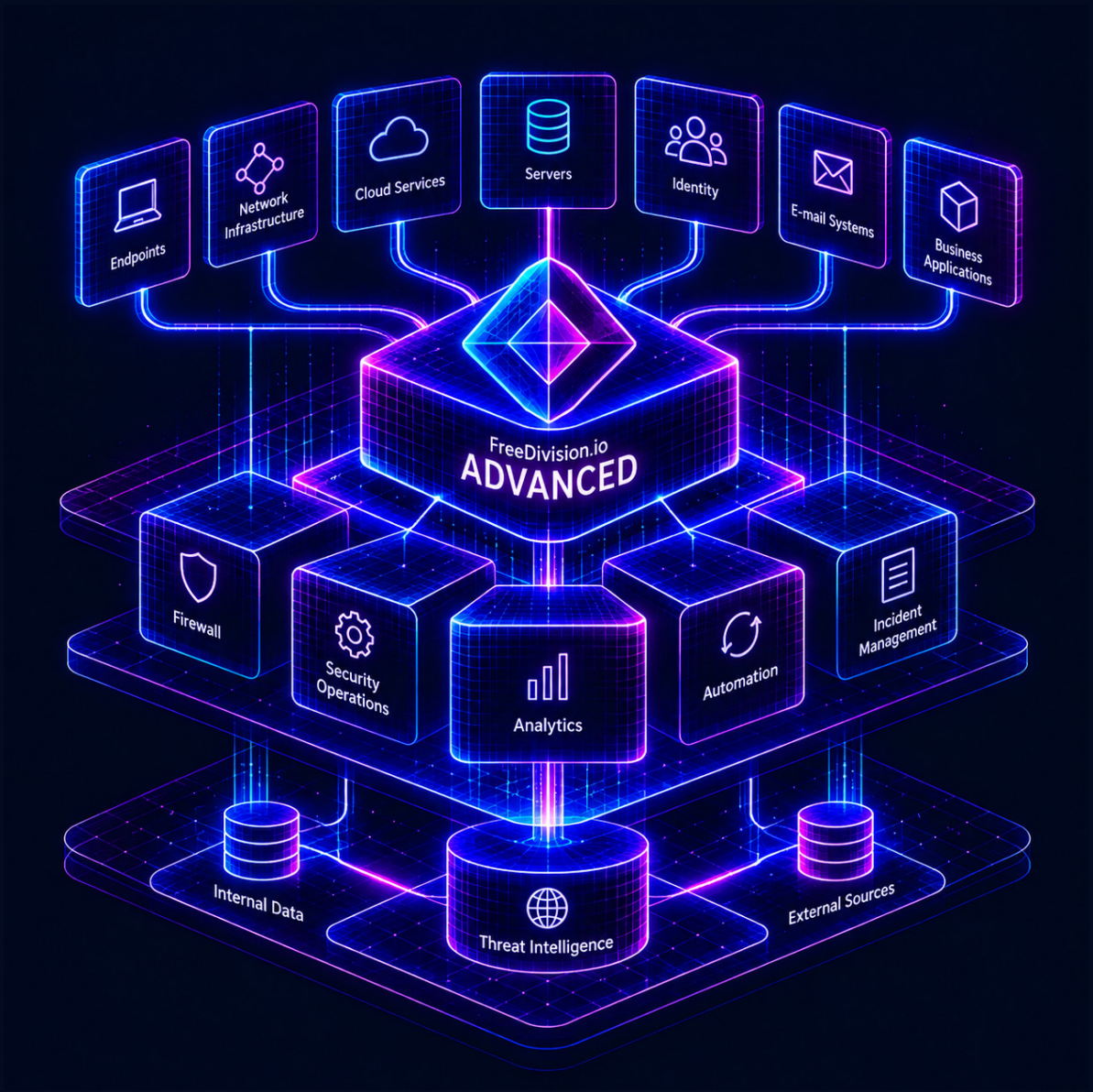
FreeDivision.io Advanced funguje jako centrální vrstva bezpečnostních operací, která propojuje jednotlivé technologie a bezpečnostní procesy.

Na vstupu jsou endpointy, síťová infrastruktura, firewally, servery, cloudové služby, identity, e-mailové systémy a podnikové aplikace. V centrální vrstvě dochází ke sběru a normalizaci dat, jejich korelaci, behaviorální analýze, automatizaci procesů, řízení incidentů a obohacení o informace z Threat Intelligence.

Výstupem je společné operační prostředí pro bezpečnostní týmy a reporting poskytující managementu přehled o bezpečnostním stavu organizace.

Architektura je navržena modulárně. Organizace může postupně rozšiřovat počet integrovaných zdrojů, automatizovaných procesů i bezpečnostních služeb bez zásadních změn základního prostředí.

FreeDivision.io Advanced tak funguje jako centrální operační bod Security Operations a zároveň jako strategická vrstva platformy FreeDivision.io.



Typické scénáře použití

FreeDivision.io Advanced nachází uplatnění zejména v následujících situacích:

Naplnění požadavků compliance

S příchodem novely ZoKB aplikující nařízení EU NIS2 se organizace musí vypořádat s požadavkem na sběr a uchovávání bezpečnostních událostí po dobu 18 měsíců.

Centralizace bezpečnostních operací

Organizace s rozsáhlým nebo heterogenním IT prostředím mohou propojit endpointy, firewally, cloudové služby, systémy správy identit, síťovou infrastrukturu a podnikové aplikace do společného operačního prostředí.

Zrychlení detekce a reakce na incidenty

Incident může vzniknout kombinací několika zdánlivě nesouvisejících událostí.

Například phishing může vést ke kompromitaci identity, následnému přihlášení z neobvyklého místa, pohybu v síti a pokusu o přístup k citlivým datům.

Výhodou je možnost vyhodnotit celý řetězec událostí jako jeden incident a reagovat dříve, než dojde k významnému dopadu na provoz organizace.

Automatizace rutinních činností

Bezpečnostní týmy často věnují významnou část kapacity opakovaným úkonům, jako je ověřování alertů, dohledávání souvisejících informací, vytváření tiketů nebo eskalace standardních incidentů.

Tyto činnosti lze pomocí předdefinovaných pracovních postupů automatizovat a sjednotit.

Podpora interního SOC

Organizace s vlastním Security Operations Center získávají prostředí pro centralizaci bezpečnostních informací, standardizaci procesů a předávání incidentů mezi analytiky.

Řešení podporuje také dokumentaci jednotlivých kroků a dohledatelnost průběhu řešení incidentů.

Rozvoj bezpečnostní architektury

FreeDivision.io Advanced poskytuje základ, který lze postupně rozšiřovat o nové technologie, zdroje dat, automatizované procesy a specializované bezpečnostní služby.

Organizace tak může rozvíjet své Security Operations podle aktuálních potřeb bez nutnosti zásadně měnit základní architekturu.

Přínosy pro organizaci

FreeDivision.io Advanced přináší přínosy na technické, provozní i strategické úrovni.

Jednotný přehled napříč IT prostředím

Bezpečnostní data jsou dostupná v jednom pracovním prostředí a lze je vyhodnocovat v souvislostech napříč infrastrukturou.

Jednotný přehled přináší méně slepých míst a lepší kontrolu nad bezpečnostním děním napříč IT prostředím.

Vyšší efektivita bezpečnostních týmů

Za každým úspěšným bezpečnostním řešením stojí lidé.

Naši specialisté navrhují architekturu řešení, zajišťují implementaci, pomáhají s optimalizací bezpečnostních politik a podle zvolené varianty poskytují také průběžný dohled nad bezpečnostním prostředím.

Organizace tak získává partnera, který rozumí technologii i praktickému provozu.

Rychlejší rozhodování

Bezpečnostní události jsou doplněny o technický a provozní kontext.

Tým tak může rychleji určit, kterých systémů, uživatelů nebo služeb se incident týká a jaká opatření je potřeba přijmout.

Lepší podpora řízení rizik

Management získává přehled o vývoji incidentů, dlouhodobých trendech, vytíženosti bezpečnostních týmů a oblastech vyžadujících další pozornost.

Bezpečnostní informace tak mohou sloužit také jako podklad pro plánování dalších opatření a investic.

Porozumění vlastnímu prostředí

Bezpečnostní události lze vyhodnocovat v souvislostech s aktivy, uživateli, chováním a dalšími bezpečnostními daty. Tento kontext umožňuje lépe pochopit, co se v prostředí skutečně děje, a přesněji určit, které události představují skutečné riziko.

Interní reporting a splněná legislativní povinnost

Management získává přehled o vývoji incidentů, dlouhodobých trendech, vytíženosti bezpečnostních týmů a oblastech vyžadujících další pozornost.

Bezpečnostní informace tak mohou sloužit také jako podklad pro plánování dalších opatření a investic.

Proč FreeDivision

Úspěšné Security Operations nejsou založeny pouze na jedné technologii. Výslednou úroveň ovlivňuje také způsob integrace, odbornost lidí a nastavení procesů.

Proto stavíme FreeDivision.io Ecosystem na třech pilířích:

Technologie s přidanou hodnotou

Využíváme ověřené bezpečnostní technologie a propojujeme je do jednotného operačního prostředí.

Nejde o vytváření další vrstvy nástrojů, ale o jejich efektivní spolupráci. Výsledná podoba řešení vychází z expertní práce týmu FreeDivision a praktických zkušeností získaných při jeho implementaci a provozu u našich klientů.

Experti

Naši konzultanti a bezpečnostní specialisté se podílejí na návrhu architektury, implementaci, integraci i dlouhodobém rozvoji bezpečnostních operací.

Zkušenosti z různých prostředí využíváme při návrhu řešení odpovídajícího konkrétním potřebám organizace.

Procesy

Technologie potřebují odpovídající procesní rámec.

FreeDivision.io Advanced podporuje standardizovaný způsob monitorování, analýzy, eskalace a řešení bezpečnostních incidentů a umožňuje tyto procesy dále rozvíjet podle potřeb organizace.

Technologie + Zdroje + Bezpečnost

FreeDivision.io Advanced propojuje technologické schopnosti, odborné znalosti a procesy do jednoho přístupu k řízení Security Operations.

FreeDivision.io jako platforma pro řízení kybernetické bezpečnosti

Moderní kybernetická bezpečnost není tvořena jednou technologií. Organizace potřebují architekturu, ve které jednotlivé vrstvy ochrany spolupracují, sdílejí informace a lze je postupně rozvíjet.

Na tomto principu je postavena platforma FreeDivision.io.

Jednotlivá řešení platformy představují navazující stavební bloky, které lze využívat podle velikosti, vyspělosti a potřeb konkrétní organizace.

FreeDivision.io Advanced v této architektuře plní roli centrálního operačního bodu a vytváří společný základ pro řízení bezpečnostních operací.n.io.

Od ochrany endpointů k řízení bezpečnostních operací

Pro mnoho organizací je prvním krokem modernizace bezpečnosti ochrana koncových zařízení prostřednictvím řešení FreeDivision.io Essential.

Tato vrstva zajišťuje monitoring endpointů, detekci bezpečnostních hrozeb a podporu reakce na incidenty na pracovních stanicích, noteboocích a serverech.

S rostoucí potřebou širšího kontextu je možné tyto informace propojit s dalšími částmi infrastruktury.

Na tuto potřebu navazuje FreeDivision.io Advanced.

Rozšiřuje pohled z jednotlivých zařízení na celou organizaci a propojuje informace z endpointů, síťové infrastruktury, firewallů, cloudových služeb, identit, serverů a podnikových aplikací.

Organizace tak může postupně přejít od ochrany jednotlivých zařízení k řízení bezpečnostních operací napříč celou infrastrukturou.

Otevřená architektura připravená na další rozvoj

Požadavky na kybernetickou bezpečnost se v čase mění. Přibývají nové informační systémy, cloudové služby, regulatorní požadavky i nové typy hrozeb.

FreeDivision.io Advanced je proto navrženo jako otevřená platforma, kterou lze rozšiřovat o další bezpečnostní oblasti bez zásadních změn základní architektury.

Podle potřeb organizace lze postupně doplňovat například:

- skenování a řízení zranitelností
- správu privilegovaných přístupů
- ochranu dat
- řízení bezpečnostních rizik
- správu identit
- pokročilé služby Threat Intelligence
- phishingové kampaně
- akreditované vzdělávání v oblasti kyberbezpečnosti
- další specializované komponenty ekosystému FreeDivision.io

Jednotlivá rozšíření tak mohou navazovat na existující architekturu bez nutnosti budovat samostatná prostředí.

Výsledkem je architektura, která může růst společně s organizací.

For Safety Reasons. Be Best. Not First.

Závěr

FreeDivision.io Advanced poskytuje společný operační základ pro řízení bezpečnostních operací.

Propojuje bezpečnostní technologie, data a procesy a umožňuje organizaci postupně rozvíjet její bezpečnostní architekturu podle aktuálních potřeb.

V rámci platformy FreeDivision.io představuje Advanced strategickou vrstvu, na kterou lze navazovat dalšími specializovanými řešeními.

Připraveni sjednotit bezpečnostní operace?

Každá organizace má jinou architekturu, provozní požadavky i úroveň bezpečnostní vyspělosti.

FreeDivision.io Advanced proto poskytuje nástroje, které lze přizpůsobit konkrétnímu prostředí a postupně rozvíjet podle jeho potřeb. Společně s vaším týmem navrhneme způsob, jak propojit bezpečnostní technologie, data a procesy do funkčního prostředí Security Operations.

FreeDivision.io Advanced
Jednotný základ pro řízení bezpečnostních operací – od centralizace bezpečnostních dat přes automatizaci procesů až po další rozvoj kybernetické bezpečnosti.

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