FREEDIVISION

Kybernetická bezpečnost nové generace: SOC s FREEDIVISION.IO

Použité pojmy a zkratky

Alert – upozornění na hrozící nebezpečí nebo na útok. A

Compliance – dodržování shody s předpisy. C

Cyber Specialist – kybernetický specialista. C

Cyber Threat Intelligence (CTI) – Zpravodajství o kybernetických hrozbách a predikce kybernetických útoků. C

Data Loss Prevention (DLP) – bezpečnostní koncepce, která identifikuje nebezpečné nebo nevhodné sdílení, přenos nebo používání citlivých dat a pomáhá mu zabránit. D

Data/ Identity/ Endpoint/ Network/ Gateway Protection – Ochrana dat/ identity/ koncových bodů/ sítě/ vstupní brány. D

Data Governance – strategický rámec pravidel, procesů, rolí a standardů pro správu dat v organizaci. D

DORA – Digital Operational Resilience; Nařízení Evropské unie o digitální provozní odolnosti ve finančním sektoru. D

EDR – Endpoint Detection and Response; Detekce a reakce v koncových bodech. E

External Landscape and Reputation Protection – Ochrana vnějšího prostředí a reputace značky. E

GDPR – General Data Protection Regulation; Obecné nařízení o ochraně osobních údajů. G

HIPAA – Health Insurance Portability and Accountability Act; Zákon o ochraně soukromí a bezpečnosti osobních zdravotních informací. H

IEEE – standardy, technické specifikace a normy vyvíjené organizací IEEE (Institute of Electrical and Electronics Engineers), které definují postupy, protokoly a rozhraní pro elektrotechniku, elektroniku a informační technologie. I

Incident Case Management – Řízení incidentů; Obnovení neočekávaně přerušených či zhoršených služeb v co nejkratším čase s cílem minimalizovat dopad na chod organizace. I

Inventory and Assets – Inventář a aktiva. I

IoT – Internet of Things; Internet věcí - síť připojených chytrých zařízení, která sbírají data pro různé aplikace a vyměňují si je přes internet. I

ISO – International Organization for Standardization; Mezinárodní organizace pro normalizaci. I

KPI – Key Performance Indicator; Klíčový ukazatel výkonnosti. K

MDR, MDDR – Managed (Data) Detection and Response; Služba monitorování, detekce hrozeb a rychlé reakce na incidenty (specificky pro data a zálohovací prostředí organizace). M

NIS2 – Network and Information Security; Aktualizovaná směrnice Evropské unie o kybernetické bezpečnosti. N

OT – Operational Technology; Technologie pro řízení a monitorování fyzických procesů v průmyslových prostředích. O

PCI DSS – Payment Card Industry Data Security Standard; Soubor mezinárodních bezpečnostních norem určených k ochraně dat držitelů platebních karet. P

PoV – Proof of Value; Pilotní realizace projektu za účelem otestování a prokázání jeho proveditelnosti a životaschopnosti v reálném prostředí uživatele. P

SLA – Service-level agreement; Smlouva o úrovni služeb. S

SIEM – Security Information and Event Management; Management bezpečnostních informací a událostí. S

SOC – Security Operating Center; Centrum bezpečnostních operací. S

SOAR – Security Orchestration, Automation, and Response; Služba orchestrace, automatizace a reakce na kybernetické bezpečnostní incidenty. S

Storage and Backup Protection – Ochrana úložiště a zálohování. S

Threat Hunter – lovec hrozeb. T

UEBA – User and Entity Behavior Analytics; Analýza chování uživatelů a entit. U

UEM – Unified Endpoint Management; Unifikovaná správa koncových bodů. U

Unifikovaná správa bezpečnostních informací – Unifikovaná správa bezpečnostních informací. U

ZoKB – Zákon o kybernetické bezpečnosti. Z

Pojmy FreeDivision.io

FREEDIVISION.IO – unikátní platforma pro komplexní přístup ke kybernetické bezpečnosti.

FreeDivision.io Active Directory – audit zaměřený na odhalení nejčastějších bezpečnostních a konfiguračních problémů MS AD.

FreeDivision.io Advanced – unifikovaná a komplexní služba bezpečnostního centra typu SIEM/SOAR.

FreeDivision.io CTI – predikce kybernetických útoků formou dohledu vnějšího kyberprostředí organizace.

FreeDivision.io Data – ochrana citlivých dat a prevence úniku informací napříč celou organizací.

FreeDivision.io Endpoint – centralizovaná správa, monitoring a ochrana všech koncových zařízení.

FreeDivision.io Essential – služba bezpečnostního centra postavená na EDR enterprise řešení.

FreeDivision.io PAM – kontrola nad privilegovanými a servisními účty.

FreeDivision.io Phishing – testovací kampaně pomocí simulace phishingových útoků.

FreeDivision.io Professional Services – komplexní služby seniorního týmu FreeDivision.

FreeDivision.io Risk – správa aktiv, včetně detekce a hodnocení jejich rizik.

FreeDivision.io Vulnerability – kontinuální sken zranitelnosti neomezeného počtu IP adresf ormou onprem nebo SaaS.

Úvod

Našim cílem je efektivní optimalizace IT prostředků a jejich využití pro zvýšení ochrany pracovního prostředí s důrazem na preventivní bezpečnost. Základem našeho přístupu je využití stávajících technologií, do kterých zákazník již investoval nemalé prostředky. Jejich potenciál není často plně využitý, což se projevuje již v nastavení bezpečnostních nástrojů jako jsou firewall a antivir/EDR.

Security Operations Center (SOC) od společnosti FreeDivision reprezentuje komplexní a moderní přístup ke kybernetické bezpečnosti. Využíváme vaše stávající bezpečnostní nástroje a doplňujeme je o integrační vrstvu pro efektivní sběr dat. Pro další zvýšení efektivity nabízíme rozšíření o nástroje z naší platformy FreeDivision.io.
Platforma nabízí nejen centralizovaný monitoring a pokročilou analýzu bezpečnostních událostí, ale také integruje bezpečnostní nástroje, jako jsou EDR, PAM, firewally, IDM, antivirová řešení a další, a umožňuje sběr a kontinuální vyhodnocování logů ze serverů, databází, aplikací i cloudových služeb. Navíc disponuje také prostředky automatizace, zejména v oblasti rutinních činností SOC, které dokážou výrazně zkrátit reakční časy na incidenty, minimalizovat dopady útoků a zároveň podpořit splnění legislativních a regulatorních požadavků.

Pilíře služby tvoří především Log Management, SIEM, SOAR, UEBA, Cyber Threat Intelligence a Incident Case Management (ICM). Řešení navíc kontinuálně rozvíjíme o další prvky moderní ochrany.

Zákazník má na výběr ze dvou variant nasazení řešení:
- provoz ve vlastní infrastruktuře (on-premise)
- provoz z datového centra FreeDivision (SaaS)

V obou případech zákazník obdrží nezbytné služby jako je nepřetržitý dohled nad IT prostředím, včasná identifikace hrozeb, rychlá a efektivní reakce na bezpečnostní incidenty a reporting. Veškerý provoz a dohled přitom zajišťuje zkušený tým analytiků FreeDivision, takže zákazníci získávají kvalitní úroveň ochrany bez nutnosti budovat vlastní odborné kapacity.

Pro účely manažerské analýzy a povinného výkaznictví poskytuje platforma rovněž detailní reporty monitorovaného prostředí, včetně reportu o provozu samotné služby bezpečnostního operačního centra (SOC).

Monitoring

Nepřetržitý bezpečnostní dohled nad infrastrukturou.

Nepřetržitá detekce 24/7. Odborná analýza na úrovních L1, L2 a L3 v režimu 10/5 v pracovních dnech.

Analýza alertů

Vyhodnocování a kategorizace bezpečnostních událostí.

Bezpečnostní události průběžně analyzujeme, vyhodnocujeme jejich závažnost a kategorizujeme podle rizika a dopadu na provoz.

Lov hrozeb

Aktivní vyhledávání potencionálních rizik.

Proaktivní služba na vyžádání zaměřená na dosažení nejvyšší úrovně zabezpečení prostřednictvím manuální práce analytického týmu.

Reakce

Rychlé řešení bezpečnostních incidentů.

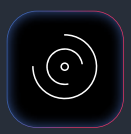
Manuální či automatizované zásahy v systémech zákazníka zacílené na rychlé zastavení a omezení bezpečnostních incidentů.

Doporučení

Pravidelně navrhujeme nápravná opatření.

Analytický tým vytváří návrhy na změny a nastavení jednotlivých systémů.

Reporting



Podrobná dokumentace a analýza výstupů.

Jsou poskytovány detailní reporty monitorovaného prostředí včetně provozu samotné služby dohledového centra.

Oblasti řešení

Jedná se o širokou škálu standardů IT bezpečnosti, řízení kvality a regulatorních pravidel, zaměřenou na detekci potenciálního narušení, hrozeb v reálném čase i v klidovém stavu dat a na prevenci exfiltrace citlivých informací. V duchu proaktivního přístupu Data Loss Prevention (DLP) zajišťujeme sledování, identifikaci a blokování citlivých dat při jejich pohybu, čímž poskytujeme hluboký přehled, detailní kontrolu a široké pokrytí ochrany dat napříč organizací.

External Landscape and Reputation Protection

- METLM – Managed External Threat Landscape Management ✓

Data Protection

- MDDR – Managed Data Detection and Response ✓

Identity Protection

- MEIS – Managed Endpoint and Identity Security ✓
- MEAS – Managed Endpoint Authentication Security ✓
- MIAM – Managed Identity and Access Management ✗
- MUEBA – Managed User Entity and Behavior Analytics ✓

Endpoint Protection

- MDR – Managed Endpoint Detection and Response ✓
- MEMS – Managed Endpoint Management and Security ✓
- MESS – Managed Endpoint Security Solution ✓

Network Protection

- MDDI – Managed DNS, DHCP, and IP address management ✓
- MNDR – Managed Network Detection and Response ✗
- MNAC – Managed Network Access Control ✗

Gateway Protection

- Managed FW ✗
- Managed VPN ✗
- Managed WAF ✗
- Managed Sandboxing ✓
- MDSIR – Managed DDoS Security Incident Response ✗

OT/IoT Protection

- Industrial Control Systems – ICS Security ✗
- SCADA Security (Supervisory Control And Data Acquisition) ✗

Inventory and Assets

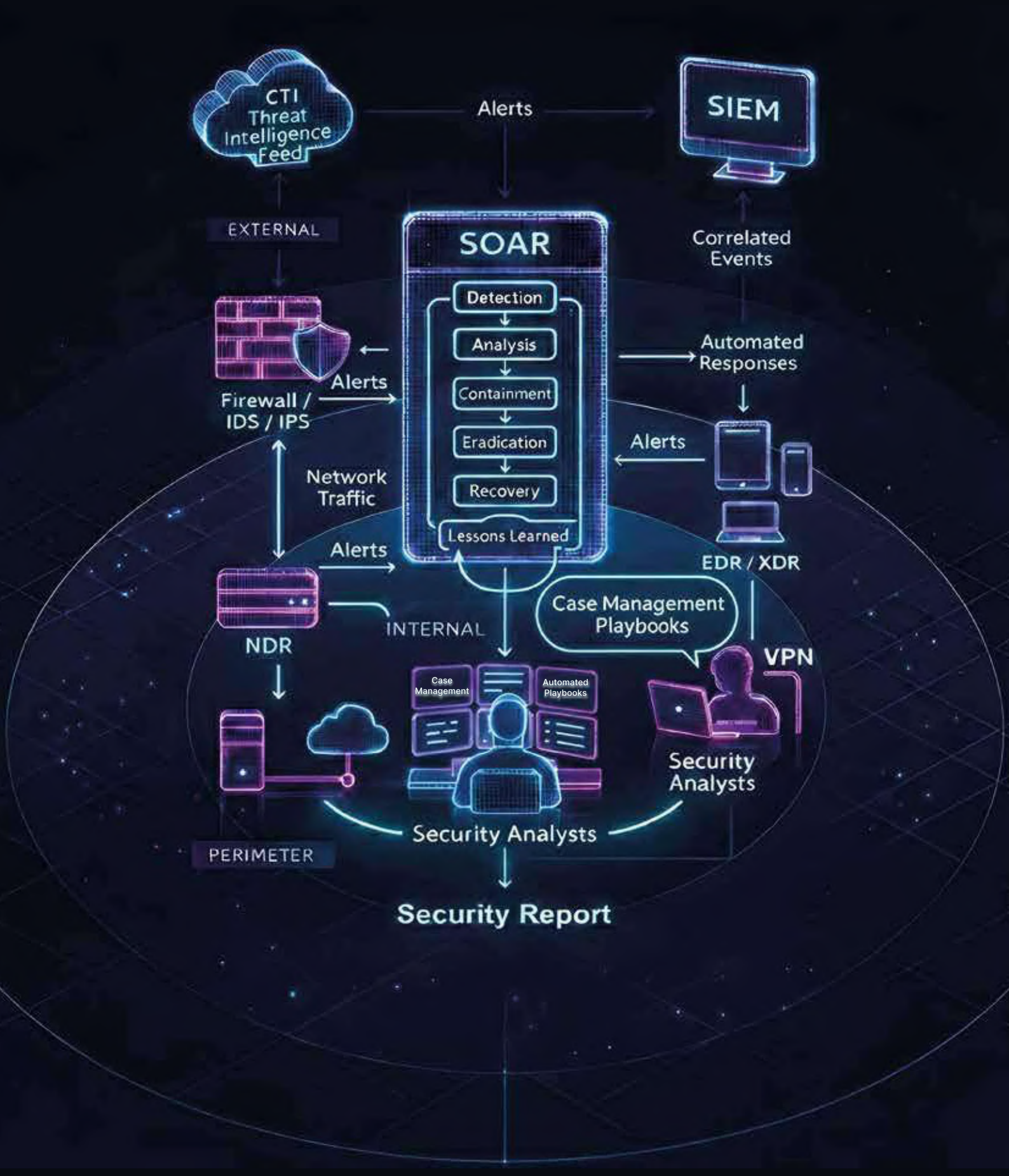
- MITAM – Managed IT Asset Management Solution ✗
- MDC – Managed Device Control ✓

Storage and Backup Protection

- Data Storage Management ✓
- Storage Security Management ✓
- Storage Area Network Security ✓
- Managed Storage Solutions ✗

Compliance

- ZoKB ✓
- GDPR ✓
- NIS, NIS2 ✓
- PCI ✓
- HIPPA ✓
- ISO 27001, 9001 ✓
- IEEE ✓
- DORA ✓


CTI
Threat
Intelligence
Feed
Alerts
SIEM
EXTERNAL
SOAR
Correlated
Events
Detection
Analysis
Containment
Eradication
Recovery
Lessons Learned
Automated
Responses
Alerts
Firewall /
IDS / IPS
Alerts
Network
Traffic
EDR / XDR
Alerts
NDR
INTERNAL
Case Management
Playbooks
VPN
Case
Management
Automated
Playbooks
Security
Analysts
Security Analysts
PERIMETER
Security Report

Komponenty služby

Korelace bezpečnostních událostí – SIEM

FreeDivision.io Advanced

SIEM slouží jako centrální bod pro sběr, korelaci a analýzu bezpečnostních událostí z různých systémů a zařízení. Podporuje více než 500 předdefinovaných korelačních pravidel a umožňuje vytvářet vlastní pravidla dle potřeb zákazníka. Integrace SIEM s více než 40 Cyber Threat Intelligence feedy umožňuje identifikovat známé hrozby a anomálie v reálném čase a díky obohacení o fukcionality UEBA může SIEM indikovat kompromitaci účtu, insider threat nebo zneužití oprávnění. Součástí je také pokročilá vizualizace dat, dashboardy a reporting pro auditní a compliance účely.

Automatizace a orchestrace bezpečnosti – SOAR

FreeDivision.io Advanced

SOAR umožňuje automatizaci a orchestraci bezpečnostních procesů. Díky předdefinovaným playbookům lze rychle nasadit automatizované reakce na incidenty, jako je blokace IP adresy, izolace zařízení nebo eskalace na vyšší úroveň. SOAR také umožňuje dokumentaci znalostí a přenos know-how mezi členy týmu. Pomocí předdefinovaných playbooků lze rychle nasadit automatizované reakce na incidenty, jako je blokace IP adresy, izolace zařízení nebo eskalace na vyšší úroveň.

Ochrana koncových zařízení EDR/XDR/MDR

FreeDivision.io Essential

Jde o službu nezbytné ochrany, tj. řešení pro detekci a reakci na hrozby, které v reálném čase identifikuje škodlivé aktivity na koncových zařízeních (počítače notebooky, servery), umožňuje jejich okamžitou izolaci a minimalizuje dopady na provoz organizace. Pomocí nativní integrace s naší unifikovanou bezpečnostní platformou poskytuje komplexní ochranu proti aktuálním sofistikovaným kybernetickým útokům.

Bezpečná a chytrá správa koncových zařízení

FreeDivision.io Endpoint

Řešení pro správu koncových zařízení poskytuje centralizovaný přístup k automatizovanému deploymentu softwaru, patch managementu a skenování zranitelností napříč celým IT prostředím. Díky vysoké míře automatizace výrazně snižuje provozní a personální (HR) náklady, eliminuje manuální práci IT týmů a umožňuje spravovat rozsáhlou infrastrukturu s minimálními interními zdroji. Současně zajišťuje průběžnou identifikaci bezpečnostních slabin, jejich prioritizaci a rychlou nápravu a snadno se integruje do prostředí naší platformy.

Ochrana a zabezpečení dat (DLP)

FreeDivision.io Data

Řešení Data Governance Security je navrženo pro ochranu citlivých dat, identifikaci bezpečnostních rizik a prevenci úniků informací napříč celou organizací. Pomocí pokročilé analytiky monitoruje přístupy k datovým úložištím, sleduje chování uživatelů a včas upozorňuje na podezřelé či neobvyklé aktivity. Platforma podporuje (Nástroj umožňuje) automatizované reakce na bezpečnostní incidenty, poskytuje přehledný reporting pro auditní a compliance účely a díky integraci s ostatními SOC řešeními zajišťuje komplexní a jednotnou ochranu dat.

Predikce kybernetických útoků

FreeDivision.io CTI

Odraďte útočníky proaktivní inteligencí tak, že použijete jejich pohled na Vaši organizaci, aniž by se o tom dozvěděli. Zjistíte, co o vás útočníci ví a v případě chystaného útoku obdržíte včasné varování s doporučením, jak útoku zabránit. Naší specialitou je zobrazení kritických míst (uniklá data, přístupové údaje, zranitelnosti.) Umožníme vám držet krok s hackery a skupinami hacktivistů. Inteligentní rozpoznání hrozeb a včasná detekce jsou klíčové pro zachování kontinuity fungování.

Komponenty služby

Evidence aktiv a hodnocení rizik

FreeDivision.io Risk

Tvorba a správa registru aktiv je klíčová pro pochopení hodnoty a fungování organizace. Řešení FreeDivision.io Risk umožňuje kategorizovat aktiva podle jejich kritičnosti, zavést metodiku hodnocení rizik a stanovit jejich priority. Součástí je také plán zvládání rizik, který zahrnuje návrhy opatření, mitigaci hrozeb a řízení zbytkového rizika, doplněné o grafické zobrazení aktiv a jejich vzájemných vztahů. Nástroj zároveň poskytuje funkce pro správu auditů a tvorbu auditních zpráv.

Skenování zranitelností

FreeDivision.io Vulnerability

Pravidelné skenování zranitelností vám pomůže identifikovat, které systémy jsou ohroženy. Samozřejmostí je míra relevance rizika. Na základě těchto ukazatelů stanovujeme priority při sjednání nápravy. V kombinaci s FD.io Advanced lze automatizovat zadávání požadavků na řešení těchto rizik pro provozní tým. Doporučujeme tyto skeny provádět na týdenní bázi a výsledky vizualizujeme v přehledných dashboardech.

Ochrana privilegovaných účtů

FreeDivision.io PAM

Naše zkušenost ukazuje, že více než 50 % závažných bezpečnostních incidentů přichází přes dodavatelské řetězce a zneužití administrátorských účtů. Z tohoto důvodu je klíčové zajistit jejich správu, audit a kontrolu využívání. Řešení umožňuje centralizovaný dohled nad privilegovanými identitami, zaznamenávání přístupů i detekci anomálního chování. Úroveň zabezpečení i detail monitoringu lze nastavit tak, aby byla zachována rovnováha mezi vysokou úrovní bezpečnosti a plynulým provozem IT prostředí.

Phishingové kampaně

FreeDivision.io Phishing

Poskytujeme také phishingové kampaně, a to jak jednorázové, tak kontinuální. Velkou výhodou je okamžitá zpětná vazba a přehled o selhání jednotlivých uživatelů. Pokud uživatel na phishingový e- mail reaguje (např. proklikem), je mu ihned vysvětleno, v čem byla chyba, a přímo na konkrétním příkladu je edukován, jak phishing rozpoznat. Tento přístup umožňuje rychlé zvyšování bezpečnostního povědomí uživatelů přímo v momentě porušení interních bezpečnostních pravidel.

Profesionální služby

FreeDivision.io Professional Services

Společnost poskytuje široké spektrum profesionálních služeb souvisejících s dodávanými bezpečnostními řešeními. Patří mezi ně servisní podpora v režimu SLA, projektové řízení, odborná školení a konzultace bezpečnostních inženýrů na úrovni L2 a L3. Součástí portfolia jsou také komplexní dohledové služby SOC zajišťující nepřetržitý monitoring bezpečnostních událostí. Zároveň pořádáme odborné workshopy a vystupujeme jako řečníci na významných bezpečnostních konferencích.

Lightspeed audit MS Active Directory

FreeDivision.io Active Directory

Pomocí přibližně 140 PowerShell skriptů provádíme automatizovaný sběr informací z prostředí Microsoft Active Directory. Jde o rychlý „lightweight“ audit zaměřený na odhalení nejčastějších bezpečnostních a konfiguračních problémů, jako jsou prázdné skupiny, rizika spojená s Golden Ticket útoky nebo nastavení a komplexita hesel. Výsledky jsou vizualizovány v nástroji FD.io Advanced v přehledných dashboardech. Audit doporučujeme provádět na týdenní bázi.

Klíčové přínosy

Maximální využití stávajících technologií zákazníka

Zajišťujeme plynulou integraci a efektivní využití existujícího IT a bezpečnostních technologií zákazníka (antivir, firewal, O365). Navazujeme na to, co již funguje, a zvyšujeme návratnost stávajících investic bez zbytečných technologických změn.

All-in-One SOAR

Používáme centralizovaný nástroj pro správu logů, bezpečnostní analytiku, korelaci událostí, alerting a kontinuální dohled. To vše propojujeme v jednom řešení řízeném odborníky SOC, které lze rozšiřovat o komponenty třetích stran (např. open-source) a další nativně podporované komponenty FreeDivision.io, jejichž nasazení a propojení je takřka okamžité.

Pokročilá detekce a inteligentní alerting

Naším cílem je rychle identifikovat skutečné hrozby a minimalizovat falešné poplachy. Toho dosahujeme prostřednictvím propojování bezpečnostních událostí do souvislostí s inteligentní prioritizací. Poskytujeme cenné know-how pro definici a nastavení funkčních alertů, vycházejících z našich zkušeností napříč všemi typy zákazníků (velikost, obor činnosti, compliance).

Rychlá a efektivní reakce na bezpečnostní incidenty

Máme předem definované postupy reakce, jasná pravidla eskalace a podporu SOC specialistů při řešení incidentů. Díky tomu lze rychle omezit dopady a co nejdříve obnovit běžný provoz. Klíčové je porozumět fungování uvnitř vaší organizace a společně navrhnout bezpečnost na míru.

Threat Hunting

Hrozby aktivně vyhledáváme i nad rámec běžné automatické detekce a postupy přizpůsobujeme úrovni zabezpečení i konkrétnímu prostředí zákazníka. Na analýze se podílí specialisté s různými certifikacemi od ethical hacker až po security analyst, kteří jsou součástí FreeDivision.io blue-team.

Reporting, compliance a připravenost na audit

Významnou součástí služby jsou provozní i manažerské reporty, které pomáhají plnit regulatorní a legislativní požadavky (compliance, audity, interní kontroly). Od začátku máte k dispozici FreeDivision.io reportní sadu, která odpovídá aktuálním požadavkům dle jednotlivých norem a zákonů a neustále dochází k její aktualizaci ve vztahu platné legislativy. Tyto aktualizace jsou nedílnou součástí samotné služby.

Projektová realizace a kompletní dokumentace

Projekt řídíme systematicky, s transparentními procesy a kompletní dokumentací SOC služeb. Díky tomu máte přehled, kontrolu a řešení, které je dlouhodobě udržitelné. Každý projekt má svůj dedikovaný implementační tým s jasně určenými odpovědnými osobami. Po dokončení projektu obdrží klient dokumentaci skutečného provedení a projekt se předává SOC týmu pro zajištění dohledu. Klient tak neplatí za SOC služby během fáze implementace.

Rychlé nasazení a kontinuální zlepšování

Služba přináší rychlé výsledky a pravidelné konzultace pomáhají sledovat trendy, modernizovat řešení a postupně zvyšovat úroveň zabezpečení.

Licencování

Náš licenční model FreeDivision.io Advanced je založený na počtu připojených zdrojů, kde je možné využít vysokou míru agregace. Například koncová zařízení uživatelů sbíráme agregací až 1:50. Tedy odpadá problém s EPS či licencováním na datový prostor. Celý tento model je pro zákazníky transparentní s jasným výhledem do budoucna.

Rozvoj, trendy, modernizace

Formou pravidelných konzultací klienta dlouhodobě provázíme rozvojem bezpečnostní platformy a implementací nejnovějších trendů.

FREEDIVISION

Proces nasazení a provozu

Nasazení služby probíhá v několika fázích:

- Analýza prostředí a architektury
- Detailní seznámení s IT prostředím zákazníka a návrh cílové architektury řešení.
- Integrace systémových komponent a logovacích zdrojů
- Napojení relevantních systémů, aplikací a zdrojů dat včetně automatizačních nástrojů.
- Konfigurace korelačních pravidel a playbooků
- Nastavení bezpečnostních scénářů, automatizovaných reakcí a detekčních mechanismů.
- Školení bezpečnostního týmu zákazníka
- Předání znalostí, vysvětlení procesů a práce s výstupy služby.
- Zahájení provozu a průběžné vyhodnocování efektivity
- Spuštění služby do ostrého provozu, pravidelné vyhodnocování a optimalizace.

Doporučujeme využít možnost pilotního provozu (PoV) pro ověření funkčnosti a kvality služby FreeDivision.io.

Služby a SLA

Služba SOC zahrnuje:

- Nepřetržitou detekci a monitoring bezpečnostních událostí 24/7.
- Analytický tým dohledového centra, který je dostupný v prac. dny od 8:00 do 18:00 s možností rozšíření na 24/7.
- Eskalaci bezpečnostních incidentů podle závažnosti a dohodnutých postupů (L1, L2, L3).
- Pravidelný reporting a vyhodnocení KPI.
- Rozšíření o pokročilé analýzy Cyber Threat Intelligence a detailnější přehled o hrozbách.
- Podporu při auditech a compliance kontrolách (NIS2, ISO, DORA, TISSAX).
- Odborné konzultace a doporučení pro zlepšení celkového bezpečnostního stavu organizace.
- Možnost rozšíření služby o EDR, ochranu dat, správu koncových zařízení a další.

POSKYTOVANÉ SLUŽBY	DETAILNÍ POPIS	SCÉNÁŘE NASAZENÍ	DETAILNÍ POPIS
Monitoring a reakce na incidenty.	Průběžné sledování bezpečnostních událostí na koncových zařízeních, analýza hrozeb v reálném čase a rychlá identifikace potenciálních problémů.	Analýza prostředí a návrh architektury.	Podrobná analýza infrastruktury zákazníka za účelem návrhu bezpečnostní architektury přizpůsobené konkrétním potřebám.
Pravidelné bezpečnostní reporty a přehledy KPI.	Generování pravidelných zpráv o bezpečnostních operacích, obsahujících klíčové ukazatele výkonnosti (KPI) a doporučení pro optimalizaci.	Integrace logovacích zdrojů a systémových komponent.	Zapojení různých logovacích zařízení a integrace bezpečnostních systémů do jednotného prostředí.
Eskalace incidentů dle SLA.	Zajištění rychlého řešení bezpečnostních incidentů na základě dohodnutých servisních úrovní (SLA).	Konfigurace korelačních pravidel a automatizačních playbooků.	Nastavení specifických pravidel pro korelaci událostí a vytvoření automatizovaných scénářů pro řešení incidentů.
Možnost rozšíření služby o MDR, MDDR a METLM.	Rozšíření základní služby o další pokročilé nástroje pro detekci a reakci na hrozby, které zvyšují bezpečnostní kapacity zákazníka.	Školení bezpečnostního týmu zákazníka.	Poskytnutí školení a praktických návodů pro zlepšení odborných znalostí bezpečnostního týmu zákazníka.
Podpora při auditech a compliance kontrolách.	Asistence při přípravě na audity a zajištění souladu s legislativními požadavky, jako jsou NIS2, DORA a ISO 27001.	Zahájení provozu a pravidelné vyhodnocování efektivity.	Plné spuštění služby s pravidelným hodnocením její účinnosti a úpravami dle aktuálních potřeb.
Konzultace a doporučení.	Poskytování odborných konzultací a návrhů pro zlepšení bezpečnostních procesů a postupů.	Pilotní provoz (PoV) pro ověření funkčnosti v reálném prostředí.	Možnost testovacích služeb v reálném prostředí zákazníka před jejich plným nasazením.

Dostupnost služby a reakční časy

Naše služba SOC je navržena pro zajištění nepřetržitého sběru dat, jejich kategorizace a vyhodnocování předem definovaných hrozeb, nad nimiž jsou prováděny automatizované reakce.

Dohledové služby:

- Režim 24/7
  Nepřetržitá detekce a automatizované reakce prostřednictvím SOAR playbooků umožňují okamžité rotiakce na bezpečnostní události, jako je blokace uživatelských účtů, omezení síťové komunikace nebo izolace zařízení. Tento přístup zajišťuje vysokou úroveň ochrany i mimo pracovní dobu bez nutnosti nákladného provozu SOC 24/7.
- Režim 10/5 (pondělí–pátek, 8:00–18:00)
  Aktivní dohled nad bezpečnostními událostmi a přímá reakce zkušeným týmem analytiků SOC.

Komunikační kanály:

- Primární komunikace probíhá prostřednictvím dedikovaného portálu pro správu incidentů a e-mailu. V případě kritických incidentů je zajištěn telefonický kontakt.

Service Level Agreement (SLA)

Definujeme klíčové parametry kvality a dostupnosti služby:

METRIKA	POPIS	CÍLOVÁ HODNOTA (10/5)	CÍLOVÁ HODNOTA (MINO 10/5)
Dostupnost služby	Časové pokrytí, kdy je monitorovací systém plně funkční a sbírá data.	99,5 %	99,5 %
Doba prvotní reakce na kritický incident (P1)	Doba od detekce kritického incidentu do zahájení vyšetřování analytikem SOC.	Do 30 minut	Do 60 minut (eskalace SOAR)
Doba prvotní reakce na vysoký incident (P2)	Doba od detekce incidentu vysoké priority do zahájení vyšetřování analytikem SOC.	Do 60 minut	Automatické vyhodnocení SOAR
Doba prvotní reakce na střední incident (P3)	Doba od detekce incidentu střední priority do zahájení vyšetřování analytikem SOC.	Do 4 hodin	Automatické vyhodnocení SOAR
Měsíční reportování	Frekvence zasílání souhrnných reportů o bezpečnostních událostech a trendech.	Měsíčně	Měsíčně
Kontrola kvality	Frekvence hodnotících schůzek	Měsíčně	Měsíčně
Ukládání incidentů	Incidenty a logy se ukládají na straně poskytovatele. Poskytovatel nemá oprávnění přistupovat ke klientským datům.	Do 7 dnů	Do 7 dnů

Standardní harmonogram nasazení a provozu pro organizaci do 500 zaměstnanců.

Následující harmonogram představuje typický průběh nasazení a zahájení provozu služby SOC. Konkrétní kroky a časové osy budou upřesněny na základě detailní analýzy vašeho IT prostředí a dohodnutého rozsahu služby.

1 **Podpis smlouvy** (1 týden)

2 **Fáze 1 – analytická** (3 týdny)

3 **Fáze 2 – implementační** (4 týdny)

4 **Fáze 3 – produkční** (2 týdny)

5 **Fáze 4 – monitorovací** (kontinuálně 24/7)

2 Analýza a plánování

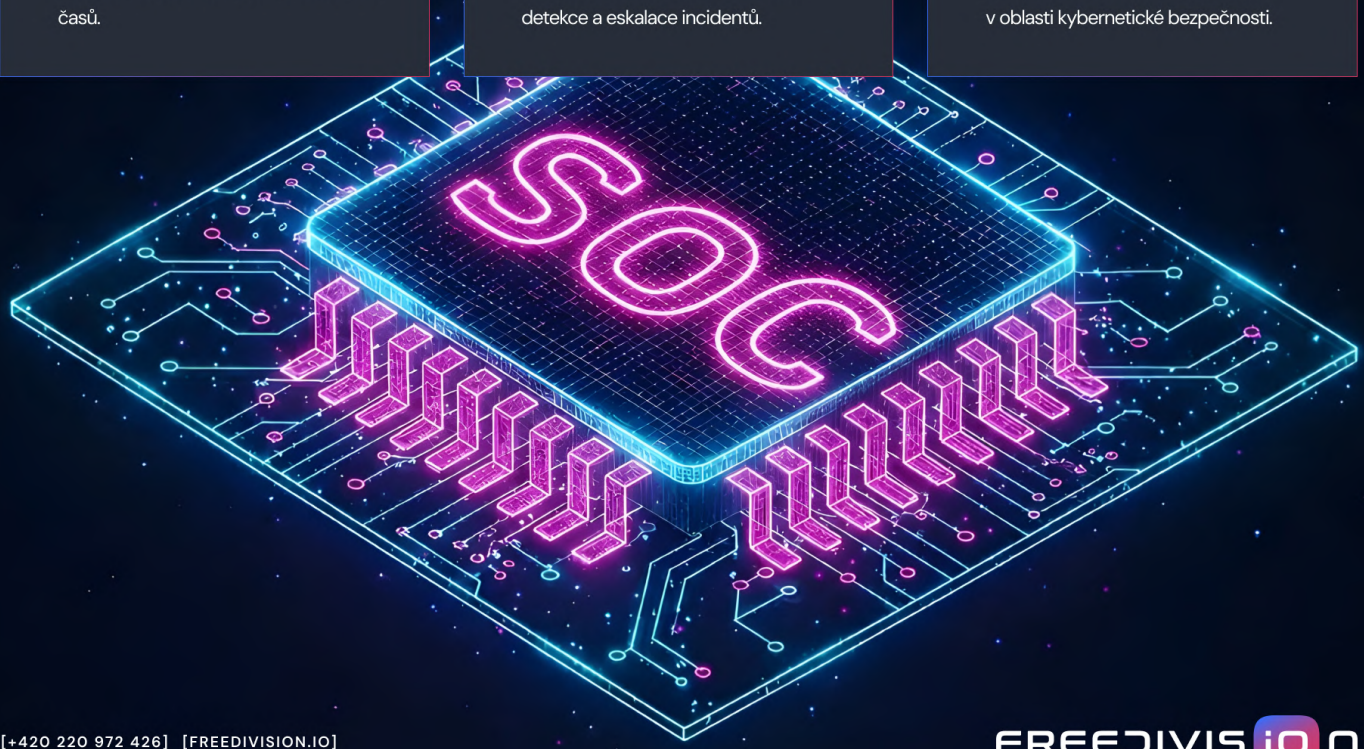
- Úvodní schůzka: Představení týmu, detailní diskuze o požadavcích a očekáváních zákazníka.
- Analýza infrastruktury: Provedení auditu a sběr informací o vašem IT prostředí, síťové topologii, klíčových systémech a datových tocích.
- Definice rozsahu: Specifikace monitorovaných systémů, zdrojů logů, dat ke sběru a nastavení priorit.
- Návrh architektury: Detailní návrh integrace a konfigurace jednotlivých SOC komponent (SIEM, EDR, CTI, UEM, Data Governance, PAM, Risk Management atd.).
- Návrh SLA: Upřesnění a odsouhlasení konkrétních parametrů SLA a reakčních časů.

3 Implementace

- Nasazení komponent: Instalace a konfigurace systémů SIEM, EDR, UEM, Data Governance a CTI.
- Integrace zdrojů: Napojení všech relevantních zdrojů logů do SIEM (firewally,
- servery, síťové prvky, aplikace atd.).
- Nastavení detekčních pravidel: Konfigurace a optimalizace detekčních pravidel, korelací a playbooků pro efektivní detekci hrozeb.
- Ladění nástrojů: konfigurace a ověřování pravidel pro automatické vyhodnocení a uzavírání alertů mimo pracovní dobu SOC.
- Testování: Důkladné testování funkčnosti celého systému, včetně sběru dat, detekce a eskalace incidentů.

4 Produkce

- Produkční provoz: Přechod na plný provoz služby SOC s nepřetržitým monitoringem.
- Proaktivní monitoring a reakce: Náš SOC tým s využitím prvků automatizace neustále monitoruje vaše prostředí, detekuje a řeší bezpečnostní incidenty.
- Pravidelné reportování: Měsíční reporty s přehledem bezpečnostních událostí, trendů a doporučení.
- Optimalizace a ladění: Kontinuální optimalizace detekčních pravidel, procesů a nástrojů automatizace pro zvýšení efektivity a snížení falešných poplachů.
- Školení a osvěta: Poskytování školení a doporučení pro vaše interní týmy v oblasti kybernetické bezpečnosti.



Náš SOC team

Náš tým Security Operations Center (SOC) je strukturován do několika úrovní, které zajišťují efektivní a komplexní ochranu bezpečnostního prostředí zákazníka. Jednotlivé úrovně mají specifické role a odpovědnosti, které dohromady vytvářejí robustní systém pro detekci, hlášení a řešení bezpečnostních incidentů.
Tento model umožňuje efektivní rozložení odpovědností a dovedností, což zajišťuje vysokou úroveň bezpečnosti a rychlé reakce na hrozby. Každá úroveň v SOC týmu hraje klíčovou roli v zajištění bezpečnostního stavu zákazníka a přispívá k dosažení společného cíle – ochrany dat a systémů před kybernetickými hrozbami.

SOC L1 – Junior analytik (Tier 1 / triage / monitoring)

Typické úkoly:

- Monitoring alertů v systému SIEM.
- Eskalace bezpečnostních incidentů na vyšší úrovně (L2/L3).
- Provádění prvotní analýzy a třídění incidentů.
- Komunikace s dalšími členy týmu na vyšších úrovních.
- Podpora produktů a služeb souvisejících s bezpečností.
- Reporting zákazníkům o aktuálních bezpečnostních aktivitách a incidentech.

SOC L2 – Incident Responder / analytik (Tier 2)

Typické úkoly:

- Pokročilá analýza bezpečnostních incidentů identifikovaných L1 analytiky.
- Incident response – implementace opatření k minimalizaci dopadů bezpečnostních incidentů.
- Proaktivní vyhledávání hrozeb provádí SOC L3, takže je potřeba přesunout toto dolů, do pozice SOC L3 - Senior analytik.
- Spolupráce na detailním forenzním šetření.
- Podpora při implementaci bezpečnostních opatření a procesů.

SOC L3 – Senior analytik / architekt / Threat Hunter (Tier 3)

Typické úkoly:

- Hluboká forenzní analýza komplexních bezpečnostních incidentů.
- Navrhování a implementace pokročilých bezpečnostních strategií a architektur.
- Mentoring a školení členů nižších úrovní (L1 a L2).
- Koordinace s externími partnery a technologickými dodavateli.
- Předkládání doporučení pro kontinuální zlepšování bezpečnostních procesů.

Reference a důvěra

Společnost FreeDivision disponuje certifikacemi ISO 27001 a ISO 9001 a je dlouhodobým, výhradním oceňovaným partnerem předních výrobců bezpečnostních řešení (Varonis, Absolute, Cyfirma, Logsign). Naše řešení jsou úspěšně nasazena napříč různými odvětvími – od zdravotnictví, finančního sektoru a energetiky až po veřejnou správu – což potvrzuje naši odbornost, stabilitu a schopnost dodávat bezpečnostní služby i v náročných a regulovaných prostředích.

ctp

Od: 2020
Počet zařízení: → 1.200
Řešení: Essential, Advanced, Data, CTI

„Společnost FreeDivision je pro nás klíčovým partnerem v oblasti bezpečnosti. Naše spolupráce začala v době, kdy jsme měli přibližně 300 zaměstnanců. Dnes díky ní zajišťujeme bezpečnost ve více zemích, pro stovky serverů a více než 1 200 koncových zařízení. Nejvíce si ceníme proaktivního SOC týmu, který aktivně vyhledává slabá místa a navrhuje odpovídající bezpečnostní opatření."

Michal Slejzák | Head of Infrastructure společnosti CTP Invest, spol. s.r.o.

ova.net

Od: 2011
Počet zařízení: → 4.000
Řešení: Advanced, Data

„S produktem Varonis jsem se poprvé setkal až po mém nástupu do funkce. Na základě víceleté zkušenosti shledávám, že se jedná o velmi jednoduchý a zároveň efektivní nástroj. K produktům využíváme podporu přímo od zastoupení výrobce a s potěšením mohu konstatovat, že zde působí profesionální tým, který disponuje detailními znalostmi nejenom ve vztahu k produktu Varonis, ale k celé problematice řízení přístupových práv a bezpečnosti."

Ing. Michal Hrotík | Člen představenstva společnosti OVANET, a.s. – poskytovatel služeb outsourcingu ICT městu Ostrava !!!

For Safety Reasons.
Be Best. Not First.

Jak stanovujeme cenu

Cena našich řešení je stanovována individuálně na základě skutečných potřeb zákazníka, které ověřujeme prostřednictvím Proof of Value (PoV). PoV probíhá po dobu 30 dní přímo v prostředí zákazníka a jeho cílem je prokázat reálný přínos navrženého řešení v praxi. Po celou dobu jsou zákazníkovi k dispozici seniorní technici FreeDivision, kteří formou workshopů provádějí implementaci, nastavují konkrétní scénáře využití a společně se zákazníkem vytvářejí „jízdní řád" dalšího rozvoje. Výstupem PoV je jasné vyhodnocení přínosů a doporučení optimálního řešení, které slouží jako podklad pro finální nabídku.

Shrnutí

Ve FreeDivision stavíme kybernetickou bezpečnost na odbornosti, kontinuálním vzdělávání a sledování nejnovějších bezpečnostních trendů, které přenášíme do praxe v České republice. Naše služby jsou navrženy tak, aby výrazně zvyšovaly schopnost organizací včas odhalit a účinně čelit kybernetickým hrozbám, aniž by bezpečnost omezovala běžný chod firmy. Naším cílem je zajištění kontinuity podnikání, ochrana klíčových dat a systémů a vytvoření takového bezpečnostního prostředí, které podporuje růst a stabilitu byznysu. Současně reflektujeme rostoucí regulatorní požadavky a klademe důraz na kvalitní reporting, auditovatelnost a dlouhodobou udržitelnost bezpečnostních procesů.

ADRESA

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

KONTAKT

assistant@freedivision.com
+420 220 972 426

www.freedivision.com