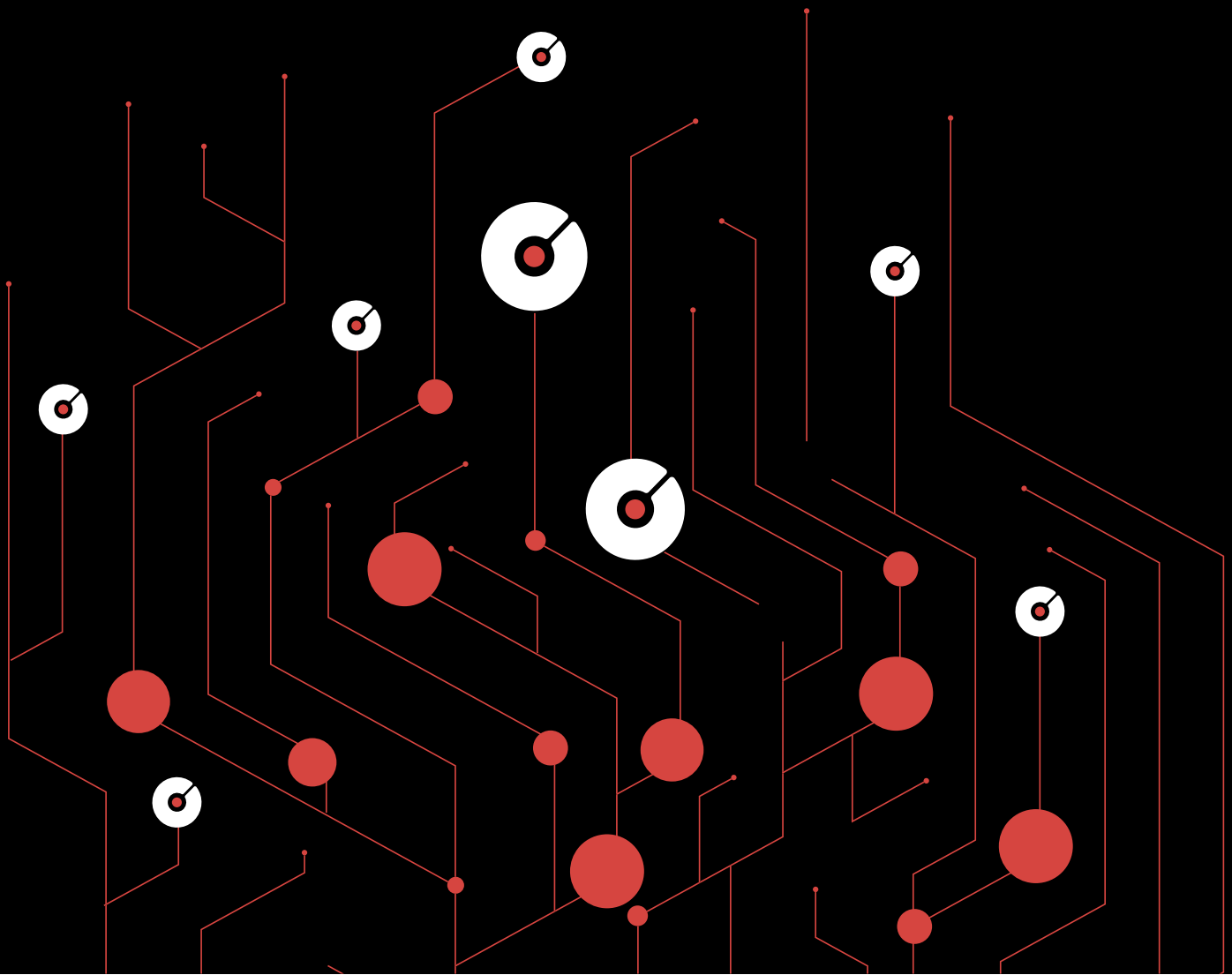
CYFIRMA
DECODING THREATS

FREEDIVISION

Přehled funkcionalit systému Cyfirma



1. Architektura a obecné vlastnosti

Systém

- šifruje veškerá data při přenosu (Transport Layer Security - TLS 1.2) i v klidu pomocí Advanced Encryption Standard (AES) 256bitového šifrování.
- nepřetržitě aktivně používá automatické geografické blokování a implementace WAF.
- nepřetržitě aktivně používá ochranu proti DDoS útokům.
- poskytuje rozsáhlé řízení přístupu k platformě s povinným přístupem nejmenších oprávnění, tzv. multitenant.
- nepřetržitě podléhá penetračnímu testování prováděnému přímo týmem bezpečnostních expertů výrobce.
- podléhá rutinním pravidelným i nepravidelným externím penetračním testům.
- nepřetržitě monitoruje vlastní prostředí dle zavedených zásad ochrany a brání tak před ztrátou dat u výrobce.
- vyžaduje účast analytiků kybernetického týmu výrobce na vzdělávacím programu kybernetické bezpečnosti každé čtvrtletí.
- automaticky blokuje účty v případě opakovaného neúspěšného pokusu o přihlášení.
- poskytuje rozsáhlé záznamy pro protokolování a auditování na všech uživatelských úrovních.
- poskytuje povinné vícefaktorové ověřování na všech úrovních.
- poskytuje komplexní program sledování hrozeb a automatické bezpečnostní skenování.

2. Funkce pro čerpání zpravodajských zdrojů

Systém

- umí nepřetržitě sledovat a zpracovávat informace z veřejně dostupných a ověřených zpravodajských zdrojů (OSINT).
- umí nepřetržitě sledovat a zpracovávat informace z fór dark webu a hackerských chatů.
- umí analyzovat veškerá data ze všech sociálních médií a obdobných platforem se schopností rozesílání zpráv (Discord, Telegram atd.).
- umí analyzovat veškerá data z těchto zdrojů:
  - Surface web,
  - Dark web,
  - Deep web,
  - formuláře pouze pro zvané,
  - podzemní tržiště,
  - peer to peer kanály,
  - zpravodajské komunity,
  - fóra za zavřenými dveřmi,
  - fóra pouze pro zvané,
  - stránky pro ukládání textů (Pastebin),
  - stránky sloužící jako datová skládka (Dump Site),
  - GitHub,
  - stránky pro sdílení kódu,
  - tržiště s kradenými záznamy.

- umožňuje sledování až 2200 kyberzločineckých skupin.
- umožňuje sledování až 2800 kyberzločineckých kampaní.
- je schopen porozumět až 31 jazykům u zdroje se související heuristickou analýzou:
  - Angličtina,
  - Arabština,
  - Čeština,
  - Čínština (zjednodušená),
  - Čínština (tradiční),
  - Dánština,
  - Estonština,
  - Finština,
  - Francouzština,
  - Hebrejština,
  - Hindština,
  - Indonéština,
  - Italština,
  - Japonština,
  - Korejština,
  - Maďarština,
  - Malajština,
  - Němčina,
  - Nizozemština,
  - Norština,
  - Perština (Farsí),
  - Polština,
  - Portugalština,
  - Rumunština,
  - Ruština,
  - Řečtina,
  - Španělština,
  - Švédština,
  - Thajština,
  - Turečtina,
  - Vietnamština.

3. Funkce pro situační povědomí

Systém

- monitoruje hrozby v reálném čase.
- průběžné monitoruje globální prostředí hrozeb a identifikovat vznikající hrozby, aktivní kampaně a potenciální indikátory kompromitace.
- sleduje a analyzuje významné globální a regionální geopolitické události, které by mohly ovlivnit prostředí kybernetických hrozeb, jako jsou mezinárodní spory, ekonomické sankce nebo politické volby.
- poskytuje informace o státem sponzorovaných nebo na stát napojených aktérech hrozeb, jejich motivacích, metodikách a potenciálních cílech, zejména v kontextu větších geopolitických událostí nebo napětí.
- mapuje geopolitické události s pozorovanými změnami v prostředí kybernetických hrozeb, s cílem pochopit, zda by se mohl subjekt stát cílem útoku vzhledem ke své geografické přítomnosti, odvětví nebo asociacím.
- poskytuje zpravodajské informace na míru na základě konkrétního odvětví.
- umožňuje zobrazit ucelený pohled na prostředí hrozeb, propojený s geopolitickými událostmi.

4. Funkce pro zjištění povrchu útoku (Attack Surface)

Systém

- je schopen identifikovat vystavená klientská aktiva jako je doména, subdoména, rozsah IP adres, verze softwaru/zranitelnosti atd.
- je schopen hlubšího pohledu na hrozby přítomné ve vlastním prostředí, které jsou zneužitelné z pohledu útočníka:
  - zranitelnost domény/IP,
  - slabá místa certifikátů,
  - nesprávné konfigurace,
  - otevřené porty,
  - pověst IP/domény,
  - slabost cloudu.
- poskytuje v této oblasti:
  - mapování digitální stopy,
  - skenování zranitelností,
  - analýzu vystavení sítě,
  - zjišťování stínových IT,
  - informace o rizicích třetích stran a dodavatelů,
  - detekci chybné konfigurace,
  - informace o stavu a chování zařízení internetu věcí (IoT),
  - kontrolu konfigurace cloudu,
  - upozornění a monitorování v reálném čase,
  - doporučení k nápravě,
  - interaktivní vizualizaci.
- má pro zpravodajství o kybernetických hrozbách rozhraní, které zajistí integraci s bezpečnostními produkty používanými pro detekci a reakci. Pomocí tohoto rozhraní budou moci detekční a zásahové funkce fungovat automaticky.

5. Funkce pro kybernetické zpravodajství

Systém

- poskytuje kontextuální, kurátorské a personalizované zpravodajství formou komplexního pochopení klíčových prvků a vztahů v rámci kybernetického útoku, konkrétně: kdo útočí, na jaká aktiva útočí, proč útočí, jak a kdy může k útoku dojít.
- je schopen rozpoznat chování aktérů hrozeb, včetně metodik útoků.
- poskytuje hodnocení zranitelností.
- poskytuje hodnocení aktivit na dark webu.
- umožňuje označit totožnost aktéra nebo aktérů hrozby, kteří stojí za hrozícím kybernetickým útokem, včetně pochopení toho, zda jsou útočníky jednotliví hackeři, organizované skupiny kyberzločinců, státem sponzorovaní aktéři, vnitřní aktéři nebo jiné subjekty.
- umí rozpoznat konkrétní cíl nebo více cílů kybernetického útoku, povinně alespoň tyto: krádež citlivých údajů, narušení provozu nebo služeb, finanční zisk, špionáž, sabotáž nebo jiné záškodnické aktivity.
- je schopen odhalit motivaci a záměry, které vedou ke kybernetickému útoku.
- umí odhalit metody, techniky a nástroje, které útočníci použili k provedení kybernetického útoku. Patří sem využití zranitelností, nasazení malwaru, taktiky sociálního inženýrství, phishingové útoky, útoky hrubou silou nebo jiné prostředky použité k průniku do cílových systémů nebo sítí a jejich kompromitaci.
- umí určit potenciální časový rámec kybernetického útoku.
- je schopen pochopit kdy může útok proběhnout, v jakém stavu se kampaň aktuálně nachází a jaký(-á) je její vývoj/trajektorie z důvodu zadržení či alespoň zmírnění následků.
- umí sladit zpravodajské informace s jedinečným kybernetickým profilem organizace.
- je schopen použít pokročilé algoritmy strojového učení k odhalování vzorců a souvislostí mezi diskrétními soubory dat, které by jinak mohly zůstat nepovšimnuty.
- umí nepřetržitě aktivně vyhledávat v dark webu s kontextem k dané organizaci a aktivně informovat o vznikající hrozbě formou vizualizace a automatické notifikace.
- je schopen aktivně vyhledávat informace o aktérech hrozeb ve všech zdrojích, jejich korelace v rámci databáze a vše vizualizovat.
- umí vizualizovat ucelené informace o metodách útoku - kdy, jak a s jakými prostředky útočník útočil.
- je schopen zobrazit související rizika ve formě detailního popisu skutečností o tom, kde bylo riziko nalezeno, kdo a co je zdrojem rizika, kdo riziko zneužívá (jedinec nebo skupina) včetně doporučení jak se před rizikem chránit.
- poskytuje zpravodajské modelování k odhalení závažnosti jednotlivých rizik.

10. Funkce pro včasné varování

Systém

- poskytuje možnost včasného upozornění na vznikající potenciální kybernetické hrozby.
- v rámci vytváření včasného upozornění pracuje s indikátory hrozeb jako jsou technické údaje nebo vzorce chování, které jsou spojeny se škodlivými aktivitami. Příkladem jsou signály chatu, výměna dat, identifikace a pozorování škodlivých IP adres, adres URL, hashů souborů a další.
- v rámci vytváření včasného upozornění pracuje s identifikací útočníků a umí rozpoznat, zda se jedná o jednotlivce nebo skupinu, případně více skupin.
- v rámci identifikace aktéra umí rozpoznat taktiky, techniky a postupy (TTP) útočníků, jejich motivaci a veškeré minulé aktivity, na kterých se podíleli.
- je schopen posoudit potenciální dopad případného úspěšného útoku, tedy co by se mohlo stát, kdyby se hrozba naplnila. To zahrnuje narušení dat, finanční ztráty, poškození pověsti fyzických a právnických osob, nucené zastavení činnosti apod.
- umí nabídnout doporučení ve formě konkrétních kroků, které má organizace (příp. fyzická osoba) podniknout ke zmírnění potenciální hrozby. Může se jednat o záplatování určitého softwaru, revizi bezpečnostních zásad, školení zaměstnanců apod.
- je schopen pracovat se souvislostmi jednotlivých informací a zobrazit je v reálném čase. Například pokud byl konkrétní aktér hrozby pozorován při útocích na jinou organizaci ve stejném odvětví, musí tyto informace poskytnout.
- poskytuje podrobnosti o konkrétních zranitelnostech (softwarových, hardwarových i procedurálních), které by mohl útočník zneužít.
  umožňuje vygenerovat včasné upozornění na vznikající potenciální kybernetické hrozby v podobě zprávy ve formátu pdf.
- v rámci vygenerování „Zprávy o potenciálních kybernetických hrozbách“ poskytuje ověření zprávy analytickým týmem výrobce.
- v rámci vygenerované „Zprávy o včasném varování“ poskytuje informace o všech aktérech a indikátorech hrozeb, o jejich potenciálních dopadech a také doporučení vedoucí k jejich zmírnění nebo zamezení, přičemž aktéry rozumíme jak útočníky (příp. skupiny útočníků) tak i potenciální oběti - právnické a fyzické osoby i jiná aktiva.

11. Funkce pro eliminaci škodlivých a podvržených aktiv

Systém

- V rámci služeb výrobce poskytuje podklady pro službu eliminace škodlivých či podvržených:
  - domén,
  - subdomén,
  - emailových účtů,
  - telefonních čísel,
  - sociálních účtů,
  - obchodních a produktových značek,
  - aplikací.

- v rámci procesu eliminace poskytuje službu, kdy výrobce zasílá oznámení (včetně důkazů) upozorňující provozovatele na to, že jím provozovaná služba slouží k podvržení nebo poškození aktiv vyjmenovaných v předchozím bodu.
- v rámci procesu eliminace poskytuje službu, kdy výrobce zasílá porušovateli práv výzvu k zastavení protiprávního jednání, pokud je porušovatel známý a jednoznačně identifikovatelný.
- v rámci procesu eliminace poskytuje službu, kdy výrobce informuje klienta (poškozeného) o všech krocích a nových skutečnostech, které v té věci podnikl či nastaly v průběhu procesu řešení písemnou formou přímo v rozhraní systému buď v podobě archivovatelné notifikace nebo v podobě dokumentu ke stažení - MS Word, Excel nebo PDF.

12. Funkce pro integrace s jinými bezpečnostními ovládacími prvky

Systém

- podporuje rozhraní API kompatibilní se standardy STIX a TAXII a integraci výstupů systému do jiných bezpečnostních ovládacích prvků:
  - bezpečnostní brány,
  - bezpečnostní analytické nástroje typu SIEM/SOAR,
  - nástroje pro pokročilé a automatizované řízení IT služeb.

FREEDIVISION

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

www.freedivision.com
assistant@freedivision.com
+420 220 972 426