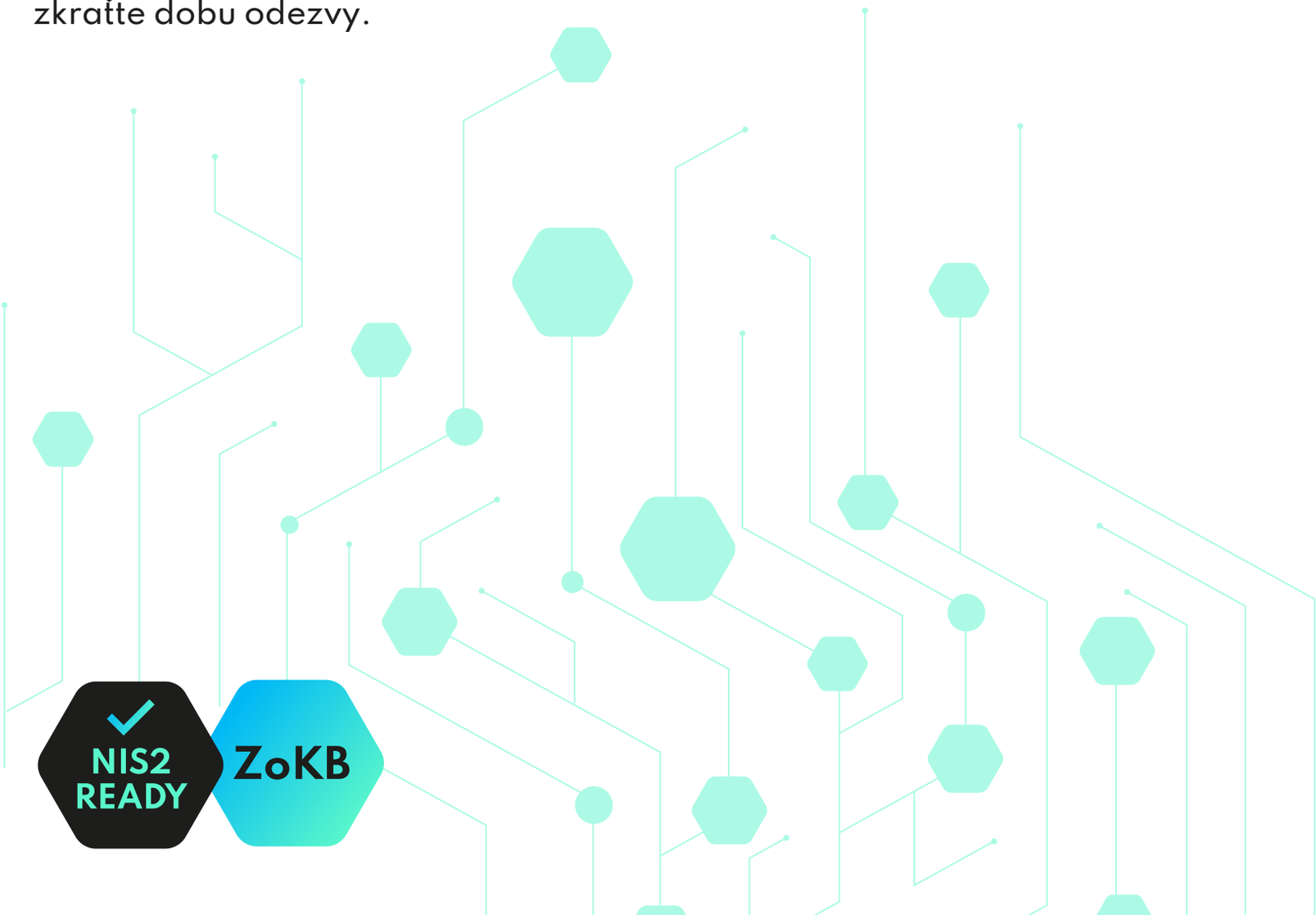
Logsign

FREEDIVISION

Orchestrace zabezpečení, automatizace a reakce na incidenty (SOAR)

Zjednodušte své bezpečnostní operace na centralizované a komplexní platformě.

Automatizujte pracovní postupy, organizujte nástroje a lidi, zkraťte dobu odezvy.



NIS2 READY

ZoKB

Platforma Logsign pro orchestraci zabezpečení, automatizaci a reakci na incidenty

Automatizace zabezpečení má zásadní význam pro vytvoření agilního a efektivního bezpečnostního prostředí. Jakmile budou opakující se a časově náročné úkoly automatizovány, analytici nebudou vyčerpaní a budou mít čas zaměřit se na incidenty, které jsou kritické a vyžadují rozhodovací proces. Automatizace a větší využití analytiků na kritických úkolech tak výrazně zlepší schopnost organizace reagovat na incidenty. Lepší a rychlejší vyšetřování a zkrácení doby detekce a reakce jsou reálné pouze s dobře navrženým, široce založeným systémem SOAR.

Automatizace

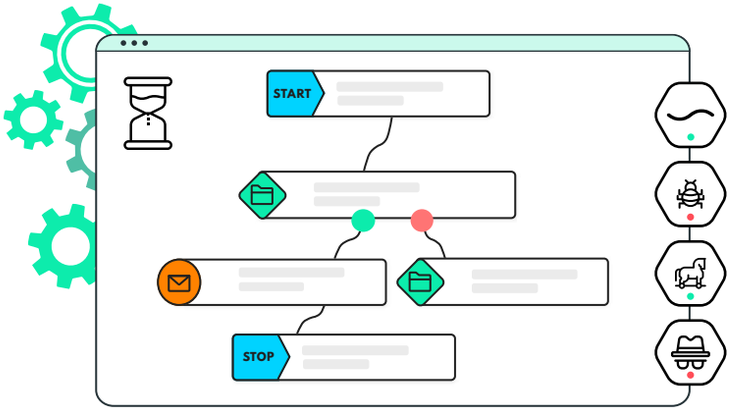
Automatizace zabezpečení se týká automatizovaných procesů v oblasti prevence, detekce, vyšetřování, třídění a reakce bez zásahu člověka. Pracovní postupy můžete snadno automatizovat pomocí botů a playbooků určených pro integrace bezpečnostních i nezabezpečených zařízení v síti. Tyto automatizace zkracují střední dobu detekce a reakce, čímž zlepšují kapacitu organizace určenou pro řešení incidentů (IR – Incident Response).

Reakce na incidenty

Bezpečnostní týmy tráví většinu dne vyšetřováním událostí a reakcemi na ně. To neumožňuje standardizovat procesy reakce na incidenty nebo zvýšit kvalitu reakce na incidenty. Logsign SOAR je dodáván s kompletními příručkami pro reakci na incidenty během celého životního cyklu, které vycházejí z metodik SANS pro řešení incidentů.Takto nastavený proces řešení incidentů umožňuje řídit životní cyklus bezpečnostních incidentů od analýzy po jejich potlačení, odstranění a obnovu.

Orchestrace

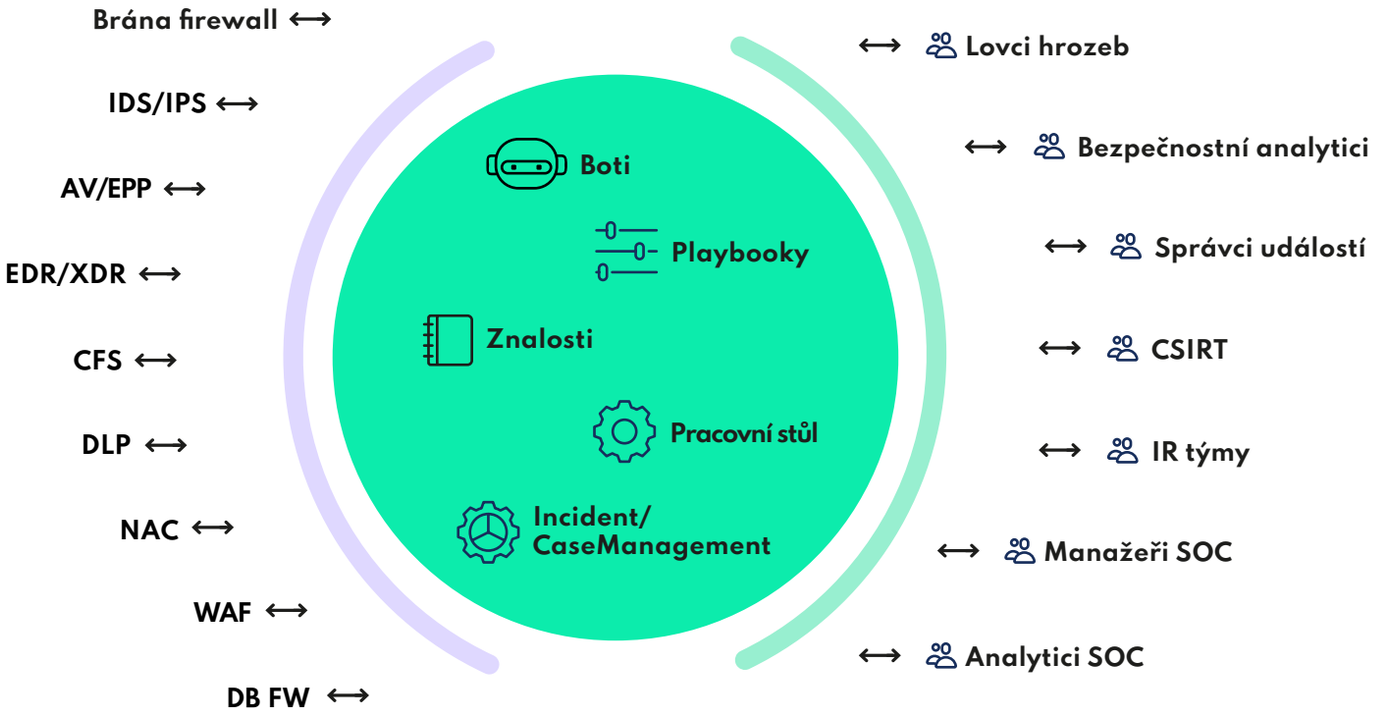
Bezpečnostní orchestrace je metoda propojení všech nástrojů, týmů a procesů, ať už jsou zaměřeny na bezpečnost, nebo ne, pro efektivní a silnou kybernetickou bezpečnost tak, aby byly zajištěny potřebné operace a bezchybný zásah při kybernetických incidentech. Bezpečnostní orchestrace je harmonická práce lidí, procesů a technologií.



Logsign

Jak to funguje?

Logsign SOAR je 100% technologicky nezávislý, bezproblémově integruje všechny vaše bezpečnostní technologie a jednoduše začne dělat svou práci, tj. orchestrovat. Kromě stovek předdefinovaných integrací umožňuje díky přístupu API-first rychlé nasazení Logsign SOAR bez jakýchkoli starostí s dodavateli jednotlivých bezpečnostních prvků. Díky využití předdefinovaných botů a playbooků můžete snadno automatizovat své pracovní postupy. SOAR automaticky vyšetřuje, detekuje a třídí incidenty, takže bezpečnostní analytici mohou začít pracovat na přidělených úkolech, cílech nebo spolupracovat na případech, kde je zapotřebí jejich know-how. Správa bezpečnostních událostí zlepšuje procesy reakce, pracovní prostředí zaměřuje analytiky na správný úkol ve správný čas a know-how je dokumentováno a předáváno nováčkům. V důsledku toho se zlepšuje (IR – Incident Response) kapacita organizace určená pro řešení incidentů.



Proč Logsign SOAR?

Správa událostí

Posiluje přínos a spolupráci analytiků

Každý analytik může přispět k řešení případu tak, že vlastník a přispěvatelé spolu snadno komunikují, aby mohli událost vyřešit, odpovědět na ni nebo ji dále eskalovat.

Boti a playbooky

Multiplikační efekt síly

Boty jsme vytvořili, abychom zvýšili výkon analytiků. Zařaďte boty Logsign do svého týmu. Nechte je spouštět playbooky a pracovat současně s analytiky.

Pracovní plocha

Navrženo pro správný cíl

Logsign SOAR vítá vždy analytiky personalizovaným dashboardem, který je nasměruje ke správnému CÍLI ve správný čas.

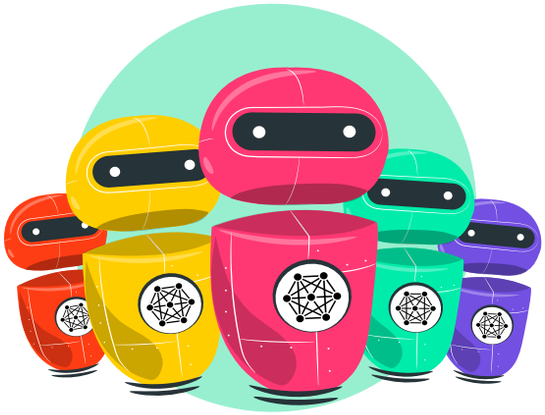
Zvýrazněné funkce

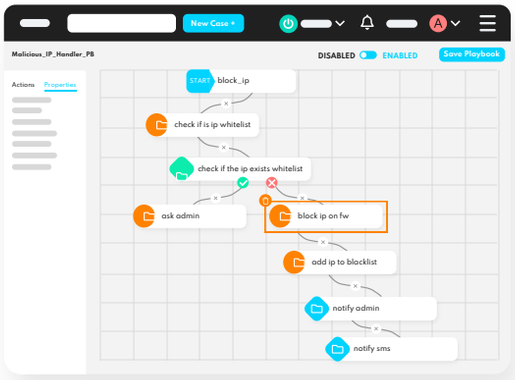
Humanoidní roboti

Přidání humanoidních botů Logsign do týmu

Základní produkty SOAR jsou zaměřeny pouze na playbook a pracovní postupy. Vyžadují konfiguraci sešitu úloh pokaždé, když dojde k změnám. To je nesmírně těžké a složité pro udržení kontinuity práce a zpracování bezpečnostní strategie vaší organizace. Boti Logsign jsou navrženi tak, aby tento proces moderním způsobem změnili a zjednodušili. Boti zapojují a spouštějí playbooky, odesílají akce a změny tak, aby konfigurace playbooků probíhaly současně, fungovaly a vše běželo nepřetržitě.

Jejich pokročilé funkce posilují výkonnost bezpečnostních analytiků. K dispozici je mnoho vestavěných botů a je snadné vytvářet nové pro nové akce nebo pracovní postupy. Interagují s analytiky, jinými boty nebo playbooky v nich a všechny automatizované akce fungují dál.





Vizuální příručky

Snadná automatizace pracovních postupů

Existuje mnoho předdefinovaných playbooků. Kromě toho Logsign umožňuje uživatelům vytvářet libovolné playbooky **bez kódu**. Takto lze jednoduše přizpůsobit nebo vytvořit nové playbooky pomocí jednoduchého přetahování drag-and-drop, **vizuálního editoru** nebo s podporou **DSL**.

Více než 300 vestavěných playbooků
Připraveno k automatizaci podle modelu reakce na incidenty SANS PICERL.

Simulační nástroj
Zajišťuje, že playbooky běží a simuluje jejich pracovní postup.

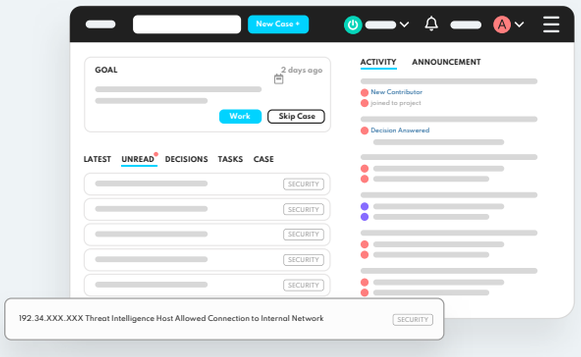
Snadná konfigurace
Playbooky jsou připraveny ke změnám v konfiguraci podle změn v řešení daného vendora nebo akce.

Osobní pracovní plocha

Navrženo pro správný CÍL

Logsign Workbench vítá bezpečnostní analytiky s cíli a úkoly, na které by se měli zaměřit. Obsahuje kritické události, prioritní události nebo úkoly, které potřebují jejich zapojení, stejně jako žádosti a nepřečtené zprávy.

Je navržen moderně, s cílem **zajištění vysoké efektivity práce analytiků** při zachování principů agility a spolupráce.



Logsign

Správa incidentů a událostí

Komunikace a spolupráce vždy vítězí

Funkce správy událostí Logsign umožňují rychlou spolupráci a reakci na incidenty s cílem zabezpečit prostředí tím, že bezpečnostní analytici jsou společně na stejné vlně. Automatizované nebo manuální vyšetřování, detekce a reakce na jediné obrazovce zkracují křivku učení analytiků a dobu reakce.

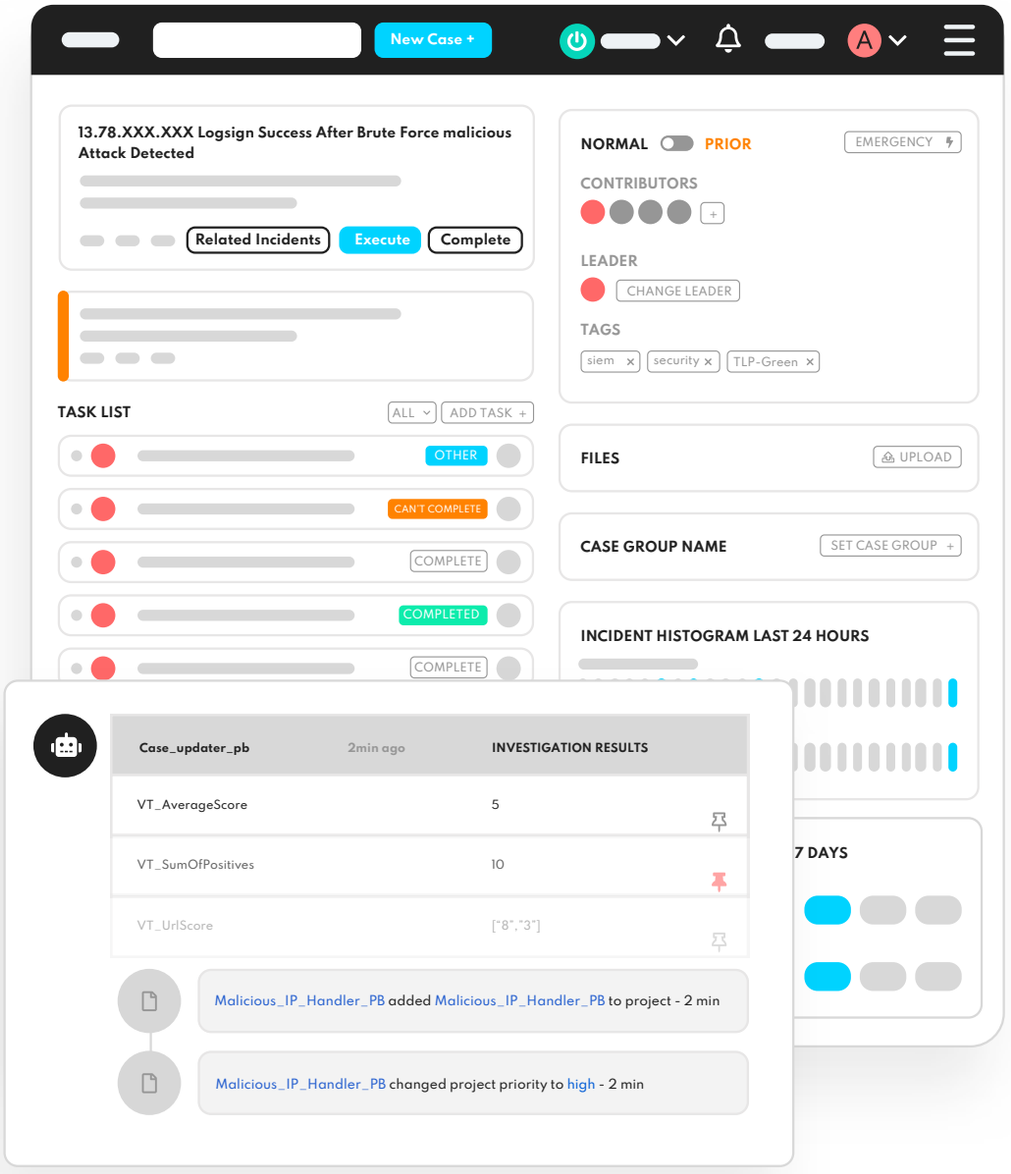
Vyšetřování a stanovení priorit
Ruční nebo automatizované vyšetřování a třídění je k dispozici.
Analytici jsou seznámeni s prioritními událostmi a úkoly, aby se nejprve zaměřili na ty vysoce kritické.

Vytváření událostí a úkolů
Vytváří události automaticky nebo umožňuje ruční vytváření událostí a úkolů.

Zadání události
Ruční nebo automatizované vytváření událostí a úkolů je snadné i díky přiřazení správné osoby. Vlastník může provádět úpravy a vytvářet SLA pro události.

Seskupení událostí
Související upozornění a události lze seskupit do jednoho případu a reagovat tak rychleji.

Reakce na jedno kliknutí
Umožňuje analytikům ručně odpovídat na stránce události.



Spolupráce a sdílení informací
Přístup společnosti Logsign ke správě událostí usnadňuje komunikaci mezi analytiky s cílem řešit události a rychleji reagovat. Vašemu týmu umožňuje rychlé učení.

Stovky integrací

Neváhejte spolupracovat s dodavatelem libovolného IT řešení.

Využijte stovky připravených integrací, bezplatnou integrační službu a široké možnosti založení nových integrací bez ohledu na vendorovi. Logsign SOAR využívá přístup založený na API, který automatizuje a obousměrně orchestruje bezpečnostní a provozní IT nástroje. Snadno se integruje i s nástroji, které nemají rozhraní API.

Zpravodajství o hrozbách

ANOMALI · ALIENVAULT · VIRUSTOTAL · COFENSE · CYMON.IO · DOMAINTOOLS · FARSIGHT SECURITY · OpenPhish · Recorded Future · paloalto

SIEM

exabeam · DEVO · elastic · LogRhythm · MICRO FOCUS · JASK · Radar · McAfee · FORTINET · sumo logic · splunk> · McAfee

Zprávy

Exchange · PagerDuty · slack · twilio · zoom

Zabezpečení sítě

Check Point · paloalto · f5 · PROTECTWISE · Signal Sciences · zscaler

Koncový bod

Carbon Black. · CROWDSTRIKE · CounterTack · SentinelOne · cybereason · CYLANCE · Symantec · TANIUM · CORTEX

Analýza malwaru

CISCO · CUCKOO · FIREEYE · INTEZER · JoeSecurity · paloalto · lastline

Ticketovací nástroje

cherwell · easyVISTA · freshdesk · Jira Software · salesforce · zendesk

Bezplatná služba integrace
Bezplatná integrace pro bezpečnostní i jiné nástroje.

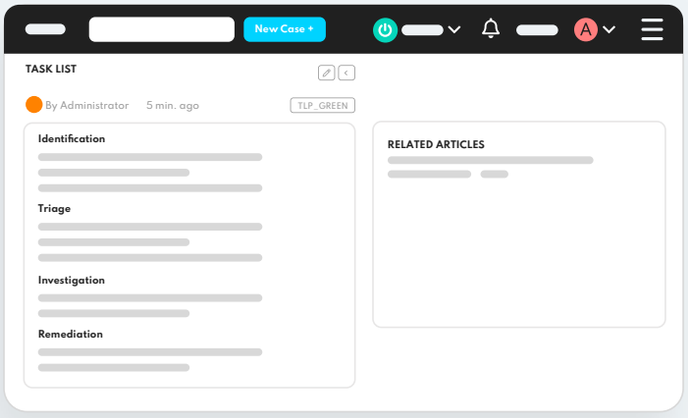
Široká škála integrací
Nekonečný příběh. Počet a rozmanitost integrací se každým dnem zvyšuje.

Vendor-Agnostic
Možnost obousměrné integrace bez zapojení vendora.

Databáze znalostí

Ve znalostech je síla

Databáze znalostí je druh knihovny. Je to vaše organizační kybernetické know-how, které umožňuje bezpečnostním analytikům snadno získávat znalosti nebo sdílet své informace a zkušenosti. Tato znalostní základna také posiluje orientaci nováčků.



Logsign

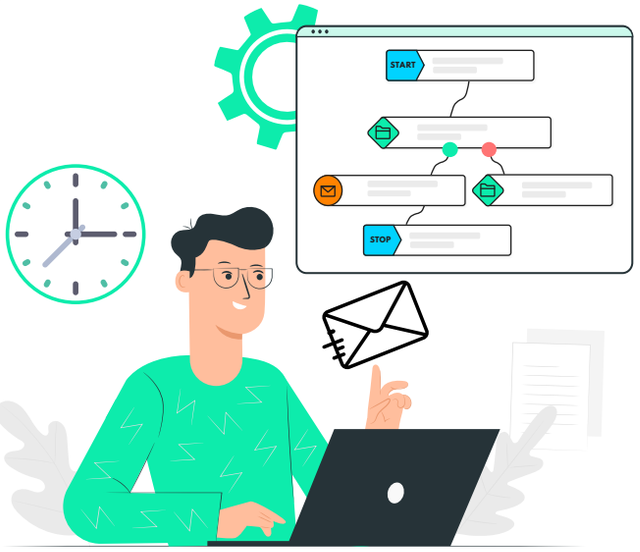
Oblasti řešení

Podnikové týmy pro bezpečnostní operace vybavujeme inteligentními nástroji SOAR a SIEM, které zvyšují efektivitu práce a umožňují lepší a rychlejší vyšetřování a reakce. Kromě nejnovějších technologických produktů poskytujeme také řadu služeb, které uživatelům pomáhají s řízením operací kybernetické bezpečnosti a přinášejí jim přidanou hodnotu. Řešení problémů při nasazení a používání, zlepšení kapacity reakce, vyšetřování a analýzy, třídění incidentů nebo vytváření nových playbooků a botů, to vše je nezbytné pro efektivní používání platforem. Náš kompetentní a vyškolený tým podpory je vám k dispozici 24 hodin denně, 7 dní v týdnu a kdykoli vám poskytne podporu.

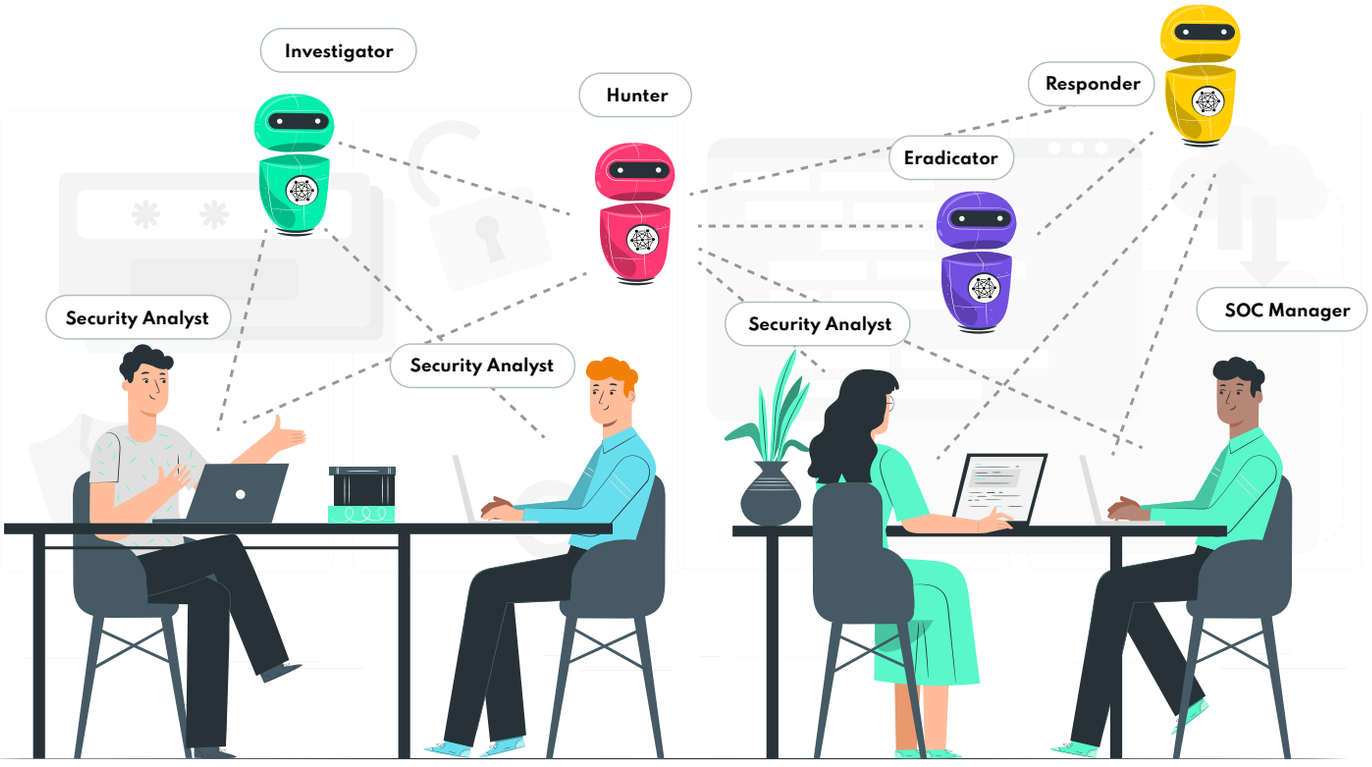
Zjednodušujeme vaše bezpečnostní operace na centralizované, komplexní platformě.

Logsign SOAR zefektivňuje vaše SecOps díky svým pokročilým funkcím. Automatizace nejen opakujících se úloh, ale všech pracovních postupů, které lze automatizovat, sníží pracovní zátěž analytiků v oblasti bezpečnosti. Vyšetřování, vyhledávání hrozeb, třídění upozornění nebo řešení incidentů lze automatizovat s dobře navrženým systémem SOAR. Kromě toho automatizace také zajišťuje, že mezi ostatními nástroji není žádná mezera.

Orchestrace zlepšuje přínos analytiků a jejich spolupráci, takže se zkracuje doba odezvy a přijímají se proaktivní opatření. Komplexní schopnost řešení incidentů je dosažena pomocí Logsign SOAR, takže SecOps jsou zefektivněny. Organizace posiluje svou pozici v oblasti kybernetické bezpečnosti.



- Plně a částečně automatizované pracovní postupy s využitím botů a playbooků.
- Zlepšení komunikace a přínosu analytiků.
- Komplexní řešení incidentů a událostí.
- Automatizace správy úkolů.
- Efektivní práce s personalizovanou pracovní plochou.



Zvyšujeme vyspělost bezpečnostního balíčku IT

Každý nástroj nebo software přidaný do zásobníku kybernetické bezpečnosti nebo IT může způsobit velkou zranitelnost organizace nebo zavádějící operace, pokud nejsou automatizovány nebo integrovány s jinými nástroji. Jen těžko dosáhnete efektivně cíle při práci s nástroji od více různých vendorů, jejichž bezpečnostní aplikace musíte umístit na vyšší počet vzdálených lokalit, pokud nezvolíte jednoduché centralizované řešení pro celou organizaci.

Vzorce útoků se mění, přicházejí nové technologie a digitalizace a modernizace organizací se vyvíjí každým dnem. SOAR tento problém řeší.

- Organizace a ovládání aktivních i pasivních bezpečnostních nástrojů.
- Automatizace prosazování zásad napříč různými řešeními.
- Flexibilní schopnost integrace řešení nezávislých na vendorech.
- Zlepšení vymahatelnosti bezpečnostních politik a protokolů.
- Hierarchická struktura uživatelů pro více lokalit nebo podniky s více organizacemi.

Zvyšujeme efektivitu týmu a řešíme problémy s nedostatkem IT personálu

V oboru kybernetické bezpečnosti je vždy těžké najít, vyškolit nebo zorientovat příslušné pracovníky a nováčky v organizaci. Řešením je snížení pracovní zátěže a fluktuace bezpečnostních analytiků. Zvýšení efektivity analytiků lze dosáhnout tím, že přestanou trávit čas manuálními, jednoduchými nebo opakujícími se úkoly a zaměří se na události, které mají zásadní význam pro rozhodnutí. Cítí se tak mnohem profesionálněji, aniž by byli zahlceni a mohli se soustředit na správné cíle a úkoly. SOAR zvyšuje týmovou spolupráci, což analytikům umožňuje reagovat na události a zkracuje dobu odezvy.

- Personalizovaná pracovní plocha zvyšuje efektivitu práce analytiků.
- Boti posilují ruce analytiků při řešení událostí, pracují vedle nich a pro ně.
- Interaktivní komunikace zlepšuje výsledky.
- Se znalostní databází již není orientace problémem.
- Menší fluktuace, méně problémů a nákladů v oblasti lidských zdrojů je příjemný benefit.

Produkty

SIEM | SOAR

Zpravodajství o hrozbách

Služby s přidanou hodnotou

SOC | Spoluřízený SIEM

Podpora & Onboarding

Seznamte se s Logsign SIEM

Kdo jsme

Dodáváme řešení kybernetické bezpečnosti založené na automatizaci a snažíme se poskytovat nejchytřejší, nejsnáze použitelné a cenově dostupné řešení detekce a reakce v rámci kybernetické bezpečnosti a služby s přidanou hodnotou.

Společnost Logsign byla založena v roce 2010 s cílem umožnit pracovníkům v oblasti kybernetické bezpečnosti pracovat efektivněji pomocí inteligentního softwaru nové generace, který neobsahuje žádné překážky. Zabezpečení IT systémů a řízení operací v oblasti kybernetické bezpečnosti by neměly být tak složité, časově náročné a předražené. Proto jsme vyvinuli náš inteligentní a snadno použitelný software SIEM a SOAR s ohledem na současné i budoucí potřeby trhu. Automatizace zahajuje novou éru kybernetické bezpečnosti. Jsme přesvědčeni, že v této době automatizace zvládne až 98 % manuální práce lidí. Efektivita operací v oblasti kybernetické bezpečnosti tak již není snem. Software platformy SOAR je v srdci operací povyšujících práci bezpečnostních týmů na inteligentní, efektivní a spolupracující prostředí. Nemůžete chránit, dokud nevidíte a nedetekujete. Shromažďování jakýchkoli dat, jejich vizualizace a přeměna na využitelné informace jsou možné prostřednictvím našeho nekonečně škálovatelného a clusterového systému SIEM. Společnost Logsign s více než 10 lety zkušeností je upřímným týmovým hráčem, kterému důvěřuje více než 500 podniků, ministerstev a státních úřadů.

www.freedivision.com

FREEDIVISION
for safety reasons

Info Security Products Guide 2020 GLOBAL EXCELLENCE BRONZE ★★★★★

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2019

Info Security Products Guide 2019 GLOBAL EXCELLENCE SILVER ★★★★★

Info Security Products Guide 2019 GLOBAL EXCELLENCE GOLD ★★★★★

CYBER DEFENSE GLOBAL AWARDS CYBER DEFENSE MAGAZINE 2018 WINNER

Nepřetržitá správa bezpečnostních incidentů

Služba zabezpečení uživatelského prostředí formou orchestrace bezpečnostních nástrojů s možnostmi hlubší detekce a podrobnější analýzy vnitřního i vnějšího prostředí organizace je obvykle označována zkratkou SOAR - Security Orchestration, Automation and Response.

Jak na to jdeme?

Služby orchestrátoru FreeDivision IO tvoří automatizované a manuální činnosti v takové kombinaci, která vede co nejrychleji k cíli, a tím je neprůstřelná ochrana uživatelského prostředí. Jedině takové prostředí je pro útočníka natolik neatraktivní, že se přestane zabývat plánováním útoku.

Co tvoří základ služby?

Centrální mozek aplikací **FreeDivision IO** tvoří **SOAR** systém.

Základem služby zabezpečení uživatelského prostředí je jeho monitoring s využitím IA/ML a Threat Intelligence nástrojů ve třech variantách:

A) Monitoring prostředí s využitím vlastních bezpečnostních prvků jako jsou FW, Antivir/EDR a další.
B) Monitoring prostředí s využitím bezpečnostních prvků FreeDivision IO.
C) Kombinace předchozích variant.

Jaké hlavní činnosti služba obsahuje?

- **Monitoring**
- **Analýza alertů**
- **Lov hrozeb**
- **Reakce**
- **Náprava**
- **Reporting**

Datasheet

FREEDIVISION