Logsign®

Zlepšení kybernetické odolnosti. Snížení rizik. Eliminace chaosu.

Jedna platforma pro všechny bezpečnostní operace

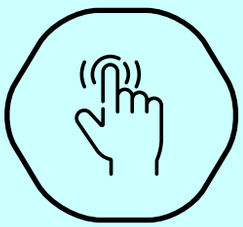
Jednoduchá. Rychlá. Unifikovaná. Škálovatelná.

Společnost Logsign pomáhá organizacím zvýšit jejich kybernetickou odolnost tím, že předchází rizikům a chaosu, a navíc zajišťuje soulad s příslušnými předpisy tím, že sdružuje všechna data, detekci hrozeb, vyšetřování a možnosti reakce na incidenty na jediné, unifikované platformě. Toho je dosaženo integrací různých nativních nástrojů společnosti Logsign, jako je správa bezpečnostních informací a událostí (Security Information and Event Management, SIEM), analýza hrozeb (Threat Intelligence), analýza chování uživatelů (User Entity Behaviour Analytics, UEBA) a také detekce, vyšetřování a reakce na hrozby (Threat Detection, Investigation, and Response, TDIR).

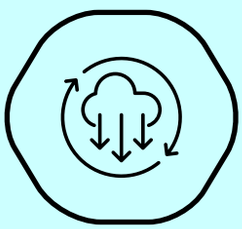
> Integrace mezi jednotlivými nástroji často nestačí. Jsou sice považovány za jednotný funkční celek, ale ve skutečnosti netvoří ucelené řešení.

Čím se liší platforma Logsign Unified SO?

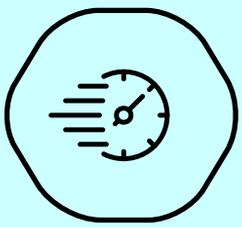
Unifikovaná platforma



Snadné používání



Bezproblémové nasazení a připojení zdrojů



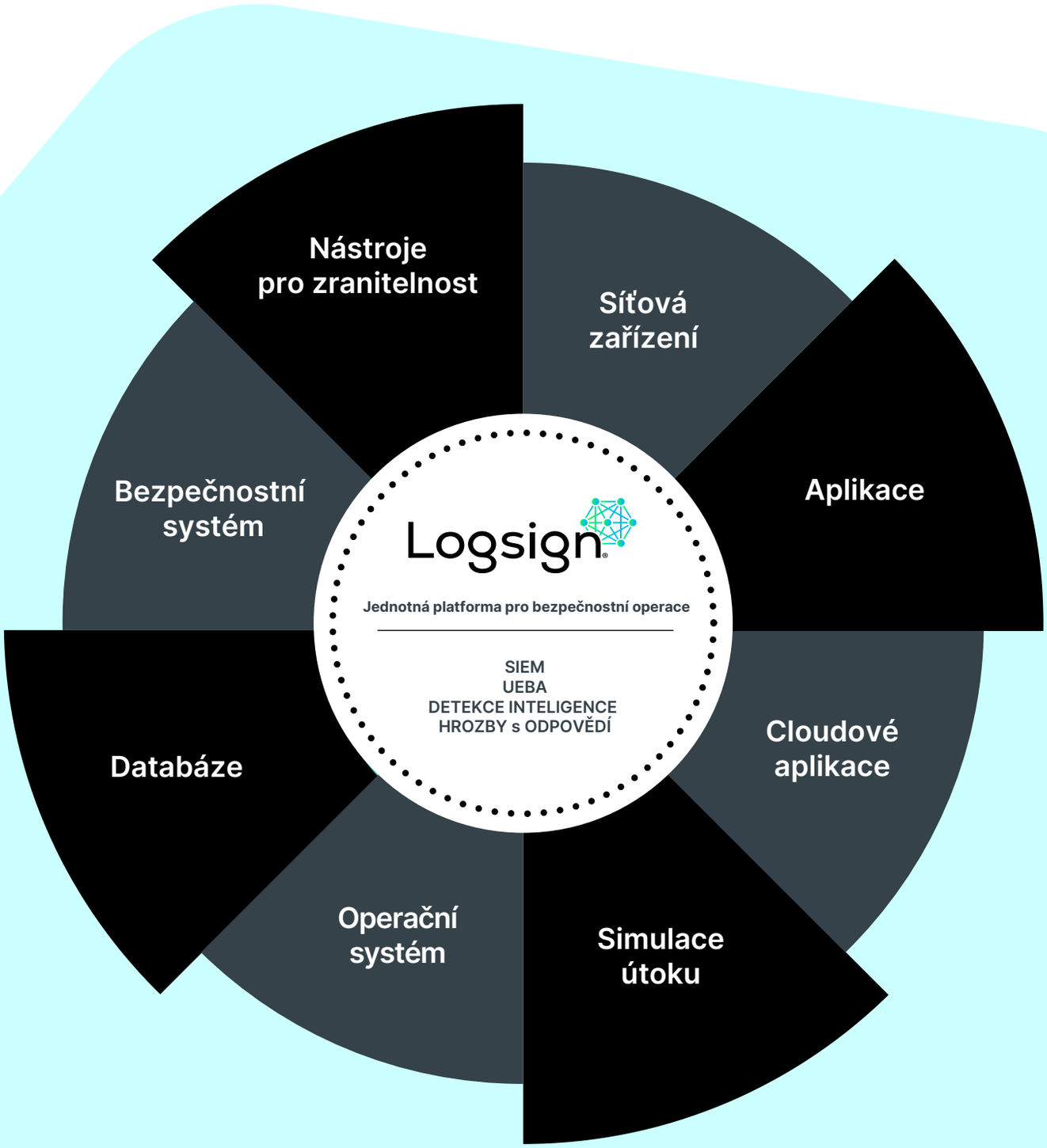
Rychlost detekce a reakce

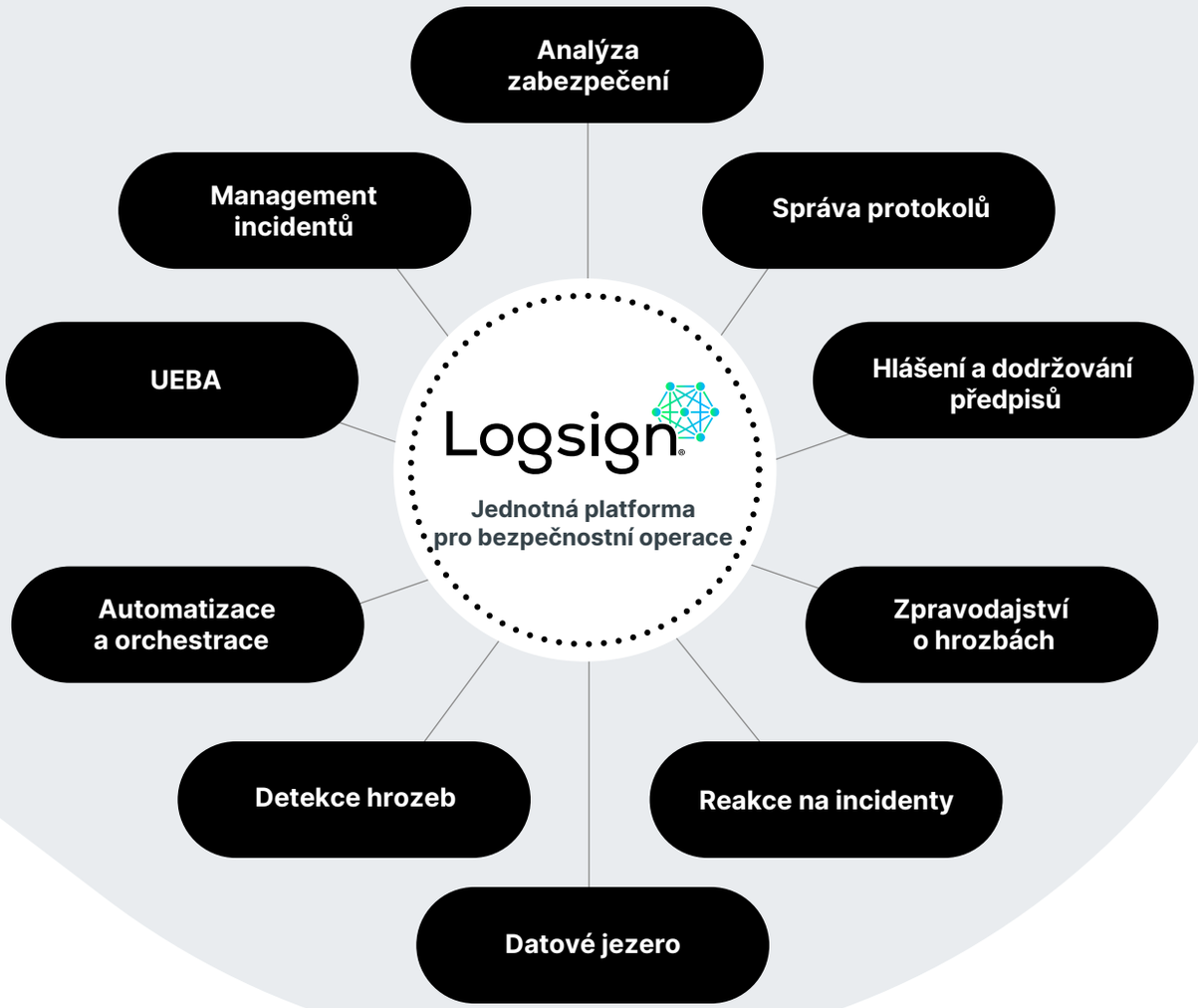
Žádné EPS poplatky,žádné skryté náklady

Jak funguje platforma Logsign Unified SO?

Logsign Unified SO je komplexní bezpečnostní nástroj, který umožňuje vytvářet datové jezero, zkoumat hrozby a zranitelnosti, analyzovat rizika a automaticky reagovat na hrozby.

Možnosti automatizace a orchestrace platformy vycházejí ze zkušeností SOAR a jsou zapojeny do všech fází procesu detekce, vyšetřování a reakce. To umožňuje likvidaci a zmírnění hrozeb a zranitelností během několika sekund, čímž se snižuje průměrná doba detekce a reakce (MTTD, MTTR).





Platforma Logsign Unified SO se bezproblémově integruje se všemi ostatními nástroji SOC, aby umožnila nejlepší správu zabezpečení a týmovou práci. Logsign je srdcem celého procesu. Disponuje rozsáhlou integrační knihovnou s více než 500 předdefinovanými integracemi, bezplatnými plug-in službami a možnostmi vlastního zpracování. Jako platforma Unified Security Operations bezproblémově spolupracuje s ostatními součástmi centra bezpečnostních operací.

400+ kompatibilních zdrojů logů a 100+ integrací s odezvou

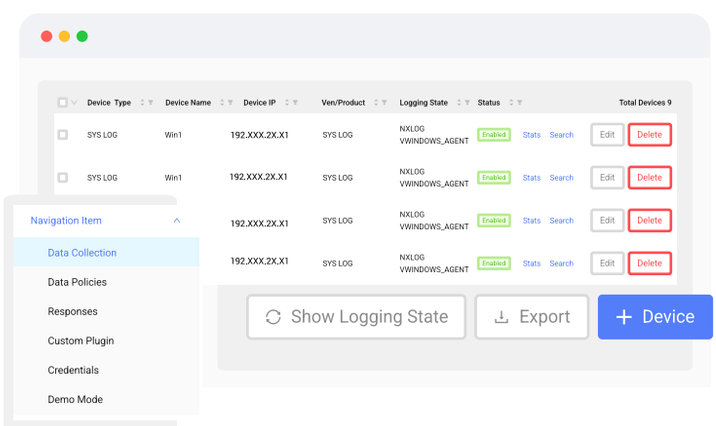
Vytváříme silně zabezpečené datové jezero

Logsign shromažďuje data ze všech zdrojů, aby s nimi pracoval a vytvořil silně zabezpečené datové jezero. Klíčovým faktorem úspěchu je architektura:

- → Vertikální a horizontální škálovatelnost na podnikové úrovni.
- → Nasazení clusteru a vysoká dostupnost.
- → Dlouhodobé ukládání dat.
- → Pokročilé uchovávání dat pro horká a studená data.
- → Rychlé a jednoduché nasazení pro hybridní prostředí.
- → Klíčový uzel pro distribuované sítě pro snadnou centralizaci a správu dat (vysokokapacitní sběrač dat).
- → Filtrování dat a redukce šumu pomocí Data Policy Manager.
- → Režim Demo: Simulace generování protokolu pro nový zdroj.

Správa logů

Logsign dokáže shromažďovat data, která souvisejí se zabezpečením a dodržováním předpisů, ze stovek různých typů produktů od různých výrobců. V současné době dokáže shromažďovat a reagovat prostřednictvím více než 500 předdefinovaných integra

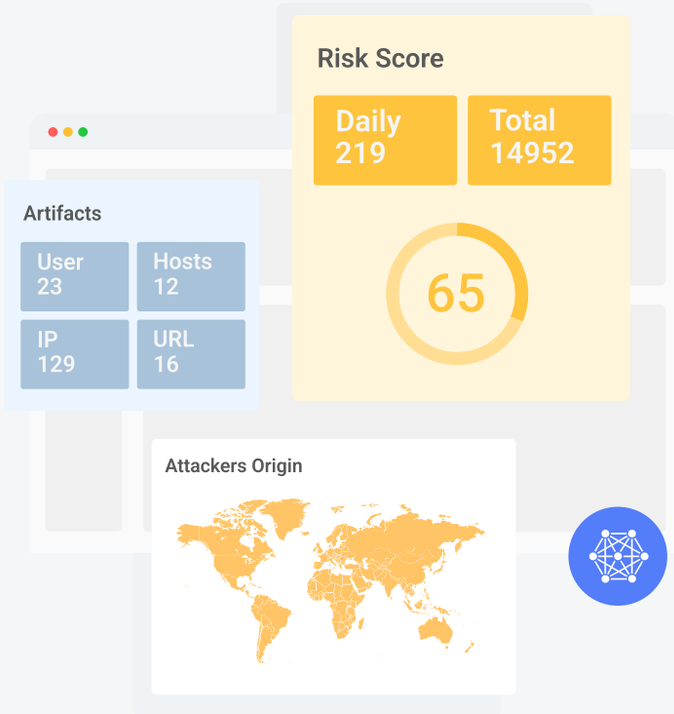


- → Více než 400 předdefinovaných integrací sběru dat.
- → 100+ předdefinovaných integrací detekce a reakce.
- → Bezplatná služba pluginů na neomezenou dobu
- → Vlastní parser pro ty, kteří si jej chtějí vytvořit sami.
- → Pokročilé techniky parsování a indexování.
- → Snadná práce s normalizovanými, klasifikovanými daty.
- → Zpracování dat a jejich modifikace.
- → Více technik sběru dat: API, NetFlow, WMI, Syslog, Oracle, SFTP, FTP, SQL, SMB, JDBC.

Detekce hrozeb a vyšetřování

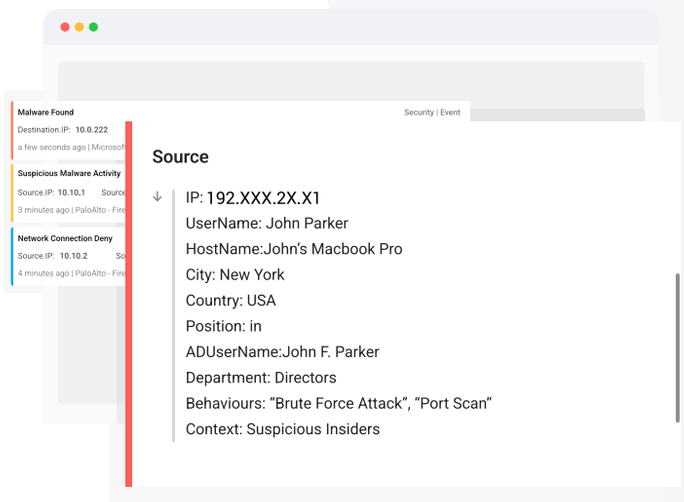
Snadno a jednoduše vytvoříte libovolný dotaz a dosáhnete rychlých, srozumitelných a použitelných výsledků.

- Hlubší kontextové vyhledávání, fulltextové a pokročilé vyhledávání, vyhledávání systémem Lucene.
- Odpovědi na dotazy v řádu milisekund.
- Zkoumá korelovaná a obohacená data.
- Vyhledávání skrytých hrozeb, IOC a IOA.
- Ověřování úrovně hrozeb.
- Třídění událostí.
- Forenzní vyšetřování.
- Rámce MITRE ATT&CK a Cyber Kill Chain
- Hodnocení rizik.



Obohacování dat v reálném čase a pokročilá korelace

Logsign obohacuje data a koreluje je mnoha způsoby, aby odhalil a narušil všechny skryté, komplexní nebo moderní hrozby pomocí rámce MITRE ATT&CK.



Pro obohacení:

- Obohacení aktiv a identity.
- Geo IP, poloha, umístění, LDAP/AD. Kontext, možnost vlastního obohacení.
- Obohacení chování.
- Zpravodajské kanály o hrozbách.
- Pozice v síti, pobočka atd. Okamžité zpracování dat.

Pro korelaci:

- Metody vícenásobné korelace založené na křížové korelaci, historické korelaci, korelaci založené na pravidlech, korelaci založené na chování, korelaci založené na zranitelnosti a korelaci založené na hrozbách.
- Více než 500 předdefinovaných korelačních pravidel.
- Vestavěné korelace pro Threat Intelligence.

Zpravodajství o hrozbách (Threat Intelligence - TI)

Logsign shromažďuje všechna data, obohacuje je a porovnává s dostupnými informacemi o hrozbách v reálném čase. Útočníky odhalí hned při prvním pokusu.

Platforma Logsign Unified SO rychle zkoumá skryté hrozby, indikátory kompromitace (IOCs) a podezřelé vektory útoků pomocí kombinace globálních dat o hrozbách.

Využívá také interní zdrojové kanály hrozeb k prioritizaci rizik. Logsign TI zpracovává více než 40 zdrojových seznamů Threat Intelligence a vizualizuje je pomocí předdefinovaných dashboardů, alertů a reportů, které umožňují sledovat potenciální incidenty vyplývající ze zpravodajských informací o hrozbách.

Logsign používá pouze důvěryhodné zdroje TI, které obohacují vaše data a poskytují vám poznatky pro odhalování hrozeb a útoků.

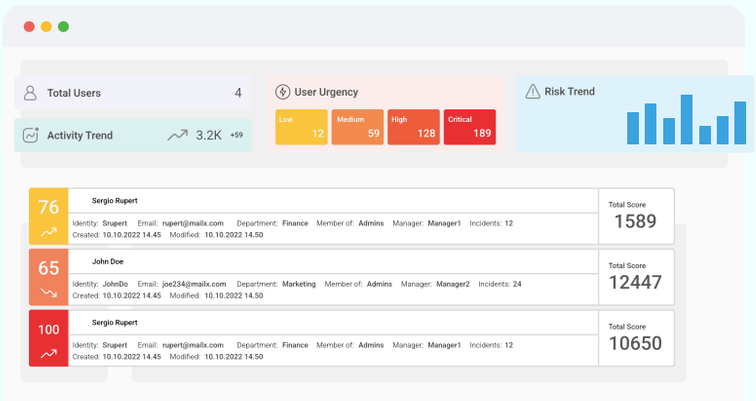
40+

důvěryhodných zdrojů TI, které obohacují vaše data a poskytují vám poznatky k odhalování hrozeb a útoků.

Analýza chování uživatelů a entit

Logsign UEBA využívá pokročilou analytiku ke shromažďování a analýze dat týkajících se aktiv a identity.

Analyzuje konkrétní údaje o hrozbách a určuje, zda určité typy chování představují hrozbu pro kybernetickou bezpečnost. Zjednodušeně řečeno, Logsign UEBA pomáhá odhalovat kybernetické hrozby a předcházet jim tím, že analyzuje chování uživatelů a upozorňuje je na potenciální rizika.



- → Přesné odhalování pokročilých a vnitřních hrozeb.
- → Vyhledávání alertů s nejvyšším rizikem a upřednostňování nízkých hrozeb s negativním trendem.
- → Upřednostňuje vysoce rizikové hrozby pomocí analýzy chování zaměřené na identitu, která odpovídá rámci MITRE ATT&CK.
- → Prevence a zastavení škodlivých útoků zevnitř pomocí pokročilé analýzy chování od společnosti Logsign.
- → Monitoruje přístup uživatelů ke kritickým datům.
- → Zabraňuje infekci botnetem.
- → Zjišťuje rizikové chování všech uživatelů a uživatelů ze seznamu sledovaných osob.
- → Kontext entit v reálném čase.
- → Zastavení exfiltrace dat.

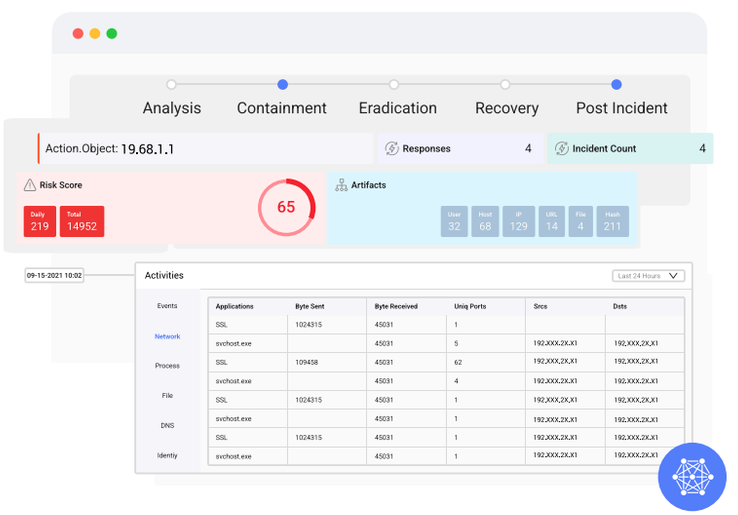
Analýza zabezpečení

Logsign nabízí vysokou kvalitu vizualizace, která se zaměřuje na bezpečnostní analýzu prostřednictvím stovek předdefinovaných vizualizačních nástrojů.

- Stovky vestavěných widgetů, alertů, dashboardů a reportů umožňují získat, za pomoci průvodců, užitečné informace.
- Snadné přizpůsobení a konfigurace nových ovládacích panelů a widgetů.
- Mocní průvodci.
- Delegace: Řízení přístupu na základě rolí.
- Dynamické vyhledávací filtry, vyhledávání s možností prohloubení na přístrojových panelech.
- Filtrování v přístrojových panelech s přizpůsobitelným časovým rámcem.

Management incidentů

Logsign poskytuje životní cyklus reakce, který odkazuje na rámec NIST pro reakci na incidenty. Tento životní cyklus je spojen s akcemi nabízenými společností Logsign. Při každém provedení akce se automaticky zobrazí, které fáze životního cyklu reakce jste dokončili.

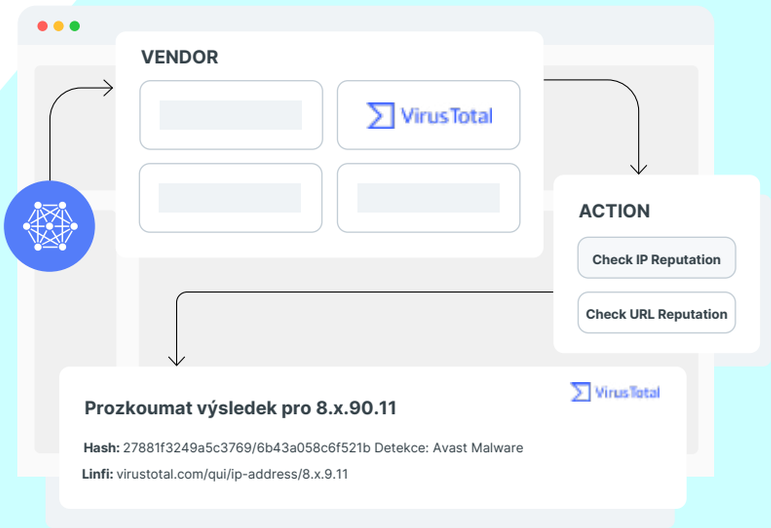


- Správa objektů, aktiv a identit.
- Časová osa incidentu.
- Životní cyklus incidentu podle NIST.
- Souhrnné a podrobné zobrazení událostí.
- Vizuální karty pro vyšetřování, detekci a reakci.

Reakce na incidenty

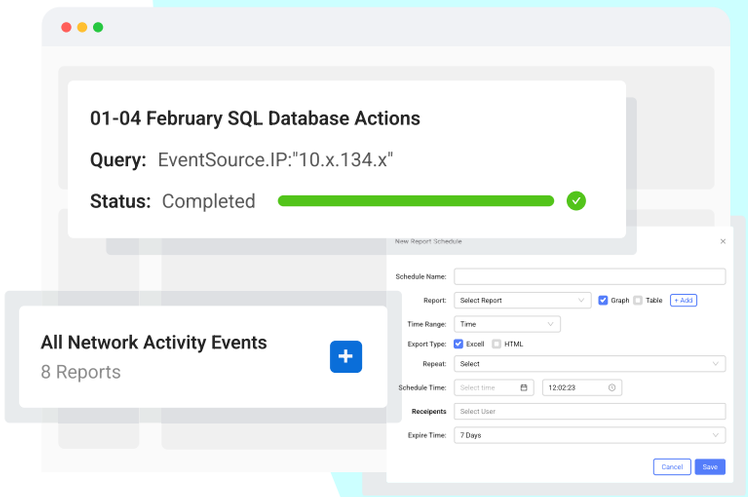
Proaktivní přístup k reakci na incidenty: Podrobný přehled incidentů, jejich zmírnění, eliminace a náprava v reálném čase.

- **Automatická reakce:** Platforma Logsign USO může provádět automatické akce. Tuto funkci nazýváme "Rychlé akce" (Quick Actions).
- **Poloautomatická reakce:** Některé incidenty vyžadují manuální zásahy i po automatických zásazích. To je možné díky "akčnímu tlačítku", které je k dispozici v celém prostředí USO vždy snadno na jedno kliknutí.
  Poskytuje jediné místo pro vyšetřování, zpravodajství, analýzu a reakci a zároveň spravuje incident na jediné stránce.



Auditování a reporty

Připravenost na audity a manažerské reporty. GDPR, PCI DSS, ISO/IEC 27001, HIPAA atd.



- Stovky vestavěných reportů.
- Snadné vytváření a konfigurace nových reportů.
- Vytváření a export během několika sekund.
- Vestavěné reporty o dodržování předpisů.
- Automatizované a naplánované reporty.
- Ad-hoc reporting, manažerský reporting.
- Delegování: Přístup na základě rolí.

Easiest To Use SPRING 2023 · High Performer SPRING 2023 · Easiest Setup SPRING 2023 · CYBER SECURITY EXCELLENCE AWARDS WINNER 2020 · 2021 GLOBE AWARDS SILVER WINNER CYBER SECURITY GLOBAL EXCELLENCE AWARDS · GLOBAL INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2021

Logsign

Recenze Logsign
v oblasti správy bezpečnostních informací a událostí
4.4 ★★★★½
Produkty: Logsign Další