Logsign

Výhody Logsign

Obsah

Správa bezpečnostních informací a událostí Logsign

Architektura pro velká data s nekonečnou škálovatelností

Rychlé nasazení a snadná konfigurace v každém prostředí.

Neomezený sběr a ukládání logů.

Rozsáhlý harmonizovaný systém odolný proti chybám.

Dlouhodobé uchovávání dat.

Neomezený sběr a ukládání logů

Shromažďuje všechny logy z každého zdroje a prostředí s různými, flexibilními možnostmi stanovení cen.

Pokročilé techniky parsování a indexování.

Snadná práce s normalizovanými, klasifikovanými a obohacenými daty.

Detekce komplexních hrozeb

Komplexní korelace všech údajů.

Urychlené a podrobné vyšetřování incidentů.

Včasné odhalení hrozeb kybernetické bezpečnosti.

Odhaluje anomálie a IOC.

Rychlá a účinná ochrana dat

Zmírnění a vymýcení hrozeb.

Automatizované oznamování incidentů, reakce na ně a jejich náprava.

Minimalizace doby odezvy snižující únavu z alertů.

Včasná prevence phishingu prostřednictvím detekce podezřelého síťového provozu.

Proč Logsign SIEM?

360 stupňová vizualizace dat

Vizualizace se stovkami vestavěných dashboardů a reportů založených na analýze zabezpečení.

Chytře navržené uživatelské rozhraní

Snadno použitelná platforma a vestavěné moduly s možností vytvářet nové.

Cenově dostupné zabezpečení

Výpočet nákladů je jednoduchý díky několika flexibilním možnostem tvorby cen společnosti Logsign.

Funkce systému Logsign SIEM

Chytře navržené prostředí pro zpracování velkých objemů dat

- Architektura pro velká data založená na Hadoop file systému a NoSQL databázi. Vytvoření vlastního datového jezera
- Více než 400 vestavěných integrací a integrační funkce na míru, nezávislé na vendorech.
- Neomezená škálovatelnost na úrovni petabajtů.
- Rozsáhlý harmonizovaný systém s možností přidat libovolný počet uživatelů, poznámek nebo zdrojů.
- Rychlé a snadné nasazení.
- Nepřetržitě aktivní s nulovou ztrátou výkonu.
- Neomezené ukládání logů.
- Dlouhodobé uchovávání dat.

Vyhledávání skrytých hrozeb

- Fulltextové vyhledávání Logsign s hloubkového, kontextového prohledávání.
- Zrychlené vyšetřování incidentů.
- Odhaluje hrozby, anomálie a IOC pomocí rámce MITRE ATT&CK.

Rozsáhlá a flexiblní vizualizace

- Více než 200 vestavěných upozornění, dashboardů a reportů se snadným přizpůsobením.
- Snadno použitelní průvodci.
- Přístup založený na rolích zajišťující viditelnost a odpovědnost.

Vytvoření vlastního datového jezera

- Více než 400 vestavěných integrací a integrační funkce na míru, nezávislé na vendorech.
- Parsování nestrukturovaných dat pomocí bezplatné služby zásuvných modulů.
- Neomezený sběr dat z jakéhokoli zdroje a prostředí.
- Obohacení dat o informace o hrozbách v reálném čase.
- Flexibilní správce datových politik.

Detekce komplikovaných hrozeb

- Komplexní korelace dat.
- Třídění incidentů na základě rizikového skóre.
- Pokročilá detekce s minimálním šumem.

Zabezpečení vašich dat

- Automatizovaná reakce na incidenty.
- Včasné oznámení incidentu.
- Automatizovaná opatření k nápravě hrozeb a zranitelností.
- Snadno použitelná platforma a vestavěné moduly s možností vytvářet nové.
- Jednoduchý výpočet nákladů a flexibilní stanovení cen.