LOG MANAGEMENT / SIEM
ELISA SECURITY MANAGER

Jak na snadný sběr a vyhodnocování kyberbezpečnostních i provozních událostí?

ELISA Security Manager je robustní, výkonné, zároveň však nákladově velmi efektivní řešení pro sběr, korelace a analýzu logů. Systém poskytuje vysoký komfort při analýze detekovaných událostí a logů s proklikem do vizuálního editoru pravidel.

Řešení vyhoví potřebám většiny organizací a je v souladu s požadavky zákona o kybernetické bezpečnosti kladenými na významné i kritické informační systémy.

Odhalte a odstraňte problémy v infrastruktuře dříve, než negativně ovlivní chod vaší organizace.

V ČEM VÁM ELISA POMŮŽE

S rozrůstající se infrastrukturou je obtížné mít ucelený přehled bez využití specializovaného nástroje. Řešením je mít jeden systém, kam jsou směrovány veškeré události a informace.

Řešíte často otázky typu:
Kdo smazal soubory na sdíleném disku? Kdo provedl změnu v databázi? Kdo se snaží uhádnout přístupové heslo?

Hledáte nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí, který se přizpůsobí vašim potřebám a je v souladu s normami?

Provozujete vlastní dohledové centrum a potřebujete centrální konzoli k řešení událostí operátory dohledového centra?

Využíváte více bezpečnostních systémů a rádi byste informace sjednotili do jedné platformy?

JEDNO ŘEŠENÍ, MNOHO VÝHOD

- Centrální konzole bezpečnostního dohledu.
- Viditelnost a rychlý rozbor problému.
- Ucelený nástroj pro provozování SOC.
- Soulad se zákony a normami.
- Interaktivní rozhraní, vč. vizuálního editoru pravidel.
- Podpora kontextových korelací.
- Integrace s OpenVAS, GSM, Flowmon, Greycortex aj.
- Integrace s Microsoft Cloud (Azure, Office 365)
- Zabudovaný „Change auditor“.
- Centrální správa agentů.
- Distribuovaný sběr logů.
- Výpočet míry rizika pro každou událost.

V ČEM SE ODLIŠUJEME

- Integrovaný provozní monitoring ZABBIX.
- Škálovatelnost a přizpůsobení implementace.
- Integrovaný tiketovací systém.
- Podpora všech textově koncipovaných logů.
- Koordinace při řešení a proaktivita našich specialistů.
- Český výrobce s přímou technickou podporou.
- Rozhraní i dokumentace v českém jazyce.
- Nízké pořizovací náklady.
- Vysoký výkon (až 10 000 EPS).

„ELISA u jednoho z našich zákazníků dosáhla během 3 měsíců lepších výsledků při vyhodnocování a prošetřování událostí než jejich předchozí SIEM za 3 roky. Navíc za zlomek ceny.

OD LOG MANAGEMENTU K NÁSTROJI TYPU SIEM

Pokročilé korelace

ELISA obsahuje pokročilý korelační mechanismus s podporou kontextových korelací v časovém intervalu až několika měsíců. Lze jím jednoduše detekovat bezpečnostní incidenty – např. na základě opakujících se elementárních událostí, ale také i šíření skrytého malwaru v síti nebo přihlášení uživatelek aplikaci po několika týdnech neaktivity.

Výpočet skóre rizika

Systém umožňuje události obohacovat o údaje z externích zdrojů a pro události počítá tzv. „skóre rizika", díky kterému lze snadno prioritizovat kroky vedoucí k vyřešení indikovaných alarmů. Podporuje taktéž integrace Cyber Thread Intelligence zdrojů dle STIX/TAXII standardu nebo white a blacklistů v libovolném formátu.

Detekce změn konfigurací

Součástí řešení je také podpora pro pravidelnou kontrolu konfigurací (Change Auditor).
ELISA obsahuje File Integrity Monitoring a Registry Integrity Monitoring modul.

Prošetřování událostí a incidentů

Výhodou je také přehledný interní ticketing, který staví na MITRE ATT&CK® a MISP taxonomii. Poskytuje vizualizaci časového průběhu jednotlivých fází incidentu či útoku.

Integrace a podporované zařízení

Díky podpoře standardních protokolů a průmyslových standardů podporuje ELISA na úrovni zpracování bezpečnostních alarmů integraci prakticky jakéhokoli nástroje, včetně cloud aplikací jako např. Microsoft Cloud App Security (Azure, Office 365) nebo sběr trace logů z Exchange Online.

NABÍZENÉ EDICE

	SIEM	LM
Sběr a zpracování logů	✓	✓
Vizuální editor pravidel	✓	✓
Předpřipravené sady dashboardů	✓	✓
Integrovaný provozní monitoring	✓	✓
Integrace se systémy třetích stran	✓	✓
Pokročilé kontextové korelace	✓	
Korelace s existujícími zranitelnostmi	✓	
Detekce změn konfigurací	✓	
Obohacování událostí z jiných zdrojů	✓	
Interní ticketing	✓	
Výpočet skóre rizika	✓	

MODELY NASAZENÍ

Fyzické appliance jsou kompletním řešením v podobě předinstalovaného fyzického serveru, které jsou optimalizované pro trvalé zpracování až 10 000 událostí za sekundu (EPS) a krátkodobě pro příjem až 30 000 EPS.

Propustnost systému a kapacitu centrálního úložiště logů lze zvyšovat horizontálním škálováním, tj. pořízením dalších zařízení a provedením clusterové instalace.

ELISA je dostupný též jako virtuální appliance (VMware, Hyper-V). Při dostatečné alokaci výkonových prostředků lze ve virtuálním prostředí dosahovat analogických propustností. Výkonnost distribuovaného systému sběru dat lze navyšovat i vertikálním škálováním.

LICENCOVÁNÍ

Softwarová licence (roční předplatné) je licencována dle počtu monitorovaných zařízení. Základní licence začíná na 50 zařízeních až po neomezenou licenci.

S výběrem správné edice či modelu vám rádi pomůžeme.