ELISA SECURITY MANAGER

NÁSTROJ PRO SBĚR A VYHODNOCENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

DATASYS

DATASYS ELISA SECURITY MANAGER (ESM) je robustní, výkonné, zároveň však nákladově velmi efektivní řešení pro sběr, korelace a analýzu logů. Systém poskytuje **vysoký komfort při analýze detekovaných bezpečnostních incidentů** a relevantních logů.

Uživatelské prostředí je webový prohlížeč. **Vyhledávání v databázi je podobné s hledáním v internetovém vyhledávači.** Po krátkém zaškolení dokáže i nezkušený uživatel formulovat komplexní filtry.

Nástroj ELISA byl původně vyvíjen jako log management a takový stále zůstává ve své základní edici. Od verze 4 je však k dispozici také edice rozšířená, představující ELISU jako komplexnější **nástroj typu SIEM**.

ELISA Security Manager obsahuje pokročilý **korelační mechanismus** s podporou kontextových korelací v časovém intervalu až několika měsíců. Lze jím detekovat kybernetickou bezpečnostní událost nejen např. na základě opakujících se elementárních událostí, ale třeba i šíření skrytého malwaru v síti nebo přihlášení uživatele k aplikaci po několika týdnech neaktivity.

ESM umožňuje události obohacovat o údaje z externích zdrojů a pro všechny události počítá, **„skóre rizika"**, z něhož lze snadno prioritizovat kroky vedoucí k vyřešení indikovaných alarmů. Součástí je také podpora pro **pravidelnou kontrolu konfigurací** (tzv. Change Auditor) a další pokročilé SIEM funkce.

KLÍČOVÉ VLASTNOSTI

- Automatizované vyhodnocování.
- Detekce bezpečnostních rizik.
- Přehledné uživatelské rozhraní.
- Soulad se ZKB, GDPR, ISO, PCI.
- Zabudovaný „Change Auditor".
- Další pokročilé SIEM funkce.
- Integrace s OpenVAS a GSM.
- Integrace s Flowmon ADS.
- Fyzické i virtuální appliance.
- Distribuované kolektory logů.
- Horizontální škálovatelnost.
- Vysoký výkon (až 10 000 EPS).
- Nízké pořizovací náklady.

JAKÉ INFORMACE S ŘEŠENÍM ELISA ODHALÍTE

Z JAKÝCH MÍST LIDÉ PŘISTUPUJÍ NA FIREMNÍ WEB?

KDO PROVEDL ZMĚNU V DATABÁZI?

KTEŘÍ UŽIVATELÉ STAHUJÍ NEJVÍCE DAT Z INTERNETU?

KDO SMAZAL SOUBORY NA SDÍLENÉM DISKU?

K JAKÝM CHYBÁM DOCHÁZÍ V PODNIKOVÉM IS?

KDO SE SNAŽÍ UHÁDNOUT PŘÍSTUPOVÉ HESLO?

EDICE ELISA SECURITY MANAGER

V SIEM edici ELISA 4.0 jsou oproti Log management edici navíc tyto funkcionality:

POKROČILÉ KONTEXTOVÉ KORELACE V ČASOVÉM INTERVALU I NĚKOLIKA MĚSÍCŮ

- Detekce opakovaného výskytu události s možností dynamicky definovat korelační klíč.
- Pokročilé kontextové korelace pro dynamické provázání různých typů událostí.
- Detekce chybějícího výskytu definované události za časový interval.
- Detekce nové unikátní hodnoty v definované události.

KORELACE S EXISTUJÍCÍMI ZRANITELNOSTMI S VYUŽITÍM STANDARDNÍ CVE KLASIFIKACE

- Integrace s „vulnerability mgmt“ nástrojem Greenbone Security Manager nebo OpenVAS.

DETEKCE ZMĚN KONFIGURACÍ AGENTEM

- ELISA obsahuje File Integrity Monitoring a Registry Integrity Monitoring modul.

DETEKCE ZMĚN KONFIGURACÍ ZAŘÍZENÍ

- Periodickým načítáním exportu konfigurací.

DETEKCE INCIDENTŮ S VYUŽITÍM EXTERNÍCH ZDROJŮ

- Podpora integrace Cyber Thread Intelligence zdrojů dle STIX/TAXII standardu.

ŘEŠENÍ INCIDENTŮ - INTERNÍ TICKETING

- ELISA staví na MITRE ATT&CK® a MISP taxonomii.

VÝPOČET SKÓRE RIZIKA

- Možnost nastavit míru dopadu per zařízení nebo i pro specifický zdroj logů.
- Skóre rizika = Míra dopadu x Závažnost události x Spolehlivost detekce.

SPECIFIKACE NABÍZENÝCH MODELŮ

Fyzické appliance jsou kompletním ELISA Security Manager systémem v podobě předinstalovaného fyzického serveru s „On-Site Service“ hardwaru „následující pracovní den“ na 5 let. Jedná se o modely optimalizované pro trvalé zpracování až 10000 událostí za sekundu (EPS) a krátkodobě pro příjem až 30000 EPS.

Model	Propustnost (EPS)	Kapacita úložiště	Odhad retence (poloviční EPS)	Odolnost úložiště (RAID)	Redundantní napájení
ESM Appliance XL	10 000	100 TB	12 měsíců	2 disky	Ano
ESM Appliance L	6 000	42 TB	9 měsíců	2 disky	Ano
ESM Appliance M	2 000	12 TB	8 měsíců	1 disk	Ano
ESM Appliance S	1 000	4 TB	3 měsíce	1 disk	Ano

Propustnost systému ELISA Security Manager a kapacitu centrálního úložiště logů lze zvyšovat horizontálním škálováním, tj. pořízením dalších zařízení a provedením clusterové instalace.
ELISA Security Manager je dostupný též jako virtuální appliance (VMware, Hyper-V, KVM).
Při dostatečné alokaci výkonových prostředků lze ve virtuálním prostředí dosahovat analogických propustností. Výkonnost distribuovaného systému sběru dat lze navyšovat i vertikálním škálováním.

LOG MANAGEMENT SYSTÉM **ELISA OCENÍ** NEJEN **BEZPEČNOSTNÍ SPRÁVCI,** ALE I **SPRÁVCI ODPOVĚDNÍ ZA PROVOZ SYSTÉMŮ.**

VYHLEDÁVÁNÍ V UDÁLOSTECH VZNIKAJÍCÍCH V INFORMAČNÍCH SYSTÉMECH UŽ PRAKTICKY **NEMŮŽE BÝT JEDNODUŠŠÍ!**