PŘÍPADOVÁ STUDIE

Centrální log management (nejen) ve vysoce zabezpečené části sítě

MZV ČR potřebovalo plošně nasadit moderní log management a SIEM nástroj pro dosažení souladu s požadavky ZKB a zákona o ochraně utajovaných informací. Nástroj ELISA SM skvěle vyhovuje všem.

VÝCHOZÍ STAV

Odbor kybernetické bezpečnosti MZV hledal nástroj k zajištění spolehlivého sběru auditních logů z desítek centrálních serverů, ze síťových prvků a z více než stovky zahraničních úřadů s různou úrovní konektivity. Je důležité zmínit, že MZV je správcem několika významných informačních systémů (dle ZKB). Nadto provozuje komunikačně oddělenou síť pro zpracování utajovaných informací s velmi striktními bezpečnostními požadavky na všechny instalované systémy a aplikace.

Prioritou bylo pořídit jednotný nástroj, který se přizpůsobí potřebám bezpečnostního dohledu v takto různorodém prostředí, který bude možné instalovat na EAL4+ certifikovaný operační systém a který po instalaci úspěšně projde i OSCAP testy. Nástroj, který zajistí spolehlivý sběr KBU z již pořízených bezpečnostních nástrojů, včetně nástrojů pro vyhodnocování anomálních datových toků v síti. ELISA SM tyto potřeby splňuje.

PŘEHLED VLASTNOSTÍ DODANÉHO ŘEŠENÍ

Log management – Robustní, výkonné, zároveň však nákladově velmi efektivní řešení pro sběr, vyhodnocování a analýzu logů. Systém poskytuje vysoký komfort při analýze detekovaných bezpečnostních událostí a relevantních logů s proklikem do vizuálního editoru pravidel.

Pokročilé korelace – 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.

Výpočet skóre rizika – ELISA SM 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. Výhodou je též podpora integrace Cyber Thread Intelligence zdrojů dle STIX/TAXII standardu nebo i white či blacklistů v téměř libovolném formátu.

Detekce změn konfigurací – Součástí řešení je rovněž podpora pro pravidelnou kontrolu konfigurací (tzv. Change Auditor). ELISA SM obsahuje File Integrity Monitoring a Registry Integrity Monitoring modul.

„ELISA se nám osvědčila v kombinaci s netflow monitoringem, kdy v log managementu dohledáváme detaily bezpečnostních událostí."

Luboš Pilař, IT Security Manager, MZV ČR

OBOR:

Státní správa

PŘEDSTAVENÍ – MZV ČR:

Ministerstvo zahraničních věcí je ústředním orgánem státní správy České republiky pro oblast zahraniční politiky, v jejímž rámci vytváří koncepci a koordinuje zahraniční rozvojovou pomoc a koordinuje vnější ekonomické vztahy.

CÍL PROJEKTU:

Poskytnout zejména analytikům jednotnou konzoli pro rychlé vyhledávání v auditních logách z aplikací, databází, stanic i serverů, z firewallů, síťových prvků atd. Analýza je běžně prováděna i mnoho měsíců do minulosti a jedná se o stovky GB dat denně.

ŘEŠENÍ:

Dodali jsme SIEM nástroj ELISA Security Manager založený na technologii Elasticsearch jako vysoce dostupné řešení tří fyzických a virtuálních appliancí a mnoha centrálně spravovaných kolektorů dat.

SHRNUTÍ PŘÍNOSŮ:

- Jednotná konzole pro analytiky bezpečnostních událostí.
- Rychlé a intuitivní přehledy pro vyhledávání nových hrozeb.
- Prioritizace událostí výpočtem skóre rizika z několika faktorů.
- Více než 120 odlehčených kolektorů dat na úřadech.
- Bezkonkurenční cena.