PŘÍPADOVÁ STUDIE

DATASYS

Centrální bezpečnostní dohled pro podporu procesů interního SOC

Česká pošta potřebovala moderní SIEM nástroj pro automatizované vyhodnocování kybernetických bezpečnostních událostí a pro jejich prošetřování. Náš produkt ELISA se v ČP osvědčil jako nákladově efektivní a plně funkční řešení.

VÝCHOZÍ STAV

Pracovníci bezpečnostního dohledu České pošty se několik let potýkali s náročným nasazením SIEM nástroje globální značky, a i po nákladné spolupráci specialistů dodavatele dosahovali jen dílčích úspěchů. V souvislosti s budováním interního SOC se bezpečnostní manažer ICT rozhodl k razantní změně – k výběru nového SIEM nástroje a k migraci a zásadnímu rozvoji používaných pravidel vyhodnocování KBU.

Prioritou bylo pořídit nástroj, který se přizpůsobí potřebám bezpečnostního dohledu v prostředí specifických informačních systémů České pošty, a který zajistí spolehlivý sběr KBU z již pořízených bezpečnostních nástrojů, včetně PAM nástroje pro nahrávání relací uživatelů přistupujících privilegovanými účty.

PŘEHLED VLASTNOSTÍ DODANÉHO ŘEŠENÍ

Log management – Jde o 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 jednoduše, 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 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 téměř libovolném formátu.

Detekce změn konfigurací – Součástí řešení je také podpora pro pravidelnou kontrolu konfigurací (tzv. 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 prošetřovaného incidentu či útoku.

„S řešením od DATASYS jsme během tří měsíců dosáhli za zlomek ceny lepších výsledků při vyhodnocování a prošetřování událostí než s předchozím SIEM nástrojem za tři roky."

Ing. Luděk Tichý, ICT Security Manager, Česká pošta, s.p.

OBOR:

Poštovní služby

PŘEDSTAVENÍ – Česká pošta:

Tradiční poskytovatel služeb z oblasti zprostředkování informací, plateb a zboží tradičními i elektronickými formami. V roce 2020 měla Česká pošta téměř 30 tisíc zaměstnanců.

CÍL PROJEKTU:

Poskytnout zejména operátorům dohledového centra přehlednou konzoli detekovaných rizikových událostí, dovolit operátorům snadno vyhodnotit tyto události v kontextu situace a umožnit rychlé zpracování každé události i jen jedním kliknutím.

ŘEŠENÍ:

Dodali jsme SIEM nástroj ELISA Security Manager založený na technologii Elasticsearch. Jedná se o vysoce dostupné řešení dvou fyzických appliancí a centrálně spravovaných kolektorů dat.

SHRNUTÍ PŘÍNOSŮ:

- Jedna konzole k řešení událostí operátory dohledového centra.
- Rychlé a intuitivní přehledy pro vyhledávání nových hrozeb.
- Prioritizace událostí výpočtem skóre rizika z několika faktorů.
- Výrobcem na míru uzpůsobené workflow zpracování událostí.
- Bezkonkurenční cena.