ELISA

Security Manager

Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Novicom 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 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 systém**, který byl postupně **rozšířen do komplexnějšího nástroje typu SIEM.**

Novicom ELISA Security Manager také 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.

ELISA 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 ELISY je také podpora pro pravidelnou kontrolu konfigurací (tzv. Change Auditor) a další pokročilé SIEM funkce.

Jaké informace s nástrojem Novicom ELISA odhalíte

Přehled funkčních vlastností

ELISA

UPOZORNĚNÍ NA CHYBY APLIKACÍ NEBO SYSTÉMŮ

- **SOFISTIKOVANÉ VYHODNOCOVÁNÍ KORELACEMI**
  - Detekce bezpečnostních incidentů
  - Potlačení falešných alarmů a notifikací
- **KONKRÉTNÍ JEDNOTLIVÉ CHYBY**
  - Pružněji než běžný provozní monitoring (Nagios, Zabbix, ...)
- **SROZUMITELNOST**
  - Překlad chybových kódů
  - Překlad IP adres na DNS jména

BEZPEČNOSTNÍ MONITORING

- **CENTRÁLNÍ KONZOLE ALARMŮ**
  - Antivirový systém
  - Systém prevence průniku (IPS)
  - Systém prevence ztráty dat (DLP)
- **ANALÝZA DOPADŮ**
  - Komu byla doručena infikovaná příloha e-mailu?
  - Jaké stanice vykazují příznaky virové nákazy?
  - Které uživatelské účty byly při útoku kompromitovány?

PROVOZNÍ MONITORING

- **INTEGROVANÝ SYSTÉM ZABBIX**
  - Grafické znázornění dostupnosti a zatížení sítě
  - Plně automatizovaný monitoring VMware infrastruktury
  - End-user monitoring webových aplikací
  - Vyhodnocování plnění SLA dodavateli

ANALÝZA PROVOZU V SÍTI

- **WEBOVÁ PROXY**
  - Nejvíce navštěvované weby
  - Největší stahovači dat
- **WEBOVÝ SERVER**
  - Z jakých měst lidé přistupují?
  - Detekce nefunkčních odkazů na firemním webu
- **FIREWALL, ROUTER**
  - Detekce skenování portů útočníkem
  - Detekce DoS a DDoS útoků
- **INTERNÍ PŘEPÍNAČ**
  - Jaké aplikace nejvíce zatěžují síť
  - Která zařízení generují nejvíc provozu v síti?
  - Kontrola řízení přístupu zařízení k síti dle 802.1x

AUDITOVÁNÍ ZMĚN A ČINNOSTÍ

- **DATABÁZE**
  - Kdo změnil číslo bankovního účtu?
  - Kdo si prohlíží osobní údaje zaměstnanců?
- **DOKUMENTY A SOUBOROVÉ SYSTÉMY**
  - Kdo smazal nabídkové dokumenty?
  - Kdo si kopíruje neobvyklé množství výkresů?
- **ZMĚNY KONFIGURACE**
  - Síťových prvků a bezpečnostních zařízení
  - Adresářových služeb a operačních systémů
  - Aplikací a databází
- **SOULAD S NORMAMI**
  - ČSN ISO 27001
  - Zákon o kybernetické bezpečnosti
  - PCI, SOX a další

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 nástroji monitoringu a řízení sítě
- Fyzické i virtuální appliance
- Distribuované kolektory logů
- Horizontální škálovatelnost
- Vysoký výkon (až 10 000 EPS)
- Nízké pořizovací náklady
- Navrženo pro využití výhod strategie aktivního SOCu

ELISA – využité technologie

ELASTICSEARCH poskytuje díky své architektuře **bleskové odezvy** i v případě objemných indexů/databází. Uživateli je v základu zobrazen histogram počtu výskytů vyhovujících záznamů za zvolený časový interval a jejich tabulkový stránkovaný přehled.

V odladěné konfiguraci našeho řešení ELISA jsou události přenášeny do analytické databáze v původní, strukturu záznamu zachovávající podobě, s bezproblémovou podporou diakritiky.

Označením konkrétní události získá uživatel přehled o všech jejích atributech a možnost drill-down analýzy.

Výběrem některého z atributů totiž uživatel získá statistický přehled výskytu jeho různých hodnot s možností rychlého (i negativního) filtrování dle dané hodnoty.

NXLOG je agent určený k **instalaci na monitorované systémy**, které nedokáží záznamy z logů zpracovat a odeslat autonomně. NXlog podporuje sběr událostí z textových logů, windows eventlogů, různých typů strukturovaných logů (CSV, j2log a mnohých dalších) a z tabulek relačních databází.

ZAJÍMAVÉ VLASTNOSTI PROGRAMU NXLOG:

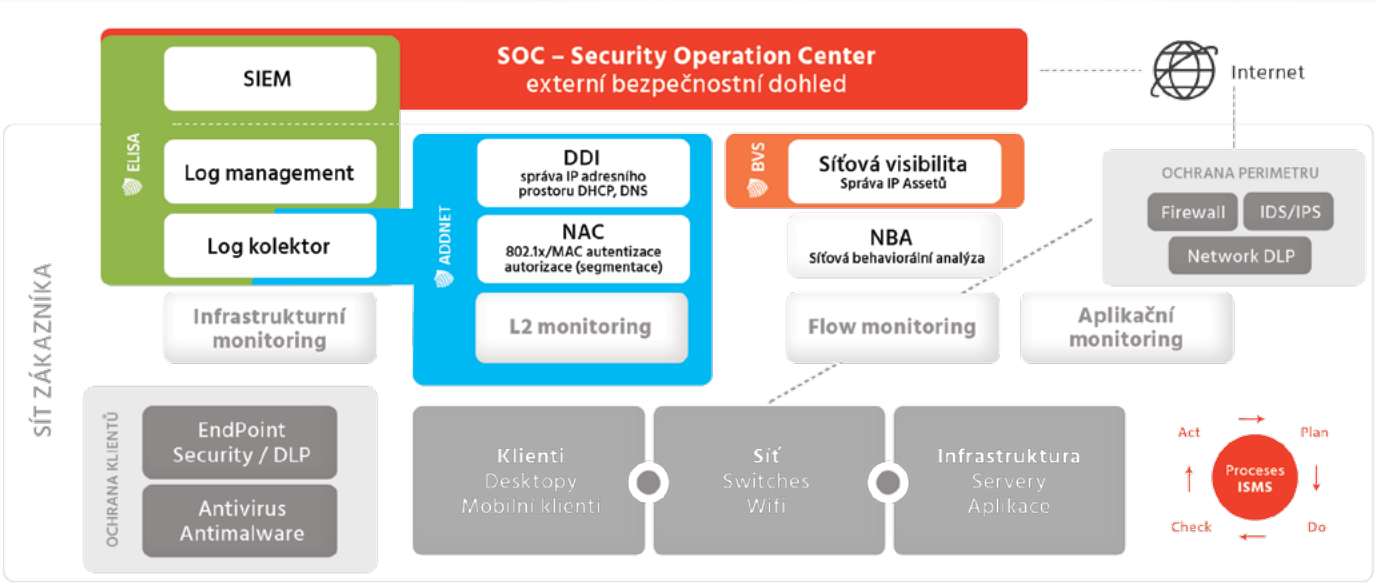
- Agent multiplatformní a nenáročný na zdroje
- Vytváří buffer událostí v případě nedostupnosti centrálního systému
- Pamatuje si pozici již zpracovaných událostí i po restartu
- Podporuje rotované log soubory, různé typy kódování a víceřádkové záznamy
- Umožňuje filtrování a korelace událostí už na monitorovaném systému
- Podporuje přenos strukturovaných záznamů v binárním formátu a šifrovaný přenos (TLS)

Specifikace nabízených modelů Novicom ELISA

Fyzické appliance jsou **kompletním systémem Novicom ELISA Security Manager** v podobě předinstalovaného fyzického serveru **s vysokou úrovní standardní podpory** – „On-Site Service" hardwaru „následující pracovní den" po dobu 5 let.

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. **Novicom ELISA Security Manager 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.**



ELISA a aktivní SOC

ELISA je významnou součástí strategie Aktivní SOC (Security Operation Center), kterou se Novicom, spolu se svými SOC partnery, snaží na trhu prosadit. **ELISA**, společně s řešením **ADDNET** pro efektivní správu síťových služeb a řízení přístupu do sítě, a s řešením **BVS** pro vizualizaci síťových assetů včetně jejich návaznosti na business procesy, **tvoří unikátní portfolio**, které připravuje zákazníky k rychlému a bezproblémovému připojení ke službě SOC. Zákazníci, využívající tuto platformu produktů, pak mohou plně využít výhod nadstandardních služeb Aktivního SOCu. Vybraní SOC operátoři jsou díky tomu schopni garantovat plně kvalifikovanou aktivní reakci na kybernetické útoky v režimu 24x7 bez nutné součinnosti se správci systémů u zákazníka. To plně odpovídá současnému trendu využívání vrcholového bezpečnostního dohledu (SOC) formou služby. Tím se eliminuje ekonomická nevýhodnost při pořizování kompletního spektra jednoúčelových technologií a při nutnosti mít inhouse k dispozici vysoce specializovaný tým schopný postavit se kdykoliv profesionálním hackerům.

Nástroj Novicom ELISA ocení nejen bezpečnostní správci, ale i správci odpovědní za provoz systémů.

novicom

Novicom, s.r.o.
Praha, Česká republika

www.novicom.cz
sales@novicom.cz

ELISA