DATA SYS

NÁSTROJ PRO SBĚR A VYHODNOCENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

(§21 a §23 vyhlášky k ZoKB)

ELISA

- **Automatizované vyhodnocování logů**
- **Robustní noSQL databázové jádro**
- **Podpora standardních protokolů**
- **Nízké pořizovací i provozní náklady**
- **Zachovává strukturu původní události**
- **Líbivé webové uživatelské rozhraní**
- **Extrémní škálovatelnost a HA**
- **Vysoký výkon (až 6000 eps)**

PŘEDSTAVENÍ

DATASYS ELISA je robustní, výkonné, zároveň však nákladově velmi efektivní řešení pro sběr, korelace a analýzu logů. Jádrem systému je „noSQL“ analytická databáze ElasticSearch s uživatelským rozhraním Kibana, které poskytuje vysoký komfort při analýze detekovaných bezpečnostních incidentů a relevantních logů. ElasticSearch databázi je běžné distribuovat na více serverů za účelem rozdělení zátěže a vysoké dostupnosti indexovaných dat. Nedílnou součástí ELISA je celosvětově rozšířený nástroj provozního monitoringu ZABBIX, jehož webové rozhraní je současně rozhraním pro správu konfigurací sběru a vyhodnocování logů v ELISA.

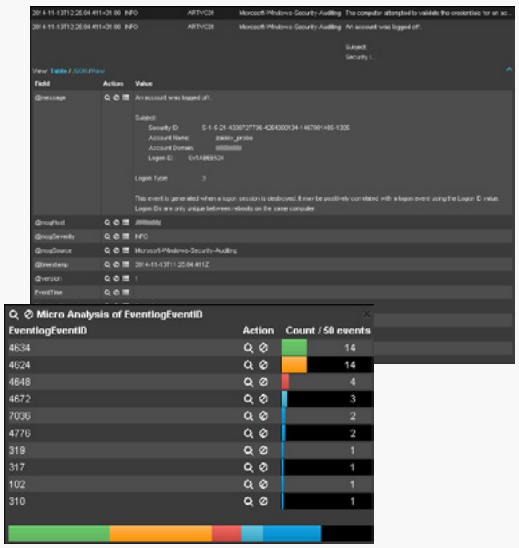
Uživatelským prostředím je webový prohlížeč. Vyhledávání v databázi událostí je podobné s hledáním v internetovém vyhledávači – prováděno jednoduše zadáním klíčových slov. Po krátkém zaškolení dokáže ale i nezkušený uživatel formulovat též komplexní filtry, které široce přesahují možnosti vyhledávání v relačních databázích. Definice filtrů lze ukládat pro opakované použití.

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.



BEZPEČNOSTNÍ UDÁLOSTI JSOU V SYSTÉMU ELISA VYHODNOCOVÁNY NA DVOU ÚROVNÍCH:

1.) na vstupu při prvotním zpracování událostí
- detekce výskytu konkrétních událostí
- korelace mezi událostmi
  - opakované výskyty
  - relace mezi různými událostmi
  - kontextové korelace

2.) definovanými periodickými dotazy do databáze
- statistické anomálie
- „first“ události apod.

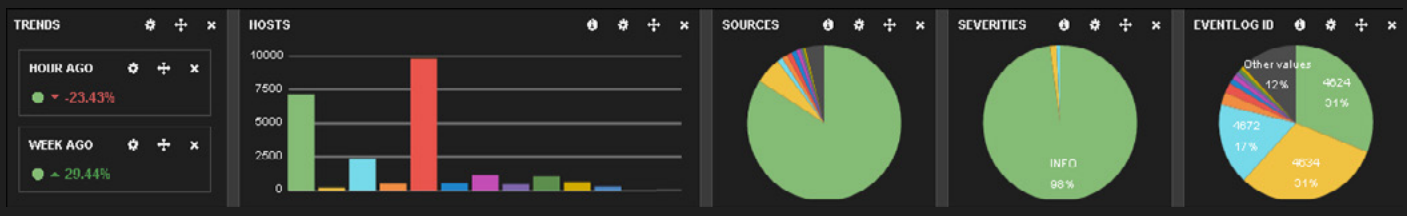
HLAVNÍMI VSTUPNÍMI KANÁLY SYSTÉMU ELISA JSOU:

- binární protokol pro přenos strukturovaných událostí
- syslog (udp i tcp)
- SNMP trapy

VÝZNAČNÉ VLASTNOSTI PROGRAMU NXLOG:

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.

- 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)



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!

elasticsearch.

DATASYS

CENTRÁLA - PRAHA
Jeseniova 2829/20
130 00 Praha 3
tel.: +420 225 308 111
e-mail: datasys@datasys.cz

HRADEC KRÁLOVÉ
Hořická 283/22
500 02 Hradec Králové
tel.: +420 225 308 640

PLZEŇ
Schwarzova 50
301 00 Plzeň
tel.: +420 225 308 633

DĚČÍN
Labská 694/24
405 02 Děčín
tel.: +420 225 308 250

OSTRAVA
Vysoká škola báňská
Technická univerzita Ostrava
Studentská 6202/17
708 33 Ostrava-Poruba
tel: +420 724 065 027