ELISA

DATASYS

NÁSTROJ PRO SBĚR A VYHODNOCENÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ *(§21 a §23 vyhlášky k ZoKB)*

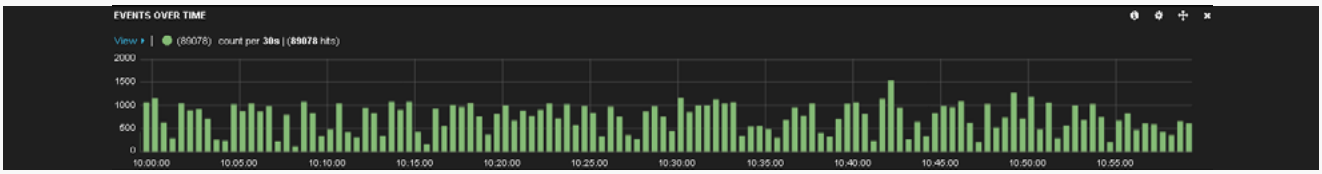
- Svobodný software s podporou výrobce
- Robustní noSQL databázové jádro
- Podpora standardních protokolů
- Nízké pořizovací i provozní náklady

- Zachovává strukturu původní události
- Líbivé webové uživatelské rozhraní
- Extrémní škálovatelnost a HA
- Vysoký výkon (až 5000 eps)

PŘEDSTAVENÍ

DATASYS ELISA je robustní, výkonné, přitom však levné 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.

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.

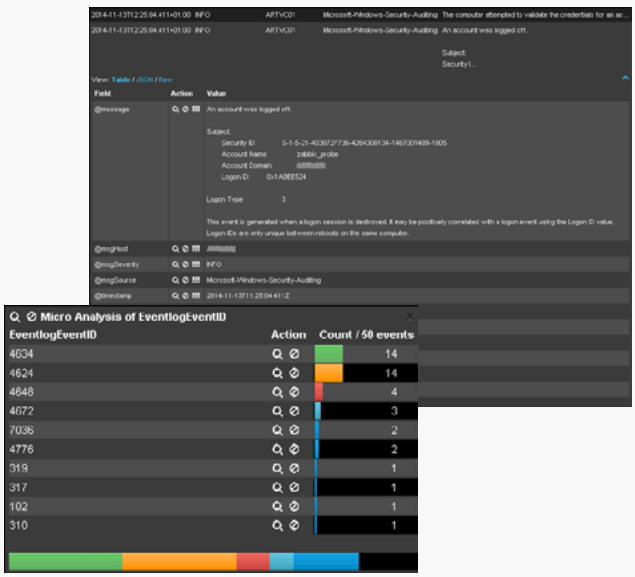


ElasticSearch poskytuje díky své architektuře bleskové odezvy i v případě objemných indexů/databází. Uživateli je v základu zobrazen histogram počtu výskytů vyhovujících záznamů za zvolený časový interval a jejich tabulkový stránkovaný přehled.

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.



ELISA

EVENT LOG INTERCEPTION STORAGE AND ANALYSIS

elasticsearch.

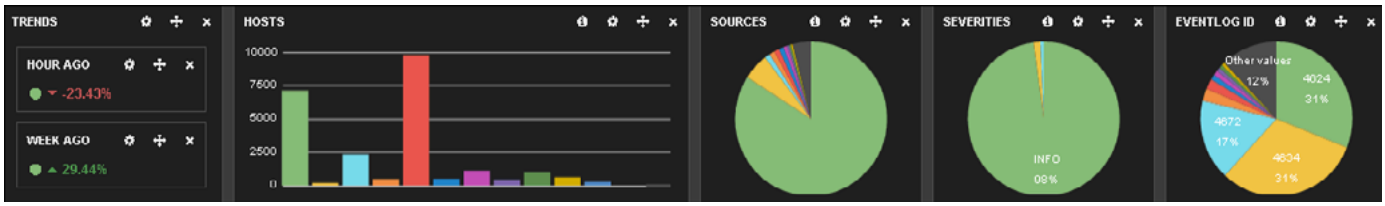
Bezpečnostní události jsou v systému ELISA vyhodnocovány na dvou úrovních:

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



Doprovodný nástroj DATASYS DSlog je určen k instalaci na monitorované systémy, které nedokáží záznamy z logů zpracovat a odeslat autonomně. DSlog podporuje sběr událostí z textových logů, windows event-logů, různých typů strukturovaných logů (CSV, j2log a mnohých dalších) a z tabulek relačních databází.

Význačné vlastnosti programu DSlog:

- multiplatformní a nenáročný na zdroje
- vytváří buffer událostí v případě nedostupnosti centrálního systému ELISA
- 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 (SSL)

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!

DATA SYS

DATASYS S.R.O.
Jeseniova 2829/20
130 00 Praha 3
tel.: +420 225 308 111
fax: +420 225 308 110
e-mail: datasys@datasys.cz

HRADEC KRÁLOVÉ
DATASYS s.r.o.
U Koruny 414
500 02 Hradec Králové
tel.: +420 495 401 051
fax: +420 225 308 110

PLZEŇ
DATASYS s.r.o.
Slovanská alej 30
326 00 Plzeň
tel.: +420 377 410 306
tel.: +420 377 410 325

DĚČÍN
DATASYS s.r.o.
Labská 694/24
405 02 Děčín
tel.: +420 222 208 631
fax: +420 225 308 631

SERVICEDESK/ HELPDESK
tel.: +420 225 308 250
fax: +420 225 308 444
email: support@datasys.cz
skype: datasys.servicedesk
WWW.DATASYS.CZ