KONTROLA PRIVILEGOVANÝCH PŘÍSTUPŮ NAHRÁVÁNÍM RELACÍ

DATA SYS

EKRAN

Privilegovaní uživatelé, **zaměstnanci i pracovníci třetích stran,** hrají klíčovou roli při provozování jakéhokoli informačního systému. Účty s eskalovanými oprávněními nebo správci systému a databází mívají neomezený přístup nejen ke konfiguraci systému, ale i k datům. Mohou spravovat účty jiných uživatelů a jejich oprávnění.

NÁSTROJ PRO ZAZNAMENÁVÁNÍ UŽIVATELSKÝCH RELACÍ

NÍZKONÁKLADOVÉ A VELMI PŘÍMOČARÉ ŘEŠENÍ

NEVYŽADUJE ŽÁDNOU ZMĚNU V POSTUPECH SPRÁVY SYSTÉMŮ

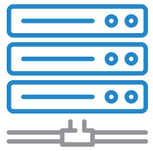
Srozumitelná kontrola činností privilegovaných uživatelů je jednou z nejdůležitějších součástí firemních bezpečnostních opatření a auditování privilegovaného přístupu uživatelů je vyžadováno mnoha různými průmyslovými předpisy.

Nástroj **Ekran System** naplňuje tyto potřeby tím, že v informačním systému ustavuje proces trvalého průběžného monitorování činností administrátorů. Řešení může být snadno nasazeno na kritických serverech a od té chvíle **poskytne detailní videozáznam** všech nebo jen vyjmenovaných uživatelských relací.

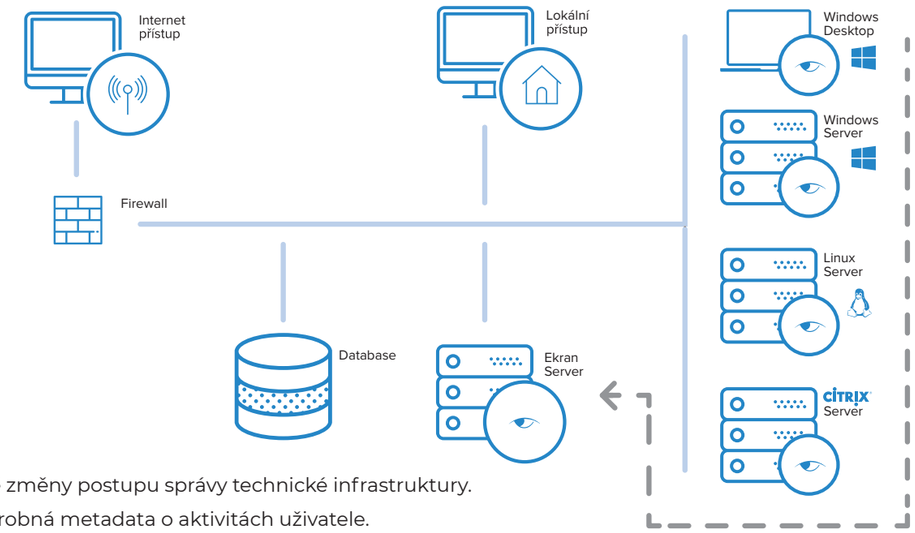
Video formát je indexován a díky metadatům o aktivním okně, spuštěném systémovém procesu či o administrátorem provedeném příkazu supervizor rychle vykoná rámcovou analýzu i několikahodinové relace. Nástroj podporuje **sledování aktuálního průběhu živé relace** a notifikace podezřelých činností. Pokročilý režim **ochrany agenta** zabrání neoprávněným pokusům o jeho zastavení nebo odinstalaci. Nástroj může též vynutit **druhou úroveň ověření uživatele** při přihlášení sdílenými systémovými účty, jako jsou např. „admin“ nebo „root”.

PODPOROVANÉ PLATFORMY:

- **Microsoft Windows** s nahráváním místních, vzdálených i terminálových relací. Nástroj umožňuje též monitorovat aktivitu uživatelů v aplikacích publikovaných v **Citrix XenApp** a virtuální desktopy **XenDesktop.**
- **Linux and Unix** servery, na kterých jsou zaznamenávány Telnet a SSH relace, včetně všech uživatelem spuštěných příkazů.

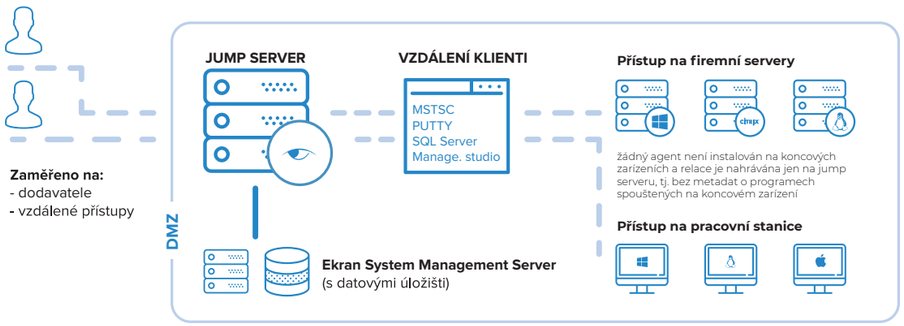


OBVYKLÝ ZPŮSOB NASAZENÍ



- Nevyžaduje žádné změny postupu správy technické infrastruktury.
- Shromažďuje podrobná metadata o aktivitách uživatele.
- Minimální dopad na výkon.
- Snadná údržba.

NAHRÁVÁNÍ JEN NA PŘÍSTUPOVÉM SERVERU



Chráněný okruh

- Jedná se o bezagentský režim, agent je instalován jen na přístupovém, tzv. jump serveru
- Centrální Ekran server může být provozován v clusteru, tj. v režimu vysoké dostupnosti.
- K dispozici je i "multi-tenant" instalace.

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

DATA SYS

ELISA

- automatizované vyhodnocování logů
- robustní noSQL databázové jádro
- podpora standardních protokolů
- nízké pořizovací i provozní náklady
- zachování struktury původní události
- líbivé webové uživatelské rozhraní
- extrémní škálovatelnost a HA
- vysoký výkon (až 6000 eps)

DATASYS ELISA je robustní a 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.

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.

elasticsearch

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.

VÝZNAČNÉ VLASTNOSTI PROGRAMU NXLOG:

- 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)

NXLog ENTERPRISE EDITION

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

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!**