**1. 4. 2022 00:00 – 30. 4. 2022 23:59**

**Bezpečnostní zpráva**

**Vyhodnocení kybernetických bezpečnostních událostí**

**Pro zákazníky**

**Vysoké školy v projektu CRP-KYBER22**

Za tým support **EDUSOC**:

Ing. Karel Šimeček, Ph.D. - VŠE

Ing. Pavla Němcová - MENDELU

RNDr. Martin Laštovička, Ph.D. - MUNI

Datum vytvoření: **9. 5. 2022**

verze 1.0

**Obsah:**

Obsah

[1 Evidence změn 3](#_Toc103072464)

[2 Zkratky 3](#_Toc103072465)

[3 Manažerský souhrn 4](#_Toc103072466)

[3.1 Evidované bezpečnostní incidenty 4](#_Toc103072467)

[3.2 Barevně označený text ve zprávě prezentuje důležitost nálezu 4](#_Toc103072468)

[3.3 Souhrn 4](#_Toc103072469)

[4 Systém Network Anomaly Detection 6](#_Toc103072470)

[4.1 Síťové události 7](#_Toc103072471)

[5 Authentications – Failed access 8](#_Toc103072472)

[5.1 Neúspěšná přihlášení v Unix prostředí 9](#_Toc103072473)

[5.2 Neúspěšná přihlášení ve Windows prostředí 11](#_Toc103072474)

[6 Assets&Log sources 11](#_Toc103072475)

[6.1 Assets 11](#_Toc103072476)

[6.1.1 Log sources 12](#_Toc103072477)

# Evidence změn

|  |  |  |  |
| --- | --- | --- | --- |
| **Verze** | **Datum** | **Popis změny** | **Provedl** |
| 1.0 | 9. 5. 2022 | Vytvoření dokumentu | Šimeček  Němcová  Laštovička |
|  |  |  |  |

# Zkratky

* ADS – Anomaly Detection System
* BB – Building Block
* BZ – Bezpečnostní zpráva
* CP – CheckPoint
* CRP KYBER22 – Centrální rozvojový projekt
* CVE – Common Vulnerabilities and Exposures
* DNS – Domain Name Service
* DOS – Denial Of Service
* FMC – Flowmon Monitoring Center
* FW – Firewall
* ICMP – Internet Control Message Protocol
* IPAM – IP Address Management
* NAT – Network Address Translation
* NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost
* OS – Operation system
* SIEM - Security Information and Event Management
* SMTP – Simple Mail Transfer Protocol
* SSH – Secure Shell
* TCP – Transmission Control Protocol
* VM – Virtual Machine
* VPN – Virtual Private Network

# Manažerský souhrn

## Evidované bezpečnostní incidenty

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID tiketu | Název bezpečnostního incidentu | Datum otevření | Datum vyřešení | Stav | Řešitel |
| 971502 | *MUNI – SQL injection útok na servery MUNI* | 08.04.2022 13:17 |  | V řešení | T. Plesnik (MUNI)  M. Laštovička (**EDUSOC**) |
| 432 | *VŠE - podezřelá komunikace* | 18.04.2022 16:01 |  | V řešení | K. Šimeček (VŠE)  M. Laštovička (**EDUSOC**) |
| 441 | *MENDELU - komunikace portem 6667* | 26.04.2022 13:31 | 05.05.2022 13:41 | Vyřešen | P. Němcová (MENDELU)  M. Laštovička (**EDUSOC**) |

**Za měsíc duben 2022 nebyl evidován žádný bezpečnostní incident**.

Celkem jsou otevřeny **dva** bezpečnostní incidenty.

**Dále zůstává otevřen Provozní požadavek 390 – měření CPU u Fortinet IPS VŠE.**

## Barevně označený text ve zprávě prezentuje důležitost nálezu

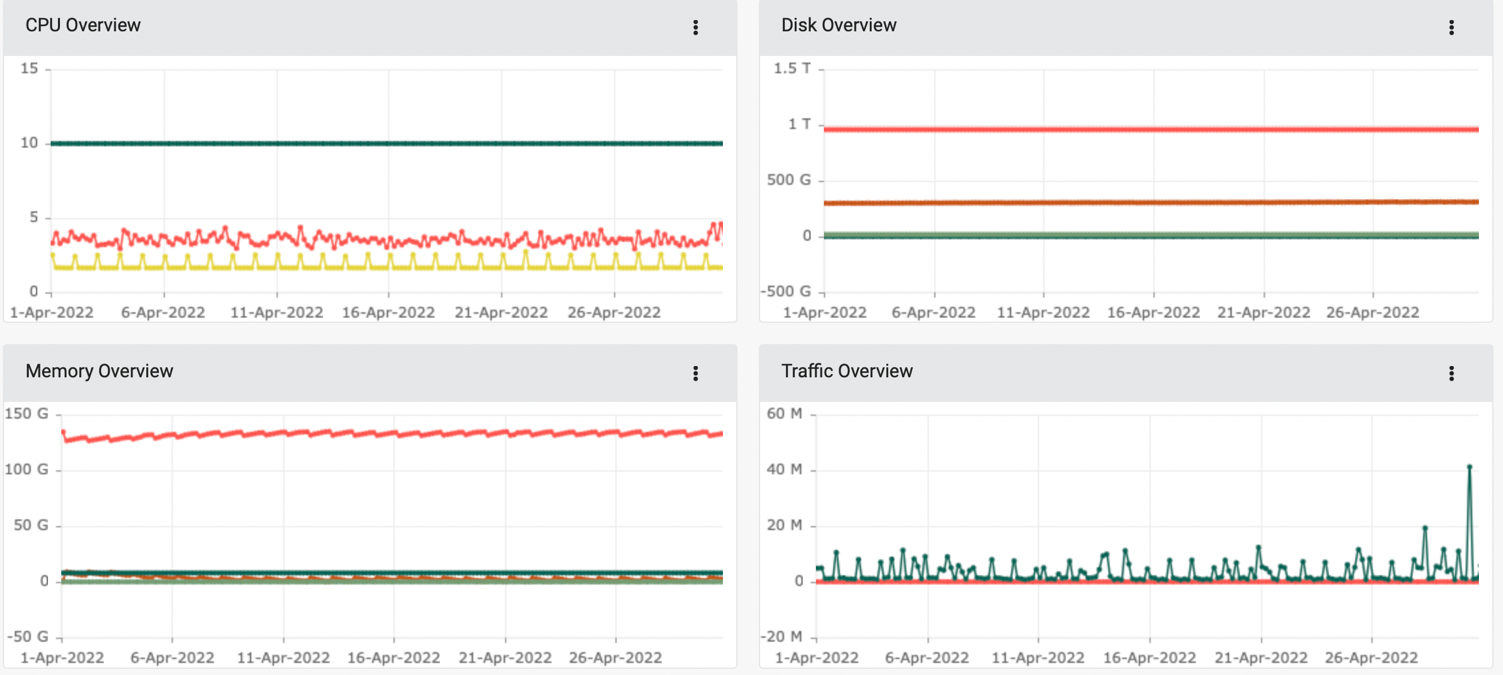
|  |  |
| --- | --- |
| **Barva** | **Důležitost** |
| Červená | Velmi závažný nález |
| Oranžová | Závažný nález |
| Žlutá | Méně závažný nález |
| Zelená | Komentář klienta **EDUSOC** |

## Souhrn

1. Od **8. 4. 2022** jsou na VŠE systémem LOGManager přijímány logy z **Windows** přes agenty BEATS**.** Doporučujeme dopracovat detekci těchto událostí.
2. V LOGManager je patrný **vysoký počet neúspěšných přihlášení** na systém **ADAPPL** (viz kapitola 5.2).
3. Od 25. 4. 2022 se generuje Fortianalyzer VŠE velké množství korelovaných událostí. S pravidly je nutné začít pracovat, aby se zpřesnila detekce systému.
4. Registrujeme velké množství blokované komunikace na porty související s poštou. **Doporučení: Z hlediska kybernetické bezpečnosti doporučujeme bezpečnost prioritně zaměřit na ochranu e-mailové komunikace**.
5. **Dne DD.MM.RRRR byl otevřen požadavek na prověření blokování doménových účtů. Zatím se nepodařilo vyřešit automatické zamykání doménových účtů.**
6. Věnujte pozornost provoznímu monitoringu.
7. ESET antivirová ochrana – nastaveno zasílání syslog logů do LOGManageru.
8. Aktivace korelačního pravidla 30 neúspěšných přihlášení/5minut v systému LOGManager.

# Systém Network Anomaly Detection

Stav systému Greycortex k datu 1. 5. 2022.



Uložená data jsou v systému Greycortex k dispozici od 5. 3. 2021, retence dat je tedy přes 12 měsíců. Starší data jsou k dispozici už jen jako statistika.

Jednotlivé zdroje systému jsou používány v akceptovatelných limitech.

Aktuální verze systému:

Greycortex 3.7.0 – možnost aktualizace na 3.8.0.

NEW FEATURES 3.8.0:

* Zavedení Asset Discovery
* Spojení událostí s MITTRE Attack framework
* Lepší identifikace sítí a subsítí
* Vylepšení modelů analýzy a detekce
* Vizualizace vztahů aktiv v širším kontextu

Lze doporučit upgrade SW na verzi 3.8.0.

## Síťové události

Tato kapitola uvádí zaznamenané události v datové síti pro analýzu příčin vzniku nebo k posouzení rizikovosti dopadů na připojená zařízení či jimi zajišťované služby a procesy.

Obsah obrázku stůl

Popis byl vytvořen automaticky

Ve sledovaném období jsou detekované dvě významné události SSH port Sweep a SSH Bruteforce Attack. Obě události spadají do aktuální situace v kybernetickém prostředí.

Zajímavostí je detekce exploit zranitelností Apache log4j na kterou upozorňuje NÚKIB od prosince 2021, především jde o události:

* Exploit: **Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (Outbound) (CVE-2021-44228)**
* Exploit: **Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (CVE-2021-44228)**
* Exploit: **Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)**

Jejich detekce začala **1.4.2022** a zdrojovými systémy jsou:

* **vproxy3.vse.cz** **146.102.22.85** v síti VMWare (146.102.22.0/24) na protokolu NFS.
* **node403.vse.cz** **146.102.22.43** v síti VMWare (146.102.22.0/24) na protokolu iSCSI.

Detekce je události je vázana na komunikaci uvedených systémů se zálohováním na serveru **Blatouch**.

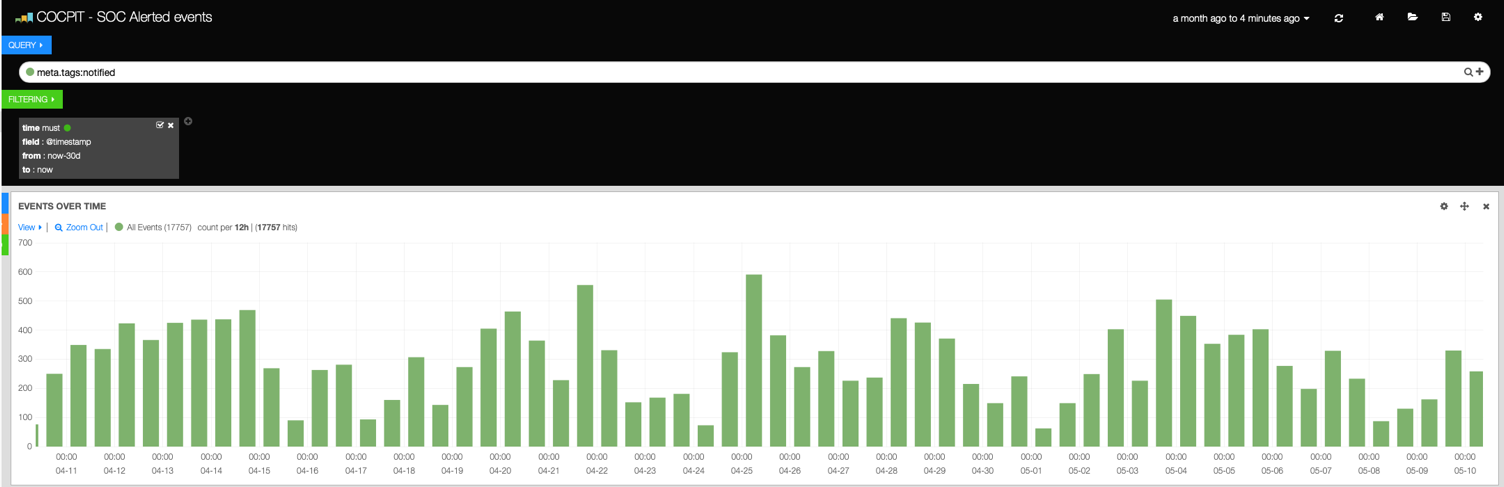
**Hypotéza:** Jde o **False-Positive Alarm** neboť na souborovém disku uvedených zařízení je zřejmě v konfiguračním souboru bezpečnostního systému vložen obdobný detekční pattern jako v Greycortex. Při zálohovacím procesu probíhá přenos dat přes síť v otevřené podobě a network anomaly detection zachytil nějakou část detekčního vzorce.

Prosím přes **grep** prověřit nález soubor obsahující vzorec: **pcre:"/^(l|r|d|\x24\x7b(lower|upper)\x3a(l|r|d)\x7d)(d|n|m|\x24\x7b(lower|upper)\x3a(d|n|m)\x7d)(a|i|s|\x24\x7b(lower|upper)\x3a(a|i|s)\x7d)(p|\x24\x7b(lower|upper)\x3a(p)\x7d)/Ri"**

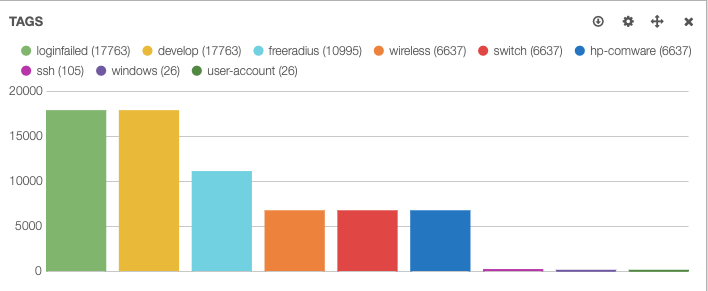
# Authentications – Failed access

Tato kapitola se věnuje analýze neúspěšných přihlášení, především anomáliím poukazující na provozní problémy v prostředí.

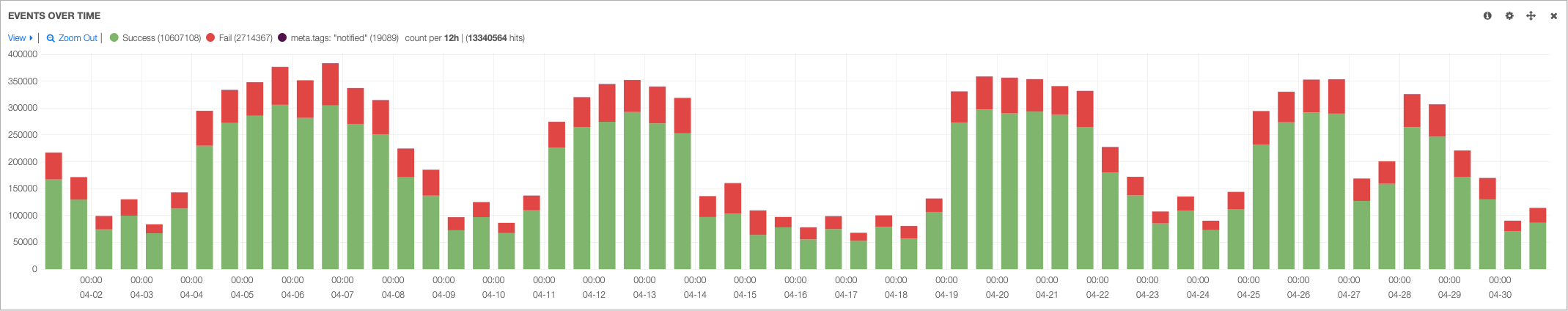
Trend průběhu alertovaných událostí pro pravidlo **30 neúspěšných přihlášení v intervalu 5 minut**.

****

Trend vykazuje neobvyklé charakteristiky. Na následujícím grafu je zajímavostí od událostí neúspěšných přihlášení z **unix prostředí SSH** a taktéž i z **Windows prostředí**. V dalších kapitolách bude tyto události více rozebrány.

****

Dominantním problém s přihlašováním je v síťové infrastruktuře, především WiFi prostředí, který je dán provozní povahou VŠE umožňující studentům přístup k WiFi přes eduroam. Následující graf ukazuje trend poměru úspěšných přihlášení (zelená barva) k neúspěšným přihlášením (červená barva).



Trend reflektuje pracovní a volné dny. Zatím není řešitelné zmenšit trend neúspěšných přihlášení k eduroam, protože jde o projev slabiny principu BYOD, který nelze systémově řešit. Možnou cestou je hlubší osvěta na uživatele s podporou zveřejněných pokynů jak si správně nakonfigurovat vlastní zařízení pro připojení k eduroam.

Doporučujeme:

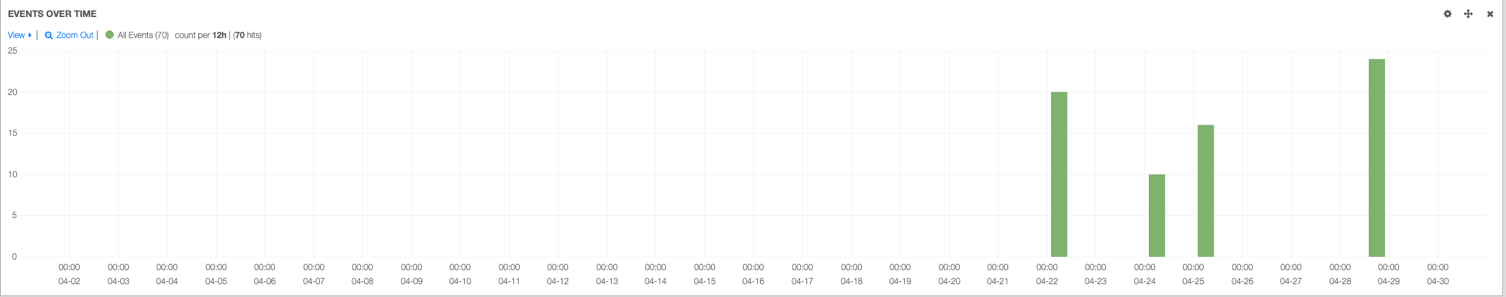
* sledovat i velké anomálie, tj. delší interval neúspěšných pokusů daného zařízení či uživatele nebo více jak
* kontaktovat uživatele zařízení na obrázku níže, především uživatele **mora13, fabm04, bora15, hold09, patp02, kovk02, seda07**, kteří mohou mít chybnou či nekorektní konfigurace svého zařízení (telefon, notebook, tablet).

Obsah obrázku stůl

Popis byl vytvořen automaticky

## Neúspěšná přihlášení v Unix prostředí

Za období duben 2022 byly detekovány 4 alerty s neobvyklými průběhem neúspěšných přihlášení, viz graf



Zajímavostí je analýza neúspěšných uživatelů, především účet **admin, root, adm** a účty obsahující čísla, viz tabulka.

Obsah obrázku stůl

Popis byl vytvořen automaticky

**Hypotéza:**

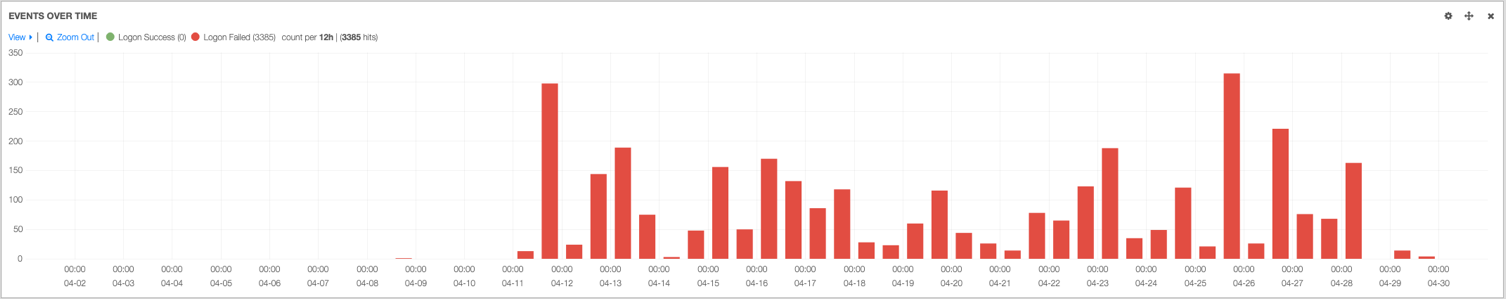
Čísla se v username objevují v důsledku selhání lidského faktoru, kdy uživatel místo username vkládá své skutečné heslo.

Doporučení pro Manažera KB:

Pro účty **admin, root, adm** přimějte jejich vlastníky změnit neprodleně heslo s vyšší silou hesla. J

## Neúspěšná přihlášení ve Windows prostředí

Za období duben 2022 byl detekován fenomén s neobvyklými průběhem neúspěšných přihlášení, viz graf



Příčinou je počítač **ALIENWARE-17-R4** od uživatelky [guoz00@vse.cz](mailto:guoz00@vse.cz), více viz grafy

|  |
| --- |
| **Obsah obrázku text  Popis byl vytvořen automaticky** |
| **Obsah obrázku text  Popis byl vytvořen automaticky** |

Doporučení pro Manažera KB:

Kontaktujte uživatelku **guoz00**, ať se neprodleně dostaví na *Centrum informatiky, Centrum podpory* pro doladění konfigurace jejího počítače, který negativně ovlivňuje server **ADAPPL**.

# Assets&Log sources

## Assets

V Greycortex je k **30. 4. 2022** evidováno 2479 unikátních Assets v kategoriích podle Operačního systému, dle tabulka níže.

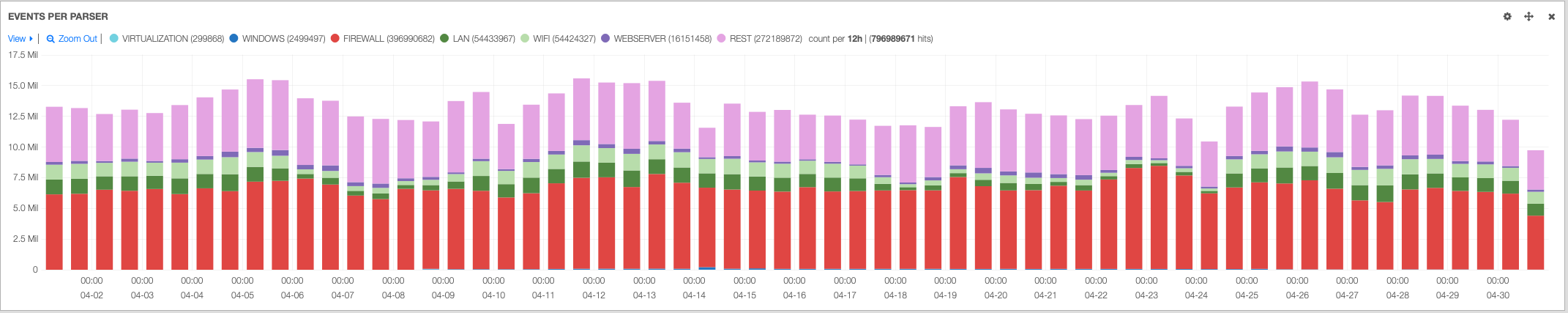


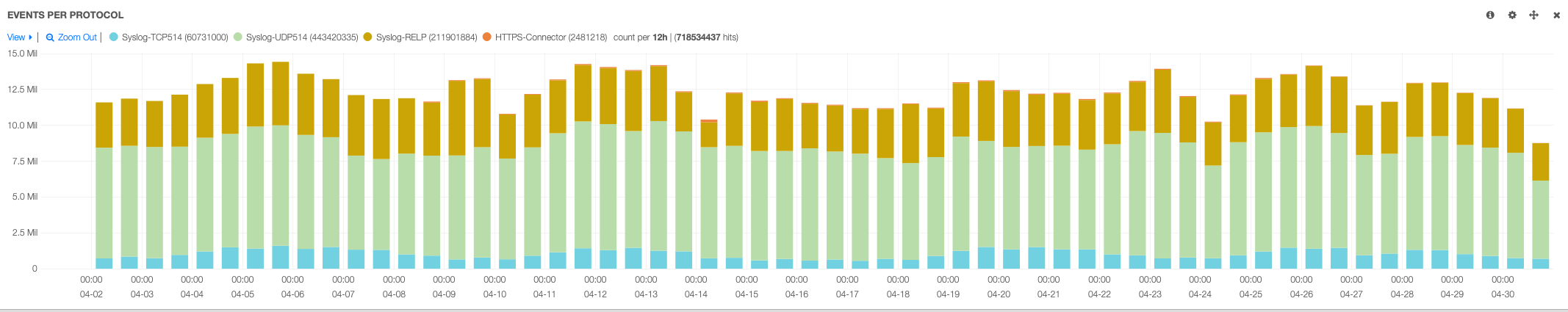
Systém Greycortex nemonitoruje kompletní sítě VŠE a pro lepší proces **inventory aktiv** doručujeme sledování kompletního rozsahu sítí.

### Log sources

Celkem je v LOGManager nakonfigurováno **91 Log Sources**. Seznam Log sources je v souboru **„LOGManager-VSE-LOG\_Sources.xlsx”**

Trendy počtu záznamů v průběhu dubna 2022 ukazují následující grafy.





Doporučujeme pokračovat v připojování dalších zdrojů log záznamů a aktivaci dalších korelačních pravidel v LOGManageru.