PROJEKT

Multitenantné operačné centrum kybernetickej bezpečnosti riešené
ako otvorená cloudová služba s prvkami strojového učenia

Previazané s balíkom KPB1 – Návrh virt. riešenia

Previazané s výstupom
V3 – Popis vybraného riešenia spĺňajúceho stanovené kritéria

typ – dokumentácia

Analýza III.

Analýza nástrojov zberu logov pre potreby NOC a SOC centra v aplikácii na menšiu spoločnosť

OBSAH

1 ANALÝZA

1.1 POPIS TÉMY

Moderné IT infraštruktúry, aj v menších organizáciách, pozostávajú z rastúceho počtu vzájomne prepojených komponentov: sieťových zariadení, serverov, operačných systémov a aplikácií. Každý z týchto prvkov neustále generuje záznamy o svojej činnosti – logy. Tieto logy obsahujú cenné informácie o stave systému, výkone, chybách, používateľskej aktivite a potenciálnych bezpečnostných hrozbách. Bez systematického prístupu k ich zberu a analýze však organizácie čelia zásadnému problému: nedostatku prehľadu a viditeľnosti do vlastnej infraštruktúry.

Na riešenie týchto výziev a zabezpečenie proaktívneho riadenia IT vznikajú špecializované tímy: Network Operations Center (NOC) a Security Operations Center (SOC). NOC sa primárne sústredí na zabezpečenie prevádzkovej stability, dostupnosti a výkonu IT služieb. Jeho cieľom je monitorovať infraštruktúru, rýchlo identifikovať a riešiť prevádzkové problémy a optimalizovať výkon. SOC sa naopak zameriava na kybernetickú bezpečnosť. Monitoruje systémy na prítomnosť hrozieb, deteguje podozrivú aktivitu, analyzuje bezpečnostné udalosti a koordinuje reakciu na incidenty s cieľom minimalizovať škody.

Aby mohli NOC a SOC efektívne plniť svoje poslanie, potrebujú nepretržitý prísun presných a včasných informácií o dianí v infraštruktúre. Práve tu zohrávajú kľúčovú úlohu systémy na správu logov (log management). Ich primárnou funkciou je centralizovať zber logov z rôznorodých zdrojov (siete, servery, aplikácie) na jedno miesto.

1.2 ŠPECIFIKÁCIA PROBLÉMU

Katedra historicky prevádzkovala alebo skúšala viacero log systémov. V poslednej dobe začína budovať NOC a SOC centrá, pre ktoré treba spraviť rozhodnutie, aké riešenie finálne vybrať. Cieľom projektu je systematicky analyzovať, utriediť a porovnať vhodnosť vybraných riešení za účelom vytvorenia systému na zber, archivácie a analýzu logov sieťových a serverových entít na KIS FRI UNIZA na základe požiadaviek. Predpoklad je, že logy budú zbierané z rôznych zariadení a rôznych operačných systémov, ktoré budú posielané na centrálny logovací server, na ktorom budú pracovať administrátori a operátori NOC a SOC centra. Medzi vybrané analyzované riešenia patrí:

- Syslog-ng
- Graylog
- Logstash
- Loki environment

2 CIELE PRÁCE

2.1 CIELE RIEŠENIA

V rámci projektu sme plnili niekoľko cieľov, medzi ktoré patria:

- Oboznámenie sa s princípmi fungovania SOC a NOC centier a definovanie požiadaviek pre tieto centrá. Taktiež bolo potreba preštudovať už existujúce riešení ktoré sa prevádzkovali na fakulte obsiahnuté v diplomových prácach ktoré spísali Ing. Droždík a Ing. Dočár
- Výskum logovacích nástrojov, preštudovanie oficiálnych dokumentácií, recenzii a dostupných štúdií. Hlavný význam bol pochopiť ako tieto nástroje fungujú a aké sú ich funkcie a prípadné obmedzenia. Medzi tieto nástroje patria:
  - Syslog-ng
  - Graylog
  - Logstash
  - Loki environment
- Definovanie kritérií pre porovnávanie jednotlivých nástrojov, aby sme tieto nástroje vedeli porovnať, a vybrať vhodný nástroj pre náš účel
- Otestovanie a konfigurácia jednotlivých nástrojov v testovacom prostredí pre lepšie pochopenie fungovania a implementácie.
- Samotné porovnávanie jednotlivých nástrojov na základe kritérií ktoré sme si definovali a finálne vyhodnotenie

3 VÝSLEDKY PRÁCE

3.1 OBOZNÁMENIE SA S PRINCÍPMI FUNGOVANIA SOC A NOC

3.1.1 Security Operation Center (SOC)

Pomocou SOC (Security Operation Center) môže organizácia monitorovať a manažovať sieťovú prevádzku a hľadať hrozby – je zameraný viac na bezpečnosť. Okrem monitorovania je SOC zameraný aj na riešenie incidentov, vyhľadávanie potenciálnych hrozieb a prevenciu potenciálnych útokov.

Hlavné úlohy SOC:

- Monitorovanie správania sa sieťovej prevádzky
- Udržiavanie záznamov o aktivitách a komunikácií v prevádzke
- Hodnotenie rizika/závažnosti incidentov
- Reakcia na incidenty
- Vyšetrovanie hlavnej príčiny vzniku incidentu

Nástroje pre SOC

SOC používa pre monitorovanie siete rôzne nástroje ktoré slúžia na analyzovanie dát zo sieťovej prevádzky naprieč celou organizáciou. Tiet nástroje spadajú do nasledujúcich kategórií:

- SIEM systémy (Security Information and Event Management)
- IDS (Intrusion detection systems)
- Endpoint detection and response (EDR) riešenia

SIEM systémy slúžia na manažovanie logov a sú kombináciou Security information management (SIM) a Security event management (SEM). Tieto nástroje zaručujú monitorovanie a analýzu bezpečnostných udalostí siete v reálnom čase.

Medzi najpoužívanejšie open source SIEM nástroje patria:

- OpenSearch
- OSSEC
- SecurityOnion
- Wazuh
- OSSIM
- Prelude

IDS sú nástroje pre sieťovú bezpečnosť, ktoré monitorujú sieťovú prevádzku a zariadenia v sieti a odhaľujú škodlivé a podozrivé aktivity a porušovanie bezpečnostných politík. Sú to zvyčajne softvérové aplikácie, ktoré sa môžu nachádzať na koncových zariadeniach, zariadeniach určených na monitorovanie siete alebo v cloude. Pri odhalení podozrivej prevádzky posielajú alerty. Taktiež si vedú záznamy o bezpečnostných incidentoch alebo tieto záznamy posielajú SIEM systému vo forme logov.

IDS nie sú samostatné nástroje, ale sú súčasťou iných bezpečnostných systémov:

- IDS a SIEM
- IDS a IPS (Intrusion Prevention Systems)
- IDS a firewalls

EDR sú riešenia pre sieťovú bezpečnosť, ktoré monitorujú užívateľské zariadenia, odhaľujú a riešia kybernetické hrozby ako napríklad ransomware alebo malware. Slúžia ako prvá línia ochrany vďaka pokročilému antivírusu a antimalware ochrane. Narozdiel od bežného antivírusu ktorý má prístup k databáze už objavených hrozieb vie EDR odhaľovať ešte nepoznané hrozby.

Medzi populárne open source EDR nástroje patria:

- OSSEC
- TheHive Project
- osQuery
- SNORT

3.1.2 Network Operation Center (NOC)

NOC (Network Operation Center) slúži pre sieťových administrátorov na monitorovanie stavu siete a jej zariadení – je zameraný viac na chod siete. Hlavnou úlohou SOC je monitorovanie zdrojov využívaných v sieti a staranie sa o chod siete, riešiť výpadky siete a efektivitu.

Hlavné úlohy NOC:

- Aktualizácia, odstraňovanie problémov a inštalácia softvéru na systémoch pripojených k sieti
- Správa IT infraštruktúry a zariadení
- Zálohovanie dát a zabezpečenie ich prístupnosti v sieti
- Monitorovanie firewallov a softvéru na zabezpečenie siete
- Monitorovanie stavu siete vrátane analýzy stavu siete, podávanie správ o výkone a optimalizácia siete
- Obnova siete po prípadnom zlyhaní

Nástroje pre NOC

NOC využíva nástroje pre monitorovanie siete, identifikovanie bottleneckov, manažovanie konfigurácií a automatizovanie riešení na bežné problémy sieťovej prevádzky. Sú to nástroje z kategórií:

- Nástroje na monitorovanie siete
- Network performance analyzers
- Configuration management databases (CMDB)

Nástroje na monitorovanie siete slúžia na zabezpečenie bezproblémovej prevádzky a výkonu siete. Vďaka týmto nástrojom vieme včasne detegovať výpadky a problémy v sieti, monitorovať výkon siete, ako napr. zaťaženie serverov či odozvu. Slúžia aj na analýzu siete a zobrazujú štatistiky o výkone siete. Do

určitej miery vedia sledovať aj bezpečnostné aspekty siete, to je však zväčša práca SOC nástrojov.

Populárne open source nástroje pre monitorovanie siete sú:

- Zabbix
- Nagios
- Icinga
- Prometheus
- OpenNMS
- LibreNMS

Network performance analyzers sú nástroje na analýzu výkonu siete. Sú zamerané hlavne na analýzu kvality sieťových spojení a priepustnosti. Umožňujú podrobnú analýzu toho, ako efektívne sieť funguje, a detegujú zhoršenie výkonu.

Sú to nástroje z kategórií:

- Packet Sniffers
  - Wireshark
- Mapovanie Siete
  - Nmap
- Analýza šírky pásma
  - Wireshark
  - SolarWinds NetFlow
- Testovanie výkonu
  - iPerf
- Manažéri konfigurácie
  - Ansible
  - Puppet
- Revízie bezpečnosti

CMDB je databáza, ktorá ukladá informácie o konfigurácií hardvéru a softvéru pre IT komponenty využívané v organizácií. Sleduje detaily o hardvéri, softvéri, sieťových zariadeniach a ich vzájomných prepojeniach.

Populárne nástroje sú:

- GLPI
- Ralph
- DataGerry
- I-doit
- CMDBuild

3.2 ANALÝZA LOGOVACÍCH NÁSTROJOV

Logovacie systémy slúžia na zber logov z rôznych zariadení. Tieto logy môžu byť posielané na jeden centralizovaný logovací server kde máme celkový prehľad o tom, čo sa v sieti deje.

Medzi nami vybrané logovacie systémy patria:

- Syslog-ng
- Graylog
- Logstash
- Loki enviroment

3.2.1 Syslog-ng

Syslog-ng je nástroj na zber logov na Linuxových alebo UNIX zariadeniach. Tento nástroj je schopný logovať takmer akúkoľvek činnosť na zariadení. Tieto logy môže ukladať lokálne alebo posielať na centralizovaný logovací server.

Funkcie:

- Podpora Syslog protokolu a ďalších vstupných protokolov (napr. TCP, UDP, RELP).
- Filtrovanie, spracovanie a triedenie logov.
- Export logov do rôznych formátov (JSON, CSV, Elasticsearch).
- Šifrovanie a podpisovanie logov pre zabezpečenie integrity.

3.2.2 Graylog

Graylog je open-source platforma na správu a analýzu logov, ktorá pomáha organizáciám zhromažďovať, ukladať a analyzovať logové dáta z rôznych zdrojov. Ponúka výkonné možnosti vyhľadávania a vizualizácie, vďaka čomu je užitočný pre široké spektrum prípadov použitia.

Funkcie:

- Zber logov z rôznych zdrojov
- Spracovanie logov v reálnom čase
- Normalizácia a parsovanie logov
- Pokročilé vyhľadávanie logov
- Alerty a notifikácie pri určených udalostiach
- Vizualizácia dát
- Ukladanie logov
- Bezpečnosť a kontrola prístupu umožňuje prehľadávať logy iba oprávneným užívateľom
- Mnoho pluginov

Graylog používa na ukladanie a vyhľadávanie logov nástroj Elasticsearch. Tiež používa MongoDB databázu pre ukladanie konfigurácií, metadát a informácie o používateľoch.

3.2.3 Logstash

Logstash je open-source nástroj na spracovanie dát, ktorý prijíma, transformuje a odosiela dáta z rôznych zdrojov do rôznych cieľových systémov. Je súčasťou Elastic Stack ktorý zahŕňa aj Elasticsearch a Kibanu. Podporuje zber a transformáciu dát v reálnom čase pomocou modulárnej architektúry s pluginmi pre vstup, filtre a výstup. Bežne sa používa na centralizované logovanie, transformáciu dát a analýzu v reálnom čase. Logstash umožňuje vytvárať pracovné postupy a získavať okamžité poznatky tým, že posiela dáta do systémov, ako sú Elasticsearch alebo PubNub Iluminate, na analýzu.

Hlavné funkcie:

- Zber dát: Logstash dokáže v reálnom čase zhromažďovať a agregovať dáta z viacerých zdrojov. Podporuje širokú škálu vstupných zdrojov vrátane logovacích súborov, databáz, správcových frontov a rôznych cloudových služieb.
- Transformácia: Po získaní dát umožňuje Logstash ich spracovanie a transformáciu pomocou rôznych filtrov. Tieto filtre môžete použiť na čistenie, obohacovanie a úpravu dát pred ich odoslaním na konečné miesto určenia. Bežné transformácie zahŕňajú parsovanie neštruktúrovaných logových dát, pridávanie geografických informácií alebo anonymizáciu citlivých informácií.
- Výstup: Po spracovaní môže Logstash odosielať dáta do rôznych cieľových systémov, ako napríklad Elasticsearch (na ukladanie a vyhľadávanie), do rôznych databáz alebo do iných systémov a služieb.

3.2.4 Loki

Loki je nástroj na správu logov vyvinutý spoločnosťou Grafana Labs. Pomáha zhromažďovať, ukladať a vyhľadávať logy z vašich aplikácií, ale robí to trochu inak ako tradičné logovacie systémy. Väčšina nástrojov na správu logov, ako napríklad Elasticsearch, indexuje jednotlivé logové dáta. To môže byť veľmi náročné na systémové zdroje, najmä keď prichádza množstvo logov.

Loki indexuje len štítky (metadáta) logov—veci ako názov aplikácie, prostredie alebo iné tagy. To znamená, že Loki neindexuje celý obsah logov, čo šetrí veľa úložného priestoru a robí ho oveľa efektívnejším.

Postup spracovania logov:

- Zber logov – pomocou napr. Promtail
- Indexovanie pomocou tagov
- Ukladanie logov na časti pre šetrenie miesta
- Vyhľadávanie logov pomocou tagov

Zvyčajne sa loki používa v kombinácií s **Promtail** na automatický zber logov z prostredia a nástrojom **Grafana** na efektívne zobrazovanie a vizualizáciu logov.

3.3 DEFINOVANIE KRITÉRIÍ PRE POROVNÁVANIE JEDNOTLIVÝCH NÁSTROJOV

Jedným z cieľom bol aj výskum parametrov a kritérií, podľa ktorých môžeme porovnávať spomenuté logovacie systémy. Celkovo sme sa zhodli na 12 parametroch, pričom každý parameter je rozdelený na niekoľko menších častí, ktoré je potrebné zohľadniť.

Medzi vybrané parametre patria:

3.3.1 Výkonnosť

Parametre zamerané na spracovanie dát.

1. **Škálovateľnosť -** Vlastnosť ktorá nám určuje, či logovací systém zvládne očakávaný objem dát zo siete a z akého množstva zdrojov vie systém logy spracovať.
2. **Spracovanie dát –** spôsoby, akými vie systém dáta spracovať, obohatiť o nové informácie, filtrovať, parsovať, odstrániť citlivé informácie z dát, celkovo flexibilita spracovania dát.
3. **Podporované vstupy** - Aké zdroje dát môže systém prijímať? Napríklad: textové logy, JSON, syslog, databázy alebo cloudové služby.

3.3.2 Integrácia

Parametre týkajúce sa integrácie a komunikácie s inými aplikáciami.

1. **Integrácia s inými nástrojmi -** Dokáže systém spolupracovať aj s inými nástrojmi ako napr. SIEM nástrojmi ? Resp. vie im dáta sprístupniť?
2. **Podpora API -** Poskytuje systém rozhranie API pre integráciu s inými aplikáciami alebo automatizáciu procesov?

3.3.3 Prispôsobenie

Parametre týkajúce sa prispôsobeniu

1. **Rozšírenia a vlastné moduly** - Podporuje systém rozšírenia alebo pluginy? Môže si organizácia vytvoriť vlastné rozšírenia na mieru?
2. **Automatizácia a Tvorba skriptov** - Podpora automatizácie niektorých akcií na základe prahových hodnôt alebo iných parametrov

3.3.4 Bezpečnosť

Parametre týkajúce sa bezpečnosti uchovávania, prístupu a prenosu logov.

1. **Bezpečný prenos** - Podporuje systém šifrovaný prenos dát (napr. TLS/SSL)?
2. **Šifrovanie logov pri uchovávaní** - Môžu byť uložené dáta šifrované, aby sa zabránilo neoprávnenému prístupu?
3. **Kontrola prístupu** - Ponúka systém robustné možnosti riadenia prístupu (napr. role-based access control, autentifikáciu používateľov)?

3.3.5 Monitorovanie a analýza

Parametre týkajúce sa monitorovania a prehľadu dát.

1. **Upozornenia** - Funkcia podávania alertov v reálnom čase
2. **Event** – Podávanie upozornení na základe určených požiadaviek
3. **Reporting** - Môže systém generovať prehľadné reporty o stave siete a incidentoch?
4. **Analýza dát** - Ponúka systém nástroje na vizualizáciu dát, ako sú grafy a dashboardy? Je potrebný externý softvér na túto funkcionalitu?

3.3.6 Uchovávanie a správa dát

Parametre týkajúce sa prispôsobenia a ukladania dát a ich spravovanie.

1. **Ukladanie dát** - Aké metódy používa systém na uchovávanie dát ?
2. **Komprimácia dát** - Podporuje systém techniky kompresie na šetrenie úložného priestoru?
3. **Archivovanie dát** - Poskytuje možnosť dlhodobého ukladania dát?
4. **Rotácia dát** - Aké možnosti ponúka systém pre automatickú rotáciu logov na základe času alebo veľkosti?
5. **Vyhľadávanie dát** - Aké efektívne a flexibilné je vyhľadávanie dát (napr. full-textové vyhľadávanie, podpora regulárnych výrazov)?

3.3.7 Používateľská skúsenosť

Parametre týkajúce sa pomoci pre správu systému používateľom.

1. **Používateľské rozhranie a UX** - Má systém vstavané používateľské rozhranie? Je intuitívne a prehľadné? Aké funkcie ponúka rozhranie pre správu systému?

– **Dokumentácia** - Je dokumentácia systému podrobná, aktuálna a ľahko dostupná?

3.3.8 Inštalácia

Parametre týkajúce sa komplexnosti a možnosti inštalácie.

1. **Jednoduchosť inštalácie** - Aké náročné je nainštalovať daný systém ?
2. **Inštalácia do VM/Kubernetes** - Podporuje systém nasadenie do virtualizovaných prostredí alebo kontajnerových platforiem ako Kubernetes?

3.3.9 Údržba

Parametre ktoré určujú náročnosť starania sa o systém.

1. **Upgrade** - Aké náročné je vykonanie aktualizácie na novšiu verziu?
2. **Jednoduchosť konfigurácie** - Aké komplexné je nastavenie systému? Ponúka nástroje na zjednodušenie konfigurácie?

3.3.10 Aktualizácie a podpora

Parametre týkajúce sa podpory systému vývojármi

1. **Aktuálnosť riešenia** - Ako často sú vydávané aktualizácie? Sú vylepšenia a opravy bugov poskytované pravidelne?

3.3.11 Náklady a licencovanie

Parametre týkajúce sa nákladov na prevádzkovanie systému

1. **Licencia** - Aké sú licenčné podmienky (open-source, komerčná licencia, freemium)?
2. **Cena** - Aké sú priame a nepriame náklady na implementáciu, prevádzku a údržbu systému?

3.4 POROVNÁVANIE NÁSTROJOV

Po testovaní a zozbieraní informácií som vytvoril zoznam našich kritérií pre jednotlivé nástroje a priradil im body. Každému kritériu som priradil body na škále od 1 po 10 kde 1 predstavuje najnižšie možné hodnotenie toho, ako moc je parameter vyhovujúci oproti ostatným logovacím systémom a naopak 10 je najviac vyhovujúci. Taktiež som priradil každému parametru váhu od 1 - 10, čo prestavuje hodnotu, ktorá určuje ako moc je pre nás parameter dôležitý (1 najmenej, 10 najviac).

Parameter	Váha	Graylog	Logstash	Loki	Syslog-ng
		Hodnotenie			
Hardvérové požiadavky	8	8	7	9	10
Škálovateľnosť	7	9	8	6	7
Spracovanie dát	6	8	9	6	8
Podporované vstupy	9	8	9	7	9
Integrácia s inými nástrojmi	7	8	9	8	7
Podpora API	6	8	7	8	7
Rozšírenia a vlastné moduly	6	8	9	6	8
Automatizácia a Tvorba skriptov	5	8	7	7	7
Bezpečný prenos	8	9	9	9	9
Šifrovanie logov pri uchovávaní	5	3	3	3	6
Kontrola prístupu	5	8	5	5	5
Upozornenia	1	8	1	1	1
Event	1	8	1	1	1
Reporting	1	6	1	1	1
Analýza dát	1	8	1	1	1
Ukladanie dát	9	7	6	9	7
Komprimácia dát	8	1	1	9	5
Archivovanie dát	7	2	1	9	2
Rotácia dát	7	1	1	9	1
Vyhľadávanie dát	6	8	6	10	1
Používateľské rozhranie a UX	1	9	1	9	1
Jednoduchosť inštalácie	5	7	7	8	8
Inštalácia do VM/Kubernetes	4	8	8	10	7
Upgrade	7	6	6	8	8
Jednoduchosť konfigurácie	7	7	6	7	7
Aktuálnosť riešenia	10	9	8	9	8
Licencia	10	7	9	10	8
Cena	10	5	9	10	8
Spolu		**11.13**	**10.81**	**13.27**	**11.07**

3.4.1 Bodovanie

- **Škálovateľnosť**: Graylog/Loki majú silné klastrovanie. Logstash škálovateľný, ale môže vyžadovať viac inštancií. Syslog-ng zvláda veľa zdrojov.
- **Spracovanie dát**: Logstash má najbohatšie možnosti (pluginy). Graylog/Syslog-ng tiež silné. Loki sa zameriava menej na transformáciu, viac na indexáciu.
- **Podporované vstupy**: Logstash a Syslog-ng veľmi flexibilné. Graylog tiež široká podpora. Loki závisí viac na agentoch (Promtail, Fluentd).
- **Integrácia s inými nástrojmi**: Logstash exceluje v Elastic Stacku. Graylog má dobré integrácie (SIEM, Slack). Loki úzko s Grafanou. Syslog-ng s SIEM.
- **Podpora API**: Graylog/Loki majú REST API pre logy/konfiguráciu. Logstash pre manažment/monitoring pipeline. Syslog-ng pre automatizáciu.
- **Rozšírenia a vlastné moduly**: Logstash a Syslog-ng veľmi silné v pluginoch/moduloch. Graylog podporuje pluginy. Loki cez konfiguráciu agentov.
- **Automatizácia a Tvorba skriptov**: Graylog (streamy, pipeline). Logstash (pipeline logika). Loki (LogQL pravidlá). Syslog-ng (pravidlá, skripty).
- **Bezpečný prenos**: Všetky podporujú TLS
- **Šifrovanie logov pri uchovávaní**: Natívne väčšinou nie (Graylog/Loki/Logstash vyžadujú externé nástroje/disk). Syslog-ng podporuje GPG.
- **Kontrola prístupu**: Graylog má RBAC. Ostatné často závisia od externých systémov (Elastic Stack, Grafana) alebo základných OS/sieťových metód.
- **Upozornenia**: Graylog má natívne. Loki cez Grafana. Logstash/Syslog-ng vyžadujú externé nástroje (Kibana, Grafana atď.).
- **Event**: Rovnako ako upozornenia
- **Reporting**: Graylog má základné (platené lepšie). Loki cez Grafana. Logstash/Syslog-ng potrebujú externé nástroje.
- **Analýza dát**: Graylog má silné možnosti. Loki cez LogQL/Grafana. Logstash/Syslog-ng závisia na cieľovom úložisku/vizualizácii (Elasticsearch/Kibana).
- **Ukladanie dát**: Loki efektívne (chunky, cloud). Graylog (Elastic/OpenSearch). Syslog-ng (databázy, súbory). Logstash len posiela ďalej.
- **Komprimácia dát**: Loki má natívnu podporu. Graylog/Logstash závisí od databázy. Syslog-ng cez externé nástroje (gzip).
- **Archivovanie dát**: Loki (cloud/záloha chunkov). Graylog (závisí od DB, platená verzia). Logstash/Syslog-ng riešené externe (napr. logrotate).
- **Rotácia dát**: Loki má politiky. Graylog/Logstash závisí od DB. Syslog-ng externe.

- **Vyhľadávanie dát**: Graylog (fulltext). Loki (LogQL cez štítky - efektívne). Logstash (cez cieľové úložisko). Syslog-ng (cez externé nástroje).
- **Používateľské rozhranie a UX**: Graylog má silné web UI. Loki cez Grafana (veľmi dobré). Logstash/Syslog-ng nemajú natívne UI (CLI/YAML/integrácie).
- **Jednoduchosť inštalácie**: Loki/Syslog-ng relatívne jednoduché (binárky, balíky, Docker). Graylog vyžaduje DB. Logstash (YAML).
- **Inštalácia do VM/Kubernetes**: Loki je optimalizovaný pre K8s. Graylog/Logstash dobre podporované. Syslog-ng má podporu.
- **Upgrade**: Loki/Syslog-ng relatívne jednoduché. Graylog/Logstash môžu byť náročnejšie pri komplexných nastaveniach/klastroch.
- **Jednoduchosť konfigurácie**: Graylog (web UI + súbory). Loki/Syslog-ng (YAML/konfig. súbory - flexibilné). Logstash (YAML - môže byť komplexné).
- **Aktuálnosť riešenia**: Všetky sú aktívne vyvíjané a pravidelne aktualizované (Graylog veľmi často).
- **Licencia**: Loki (MIT) a Logstash (Open Source - Elastic Lic./Apache) sú najotvorenejšie. Syslog-ng (OSS + PE). Graylog (OSS + Enterprise).
- **Cena**: Loki/Logstash základ zadarmo. Syslog-ng základ zadarmo. Graylog má platenú verziu pre pokročilé funkcie s pomerne vysokou cenou.

ZÁVER

Podľa zozbieraných a kritérií a ich hodnotení môžeme usúdiť, že vhodným kandidátom pre uchovávanie logov je Loki. Exceluje najmä v ukladaní a vyhľadávaní dát a pre analýzu dát sa natívne integruje s rozhraním Grafana, čo je výborný vizualizačný nástroj pre logy a metriky. Celé riešenie je open-source čo je veľká výhoda.

Ako druhý sa umiestnil nástroj Graylog, ktorý má veľmi prehľadné rozhranie a silnú analýzu dát no je menej flexibilný pri šifrovaní úložiska a v otvorenej verzií disponuje iba základnými funkciami. Prechod na platenú verziu ktorá obsahuje množstvo dodatočných funkcií je veľmi drahý.

Tretí sa umiestnil syslog. Napriek tomu to je ale výborný nástroj na spracovanie a odosielanie logov do centrálnych úložísk čo ho robí veľmi vhodným pre použitie spolu s Loki. Je veľmi flexibilný a výkonný pri zbere, smerovaní a filtrovaní logov, má nízke nároky a dobré bezpečnostné funkcie. Chýba mu však UI a pokročilá analýza.

Ako posledný sa umiestnil Logstash. Tento nástroj exceluje najmä v spracovaní dát, je to však hlavne procesor/pipeline a zvyčajne sa integruje v rámci riešenia ELK, ktorý môže byť náročnejší na údržbu ako predošlé riešenia.