Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

SIEM a SOAR

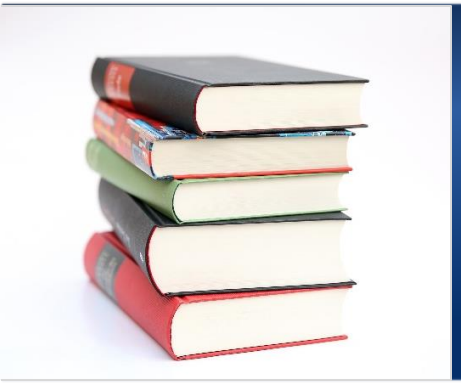
Monitorovanie bezpečnostných udalostí, riešenie incidentov, forenzná analýza (Blok VI)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk



Obsah

- Možnosti práce so sieťovými bezpečnostnými údajmi v nástrojoch pre riadenie bezpečnostných informácií a udalostí (SIEM)
- Možnosti v nástrojoch pre orchestráciu, automatizáciu a reakciu na bezpečnostné incidenty (SOAR)

Security information and event management (SIEM)

Čo je SIEM

SIEM (Security information and event management)

SIEM kombinuje:

- Security information management (SIM)
  - Centrálne ukladanie logov
  - Vykonávanie analýzy nad uloženými dátami
  - Tvorenie reportov
- Security event management (SEM)
  - Monitorovanie v reálnom čase
  - Korelácia udalostí (eventov)
  - Notifikácie

Výsledkom je centrálne miesto pre detekciu, analýzu a reakciu na bezpečnostné incidenty.

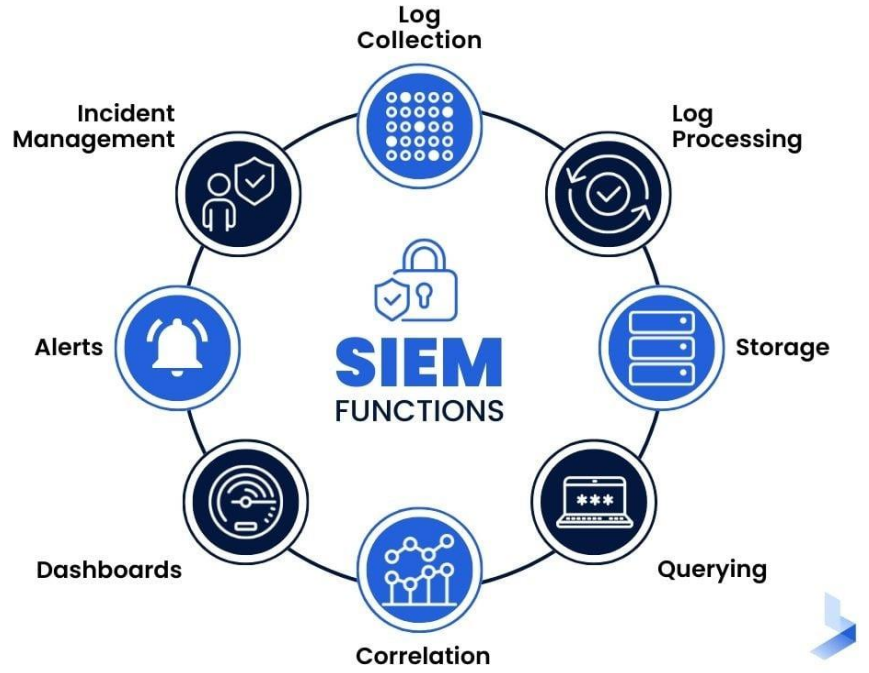
Zdroje dát môžu byť napríklad:

- Sieťové
- Aplikačné
- Hardvérové

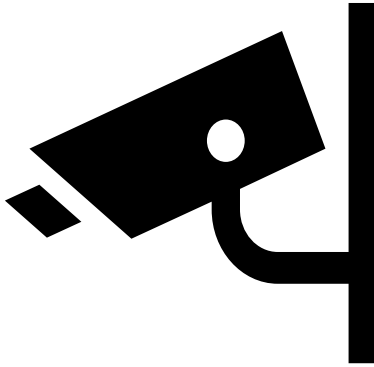
Security information and event management

Prečo potrebujeme SIEM

- Moderné siete generujú obrovské množstvo dát
- Bez centralizácie je práca s nimi náročná, dáta sú neprehľadné, v rôznych tvaroch
- SIEM umožňuje:
  - Agregácia logov z rôznych zariadení a systémov
  - Korelácia udalostí
  - Rýchla reakcia na incidenty



Hlavné funkcie SIEM



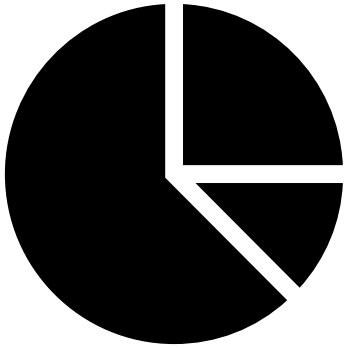
- Zber a normalizácia logov
  - V sieti sa nachádza veľa zariadení, ktoré treba monitorovať. Každé monitorované zariadenie tvorí dáta v rôznych tvaroch / formátoch. Manuálna správa dát je neefektívna, až nemožná.
  - Nutnosť dáta centralizovať. Z jedného miesta máme prístup ku všetkým logom z každého monitorovaného zariadenia.
  - Normalizácia logov umožní sprehľadnenie a jednotný tvar logov.

- Analýza a korelácia udalostí
  - Nad centralizovanými a normalizovanými logmi ide efektívnejšie vykonávať analýzu. Vieme identifikovať normálne a anomálne správanie v sieti alebo zariadeniach.
  - Korelácia udalostí umožňuje spájať viac nezávislých logov do jedného kontextu (napr. viac neúspešných loginov = možný brute-force útok).
- Detekcia anomálií a incidentov
  - Na základe analyzovaného správanie siete vieme vytvoriť detekčné pravidlá na odhaľovanie anomálií a incidentov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Hlavné funkcie SIEM

- Upozornenia a reakcie
  - Pravidlá sa aplikujú na zozbierané dáta. Ak je podmienka splnená, vznikne alert (upozornenie).
  - Alert poskytuje informácie o potenciálnej hrozbe.
  - Typy alertov podľa pravdivosti:
    - **True positive –** Pravidlo spustilo alert, korektne upozorňuje na monitorovanú udalosť. Tento stav je žiadaný
    - False positive – Pravidlo spustilo alert, nastal "planý poplach". Potreba upraviť pravidlo aby sme sa nezahltili falošnými alertami.
    - **True negetive –** Pravidlo nespustilo alert. Nediala sa žiadna nebezpečná udalosť. Tento stav je žiadaný.
    - False negative – Pravidlo nespustilo alert. Diala sa nebezpečná udalosť, len pravidlá ju nezaznamenali. Nevieme o prebiehajúcom útoku / nebezpečných udalostiach.

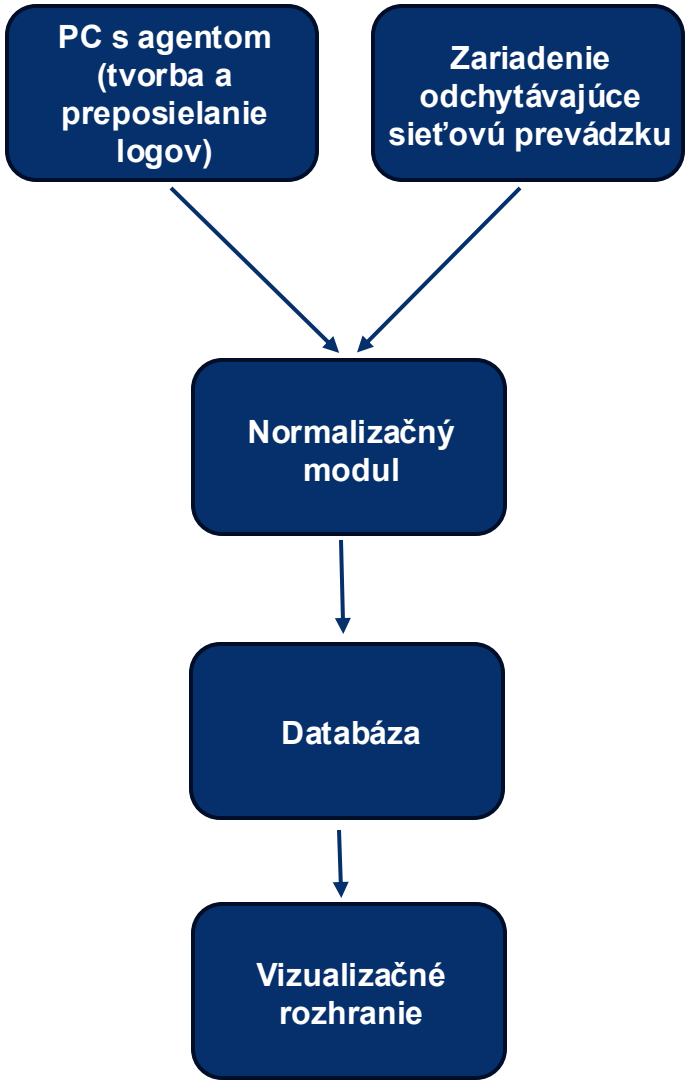


- Reportovanie a vizualizácia
  - Veľké množstvo dáta je vhodné vizualizovať. Na to nám slúžia vizualizačné nástroje. Dáta zobrazujeme v prehľadných dashboardoch, kde sú grafy, tabuľky, zosumarizované dáta... Vizualizácia pomáha rýchlejšie rozpoznať trendy, útoky alebo problémové zariadenia.
  - Dôležitou funkciou je tvorenie reportov. Reporty umožňujú sumarizovať bezpečnostné incidenty a exportovať odchytené dáta na ďalšiu analýzu.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

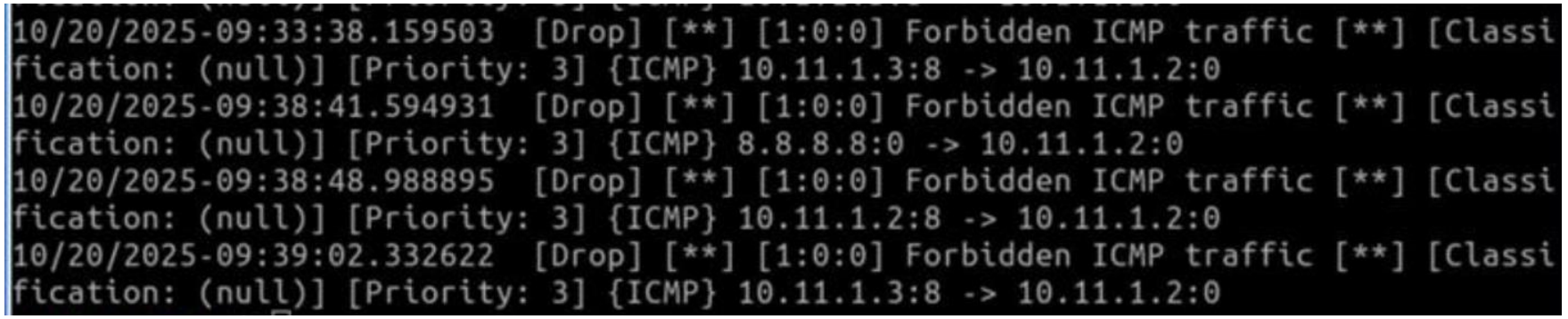
Architektúra SIEM systému

- Komponenty architektúry:
  - Zber dát
    - Odchytávanie sieťovej prevádzky
    - Zbieranie logov z koncových zariadení pomocou agentov
  - Normalizačný modul
    - Zozbierané rôzne dáta normalizuje, upraví do jednotného tvaru
  - Databáza
    - Uchováva normalizované dáta
    - Umožňuje vyhľadávanie a filtrovanie
  - Vizualizačné rozhranie
    - Korelácia a vyhodnocovanie pravidiel
    - Umožňuje zobrazovať, filtrovať dáta



Typy údajov v SIEM

- Systémové logy (napr. Windows, Linux)
  - Logy z koncových zariadení (PC alebo Servery).
  - Napr. prihlásenia používateľov, tvorba/modifikácia súborov, spúšťanie procesov, úprava systémových nastavení, zapnutie/reštart zariadenia...
- Sieťové logy (firewally, IDS/IPS, routery)
  - Logy zo sieťových zariadení
  - Aktivity IDS/IPS systémov (napr. či zariadenie nezablokovalo podozrivú prevádzku)
- Odchytávanie sieťovej prevádzky
  - Zaznamenanie celého toku sieťovej prevádzky, tzv. full packet capture.
- Aplikačné logy (web, databázy, servery)
- Bezpečnostné udalosti (autentifikácie, chyby, prieniky)



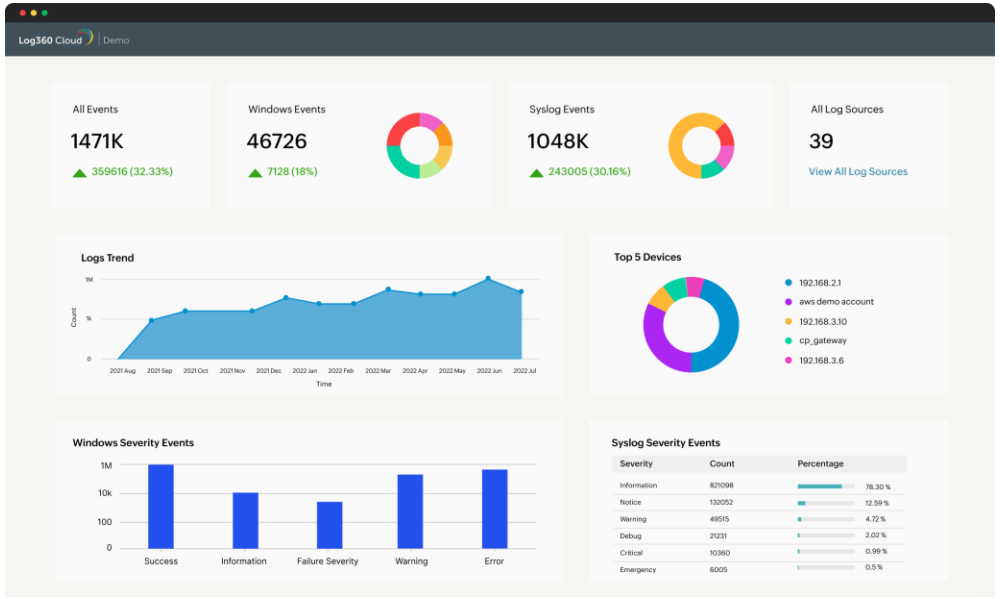
Security information and event management

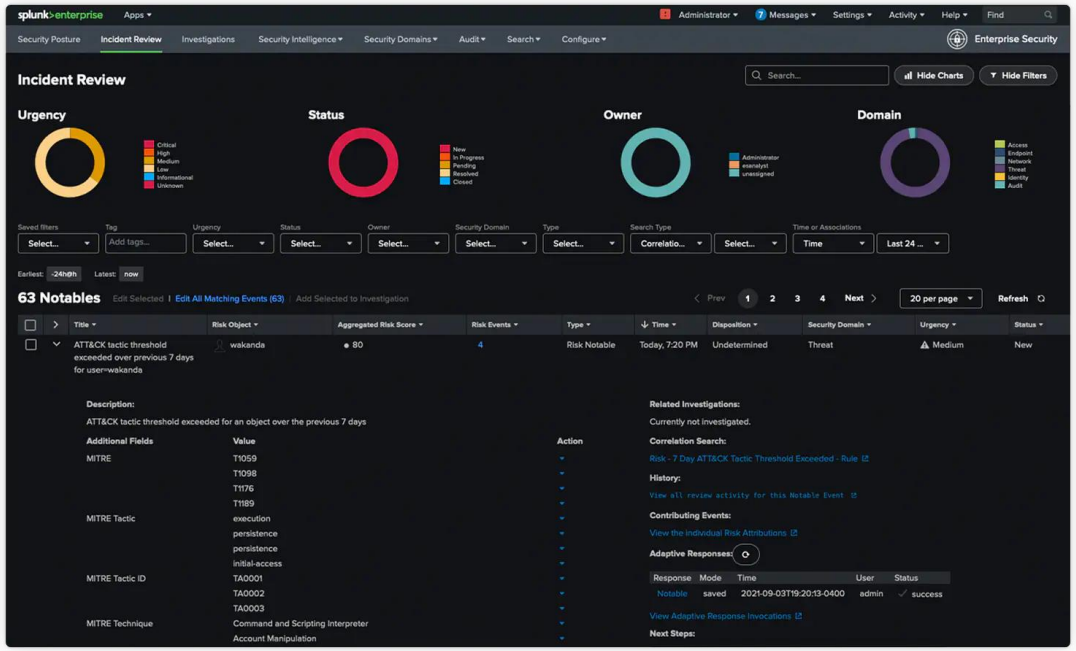
SIEM nástroje - Platené riešenia

SIEM nástroje sú pomerne robustné nástroje. Ich vývoj nie je jednoduchý a mnoho z nich je platených. Licencie sa pohybujú v desiatkach tisíc eur ročne.

Ponúkajú On-premises alebo cloudové riešenia

- On-premises
  - Administrátor si inštaláciu a údržbu riadi sám
  - Sám zodpovedá za fungovanie nástroja
- Cloudové riešenia
  - Inštaláciu a správu nástroja zabezpečuje poskytovateľ nástroja
- Platené SIEM nástroje
  - Splunk
  - Log360
  - eventLog Analyzer
  - IBM QRadar
  - AT&T Cybersecurity AlienVault Unified Security Management
  - Exabeam
  - ...





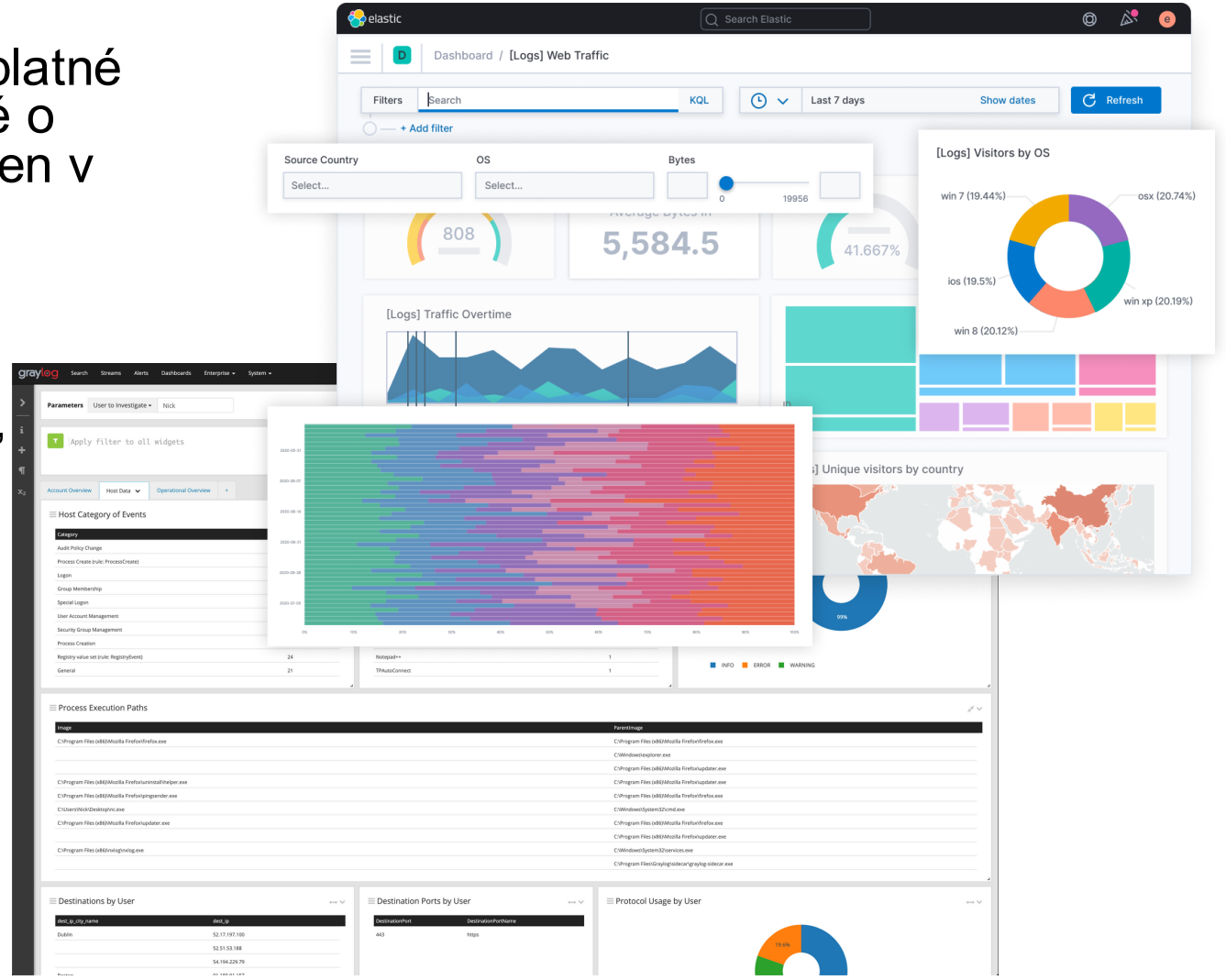
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

SIEM nástroje - Open source riešenia

Open sourcové nástroje ponúkajú aj bezplatné verzie nástrojov. Tie však bývajú ukrátené o rôzne funkcionality, ktoré sa nachádzajú len v platených verziách.

Príkladmi takýchto SIEM nástrojov sú

- ELK stack
  - Sada nástrojov (ElasticSearch, Logstash, Kibana)
    - ElasticSearch - databáza a search engine
    - Logstash – Parsovanie logov
    - Kibana - Vizualizácia zozbieraných dát
- Security Onion
- Wazuh
- Graylog
- ...



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

SIEM pomocou ELK

Elastic Stack

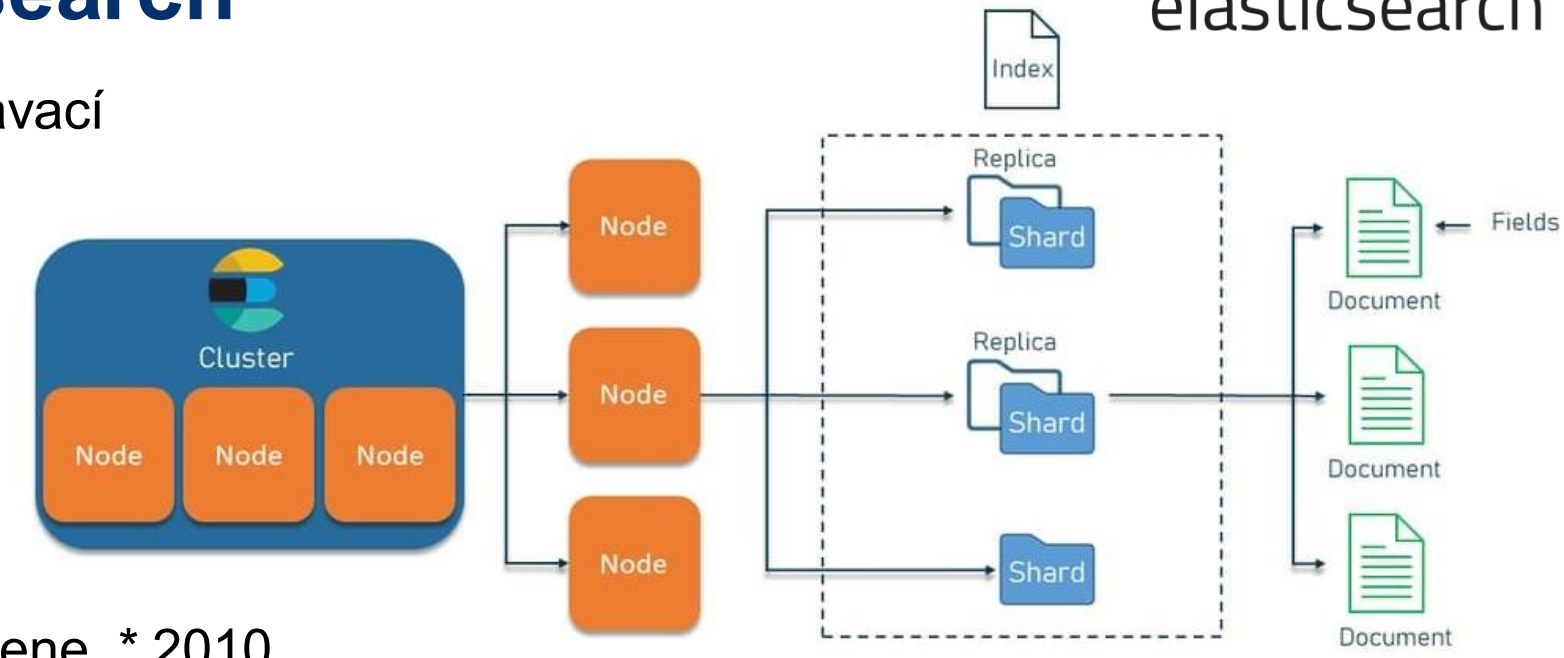
- Elastic je názov spoločnosti, ktorá stojí za produktom Elastic Stack - obsahuje nástroje:
  - Elasticsearch
  - Kibana
  - Logstash
- Pomáhajú používateľom zabezpečene spracovávať dáta
  - z ľubovoľného zdroja
  - v ľubovoľnom formáte

  následne v nich
  - vyhľadávať
  - analyzovať
  - zobrazovať v reálnom čase
- „free and open“ s možnosťou kúpy platených licencií zahrňujúcich doplnkové funkcionality
  - strojové učenie
  - zabezpečenie a reportovanie
- Umožňuje nasadenie v cloude alebo on-premise

ELK stack - Elasticsearch

elasticsearch

- bezplatný distribuovaný vyhľadávací a analytický nástroj
- pre všetky typy údajov vrátane
  - Textových
  - Číselných
  - Geopriestorových
  - Štruktúrovaných
  - aj neštruktúrovaných
- Ukladanie dát v JSON
- ES je postavený na Apache Lucene, * 2010
- Je známy pre svoje
  - jednoduché REST API
  - distribuovanú povahu
  - Rýchlosť
  - Škálovateľnosť
- Clustrovanie => distribúcia dát na viacerých inštanciách Elasticsearch databázy => rozloženie záťaže => rýchlejšie prehľadávanie a spracovanie dát



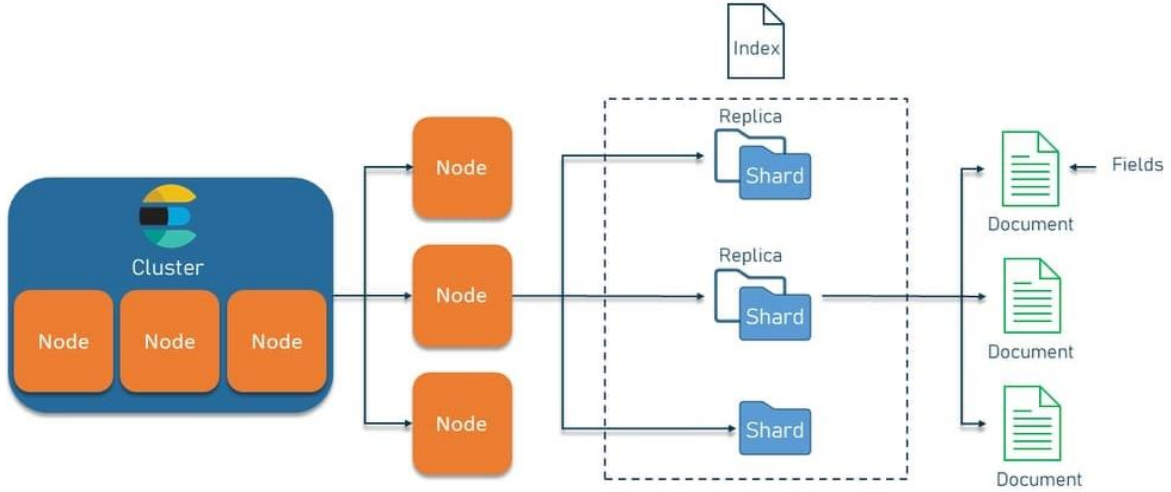
Elasticsearch (pokrač.)

- Prijíma dáta z rôznych zdrojov vrátane
  - Logov
  - systémových metrík
  - webových aplikácií
- Originálne (raw) prijímané dáta sa
  - Parsujú, normalizujú a rozširujú pred tým
  - ako sú indexované v databáze
  - Až následne sa dá spustiť komplexné dopyty (queries) nad týmito dátami a pomocou agregácií načítať komplexné súhrny dát.
- Index je zbierka dokumentov, ktoré navzájom súvisia
- ES ukladá dáta ako JSON dokumenty
- Každý dokument koreluje množinu kľúčov (názvy polí alebo vlastností) s ich zodpovedajúcimi hodnotami (reťazce, čísla, boolovské hodnoty, dátumy, polia hodnôt, geolokačné údaje alebo iné typy údajov)

- ES používa dátovú štruktúru nazývanú inverzný index (inverted index), ktorá je navrhnutá tak, aby umožňovala veľmi rýchle fulltextové vyhľadávanie
  - Inverzný index obsahuje zoznam všetkých jedinečných slov, ktoré sa vyskytujú v ľubovoľných dokumentoch
  - a identifikuje všetky dokumenty, v ktorých sa každé slovo vyskytuje
  - počas procesu indexovania ES ukladá dokumenty a vytvára inverzný index, vďaka ktorému je možné v dokumentoch vyhľadávať takmer v reálnom čase
  - indexovanie sa iniciuje pomocou indexovacieho API rozhrania, prostredníctvom ktorého je možné pridať alebo aktualizovať JSON dokument v konkrétnom indexe
- Index Lifecycle Management (ILM)
  - Cez neho je možné nakonfigurovať politiky pre automatické manažovanie indexov podľa požiadaviek na výkon a veľkosť úložiska

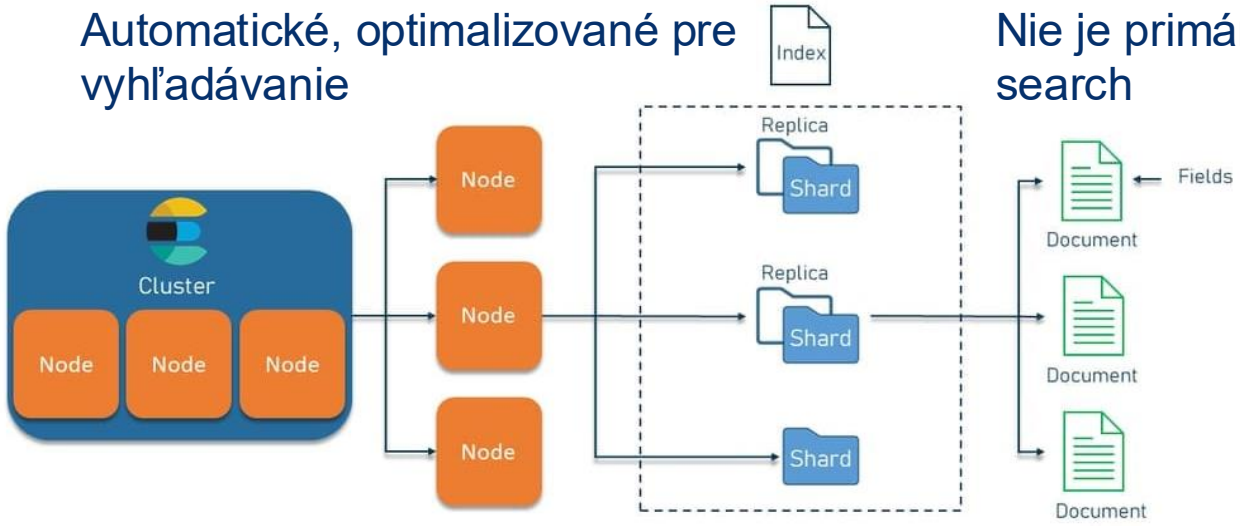
Indexy, shardy, dokumenty, a polia v ES

Termín	Čo to je v ES	Analógia z relačnej DB
Index	Kolekcia dokumentov, kde sa dá vyhľadávať	Tabuľka
Shard	Časť indexu, umožňuje rozloženie dát medzi nody a paralelné vyhľadávanie	Časť tabuľky rozdelená na segmenty
Dokument	Jeden záznam v indexe (napr. logová udalosť)	Riadok v tabuľke
Pole	Vlastnosť dokumentu (napr. `timestamp`, `source_ip`)	Stĺpec v tabuľke



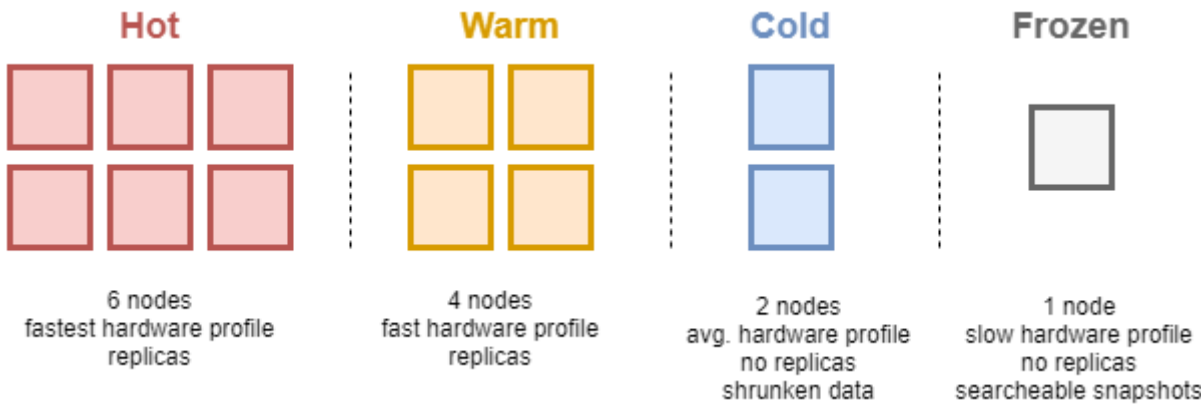
Indexy, shardy, dokumenty, a polia v ES

Vlastnosť	ElasticSearch (ES)	Relačná databáza (RDBMS)
Typ dát	Dokumentovo-orientovaná, JSON formát	Tabuľky s riadkami a stĺpcami
Vyhľadávanie	Fulltextové, veľmi rýchle, analyzované	SQL dotazy, primárne štruktúrované
Štruktúra	Index → dokument → pole	Databáza → tabuľka → riadok → stĺpec
Škálovanie	Horizontálne (shardy a nody)	Väčšinou vertikálne (výkonný server)
Dátová konzistencia	Eventuálna (eventual consistency), prioritizuje rýchlosť	ACID (silná konzistencia)
Použitie	Logging, monitoring, SIEM, fulltext search	Transakčné systémy, ERP, bankovníctvo
Zálohovanie a repliky	Automatické repliky shardov	Zálohy a repliky manuálne nastavené
Indexovanie	Automatické, optimalizované pre vyhľadávanie	Nie je primárne optimalizované pre fulltext search



ELK stack - Elasticsearch

- Cluster – Zoskupenie viacerých ElasticSearch inštancií. Možnosť priradiť inštanciám (vrcholom/nodes) role.
  - Master node - Riadi cluster, zabezpečuje jeho stabilitu, správu a koordináciu
  - Data node
    - Data - univerzálny uzol pre ukladanie dát
    - Content – slúži na uchovávanie statických dokumentov
    - Hot - optimalizovaný pre zápis a čítanie najnovších dát s vysokou aktivitou
    - Warm - určený pre dáta, ku ktorým sa pristupuje menej frekventovane
    - Cold - používa sa na historické dáta s minimálnym prístupom
    - Frozen - slúži na prístup k takmer neaktívnym dátam
  - Ingest - vykonáva predspracovanie dát
- ml - vyhradený pre úlohy strojového učenia
- remote_cluster_client - zabezpečuje komunikáciu s inými Elasticsearch cluster
- transform - slúži na transformáciu existujúcich dát do iných štruktúr

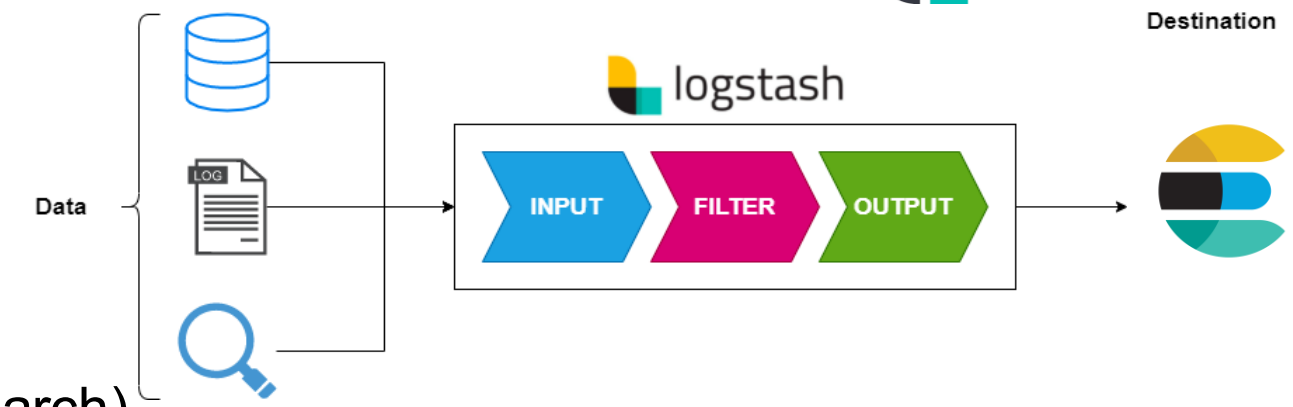


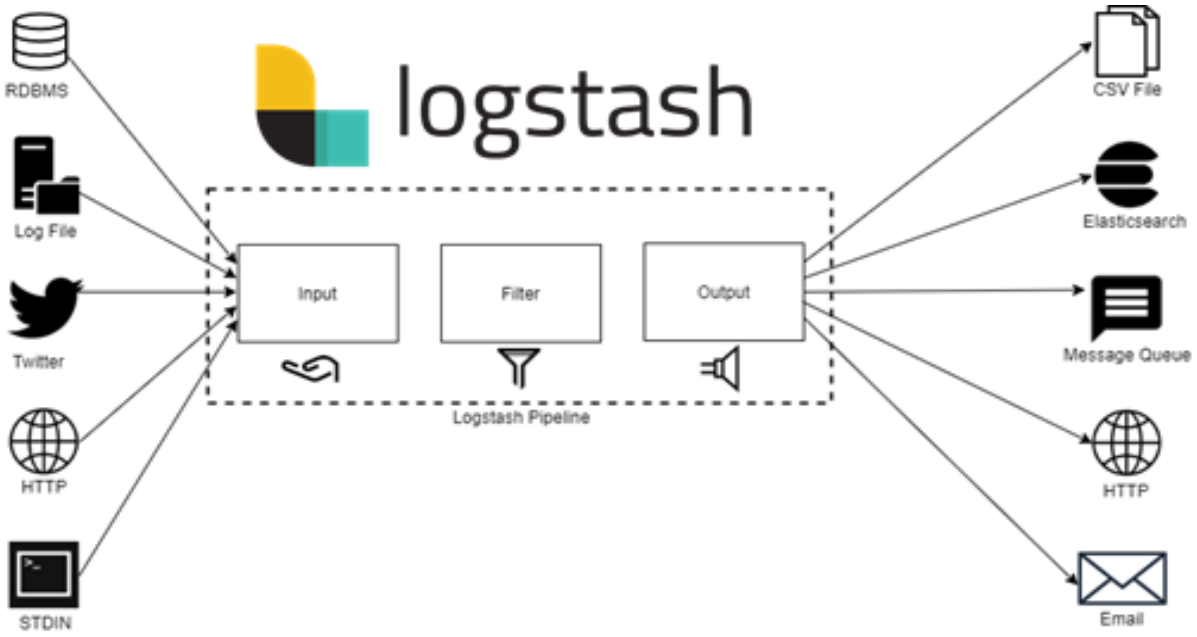
Komunikáciu medzi nodes je potrebné zabezpečiť !

ELK stack - Logstash

- Prijíma údaje z množstva zdrojov (napr. monitorovací agenti)
- Transformuje a normalizuje
- Spracované dáta posiela ďalej (ElasticSearch)
- Logstash proces sa skladá z 3 častí
  - Input – zadefinovanie odkiaľ prijímať dáta
  - Filter - transformácia dát do vhodného formátu
  - Output – kam odoslať dáta
- 200 pluginov a možnosť vytvoriť si vlastné

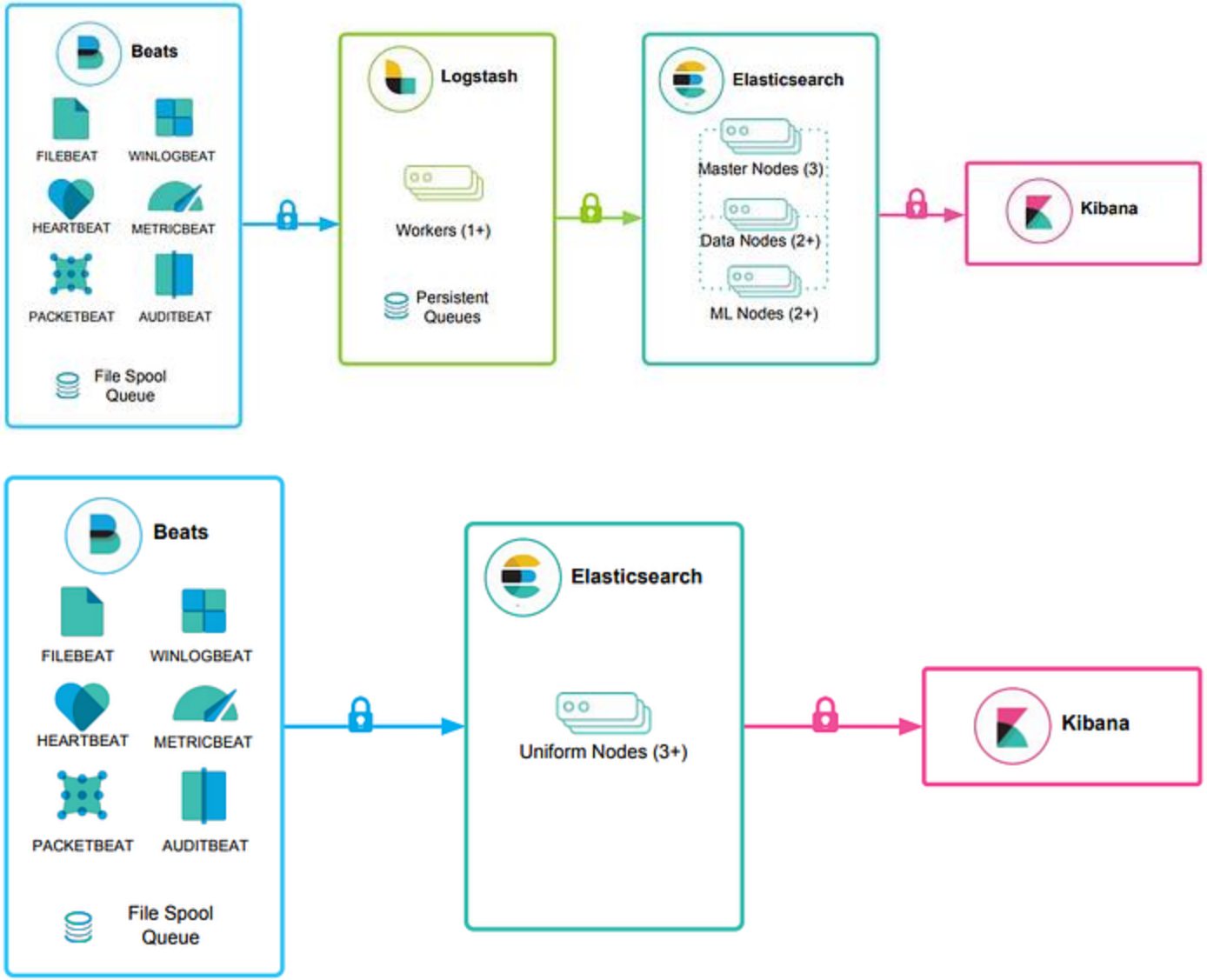
Dáta treba šifrovať pomocou certifikátov od zdroja k logstashu a od logstashu do elasticsearch !





Beats

- Beats je ďalšou súčasťou balíka Elastic.
- Ľahké, jednoúčelové **odosielače dát** sú navrhnuté na inštaláciu na vzdialené počítače, aby preposielali protokoly a metriky priamo do Logstash alebo Elasticsearch.
- **Beats -> Logstash -> Elasticsearch -> Kibana**
- **Beats -> Elasticsearch -> Kibana**



Beats agenti v ELK

Beat	Na čo slúži	Najčastejšie použitie v SOC / IT
Filebeat	Zber logov zo súborov	Aplikačné logy, systémové logy, firewall logy, SIEM ingest
Metricbeat	Zber metrických údajov zo systému	CPU, RAM, disk, sieťové metriky – monitoring serverov
Packetbeat	Zber sieťových tokov a L7 protokolov	Analýza sieťovej komunikácie, detekcia incidentov
Winlogbeat	Zber Windows Event Logs	Účetné udalosti, Windows Security logy, AD monitoring
Auditbeat	Zber bezpečnostných audit udalostí	Integrita súborov, Linux audit, sledovanie procesov
Heartbeat	Kontrola dostupnosti služieb	Ping, HTTP, TCP check – uptime monitoring
Journalbeat	Zber systemd journal logov	Moderné Linux distribúcie (systemd)
Cloudbeat (novší)	Zber cloud security events	AWS, Azure, GCP bezpečnostné konfigurácie
Community Beats	Custom beats vytvorené komunitou, viac ako **70+**	Špecifické logy a metriky pre niche systémy
Elastic Agent (náhrada všetkých Beats)	Unified agent pre všetky dáta	Centrálne riadenie, Fleet management

Beats vs. Elastic Agent – rýchle porovnanie

- **Elastic Agent zvládne:**
  - Logy (náhrada Filebeat)
  - Metriky (náhrada Metricbeat)
  - Sieťovú viditeľnosť (náhrada Packetbeat)
  - Windows eventy (náhrada Winlogbeat)
  - Audit (náhrada Auditbeat)
  - Uptime (náhrada Heartbeat)
    - Endpoint Security / Malware Prevention
    - APM
    - Centrálne riadenie cez **Fleet**

- **Vlastnosti Elastic Agent**
  - Jeden agent = všetko v jednom
  - Centrálna správa cez Kibanu (Fleet)
  - Jednoduché rollouty konfigurácie
  - Autoupdate modulov a integrácií
  - Množstvo hotových integrácií (Cisco, Fortigate, Windows, Linux, AWS, Azure, 365, atď.)
- Moderný štandard odporúčaný Elastic

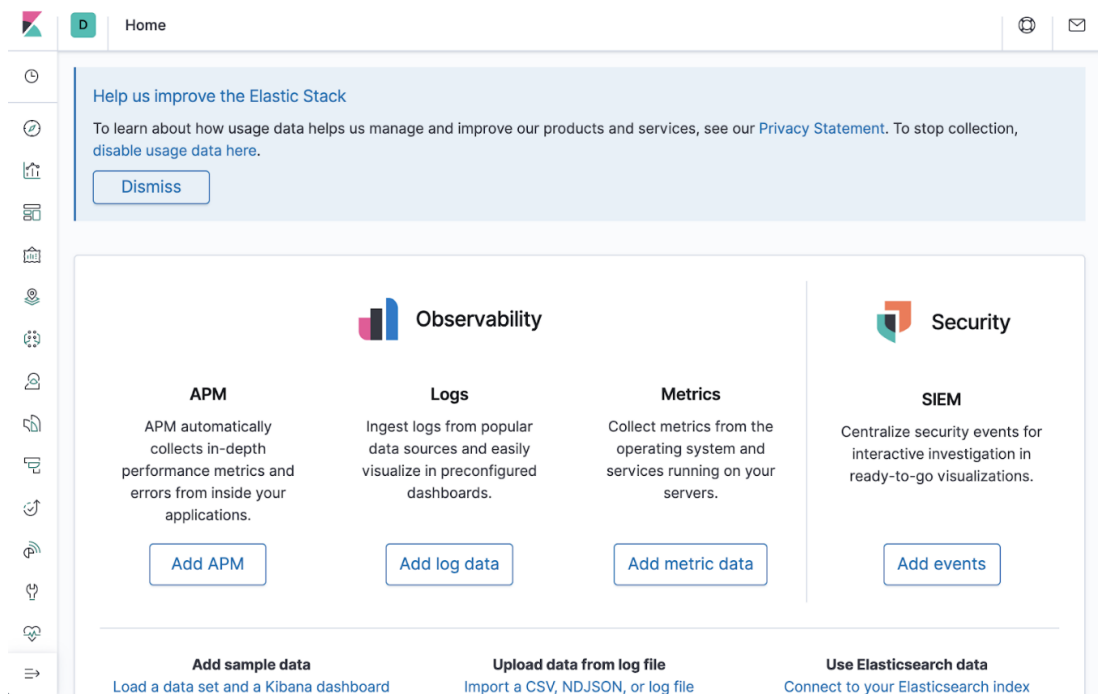
Funkcia	Beats	Elastic Agent
Počet agentov	Viac samostatných	Jeden univerzálny
Konfigurácia	Manuálne YAML súbory	Centrálne cez Fleet
Update	Ručný	Automatický
Bezpečnosť	Obmedzená	Zabudovaná Endpoint Security
Integrácie	Základné	Široká knižnica modulov
Komplexnosť	Vyššia pri väčšom počte hostov	Jednoduchá, škálovateľná
Odporúčanie Elasticu	Staršie nasadenia	Moderné nasadenia

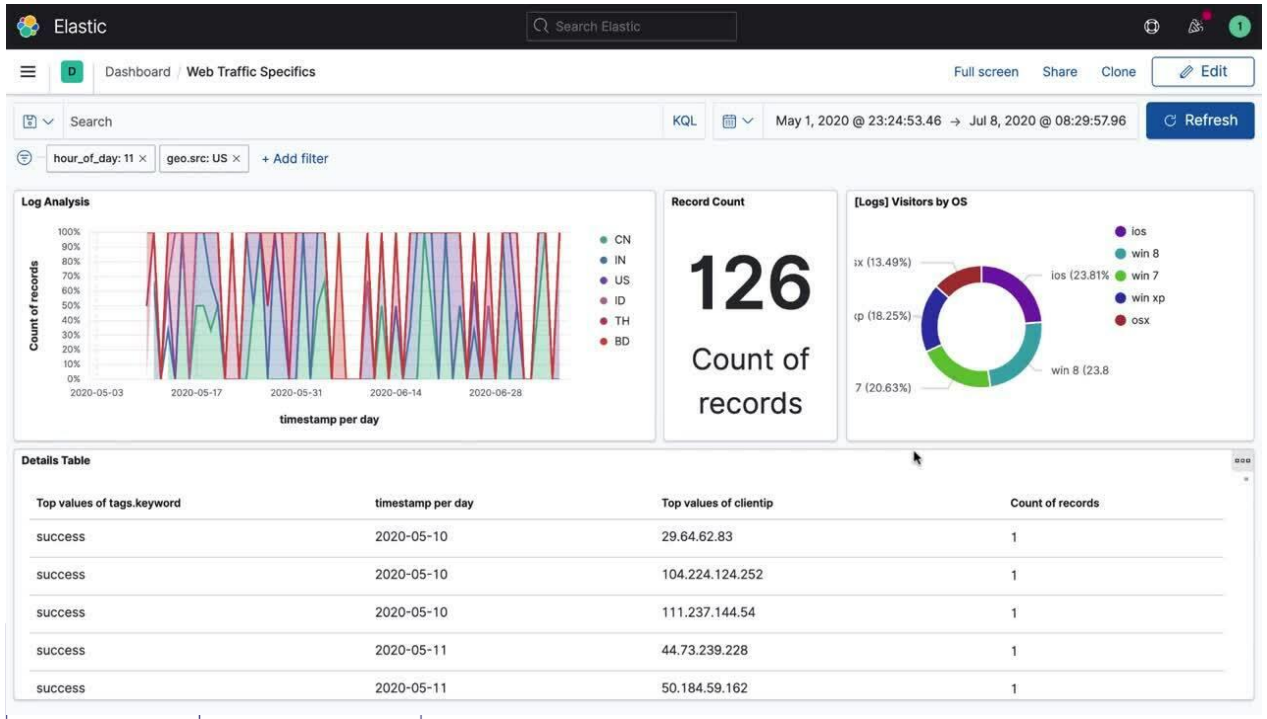
Security information and event management

ELK stack - Kibana

- Slúži na vizualizáciu dát (prehľadné tabuľky, grafy, dashboardy, mapy), alebo aj prezeranie čistých dát
- Tvorba bezpečnostných pravidiel
- Tvorba Spaces (logické priestory)
  Napr. testové a produkčné prostredie
- Alerty
- Manažovanie Elasticsearch
  - Kontrolovanie stavu databázy
  - Nastavovanie politiky pre retenciu dát
  - Tvorenie používateľských účtov
  - Tvorenie rolí

kibana

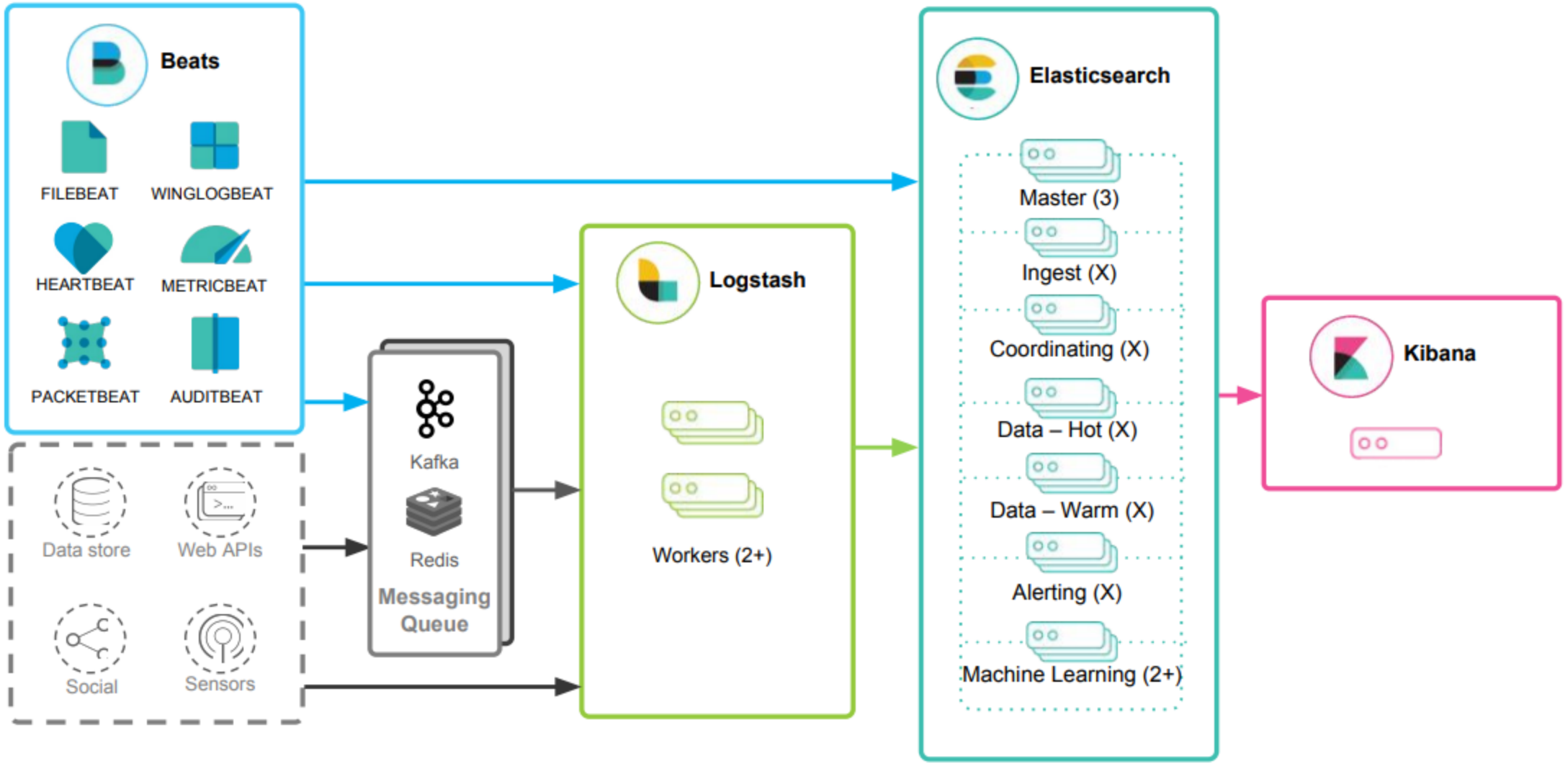




Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY

Komponenty v SIEM ELK

Architektúru Elastic stacku na vysokej úrovni je možné v prostrediach náročných na zdroje vylepšiť pridaním **Kafka** , **RabbitMQ** a **Redis** pre ukladanie do vyrovnávacej pamäte a odolnosť a **nginx** pre bezpečnosť.



Ukážka – inštalácia ELK

Inštalácia ELK stack - Elasticsearch

- Znázornený postup inštalácie je pre debianovský operačný systém

- Stiahnutie kľúča Elastic repozitára
  - `wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg`

- Pridanie Elastic repoziráta (verzia 9.x)
  - `echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/9.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-9.x.list`

- Inštalácia ElasticSearch
  - `sudo apt-get update && sudo apt-get install elasticsearch`

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

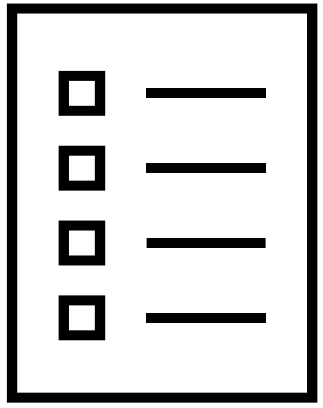
Konfigurácia ELK stack - Elasticsearch

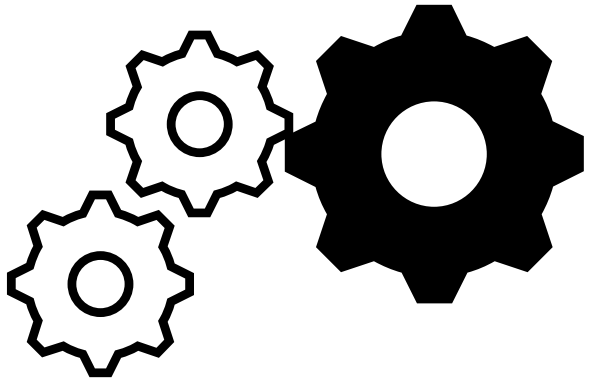
- Konfiguračný súbor sa nachádza v `/etc/elasticsearch/elasticsearch.yml`
- Ukážka config súboru pre master node:

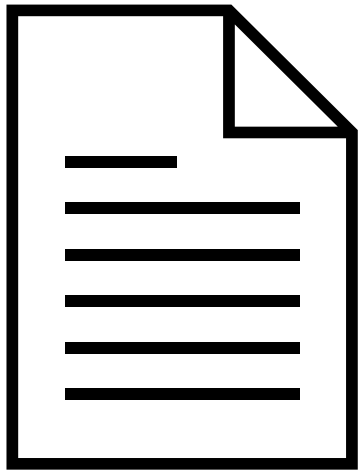
```
cluster.name: // meno clustera
node.name: // meno vrchola
node.roles: [master] // rola
path.data: /var/lib/elasticsearch-master1
path.logs: /var/log/elasticsearch-master1
network.host: // IP adresa stroja
http.port: 9200
transport.port: 9300
discovery.seed_hosts: [ // adresy ďalších vrcholov]
cluster.initial_master_nodes: ["master1"]
xpack.security.enabled: true // zapnutie zabezpečenia (v produkčnom prostredí treba zapnúť vždy)
xpack.security.enrollment.enabled: true
xpack.security.http.ssl:
  enabled: true
  keystore.path: // cesta ku keystore
xpack.security.transport.ssl:
  enabled: true
  verification_mode: certificate
  client_authentication: required
  keystore.path: // cesta ku keystore
  truststore.path: // cesta ku truststore
http.host: 0.0.0.0 // na akej IP adrese počúva
transport.host: 0.0.0.0 // na akej IP adrese počúva
xpack.security.audit.enabled: true
```

Konfigurácia ELK stack - Elasticsearch

```
xpack.security.audit.logfile.events.include: access_denied,
anonymous_access_denied, authentication_failed, connection_denied,
tampered_request, run_as_denied, security_config_change
xpack.security.audit.logfile.emit_node_host_address: true
xpack.security.audit.logfile.emit_node_name: true
xpack.security.audit.logfile.emit_node_host_name: true
```

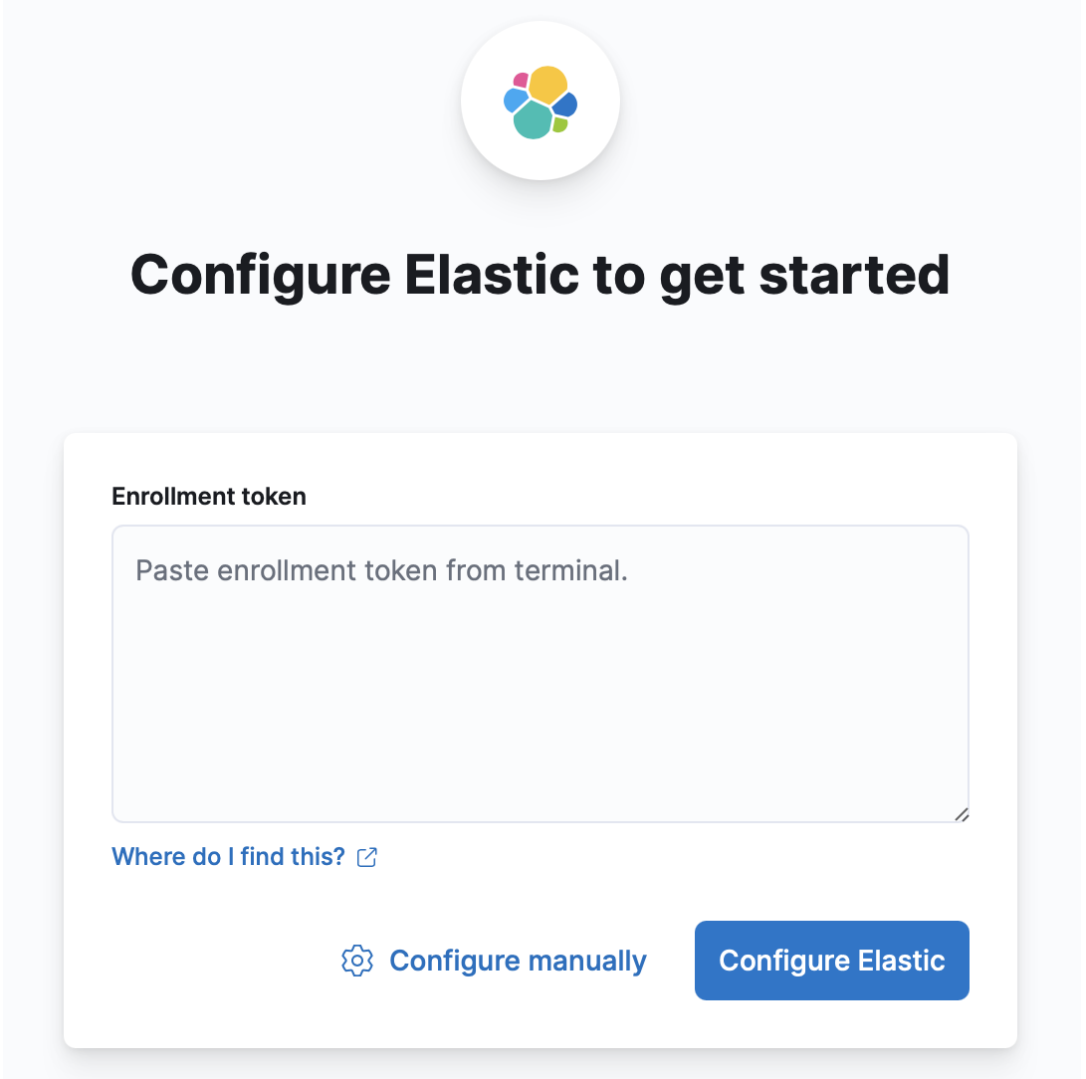






Konfigurácia ELK stack - Elasticsearch

- Zapnutie elasticsearch služby
  - sudo systemctl start elasticsearch.service
- Pri prvom zapnutí sa vygeneruje enrollment token, ktorý ide použiť pre automatické prepojenie Kibany s Elasticsearch.
- Automaticky sa nakonfiguruje zabezpečené spojenie medzi týmito dvoma službami.
- Token na prepojenie elasticsearch a kibany ide vygenerovať aj manuálne za použitia nasledujúceho príkazu:
  - bin/elasticsearch-create-enrollment-token -s kibana --url "// url "



Konfigurácia ELK stack – Logstash

- **Inštalácia**
  - sudo apt-get update && sudo apt-get install logstash
- **Spustenie služby**
  - sudo systemctl start logstash.service
- V zložke /etc/logstash/conf.d/ sa nachádzajú konfiguračné súbory pre pipelines.
- Pre prehľadnosť je vhodné rozdeliť input, filters a output do samostatných súborov.

```
Ukážka - Input.conf:
input {
  beats { // beats sú elastic agenti
    port => 5044
    ssl_enabled => true
    ssl_certificate => " // cesta k certifikátom na
zabezpečenie spojenia"
    ssl_key => "// cesta ku kľúčom"
    ssl_certificate_authorities => [" // cesta
k cert. autorite"]
    ssl_client_authentication => "required"
  }
}
```

Konfigurácia ELK stack – Logstash

Ukážka - časť z filter.conf:

```
filter {
if ("suricata-moloch" in [tags]) or ("suricata-suricata2" in [tags]) {
    # Extrakcia kľúčových hodnôt bez `metadata` prefixu
    mutate {
      rename => {
        "[suricata_parsed][src_ip]" => "source.ip"
        "[suricata_parsed][src_port]" => "source.port"
        "[suricata_parsed][dest_ip]" => "destination.ip"
        "[suricata_parsed][dest_port]" => "destination.port"
        "[suricata_parsed][proto]" => "network.protocol"
        "[suricata_parsed][event_type]" => "event.type"
        "[suricata_parsed][flow_id]" => "network.flow_id"
        "[suricata_parsed][app_proto]" => "network.application_protocol"
        "[suricata_parsed][in_iface]" => "network.interface"
```

Konfigurácia ELK stack – Logstash

Ukážka - časť z output.conf:

```
output {
  if "auditbeat-studenti" in [tags] {
    elasticsearch {
      hosts => [" // IP Elasticsearch"]
      user => "logstash_internal"
      password => "${ES_psswd}"
      ssl_enabled => true
      ssl_certificate_authorities => "// cesta k certifikačnej autorite"

      ilm_enabled => true
      ilm_rollover_alias => "// rollover alias"
      ilm_pattern => "{now/d}-000001"
      ilm_policy => "auditbeat-logs-ILM"

      manage_template => false
    }
  }
```

Konfigurácia ELK stack – Kibana

- **Inštalácia**
  - sudo apt-get update && sudo apt-get install kibana
- **Spustenie služby**
  - sudo systemctl start kibana.service

```
server.port: 5601
server.host: "0.0.0.0"
server.publicBaseUrl: " // url adresa kibany"
server.ssl.enabled: false
elasticsearch.hosts: ["// adresa ElasticSearch"]
elasticsearch.username: "kibana_system"
elasticsearch.requestTimeout: 180000
elasticsearch.ssl.certificateAuthorities: [ "// cesta k certifikačnej autorite" ]
elasticsearch.ssl.verificationMode: full
```

Konfigurácia ELK stack – Kibana

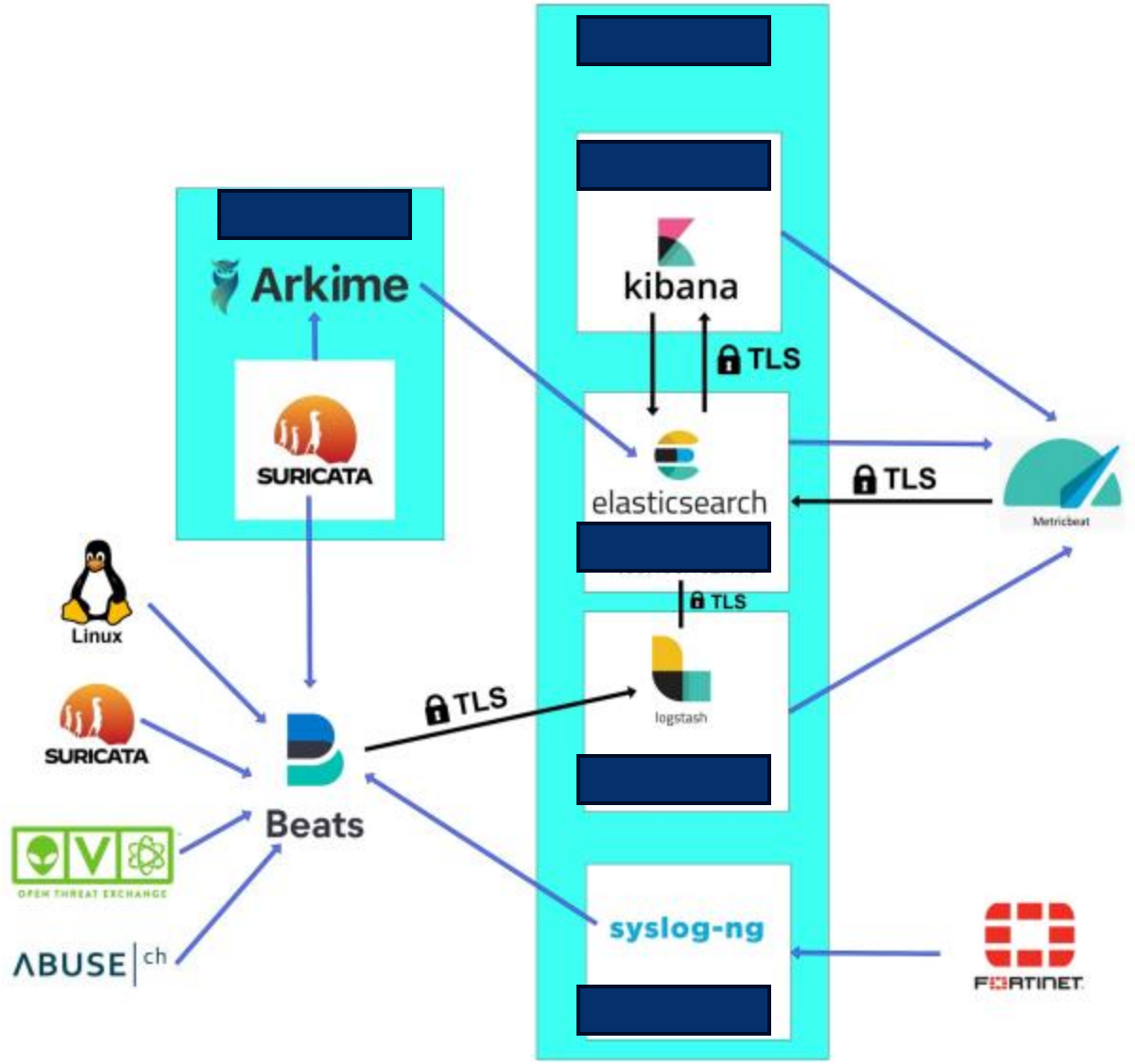
```
logging:
  appenders:
    file:
      type: file
      fileName: /var/log/kibana/kibana.log
      layout:
        type: json
  root:
    appenders:
      - default
      - file
pid.file: /run/kibana/kibana.pid
xpack.encryptedSavedObjects.encryptionKey: //
xpack.reporting.encryptionKey: //
xpack.security.encryptionKey: //
monitoring.kibana.collection.enabled: false
monitoring.ui.enabled: true
monitoring.ui.elasticsearch.hosts: ["// IP Elasticsearch"]
monitoring.ui.ccs.enabled: false
```


Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Ukážka nasadenia SIEM

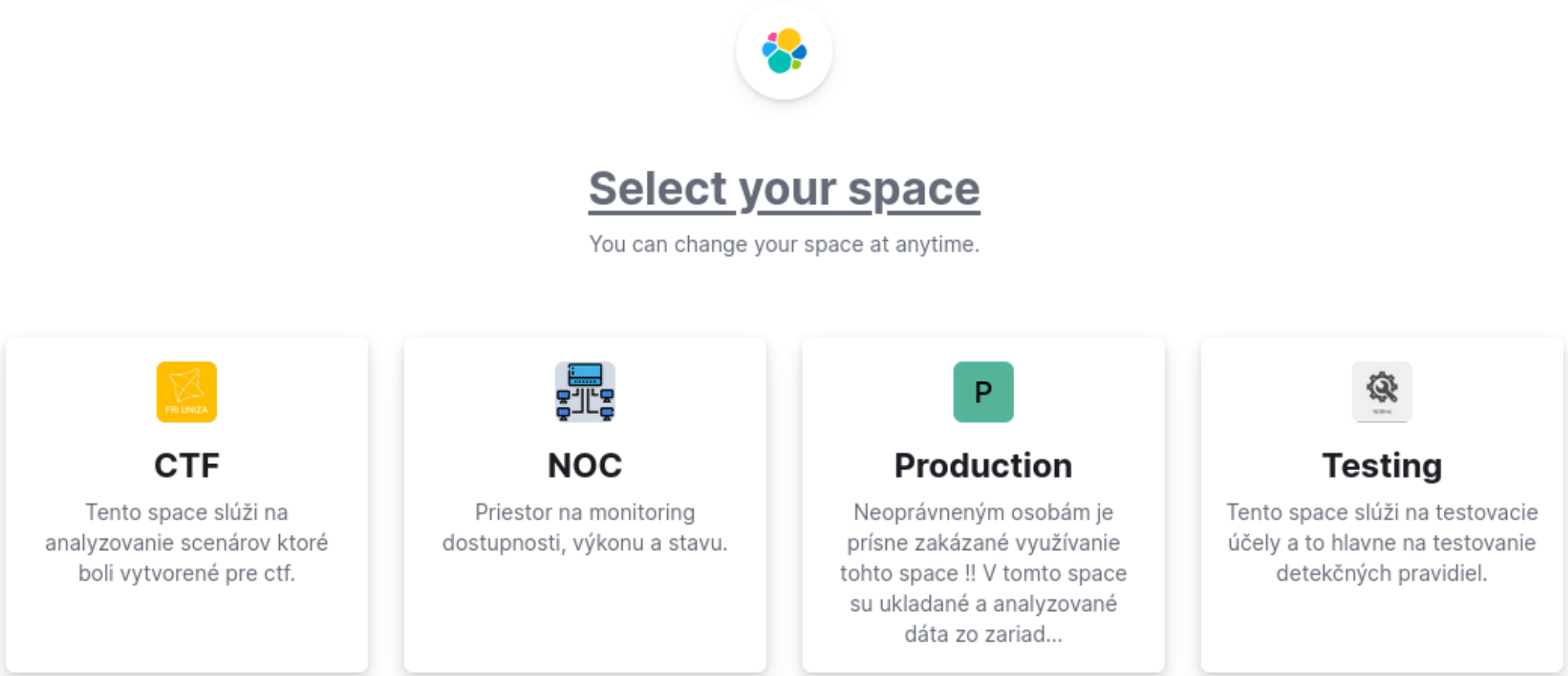
Ukážka ELK SIEM

- Aktuálne nasadenie SIEM architektúry
  - Zdroje dát
    - Arkime - Zachytáva celú sieťovú prevádzku na fakulte
    - Beats – Agenti, pomocou ktorých sa zbierajú logy na koncových zariadeniach (File beat, Audit beat, Winlog beat)
    - Syslog-ng - Zberá logy s iných zariadení
    - Metricbeat – Monitorovanie stavu ELK
  - Spracovanie dát
    - Na spracovanie dát slúži nástroj Logstash
    - Na ukladanie, vyhľadávanie sa používa Elasticsearch
  - Vizualizácia, tvorenie pravidiel, alerty...
    - Kibana



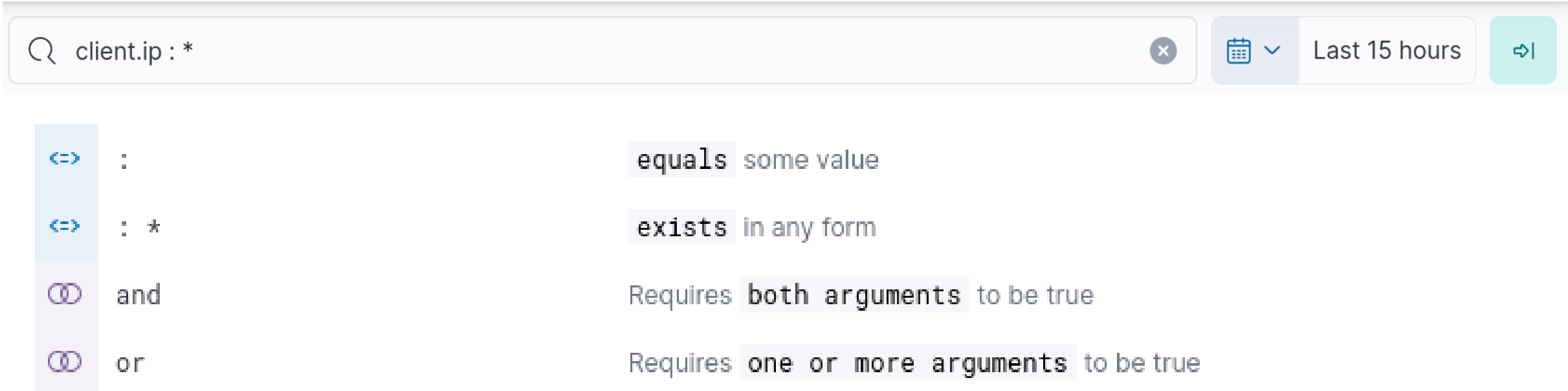
Ukážka ELK SIEM - Kibana

- Výber spaces (Logické oddelenie pracovných prostredí)



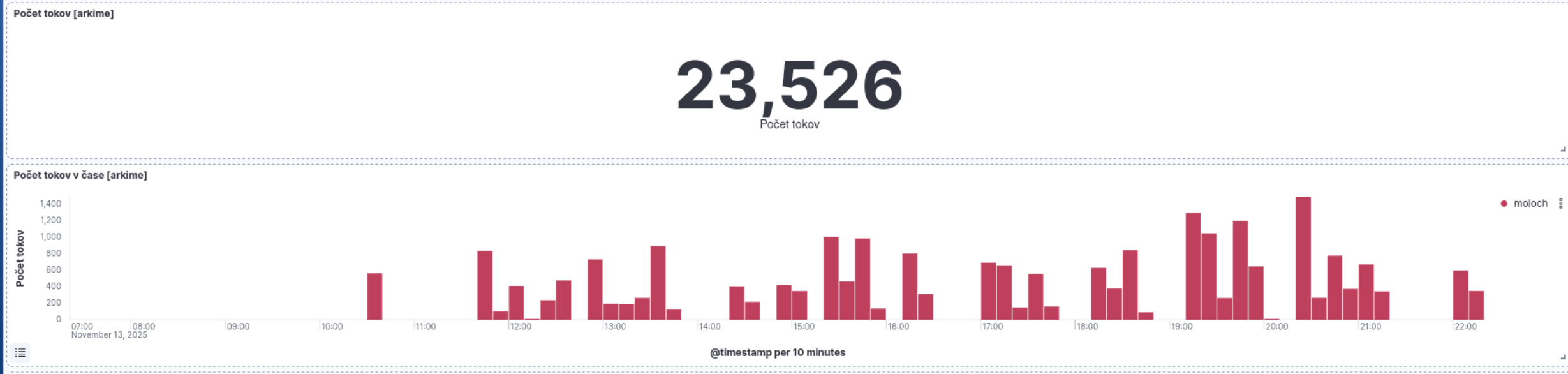
Ukážka ELK SIEM – Kibana - Arkimeview Dashboard

- Zobrazené dáta dokážeme filtrovať pomocou KQL (Kibana Query Language) syntaxe. Filtráciou dát vieme dosiahnuť lepšiu prehľadnosť.
- Taktiež si dokážeme nastaviť časové okno z ktorého chcem dáta prezerať.



Ukážka ELK SIEM – Kibana - Arkimeview Dashboard

- Dashboard Arkimeview vizualizuje dáta zachytené nástrojom Arkime. Ten odchytáva celú sieťovú prevádzku na fakultnom uplinku. Na obrázku je vidno počet odchytených dátových tokov a aj ich zobrazenie v grafe v čase.

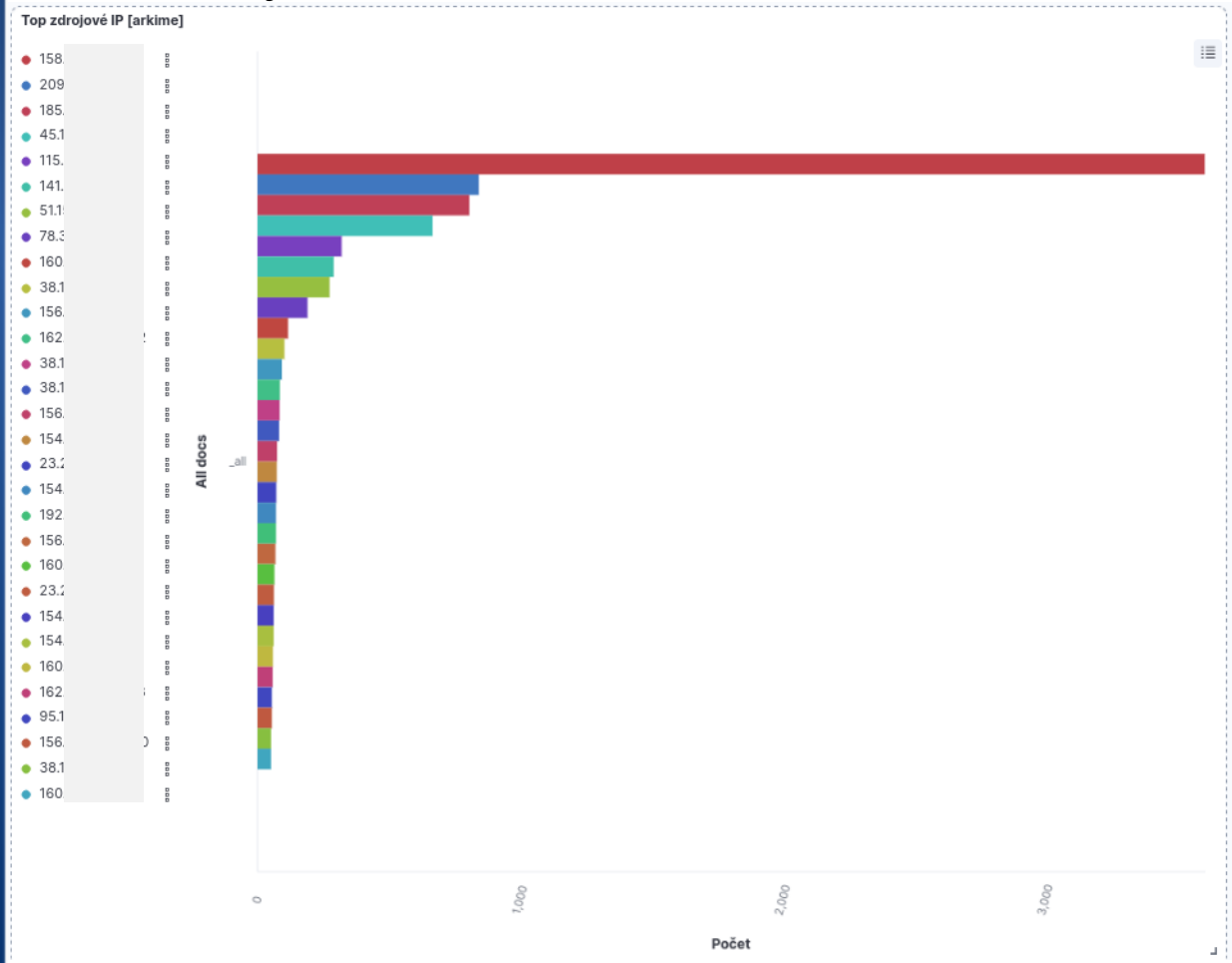


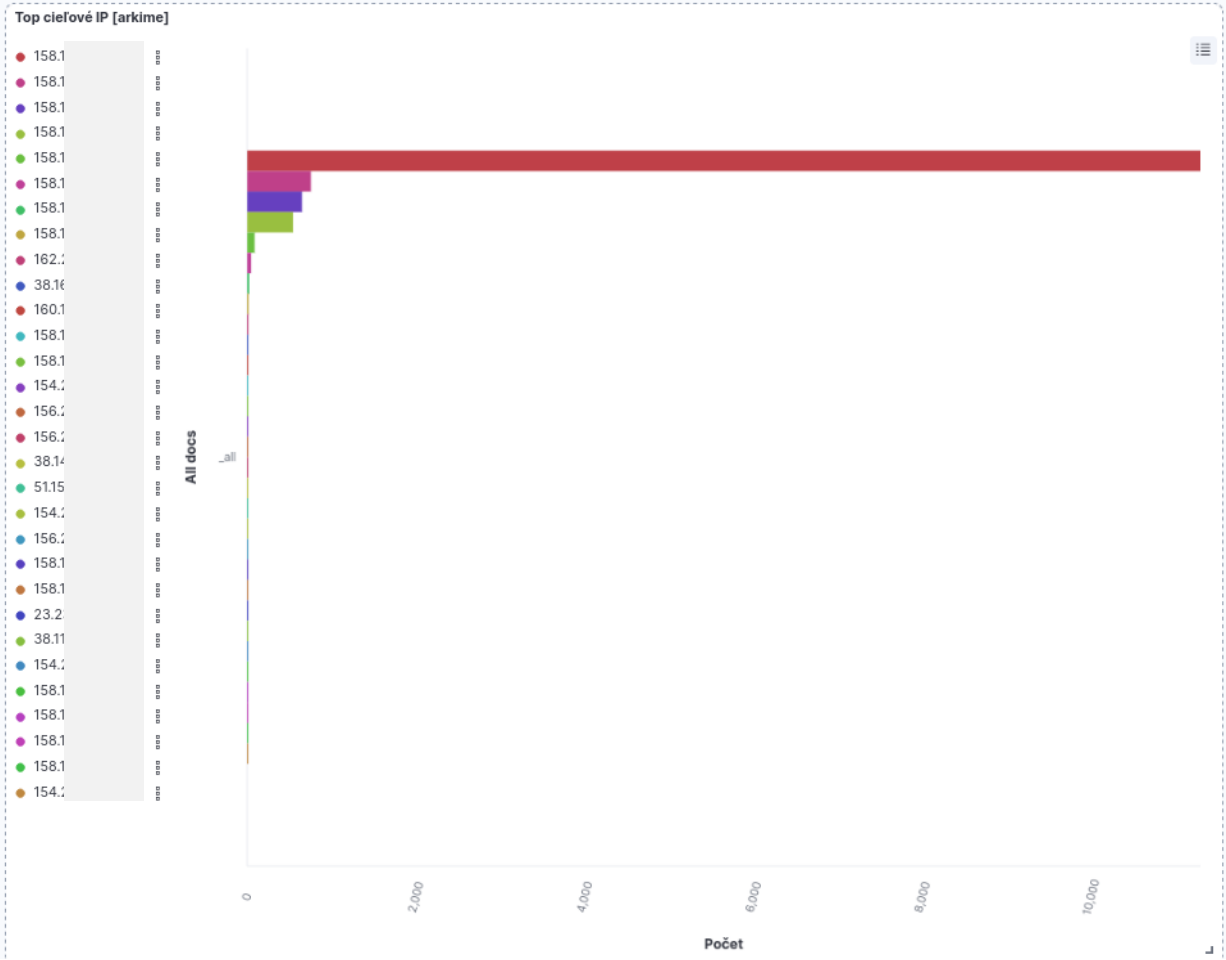
Ukážka ELK SIEM – Kibana - Arkimeview Dashboard

- Dashboard monitoringu sieťovej prevádzky - GEO mapa zdrojov / cieľov sieťových tokov

Ukážka ELK SIEM – Kibana - Arkimeview Dashboard

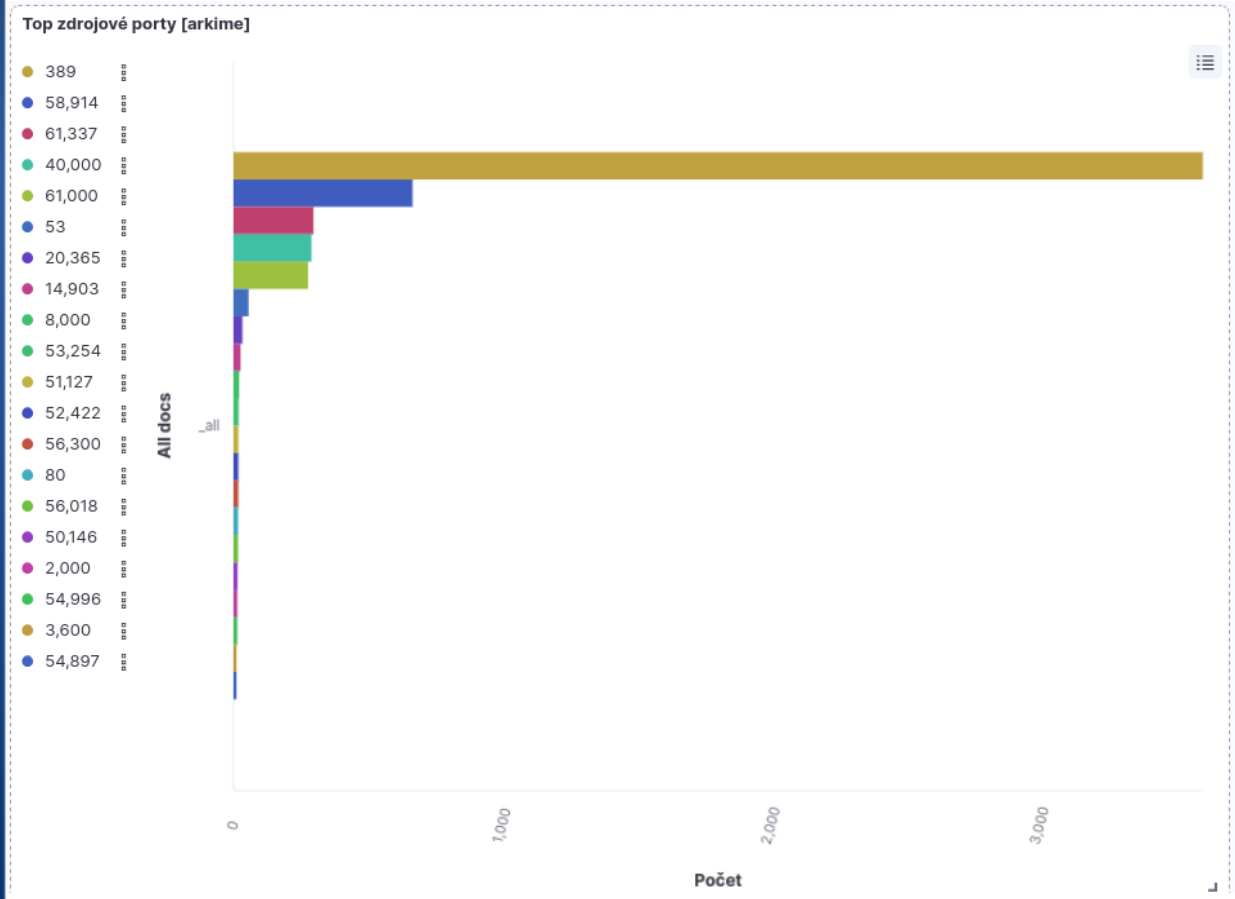
- Dashboard monitoringu sieťovej prevádzky - Graf TOP zdrojových a cieľových IP adries sieťových tokov.

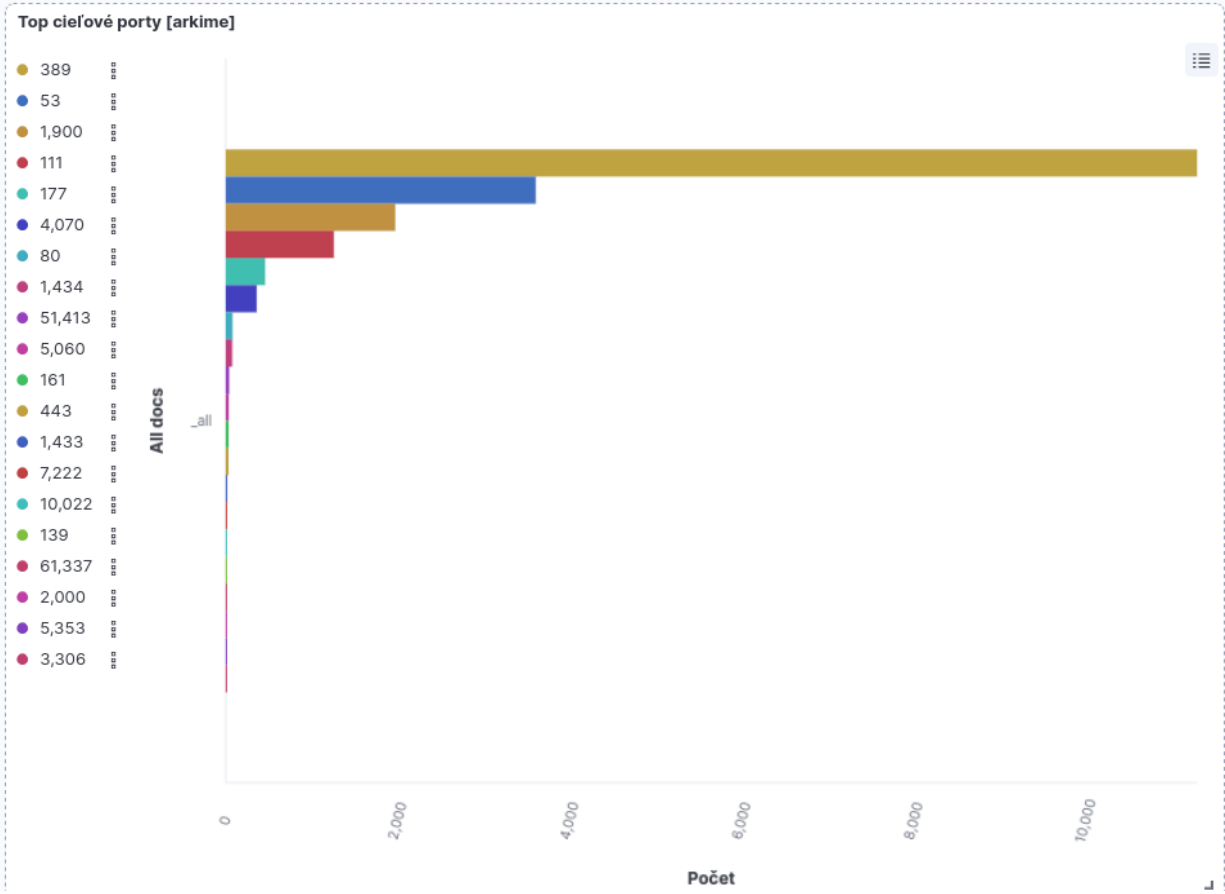




Ukážka ELK SIEM – Kibana - Arkimeview Dashboard

- Dashboard monitoringu sieťovej prevádzky - Graf TOP zdrojových a cieľových portov sieťových tokov.





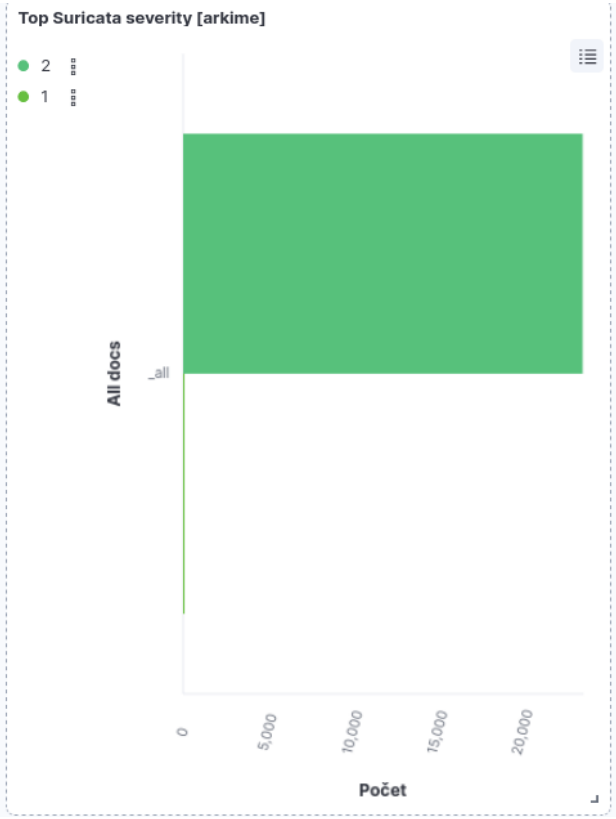
Ukážka ELK SIEM – Kibana - Suricata Dashboard

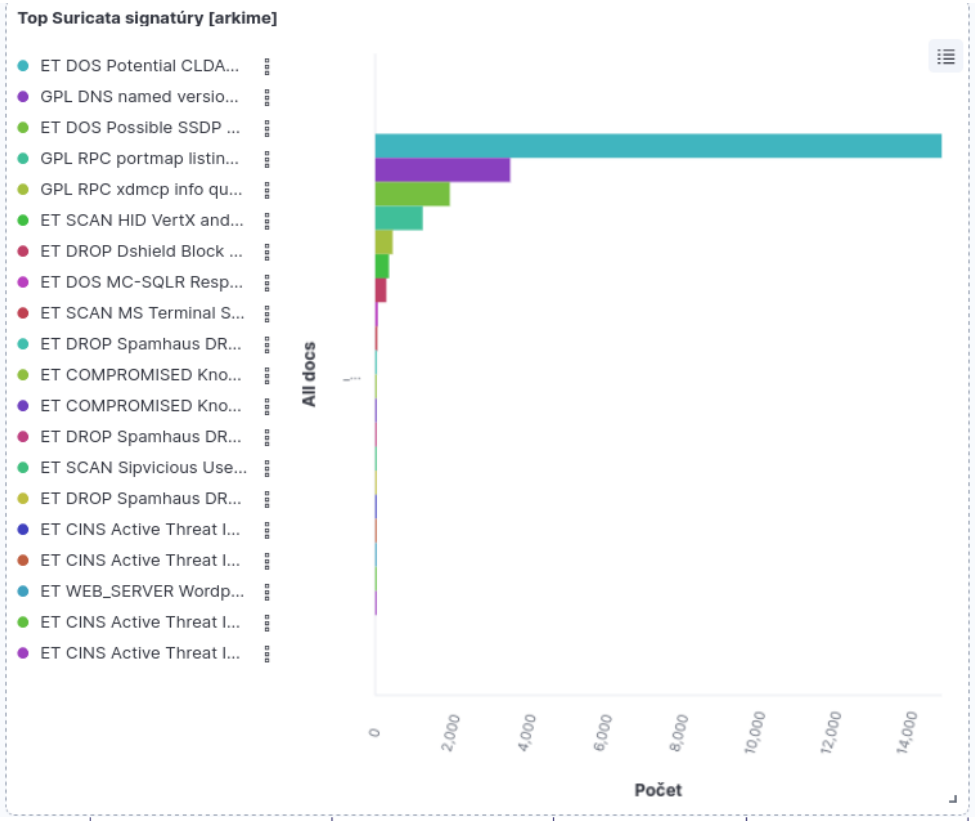
- Suricata je IDS (Intrusion Detection System) nástroj, ktorý vyhodnocuje, či monitorovaná prevádzka je potencionálne nebezpečná na základe signatúr.
  - Signatúry sú predom definované pravidlá, podľa ktorých sa určuje, či je prevádzka podozrivá alebo nie.
  - Podozrivá prevádzka je označená signatúrou.
- Jednotlivé signatúry majú pridelené závažnosti (severity).
  - Suricata závažnosti sú od 1 = najzávažnejšia po 3 = najmenej závažná.
- Suricata dokáže pracovať aj v režime IPS (Intrusion Prevention System),
  - ktorý pri vyhodnotení podozrivej prevádzky dokáže aktívne zasiahnuť a prevádzku zablokovať.
- Taktiež dokáže vykonávať Full packet capture, alebo podmienený packet capture.
  - Ten zaznamenáva prevádzku len vtedy, keď je podozrivá.
  - Bežnú bezpečnú prevádzku neodchytáva.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ukážka ELK SIEM – Kibana - Suricata Dashboard

- Na grafe je vidno závažnosť tokov označených signatúrami
- Top suricata signatúry a ich početnosti





Top Suricata signatúry - tabuľka [arkime]

Export

Suricata signatúra	Počet
ET DOS Potential CLDAP Amplification Re...	14,893
GPL DNS named version attempt	3,549
ET DOS Possible SSDP Amplification Sca...	1,961
GPL RPC portmap listing UDP 111	1,248
GPL RPC xdmcp info query	458
ET SCAN HID VertX and Edge door contr...	360
ET DROP Dshield Block Listed Source gro...	291
ET DOS MC-SQLR Response Outbound P...	67
ET SCAN MS Terminal Server Traffic on N...	53
ET DROP Spamhaus DROP Listed Traffic I...	40

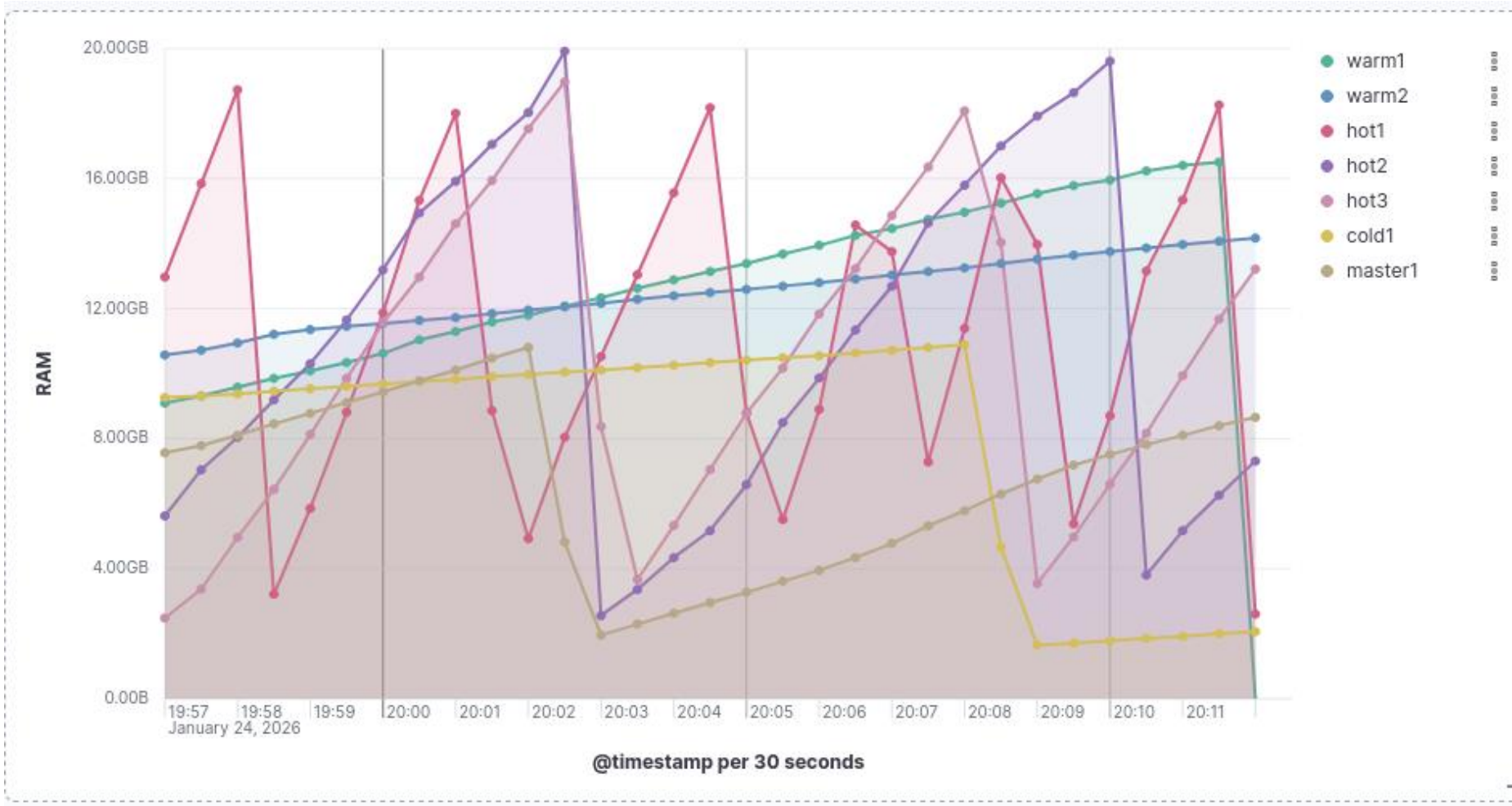
Rows per page: 10

1 2 3 4

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

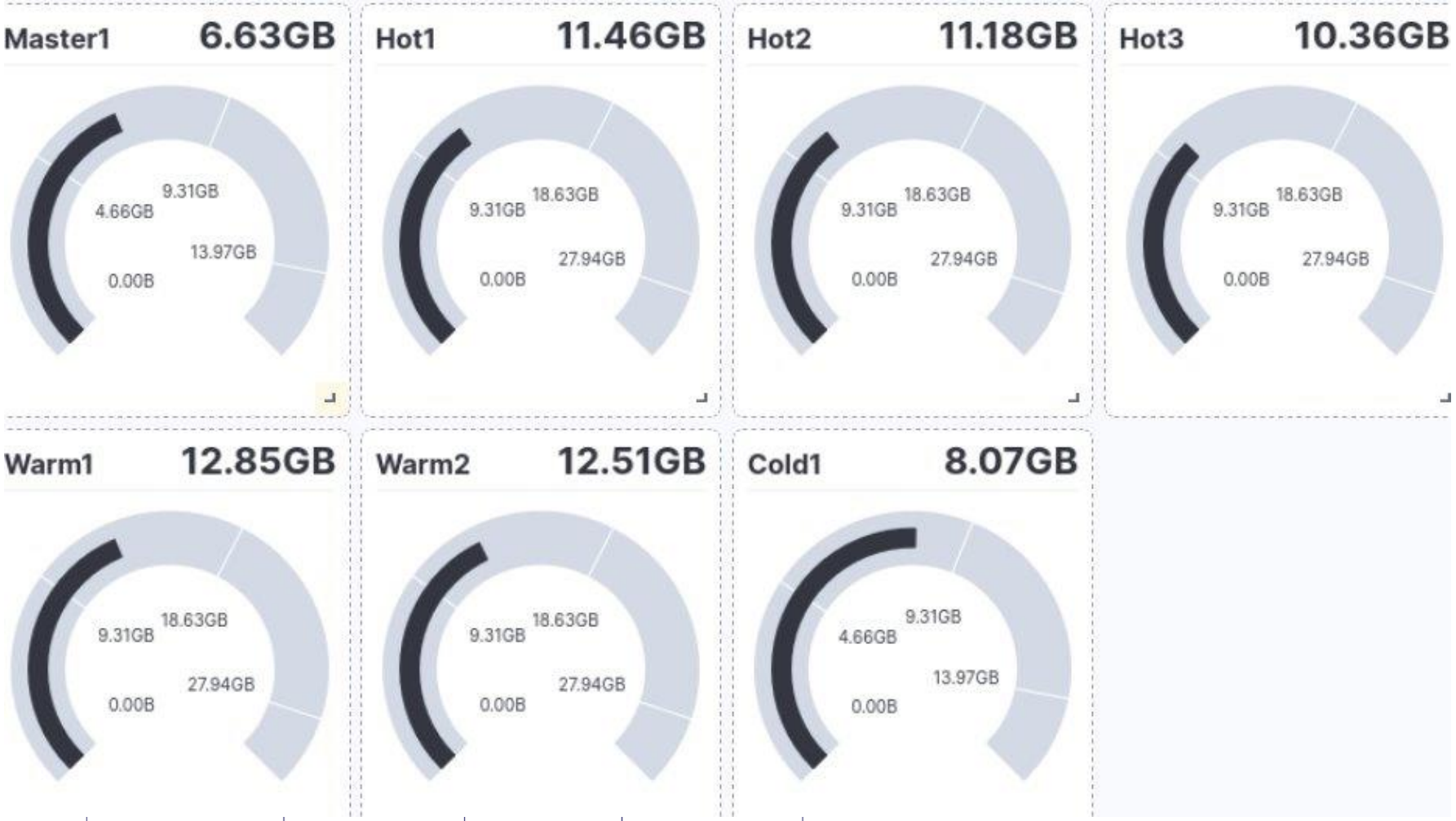
Ukážka ELK SIEM – Kibana - Zaťaženie stacku dashboard

- Dashboard zaťaženia ELK stacku
- Aktuálna záťaž RAM



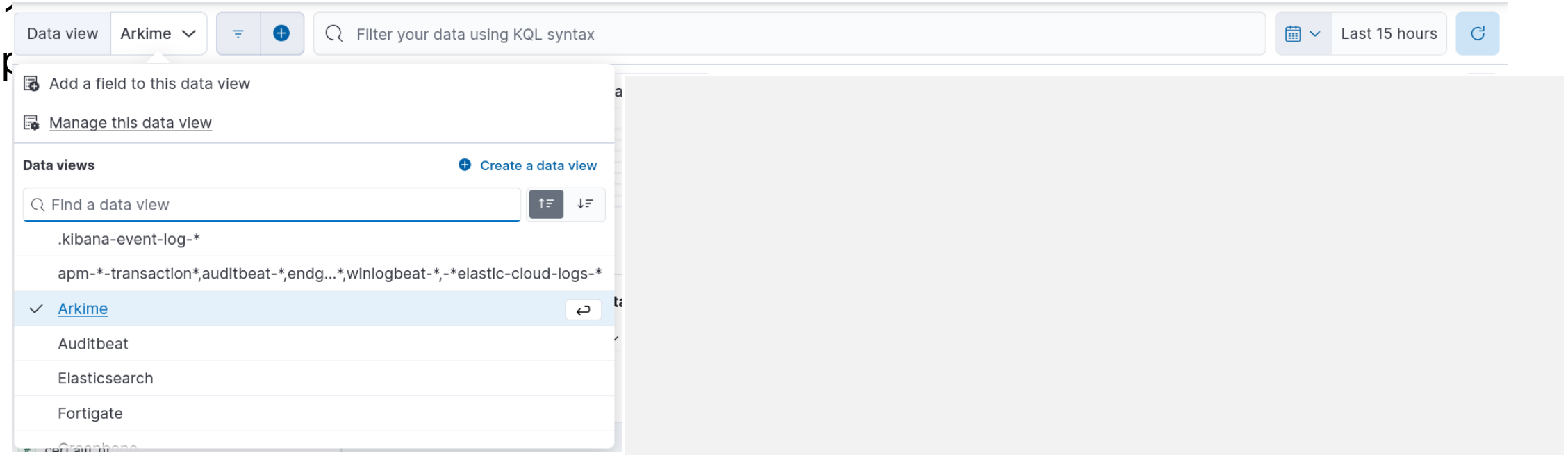
Ukážka ELK SIEM – Kibana - Zaťaženie stacku dashboard

- Dashboard zaťaženia ELK stacku
- Aktuálna záťaž RAM



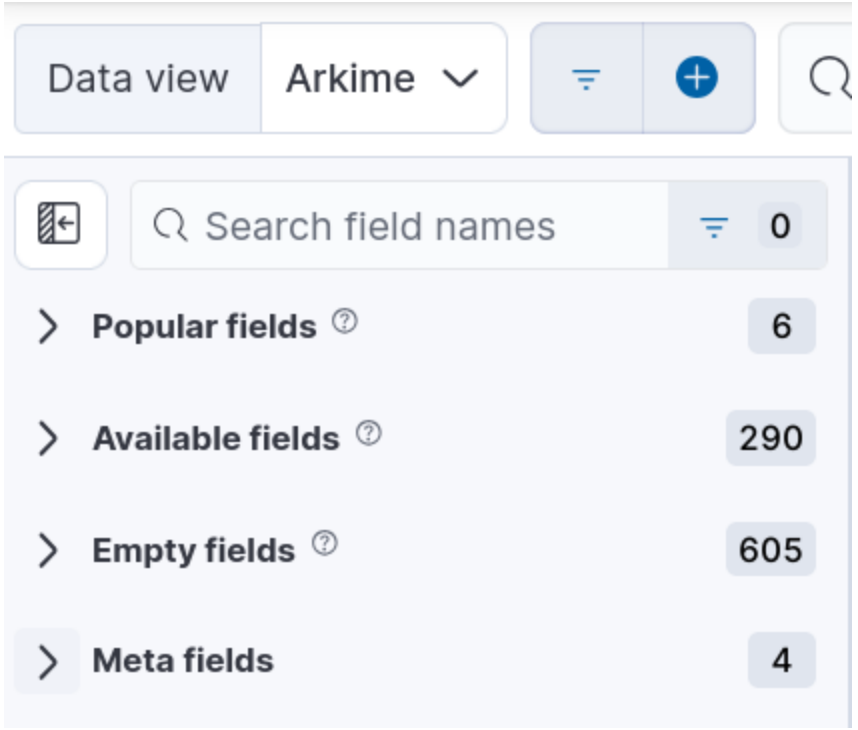
Ukážka ELK SIEM – Kibana – Discovery Arkime Data view

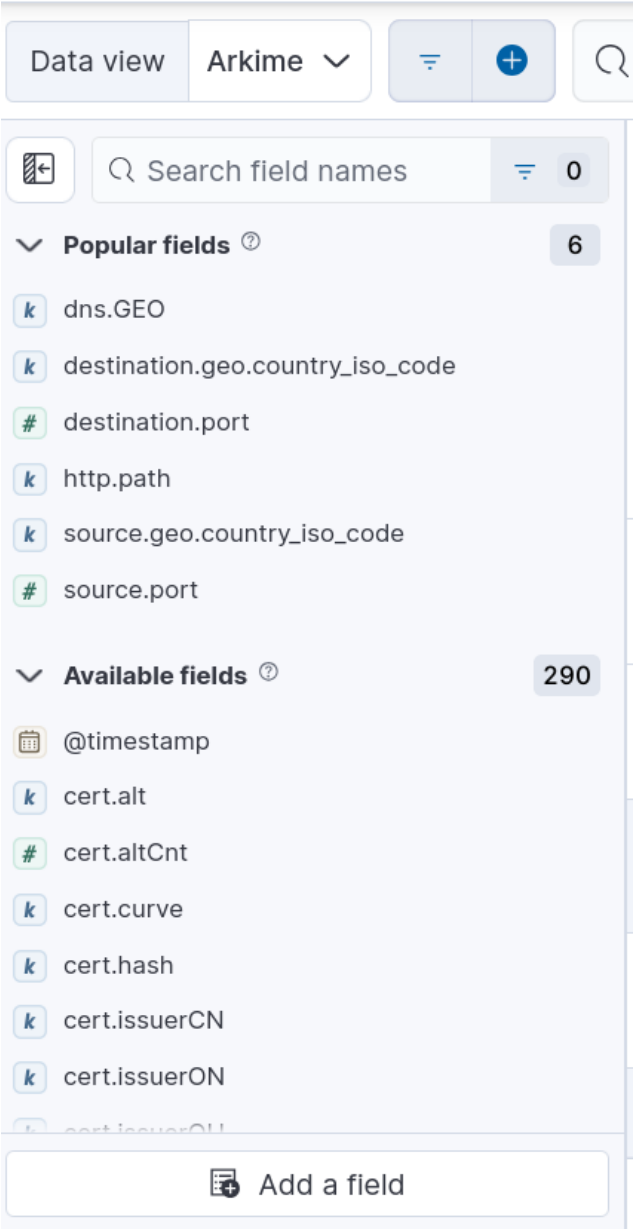
- V sekcií **Discovery** dokážeme pozerať spracované odchytené dáta. Taktiež ich dokážeme filtrovať pomocou KQL a časového okna
  - **KQL (Kibana Query Language)** je dotazovací jazyk používaný v **Kibane** (Elastic stack), najmä v sekcii **Discovery**, na rýchle a intuitívne filtrovanie a vyhľadávanie dát.
- Vľavo hore dokážeme vybrať **data view**. Data view je **množina indexov**, ktoré si vyberieme na zobrazenie na základe **index paternu**. Napr. ak máme indexy arkime-



Ukážka ELK SIEM – Kibana – Discovery Arkime Data view

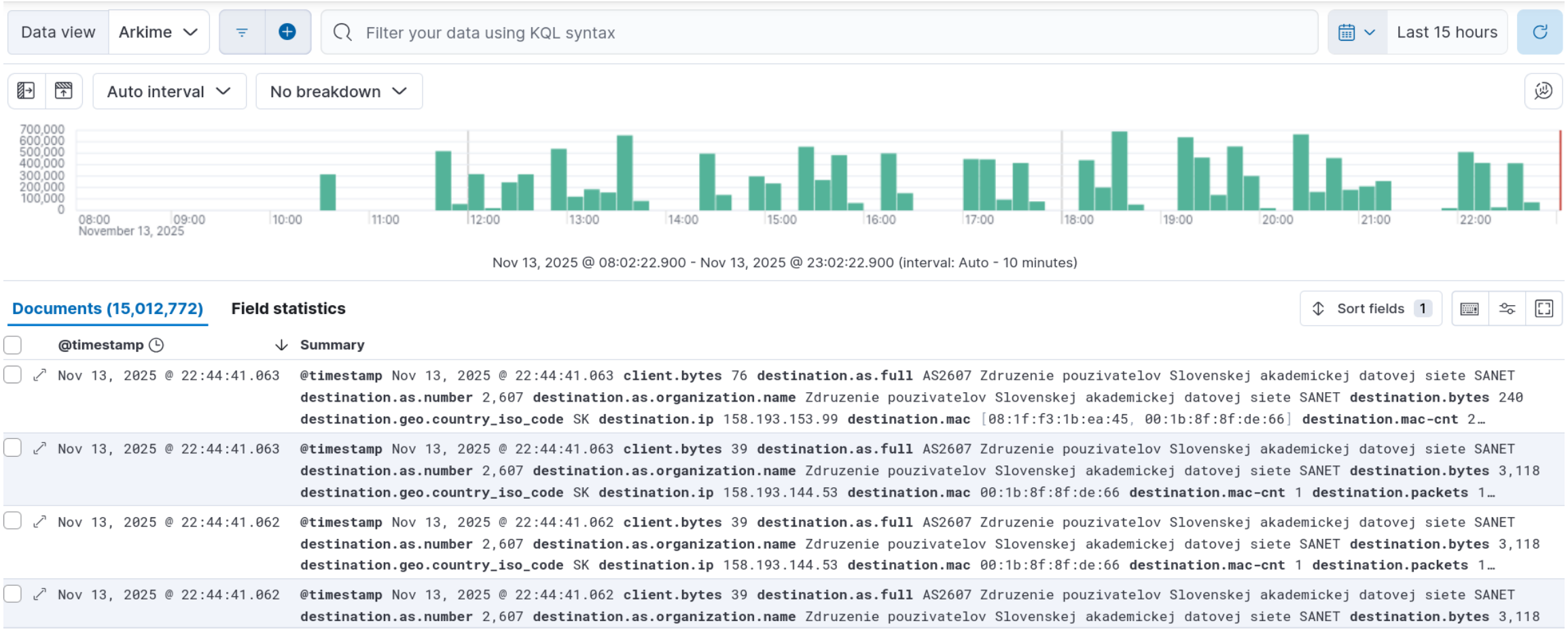
- Napravo si dokážeme vybrať s dostupných **polí - fields (stĺpcov)**
- Pomocou týchto polí/stĺpcov si dokážeme naskladať tabuľku z údajov, ktoré sú pre nás relevantné
- Nachádzajú sa tu aj stĺpce, ktoré v aktuálnom časovom okne neboli naplnené, ale sú namapované v indexoch, ktoré sa používajú pre aktuálny dataview





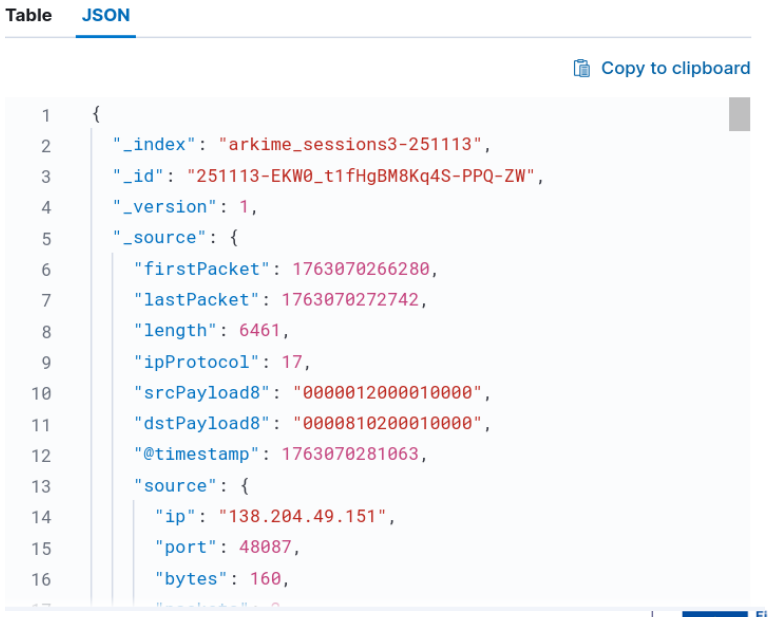
Ukážka ELK SIEM – Kibana – Discovery Arkime Data view

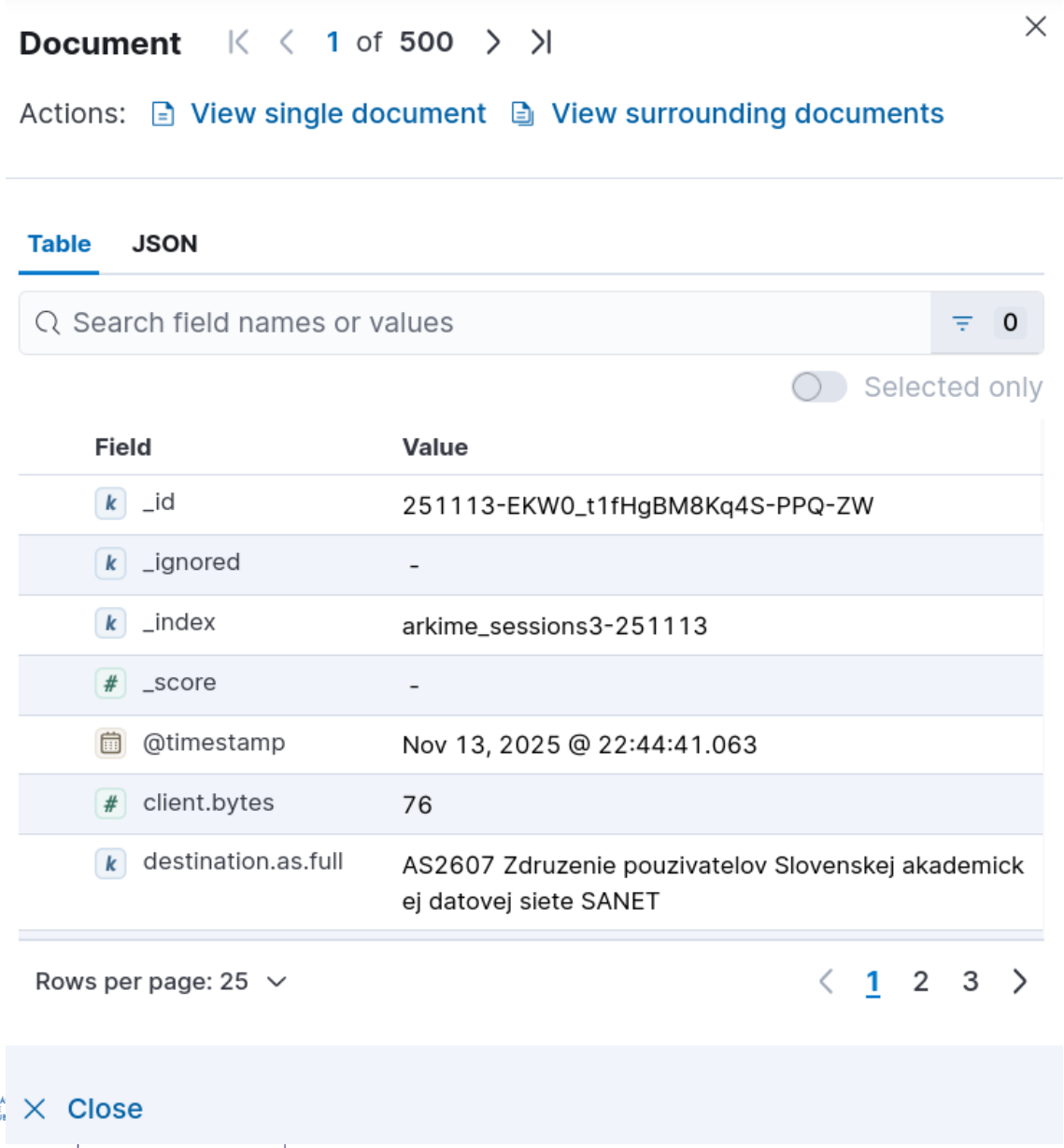
- Keď si nevyberieme žiaden stĺpec, automaticky sa zobrazí **Summary** stĺpec, ktorý obsahuje všetky dáta



Ukážka ELK SIEM – Kibana – Discovery Arkime Data view

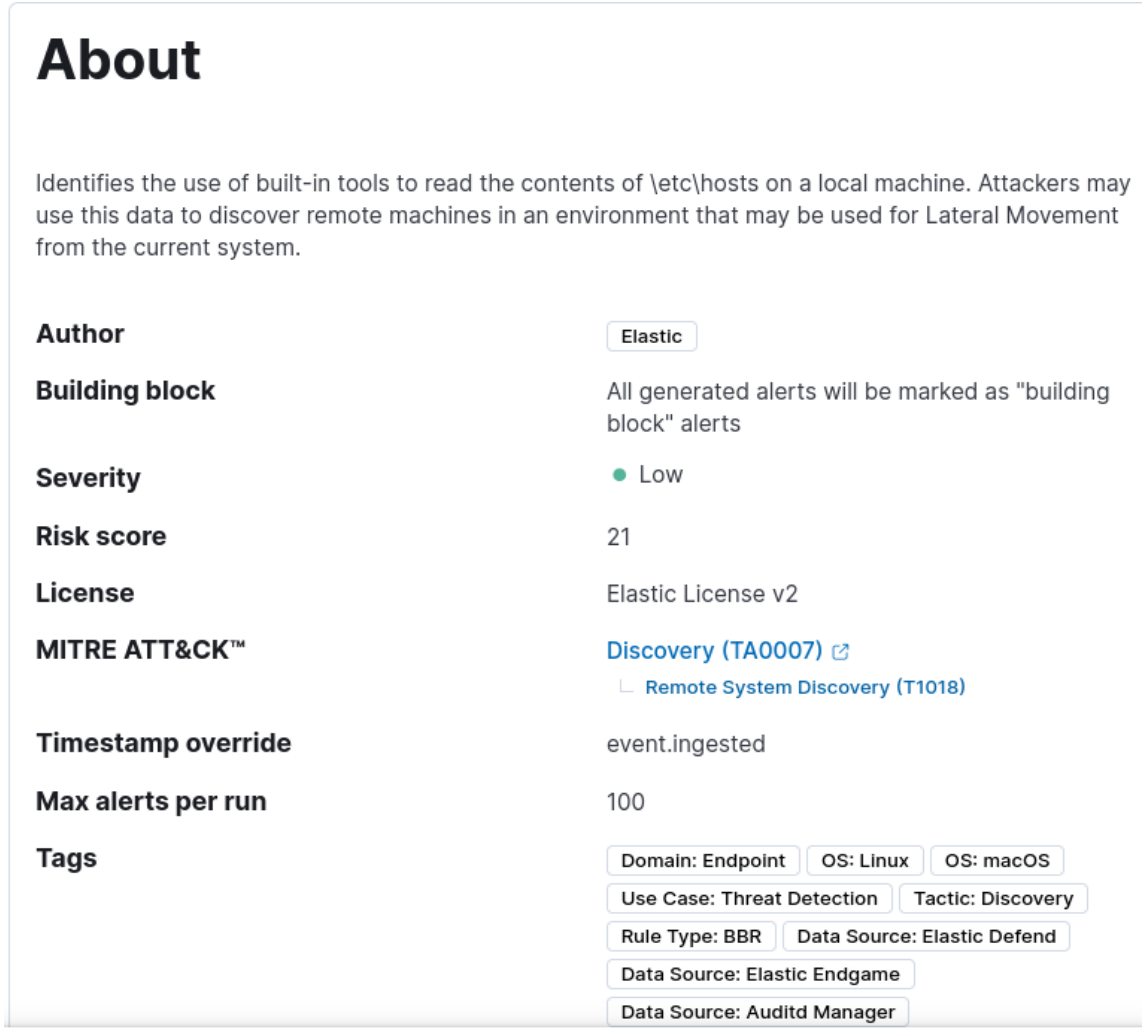
- Jednotlivé záznamy ide rozkliknúť.
  - Tým vieme prezerať celý obsah jedného záznamu
- Počas prezerania môžeme filtrovať jednotlivé stĺpce pre záznam
- Taktiež je možnosť si záznam pozrieť v JSON formáte





Ukážka ELK SIEM – Kibana Rules

- Kibana Rules sú detekčné pravidlá, pomocou ktorých spúšťame testy nad zozbieranými dátami, kde sa vyhodnocujú zadané podmienky.
  - Ak sú všetky potrebné podmienky splnené, vytvorí sa nový alert.
- Základné informácie, ktoré obsahuje pravidlo:
  - Názov pravidla
  - Závažnosť
  - Mapovanie na maticu útoku MITRE ATT&CK
  - Tagy
  - Index paterny (nad akými dátami sa má pravidlo spúšťať)
  - EQL query (Event Query Language)
    - EQL je dotazovací jazyk od Elastic pre **vyhľadávanie sekvencií udalostí** v ES, hlavne v kontexte **security a SIEM**.
  - Typ pravidla
  - Vyžadované stĺpce



Ukážka ELK SIEM – Kibana Rules

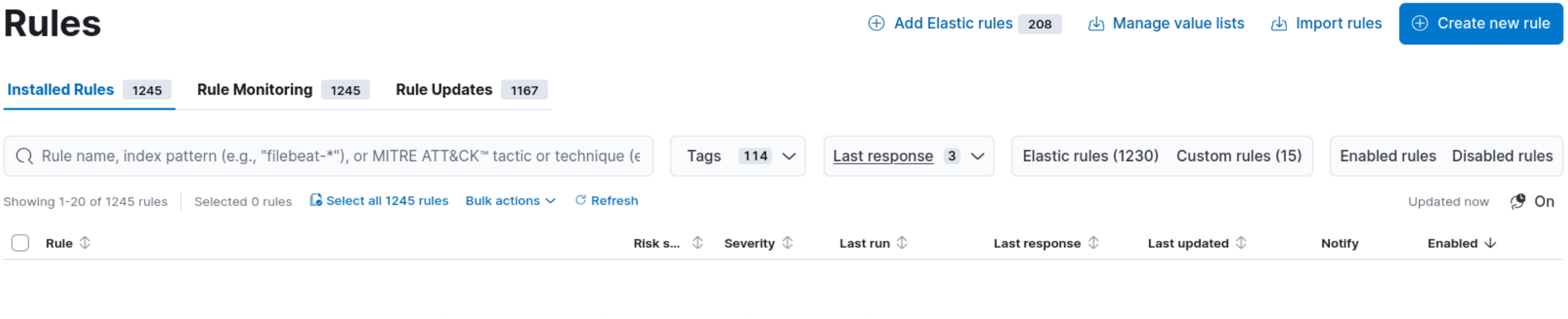
Definition

Index patterns	logs-endpoint.events.* · endgame-* · auditbeat-* · logs-auditd_manager.auditd-*
EQL query	process where event.type == "start" and event.action in ("exec", "exec_event", "executed", "process_started") and process.name in ("vi", "nano", "cat", "more", "less") and process.args == "/etc/hosts"
Rule type	Event Correlation
Related integrations	Auditd Manager Not installed Elastic Defend Disabled
Required fields	event.action, event.type, process.args, process.name
Timeline template	None

Financované Európskou úniou NextGenerationEU · PLÁN OBNOVY · Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky · Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Ukážka ELK SIEM – Kibana Rules

- Vytvorené detekčné pravidlá idú filtrovať podľa:
  - mena,
  - MITTRE taktiky,
  - stavu či sú aktívne alebo nie,
  - statusu posledného spustenia (Succeeded, Warning, Failed),
  - závažnosti,
  - poslednej doby spustenia ....



Security information and event management

Ukážka ELK SIEM – Kibana Rules

Rules

Add Elastic rules 208 | Manage value lists | Import rules | Create new rule

Installed Rules 1245 | Rule Monitoring 1245 | Rule Updates 1167

Rule name, index pattern (e.g., "filebeat-*"), or MITRE ATT&CK™ tactic or technique (e.g., "Defense Evasion" o | Tags 114 | Last response 3 | Elastic rules (1230) | Custom rules (15) | Enabled rules | Disabled rules

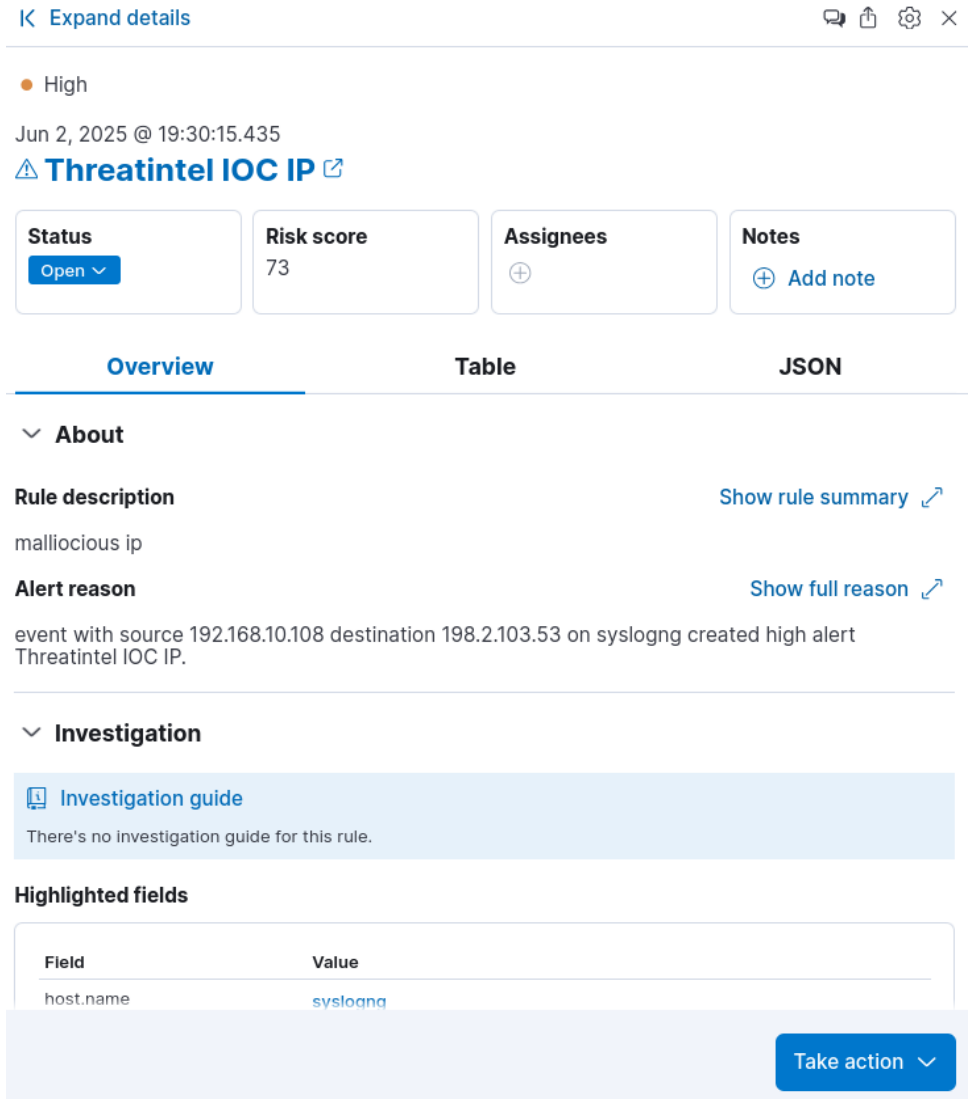
Showing 1-20 of 1245 rules | Selected 0 rules | Select all 1245 rules | Bulk actions | Refresh | Clear filters | Updated now | On

Rule			Risk s...	Severity	Last run	Last response	Last updated	Notify	Enabled
Suspicious Modprobe File Event	0/1 integrations	5	21	Low	1 hour ago	Succeeded	Mar 1, 2025 @ 15:32:5...		
Trap Signals Execution	0/2 integrations	9	21	Low	1 hour ago	Succeeded	Mar 1, 2025 @ 15:32:4...		
System Owner/User Discovery Linux	0/2 integrations	8	21	Low	1 hour ago	Succeeded	Mar 1, 2025 @ 15:32:4...		
System Hosts File Access	0/2 integrations	9	21	Low	1 hour ago	Succeeded	Mar 1, 2025 @ 15:32:4...		
Kernel Driver Load	0/1 integrations	7	21	Low	17 minutes ago	Succeeded	Mar 1, 2025 @ 15:32:5...		
ProxyChains Activity	0/4 integrations	10	21	Low	17 minutes ago	Succeeded	Mar 1, 2025 @ 15:32:5...		
Masquerading Space After Filename	0/1 integrations	7	47	Medium	18 minutes ago	Succeeded	Mar 1, 2025 @ 19:00:5...		
Hping Process Activity	0/4 integrations	10	47	Medium	18 minutes ago	Succeeded	Mar 1, 2025 @ 15:32:4...		
SSH Authorized Keys File Modification	0/1 integrations	8	47	Medium	19 minutes ago	Succeeded	Mar 1, 2025 @ 15:32:5...		
Sudo Heap-Based Buffer Overflow Attempt	0/1 integrations	8	73	High	17 minutes ago	Succeeded	Mar 1, 2025 @ 15:32:4...		
Sudoers File Modification	0/1 integrations	7	47	Medium	17 minutes ago	Succeeded	Mar 1, 2025 @ 15:32:4...		

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Ukážka ELK SIEM – Kibana Alerts

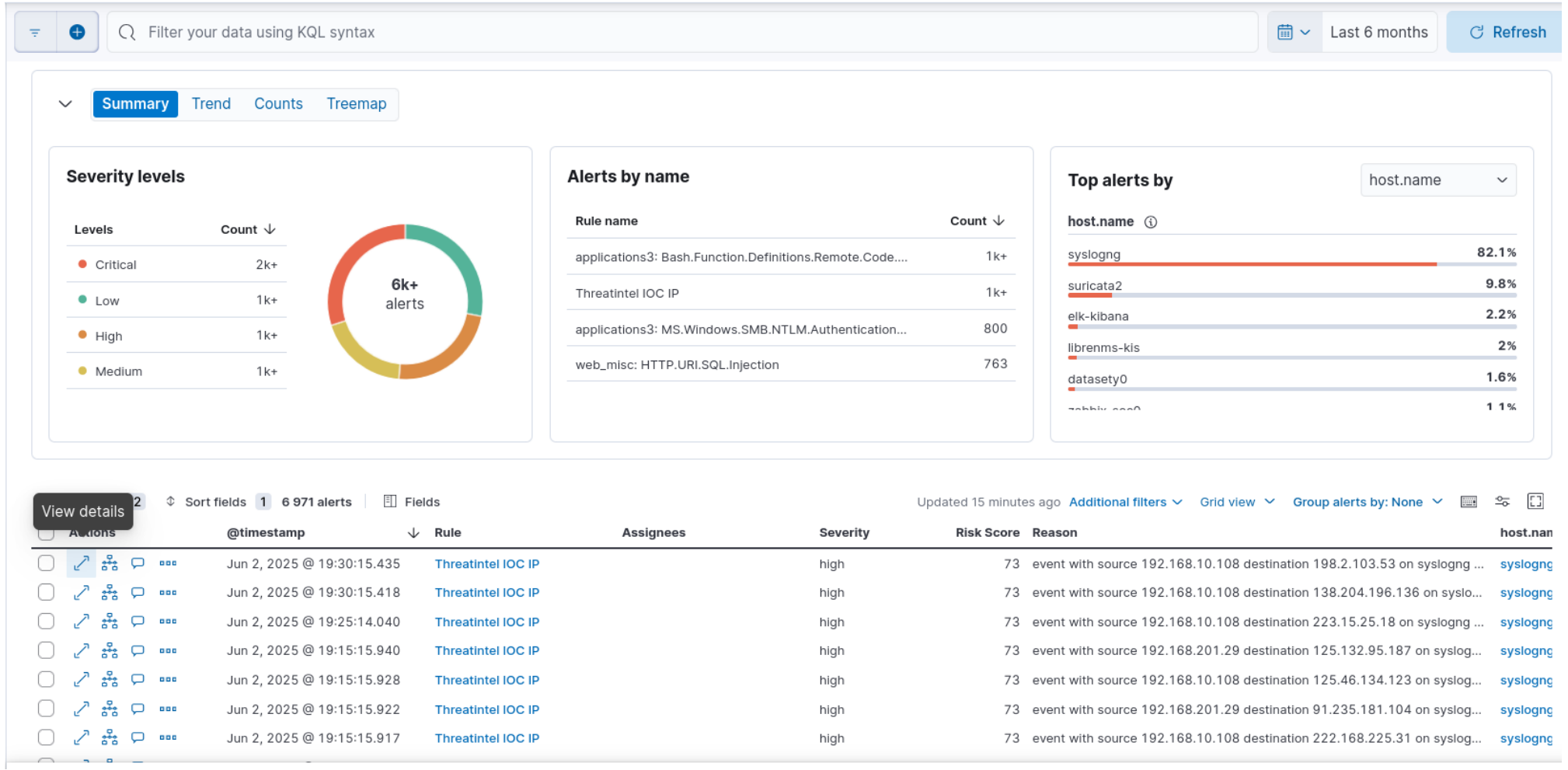
- Alerty vznikajú, keď ich vygeneruje nejaké detekčné pravidlo
- Do alertu sa nahrajú informácie, ktoré spustili detekčné pravidlo
- Alert obsahuje tieto základné informácie:
  - Meno alertu
  - Časovú pečiatku
  - Risk Score 0-100, 0=málo závažné, 100=kritické
  - Popis pravidla, ktoré alert vytvorilo
  - Dôvod prečo sa alert spustil
  - Dôležité súvisiace stĺpce



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

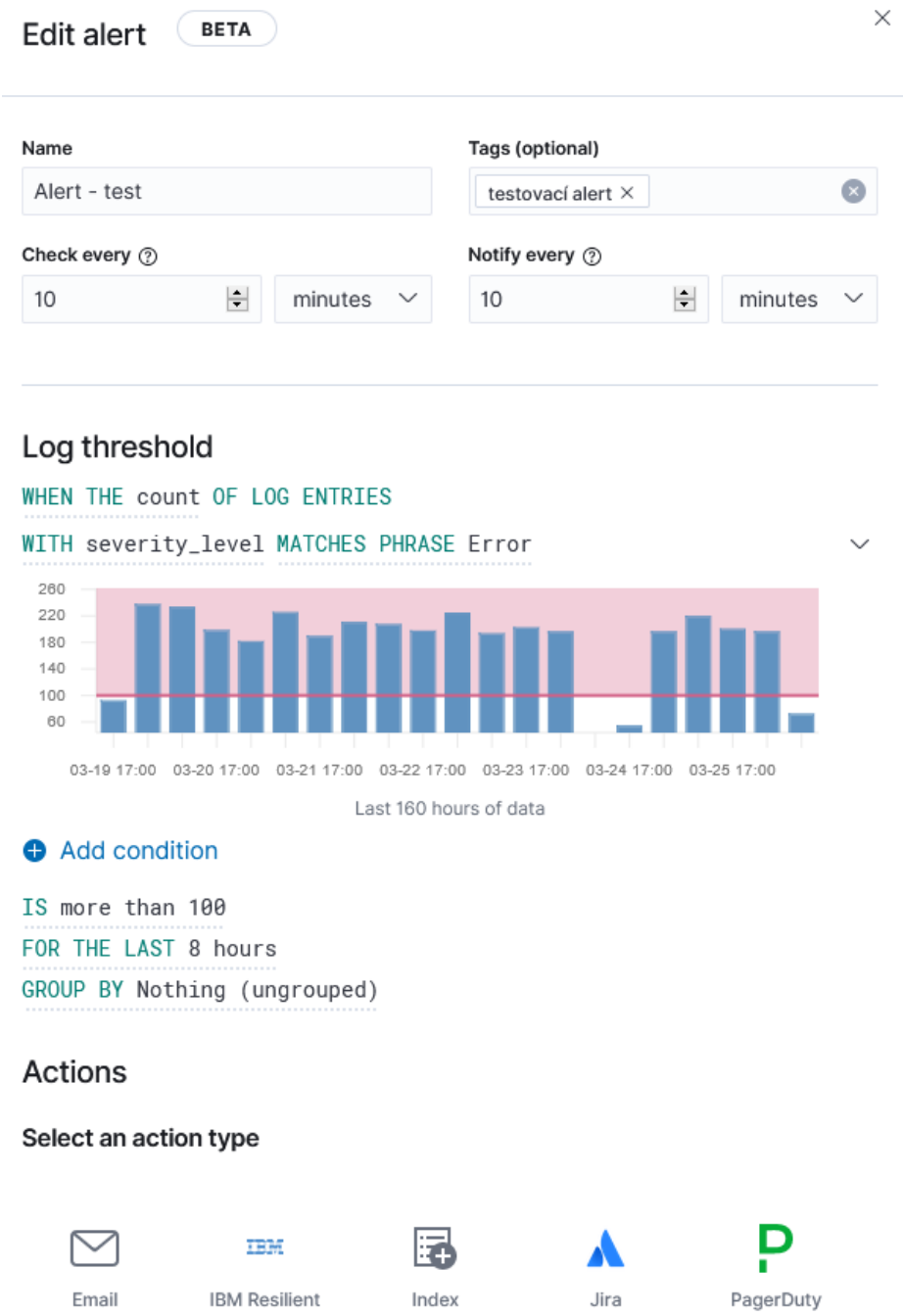
Ukážka ELK SIEM – Kibana Alerts

- Karta Alerts obsahuje prehľadný dashboard alertov, ako aj tabuľku všetkých vyfiltrovaných alertov

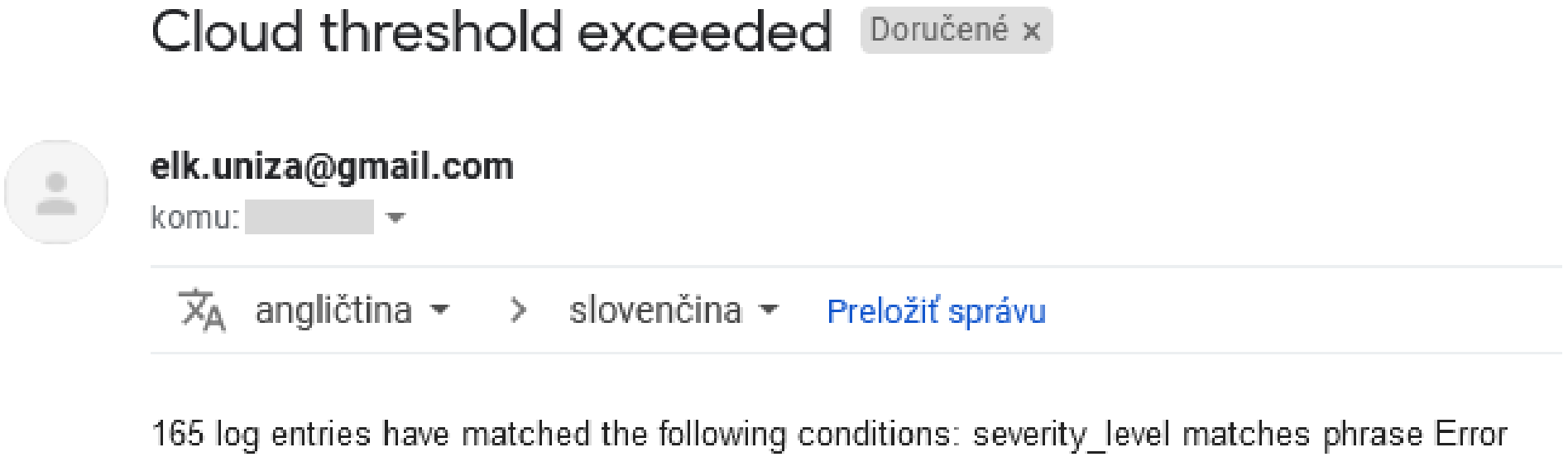


Kibana - tvoba alertov a reportov

- **Alerts/Create alert**
  - Name
    - názov alertu
  - Tags
    - voliteľné
  - Check every
    - ako často sa vyhodnocuje podmienka
  - Notify every
    - ako často sa generujú alerty pri pretrvávaní splnenia podmienky
  - Log threshold
    - query, v ktorej sa definuje podmienka
    - zobrazuje aj interaktívny graf
  - Actions
    - aká akcia sa v prípade splnenia podmienky vykoná



Kibana – vygenerovaný alert



Analýza incidentov v Kibane – Wordpress útok

- pokus o prihlásenie sa hrubou silou do WordPress aplikácie na serveri
- Počet upozornení v čase

- Počty Suricata upozornení

Suricata Signature	Count
ET POLICY Cleartext WordPress Login	2,049
ET SCAN Sipvicious User-Agent Detected (friendly-scanner)	556
ET SCAN Sipvicious Scan	260

- v Kibane sme si vedeli zobraziť aj detail HTTP requestov

```
log=admin&pwd=admin@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=ivaniga&pwd=ivaniga@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=skvarek&pwd=skvarek@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=moravcik&pwd=moravcik@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=mikus&pwd=mikus@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=papan&pwd=papan@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=bridova&pwd=bridova@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=such&pwd=such@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=segec&pwd=segec@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=uramova&pwd=uramova@2019&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
```

Analýza incidentov v Kibane – DNS útok

- DNS útok na cieľovú IP adresu v rozsahu katedrového OpenStack cloudu
- vo výraznej miere prevyšovala prevádzka na DNS port 53
  - Počas časového okna približne 14 hodín sa rapídne zvýšila prevádzka >

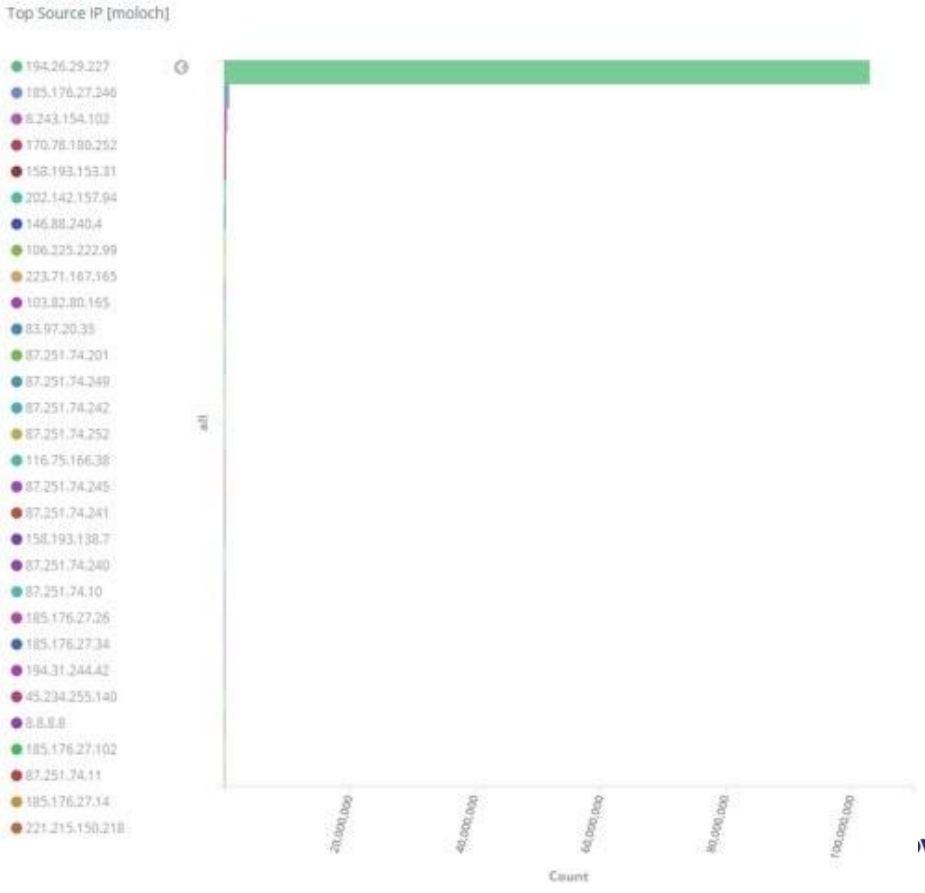
- vygenerované Suricata upozornenia >

Suricata Signature	Count
GPL DNS named version attempt	1,749

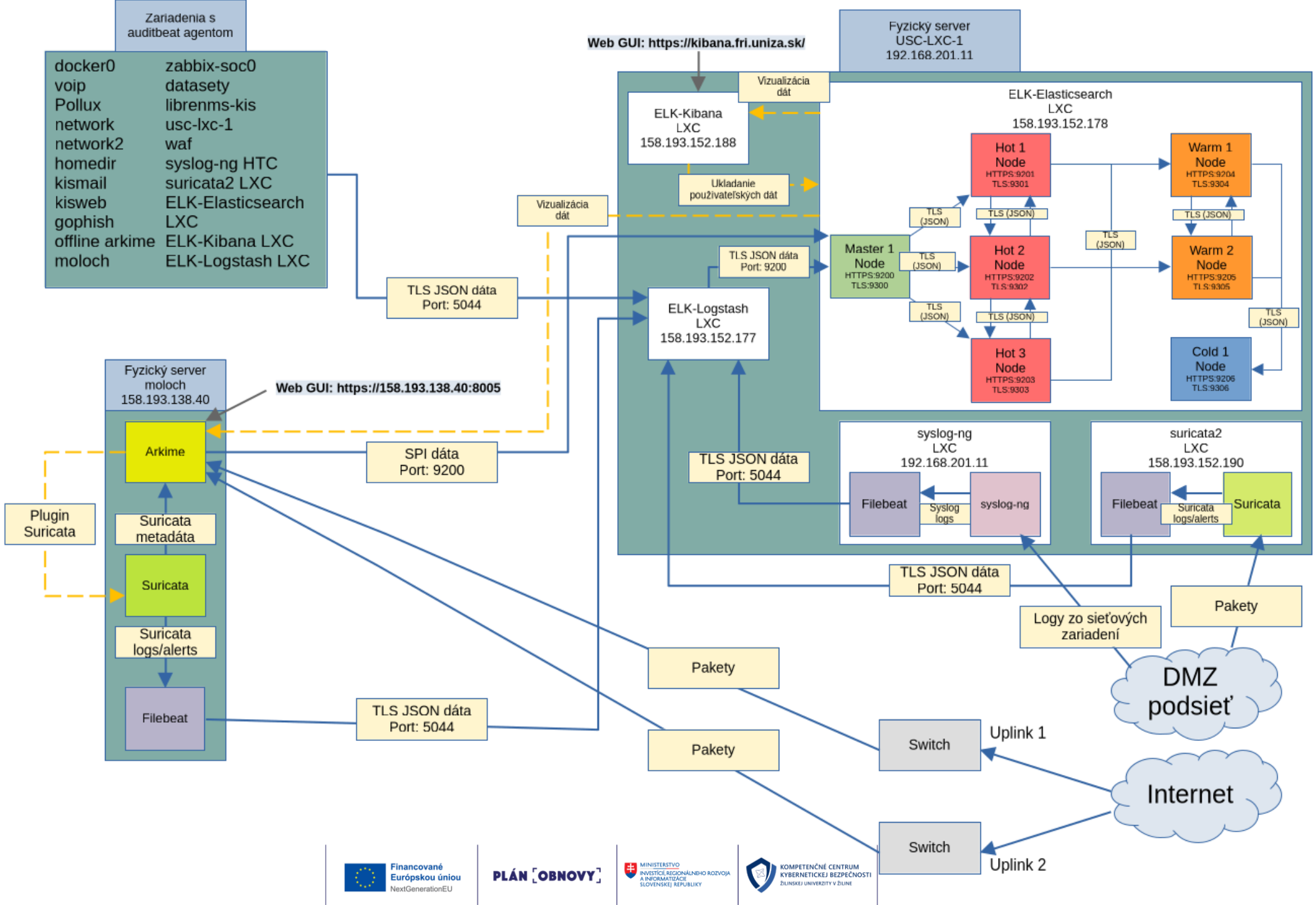
- DNS útok – zdrojové IP adresy na mape >

Analýza incidentov v Kibane – DNS útok

- Podľa cieľových portov ani podľa cieľových IP sme nič podozrivé nezistili
- Až pri analýze zdrojových IP sme zistili, že išlo o toky pochádzajúce z jedného zdroja na všetky IP z fakultného rozsahu, na porty od 1 po 65000. Suricata pri tejto podozrivej prevádzke nevygenerovala žiadne signatúry.



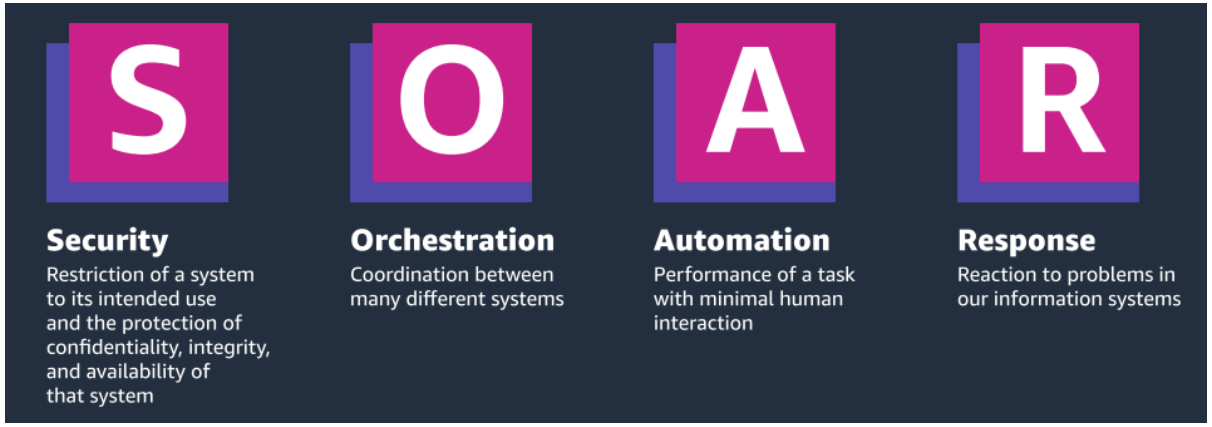
srcIp	dstIp	dstPort
194.26.29.227	158.193.128.74	1
194.26.29.227	158.193.128.74	2
194.26.29.227	158.193.128.74	3
194.26.29.227	158.193.128.74	4
194.26.29.227	158.193.128.74	5
194.26.29.227	158.193.128.74	6
194.26.29.227	158.193.128.74	7
194.26.29.227	158.193.128.74	9
194.26.29.227	158.193.128.74	10
194.26.29.227	158.193.128.74	11
194.26.29.227	158.193.128.74	12
194.26.29.227	158.193.128.74	14

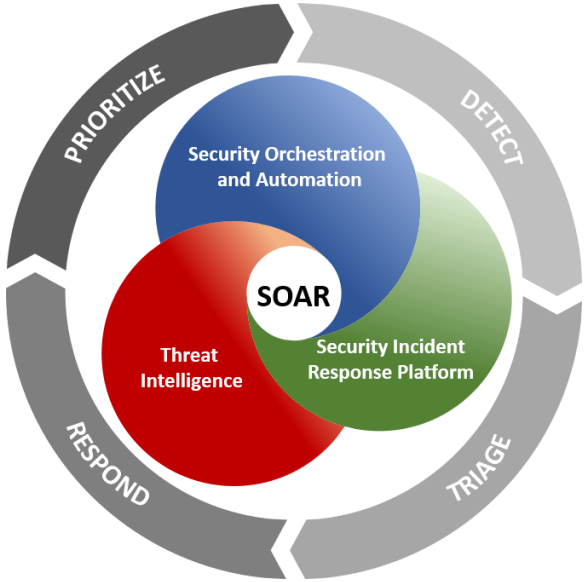

Zariadenia s auditbeat agentom
docker0
voip
Pollux
network
network2
homedir
kismail
kisweb
gophish
offline arkime
moloch
zabbix-soc0
datasety
librenms-kis
usc-lxc-1
waf
syslog-ng HTC
suricata2 LXC
ELK-Elasticsearch LXC
ELK-Kibana LXC
ELK-Logstash LXC
Web GUI: https://kibana.fri.uniza.sk/
Fyzický server USC-LXC-1 192.168.201.11
Vizualizácia dát
ELK-Kibana LXC 158.193.152.188
Ukladanie používateľských dát
ELK-Elasticsearch LXC 158.193.152.178
Hot 1 Node HTTPS:9201 TLS:9301
Hot 2 Node HTTPS:9202 TLS:9302
Hot 3 Node HTTPS:9203 TLS:9303
Warm 1 Node HTTPS:9204 TLS:9304
Warm 2 Node HTTPS:9205 TLS:9305
Cold 1 Node HTTPS:9206 TLS:9306
Master 1 Node HTTPS:9200 TLS:9300
TLS (JSON)
TLS JSON dáta Port: 9200
TLS JSON dáta Port: 5044
ELK-Logstash LXC 158.193.152.177
Fyzický server moloch 158.193.138.40
Web GUI: https://158.193.138.40:8005
Arkime
SPI dáta Port: 9200
Plugin Suricata
Suricata metadáta
Suricata
Suricata logs/alerts
Filebeat
syslog-ng LXC 192.168.201.11
Filebeat
Syslog logs
syslog-ng
suricata2 LXC 158.193.152.190
Filebeat
Suricata logs/alerts
Suricata
Logy zo sieťových zariadení
Pakety
DMZ podsieť
Switch
Uplink 1
Internet
Switch
Uplink 2
Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

SOAR – Security Orchestration, Automation and Response

Čo je SOAR?

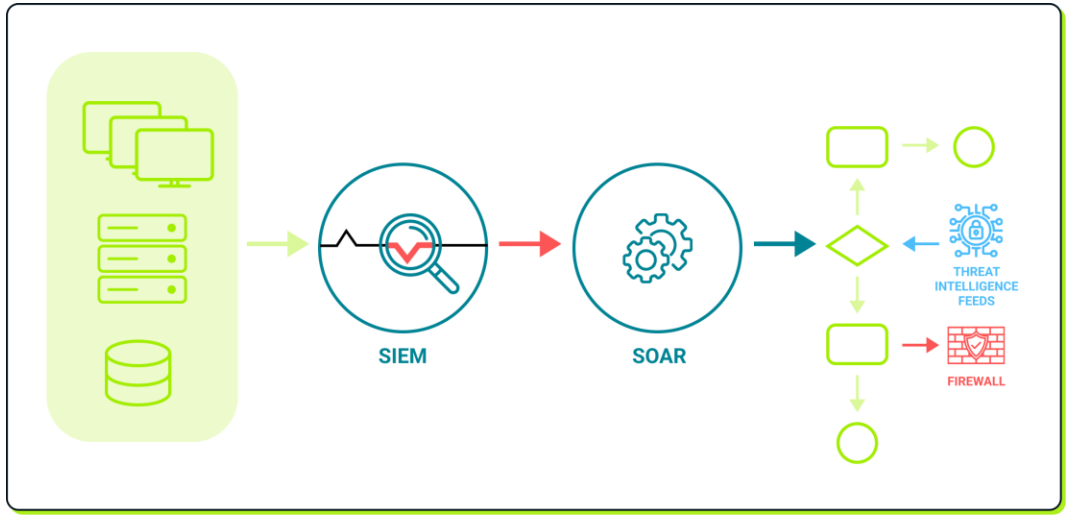
- SOAR (Security Orchestration, Automation and Response) umožňuje:
  - **Orchestráciu** – prepojenie rôznych bezpečnostných nástrojov a automatizáciu ich spolupráce
  - **Automatizáciu** – opakované úlohy vykonáva automaticky (blokovanie IP, vytváranie ticketov, obohatenie dát…)
  - **Reakciu na incidenty** – rýchle rozhodovanie a vykonanie krokov, ktoré zvyčajne robia analytici manuálne
- Cieľom je **zrýchliť reakciu**, znížiť manuálnu prácu a podporiť bezpečnostné tímy pri spracovaní veľkého množstva incidentov.



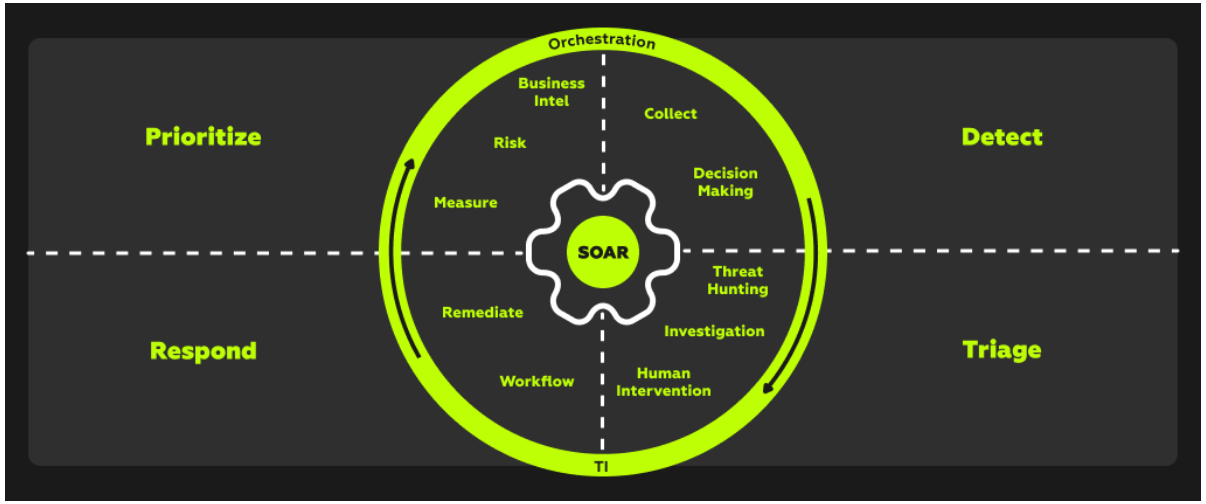


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Prečo potrebujeme SOAR?



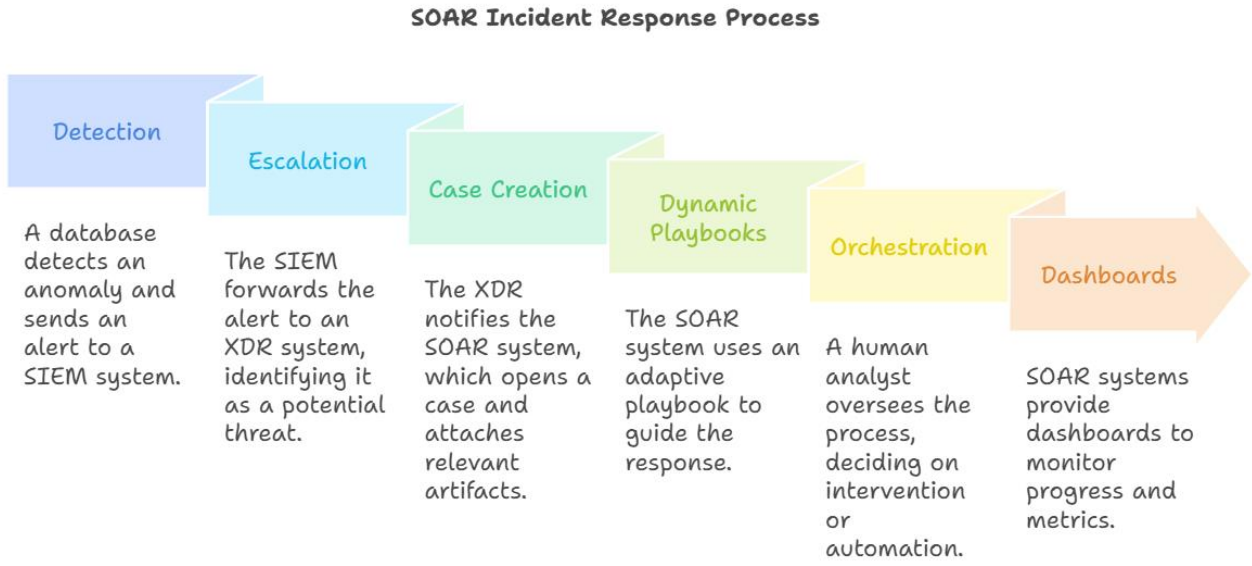
- Moderné prostredia generujú množstvo alertov → analytici nemajú kapacitu kontrolovať všetko manuálne
- SOAR automatizuje rutinné činnosti, aby analytik riešil len to najdôležitejšie
- Znižuje chybovosť, zrýchľuje reakcie a umožňuje presné dodržiavanie procesov
- SOAR umožňuje:
  - Automatické obohatenie alertov (IP reputation, WHOIS, geolokácia…)
  - Automatické blokovanie alebo karantenizáciu zariadení
  - Prepojenie so SIEM → pri detekcii spustí akciu
  - Odpovedanie podľa definovaných playbookov



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

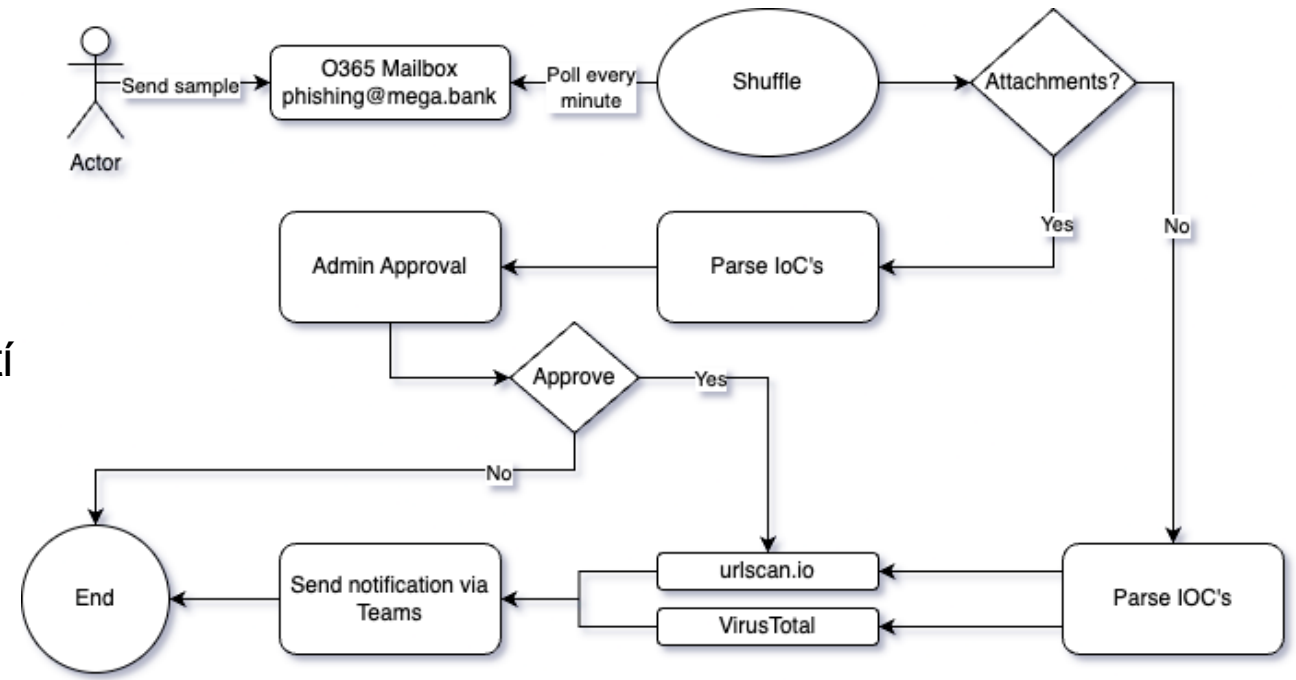
Hlavné funkcie SOAR

- **Orchestrácia -** prepojenie bezpečnostných produktov a nástrojov:
  - SIEM ↔ Firewall (napr. ELK ↔ Fortigate)
    - Prepojenie cez API – SIEM dokáže posielať príkazy do firewallu (napr. blokovať IP adresu)
    - Firewall zároveň posiela logy do SIEMu (napr. FortiGate → syslog / API → ELK) Firewall
  - SIEM ↔ EDR (napr. ELK ↔ Fortigate)
    - SIEM prijíma alerty z EDR systému (napr. Defender, CrowdStrike)
    - Naopak, SIEM môže iniciovať príkaz (napr. izolovať endpoint) cez EDR API
- **Automatizácia -** vytváranie playbookov pre opakované procesy:
  - Automatická kontrola IP/URL v reputačných databázach
    - SOAR (napr. Shuffle) automaticky kontroluje IP adresy, URL alebo domény, ktoré sa objavia v alertoch zo SIEMu
  - Automatické vytvorenie ticketu pri incidente
  - Automatické blokovanie na firewalli
- **Reakcia na incidenty -** SOAR umožňuje:
  - poloautomatickú reakciu (analytik potvrdí krok)
  - plne automatickú reakciu (vykonáva sám)
  - manuálne zásahy cez jednotné rozhranie



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY

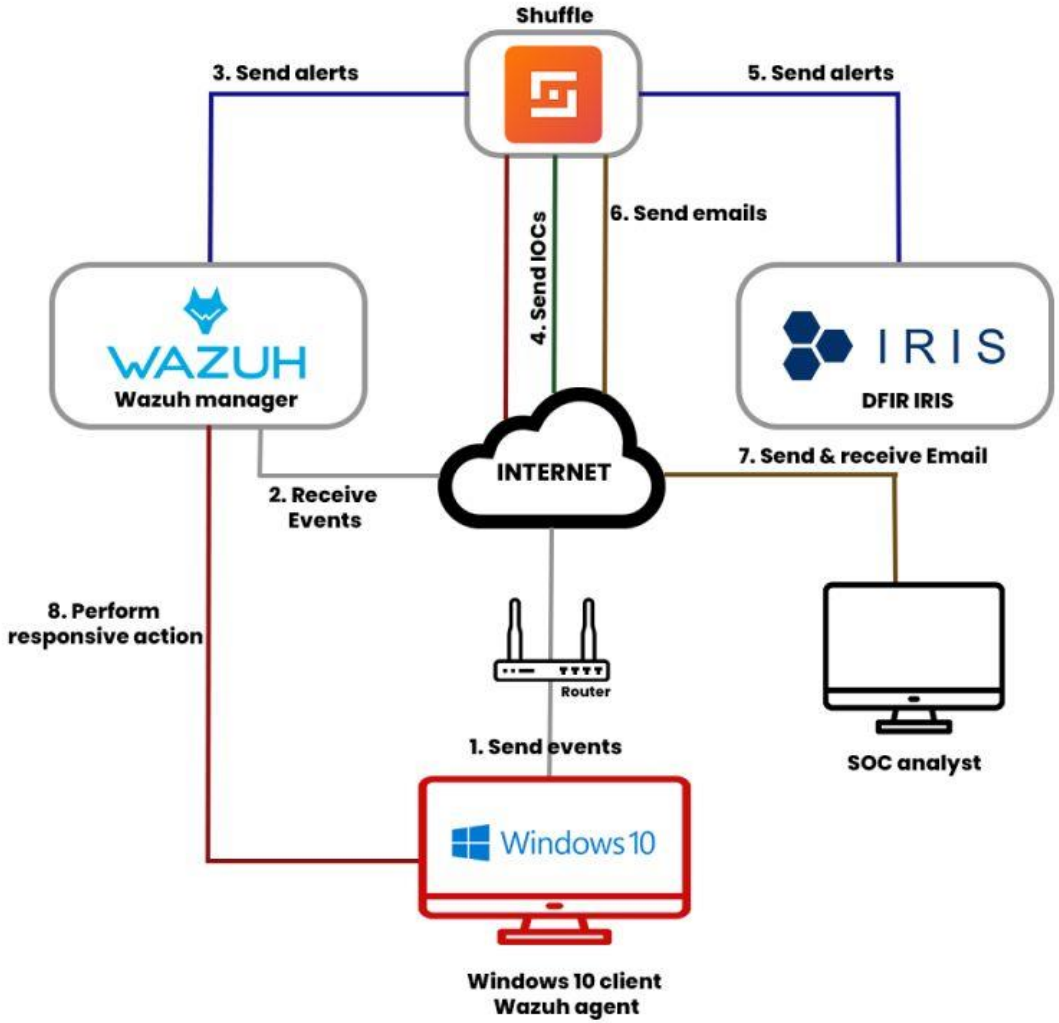
Scenár - podozrivý e-mail



- **1) Detekcia incidentu:** SIEM zachytí alert:
  - „Používateľ nahlásil e-mail obsahujúci podozrivý odkaz na login-microsoft-support[.]com.“
  - Alert sa automaticky odošle do SOAR platformy
- **2) Automatizácia a orchestrácia:** SOAR spustí playbook pre phishingové incidenty:
  - Prepojenie na Threat Intelligence feedy (VirusTotal, AbuseIPDB, MISP).
  - Ak má doména „malicious score“ > *80*, označí ju ako škodlivú.
  - Vytvorenie ticketu: Automaticky založí incident v ServiceNow/Jira so všetkými informáciami a výsledkami kontrol.
- **3) Reakcia na incident:** Podľa výsledkov playbooku SOAR rozhodne:
  - Ak je hrozba **potvrdená**: Automaticky blokuje doménu a IP na firewalle. Izoluje endpoint v EDR.
  - Ak je hrozba **neistá**: SOAR požiada analytika o potvrdenie pokračovania v blokovaní

Scenár – udalosť na Win 10 klientovi

1. **Wazuh Agent (klient Windows 10)** odosiela udalostné dáta.
2. **Wazuh Manager** prijíma a spracúva tieto udalosti.
3. **Upozornenia (alerty)** sú odoslané do nástroja **Shuffle** na orchestráciu.
4. **Shuffle** obohacuje **IOC (Indicators of Compromise – indikátory kompromitácie)**.
5. **Alerty** sú následne odoslané do **DFIR-IRIS** na hlbšiu analýzu a vyšetrovanie.
6. **E-mailové notifikácie** sú spustené s cieľom informovať **SOC analytikov**.
7. **Analytici** analyzujú alerty a komunikujú prostredníctvom e-mailov v systéme **IRIS**.
8. **Reakčné opatrenia** sú vykonané späť na **Wazuh klientovi**, čím sa uzatvára celý incidentný cyklus.

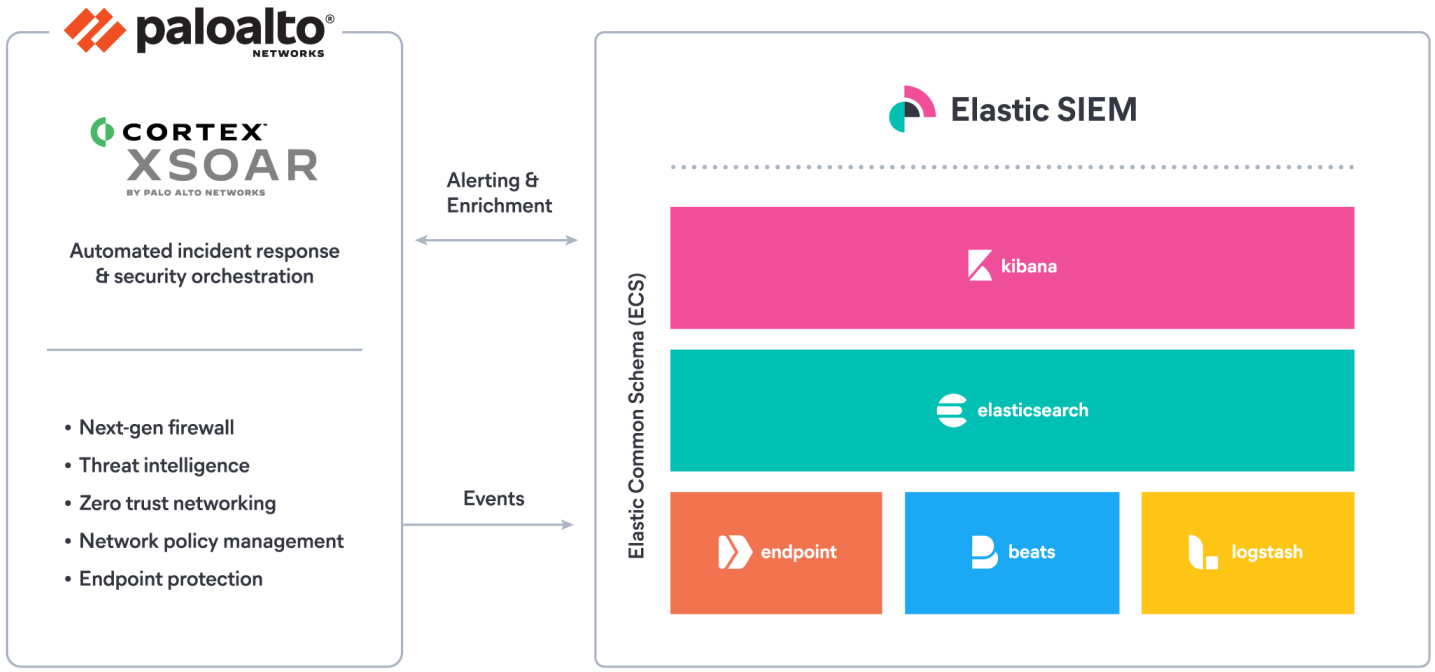


SOAR architektúra

- **Komponenty:**
  - Konektory pre integráciu nástrojov - Umožňujú prepojiť SOAR s rôznymi bezpečnostnými systémami a službami
    - API konektory (REST, SOAP) – napr. pre SIEM (Splunk, ELK, QRadar), EDR (CrowdStrike, Defender), Firewally (Fortigate, Palo Alto)
    - Webhooky – event-driven notifikácie (napr. Slack, MS Teams, Jira)
  - Playbook engine – vykonáva automatizačné kroky
    - Vyhodnocuje podmienky
    - Volá API volania do integrácií (konektorov)
    - Spracováva odpovede, rozhoduje o ďalších krokoch
  - Ticketing a workflow – SOAR môže mať vlastný jednoduchý ticketing systém (napr. Hive, Shuffle Incident Tracker), alebo sa integruje s externými nástrojmi (Jira, ServiceNow)
- **Typické SOAR úlohy**
  - Vyžiadanie logov zo SIEM-u
  - Blokovanie prístupu
  - Karantenizácia zariadenia
  - Vytváranie ticketov
  - Automatizované mailové notifikácie

Príklady SOAR

- **Platené SOAR systémy:**
  - Palo Alto Cortex XSOAR
  - IBM Resilient
  - Splunk Phantom
  - Rapid7 InsightConnect
- **Open-source a bezplatné SOAR systémy:**
  - Shuffle
  - TheHive
  - Cortex
  - StackStorm



SHUFFLE

TheHive

StackStorm

Shuffle – SOAR platforma

- Open-source SOAR platforma s podporou vizuálneho vytvárania workflow-ov
- Založená na princípe low-code/no-code automatizácie
- Využíva prepojenie cez REST API a webhooky
- Modularita umožňuje prepojenie desiatok bezpečnostných systémov
- Vhodná pre menšie SOC, univerzity, štátne inštitúcie aj podnikové prostredí
- Používaný hlavne pre:
  - obohacovanie incidentov
  - automatizáciu rozhodovania
  - vytváranie playbookov na reakciu
  - prepojenie viacerých nástrojov do jedného logického celku

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

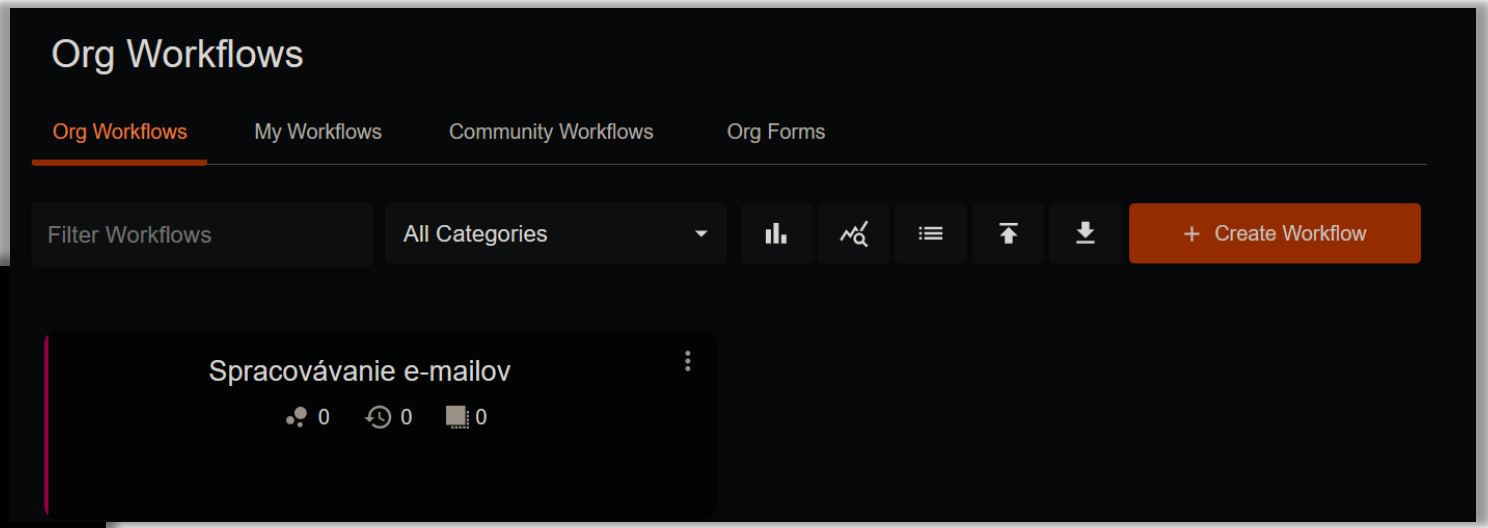
Shuffle – Workflows

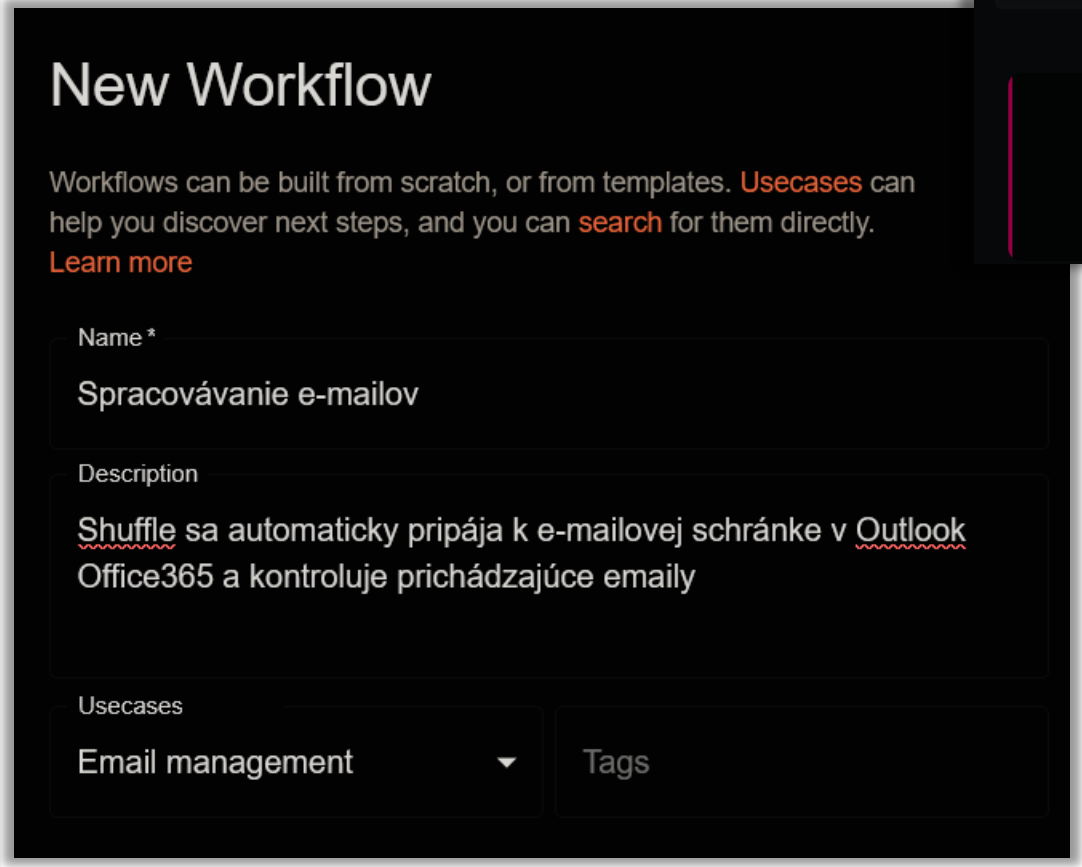
- Technický proces, ktorý vykonáva sériu krokov automaticky
- Určuje ako sa niečo robí (postup, logika, kroky)
- Pracuje s aplikáciami, dátami, podmienkami, filtrami a akciami
  - Napr. načítanie e-mailov z Outlooku → filtrovanie → vytvorenie ticketu
- Znižujú manuálnu prácu – napr. automatické čítanie e-mailov, vytváranie ticketov alebo upozornení
- Možnosť vytvárať subflowy – podprocesy na ďalšie automatické úlohy
- Liquid formátovanie – pre pokročilé logické podmienky a prácu s dátami
- Použitie v bezpečnostných, IT aj biznis automatizáciách

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Security Orchestration, Automation and Response

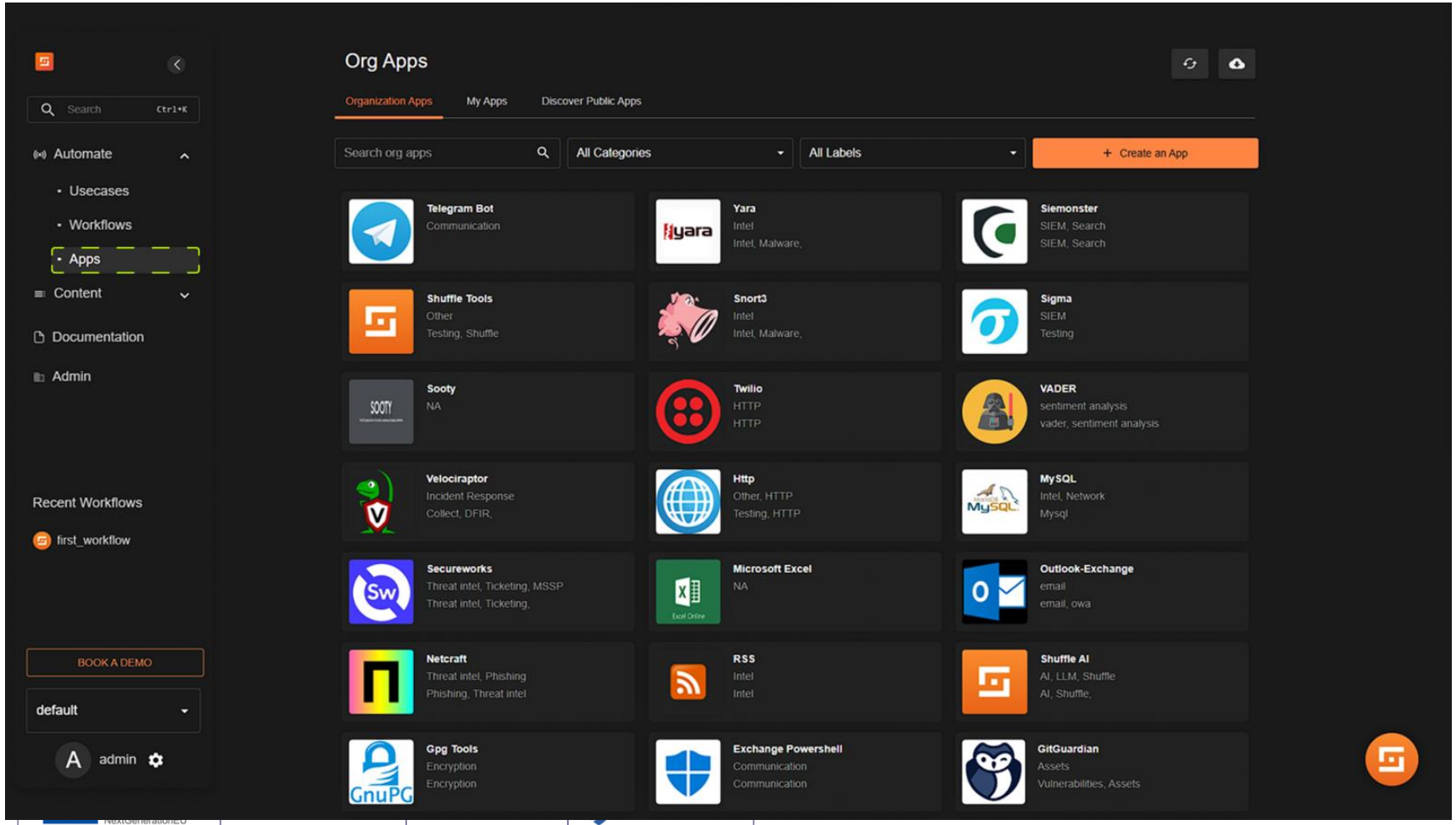
Vytvorenie nového Workflow v Shuffle



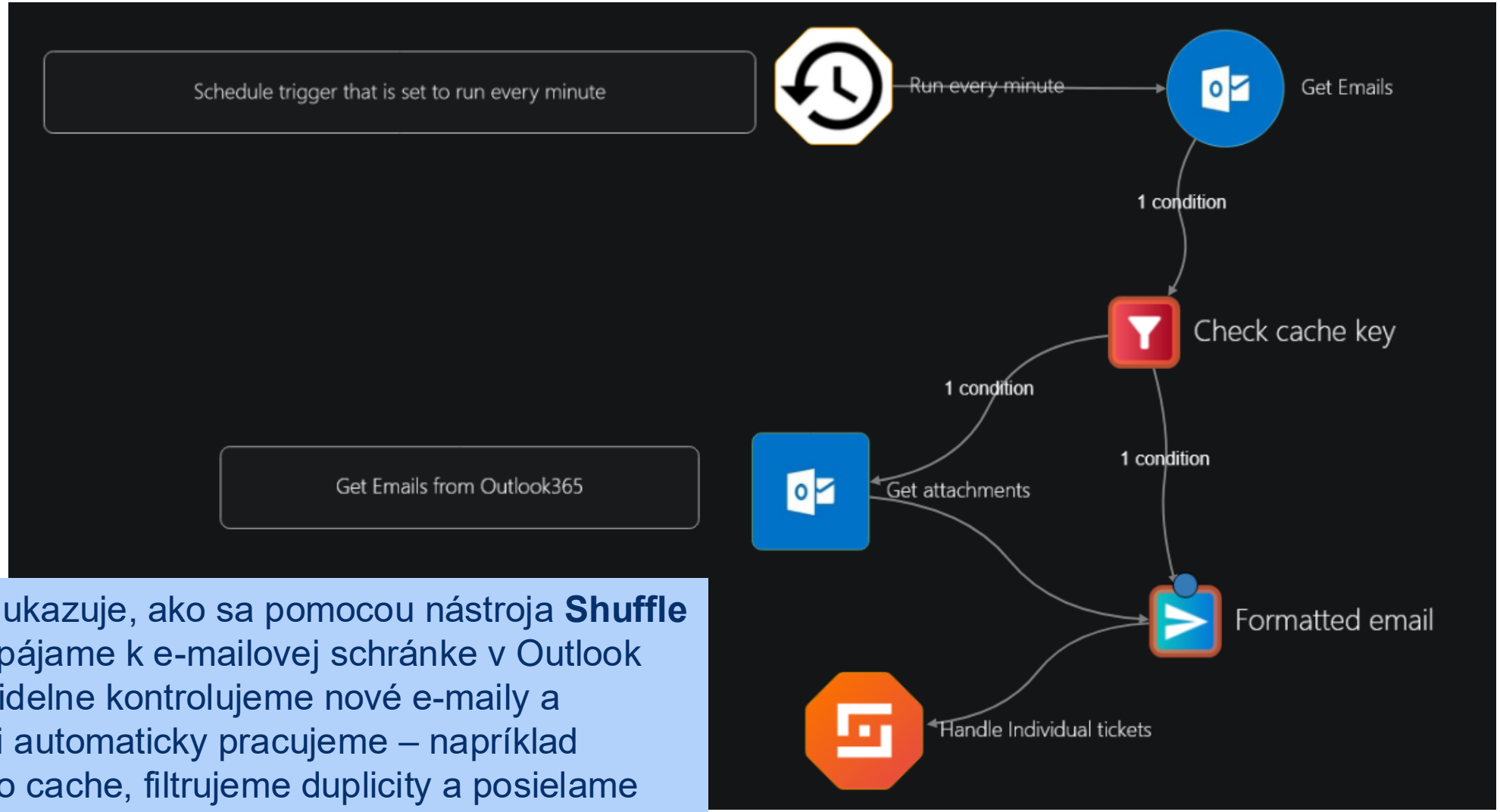


Aplikácie v Shuffle

- Shuffle má momentálne viac ako 2 000 hotových aplikácií, ktoré vývojári a komunita neustále rozširujú



Príklad workflow v Shuffle na spracovávanie e-mailov

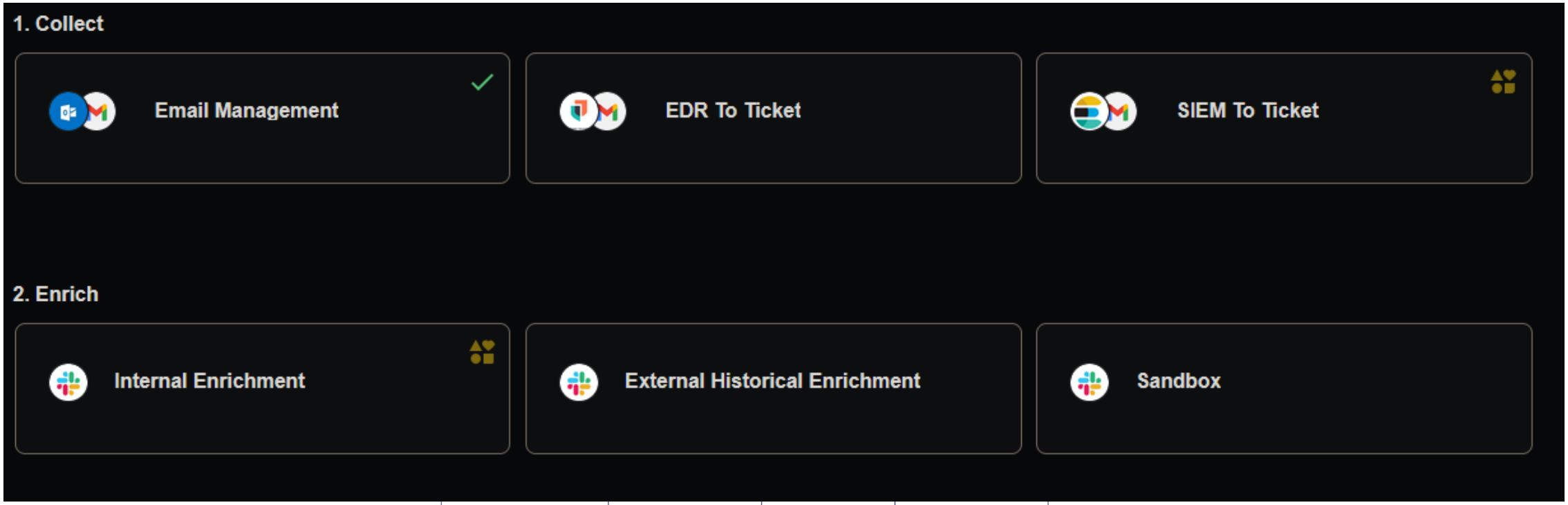


Tento workflow ukazuje, ako sa pomocou nástroja **Shuffle** automaticky pripájame k e-mailovej schránke v Outlook Office365, pravidelne kontrolujeme nové e-maily a následne s nimi automaticky pracujeme – napríklad ukladáme ich do cache, filtrujeme duplicity a posielame ďalej do subflow na vytváranie ticketov alebo upozornení v iných systémoch.

Shuffle – Usecase

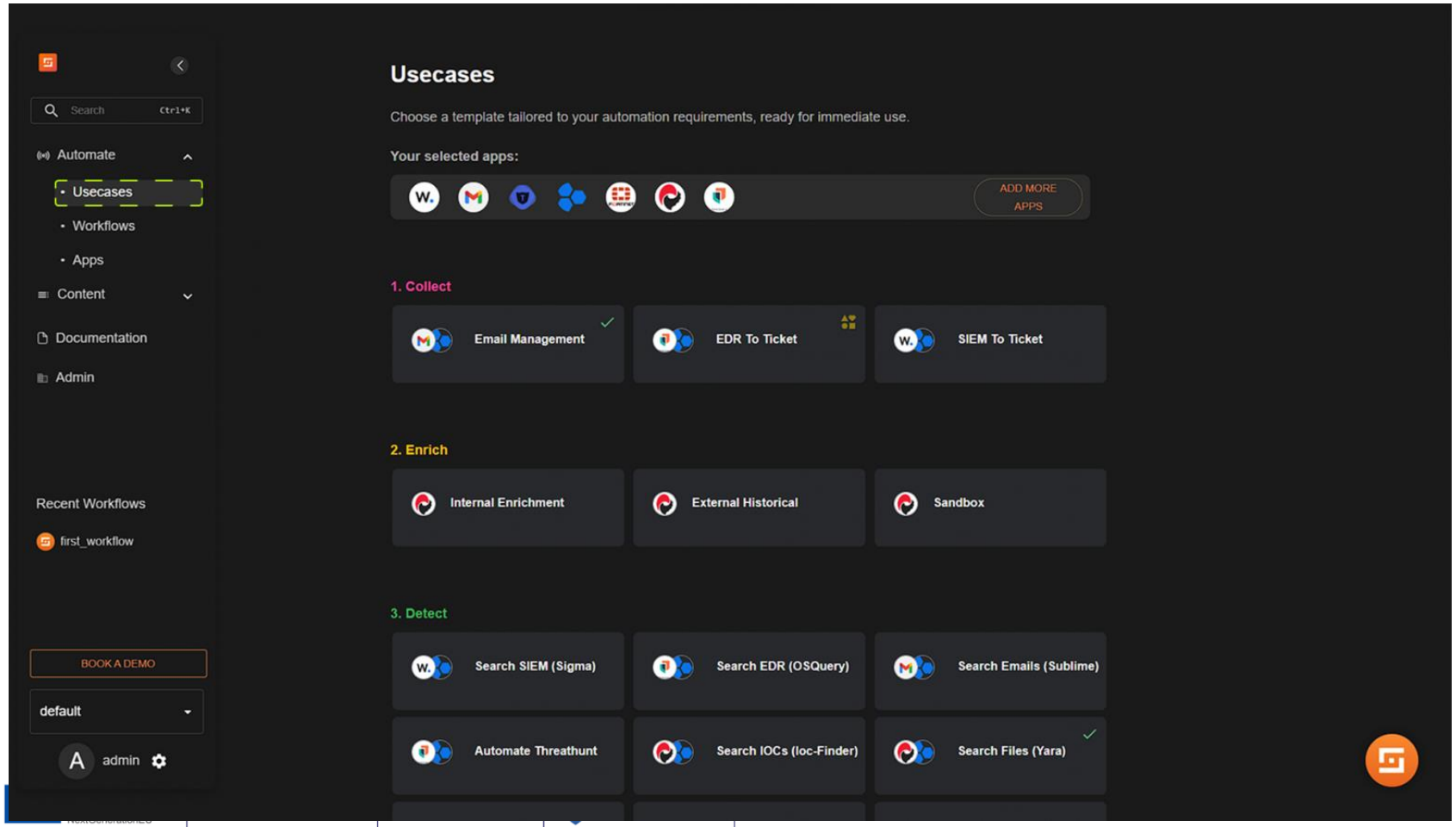
Na obrazku je ilustrácia usecasov, po kliknutí na email management (zelená ikonka znamená, že je implementovaný) sa viem dostať priamo na daný workflow

- Reálny scenár použitia – opisuje prečo sa workflow používa
- Ukazuje aký problém rieši alebo aký cieľ dosahuje
- Pomáha pochopiť prínos automatizácie
- Napr. „Automatické vytváranie ticketov z e-mailov“ alebo „Detekcia phishingu“



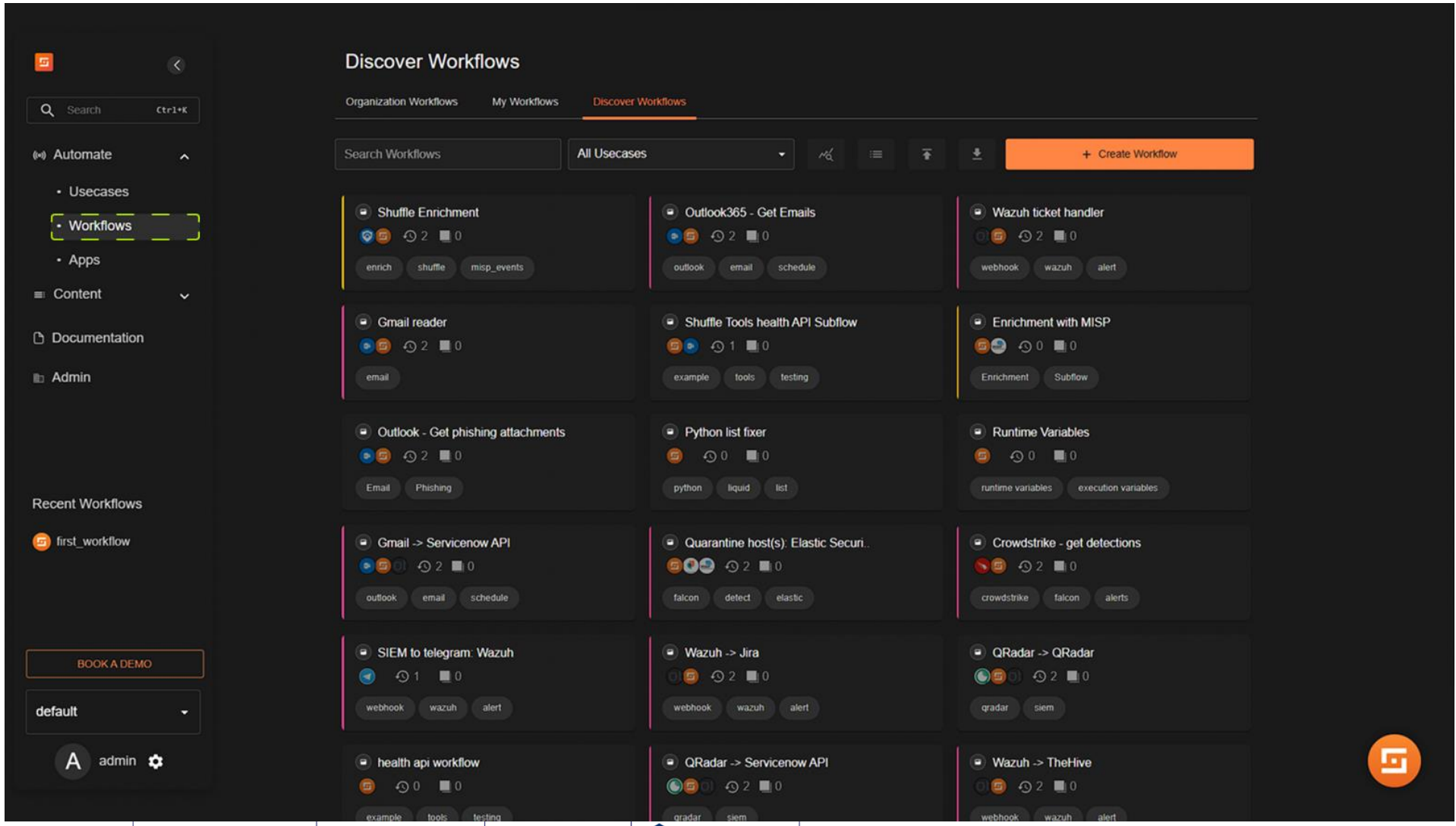
Usecases

- Tu nájdeme päť hlavných kategórií (podobných jednej verzii rámca kybernetickej bezpečnosti NIST):
  - *Zhromažďovanie* ,
  - *Obohatenie*,
  - *Detekcia*,
  - *Reakcia* ,
  - *Overenie*
    - opisujú celý cyklus riešenia KBI.
- Každá kategória obsahuje niekoľko preddefinovaných možností akcie.



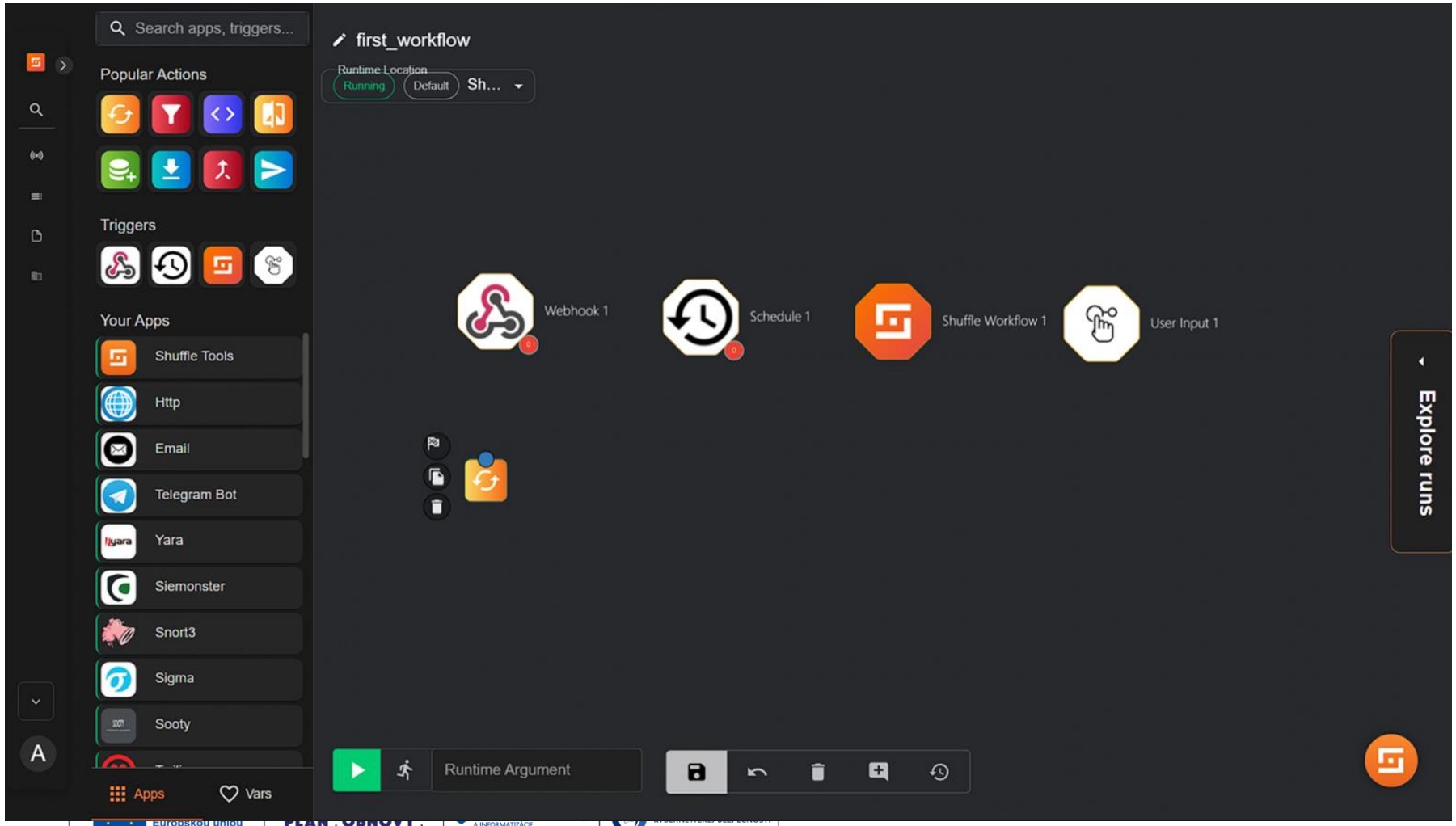
Workflows

- Tu si môžeme vytvoriť vlastné procesy alebo použiť vopred pripravené a overené možnosti.



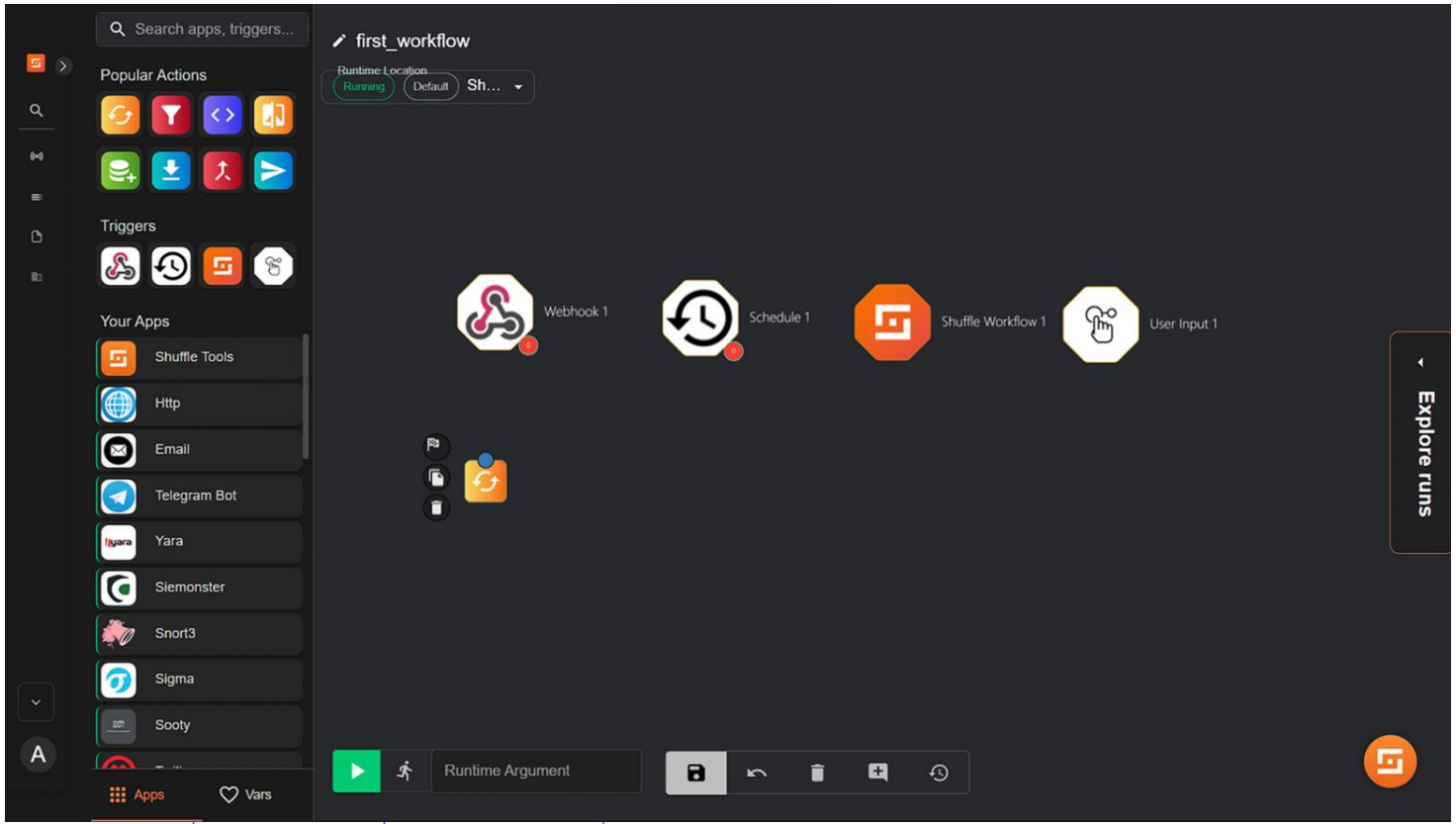
Hlavné kategórie nástrojov pre workflows

- Pracovné postupy používajú 4 hlavné kategórie nástrojov:
  - **aplikácie**,
  - **spúšťače** ,
  - **podmienky**
  - **premenné** na vytvorenie výkonnej automatizácie.



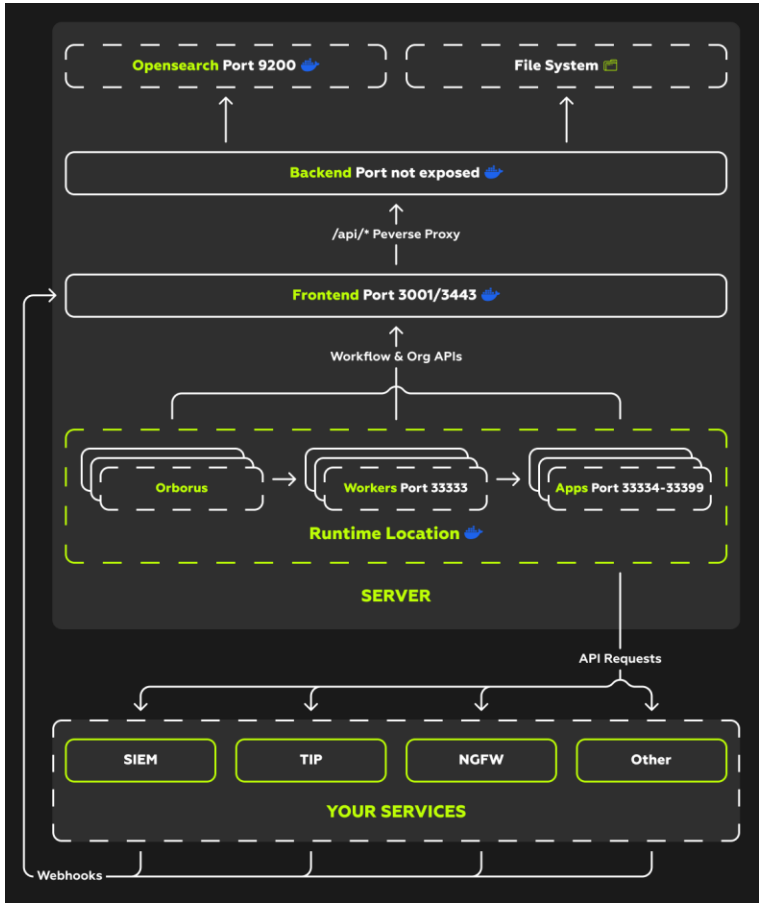
Hlavné kategórie nástrojov pre workflows

- Sekcia **Vaše aplikácie** obsahuje zoznam aplikácií pripravených na implementáciu v procese.
- Sekcia **Spúšťače** obsahuje štyri hlavné **spúšťače** – operátory používané na automatické spustenie pracovného postupu. Najčastejšie akceptujú argument spustenia, ktorý sa použije na spustenie daného pracovného postupu.
- Obrázok zobrazuje: ***Webhook*** (spracovanie údajov v reálnom čase prostredníctvom metód HTTP), ***Plán*** (lokálne plány, podobne ako Cron), ***Náhodný pracovný postup*** (spúšťanie procesov v rámci iných procesov, podobne ako podpoložkové postupy) a ***Používateľský vstup*** (používateľský vstup, povolenie).
- Sekcia **Obľúbené akcie** obsahuje často používané akcie (spustenie kódu Pythonu, extrahovanie metadát zo súboru a ďalšie) z vstavanej aplikácie Shuffle Tools. Zoznam všetkých vstavaných akcií získate kliknutím na samotnú aplikáciu a následným kliknutím na ikonu dokumentov, čím sa otvorí dokumentácia aplikácie (toto funguje pre všetky aplikácie).



Architektúra Shuffle

- Frontend (UI)
  - vizuálny editor workflowov
  - správa integrácií
  - stroje na správu používateľov, tokenov, logov
- Backend (UI)
  - spracováva udalosti
  - riadi spúšťanie playbookov
  - kontroluje logiku a postup krokov
- Workers
  - vykonávajú jednotlivé moduly
  - umožňujú paralelné spracovanie
  - komunikuje s API externých systémov
- Database (SQLite / PostgreSQL podľa nasadenia)
  - ukladá konfigurácie, playbooky, comms

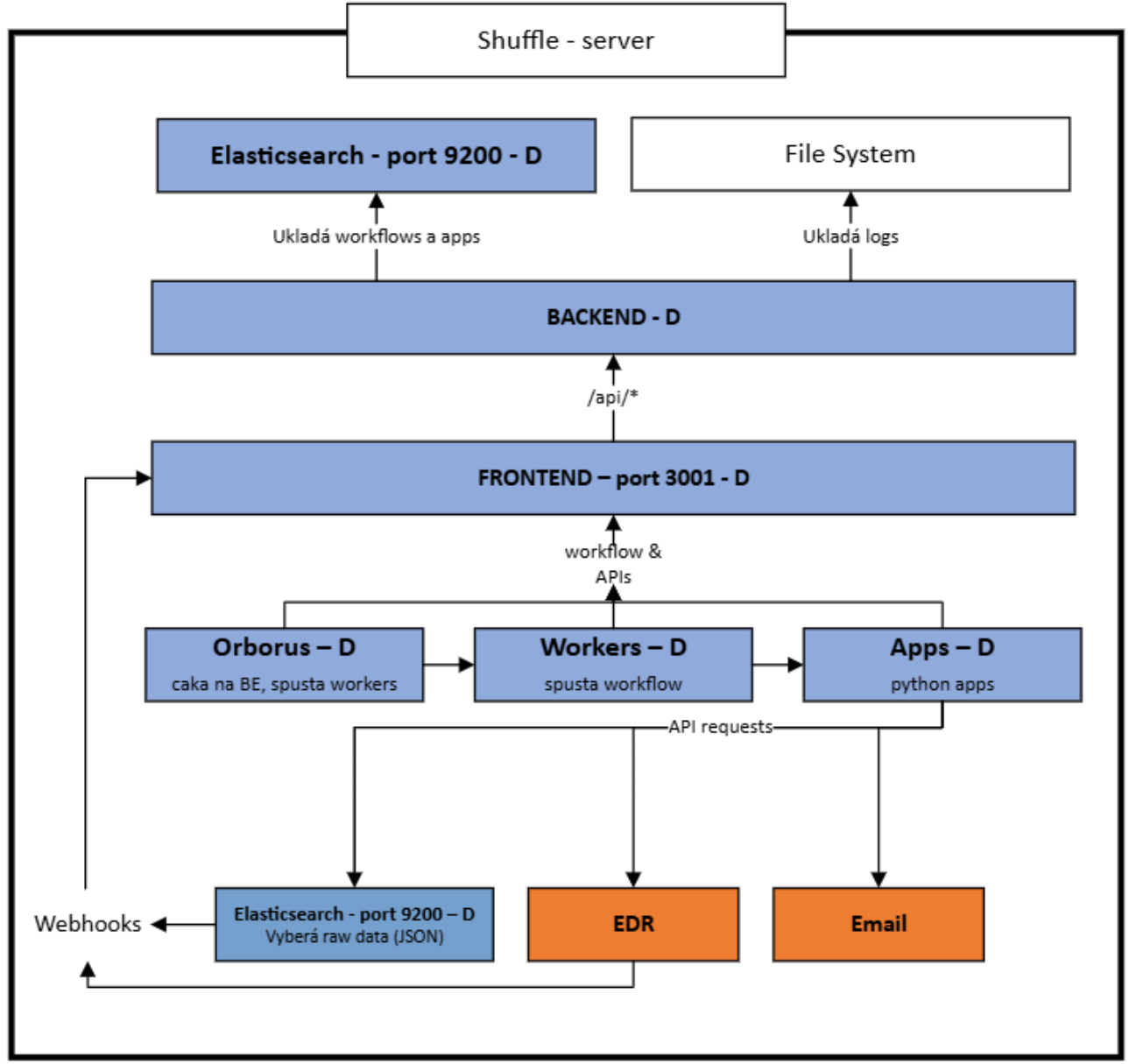


- Integrations Marketplace
  - stovky hotových integrácií (Elastic, Wazuh, Cortex, Slack, MISP…)
  - jednoduché doplnenie vlastnej integrácie cez REST

Prepojenie Shuffle (SOAR) + Elastic (SIEM)

- **Ako to spolu funguje:**
  - Elastic SIEM
    - vytvorí alert (kibana alert / detection rule)
    - pošle alert cez webhook → Shuffle endpoint
  - Shuffle
    - spustí príslušný playbook podľa typu incidentu
    - overí údaje + obohatí IOC
  - Ak je hrozba potvrdená → vykoná akciu
- **Typické akcie:**
  - blokovanie IP
  - zaslanie notifikácie
  - aktualizácia stavu incidentu
  - získanie viac logov z Elasticu (ElasticSearch Search API)

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Otvorená reflexia

- **Zabezpečuje SIEM centralizáciu logov?**
  - a) ÁNO
    b) NIE
- **Aká sú úlohy Logstashu?**
  (2 správne)
  - a) Tvoriť logy
    b) Normalizovať logy
    c) Alertovať
    d) Odoslať logy do databázy
- **Nastal bezpečnostný incident, ale SIEM systém nevytvoril žiaden alert. O ktorý typ alertu podľa pravdivosti sa jedná?**
  - a) True positive
    b) True negative
    c) False positive
    d) False negative
- **Ktorá z nasledujúcich možností najlepšie vystihuje úlohu SOAR platformy v SOC?**
  - A) Slúži primárne na centralizované ukladanie logov a vizualizáciu dát
    B) Automatizuje reakčné postupy, orchestruje nástroje a zjednodušuje incident response
    C) Monitoruje sieťové toky na úrovni L7 a vykonáva DPI analýzu
    D) Slúži na správu používateľských účtov a autentizácie
- **Čo je typickým výsledkom úspešnej implementácie SOAR v SOC?**
  - A) Zvýšenie množstva manuálnej práce analytikov
    B) Spomalenie reakčného času pri incidentoch
    C) Automatizácia rutinných úloh, rýchlejšia reakcia a konzistentné playbooky
    D) Zníženie počtu logov prijímaných od bezpečnostných nástrojov

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

SIEM a SOAR

Monitorovanie bezpečnostných udalostí, riešenie incidentov, forenzná analýza (Blok VI)

Kurz: Špecialista kybernetickej bezpečnosti vo verejnej správe

Mgr. Jana Uramová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Jana.Uramova@fri.uniza.sk