PROJEKT

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

Dashboardy – vizualizácia dát z nástrojov

Previazané s balíkom KPB2
Dashboardy – analýza bezpečnostných udalostí

Previazané s výstupom
V6 – Popis dashbordov, monitorovacieho a reportovacieho systému

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Obsah

Kibana – Dashboard 3
Discover 4
Dasboards 11
Alerts 13
Vyšetrenie bezpečnostného upozornenia 15

Zoznam obrázkov

Obrázok 1 3
Obrázok 2 4
Obrázok 3 4
Obrázok 4 5
Obrázok 5 5
Obrázok 6 6
Obrázok 7 6
Obrázok 8 6
Obrázok 9 7
Obrázok 10 7
Obrázok 11 8
Obrázok 12 8
Obrázok 13 9
Obrázok 14 9
Obrázok 15 10
Obrázok 16 10
Obrázok 17 11
Obrázok 18 12
Obrázok 19 13
Obrázok 20 13
Obrázok 21 14
Obrázok 22 14
Obrázok 23 15

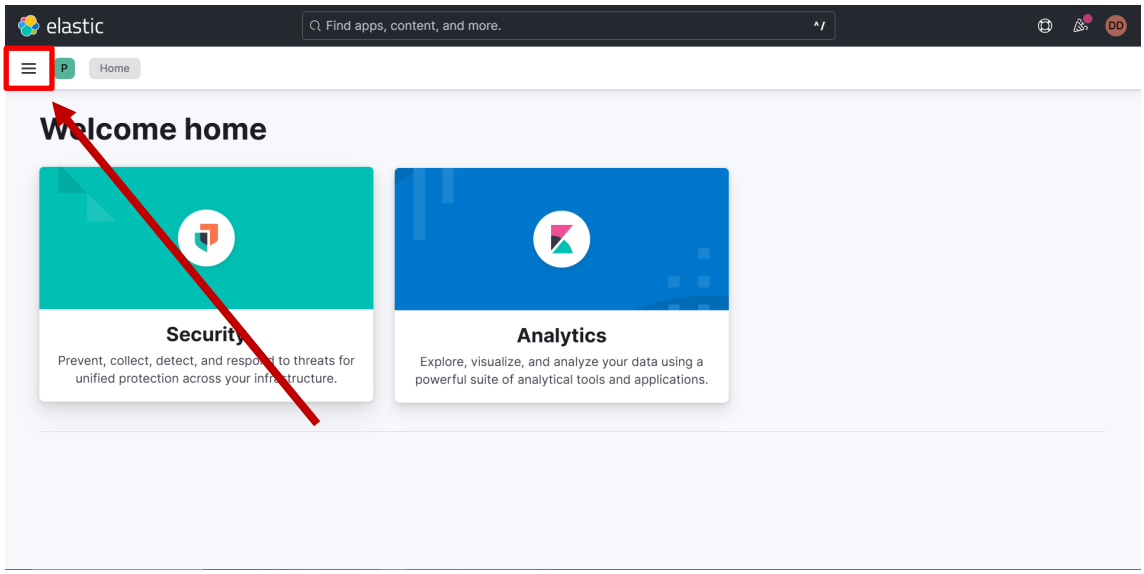
Kibana – Dashboard

V Kibane je možné vytvárať tzv. space. Tieto priestory slúžia na logické oddelenie dát.

Účty v Kibane sú vytvárané podľa špecifickej role, ktorá umožňuje prístup len do potrebného space.

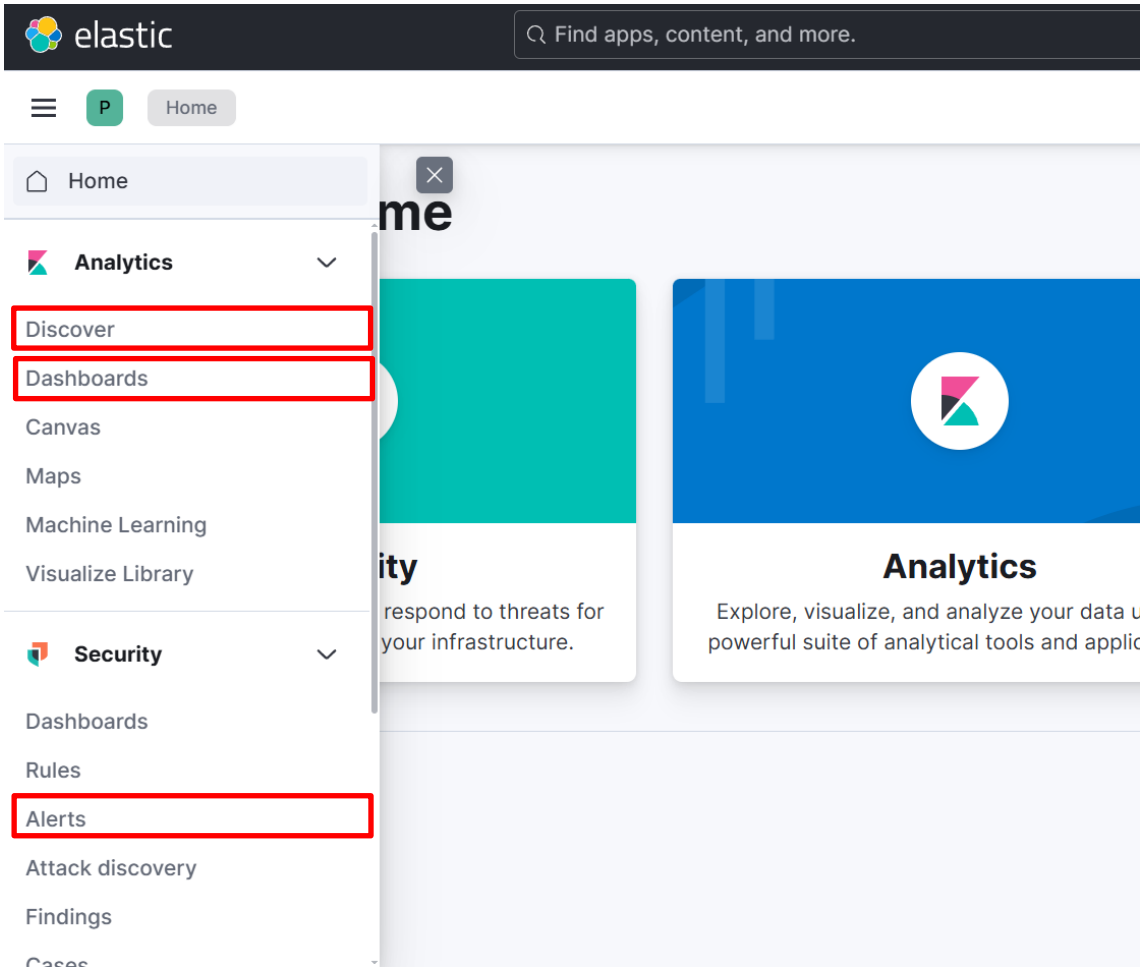
Tri najdôležitejšie časti v našom nasedení sú aktuálne časť *Discover*, *Dashboards* a *Alerts* ***(časť Security)***. Časť Discover slúži na zobrazenie zozbieraných údajov v textovej podobe. Časť Dasboards na zobrazenie vytvorených vizualizácii zozbieraných dát. Časť Alerts slúži na zobrazenie bezpečnostných upozornení, alert-ov.

K jednotlivým častiam sa dostaneme pomocou „hamburger“ tlačidla v ľavom hornom rohu obrazovky.



Obrázok 1

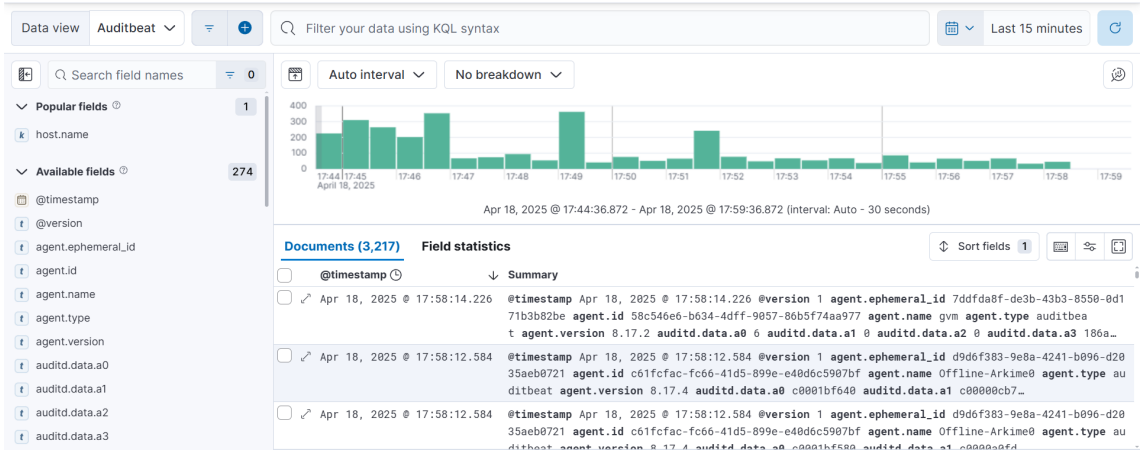
Po kliknutí sa nám rozbalí menu kde sa nachádzajú jednotlivé časti.



Obrázok 2

Discover

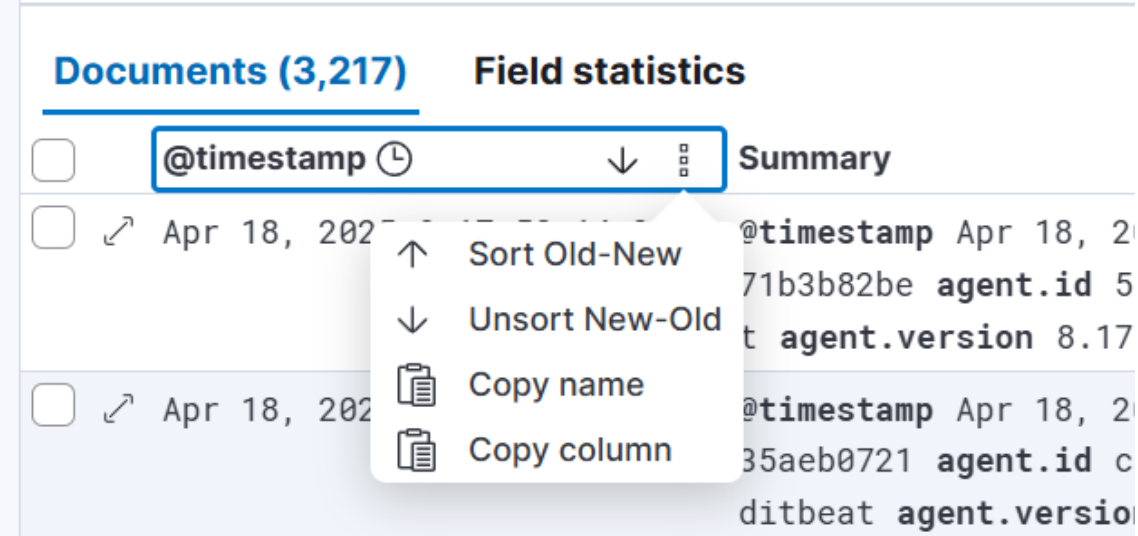
Časť discover vyzerá nasledovne.



Obrázok 3

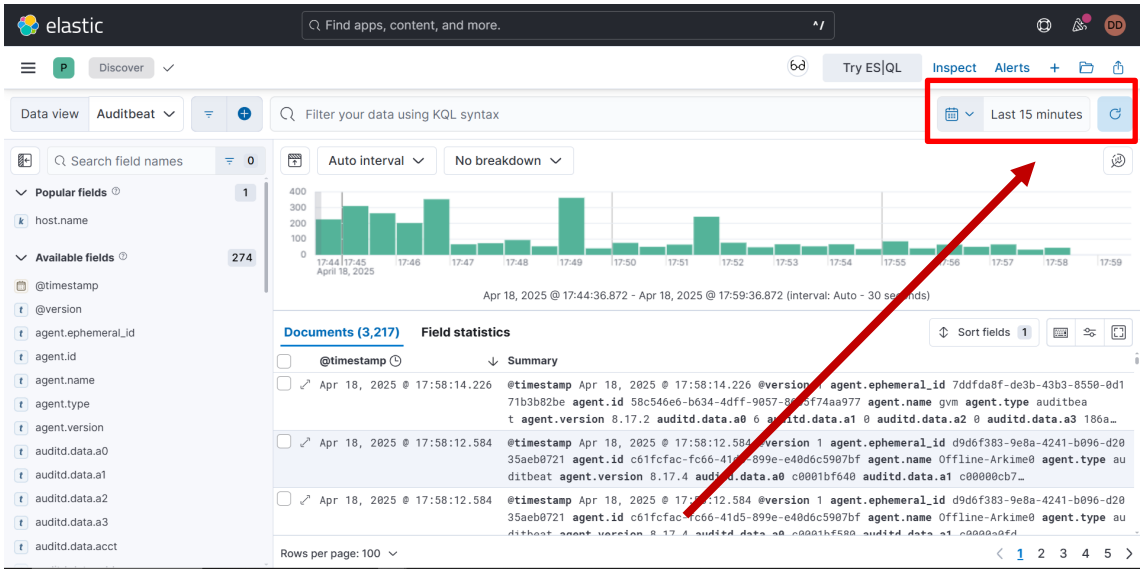
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Ako môžeme na obrázku vidieť, jednotlivé prijaté dáta sú uložené ako záznamy, dokumenty. Dokumenty sú usporiadané na základe času, poľa *timestamp*. Záznamy môžeme usporiadať vzostupne alebo zostupne.



Obrázok 4

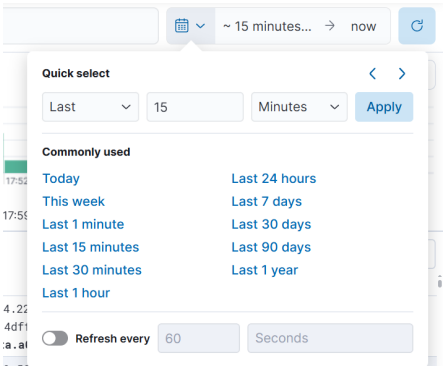
Čas je pre správnu analýzu veľmi dôležitý, preto je potrebné si ako prvé nastaviť správny časový rozsah, časové okno. V pravom hornom rohu nájdeme nastavenie pre nastavenie časového rozsahu.



Obrázok 5

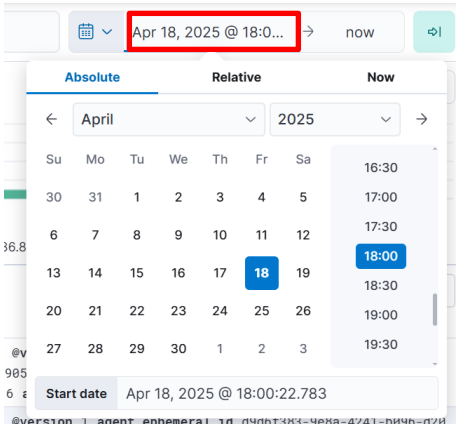
Ak klikneme na ikonu kalendáru máme na výber niekoľko možností výberu časového okna. Tieto možnosti sú predvolené a vzťahujú sa od nejakého bodu v minulosti po aktuálny okamih.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY



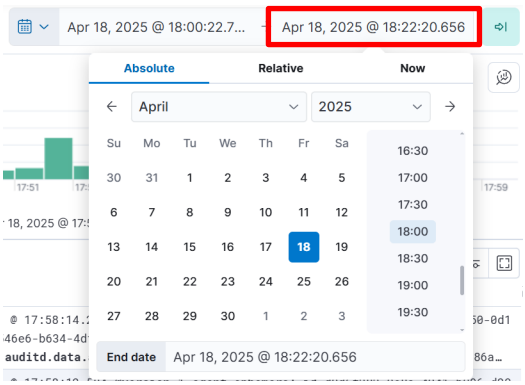
Obrázok 6

Z obrázka vidíme, že vieme nastaviť aj automatický refresh údajov, toto je vhodné pri dashboard-och alebo alert-och, pre discover toto neodporúčame. Ak klikneme na časť tesne za ikonou kalendára vyberáme „Start date“.



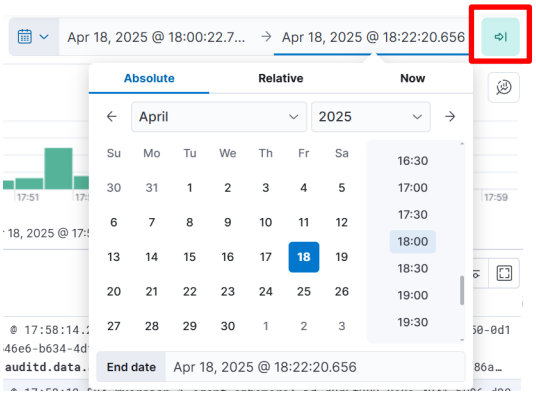
Obrázok 7

Máme na výber možnosti *Absolute*, *Relative* a *Now*. Možnosť *Relative* slúži na vybranie preddefinovaných hodnôt. Možnosť *Absolute* slúži na vybranie konkrétneho časového okamžiku. Obdobne ak klikneme na zadnú časť za symbolom kalendára vyberáme „End date“.



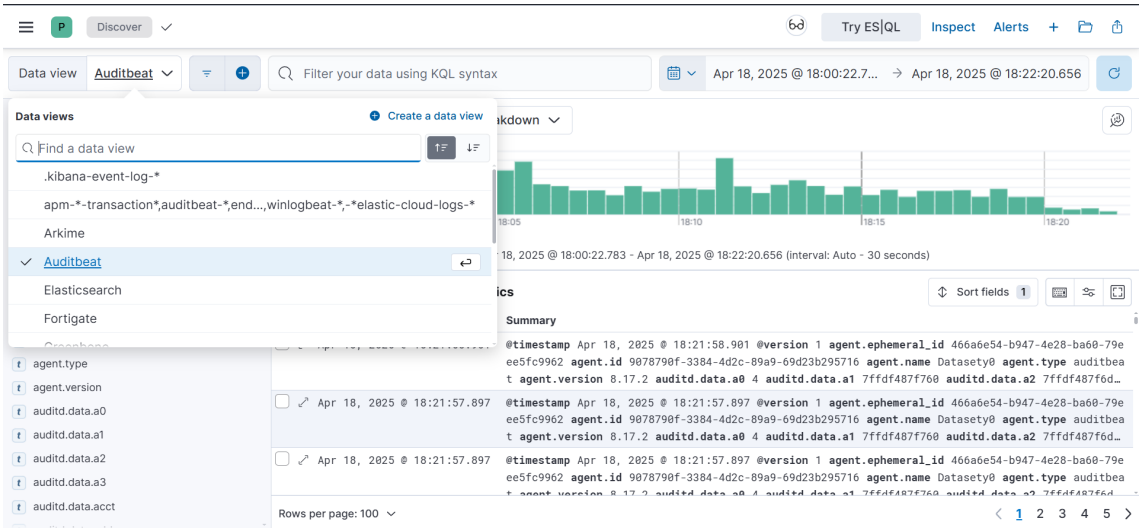
Obrázok 8

Výber časového okna je samozrejme nutné potvrdiť.



Obrázok 9

Ešte dôležitejšie ako výber správneho časového okna je výber správneho zdroja údajov. Zdroje údajov máme reprezentované pomocou *Data view*. Data view si vyberáme v ľavom roku obrazovky.



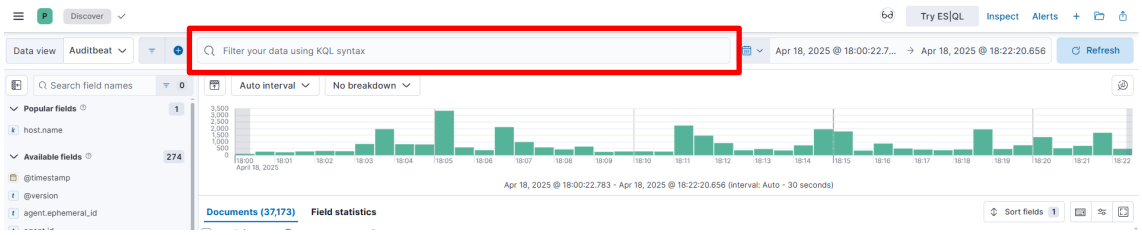
Obrázok 10

Máme na výber niekoľko nami vytvorených data views.

- **Auditbeat** – údaje z linux zariadení
- **Arkime** – údaje z nástroja arkime
- **Elasticsearch** – rozšírené logovanie nastroja elasticsearch
- **Fortigate** – údaje z firewall zariadenia
- **Monitoring** – údaje z metricbeat, pre potreby dashboard-ov
- **Suricata** – údaje z oboch suricata IDS
- **Threatintel** – zber CTI informácií
- **WAF** – zber údajov z WAF zariadenia

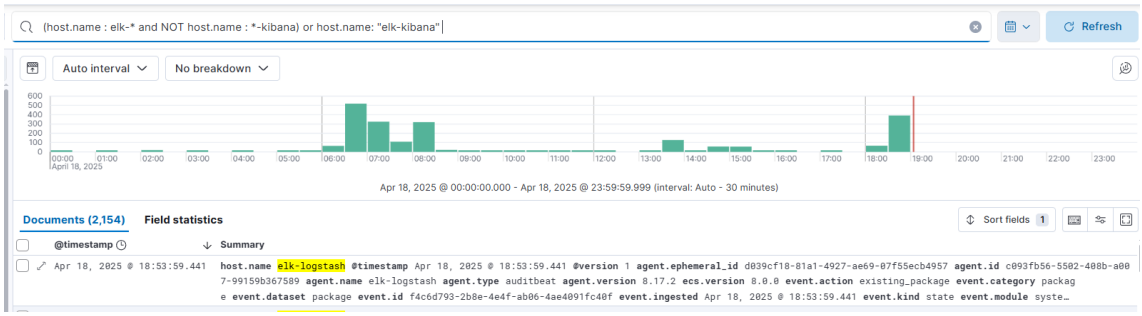
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Pre efektívne vyhľadávanie údajov v časti discover je nutné pracovať filtrami. Filtrovať môžeme pomocou KQL (Kibana Query Language), pomocou jednotlivých polí v dokumentoch alebo pomocou vytvárania grafických filtrov. Pre rýchle filtrovanie odporúčame používať KQL alebo filtrovať na základe polí dokumentov. KQL sa píšu v hornej časti stránky v search poli.



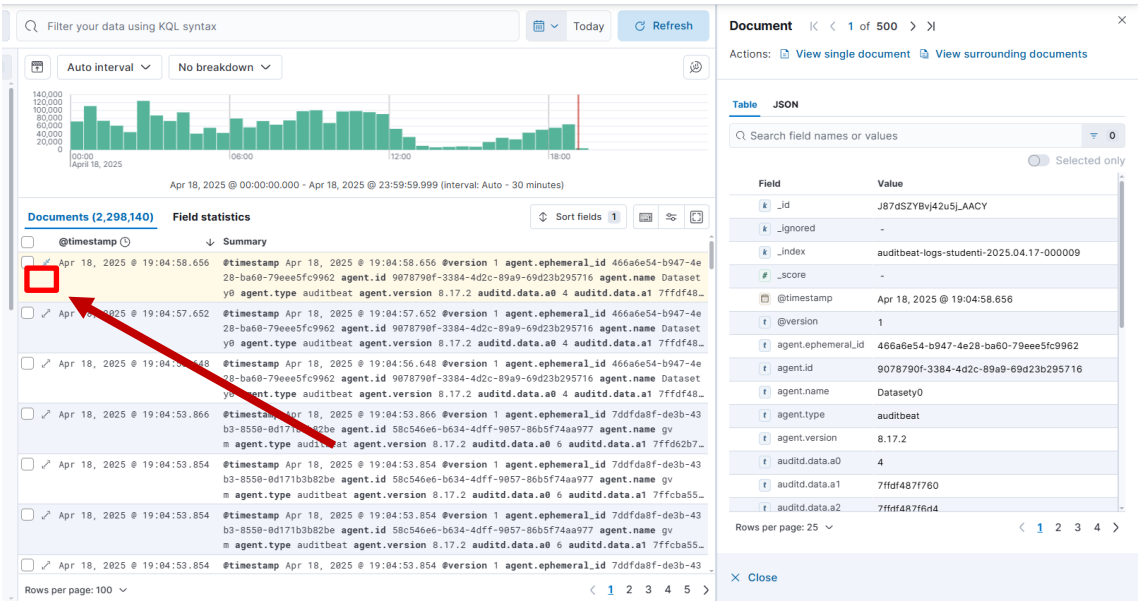
Obrázok 11

V tomto boli je možné použiť aj tzv. fulltextové vyhľadávanie. Ak chceme vyhľadať nejakú časť textu, tento text obalíme úvodzovkami, “text“. Najčastejšie tvoríme filter kde špecifikujeme pole a jeho hodnotu. V hodnotách môžeme používať tzv. wildcards, teda * ktoré zastupujú ľubovoľný počet ľubovoľných znakov. Symbol = je že hodnota sa rovná. Vo filtroch môžeme použiť aj logické operátory *and*, *or* a *NOT*. Taktiež môžeme logiku filtrov rozšíriť pomocou zátvoriek () .



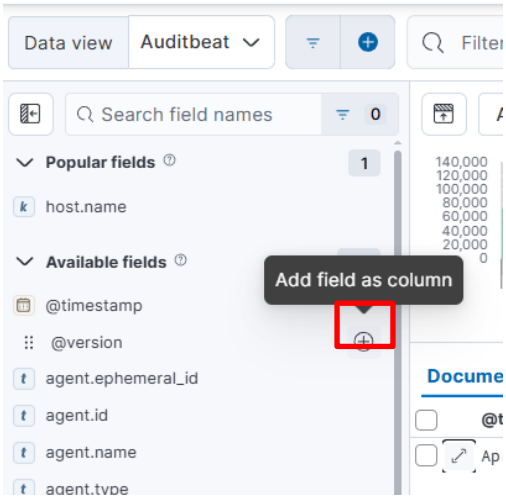
Obrázok 12

Obrázok vyššie zobrazuje použitie zložitejšieho filtra v KQL. Všetky údaje o danom zázname, dokumente si zobrazíme pomocou obojstrannej šípky na začiatku záznamu. bližšie informácie o danom zázname sa zobrazia v pravej časti.



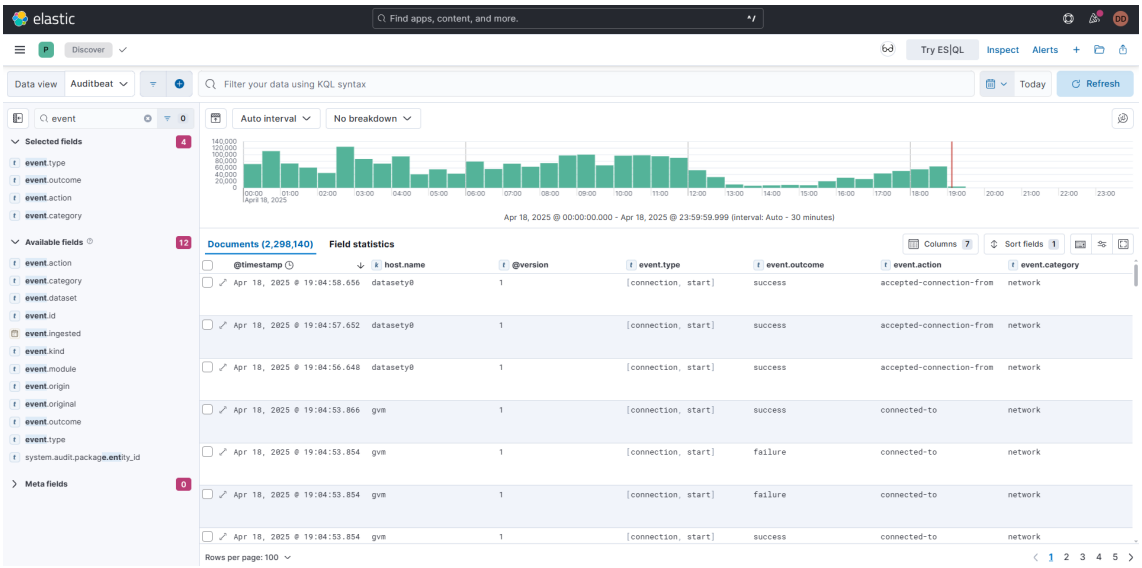
Obrázok 13

Pravá časť ktorá obsahuje informácie o danom zázname ponúka možnosť filtrovania pomocou search poľa. Prehľadnosť dokumentov môžeme zvýšiť zobrazením relevantných informácií priamo v náhľade dokumentu. V ľavej časti sa nachádza zoznam jednotlivých polí dokumentov. Ak klikneme na symbol plus pri tomto poli v hlavnom náhľade sa zobrazí len takto zvolené polia.



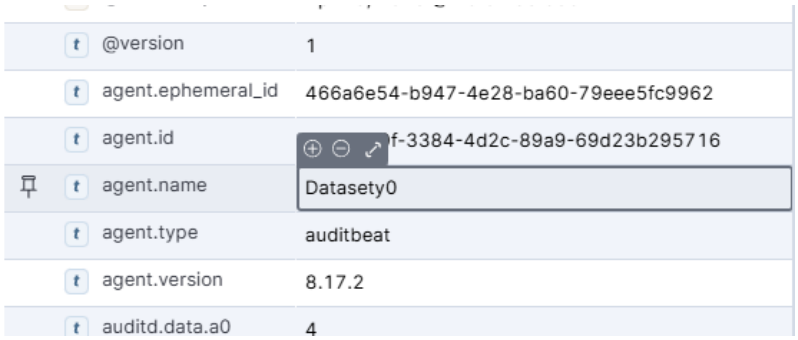
Obrázok 14

Prispôsobený hlavný náhľad môže vyzerať napríklad nasledovne.



Obrázok 15

Ak chceme filtrovať pomocou poľa daného dokumentu môžeme tak vykonať v hlavnom zobrazení alebo v zobrazení kde sú zobrazené podrobnosti daného dokumentu. Prejdeme na dané pole v dokumente a symbolom plus zobrazíme plen záznamy s touto hodnotou, alebo symbolom mínus zobrazíme záznamy ktoré neobsahujú túto hodnotu.



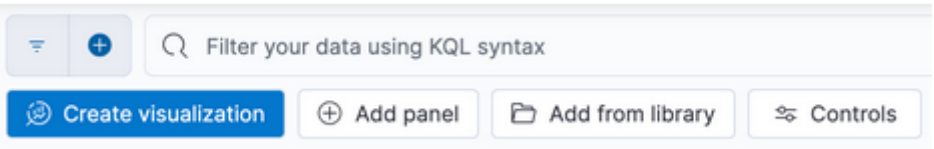
Obrázok 16

Dasboards

V riešení je vytvárať dashboard-y, ktoré zobrazujú napríklad sieťové štatistiky, úspešné/neúspešné prihlásenia.

Postup vytvorenia nového dashboard-u:

1. Otvorte stránku Dashboards v Kibane.
2. Vyberte možnosť Vytvoriť dashboard a začnite s prázdnym dashboardom.
3. Po vytvorení dashboardu sa automaticky dostanete do režimu úprav a môžete na dashboarde vykonávať zmeny.
4. Pridajte obsah na dashboard. Máte niekoľko možností, ktoré sú podrobnejšie popísané v sekcii Vizualizácie:



Obrázok 17

Vytvoriť vizualizáciu. Táto možnosť je skratkou na vytvorenie grafu pomocou Lens, predvoleného editora vizualizácií v Kibane.

Pridať panel. Vyberte jeden z dostupných panelov na pridanie a konfiguráciu obsahu na dashboard.

Pridať z knižnice. Vyberte existujúci obsah, ktorý už bol nakonfigurovaný a uložený do knižnice Visualize.

Ovládacie prvky. Pridajte ovládacie prvky, ktoré vám pomôžu filtrovať obsah dashboardu.

5. Možnosti pridania obsahu na dashboard
6. Usporiadajte si dashboard usporiadaním rôznych panelov.
7. Definujte hlavné nastavenia dashboardu z ponuky **Nastavenia**, ktorá sa nachádza na paneli s nástrojmi.
8. Zmysluplný názov, popis a značky vám umožnia rýchlo nájsť dashboard neskôr pri prehliadaní zoznamu dashboardov alebo pomocou vyhľadávacieho panela Kibana.

   Ďalšie možnosti zobrazenia vám umožňujú zjednotiť vzhľad a dojem z panelov na dashboarde:

   Uložiť čas s dashboardom – Uloží zadaný filter času.

Použiť okraje medzi panelmi – Pridá okraj medzi jednotlivými panelmi.

Zobraziť názvy panelov – Zobrazí názvy v hlavičkách panelov.

Synchronizovať farebné palety medzi panelmi – Použije rovnakú farebnú paletu na všetky panely na dashboarde.

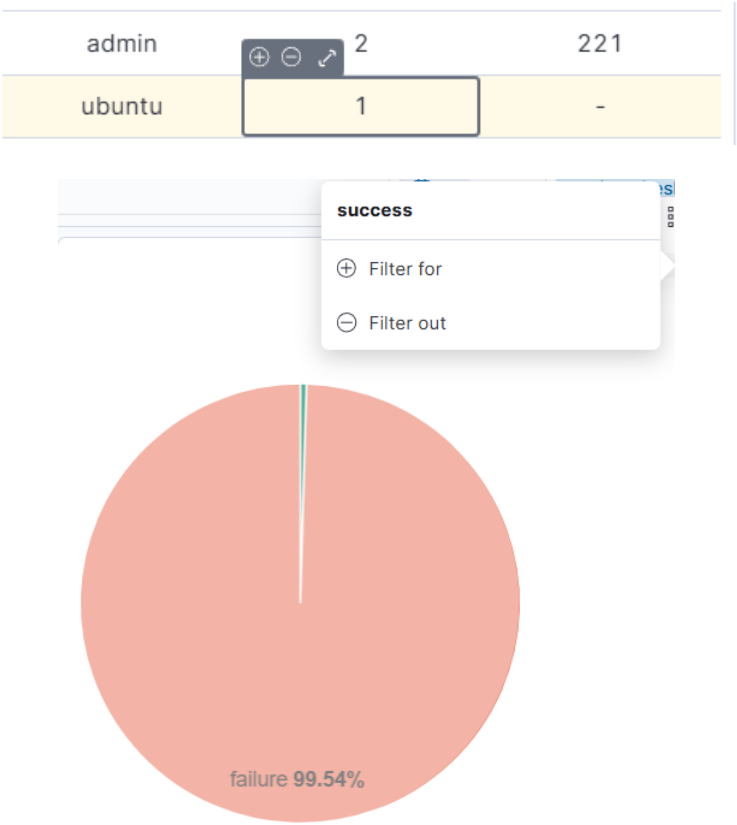
Synchronizovať kurzor medzi panelmi – Keď podržíte kurzor myši nad grafom časových radov alebo tepelnou mapou, kurzor sa automaticky zobrazí na všetkých ostatných súvisiacich grafoch dashboardu.

Synchronizovať popisy nástrojov medzi panelmi – Keď podržíte kurzor myši nad grafom Lens, automaticky sa zobrazia popisy nástrojov na všetkých ostatných súvisiacich grafoch dashboardu.

9. Kliknite na Použiť.

Príklad: **Login Activity Monitoring** – zobrazenie informácií o úspešných, prípadne neúspešných prihlásenia používateľov na jednotlivé monitorované servery

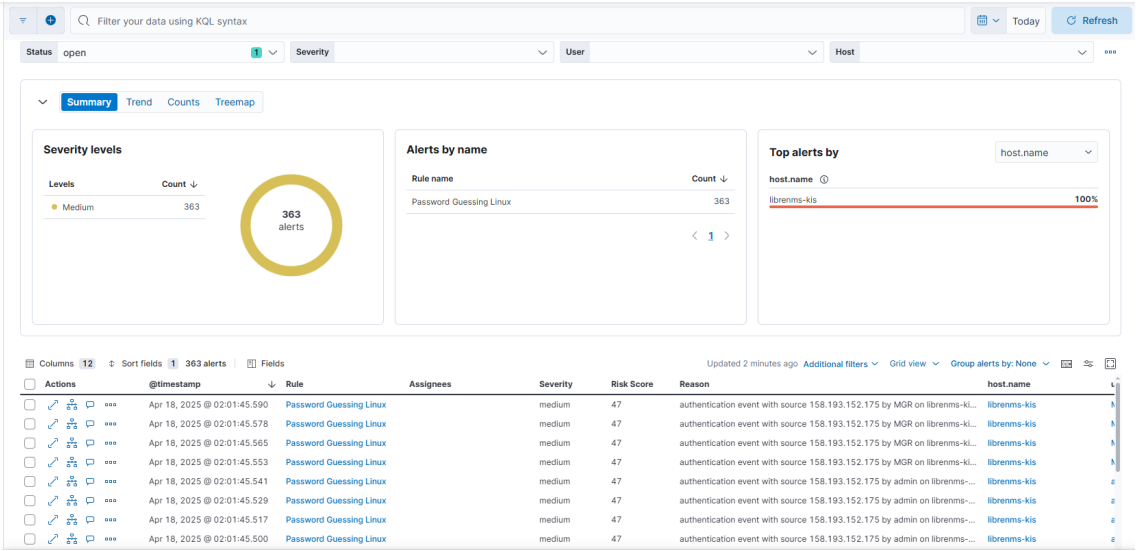
V dashboardoch, obdobne ako v discover, platí zásady filtrovania a nastavania časového okna.



Obrázok 18

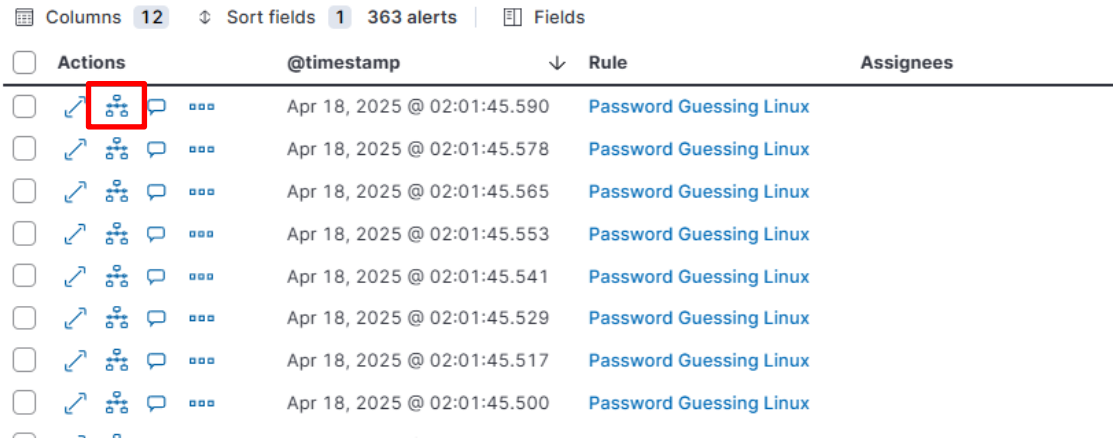
Alerts

Alerts zobrazujú bezpečnostné upozornenia, ktoré boli vytvorené na základe predefinovaných detekčných pravidiel. Pravidlá môžu byť predvolené (elasticsearch) alebo vlastné. V rámci vlastných pravidiel sme vytvorili pravidlá na detegovanie bruteforce útoku, transformačné pravidlá a pravidlá ktoré porovnávajú prijaté dáta s CTI dátami.



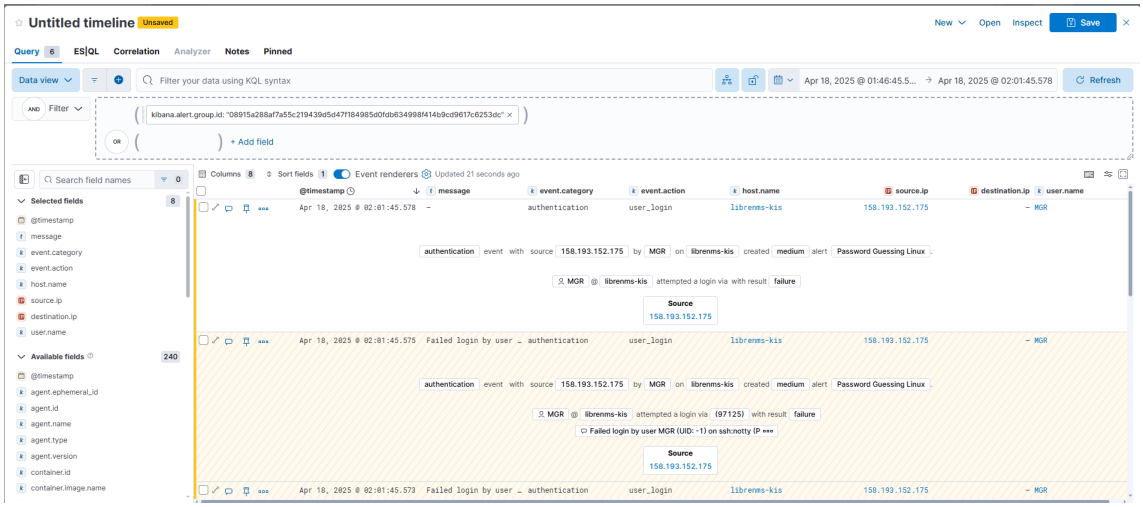
Obrázok 19

Aj v časti alerts sa filtrovanie a nastavenie časového okna používa rovnako ako v častiach discover a dashboards. Jedno bezpečnostné upozornenie môže byť vyvolané jedným alebo viacerými záznamami. Overíme to pomocou otvorenie tzv. timeline.



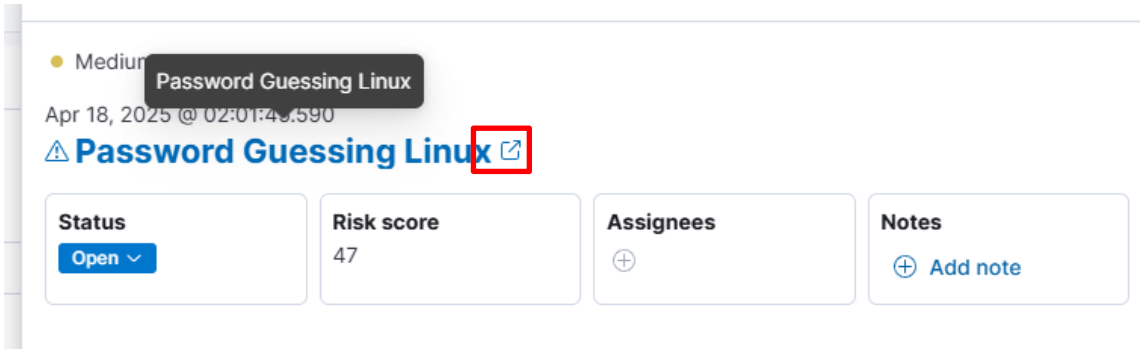
Obrázok 20

Po kliknutí sa zobrazí jeden alebo viacero záznamov, dokumentov.



Obrázok 21

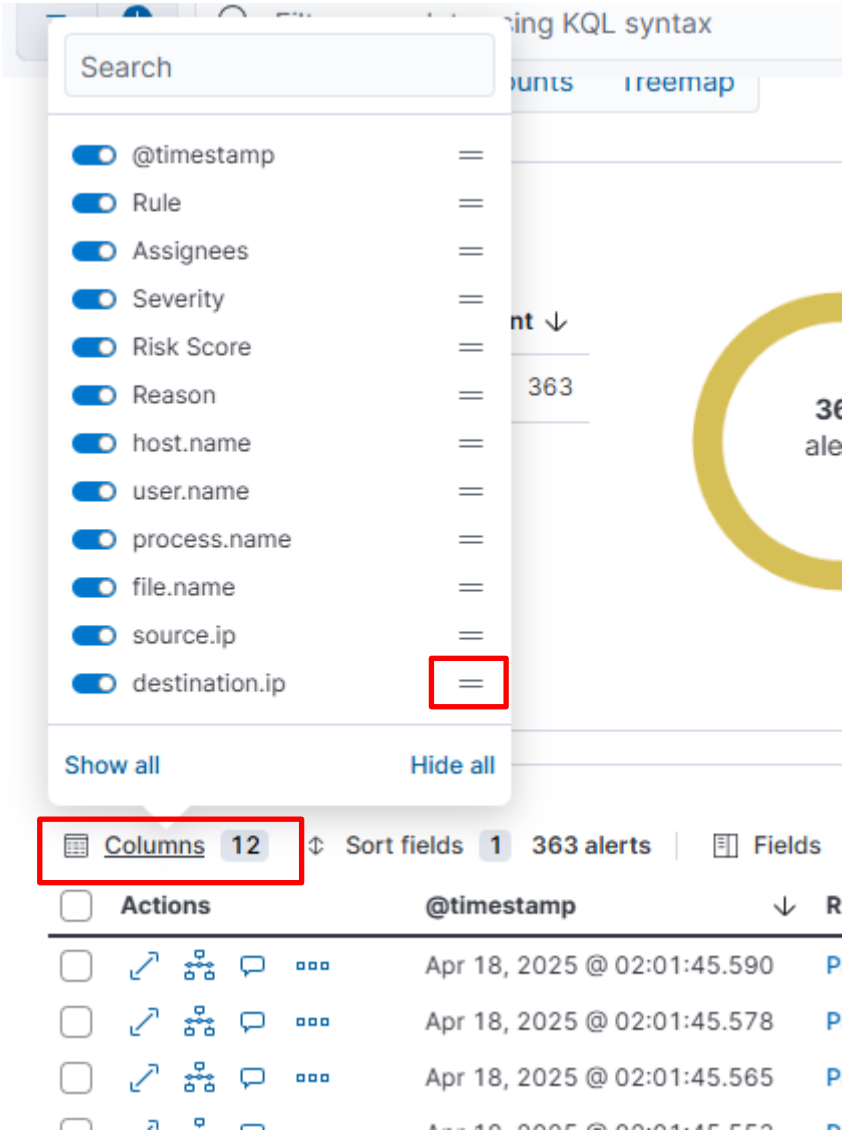
Zobrazenie bližších informácií o bezpečnostnom upozornení vykonáme obdobne ako pre zobrazenie informácií o dokumente v discover. Pre lepšie pochopenie pravidla je možné si zobraziť detail tohto pravidla a zamerať sa na jeho logiku.



Obrázok 22

Toto však neplatí pre nami vytvorené transformačné pravidlá.

Pre lepšiu prehľadnosť je možné nastaviť, ktoré polia sa majú zobraziť pri jednotlivých bezpečnostných upozornenia a v akom poradí.



Obrázok 23

Vyšetrenie bezpečnostného upozornenia

V prvom rade je nutné povedať, že používateľ nemôže poznať všetky detekčné pravidlá. Z tohto dôvodu je nutné najskôr pochopiť prečo bolo dané bezpečnostné upozornenie vyvolané. Pomôcť pri tom môže zobrazenie informácií o danom pravidle. Veľmi nápomocné môžu byť aj jazykové modeli. Veľmi dôležité je potrebné informácie overiť. Pri riešení bezpečnostného incidentu, nie všetky informácie zo stroja ku ktorému sa viaže bezpečnostné upozornenie sú monitorované, je vhodné komunikovať s vlastníkom systému, ku ktorému sa dané bezpečnostné upozornenie viaže. Pri vyšetrovaní odporúčame pracovať v časti discover. Analýza si vyžaduje vnímať systém ako celok. Zameranie sa na jednu aktivitu, na ktorú bolo vyvolané upozornenie, je nesprávne. Ak

by išlo o útok je potrebných viacej krokov na jeho realizáciu. Odporúčame pozrieť *Cyber Kill Chain* a *MITRE ATT&CK*. Je vhodné taktiež požívať online nástroje:

- www.virustotal.com – kontrola IP adries a súborov
- www.abuseipdb.com – kontrola IP adries
- www.any.run - sendbox
- www.tria.ge – sendbox
- www.urlscan.io – kontrola webstránok

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY