PROJEKT

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

Dashboardy – vizualizácia dát z nástrojov

Previazané s balíkom KPB2– Návrh SOCaaS služby

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

Obsah

Zoznam obrázkov 3

Dashboard v nástroji Kibana 4

Dashboard IDS 4

Dashboard Login Activity Monitoring 6

Dashboard analýzy zaťaženia systému 7

Zoznam obrázkov

Obrázok 1 Dashboard IDS DMZ, alerty 4
Obrázok 2 Dashboard IDS DMZ, top signatúry 4
Obrázok 3 Dashboard IDS DMZ, top source IPs 5
Obrázok 4 Dashboard IDS DMZ, mapa 5
Obrázok 5 Dashboard Login Activity Monitoring, základné informácie 6
Obrázok 6 Dashboard Login Activity Monitoring, grafy 6
Obrázok 7 Dashboard Login Activity Monitoring, tabuľky 6
Obrázok 8 Dashboard Zaťaženie Stacku, Elasticsearch 7
Obrázok 9 Dashboard Zaťaženie Stacku, Kibana 7
Obrázok 10 Dashboard Zaťaženie Stacku, Loghstash 8

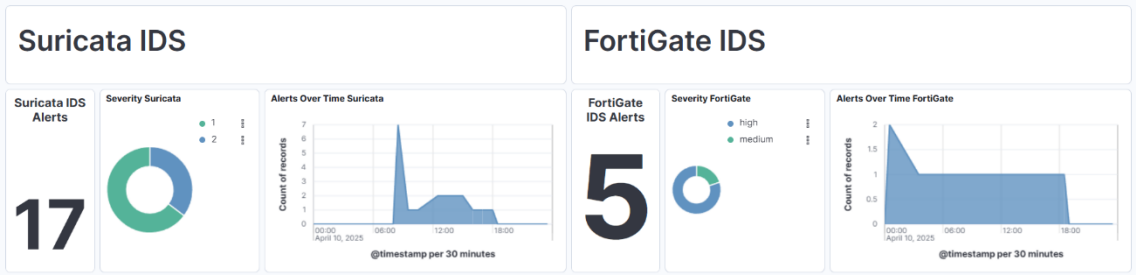
Dashboard v nástroji Kibana umožňuje rýchlo vytvárať zobrazenia, ktoré spájajú grafy, mapy a filtre. Tieto zobrazenia slúžia na zobrazenie úplného obrazu údajov uložených v Elasticsearch.

Dashboard IDS

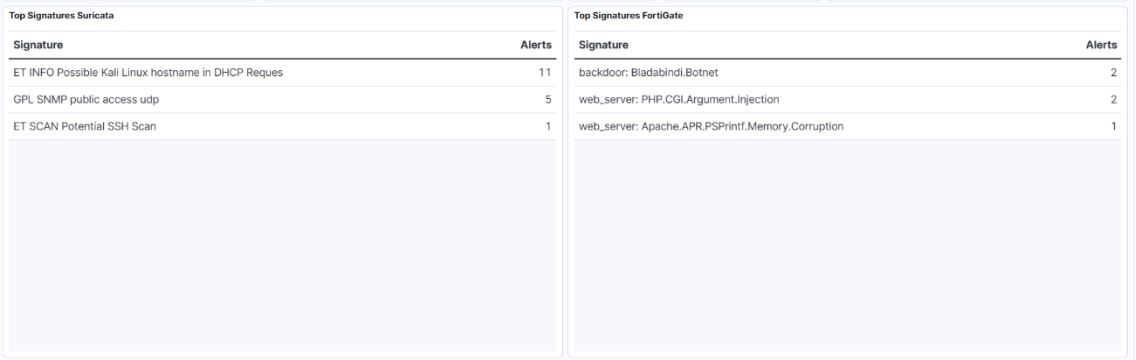
Tento dashboard slúži na zobrazenie vizualizovaných dát z nástrojov IDS, ktoré monitorujú dátový tok. Dashboard IDS názorne ukazuje počet detekcií sondami IDS a taktiež vzájomné porovnanie detekcií IDS *Suricata* a IDS modulom vo Fortigate. Z dashboard je jasne vidno, že IDS sondy detegujú rozdielne udalosti, aj keď monitorujú rovnaký tok dát.

Pri nasadzovaní IDS bol predpoklad, že množiny detekcií vytvorené IDS sondami, od rôznych dodávateľov, monitorujúce rovnaký tok dát budú mať výrazný prienik. Tento predpoklad sa nenaplnil.

Obrázok 1, obrázok 2, obrázok 3 a obrázok 4 zobrazuje jednotlivé vizualizácie v danom dashboard.



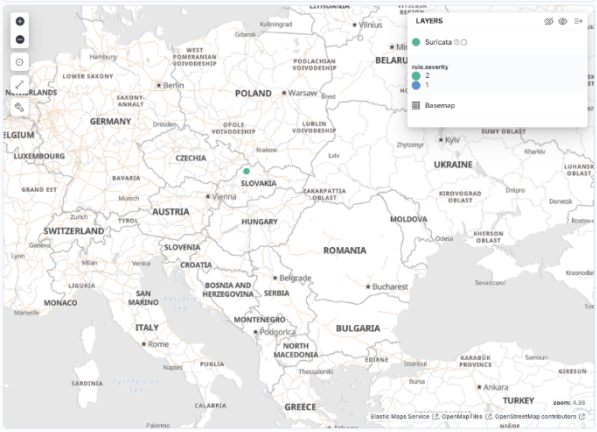
Obrázok 1 Dashboard IDS DMZ, alerty



Obrázok 2 Dashboard IDS DMZ, top signatúry



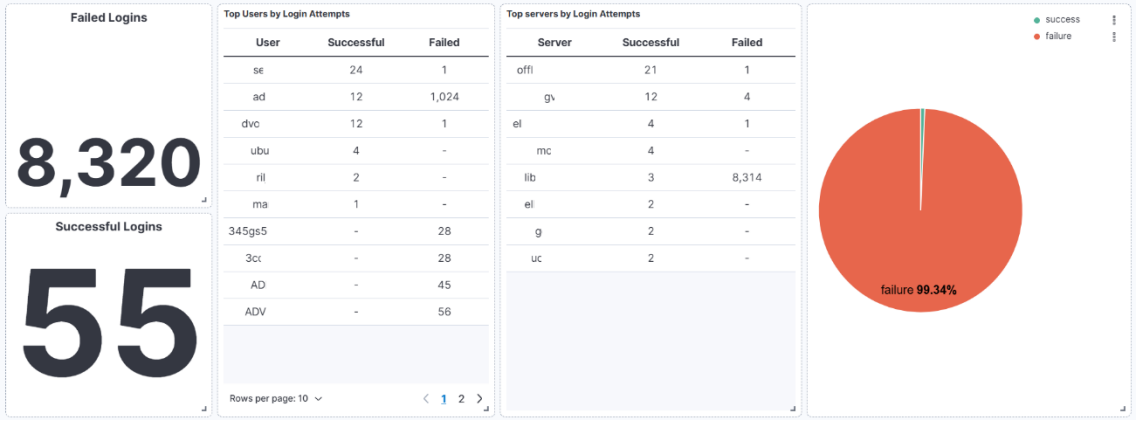
Obrázok 3 Dashboard IDS DMZ, top source IPs



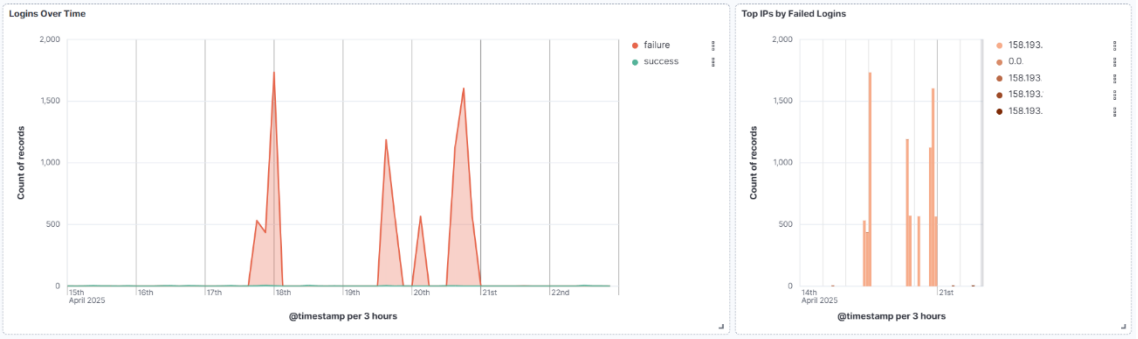
Obrázok 4 Dashboard IDS DMZ, mapa

Dashboard Login Activity Monitoring

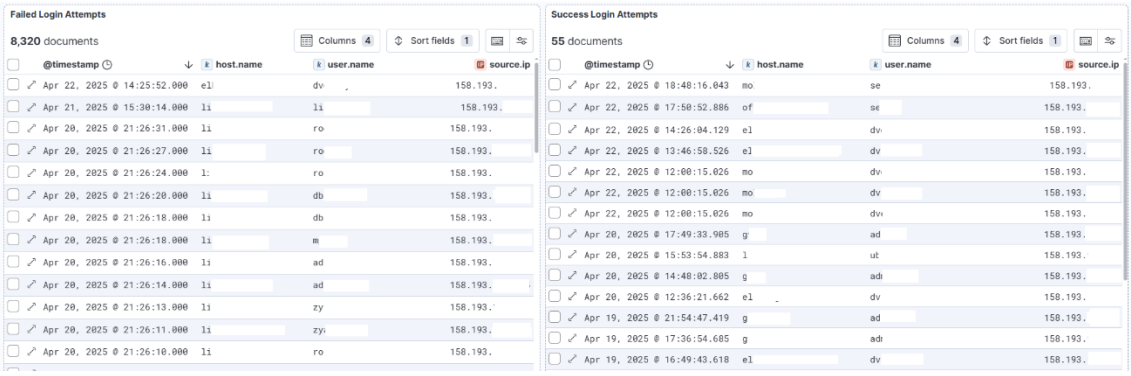
Tento dashboard sme vytvorili na vizualizáciu udalostí prihlásenia na monitorovaných serveroch. Prehľadná vizualizácia úspešných a neúspešných prihlásení v kombinácií s používateľskými menami a menami serverov, môže uľahčiť vyšetrovanie potencionálnych bezpečnostných incidentov zaznamenaných pomocou bezpečnostných upozornení. Obrázok 5, obrázok 6 a obrázok 7 zobrazuje jednotlivé vizualizácie v danom dashboard.



Obrázok 5 Dashboard Login Activity Monitoring, základné informácie



Obrázok 6 Dashboard Login Activity Monitoring, grafy



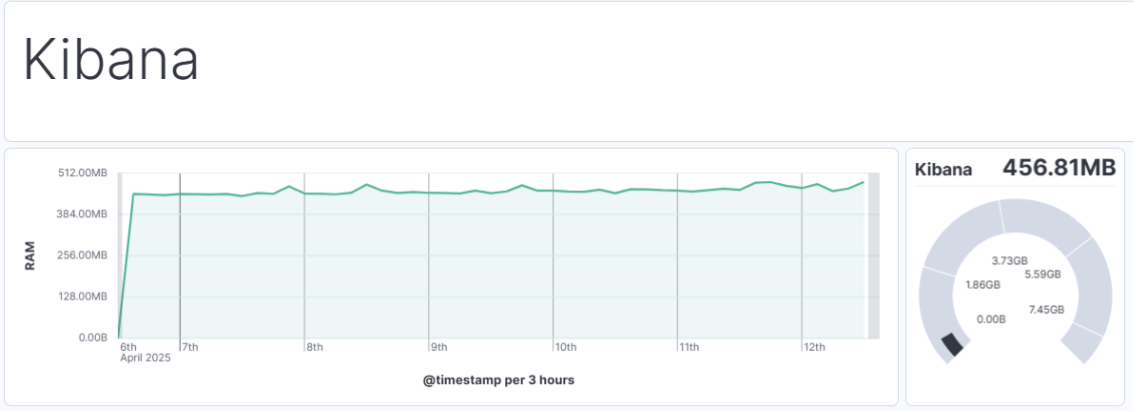
Obrázok 7 Dashboard Login Activity Monitoring, tabuľky

Dashboard analýzy zaťaženia systému

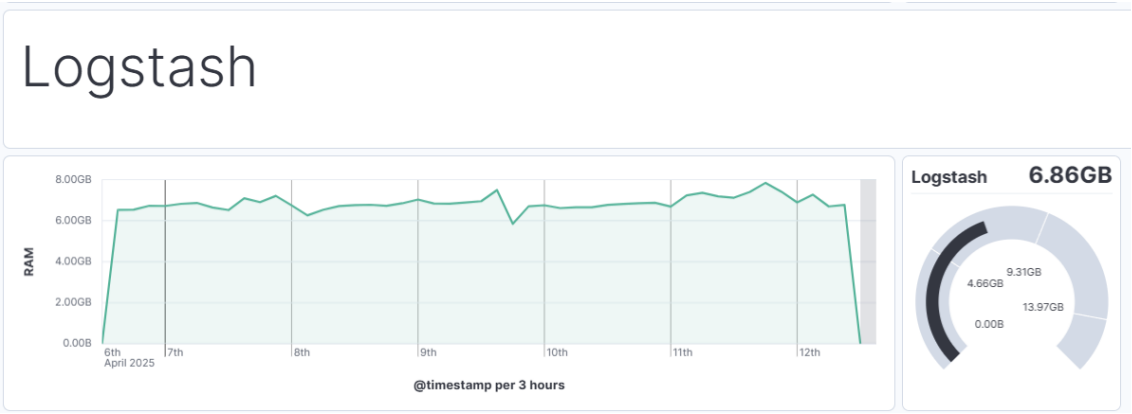
V časti analýza zaťaženia systému sme sa primárne zamerali na využitie pridelenej operačnej pamäte jednotlivým častiam ELK stack, Elasticsearch uzly, Logstash a Kibana. Pre efektívne monitorovanie zaťaženia operačnej pamäte boli využité údaje zozbierané pomocou nástroja metricbeat. Predvolená časť aplikácie Kibana pre monitorovanie komponentov Elastic Stack, tzv. stack monitoring, pracuje práve s týmito metrikami. V zobrazení monitorovania ELK komponentov si však vieme pozrieť len zaťaženie v určitom časovom okamihu. Pre potreby zobrazenia priemernej záťaže sme si vytvorili prehľadný dashboard, ktorý sme nazvali Zaťaženie Stacku. Na obrázku 8, obrázku 9 a obrázku 10 je zobrazené priemerné zaťaženie za časové obdobie šiestich dní.



Obrázok 8 Dashboard Zaťaženie Stacku, Elasticsearch



Obrázok 9 Dashboard Zaťaženie Stacku, Kibana



Obrázok 10 Dashboard Zaťaženie Stacku, Loghstash

Ako je možné z obrázkov vyššie pozorovať, riešenie efektívne využíva pridelenú operačnú pamäť a nevzniká preťaženie. Navyše pridelená operačná pamäť poskytuje priestor na rozšírenie do budúcna, prípadný prechod na 10 GB infraštruktúru. Prechod by mohol mať za následok zväčšenie objemu dát za určitý čas, ktorých spracovanie by si vyžadovalo väčšie hardvérové nároky.

Ak sa zameriame na jednotlivé uzly podľa ich typu, môžeme vidieť, že *Elasticsearch* zaťažuje najviac dátové uzly, ktoré majú označenie hot. Následne sú zaťažované uzly s označením warm a poslednom rade uzly s označením cold.

V tabuľke 1 je zobrazené priemerné využitie pamäte jednotlivých systémov v rámci ELK stack.

Systém	Využitie RAM [GB]	Pridelená RAM [GB]
master1	6.3	16
hot1	9.98	31
hot2	11.44	31
hot3	10.98	31
warm1	8.80	31
warm2	4.50	31
cold1	2.91	16
kibana	0.457	8
logstash	6.86	16

Tabuľka 1, Reálne využitie operačnej pamäte