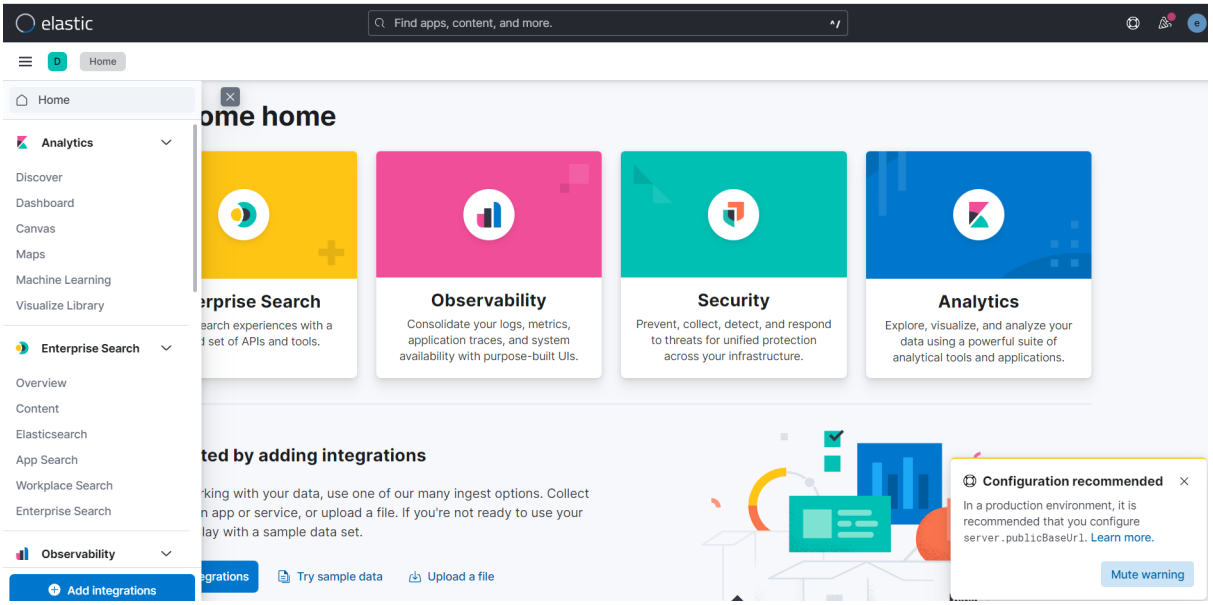
Používateľská príručka pre nástroj SIEM

Tento dokument slúži ako používateľská príručka pre nástroj SIEM. Predmetom tejto príručky je popísať možnosti prehliadania informácii o udalostiach v systéme SIEM. Ďalej popisuje postup prehliadania vygenerovaných upozornení, možnosti modifikácie a pridania existujúcich pravidiel na generovanie upozornení ako aj spôsob vytvárania vizualizácii zo zachytených dát.

Vytvorený systém SIEM

Nami nasadený systém SIEM je tvorený ELK zásobníkom [1] teda ElasticSearch, Logstash a Kibana. Kibana je webová aplikácia slúžiaca na prehliadanie a analyzovanie zachytených dát. Systém Siem je dostupný po pripojení na internú laboratórnu sieť v miestnosti 1.04 na FIIT STU, buď fyzicky alebo prostredníctvom VPN pomocou nasledovnej URL http://10.0.130.124:5601/.



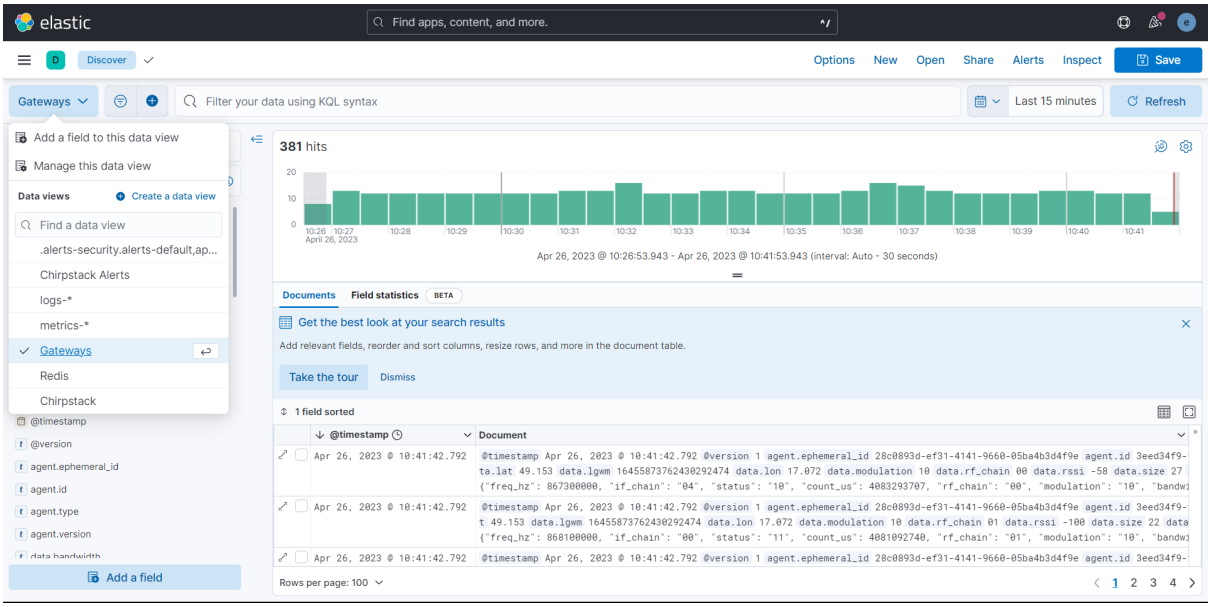
Obrázok č. 1: Webový nástroj Kibana súčasťou ELK zásobníku [1]

Prehliadanie dát v Kibane

Po prihlásení do Kibany je možné prehliadať dáta zhromaždené v systéme pomocou kliknutia na možnosť “Discover” v rámci časti “Analytics”.

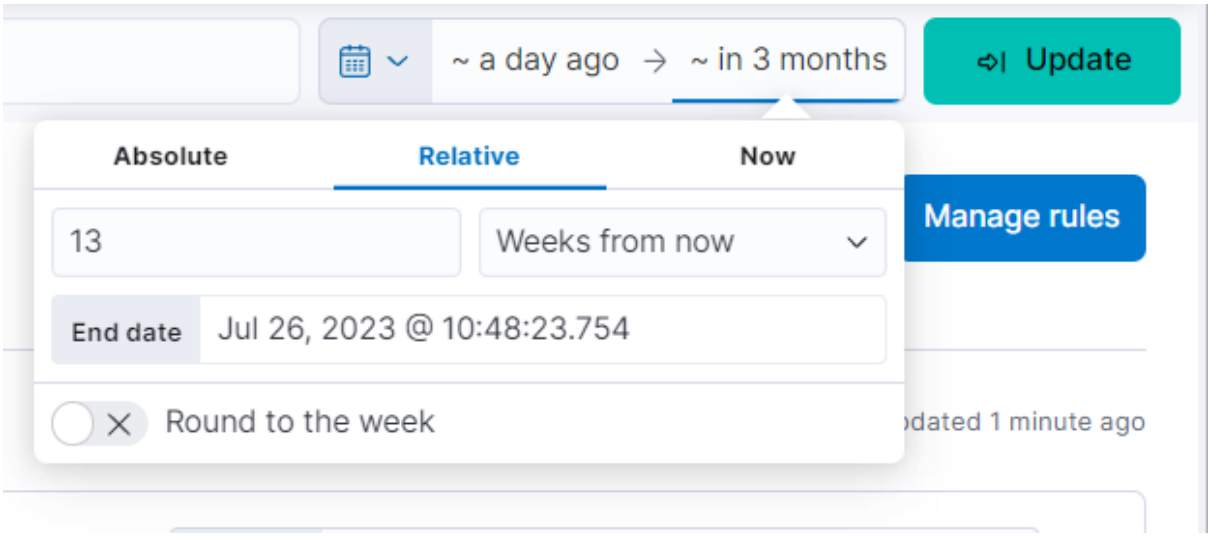
V našom prípade zbierame dáta z niekoľkých auditných zdrojov, pričom sú rozdelené nasledovne:

- Gateways - obsahuje auditné záznamy z LoRa brán
- Redis - obsahuje auditné záznamy z databázy Chirpstacku
- Chirpstack - obsahuje auditné záznamy z LoRa koncových zariadení



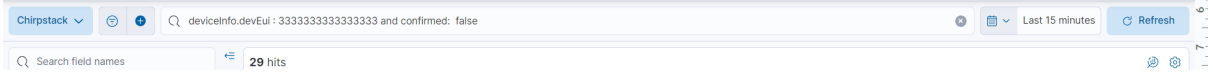
Obrázok č. 2: Zobrazenie auditných udalostí zozbieraných zo sledovaných zariadení v nástroji Kibana

Pričom v pravom hornom rohu je možné špecifikovať časové obdobie z ktorého chceme zobraziť záznamy.



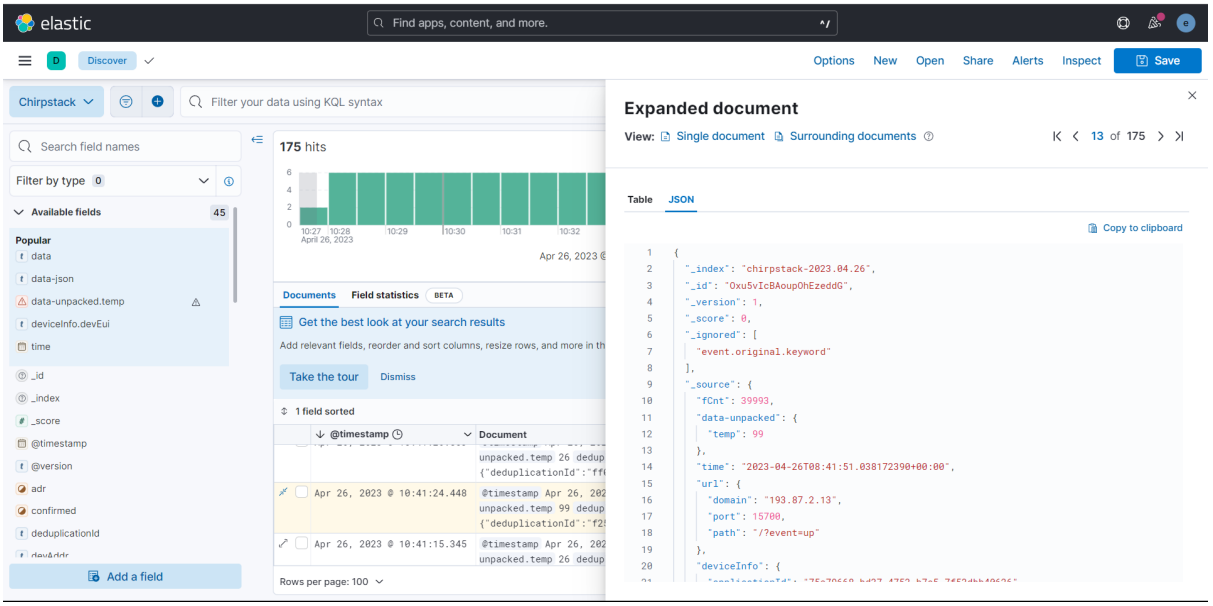
Obrázok č. 3: Špecifikácia časového obdobia z ktorého chceme zobraziť sledované auditné záznamy

Ďalej je možné v auditných záznamoch fulltextovo vyhľadávať vo vybraných poliach sledovaných auditných záznamoch.



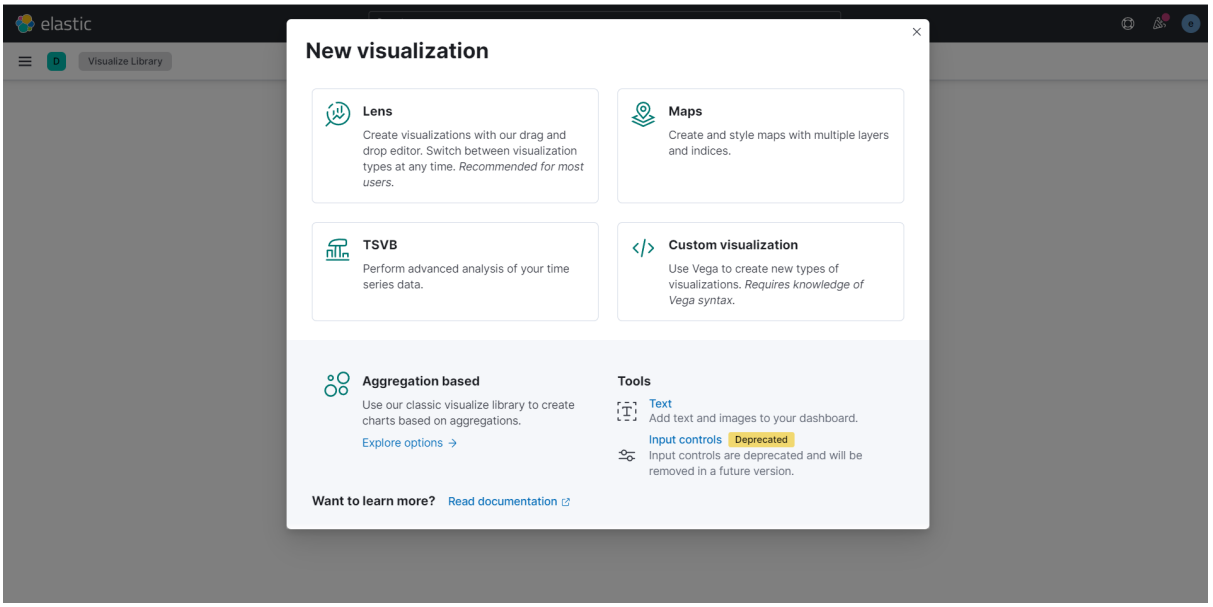
Obrázok č. 4: Vyhľadávanie vybraných auditných udalostí podľa špecifikovaných kritérií

Po kliknutí na vybraný záznam si vieme zobraziť detaily danej auditnej udalosti vo formáte JSON



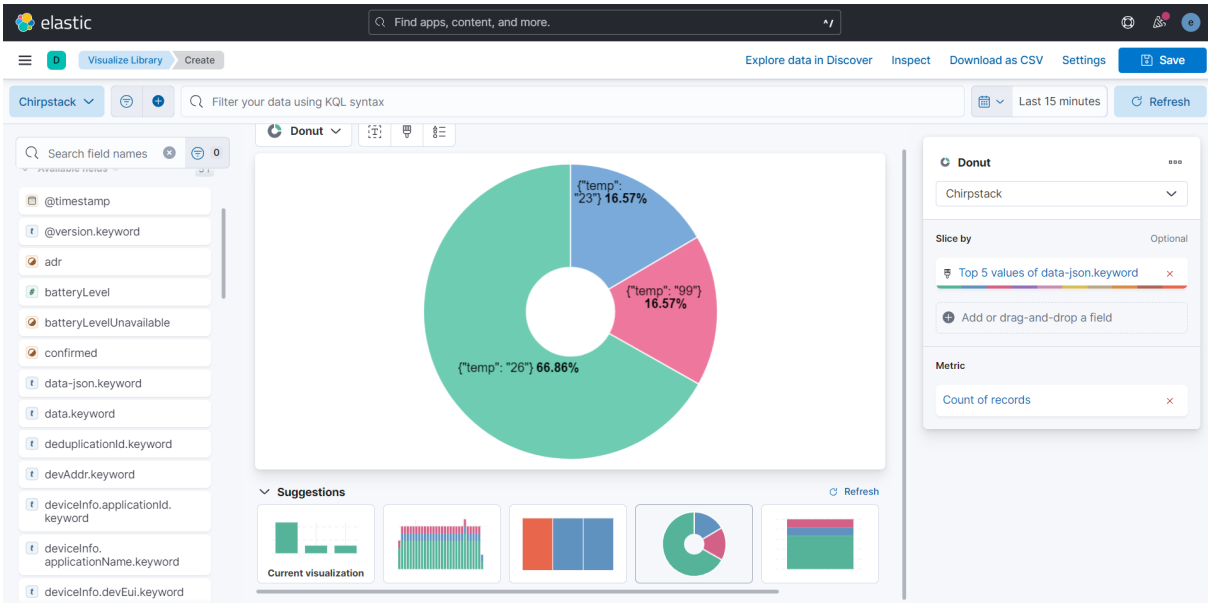
Obrázok č. 5: Zobrazenie detailov vybranej auditnej udalosti vo formáte JSON

V prípade ak chceme z vybraných auditných záznamov vytvárať vlastné vizualizácie je to možné pomocou možnosti “Visualize” v časti “Analytics”, následne využijeme možnosť “Lens” a vytvoríme vizualizáciu vybraných dát podľa potreby.



Obrázok č. 6: Vytvorenie novej vizualizácie zo sledovaných dát

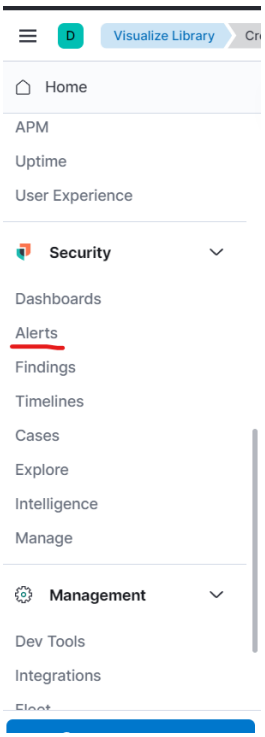
V rámci vytváraných vizualizácii je možné sledovať a tvoriť vizualizácie pre rôzne sledované hodnoty z vybraného auditného zdroja za špecifikované časové obdobie.



Obrázok č. 7: Príklad vytvorenej vizualizácie zobrazujúcej prevalentnosť výskytu jednotlivých hodnôt parametra temp

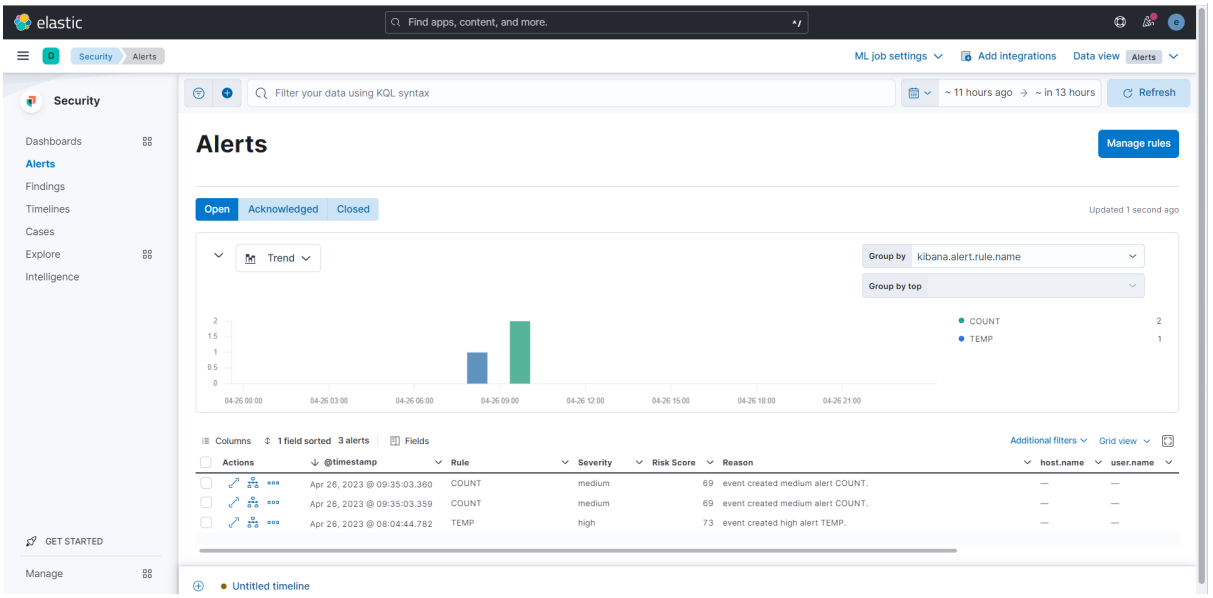
Sledovanie Upozornení

Sledovať upozornenia vygenerované pravidlami je možné po vybratí možnosti “Alerts” v časti “Security”



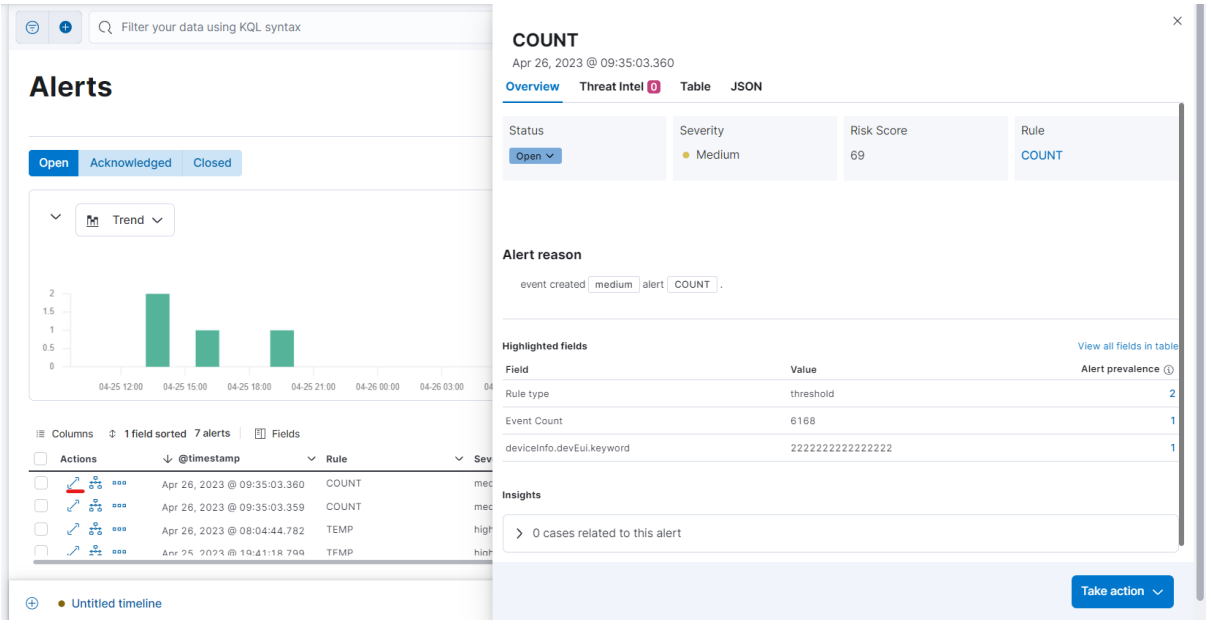
Obrázok č. 8: Prehliadanie vygenerovaných upozornení

Rovnako ako pri auditných záznamoch možno zvoliť časové obdobie, za ktoré chceme upozornenia zobraziť.



Obrázok č. 9: Prehľad vygenerovaných upozornení za posledných 13 hodín

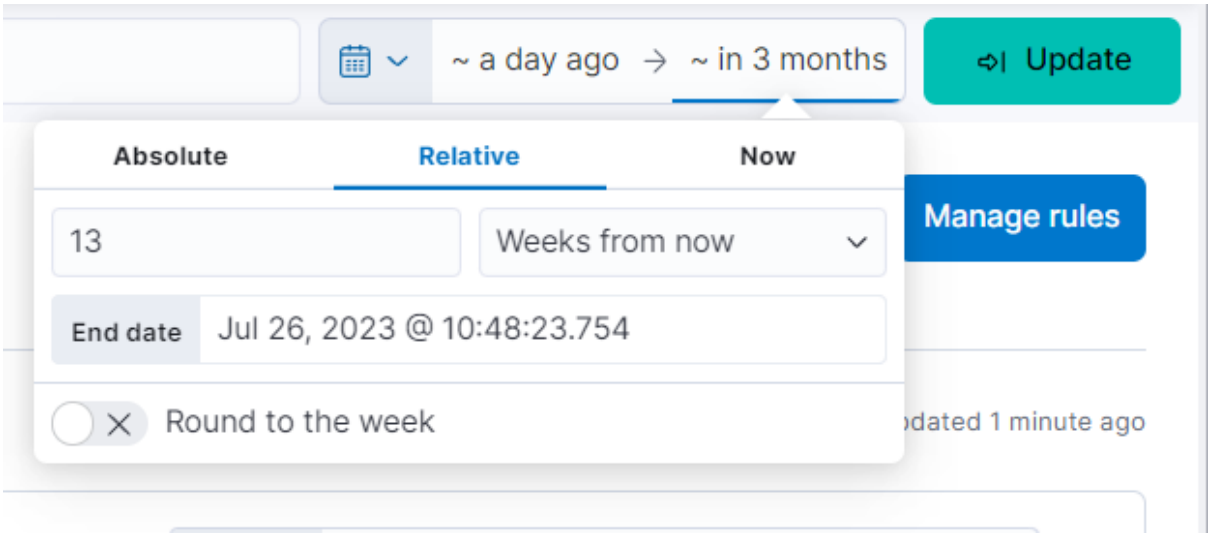
Následne po kliknutí na vybrané upozornenie z prehľadu možno zobraziť detaily ako aj dôvody vygenerovania daného upozornenia.



Obrázok č. 10: Zobrazenie detailov vygenerovaného upozornenia

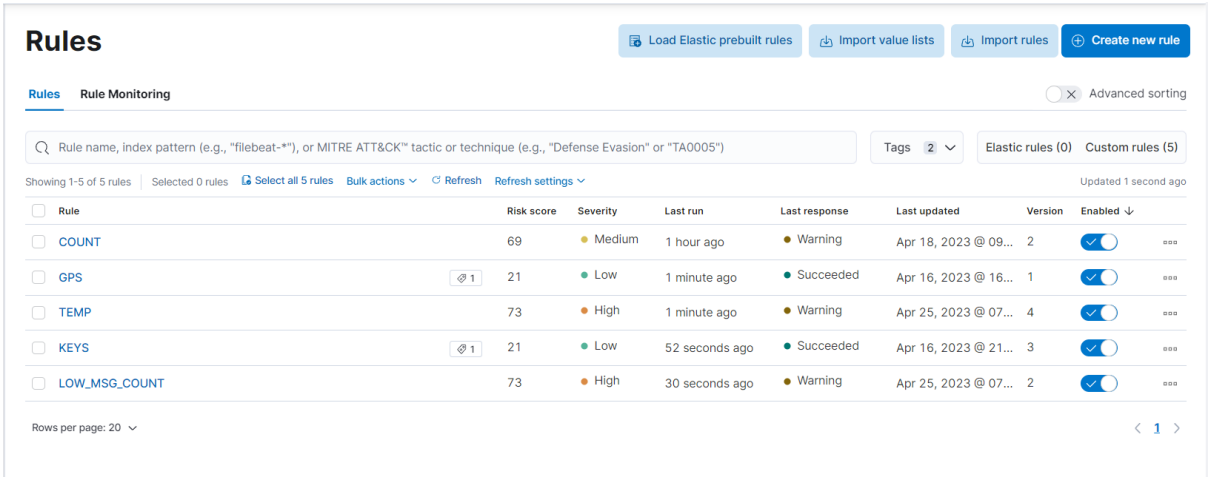
Vytvorenie a manažment pravidiel

Kontrolovať a spravovať pravidlá je možné po vybratí možnosti “Manage Rules” v časti “Alerts”.



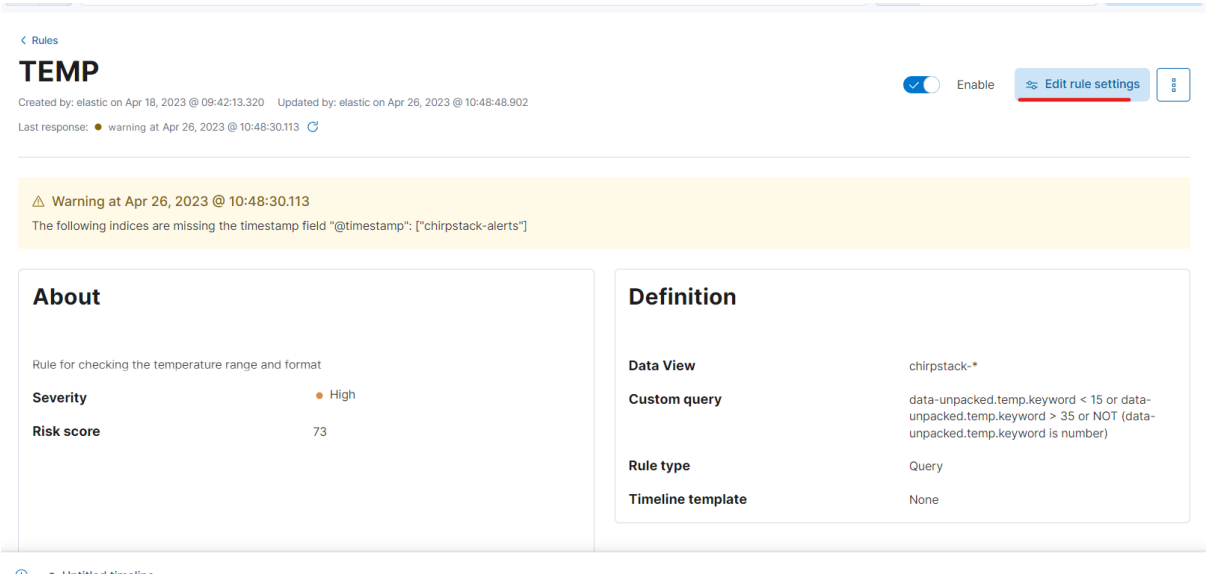
Obrázok č. 11: Manažment pravidiel

Následne sa zobrazí zoznam všetkých pravidiel spolu s informáciami o tom ako často sú spúšťané kontroly na dodržiavanie jednotlivých pravidiel, či sú tieto pravidlá aktívne, prípadne ako závažné resp. kritické je porušenie daného pravidla. V tejto časti je možné aj pridávať nové pravidlá kliknutím na možnosť "Create new rule".



Obrázok č. 12: Prehľad existujúcich aktívnych pravidiel

Po kliknutí na vybrané pravidlo je možné si prezrieť detaily vybraného pravidla. Ako aj pomocou možnosti "Edit Rule Settings" vykonať úpravu daného pravidla.



Obrázok č. 13: Zobrazenie detailov vytvoreného pravidla, prípadná úprava daného pravidla

Referencie

1. Elasticsearch B.V. (2021). Elastic Stack and Product Documentation. Retrieved April 26, 2023, from https://www.elastic.co/guide/index.html