ELK STACK PLATFORMALARIDAN FOYDALANISH ORQALI KIBERHUJUMLARNI ANIQLASH VA BARTARAF ETISH

O.Tirkashev, TATU magistratura talabasi, tirkashevoybek1998@gmail.com
+998(91)5648505

Anatatsiya: ELK stack, ma'lumotlar tahlilatining oson va samarali qilinishi uchun ishlatiladigan bir birlashma tizimi hisoblanadi. Bu nom Elk stackning uchta asosiy komponentlarini (Elasticsearch, Logstash, Kibana) ifodalaydi. Bu modullar quyidagi funksiyalarni bajarish uchun ishlatiladi

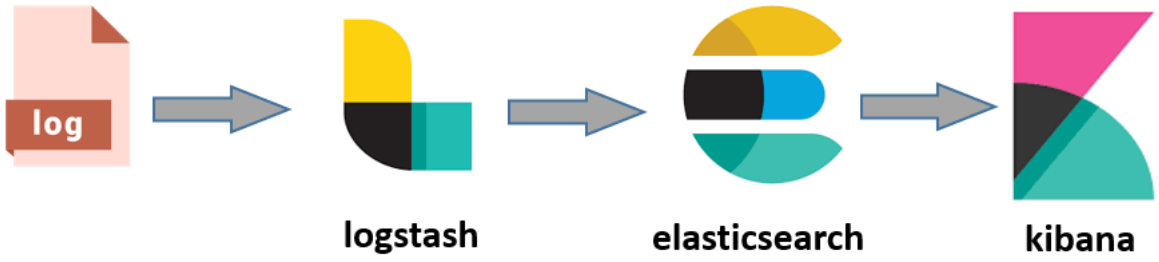
Kalit so‘zlar: ELK-STACK , siem, splunk, logstash, kibana, elasticsearch

Axborot va kiberxavfsizlikni xavfsizligini ta’minlashda monitoring tizimlaridan foydalanish eng afzal yechimlardan biri hisoblanib kelinmoqda. Hozirgi kunga kelib axborot va kiberxavfsizlikni ta’minlash yuzasidan hodisalarni kuzatish va boshqarish tizimlari (SIEM) bir qancha turlari mavjud. Bularga ELK-Stack, Splunk, QRadar, AlientVault USM, AlientVault USM, McAfee USM va boshqa turlari mavjud. SIEM monitoring tizimlari funksiyalariga qarab o‘zaro bir biridan farqlanadi.

ELK-Stack bu ochiq kodli monitoring tizimi hisoblanadi va real vaqt rejimida ma’lumotlarni to‘plash, saqlash, tahlil qilish va vizuallashtirish , jurnallarni boshqarish va monitoring qilish imkoniyatlarini beradi. ELK-STACK monitoring tizimlari tuzilish jihatdan LOGSTASH, ELASTICSEARCH, KIBANA tizimlarining o’zaro integratisyalashganligidan hosil bo’ladi. Bu yerda xavfsizlik tizimlaridan kelayotgan loglarni parsing qilib berishda ishlatiladi yani loglarni filtrdan o’tqazib beriladi.

Elasticsearch, ma'lumotlarni indeksatsiya qilish, qidiruv qilish va tahlil qilish uchun foydalaniladigan yagona kataloglash tizimini taqdim etuvchi ma'lumotlar bazasi tizimidir. U, ko'p yordamchi va uzoq ma'lumotlarni tez va samarali bir qanday olishni osonlashtiradi. Elasticsearch ma'lumotlar bazasi, "JSON" formatidagi ma'lumotlarni saqlash va unga boshqa so'rov yuborish orqali ma'lumotlarni izlash imkoniyatiga ega. Kibana, Elasticsearch, Logstash va Beats

kabi Elastic stack (ELK stack) modullaridan biri hisoblanadi. Bu modul Elasticsearch ma'lumotlar bazasidagi ma'lumotlarni vizualizatsiya qilish, monitoring qilish va boshqa tahlilatlar uchun foydalaniladi. Kibana web-interfays orqali ishlatiladi va ma'lumotlarni grafiklarda, kodlarda, xaritalarda va boshqa ko'rinishlarda ko'rsatishga imkoniyat yaratadi. Bu modul yordamida ma'lumotlar tahlili va nazorati oson va samarali bo'ladi.



1-rasm. ELK STACK tuzilish sxemasi

ELK stackda Machine Learning (ML) ma’lumotlarni tahlil qilish, anomaliyalarni aniqlashda ishlatiladi. Bu Elasticsearch Mashinalar o‘rganish tilining komponenti orqali amalga oshiriladi. Ushbu funksiyalar asosan real vaqt rejimida log va metrikalarni tahlil qilish uchun mo‘ljallangan hisoblanadi.

Elasticsearchning mashinalar tili modeli anomaliyalarni avtomatik aniqlash va vaqt serialari (time series) ma’lumotlarini tahlil qilishga mo‘ljallangan. Bu quyidagi jarayonlarni bajaradi:

- Anomaliyalarni aniqlash: Loglar va metrikalardagi odatiy bo‘lmagan xatti-harakatlarni aniqlash.
- Tendensiyalarni prognozlash: Kelajakdagi tendensiyalarni taxmin qilish.
- Avtomatik tahlil: Ma'lumotlar oqimini doimiy kuzatish va o‘zgacha vaziyatlarda ogohlantirish.

Kibana interfeysi orqali Machine Learning tahlillarini vaqt oralig‘ida va ma’lumotlarni mablarini tanlashda bajarish mumkin. Mashinalar tillarining algoritmlari natijalari grafiklar, diagrammalar va hisob-kitoblar orqali Kibana dashboardida ko‘rsatiladi.

Xulosa qilib aytganda, Axborot va kiberxavfsizlikni ta’minlash yuzasidan hodisalarni kuzatish va boshqarish tizimlarini eng afzali sifatida ELK STACK

monitoring tizimi funksionalligi, imkoniyatlari ko’pligi bois keng foydalanib kelinmoqda.Integratsiya jarayonlari orqali tarmoq xavfsizligini boshqarishda markazlashgan tizimni yaratish mumkin. ELK Stack yordamida turli xavfsizlik qurilmalaridan kelgan log ma'lumotlarini yig'ish, qayta ishlash va vizualizatsiya qilish samaradorligi oshiradi. Kiberhujumlarni aniqlash mexanizmlarini yaxshilash uchun tahliliy yondashuvlar ishlab chiqiladi. Olingan log ma'lumotlari asosida avtomatlashtirilgan va real vaqt rejimida hujumlarni aniqlash imkoniyati yaratiladi. PfSense, Fortinet va Checkpoint tizimlarining ELK Stack bilan birlashtirilishi loglarni qayta ishlash tezligini oshirishga va xavfsizlik hodisalarini tezkor aniqlashga yordam beradi.

Foydalanilgan adabiyotlar

1. https://www.elastic.co/guide/en/machine-learning/current/index.html
2. https://www.ibm.com/topics/siem
3. Packt Publishing- Elasticsearch 8.x Cookbook: Over 180 recipes to perform fast, scalable, and reliable searches for your enterprise, 5th Edition
4. Piter- Elasticsearch, Kibana, Logstash I Poiskovye Sistemy Novogo Pokoleniya