TÍM č. 14 SI-IS

Talented Otters

Názov projektu:
SecMon

Členovia tímu (študenti):
Norbert Danišik, Matej Guráň, Matúš Jurika, Štefan Kadlic, Roland Lang, Matej Puk

Ved. tímu (pedagóg):
Dr. Ján Laštinec

Motto tímu:
SecMon – Security Events Correlator done right!

O ČOM JE NÁŠ PROJEKT?

V dnešnej dobe komplexných sieťových riešení a nastupujúceho Internetu vecí je dôležitá nielen aktívna ochrana bezpečnostnými uzlami v sieti, ale predovšetkých zber údajov a ich včasné efektívne vyhodnocovanie a následná exekúcia potrebných bezpečnostných opatrení.

Tieto požiadavky sú zabezpečnované SIEM (Security Information and Event Managment) nástrojmi, ktoré ale často vyžadujú odbornú znalosť a drahé licencie na ich prevádzku. Preto sme sa v rámci nášho projektu rozhodli vytvoriť voľné širiteľný nástroj na zber a koreláciu logov z rôznych sieťových zariadení.

Jadrom nášho systému je nástroj SEC, ktorý dokáže prúdovo spracúvať záznamy zo zariadení a priamo hľadať medzi nimi súvislosti v medziach sieťovej bezpečnosti. Avšak SEC je realizovaný iba v príkazovom riadku a preto bolo vhodné postaviť prehľadnú, konfigurovateľnú a škálovateľnú webovú aplikáciu, ktorá bude slúžiť nielen skúseným bezpečnostným inžinierom, ale aj bežným používateľom, ktorí chcú vo svojej domácnosti prevádzkovať hĺbkovú ochranu a monitorovanie svojich informačných technológií.

Architektúra nášho systému je postavená na Apache Web serveri, na ktorom beží PHP aplikácia, ktorá riadi činnosť nástroja SEC. Databáza PostgreSQL slúži na ukladanie korelovaných udalostí, ale aj nekorelovaných logov, ktoré je možné spätne naviazať na jednotlivé skorelované bezpečnostné udalosti. Tento prístup poskytuje bližší náhľad do príčin vzniku danej kritickej udalosti a možnosť hĺbkovej analýzy problému.

Aplikácia ponúka správu používateľov, ktorých je možné rozdeliť do viacerých podskupín na základe ich práv. Vďaka tomu je SecMon univerzálnym nástrojom, ktorý je možné použiť s preddefinovanými pravidlami detekcie a upoznorňovania na bezpečnostné udalosti. Tento prístup ocenia predovšetkým menej skúsení používatelia, ktorí napriek tomu chcú pridať ďalšiu vrstvu zabezpečenia ich infraštruktúry. Na druhej strane, skúsení bezpečnostní inžinieri majú plnú kontrolu nad pravidlami, ktoré môžu prídávať, upravovať a nasadzovať na mieru tej danej sieti, v ktorej operujú.

V konečnom dôsledku je SecMon plne konfigurovateľné a škálovateľné riešenie pre všetky typy sieťových prevádzok. Nástroj postkytuje pohľad do aktivity na sieti, štatistík a vzniku bezpečnostných udalostí

a incidentov. V budúcnosti je možné tento nástroj rozšíriť o detekciu anomálií v sieti.

ČO NÁM DÁVA PRÁCA NA TOMTO PROJEKTE?

Tento projekt je pre nás príležitosť ako si vytvoriť obraz o reálnom procese plánovania, návrhu, vývoja a testovania rozsiahlych projektov v rámci domény softvérového inžinierstva a informačných systémov. Od začiatku je potrebné dbať na zosúladenie a rozdeľovanie jednotlivých podúloh medzi všetkých členov tímu na základe ich znalostí a zručností, aby boli všetky fázy vývoja softvéru od návrhu až po testovanie efektívne zvládnuté. Tento projekt sa nás taktiež snaží priučiť lepšej estimácii v rámci podúloh a časovej zodpovednosti voči zvyšku tímu. Predovšetkým sa jedná o úlohy, ktoré sú kľúčové pre pokračovanie vývoja ďalších modulov.

Po technickej stránke nám poskytuje náhľad do niekoľkých rôznych technológií, ktoré sa využívajú pri vývoji softvéru. Patria medzi ne nástroje pre manažovanie Scrum metodiky v tíme, zapisovanie a spravovanie vytvorených, začatých a dokončených úloh ale aj iných – oveľa technickejších nástrojov, ktoré slúžia na podporu vývoja a postupnú integráciu. Veľa z kolegov nemá možnosť sa priamo zoznámiť s technológiami v rámci väčších projektov a tímový projekt nám poskytol možnosť, chtiac-nechtiac začať využívať mnohé nové technológie.

Ďalej nám bezpochyby dala práca na tomto projekte aj veľa ťažkých chvíl pri písaní a dokumentovaní každého kroku jednotlivých členov tímu a generovanie redundantných informácií o projekte, ktoré sú pre každého mladého inžiniera nočnou morou v procese vývoja. A práve preto nás to naučilo, že veľakrát je prezentácia, marketing a manažment silnejšou zbraňou ako samotný produkt pri získavaní investorov a účelových hodnotení projektu.

Ale napriek tomu sme srdcom inžinieri a v rámci tímového projektu sa nám podarilo spojiť navzájom svoje sily a zabojovať voči nepriazni termínov a priniesť produkt, ktorý je lepší ako dokumentácia k nemu. Dôležité bolo v ťažkých chvíľach semestra nebyť alibista a pomôcť

spolužiakovi s jeho úlohami, aby sa darilo spĺňať prísne a intenzívne termíny jednotlivých šprintov. Dôležitý poznatok, ktorý sme si odniesli je taký, že čím častejšie sú stretnutia a stand-up meetingy, tým častejšie sa ľudia snažia pracovať na jednotlivých úlohách a nenechávajú si všetko na poslednú chvíľu.

PREČO JE NÁŠ PROJEKT ZAUJÍMAVÝ?

Náš projekt s názvom SecMon je webová aplikácia, ktorej jadrom je open-source nástroj na korelovanie udalostí a procesovanie záznamov generovaných zariadeniami – uzlami v sieti. SecMon je univerzálne riešenie monitorovania siete pre rôzne typy infraštruktúry a skupiny používateľov. Pre laikov v oblasti informačnej bezpečnosti poskytuje tento nástroj prehľadné rozhranie na sledovanie aktivity na sieti s preddefinovanými pravidlami korelovania bezpečnostných udalostí. Na druhej strane, skúsený bezpečnostný inžinier má možnosť vytvárať priamo pravidlá korelovania, nastavovať preddefinované videnia zobrazujúce štatistiky a údaje v grafoch a tabuľkách. Tento nástroj slúži predovšetkým na včasné detegovanie a zabránenie vzniku kritickej bezpečnostnej udalosti na sieti používateľa.

POUŽITÉ TECHNOLÓGIE:

SEC Simple Event Correlator, PHP YII, PostgreSQL, D3.JS

O ČOM TO VLASTNE JE?

SecMon je open-source nástroj na monitorovanie a koreláciu bezpečnostných udalostí s podporou manažmentu pre domáce aj firemné siete. Náš projekt ponúka konfigurovateľné a škálovateľné riešenie vyššej vrstvy detekcie sieťových a aplikačných útokov pomocou jednoducho rozšíriteľného korelátora logov zozbieraných z niekoľkých zariadení.