SECURITY SOLUTIONS

GO BEYOND THE LIMIT.

SPACENETWORKS.HU

SPACENET
innovate together

AUTOMATIZÁCIÓ BEVEZETÉSE CISCO FIREPOWER REST API SEGÍTSÉGÉVEL

Ügyfeleinknél az elmúlt években rengeteg Cisco Security (Firepower – ISE – ESA-ThreatGrid – WSA- AMP – Umbrella - DUO) rendszert vezettünk be, ennek köszönhetően nagyon sok tapasztalatot gyűjtöttünk ezen a területen. A tavalyi évben már elkezdtük használni a gyártó által kiadott és dokumentált REST API adta lehetőségeket és egyszerűséget azért, hogy a rendszerek „beszélgessenek" egymás között emberi beavatkozás nélkül, automatizáltan, biztonságosan és hatékonyan, ezzel is növelve a felhasználói élményt és az üzemeltetés magasabb szintre emelését.

A tendencia azt mutatja, hogy a biztonsági mérnököknek nagyon sok napi feladata van, már egy egyszerűbb hálózatban is ezért ezzel a DevNet-es fejlesztéssel levesszük a napi üzemeltetési terhet a vállukról.

A Cisco Firepower tűzfalrendszerek a legelterjedtebbek ügyfeleinknél, ezért létrehoztunk egy olyan API vezérelt felületet, amit egy általános tűzfalas tapasztalattal rendelkező mérnök is kezelni tud. A Cisco FMC (Firepower Management Center) Rest API felülete lehetőséget biztosít arra, hogy a jól ismert Grafikus User Interface (GUI) által is biztosított funkciókat gépi interface-en keresztül is el tudjuk érni.

Ezt az interface-t arra tudjuk használni, hogy egy webes felületre kivezetve szabjuk testre oly módon, hogy az az üzleti folyamatokba beilleszthető legyen.

A hierarchikus felépítésű jogosultsági rendszerben az alkalmazásfejlesztői vagy IT üzemeltetés oldalon keletkező igényeket egy webes felületen meg lehet adni, amit az üzemeltetői adminisztrátor csoport ellenőriz és állít be. Az igények érkezhetnek táblázatos formában is megfogalmazva, akár tömegesen, amelyek szintén egyszerűen betölthetők a rendszeren keresztül.

A felépített rendszer lényege, hogy a GUI-n nehézkesen és lassan elérhető és sokat használt funkciók könnyedebben és gyorsabban működjenek – a fejlesztett funkciók a rendszer rugalmassága miatt, az igények érkezésével könnyedén tovább fejleszthetők. Célja az, hogy megkönnyítse, felgyorsítsa a szabályok és a szabályok elemeinek menedzsmentjét, ezen felül egyéb segítő funkciókat implementáljon. Megvalósítása egy Python alapú, Docker környezetben futó webes alkalmazás, amely az FMC REST API-n keresztül kommunikál az FMC-vel.

MEGVALÓSÍTOTT FUNKCIÓK

Szabályok és elemeinek egyszerű menedzsmentje

– objektumok létrehozása/törlése
  - host, FQDN, network, port, URL típusú objektumok
  - ezen objektumok csoportosítása
– access-policy létrehozása
– access-policyhoz tartozó rule-ok létrehozása
– a fentikek tömeges létrehozása
– importálás táblázatos formátumból
– exportálás táblázatos formátumba

Logfeldolgozás

Célja az FMC Connection Event Reporting felületéről exportált logok feldolgozása, átdolgozása egy olyan formátumra, amely alapján szabályok készíthetők

– a logok alapján a nem ismert, betöltendő objektumok táblázatai legenerálódnak, betölthetők
– host IP vagy FQDN alapú táblázatok generálhatók
– duplikált események felismerhetőek

SPACENET
innovate together

Logfile-ok összehasonlítása

Célja a logok vagy betöltött szabályrendszerek összehasonlítása, és a különbségek megtalálása

– a különbségek exportálása
– Host IP vagy FQDN alapon is elvégezhető az összehasonlítás

Objektumok törlése

Az FMC-ben létrehozott, de policy-ban nem felhasznált objektumok törlésére van lehetőség.

Jogosultságkezelés

Authentikáció és authorizáció lokális, RADIUS és LDAP metodika alapján.
Jogosultsági szintek

– Requester
– Admin

Leaping forward to revolutionize the industry of technology.

A Requester be tud lépni a rendszer webes felületére és létre tud hozni egy szabályigényt a rendszerben található objektumok vagy akár új objektum segítségével.

Az Adminisztrátor látja a requesterek által feladott igényeket, és azokat meglévő vagy új Access-Policy-hoz tudja rendelni. Ezen felül a rendszer teljes funkcionalitásához van jogosultsága.

A projekt zárása után a fejlesztés nem állt meg, az ügyfeleknél történő éles használat során újabb fejlesztési igényeket fogalmaztunk meg, illetve további hálózati és biztonsági rendszerek API-n történő vezérlésének fejlesztése is elindult.