RSA Security Analytics

Észlelje és vizsgálja ki a legújabb fenyegetett-ségeket is

ÖSSZEFOGLALÓ

Az RSA Security Analytics Infrastruktúra

- moduláris felépítésű, elosztott architektúrájú
- Metadata alapú a gyors indexeléshez, tároláshoz és kereshetőséghez
- RSA NetWitness alapok az analízishez, elemzésekhez
- Adattárház a hosszútávú archiváláshoz

MINDEN FELMERÜLŐ ADATOT GYŰJTSÜNK, TÁROLJUNK, ANALIZÁLJUNK

Ma, a folyamatosan növekvő számú és bonyolultságú kártevők világában létfontosságú, hogy biztonságos infrastruktúrát üzemeltessünk. Ehhez pedig a logok, session információk begyűjtése, tárolása, elemzése ugyanúgy hozzátartozik, mint az analízist segítő adattárházak és az intelligens előrejelzések. Természetesen a compliance igények is egyre szigorúbbak. Az RSA Security Analytics platform ehhez nyújt segítséget, két fő komponensével, a log / hálózati csomag gyűjtő moduljával és az adattárházával.

A gyűjtéssel kapcsolatban három almodul különböztethető meg:

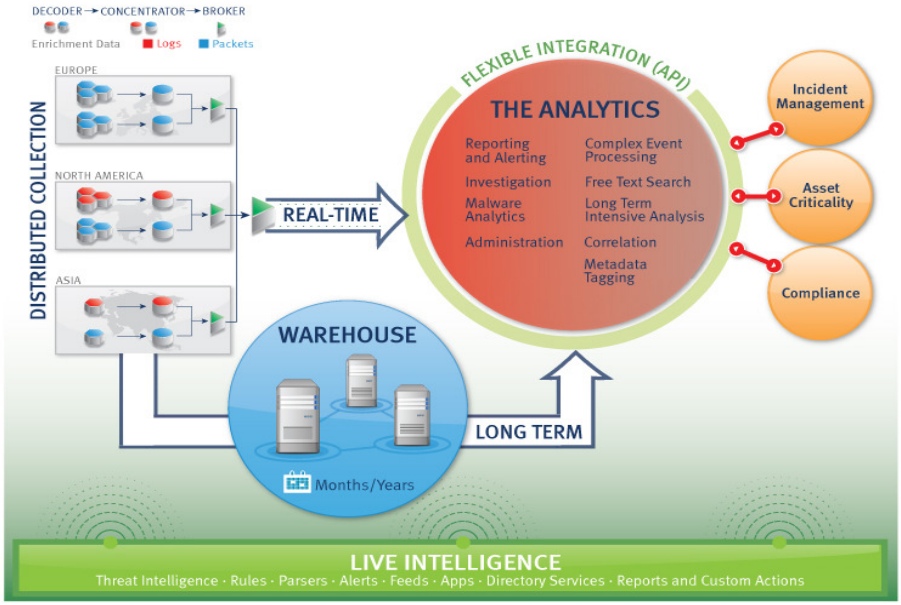
-Decoder (logokra és teljes hálózati csomag forgalomra)

-Concentrator

-Broker

Mindegyik komponens kulcsfontosságú, hiszen a stabil, skálázható, redundáns kiépítéshez mindhárom részre szükség van. Persze a valósidejű elemzésekhez, alkalmazás szintű logokhoz a megfelelő infrastruktúra is elengedhetetlen. Az RSA Security Analytics megoldás skálázható, hogy igazán nagyvállalatok igényeit is ki tudja elégíteni, és hierarchikus, hogy könnyen átlátható legyen. Sőt akár külön is választható a primary read és a write-to-disk funkcionalitás a kellő sebességért.

RSA SECURITY ANALYTICS INFRASTRUKTÚRA



RSA

EMC²

ADATGYŰJTÉS

DECODER

A Decoder a legelső, legalapvetőbb komponense a Security Analytics rendszernek. Nem csak a logok, de a hálózati csomagok gyűjtésére is alkalmas (ezek azonban külön hardveren futnak alapértelmezetten), sőt a további analízist is segíti. Minden olyan telephelyre, hálózati tartományba, zónába kell egy Decoder, ahonnan logot, session információt szeretnénk gyűjteni.

A Packet Decoder hálózati csomagokat gyűjt, normalizál, indexel mindezt az OSI 2-7. rétegében. A Packet Decoder folyamatosan képes a forgalom elemzésére.

A Log Decoder hálózati logok gyűjtésére, indexelésére lett kifejlesztve, több, mint 200 típust és formátumot támogat.

A Decoder eszközök által összegyűjtött információk indexelésével alkalmazás, felhasználó, forrás, cél, esemény, log alapján is kereshetünk, készíthetünk kimutatásokat. Compliance, és tárolási követelmények is kielégíthetők az RSA Security Analytics szerverrel kombinálva.

CONCENTRATOR

A Concentrator-ok a Decoder komponensekből származó adatok agregálására képes, hierarchikus felépítése miatt rugalmasabban skálázható. Egyetlen Concentrator több Decoder-el is állhat kapcsolatban, de vagy csak log, vagy csak packet agregálására alkalmas a dedikált Concentrator.

BROKER ÉS SECURITY ANALYTICS SZERVER

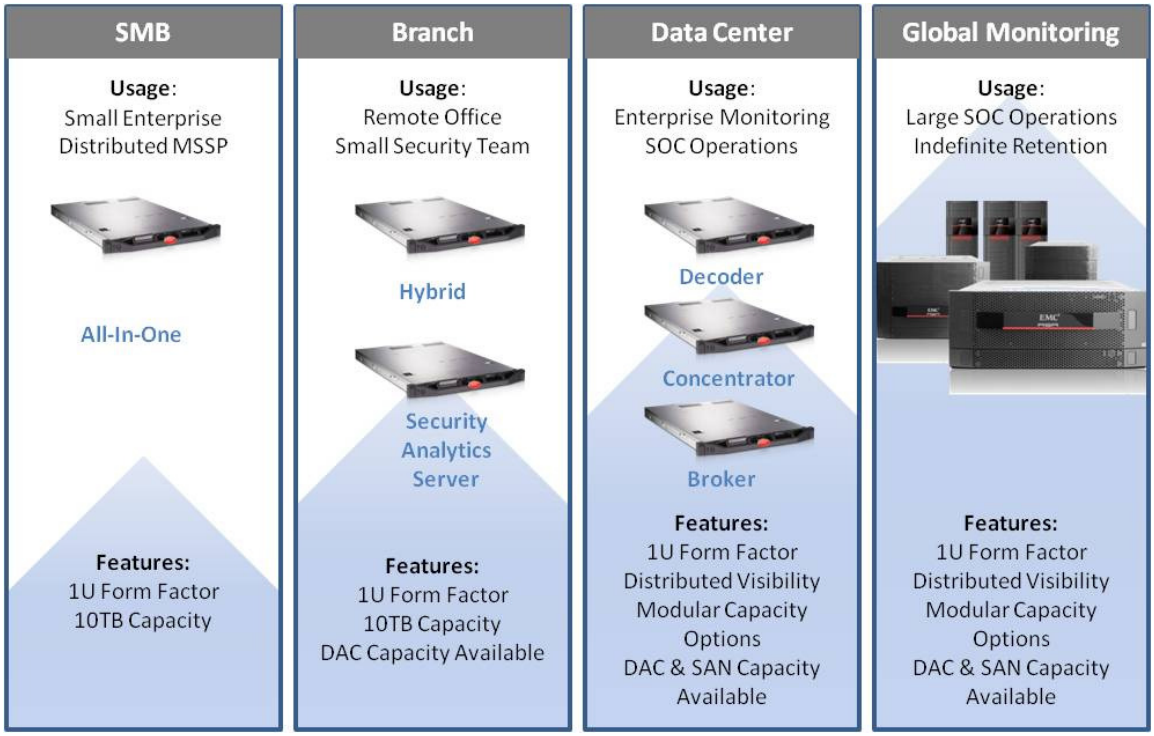
A Broker és a Security Analytics szerver alapértelmezetten egyetlen hardveren futtatható, és ezen komponensek a legmagasabb hierarchia szinten lévő modulok. A Broker szerver funkciója a lekérdezések, elemzések, kimutatások futtatása ha több Decoder, Concentrator található a rendszerben. A Broker-ek segítségével az összes metadata lekérdezhető függetlenül a hálózat kiépítésétől (késleltetés, sávszélesség, adatmennyiség).

A Security Analytics szerver a felhasználói felületet, konzolt kezeli, ezzel a discovery, investigation, reporting és administration menü érhető el. Támogatja a role based elérést, és a kétfaktoros azonosítást is (HMTL5 alapú).Továbbá adattárházak esetén az ezzel kapcsolatos tevékenységek is erről a felületről indíthatóak.

ADATTÁRHÁZ AZ ANALÍZISEKHEZ

HOSSZÚTÁVÚ ADATTÁROLÁS ÉS INTENZÍV ANALÍZISEK

Az RSA Security Analytics Warehouse egy opcionális kompones a meglévő SA rendszer mellé. Hosszútávú archiválásra, előrejelzések, riportok készítésére, testreszabott analízisek futtatására alkalmas. A Hadoop technológiának köszönhetően párhuzamos szálak futtatásával, nagyon jól méretezhető nagymennyiségű adathalmaz elemzésére is. Több storage opció is elérhető az adattárházhoz, így illeszthető az elvárásokhoz a tárolórendszer is (akár évekre visszamenőlegesen is képes adattárolásra). Eltérően a hagyományos SIEM megoldásoktól, itt nem csak a storage méretezésére van szükség, de az úgynevezett Warehouse node-okra is (elosztott adathalmazokon, szeparáltan futnak az elemzések). Minden egyes node dedikált adathalmazért felel, így a node-ok számának növelésével a teljesítmény növelhető.



SKÁLÁZÁSI OPCIÓK

Hogy minden vállalatméretre optimális megoldást tudjon az RSA kínálni, négy különböző opcióban érhető el a Security Analytics:

KIS-, KÖZÉP-, NAGYVÁLLALATOK

Kisvállalatok esetén ideális az AI-in-One megközelítés, melynél minden almodul (Decoder, Concentrator, Broker, Security Analytics szerver) egyetlen appliance-on futtatható. A megoldás magában működőképes, nincs szükség további komponensekre, de természetesen teljesítményben, méretezésben, redundanciában kompromisszumot kell kötni. A csatolt storage 10 TB kapacitású, de ez tovább bővíthető 22, vagy 32 TB-ra.

TELEPHELYEK

Telephelyek esetén kihasználható a Hybrid appliance (melyben a Decoder és a Concentrator fut egyetlen appliance-on).Ezzel a hardverrel már kielégíthetők nagyobb telephelyek igényei is és képesek vagyunk elosztott architektúrát kiépíteni. A Hybrid appliance elérhető loggyűjtésre (Hybrid for Logs) és a teljes hálózati forgalom tárolására is (Hybrid for packets). A Hybrid komponens mellé szükséges egy Security Analytics szerver is. A Security Analytics szerver viszont működhet Hybrid és külön Decoder, Concentrator környezetben is. A Hybrid appliance is kiegészíthető 22, vagy 32TB storage-el.

DATA CENTER

Magas követelményrendszernél javasolt a Security Analytics szerver, Decoder, Concentrator, Broker modulok dedikált appliance-on futtatása. Igy nagyobb sávszélesség, EPS (events per second), teljesítmény érhető el. A hierarchikus kiépítés több telephelyes vállalatnál segít a pontos méretezésben, valamint a valósidejű elemzésekben, hosszútávú logtárolásban.

SZOLGÁLTATÓK

Szolgáltatók, gerinchálózatok üzemeltetőjeként, még magasabb követelmények vannak. Itt akár több millió EPS is skálázható a rendszer, ehhez méretezett storage jár, ezzel segítve az IT biztonsági szakemberek munkáját.

RUGALMAS INTEGRÁCIÓ

A felhasználók akár a saját fejlesztésű alkalmazásaikkal is illeszthetik a Security Analytics-et, hiszen elérhető a nyílt API, így kiegészítve a két rendszer képességeit.

Azonnal láthatóvá kell tenni minden releváns információt, hogy a vállalatok reagálni tudjanak a támadásokra, pontos előrejelzések készüljenek, láthatóak legyenek a kritikus szolgáltások hibái, felfedhessük az adatszivárgást.

Az RSA megoldása képes erre, köszönhetően a loggyűjtési, hálózati csomagelemzési képességének, a threat intelligence szolgáltatásnak, az alkalamzásszintű elemzéseknek, melyek megkülönböztetik más gyártóktól.

KAPCSOLAT

Amennyiben további információra kíváncsi az RSA Security Analytics-el kapcsolatban, keresse fel az RSA magyarországi disztribútorának honlapját:

http://www.arrowecs.hu/products/rsa/rsa_products.php

Vagy keresse bizalommal az Arrow ECS kollégáit az alábbi mail címen:

rsa@arrowecs.hu