ÚJ GENERÁCIÓS SECURITY MENEDZSMENT

Hogyan lehetséges több millió logbejegyzés azonnali analízise ("Big Data" koncepció)?

ÖSSZEFOGLALÓ

- Egyre bonyolultabbá válik a security menedzsment, hiszen naponta éri támadás a vállalati hálózatot és még plusz compliance követelmények is felmerülnek
- Már nem elég csak a logbejegyzések összegyűjtése, de szükséges a valósidejű reagálás az új típusú támadásokra
- Ez a kettősség (analizáljuk az adatokat, de intelligensen reagáljunk a támadásokra) tette szükségessé a SIEM termékek következő generációját

Embert próbáló feladat manapság IT biztonsági szakemberré válni. A fenyegetettségeknek ugyanis nem csak a száma, de a bonyolultsága is növekszik. E mellett egyre nagyobb feladat a compliance is. Mindez megfűszerezve az egyre komplexebb infrastruktúrával teljes embert kíván. Azonban a "Big Data" koncepció és az ezzel járó analizáló és intelligens alkalmazások talán könnyebbé tehetik a szakemberek munkáját.

Meg kell érteni a beérkező logokat, azok minél gyorsabb feldolgozása szükséges (és persze tárolni is kell a keletkezett eseményeket). Ezért minél nagyobb segítséget kell nyújtani a szakembereknek, hogy hatékonyan dolgozzanak, a vállalatunk teljeskörű védelme megoldott legyen.

A MAI KÁRTEVŐK NEM ADNAK ESÉLYT AZ AD-HOC VÉDEKEZÉSI STRATÉGIÁKNAK

Amikor a "Big Data" kifejezést használjuk, akkor akkora mennyiségű és komplexitású adatra gondolunk, melynek a feldolgolgozása a hagyományos megoldásokkal lehetetlen. Igy az összegyűjtött adatokból a használható információk előállítása sem megoldott.

Ráadásul a hackerek sem az unatkozó kamaszok többé. Nehezen detektálható és összetett támadásokkal próbálnak adatokat szerezni. A Verizon Data Breach Investigations tanulmánya szerint a támadások 91 %-át csak napokkal később, míg 79 %-át hetek múlva észlelik csak az érintettek.

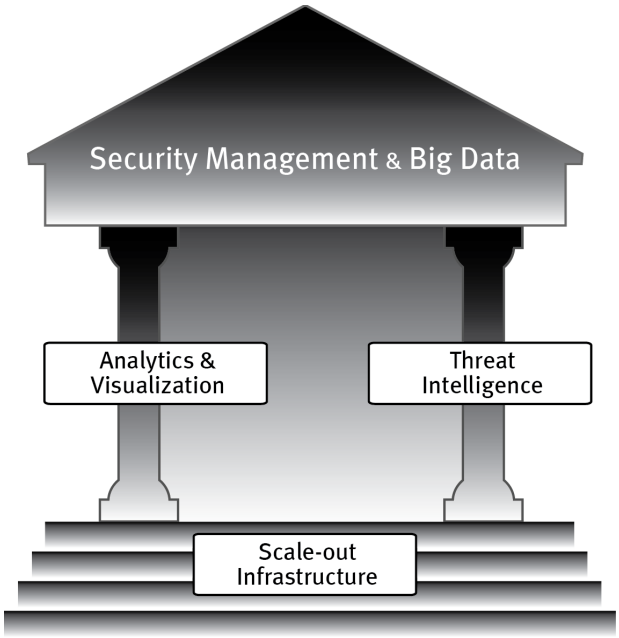
Ez a lehangoló eredmény több összetevő miatt alakulhat így:

- A támadók egyre szervezetebbek és egyre képzettebbek. A támadások dinamikusak és összetettek, de a védelem még mindig statikus. A mai kártevők a sérülékeny adatra öszpontosítanak, mely a hálózaton (belső hálózat, WiFi, szerverek, adatbázisok, közösségi hálók) bárhol feltűnhet.
- Az IT infrastruktúrák egyre komplexebbek. A rendszereknek egyre nyitottabbaknak, könnyen hozzáférhetőnek kell lennie, hiszen a mobil munkavégzés, a csoportmunka csak így támogatható. De ez sajnos nem csak új lehetőségeket, de új fenyegetettségeket, sérülékenységeket is jelent a hackerek számára.
- A compliance riportok is egyre szigorúbbak, egyre több idő kell a megfelelő kimutatások elkészítéséhez. A vállalatok nagy része (a multinacionális vállalatok) egyszerre több előírásnak, jogszabálynak, helyi törvényeknek is meg kell felelnie, ez szintén időt vesz el a szakemberektől.

Ez a hármas hatás teszi egy nehezebbé a Security menedzsment munkatársak feladatát, egyre nagyobbá a felelősségüket. A mai SIEM, sérülékenység menedzsment, konfiguráció menedzsment megoldások egyszerre könnyítik és nehezítik a szakemberek munkáját (könnyebben összegyűjthető, de órisási mennyiségű adatról van szó). Ebből a nagy mennyiségű adatból kell kiszűrni azokat az eseményeket, melyekre valósidőben reagálni kell.

A HÁROM ALAPVETŐ ELVÁRÁS A SECURITY MENEDZSMENTTEL KAPCSOLATBAN

Az igazi "Big Data" stratégia mindhárom pillérre épül - a skálázható infrastruktúrára, az analízisre és a fenyegetettségekkel szembeni intelligenciára.



1. ábra: A Security mendzsment tartóoszlopai nagyvállalati környezetben

A kusza adathalmazból kihámozni a számunkra releváns eseményeket, mindezt valósidőben, ezt jelent a "Big Data" megközelítés. Ez a következő elemekre épül:

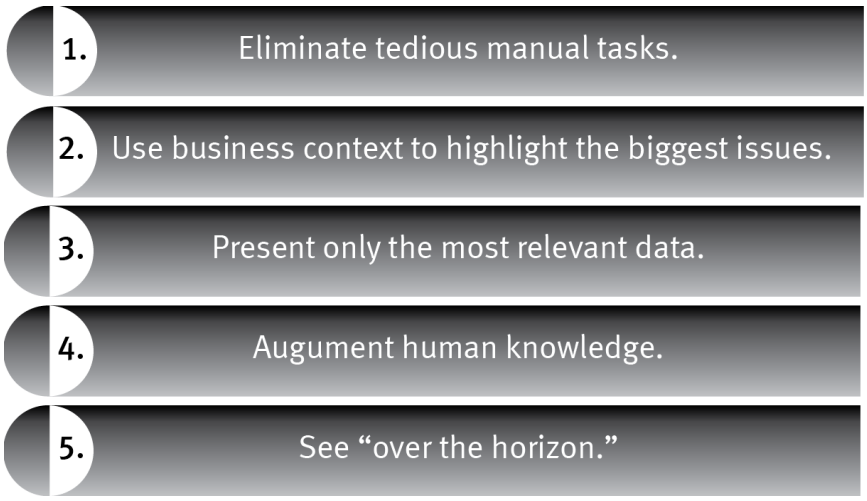
- A folyamatosan változó infrastruktúra, melynek meg kell felelnie az új kihívásoknak, mint például: mobilitás, virtulizáció, cloud, outsourcing. Sőt, ezekről az új rendszerekről a logokat össze kell gyűjteni és fel kell dolgozni. E mellett készen kell állni, minden új technológia bevezetésére, rövid idő alatt, akár heteken belül. Az infrastruktúrnák robosztusnak, megbízhatónak, de ugyanakkor skálázhatónak és könnyen bővíthetőnek kell lennie, és ezt a SIEM megoldásoknak is tudnia kell.
- Analizáló eszközök és megjelenítő alkalmazások, melyek a szakemberek minden igényét kiszolgálják, segítve az előrejelzéseket, kimutatások készítését, riportolást. Egyesek munkájához az alapszintű log bejegyzések elegendőek, de a menedzsereknek már áttekintő riportokra van szüksége, az IT biztonsági munkatársaknak pedig intelligens programokra, és nagysebességű adatfeldolgozásra. Van ahol ez sem elég és a teljes (session alapú) kommunikáció tárolása elengedhetetlen.

- A threat intelligence modul egy analizáló technológia, mely a teljes adathalmazon futtatandó. Ugyanis, a felmerülő támadásokról az érintetteknek azonnal tudomást kell szerezni és arra reagálni kell. Valamint ezeket a beérkező eseményeket korellálni is kell, hogy az irreleváns adatok ne jelenjenek meg a konzolon.

A "Big Data" megközelítés nem csak nagymennyiségű adatot jelent, hanem azt az intelligenciát az alkalmazásokban, amivel képesek értelmezni az aktuális helyzetet, és reagálni tudnak a fenyegetettségekre.

"BIG DATA ANALYTICS" JELENTI A HATÉKONY, REAKTÍV BIZTONSÁGOT

A sikeres Security menedzsment megoldás az, mellyel képesek vagyunk valósidőben kinyerni az analízishez szükséges adatokat.



2. ábra: A Security menedzsmenttel kapcsolatos követelmények nagyvállalati környezetben

Az IT biztonsági osztályok manapság óriási mennyiségű adattal dolgoznak, hiszen pontosan meg kell ismerni az "ellenséget", hogy reagálni tudjunk a lépéseire. Szükséges azt is tudni, hogy egyáltalán milyen adatokra van szükség ahhoz, hogy a megfelelő döntéseket hozzuk, ehhez pedig a megfelelő infrastruktúra fejlesztés is kell. A "Big Data" megközelítés azt is jelenti, hogy ezt folyamatosan fenn kell tartani, nem elég hirtelen egy-egy projekt, vagy analízis során összegyűjteni az adatokat, hiszen vizsgálni kell a trendeket is. A sikeres megközelítéshez a következő lépések szükségesek:

- Ki kell iktatni a manuális, emberi beavatkozást igénylő feladatokat, folyamatokat. Minimalizálni kell az összes biztonsági menedzsmenttel összefüggő lépéseket, mert így csökkenthető a hiba lehetősége, gyorsítható a folyamat. A párhuzamos feladatokat (pl.: egy támadás hatását vizsgálni mondjuk 5 különböző konzolon) is érdemes kiiktatni, ez integrált rendszerekkel érhető el.
- Vizsgálni kell a függőségeket. Nem csak azt kell tudni, hogy mikor és hol történt a támadás, de tudni kell azt is, hogy ez melyik alkalmazást érintette. Ezek az összerendelések azért is fontosak, hogy döntéshelyzetben meg lehessen találni a döntéshozókat. Igy kialakítható a teljes rendszer, ahol a felelősök, külsős munkatársak, szolgáltatók és a kritikus alkalmazások össze legyenek kapcsolva.

- Csökkentsük le azokat az eseményeket, melyekre reagálni kell, azaz minimalizáljuk a false-positive bejegyzéseket. Napi ezernél több riasztás már kezelhetetlen méretet jelent, viszont ha csak 10-20 releváns riasztás jelentkezik a rendszerben, akkor arra hatékonyan lehet válaszolni. Természetesen nem könnyű kiszűrni a téves riasztásokat, nagyon vékony a határvonal a releváns és az irreleváns esemény között. Nem csupán az adott eseményt, de a trendeket, változásokat is követni kell, így könnyebben eldönthető egy eseményről, hogy érdmel-e plusz figyelmet. Az is fontos, hogy a releváns adatokat priorizáljuk, így egyszerűsíthető a szakemberek munkája.
- Becsüljük meg a szakemberek tudását. Csak azokat a feladatokat bizzuk rá, amelyekre reagálni kell, és azokat is priorizálva lássák. Így a leghatékonyabb munkavégzés érhető el, ehhez persze szükségesek a legújabb technológiák, eszközök is, sőt a munkafolyamatokat is optimalizálni kell.
- Kapjunk teljes képet a rendszereinkről. Ne csak azt lássuk, hogy aktuálisan mi történik, de tudjuk azt is, hogy ez milyen alkalmazásokat érinthet. Ezzel gyorsítható a reagálás, hiszen a security menedzsment alapvetően harc az idővel. Ezért is szükséges, hogy a védelmi rendszerek ne a klasszikus passzív vonalat képviseljék, de használjuk ki a reaktív védelmi megoldások sebességét is.

SECURITY ANALYTICS: LÉPCSŐZETES MEGKÖZELÍTÉS A "BIG DATA" ALAPÚ SECURITY MENEDZSMENTHEZ

Igaz, hogy a jövőben testreszabható és részletes analizáló megoldások várhatóak, mint ahogy statisztikai módszerekkel működő alkalmazások is, de fontos, hogy már ma elkezdjük kiépíteni az ehhez szükséges infrastruktúrát.

- Olyan infrastruktúrát tervezzünk, mely képes a vállalattal együtt növekedni, és lehetséges legyen hozzá további modulok, rendszerek illesztése. Nem elégséges biztosítani, hogy a logok megérkezzenek, a sérülékenységek kideríthetők legyenek, követhessük a session információkat, hanem az is kell, hogy meglegyen a tudás, hogy melyik rendszer hogyan működik és mely más rendszerektől függ.
- Használjunk olyan rendszereket, ahol az ismétlődő, emberi beavatkozást igénylő lépések automatizálhatók. Ehhez kell egy olyan felület, ahol a szakember minden szükséges adatot megkap a döntéshez, nem kell további rendszereket tanulmányoznia. Legyenek automatikus értesítések, riasztások, melyek gyorsítják a munkát, láthatóvá teszik a felelősöket.
- Tegyünk minden információt láthatóvá, de minden szereplő csak a számára fontos információkat kapja. Néhány munkatársnak elég csak a káros tevékenységek ismerete, néhányan priorizált feladatlistát kapjanak, de van akinek a teljes hálózati forgalom ismerete szükséges. Másoknak csak a compliance riportok szükségesek, megint másoknak csak havi szintű kimutatások.

3. ábra: "Big Data"koncepciójú infrastruktúra kialaktása

- Használjunk további intelligens megoldásokat, hogy igazán komplex szűréseket is tudjunk készíteni. Igy teljesíthető ki a security menedzsment, hiszen a modern technológiák itt segítenek megmutatni a káros tevékenységeket, itt lehetséges a szabályok mellett a profilok, threshold-ok, automatikus válaszlépések létrehozása. Valamint itt válik igazán pontossá a priorizálási módszer, hiszen egyre pontosabb találatok lesznek , köszönhetően a fejlettebb analizáló rendszereknek.
- Mindig hangoljuk a rendszereinket. Nem elég egyszer egy működő megoldást létrehozni, kell a folyamatos finomhangolás, hogy a változó igényeinket is tökéletesen lefedje. Ezt segítheti egy tanuló rendszer kiépítése, mely a felhasználó válaszlépéseit követve, folyamatosan fejlődjön.

Szükséges a rendszer folyamatos fejlesztése, hogy intellignes rendszereink képesek legyen blacklist, whitelist létrehozására, egyedi szabályok készítésére, gyors kimutatások létrehozására, a szociális hálón áramló információk követésére, de akár az IP alapú kommunikáció rögzítésére is.

A FEJLTETT INFRASTRUKTÚRÁK MEGKÖNNYÍTIK A TESTRESZABHATÓ, HATÉKONY TECHNIKÁK HASZNÁLATÁT

Első lépésben már az is rengeteg segíthet, ha egy skálázható, robosztus rendszert építünk, melyben minimalizálva vannak a false-positive események, hiszen már ez nagyban megkönnyíti a szakemberek munkáját:

- hatékonyabb munkavégzés, kevesebb incidens, nagyobb fókusz a felmerülő riasztásokon
- csökkenti a támadások észleléséig eltelt időt, ezáltal kevesebb esély van a tényleges adatvesztésre

RSA SECURITY MENEDZSMENT: AZ RSA STRATÉGIÁJA AZ ANALÍZISRE ÉS AZ INTELLIGNES MEGOLDÁSOKRA ÉPÜL

4. ábra. RSA Security menedzsment modulok

Az RSA Security menedzsment a következő modulokra épül:

- Comprehensive visibility - az RSA integrált megoldásaival bármilyen forrásból összegyűjthetőek a logok. Egyetlen konzolon minden releváns információ elérhető, valósidőben képesek vagyunk elemzések készítésére, de akár kimutatások is készíthetőek.
- Agile analytics - az RSA megoldásai analizáló eszközöket is adnak a kezünkbe, mellyel gyorsan felderíthetőek a támadások, visszakövethetőek, priorizálhatók a felmerült események a súlyuknak megfelelően.
- Actionable intelligence - az RSA kutatóközpontjának segítségével a támadások elleni védekezés lesz hatékonyabb, hiszen több millió eszközről gyűjtik, analizálják a logokat, így gyorsan tudnak reagálni akár a zero-day támadásokra is. Mindez természetesen integrálható az RSA új generációs megoldásaival, így egyre kevesebb emberi beavatkozásra van szükség.
- Optimized incident management - ha már felmerült egy esemény, mellyel foglalkozni kell az RSA teljes workflow-t ad a kezünkbe, hogy válaszlépéseket, felelősöket rendeljünk az adott eseményhez. Követhetjük egy ilyen incidens útját, visszakereshetőek az eddigi lépések. Ez a modul integrálható akár 3rd party megoldásokkal is, a rendszerek képesek az információ megosztására.

KAPCSOLAT

Amennyiben további információra van szüksége, keresse bátran az RSA magyarországi disztribútorát:

rsa@arrowecs.hu

Vagy látogassa meg honlapunkat:

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