ArcSight Data Platform

Nyílt platform, amely értékes biztonsági felismerésekké alakítja a kaotikus adatokat

Főbb jellemzők

2016-ban a vállalatok 98%-át érte internetes támadás. A szervezetek évről-évre egyre több fenyegetéssel néznek szembe, az ennek nyomán becsült éves költség pedig eléri a 74 millió dollárt[1].

A modern biztonsági környezet működése a biztonsági adatokra épül. Az adatforrások és adatformátumok sokfélesége miatt azonban szinte lehetetlen olyan egységes adatarchitektúrát kiépíteni, amely minden igényt kielégít. Az egy év alatt létrehozott és lemásolt adatok mennyisége kétévente megduplázódik, és 2020-ra el fogja érni a 44 zettabájtot[2]. Az IoT, a fizikai környezet, az OT és az IT irányából érkező adatok volumenének és mozgási sebességének exponenciális növekedésével a biztonsági műveleti központ (Security Operations Center, SOC) egyre nehezebben tudja befogadni és feldolgozni a fenyegetések észleléséhez szükséges adattömeget. Az adathozzáférés és a kritikus rendszereknél megvalósítható csatlakozás korlátai jelentős késedelemhez és költségekhez vezetnek. A helyzetet rontja, hogy a betöltetlen internetbiztonsági állások száma 2015-ben egyedül az USA-ban elérte a 209 ezret, és 2010 és 2015 között 74%-kal nőtt az ilyen jellegű álláshirdetések száma[3].

Az SOC-nak alapjaiban kell átalakulnia ahhoz, hogy képes legyen alkalmazkodni a nagyobb adatvolumenhez, a gyorsan változó fenyegetési környezethez és a képzett biztonsági szakemberek hiányához.

A Micro Focus® ArcSight Data Platform (ADP) olyan jövőre felkészített adatkezelési megoldás, amely valós időben dolgozza fel az adatokat, és támogatja a nyílt szabványokat a fenyegetések pontosabb észlelése érdekében. Az ADP a gyűjtött adatokat valós időben kiegészítve, a gyakorlatban azonnal hasznosítható, rendszerezett információkat bocsát az elemzők rendelkezésére. Az Apache Kafka alapjaira épülő intelligens

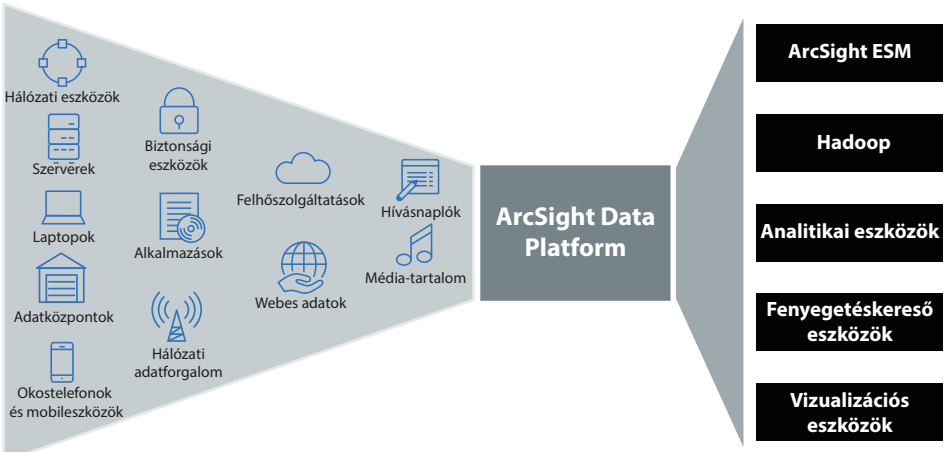
1 *Ponemon Institute – 2016, Az internetes bűnözés költségei és az üzleti innováció kockázata (Cost of Cyber Crime Study & the Risk of Business Innovation)*
2 *IDC – A lehetőségek digitális univerzuma: A „rich data" és az IoT növekvő értéke (The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things)*
3 *Az USA munkaügyi hivatalának statisztikai jelentése*

Fő képességek

- Az Apache Kafka technológiájára épülő Event Broker megoldás
- Az adatok valós idejű kiegészítése biztonsági kontextusba helyezi a nyers adatokat, és ezzel azonnal hasznosíthatóvá teszi őket
- 400+ „kulcsrakész" csatlakozó gyűjti az adatokat mindenféle adatforrásból
- A központi felügyeleti konzol teljes képet ad a biztonsági környezetről
- A „vendégadat"-funkció az összes IT-igény kiszolgálására alkalmassá teszi az Event Broker megoldást.

Főbb előnyök

- Az adatok láthatóságának kiterjesztése a támadások és a hírnévromlás kockázatának mérséklése érdekében
- A kockázat csökkentése a fenyegetések gyorsabb észlelésével és kezelésével
- A képzett biztonsági szakértők hatékony bevetése
- A meglévő beruházások hasznosítása az adatok Hadoop és analitikai eszközökkel történő feldolgozása révén
- A költségek és a komplexitás csökkentése az adatok kinyerésével és több helyszínre való terítésével



1. ábra: Adatok bárhonnan bárhova: nyílt architektúra

Event Broker megoldásnak köszönhetően az ArcSight Data Platform bárhol, bármilyen forrás adatait képes zökkenőmentesen fogadni és felhasználni.

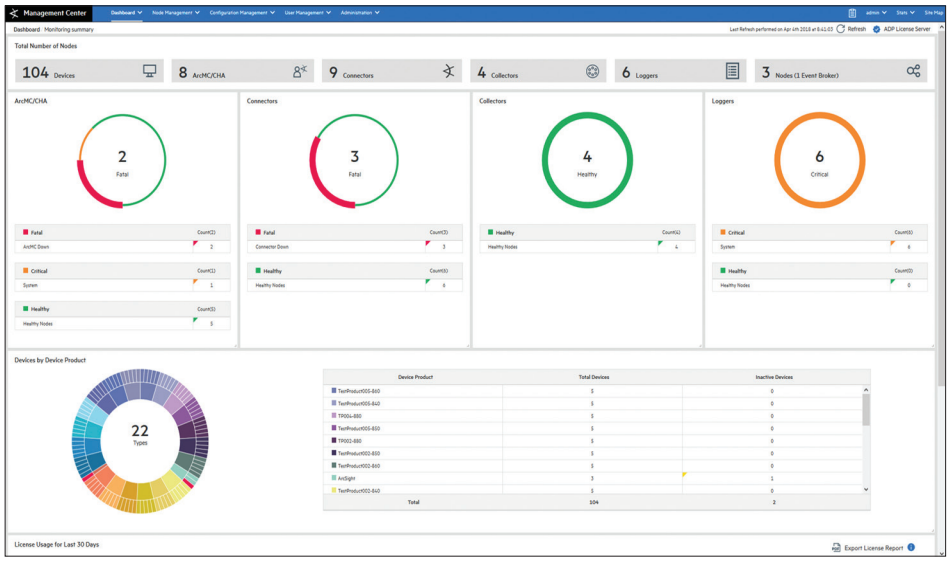
Jellemzők és előnyök

Az adatok sokféleségének és nagy mennyiségének hatékony kezelése

A több mint 400 kulcsrakész biztonságiadat-csatlakozóval és egyedi csatlakozókészítő eszközzel rendelkező ADP-vel bármilyen adatforrás adatai begyűjthetők. Az új adatforrások és a verzióváltások gyorsabban támogathatók a 4 hetente kiadott új szövegelemzőkkel (parser). Az Event Broker „Syslog Connector" megoldásával a nagyvállalatok egyszerűbben skálázhatják működésüket úgy, hogy közben a hálózati forgalmat is mérséklik. A szövegelemzők építését támogató tokenalapú eszköz javítja a konzisztenciát, és napokról órákra, illetve órákról percekre mérsékli az új csatlakozók létrehozásához szükséges időt. Az intelligens Event Broker akár 1 millió esemény/másodperc sebességgel is képes kinyerni, majd továbbítani az adatokat a célhelyekre.

Az egyre széttagoltabb adatforrások felügyelete nehéz feladat. Az ArcSight Management Center logikus elrendezésű vizuális megjelenítéssel és mérőszámokkal egyszerűsíti ezt a folyamatot. Az összes eszközről, csatlakozóról és célhelyről szolgáltatott, teljes körű kép elősegíti a problémák azonnali felismerését, és mérsékli a megoldásukhoz szükséges időt. A felügyeleti konzol minden korábbinál jobban megkönnyíti a SOC erőforrásainak kezelését, az Instant Connector Deployment funkció pedig időt takarít meg, és több száz node-esetében teszi lehetővé a műveletek egyidejű, egyszerű elvégzését.

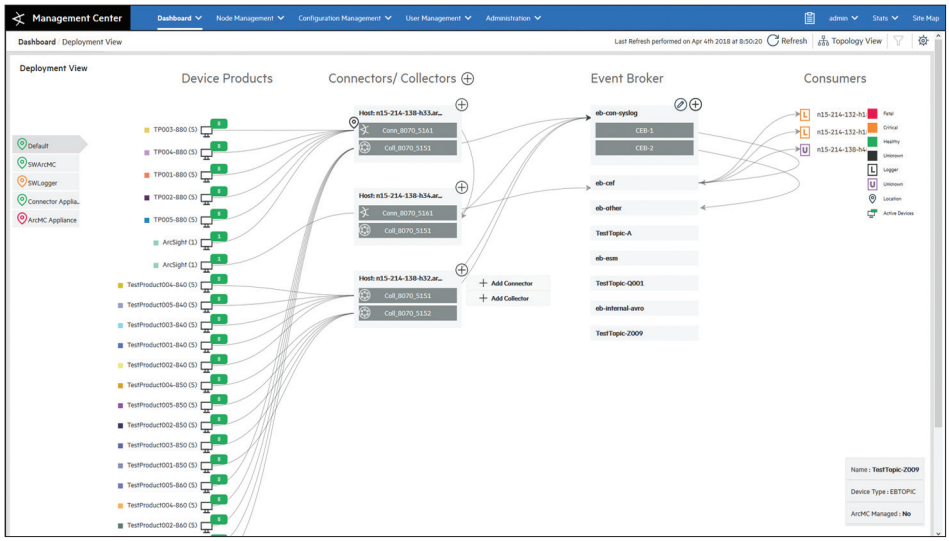
Az ArcSight Data Platform (ADP) egyszerűsíti a biztonsági központok működését, és a lefedettség bővítésével mérsékeli a támadások kockázatát. Optimalizálja a nagy volumenű, sokféle, gyorsan keletkező adat gyűjtését és kezelését.



2. ábra: Az ADP központi felügyeleti konzolja – műszerfalak

Értékes felismerések a valós idejű adatok révén

Az ArcSight Data Platform a gyűjtött adatokat valós időben kiegészítve, a gyakorlatban azonnal hasznosítható, rendszerezett információkat bocsát az elemzők rendelkezésére. Az ADP intelligens csatlakozói az ArcSight évek során felhalmozott biztonsági



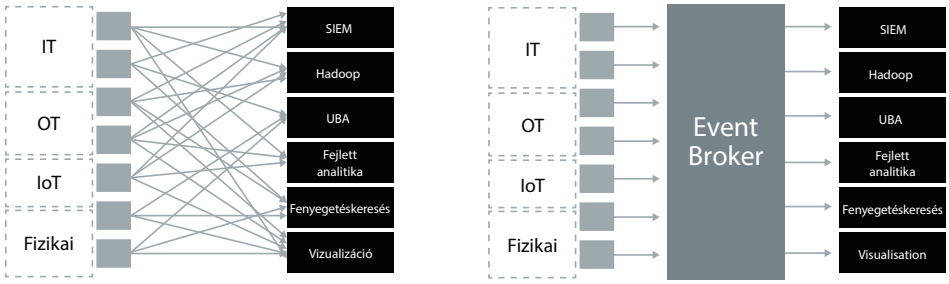
3. ábra: Az ADP központi felügyeleti konzolja – teljes körű monitorozás

szakértelmét bevetve normalizálják, kategorizálják és kiegészítik a beérkező adatokat. Az adatok így már strukturáltan és rendszerezetten érkeznek, ami gyorsabb és pontosabb vizsgálatot és eseménykorrelációt biztosít a fenyegetések észleléséhez.

A megfelelési követelmények teljesítése és az internetes támadók általi adatmanipulálás megelőzése érdekében gondoskodni kell az adatok megbízhatóságáról és sértetlenségéről. Az ADP titkosított és tömörített naplókat készít, megakadályozva az adatok lehallgatását, módosítását és törlését. Minden mozgásban lévő adatot a TLS titkosítási protokoll véd.

Nyílt architektúra

Mivel egyre több az adatforrás, és egyre nagyobb adattömeget kell több célhelyre mozgatni a valós idejű analitikához és az archiváláshoz, az N:1 architektúrák gátolják a növekedést és nem szolgálják ki a biztonsági üzemeltetés szükségleteit. Az ArcSight Data Platform részeként működő Apache Kafka-alapú Event Broker megoldás N:M architektúrája az összes forrás adatait fogadja és több célhelyre is képes továbbítani őket. Így a szervezet a biztonsági környezetét megnyitva, a gyűjtött adatokat a meglévő adattavakban, a különböző analitikai eszközökben és más technológiákban is hasznosíthatja. Ezáltal gyorsabban megtérül a beruházás, hiszen a rögzített adatok többféle módon



4. ábra: Az intelligens üzenetbusz architektúra

is felhasználhatók, és jövőbiztossá tehető a biztonsági központok működése.

A nyílt architektúra rugalmassága révén a vállalat szabadon eldöntheti, hogyan tárolja, keresi és elemzi az adatokat, és az igényeinek leginkább megfelelő megoldásokat és technológiákat használhatja.

A beruházás gyors megtérülését garantálja, hogy a megoldás az ADP Kafka-alapú Event Broker üzenetbuszával támogatja az IT-adatkezelést. Az ADP fejlett rendelkezésre állási képességeket is biztosít az Event Broker Kafka-replikációs képességeivel.

Összefoglalva tehát az ArcSight Data Platform (ADP) jövőre felkészített adatkezelési megoldás, amely a jobb fenyegetésészlelés érdekében valós időben kiegészíti az adatokat és a nyílt szabványokat is támogatja. A nyílt architektúrájú Event Broker megoldás lehetővé teszi az összes forrás adatait fogadó és több célhelyre továbbító N:M architektúra csatlakoztatását külső eszközökhöz. Így a szervezet a biztonsági környezetét megnyitva, a gyűjtött adatokat a meglévő adattavakban, a különböző analitikai eszközökben és más technológiákban is hasznosíthatja. Ezáltal a biztonsági központ, valamint az adattavak, az analitikai eszközök és a kapcsolódó technológiák működése egyaránt jövőbiztossá tehető és az ArcSight ADP segíti az ezen eszközökbe történő beruházások gyors megtérülését is. Az ADP együtt nő a vállalattal, és segít értelmezni az adatokat, hogy az így rendszerezett információk alapján az elemzők azonnal intézkedni tudjanak.

További információ:
www.microfocus.com/adp

Kapcsolatfelvétel:
www.microfocus.com

Tetszik, amit olvastál? Akkor oszd meg.