Adatlap
Biztonság

ArcSight Enterprise Security Manager

Elosztott valós idejű korreláció moduláris tartalomfejlesztési keretrendszerrel és esemény-osztályozással

A Micro Focus® ArcSight Enterprise Security Manager jelentős mértékben csökkenti az internetes fenyegetések észleléséhez, osztályozásához és a rájuk való reagáláshoz szükséges időt. Az ArcSight Enterprise Security Manager (ESM) fejlett, elosztott korrelációs motorjával segíti a biztonsági csapatokat a belső és külső fenyegetések észlelésében és az ezekre való gyors reagálásban. Ily módon órákról vagy napokról percekre csökken a reakcióidő, és a Security Operation Center (SOC) több fenyegetést kezelhet létszámbővítés nélkül az egyszerűsített SOC munkafolyamatok, valamint az ArcSight Marketplace webhelyen ingyenesen elérhető, folyamatosan frissített fenyegetéskezelő csomagok segítségével.

A termék áttekintése

Az ArcSight ESM egy nagy teljesítményű, skálázható és hatékony SIEM-megoldás

Az ArcSight Enterprise Security Manager átfogó, valós idejű fenyegetésészlelő és -elemző, munkafolyamat- és megfeleléskezelő platform, emelt szintű képességgel az adatok hozzáadott értékkel történő kiegészítésére. Az ArcSight valós időben észleli a kiberbiztonsági fenyegetéseket, mozgósítja az elemzőket, és segít az operatív biztonsági csapatoknak gyorsan reagálni a támadásokra. A fenyegetések automatikus azonosítása és rangsorolása révén a csapatok elkerülhetik az álpozitív riasztások miatt felmerülő költségeket, komplexitást és pluszmunkát. Az ESM lehetővé teszi a SecOps szervezeteknek, hogy központosított és részletes képet kapjanak több környezetről, és ezáltal hatékony workflowkat és észszerűsített folyamatokat alakítsanak ki. A továbbfejlesztett észlelésnek, valós idejű korrelációnak és workflow-automatizációnak köszönhetően a SOC-csapatok gyorsan és pontosan oldhatják meg a biztonsági incidenseket.

Az ArcSight nagy teljesítményű Smartconnector és Flexconnentor technológiáinak használata

A Micro Focus fejlett eseménygyűjtési képességeit hasznosító ESM több mint 500 különböző eszköztípus adatait elemzi és egészíti ki hozzáadott értékkel. Az ArcSight ADP SmartConnectorai minden gyakori eseményformátumot támogatnak (natív Windows események, API-k, tűzfalnaplók, syslogok, flat fájlok, Netflow, XML/JSON és közvetlen adatbázis-csatlakozás). Ezen túlmenően, FlexConnector fejlesztői keretrendszerünk használatával egyéni eseményelemző programok is készíthetők, küldhetők az ESM-hez indexálásra, valamint az iparágvezető elosztott korrelációs motorban történő felhasználásra. A több eseményforrás nagyvállalati szintű láthatóságot biztosít és lehetővé teszi, hogy a szervezet biztonsági igényeinek megfelelő, komplexebb használati forgatókönyveket dolgozzon ki.

Az ArcSight Connectorok által végzett kategorizálás és normalizálás univerzális formátumúra alakítja az összegyűjtött eredeti naplókat a SIEM-terméken belüli felhasználásra. A Micro Focus által kidolgozott CEF de facto ipari szabványt követjük – amelynek a kidolgozásához felhasznált több mint egy évtizedes tapasztalatot a Micro Focus 400-nál is több csatlakozó megépítése során halmozta fel 30 különböző biztonság- és hálózattechnológiai kategóriában. Az adatok kategorizálása és normalizálása segít gyorsan azonosítani az azonnali vizsgálatot vagy beavatkozást igénylő helyzeteket, és a figyelmet a legsürgősebb és legnagyobb kockázatú fenyegetésekre irányítja.

Valós idejű, intelligens, nagy teljesítményű, skálázható, testre szabható

- A piac legintelligensebb és legnagyobb teljesítményű korrelációs motorja, elosztott korreláció esetén 100 ezer EPS-ig skálázható
- Hozzáférés az ArcSight Activate fenyegetéskezelő keretrendszerhez és az ArcSight Marketplace tartalmakhoz a legfrissebb biztonsági korrelációs szabályok, irányítópultok, jelentések és használati forgatókönyvek eléréséhez
- A moduláris csomagok lehetővé teszik egyéni szabályok, irányítópultok és más tartalmak exportálását és megosztását több rendszer és ügyfél között
- A kevéssé hatékony SOC folyamatok kiiktatása az összes nagyvállalati biztonsági esemény kezelésének, elemzésének és jelentésének egységesítésével és központosításával
- MSP-/MSSP-kész megoldás, amely támogatja az elosztott biztonsági környezetek több-bérlős rendszereit.
- Az internetes fenyegetési intelligencia beépítésének lehetősége a STIX vagy CIF standard feedeken keresztül.

Intelligens és dinamikus eseménykockázat-értékelés és rangsorolás

Az ESM egyedi prioritási képlete (más néven fenyegetésiszint-képlete) tartalmazza az események értékelésének kritériumait, amelyek alapján a rendszer meghatározza relatív fontosságukat, illetve prioritásukat a hálózat szempontjából. A számítás sok adatpontot tartalmaz, pl. a meghatározott hálózati és eszközmodellt, a nyitott portok és a Nessusból vagy a Retinából importált sérülékenységvizsgálati elemzések eredményeit, a megfelelő sérülékenységi adatbázisokkal (X-Force, CVE és Bugtraq) párosítva. Kiderülhet például, hogy egy adott támadás a CVE-1999-0153 sérülékenységet használja ki. Ha a megcélzott rendszernél jelen van ez a sérülékenység, és az eszközön nyitva van a megtámadott port, akkor a rendszer feltételezi, hogy a támadás sikeres lesz, és magasabb prioritást rendel hozzá.

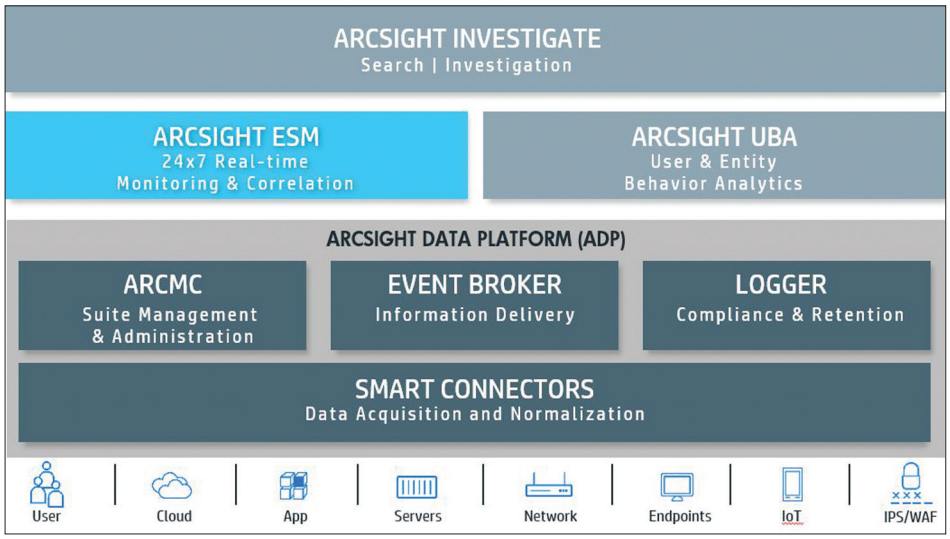
Főbb előnyök

Nagy teljesítményű, valós idejű korreláció

Az ArcSight ESM az események és a riasztások korrelálásával azonosítja a környezet magas prioritású fenyegetéseit. Az ESM nagy teljesítményű korrelációs motorja lehetővé teszi az adatok gyűjtését és az események valós idejű korrelálását a platform belső szabályait sértő fenyegetések pontos eszkalálásához. Az ESM akár 100 ezer vállalati biztonsági eseményt is képes korrelálni másodpercenként.

Kategorizálás és normalizálás

A kategorizálási és normalizálási funkció univerzális formátumúra alakítja az összegyűjtött eredeti naplókat a SIEM-terméken belüli felhasználásra. A Micro Focus által kidolgozott CEF de facto ipari szabványt követjük – amelynek a kidolgozásához felhasznált több mint egy évtizedes tapasztalatot a Micro Focus 400-nál is több csatlakozó megépítése során halmozta fel 30 különböző biztonság- és hálózattechnológiai kategóriában. Az adatok kategorizálása és normalizálása segít gyorsan azonosítani az azonnali vizsgálatot vagy beavatkozást igénylő helyzeteket, és a figyelmet a legsürgősebb és legnagyobb kockázatú fenyegetésekre irányítja.



1. ábra: Az ArcSight portfóliója

Nagy teljesítményű, moduláris tartalomfejlesztés

Miután létrejöttek az adott biztonsági forgatókönyvnek megfelelő egyéni tartalmak (szabályok, trendek, irányítópultok és jelentések), ezek a tartalmak könnyen becsomagolhatók és más rendszereken is telepíthetők, és más üzleti szervezetekkel vagy az ArcSight közösségen belül is megoszthatók. A többszintű ESM-architektúrákban több ESM állítható be úgy, hogy a tartalomkezelő rendszerek dinamikus szinkronizálása automatikusan megtörténjen. Az ArcSight Marketplace és Activate Framework csomagokat folyamatosan új biztonsági használati forgatókönyvekkel, szabályokkal és támogatott termékekkel frissítjük, hogy a szervezeteket állandóan tájékoztassuk a releváns új veszélyekről, osztályozzuk a fenyegetéseket, és gyorsan felkészítsük a meglévő SIEM-megoldást a mielőbbi beruházásmegtérülés érdekében.

**Az ArcSight ContentBrain konfigurátorhoz nyújtott ingyenes hozzáférés révén az ügyfelek követhetik, milyen csomagok állnak tesztelés, előkészítés vagy ellenőrzés alatt.

Integráció az ArcSight Data Platform (ADP) Event Brokerrel

A tömeges adatfeldolgozás, a nyitottság és a sebesség terén a Big Data által támasztott kihívásokra reagáló ArcSight ESM tökéletes integrációban működik az ADP Event Brokerrel (ADP EB). Nyitottan, jól skálázható és intelligens módon fogadja és szolgáltatja az adatokat a modern Service Operation Center számára. Az ESM küldeni és fogadni is tud (kiadói és fogyasztói szerepkör) eseményeket az ADP EB nyílt architektúrájától, ami lehetővé teszi a külső alkalmazásokkal (pl. Hadoop), adattavakkal vagy akár saját fejlesztésű, házon belüli programokkal való adatmegosztást. Így az ArcSight ESM intelligens SIEM-megoldás központi szerepet játszhat minden nagyvállalati biztonsági és analitikai eszköz működésében, segítséget nyújtva a biztonsági fenyegetések proaktív enyhítéséhez és hatásuk gyors elhárításához.

ArcSight Investigate-integráció

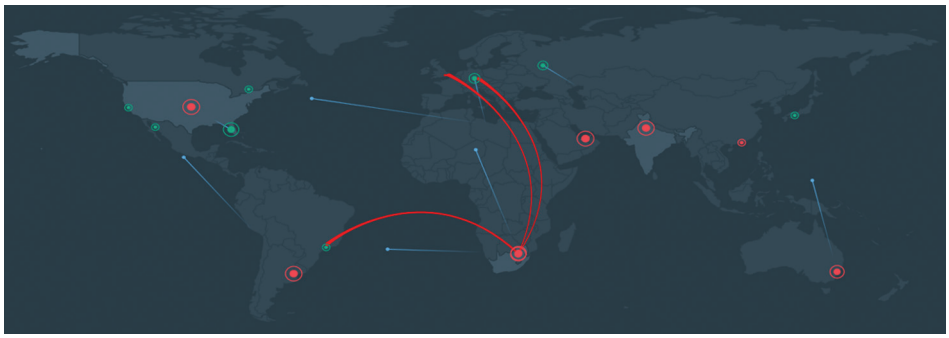
Az ArcSight ESM az ArcSight Investigate megoldással integrálva rendkívül gyors és egyszerű keresést, valamint adatvizualizációt tesz lehetővé az operatív biztonsági környezetben. A fejlett analitikai platformra épülő ArcSight Investigate következő generációs keresési és vizsgálati megoldás hatékonyan támogatja a biztonsági csapatok változó igényeit. Az ESM-et az ArcSight Investigate-tel kombinálva a SOC munkatársai intelligens nézet alapján észlelhetik és vizsgálhatják meg a nagyvállalati szervezet ismeretlen biztonsági fenyegetéseit, és gyorsan elháríthatják azok hatását vagy enyhíthetik a veszélyt még a tényleges probléma felmerülése előtt.

Workflow-automatizáció

Az ArcSight Enterprise Security Manager egyszerű módszert kínál a SOC-csapatok számára az észlelt riasztások valós idejű csatornákon, beépített esetkezelő rendszerrel történő hatékony és eredményes osztályozásához. A releváns események (Events of Interest) esethez csatolhatók és az alacsonyabb szintű válaszadóktól a magasabb szintűekhez eszkalálhatók. Az esetek változásai belső auditeseményeket hoznak létre, amelyek segítségével szorosan nyomon követhető az SLA-k és az elemzői válaszidőt mutató mérőszámok alakulása. A mérőszámok alapján a SOC-csapatok javíthatják az incidensekre adott átlagos válaszidejüket, és előbb eszkalálhatják őket megoldásra az illetékes személyhez. Az ArcSight külső hibajegykezelő rendszerekkel is integrálható.

Automatikus válasz a konzolon belül vagy szabályművelettel

A műveleti csatlakozók (CounterAct) lehetővé teszik az ArcSight integrációját külső eszközökkel. Így külső eszközök is vezérelhetők az ArcSight konzoljáról. Külső eszközökre vonatkozó parancsok végrehajthatók az ArcSighton belülről, és a parancsok eredménye visszaküldhető a konzolra az elemzők számára. A távoli parancs műveletként is végrehajtható a korrelációs szabályok motorjában vagy a csatlakozóra való jobb egérgombos kattintással. Ez a funkció költséghatékonyabb működést tesz lehetővé mert a felhasználóknak a továbbiakban nem kell váltaniuk a monitorok között, illetve az észlelés és a műveletek között az események megoldásához. Az, hogy nem kell elhagyniuk az ArcSight Console-t változtatások vagy műveletek végrehajtásához, rendkívül hasznos megoldás az ügyfeleknek, akik így integrálhatják a különböző alkalmazások parancsait. Az ESM központi hubként támogatja a műveletek meghatározását, kezelését és indítását, a naplóállományokban történő kereséseket, a külső alkalmazásokat és szkripteket.



Több-bérlős működés

Az ArcSight ESM-mel a különböző helyszíneken működő üzleti szervezetek egységes és egyszerűsített SecOps nézethez jutnak. A több-bérlős képességeknek, valamint az események szintjéig konfigurálható hozzáférésszabályozási engedélyeknek köszönhetően a nagyvállalatok központi felügyeleti képességeket vehetnek igénybe, például szabályalapú küszöbértékeket, egységes jogosultsági szerepköröket és felelősségi mátrixot. Szabályokat, jelentéseket és irányítópultokat szabhatnak testre és tehetnek hozzáférhetővé a célrendszerek üzemeltetői és az érintettek számára.

Főbb jellemzők

Opcionális ESM-csomagok

HIGH AVAILABILITY (MAGAS SZINTŰ RENDELKEZÉSRE ÁLLÁS – HA)

Teljesítményre optimalizált környezetet biztosít több ESM-rendszerrel és automatikus átállási (failover) képességekkel az elsődleges rendszer bármilyen kommunikációs vagy működési problémája esetén.

REPUTATION SECURITY MONITOR (REPSM+) – FENYEGETÉSI INTELLIGENCIA FEEDEK

Reagálás a fenyegetésekre a szabványos, felhőalapú megosztási platformtól kapott gyakorlatias fenyegetéselemzések és az elismert intelligencia alapján. A rendszer automatikusan fogadja és korrelációs eseményekhez használja fel az adatokat, keresve az egyezést az ismert problémákkal.

MEGFELELÉSI CSOMAGOK – MEGFELELÉS-AUTOMATIZÁCIÓ ÉS JELENTÉSKÉSZÍTÉS

Sokféle hatósági megfelelési követelmény egyszerű teljesítése, a kritikus problémák költséghatékonyabb és egyszerűbb azonosítása, kisebb kockázat, felkészülés az auditokra, megnövelt produktivitás és működési hatékonyság.

Egyéb jellemzők

- **Aktív listák**—Dinamikus memórialapú listák akár több millió tétellel, amelyek ellenőrző listaként működhetnek a gyanús forgalom vagy viselkedés észlelésére; az aktív listák bármilyen korrelációs szabályban felhasználhatók
- **Jelentések ütemezése**—és az eredmények automatikus továbbítása a főbb érintetteknek
- **API**—Az esemény- vagy esetadatok kinyerése az ESM-ből REST-alapú API segítségével
- **Trendek**—A releváns események egyszerű meghatározása és mentése oldaltáblákba a rendkívül gyors kereséshez és jelentéskészítéshez, akár hosszabb időszakra vonatkozóan vagy az eseménymegőrzési időablakon kívül.
- **Távoli csatlakozók konfigurálása**—A távoli csatlakozók konfigurációi az ArcSight Console.Aggregation, az Event Filtering, az Event Time Adjustments stb. funkciókból módosíthatók.

„Az ArcSight ESM kifinomult gyűjtési és korrelációs képességeivel olyan intelligens rendszerhez jutottunk, amely értelmet ad az általunk naponta generált több ezer eseménynek és naplórekordnak – így gyorsan azonosíthatjuk és kezelhetjük a fontos biztonsági incidenseket."

INFORMATION SECURITY MANAGER NETAPP

Kapcsolatfelvétel:
www.microfocus.com

Tetszik, amit olvastál? Akkor oszd meg.

- **Testre szabható képpel ellátott irányítópultok**—Az irányítópultok egyéni grafika (pl. térkép vagy szervezeti ábra) fölött jeleníthetők meg
- **Formátummegőrző titkosítás (FPE)**—A Micro Focus Voltage SecureData technológiája révén az ArcSight FPE-t használhat a korrelációs képességek megőrzéséhez anélkül, hogy kényes adatokat (pl. társadalombiztosítási azonosítószámokat vagy hitelkártyaszámokat) kellene megosztania az elemzőkkel vagy az ArcSight felhasználóival.
- **Adatbiztonság**—A letagadhatatlansági és adatintegritási követelmények teljesítése érdekében megváltoztathatatlan adattárolóval véd az adatok manipulálása ellen

További információ:
microfocus.com/arcsightesm

Ingyenes hozzáférés az ArcSight ContentBrain konfigurátorhoz, amellyel az ügyfelek követhetik, mely csomagok állnak tesztelés, előkészítés vagy ellenőrzés alatt: **https://arcsightcontentbrain.com