Security Information and Event Management

Neustále sa stupňujúce útoky, nedostatočne chránené údaje a systémy znamenajú hrozbu pre každú spoločnosť. Môže to byť strata dobrého mena a následné finančné škody, prípadne straty na výnosoch spôsobené výpadkom služieb alebo únikom citlivých informácií. Security Information and Event Management, skrátene SIEM, je integrovaný balík produktov na zber, správu a inteligentnú interpretáciu udalostí v IT infraštruktúre, ktorý pomáha pri odhaľovaní incidentov, ktoré môžu ohroziť podnikanie organizácií.

> Bezpečnosť, bez jej zodpovedajúceho monitorovania, je kybernetická forma autizmu. Systém môže byť dokonalý, ale uzavretý sám do seba.

SIEM na platforme – HP ArcSight Security Intelligence

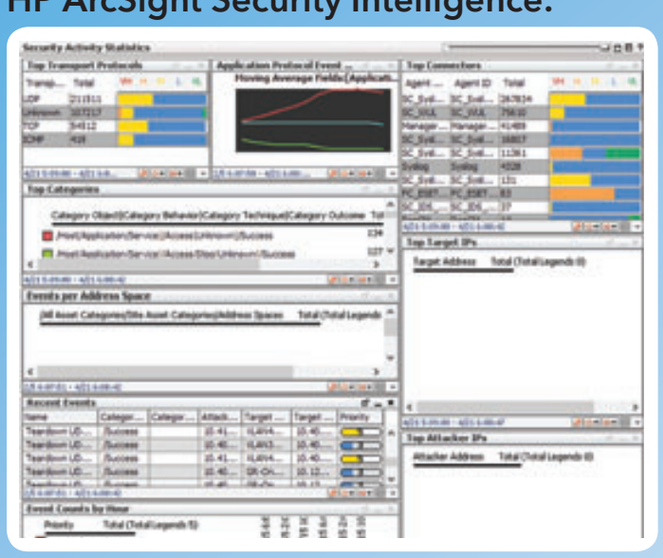
HP ArcSight Security Intelligence platforma napomáha ochraňovať organizáciu tým, že poskytuje kompletný prehľad o udalostiach v celej IT infraštruktúre:

- **vonkajšie hrozby ako malware a útoky hackerov;**
- **interné hrozby, ako narušenie dát a podvodov;**
- **riziká z aplikácie chýb a zmeny konfigurácie.**

ArcSight je lídrom na trhu SIEM riešení pre zber, analýzu a ohodnotenie bezpečnostných udalostí. Umožňuje rýchlu identifikáciu hrozieb, pomáha stanoviť priority a zjednodušuje reakciu na kybernetické útoky a hrozby aj z vnútra organizácie (insiders).

HP ArcSight Enterprise Security Manager (ESM) dokáže analyzovať a korelovať všetky (out-of-box v zmysle rozsahu podporovaných zariadení, resp. doplnením spracovania vytvorenými komponentmi) prihlásenia v podnikovej a sieťovej infraštruktúre, prístupy k súborom, databázové dotazy a všetky ostatné udalosti týkajúce sa monitorovania bezpečnosti IT infraštruktúry organizácie, od sledovania zhody (regulatory compliance) až po bezpečnostné vyšetrovania a následne prijaté opatrenia. ArcSight ESM monitoruje a prešetruje milióny bezpečnostných záznamov za účelom nájsť kritické udalosti, ktoré následne prezentuje vo forme dashboardov (monitorov, queryview-rov), reportov, upozorňuje na ne pomocou notifikácii - všetko v reálnom čase. Umožňuje presné prioritizovanie bezpečnostných rizík a porušení zhody (regulatory compliance). Po pridaní produktu HP Reputation Security Monitor je možné vyhodnocovať udalosti aj voči informáciám z reputáčnej databázy a následne tieto udalosti korelovať s bezpečnostnými udalosťami za účelom rýchlejšieho identifikovania hrozieb a sofistikovaných útokov.

Hlavné výhody riešenia - HP ArcSight Security Intelligence:



The Security Activity Statistics dashboard – jeden z klasických ESM dashboardov, ktorý cez široké spektrum monitorovaných systémov zobrazuje stav bezpečnosti vašej siete.

- **podpora hlásení rôznych platforiem a výrobcov**
- **automatizovaný zber a uchovávanie logov**
- **transformácia hlásení do jednotnej formy**
- **framework pre riešenie incidentov**
- **špecializované komponenty pre vizualizáciu a analýzu**
- **dizajn zameraný na zvládnutie veľkého množstva záznamov v reálnom čase**
- **prvky automatizujúce analýzu - napr. vizualizácia topológie, automatická korelácia pomocou dvoch korelačných nástrojov a pod.**
- **rozšírené reportovanie s možnosťou tvorby vlastných šablón**
- **vytváranie trendov pre urýchlenie tvorby reportov**
- **možnosť vytvárania a následného využitia rôznych zoznamov**
- **modelovanie IT infraštruktúry**
- **možnosť vytvárania vlastných agentov pre spracovanie hlásení z nepodporovaných typov zariadení**
- **pokročilá správa úložiska hlásení zameraná na bezpečný zber, efektívne uskladnenie a rýchly prístup k logom**
- **možnosť integrácie so scanerom zraniteľnosti, identity manažmentom**

Prínosy pre organizáciu

Implementáciou riešenia pre centrálne monitorovanie bezpečnosti získava zákazník prehľad o aktuálnej bezpečnostnej situácii v organizácii. Riešenie zároveň umožňuje efektívnejšie riadiť bezpečnostné riziká a zlepšiť možnosti vyšetrovania a prijatia následných opatrení pre identifikované bezpečnostné incidenty.

Hlavné prínosy:

- **redukovanie nákladov a čas potrebný na vyhodnocovanie bezpečnostných udalostí;**
- **zabezpečenie efektívneho monitorovania stavu bezpečnosti IS, takže napriek rastúcemu množstvu bezpečnostných incidentov nepotrebuje organizácia zvyšovať počet ľudí potrebných na ich sledovanie a analyzovanie;**
- **účinné odhaľovanie a predchádzanie neautorizovanému prístupu k informáciám, zníženie rizika bezpečnostného prieniku do systémov a tým ochrana značky, vzťahov so zákazníkmi a ochrana dobrého mena spoločnosti;**
- **pri audite alebo pri internom vyšetrovaní bezpečnostného incidentu umožňuje rýchlo**
- **a jednoducho nájsť požadované logy;**
- **jednoduché a rýchle zrekonštruovanie nepovoleného prieniku do systému a odhalenie príčin jeho vzniku. SIEM výrazne napomáha zastaviť útoky pred ich zintenzívnením, čím zmierňuje škody a šetrí finančné náklady;**
- **pomáha rýchlejšie vykonať obnovu systému a odstrániť škody;**
- **jednoduché zavádzanie zhody s legislatívnymi požiadavkami (compliance);**
- **vytváranie reportov relevantných pre rôzne typy používateľov v organizácii (operátor, analytik, manažér).**

LYNX vs. SIEM riešenia.

Firma LYNX má dlhoročné skúsenosti s implementáciou SIEM riešení od rôznych výrobcov u zákazníkov z rozličných odvetví (silový rezort, telko, bankovníctvo). Naši zákazníci SIEM realizujú monitorovanie bezpečnostnej situácie svojej infraštruktúry pomocou zberu a vyhodnocovania logov integráciou týchto typov zariadení:

- **sieťové a bezpečnostné komponenty v internej sieti a na perimetri,**
- **bezpečnostné komponenty umiestnené po ceste (aplikačné firewaly, IDS),**
- **scannery zraniteľnosti,**
- **operačné systémy,**
- **databázy,**
- **AAA systémy,**
- **bezpečnostné komponenty na hostoch a serveroch (AV, HIPS, ..),**
- **kritické aplikácie v organizácii (SAP, CRM, DWH, elektronické bankovníctvo,..).**

Neriešime len samotnú implementáciu SIEM nástrojov, ale poskytujeme komplexné riešenie monitorovania bezpečnosti, ktoré je prínosom pre organizáciu. Naša implementácia štandardne obsahuje analýzu prostredia, výber zariadení na monitorovanie, návrh logovacích štandardov v organizácii pre vybrané zariadenia, integráciu doplnkových zdrojov informácií uľahčujúcich vyšetrovanie, vytvorenie na mieru pripravených nástrojov, postupy pre analytikov a operátorov pri vyšetrovaní, post-implementačnú podporu, vrátane bezpečnostnej analýzy.

Špecializujeme sa na integráciu aplikácií a na vyšetrovanie so zameraním na detekciu insiderov. Pri integrácii nepodporovaných aplikácií využívame vlastný middleware, ktorý, umožňuje:

- **Samotný zber udalostí z aplikácie, prípadnú integráciu s identity manažmentom**
- **Automatickú koreláciu hlásení v aplikácii s hláseniami všetkých systémov pripojených do SIEM- ako napr. firewally, IPS, sieťová infraštruktúra, servery a pod.**
- **Definovanie požadovaného správania používateľov, vzorových rolí a oprávnení a následne automatickú kontrolu na odchýlky od predpísaných pravidiel v organizácii (compliance check) bez narušenia funkčnosti samotnej aplikácie**

LYNX®

www.lynx.sk

Košice
Gavlovičova 9
040 17
Tel.: 055/727 17 17
Fax: 055/728 85 55
lynx@lynx.sk

Bratislava
Jelačičova 8
821 08
Tel.: 02/501 065 11
Fax: 02/501 065 14
lynxba@lynx.sk