



HP ArcSight: soluzioni integrate per la Security Intelligence

Reportec

Sommario

Il business si trasforma	1
<i>Nuove esigenze di protezione.....</i>	<i>2</i>
La sicurezza enterprise di HP	2
HP ArcSight: la piattaforma di Security Intelligence	3
<i>HP ArcSight Enterprise Security Manager (ESM)</i>	<i>4</i>
<i>HP ArcSight Logger.....</i>	<i>5</i>
<i>HP ArcSight IdentityView.....</i>	<i>6</i>
<i>HP ArcSight ThreatDetector</i>	<i>7</i>
<i>HP ArcSight Express</i>	<i>7</i>
<i>HP ArcSight Application View</i>	<i>7</i>
<i>HP ArcSight Risk Insight.....</i>	<i>9</i>
<i>HP ArcSight Management Center.....</i>	<i>9</i>
<i>HP ArcSight Threat Response Manager.....</i>	<i>9</i>
<i>HP Reputation Security Monitor (RepSM).....</i>	<i>10</i>
Conclusioni	11



HP ArcSight: soluzioni integrate per la security Intelligence

*Dott. Riccardo Florio
Vice President Reportec*

La crescente diffusione di mobilità, cloud computing e social media sta ampliando i rischi a cui si trova esposto il patrimonio informativo aziendale e per far fronte in modo efficace a queste sfide, le aziende puntano sempre più verso una gestione della sicurezza e del rischio integrate.

Per poter affrontare le nuove esigenze di protezione, HP punta a predisporre una strategia complessiva che intervenga sia sul versante della protezione richiesta dalle aziende, sia per garantire agli utenti un accesso immediato e senza rischi alle corrette risorse aziendali, ponendo le basi per un approccio unificato alla sicurezza enterprise, in un contesto di integrazione che coinvolge servizi, applicazioni e prodotti.

All'interno della famiglia ArcSight HP ha raggruppato le soluzioni software indirizzate a proteggere i dati attraverso il monitoraggio, l'analisi e la correlazione di eventi di sicurezza provenienti da differenti tipologie di sorgenti.

Il business si trasforma

È in atto un processo di "business transformation" che sta ridefinendo completamente i processi aziendali, aumentando la produttività, cambiando le relazioni di lavoro e sviluppando attività completamente nuove.

Gli strumenti di social business o social collaboration ne sono un esempio. Un altro riguarda tutto il mondo delle App mobile che, oltre ad aprire le porte a servizi prima impensabili, sta portando alla nascita di aziende nuove dedicate a nuovi business, mentre il video ad alta definizione sta cambiando il modo di relazionarsi, riducendo gli spostamenti o permettendo servizi di nuovo tipo.

In questo scenario gli attacchi ai sistemi informatici diventano ogni giorno più frequenti e hanno mutato natura, ricadendo ormai completamente nella regia della criminalità organizzata orientata al profitto, arrivando a generare un mercato illegale stimato in oltre 100 miliardi di dollari. Nel contempo, le aziende globali spendono 5 miliardi di dollari all'anno per la compliance, mentre oltre la metà dei dipendenti utilizza i propri dispositivi mobile per accedere ad applicazioni aziendali business critical.

Nuove esigenze di protezione

In questo scenario di profonda trasformazione dell'IT il tema della sicurezza è sempre più pervasivo.

A livello di rete cresce l'impatto degli attacchi DDoS (Distributed Denial of Service) e si affacciano le APT (Advanced Persistent Threat) mentre i sistemi di difesa di tipo più tradizionale mostrano i propri limiti nel rilevare le nuove tipologie di intrusioni o nel contrastare la sofisticazione dei malware più recenti.

La mobilità rimuove gli ultimi limiti in termini di spazio e tempo aprendo enormi opportunità, ma porta con sé nuovi rischi legati alle caratteristiche dei dispositivi, alle componenti applicative e alle modalità d'utilizzo in cui scompare il confine tra personale e aziendale all'insegna del fenomeno noto come BYOD.

I rischi si espandono anche verso l'orizzonte applicativo influenzando i metodi di test dei processi di sviluppo e richiedendo modelli di protezione basati sull'analisi comportamentale anziché sulla mera classificazione del malware.

Un ulteriore aspetto distintivo del nuovo scenario della sicurezza è legato alla crescente diffusione dell'uso di risorse IT sotto forma di servizio o nel cloud, che estende, tra l'altro, le problematiche legate alla conformità normativa poiché

sposta i dati aziendali in un Web privo di confini nazionali.

Da tutto ciò emerge l'esigenza di predisporre una sicurezza dinamica e integrata basata su meccanismi automatizzati e strumenti costantemente aggiornati, in grado di analizzare la posta elettronica, le applicazioni, il traffico Web, i dati e i comportamenti di utenti e dispositivi.

La sicurezza enterprise di HP

Per rispondere alle nuove esigenze di protezione HP ha messo a punto una strategia per la gestione del rischio che prevede interventi sia sul versante della protezione richiesta dalle aziende, sia per garantire agli utenti un accesso sicuro alle corrette risorse aziendali, ponendo le basi per un approccio unificato alla sicurezza enterprise. L'approccio integrato alla sicurezza enterprise di HP risponde anche alle crescenti richieste di sicurezza dei nuovi ambienti virtualizzati e cloud.

Le soluzioni che compongono la piattaforma di sicurezza di HP sono proposte attraverso una divisione specifica denominata Enterprise Security Products (ESP) e comprendono i sistemi di nuova generazione HP TippingPoint per la prevenzione delle intrusioni

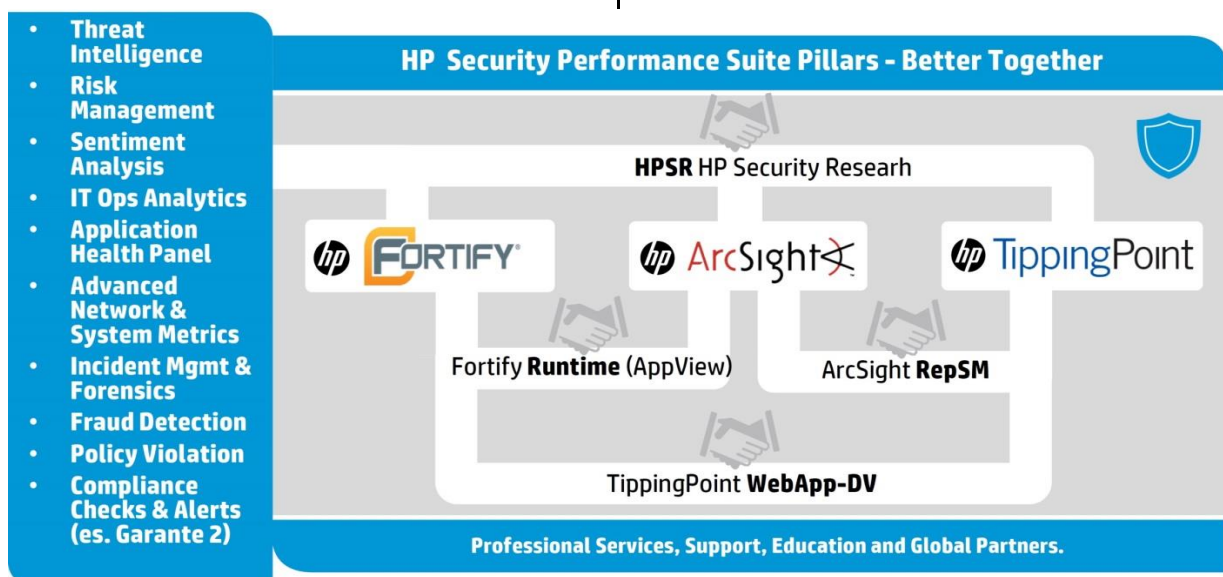
(NGIPS) e firewall (NGFW), le soluzioni di protezione dei dati ArcSight, la famiglia Fortify per la sicurezza dello sviluppo applicativo e Atalla per garantire transazioni sicure, in un contesto di integrazione che coinvolge servizi, applicazioni e prodotti.

Questa gamma di soluzioni segue un processo evolutivo che prevede sia la trasformazione e il miglioramento continuo di ciascuna tecnologia verticale, sia un'integrazione sempre più spinta delle diverse funzionalità al fine di sfruttare al massimo la sinergia di strumenti che affrontano su piani diversi il tema della protezione, migliorando la gestione e incrementando il livello di intelligenza necessario a fronteggiare le nuove minacce che operano in modo sempre più stratificato.

HP ArcSight: la piattaforma di Security Intelligence

HP ha raggruppato all'interno della famiglia ArcSight le soluzioni software indirizzate a proteggere i dati attraverso il monitoraggio, l'analisi e la correlazione di eventi di sicurezza provenienti da differenti tipologie di sorgenti.

Nel suo complesso ArcSight rappresenta una piattaforma integrata di Security Intelligence e Risk Management in grado di abbinare le funzionalità di un Sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM) con un approccio preventivo basato su un modello di analisi intelligente delle minacce, effettuato su scala globale attraverso una serie di servizi predisposti da HP.



Il SIEM rappresenta il centro di controllo dell'Intelligent Security di HP

La piattaforma HP ArcSight Security Intelligence fornisce visibilità sulle attività che interessano l'intera infrastruttura enterprise correlando log, ruoli dell'utente e flussi di rete per individuare eventi legati alla sicurezza in base ai quali definire priorità e predisporre risposte efficaci e preventive a minacce di vario tipo.

L'elemento centrale e abilitante di questa famiglia di soluzioni è il motore di analisi per la gestione di minacce e rischi HP ArcSight ESM.

HP ArcSight Enterprise Security Manager (ESM)

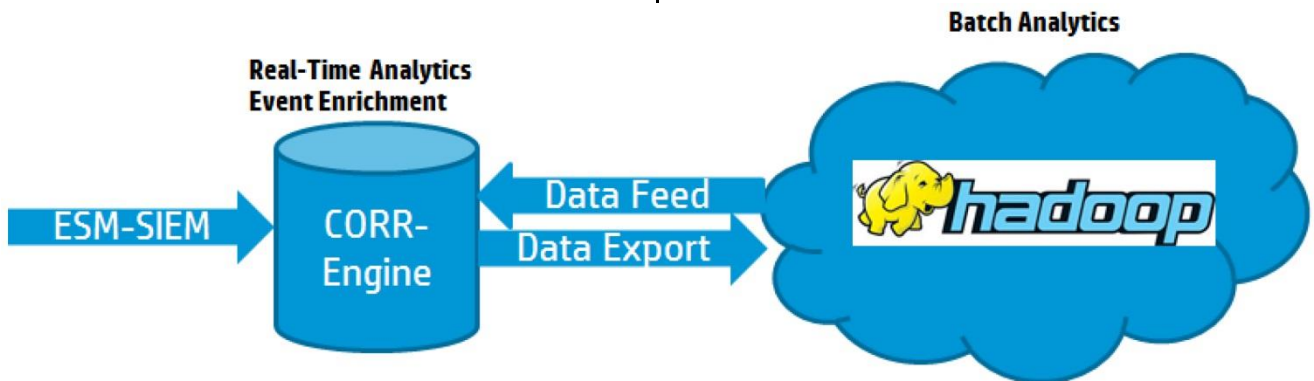
HP ArcSight ESM rappresenta l'elemento centrale e abilitante di questa famiglia di soluzioni. Si tratta di una soluzione SIEM per la raccolta, l'analisi e la correlazione delle informazioni di sicurezza e degli eventi di rischio, la protezione delle applicazioni e la difesa della rete e per il

Governance, Risk management and Compliance (GRC).

HP ArcSight ESM è in grado di effettuare analisi capaci di correlare:

- ❑ minacce esterne come malware e attacchi di hacker,
- ❑ minacce interne come le violazioni di dati e le frodi,
- ❑ rischi derivanti da flussi applicativi,
- ❑ modifiche della configurazione,
- ❑ problemi di conformità che scaturiscono dal mancato superamento dei controlli.

ArcSight ESM automatizza le operazioni di ricerca su Terabyte di dati, la produzione di report per la compliance e raccoglie dati di business intelligence. Il fulcro tecnologico di questa soluzione è costituito dalla quinta generazione (con prestazioni molto migliorate rispetto alla versione precedente) del motore di correlazione Correlation Optimized Retention and Retrieval

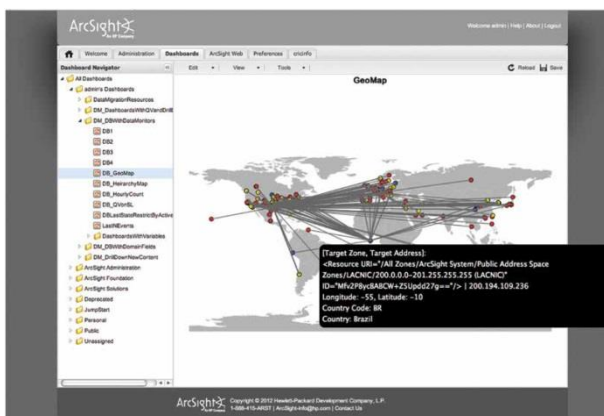


Integrazione tra ArcSight ESM e Hadoop Distributed File System (HDFS)

Engine (CORR-Engine) che permette di scalare nel livello di risposta, in funzione della minaccia che si trova a dover affrontare.

L'integrazione con il file system di Hadoop (HDFS - Hadoop Distributed File System) consente di sfruttare il CORR-Engine per effettuare funzioni avanzate di analytics in tempo reale oppure di inviare ad Hadoop, a un elevato "rate", i log normalizzati dal CORR-Engine per una lettura da HDFS (per esempio per operazioni di batch analytics).

ArcSight utilizza anche il motore HP Reputation Security Monitor che permette di analizzare in tempo reale gli indirizzi IP e i DNS potenzialmente dannosi, al fine di contrastare gli attacchi che sfruttano le vulnerabilità delle applicazioni Web.

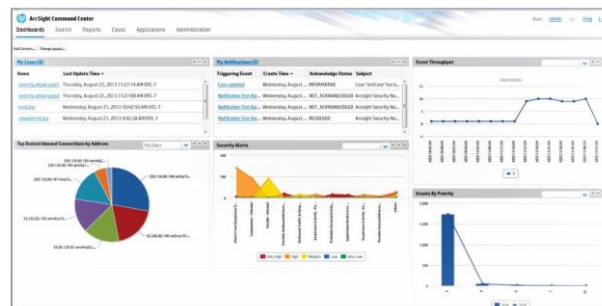


HP ArcSight ES M

L'interfaccia **HP ArcSight Command Center** riunisce funzionalità amministrative e di reportistica Web-based con funzioni di configurazione,

distribuzione, analisi dei log e gestione delle modifiche, attraverso un'impostazione basata su cruscotti altamente personalizzabili.

Anche le applicazioni di terze parti possono essere integrate direttamente all'interno del front end Web di HP ArcSight ES M.



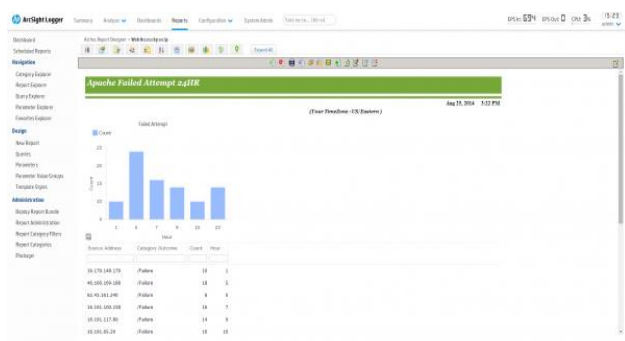
HP ArcSight Command Center

HP ArcSight Logger

All'interno della famiglia ArcSight questa soluzione abilita la raccolta di log provenienti da diversi dispositivi e in qualsiasi formato attraverso oltre 300 connettori. I dati raccolti vengono poi unificati attraverso la normalizzazione e la categorizzazione in un formato eventi comune (registrazione CEF) per poter effettuare ricerche, indicizzazione, generare report, analisi e favorirne la conservazione.

È possibile, in tal modo, migliorare le operazioni IT, dalla conformità alla gestione dei rischi, fino all'intelligence di protezione contro le minacce interne e quelle avanzate e persistenti (APT).

La release 6.0 della soluzione si caratterizza per la maggiore scalabilità che permette di gestire volumi di dati otto volte maggiori rispetto alla precedente versione con un incremento di prestazioni fino dieci volte superiori.



HP ArcSight Logger 6.0

Queste caratteristiche si rendono necessarie per affrontare le sfide imposte dall'analisi di un volume crescente di dati e favoriscono le operazioni di monitoraggio continuo e le funzioni di investigazione contestuale forense ad alta velocità.

Le funzionalità di HP ArcSight Logger 6.0 includono:

- la disponibilità di una app Mobile per attività di monitoraggio continuo anche in mobilità
- una nuova interfaccia Web 2.0 che migliora l'esperienza utente
- possibilità di effettuare raccolta e memorizzazione di log provenienti da oltre 350 fonti
- funzioni di compressione fino a 10:1

HP ArcSight IdentityView

HP ArcSight IdentityView è una soluzione software pensata per la protezione delle aziende enterprise da possibili minacce interne. Combina capacità di raccolta e analisi SIEM con le informazioni legate a utenti e ruoli relative ai diversi sistemi di accesso utilizzati.

Se l'attività di un utente sulla rete non corrisponde ai controlli di accesso consentiti o ai comportamenti tipici di un utente (valutati sulla base di dati storici correlati), la soluzione contrassegna il suo profilo perché venga sottoposto a indagini approfondite. Questo meccanismo aiuta il team di sicurezza a distinguere tra attività nocive intenzionali e involontarie. Il risultato è un meccanismo efficace per la mitigazione del rischio da minacce interne in tempo reale, che contribuisce a migliorare la governance degli accessi e che offre la possibilità di eseguire analisi forensi più rapidamente.

Questa soluzione, inoltre, arricchisce i log di sicurezza con informazioni sull'utente e il suo ruolo, fornendo un quadro completo delle attività anche per account ad alto rischio, privilegiati e condivisi.

Con il rilascio della versione 2.5 di ArcSight IdentityView, HP ha ampliato i meccanismi di correlazione dell'identità, dei ruoli e delle attività di sicurezza, incrementando di 10 volte il numero di utenti che una singola istanza è in grado di monitorare.

HP ArcSight ThreatDetector

È uno strumento pensato per gli analisti della protezione a cui fornisce gli strumenti necessari per distinguere un evento sospetto dai normali eventi che si verificano in rete.

ThreatDetector identifica il traffico normale e gli schemi di eventi sospetti attraverso un'analisi euristica effettuata sulla base dei dati storici e una serie di strumenti di visualizzazione e analisi del flusso dei dati.

Questo tool semplifica l'individuazione di worm "zero-day" e di attacchi complessi oltre a favorire il rilevamento degli errori di configurazione dei dispositivi di rete, dei sistemi e delle applicazioni. Fornisce, inoltre, supporto alla creazione di regole basate su modelli comportamentali.

HP ArcSight Express

HP ArcSight Express è una soluzione preconfigurata che viene integrata su un'appliance (disponibile in diverse configurazioni e modelli). Riunisce la piattaforma SIEM con la gestione dei log e il monitoraggio dell'attività degli utenti, integrando le funzionalità di IdentityView, Threat Detector e l'analisi del flusso di rete e utilizzo della banda.

In pratica, questa soluzione raccoglie i log da qualsiasi origine dati, consolida le informazioni per migliorare l'efficienza

dello storage e mette in correlazione gli eventi su più dimensioni, tra cui identità, vulnerabilità, analisi statistica e rilevamento di schemi per identificare le minacce avanzate prima che possano danneggiare i sistemi.

HP ArcSight Application View

Secondo gli analisti di mercato, oltre l'80% delle vulnerabilità totali sono riconducibili alle applicazioni. Un rischio cresciuto ulteriormente con la diffusione delle App: si pensi che il numero di App individuate dai vendor di soluzioni per la sicurezza IT come potenzialmente nocive per Android ha già superato l'impressionante numero di un milione.

Con il rilascio di ArcSight Application View HP mette a disposizione una soluzione per la visibilità sugli eventi di sicurezza delle applicazioni, combinando le funzionalità di Fortify e di ArcSight ESM.

HP ArcSight Application View è stato progettato in base al presupposto che, il posto migliore per individuare, comprendere e mitigare le minacce legate alle applicazioni, risieda nel software stesso.

Questa soluzione consente di controllare automaticamente le applicazioni per fornire un'analisi intelligente sulle minacce, combinando i log degli eventi di sicurezza generati dalle diverse

applicazioni, incluse quelle legacy o personalizzate che, in molti casi, non sono state progettate per fornire capacità di registrazione dei log.

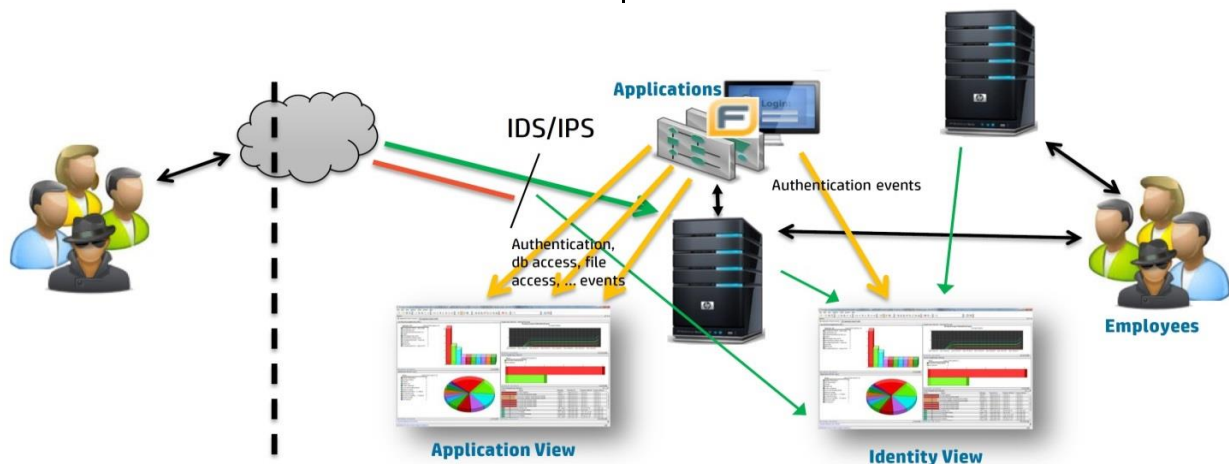
HP ArcSight Application View fornisce funzionalità di registrazione dei log senza la necessità di alcuna personalizzazione e mette i dati raccolti a disposizione di HP ArcSight ESM, integrandoli nei suoi dashboard e report.

Application View è basato su Fortify Real-Time Analyzer e rappresenta un agent a livello di Application Server, la

esempio, distingue tra l'accesso di un utente autorizzato a un'applicazione durante il normale orario di lavoro e il suo accesso ripetuto di Sabato a mezzanotte.

Rappresenta anche una soluzione complementare al software HP Identity View focalizzato sul monitoraggio dell'identità degli utenti a cui, di fatto, può mettere a disposizione ulteriori dati legati alla sicurezza.

Inoltre, consente di correlare le informazioni sugli eventi legati alle



L'azione complementare di ArcSight IdentityView e Application View

cui implementazione non richiede di effettuare modifiche alle applicazioni.

Questa soluzione fornisce una capacità di monitoraggio delle applicazioni (Java, .NET e Cold Fusion) sensibile al contesto e può essere utilizzata per contribuire a colmare le lacune di sicurezza legate alle modalità di accesso degli utenti o a un utilizzo improprio delle applicazioni: per

applicazioni con quelle associate ai sistemi IDS/IPS: per esempio gli attacchi intercettati dai sistemi IDS/IPS possono essere correlati a uno specifico login alla applicazione, per conseguire una migliore visibilità su ciò che l'attaccante sta cercando di ottenere.

Application View individua e rende disponibili ad ArcSight una serie molto

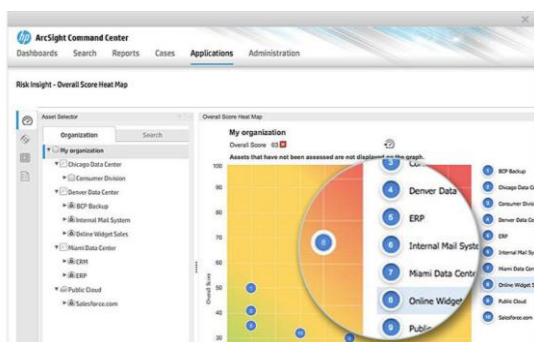
estesa di fenomeni di sicurezza tra cui citiamo, per esempio, errori nel controllo dell'autorizzazione, link interrotti, tentativi di forzare l'accesso in modalità "forza bruta", Denial of Service, modifiche ai privilegi dell'utente, navigazione nelle directory, buffer overflow, sicurezza dei cookie, violazioni della privacy, sottrazioni dei dati della carta di credito e attacchi spam.

HP ArcSight Risk Insight

HP ArcSight Risk Insight è una delle soluzioni software aggiunte più recentemente da HP al suo portafoglio d'offerta.

Abilita, tramite ArcSight ESM, funzioni di analisi del rischio e di impatto sul business, fornendo:

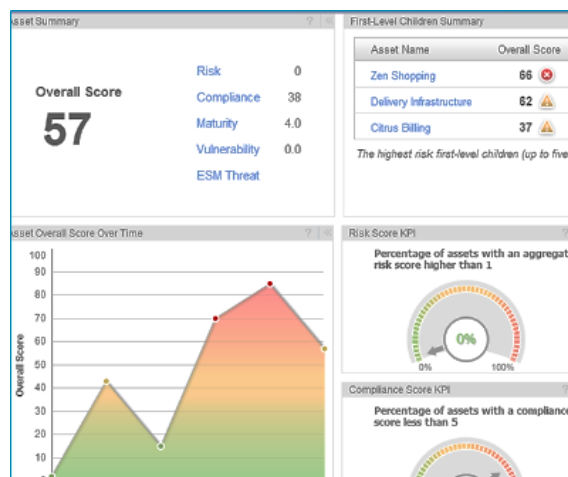
- ❑ una mappa del rischio dei servizi di business,
- ❑ una mappatura degli asset che estende il modello di ArcSight ESM,



Mappa degli asset in HP ArcSight Risk Insight

- ❑ funzioni per l'analisi di conformità dei processi di business.

- ❑ una serie di indicatori di rischio capaci di aggregare molteplici fonti,



Indicatori di rischio in ArcSight Risk Insight

HP ArcSight Management Center

HP ArcSight Management Center è la console di sicurezza unificata e centralizzata di HP che permette di configurare, distribuire e gestire l'analisi dei Log su deployment a larga scala e di fornire funzioni unificate di gestione delle modifiche.

HP ArcSight Threat Response Manager

HP ArcSight Threat Response Manager (TRM) mette a disposizione funzionalità cloud-ready per accelerare il rilevamento delle minacce e le azioni di risposta alle APT.

Rilasciato come un add-on cloud-ready per la piattaforma HP ArcSight di

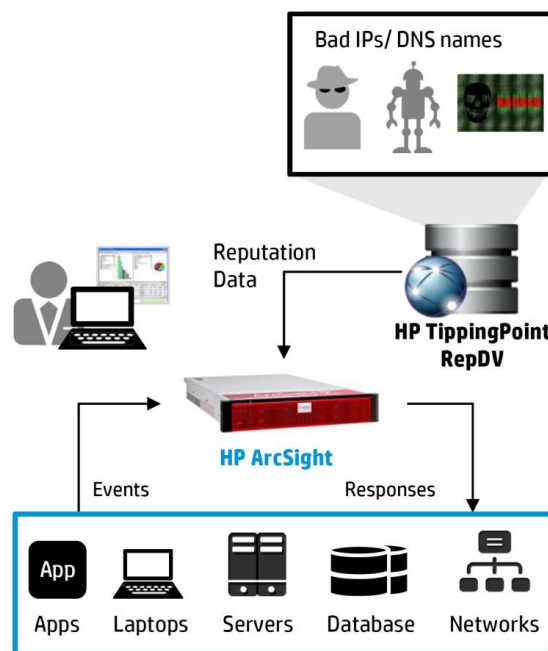
Security Information and Event Management (SIEM), ArcSight TRM è una soluzione end-to-end di sicurezza di rete e monitoraggio che accelera il rilevamento delle minacce e automatizza l'intero processo di risposta.

Questa soluzione consente di gestire e elaborare ad alta velocità le informazioni di sicurezza, analizzare i dati (strutturati e non strutturati), monitorare gli eventi e predisporre azioni automatiche una volta che una minaccia è stata rilevata. In caso di rilevamento, prima che il personale di sicurezza provveda a disattivare manualmente l'account, ArcSight TRM interviene per interrompere immediatamente l'accesso.

HP Reputation Security Monitor (RepSM)

Si tratta di uno strumento di Threat Intelligence basato su un livello di reputazione che viene definito sulla base di dati provenienti dalla comunità di sicurezza globale e di rilevazioni effettuate da HP.

RepSM fornisce un ulteriore livello di intelligenza al SIEM per operazioni di correlazione in tempo reale, abilitando una reazione attiva in risposta alle attività dannose e stabilendo il livello di priorità con cui fronteggiare attività sospette.



HP Reputation Security Monitor (RepSM)

In tal modo fornisce un utile sistema per identificare le APT, che risultano spesso non individuate dai controlli di sicurezza basati su signature e, più in generale, abilita operazioni di sicurezza in risposta ad attacchi sconosciuti con azioni manuali o automatiche.

L'utilizzo di RepSM abbinato ad ArcSight Application View permette di avere visibilità sul comportamento di un malintenzionato all'interno di un'applicazione e di controllare, per esempio, se effettua connessioni esterne e se queste sono verso un sito o un IP da considerare pericolosi.

Conclusioni

Attraverso un'offerta di soluzioni software ampia e diversificata, HP ESP mette a disposizione della aziende enterprise un insieme di componenti e strumenti adatto a rispondere alle esigenze di rilevamento delle minacce esterne e interne e a predisporre azioni di risposta che intervengono per proteggere dati, rete e applicazioni. I centri di ricerca e l'offerta di servizi distribuiti a livello globale mettono a disposizione delle aziende una "intelligence" di sicurezza globale e aggiornata in tempo quasi reale che contribuisce ad accelerare la risposta a minacce e predisporre azioni proattive nei confronti di nuove minacce come le APT.

L'offerta software HP ArcSight è in ampliamento e l'attività costante rivolta a incrementare il livello di integrazione tra le differenti famiglie di soluzioni software non potrà che contribuire a incrementare ulteriormente l'efficacia complessiva dell'approccio alla sicurezza proposto dal vendor.

REPORTEC opera dal 2002 nel settore dell'editoria specializzata sull'ICT professionale, realizzando e pubblicando riviste, report, survey, e-magazine, libri. Pubblica le riviste cartacee Direction, Solutions, Partners (edito dalla consociata Reportrade) e gli e-magazine Update Reportec, Security & Business, Cloud & Business, PartnersFlip. Ha siglato un accordo con **Tom's Hardware Italia** per la gestione dei tre canali B2B IT Pro, Manager e Resellers accessibili all'interno del dominio tomshw.it. Reportec è Media e Content Conference **Partner di IDC Italia**.



Dott. Riccardo Florio Da vent'anni opera nel settore dell'editoria specializzata professionale.

È coautore di rapporti, studi, Survey e libri nel settore dell'ICT. È laureato in Fisica ed è iscritto all'ordine dei giornalisti della Lombardia. È cofondatore e Vice President di Reportec, dove ricopre la carica di Direttore Responsabile della testata Direction e dell'e-magazine Update Reportec.



Reportec

H ArcSight: soluzioni integrate per la Security Intelligence

© Reportec S.r.l. - Ottobre 2014 - Tutti i diritti riservati

Reportec S.r.l. via Marco Aurelio, 8 - 20127 Milano

Tel: (+39) 02 36580441 Fax: (+39) 02 36580444

www.reportec.it - www.tomshw.it/index/itpro.html - www.tomshw.it/index/manager.html - www.tomshw.it/index/reseller.html

Tutti i marchi citati in questo documento sono registrati e di proprietà delle relative società.