

**Le soluzioni di
HP Enterprise Security Products
per la sicurezza applicativa**

Reportec

Sommario

Cybercrime e applicazioni	1
<i>Applicazioni e RASP</i>	<i>2</i>
La sicurezza enterprise di HP	3
HP Fortify: la sicurezza nello sviluppo.....	5
<i>HP Fortify Software Security Center</i>	<i>5</i>
<i>HP Fortify Static Code Analyzer</i>	<i>6</i>
<i>HP WebInspect.....</i>	<i>6</i>
<i>HP Fortify on Demand: la sicurezza come servizio cloud</i>	<i>7</i>
Analisi di sicurezza statica	7
Analisi di sicurezza dinamica	8
Analisi delle applicazioni mobile	8
Test delle applicazioni in produzione.....	8
<i>HP Fortify RunTime.....</i>	<i>9</i>
HP Application Defender	10
HP ArcSight Application View.....	11



Le soluzioni di HP Enterprise Security Products per la sicurezza applicativa

*Dott. Riccardo Florio
Vice President Reportec*

La diffusione di nuove tecnologie cloud e mobili ha notevolmente incrementato la richiesta di sviluppo di nuovi software contribuendo ad accelerare ulteriormente l'esigenza di fornire in tempi rapidissimi una risposta alle richieste espresse dai clienti. Tutto ciò sta mettendo alla prova la capacità di molte organizzazioni di effettuare test di sicurezza approfondita prima della distribuzione dell'applicazione e l'elevatissimo numero di vulnerabilità associato alle applicazioni ne è un'evidenza.

All'interno della propria visione complessiva per la protezione enterprise, HP fornisce una gamma di strumenti pensati per favorire uno sviluppo sicuro ed eliminare alla fonte le possibili vulnerabilità e per predisporre ambienti di test adatti a verificare le caratteristiche di sicurezza del software.

Cybercrime e applicazioni

Secondo il rapporto Clusit 2014, gli attacchi dovuti ad azioni di Cybercrime (furti o frodi, perlopiù) sono circa un quarto del totale. Il resto sono attacchi dei cosiddetti hactivist (sempre meno numerosi e sempre meno dannosi, perché crescono le protezioni contro il Distributed Denial of Service), azioni di sabotaggio e spionaggio.

Diversi sono i percorsi di attacco, ma molti di questi hanno un elemento in comune: le applicazioni, che sono poi il motivo per cui ci si collega a Internet e al Web o, se si preferisce, il motivo per cui si utilizzano dispositivi mobili e non. In ogni caso, il dato è comunque l'obiettivo finale nella stragrande maggioranza dei casi.

Per questo motivo le nuove tecniche per la prevenzione delle minacce informatiche si basano su analisi approfondite del codice in ingresso sulla rete aziendale. Non è una questione banale, perché in assoluto il traffico sta aumentando ed è destinato ad aumentare sempre di più. In particolare, proprio il traffico applicativo, con il progressivo atteso successo del Software as a Service o, più in generale, dei Web Service.

Da qui il successo e il crescente interesse verso i firewall e gli Intrusion Prevention System (IPS) di ultima generazione, che implementano soluzioni per l'analisi delle anomalie e per la simulazione del "comportamento" applicativo.

Perlopiù si tratta di soluzioni cosiddette di "sandboxing". Come nelle "scatole di sabbia" in cui giocano al sicuro i bambini nei parchi giochi, in queste sandbox è possibile depositare il codice e "giocarci" con tranquillità per verificarne le azioni e la sua pericolosità.

Tali analisi possono essere accelerate da servizi in cloud, che aggiornano prontamente tutti i dispositivi non appena una nuova minaccia viene identificata e, in qualche modo, resa immediatamente riconoscibile da tutti i sistemi.

Applicazioni e RASP

L'aspetto della rapidità non è indifferente, considerando che non si può pensare di bloccare tutto il traffico solo sulla base di un sospetto. Per questo i Web Application Firewall, devono aspettare i risultati delle analisi, ma quando lo ricevono potrebbe essere troppo tardi.

Un altro problema è rappresentato dalle più recenti tecniche impiegate dai cybercriminali nelle minacce APT

(Advanced Persistent Threat) utilizzate per attacchi mirati. In questi casi, il codice non viene prodotto per colpire un gran numero di computer, ma bersagli precisi, con più fasi. Una delle quali può essere l'annidamento di un codice nocivo non identificabile con l'analisi del comportamento. Questi malware, infatti, se vengono lanciati in esecuzione non compiono alcuna azione maligna. Ma, dopo un programmato lasso di tempo che può essere anche piuttosto lungo, attivano nuove funzioni che ne cambiano l'azione.

Non tutte le soluzioni sono in grado di rilevare queste minacce. Così come tecniche dette "evasive" possono confondere firewall e IPS. A questo si aggiunga il sempre attuale tema delle vulnerabilità e relative patch e si arriva a comprendere quanto complesso possa essere il fronte applicativo nella lotta al cybercrime.

È dunque a ragion veduta che gli analisti del Gartner, già nel 2012, avevano evidenziato l'importanza delle soluzioni per il collaudo delle applicazioni. Non solo un test statico, utile soprattutto prima del rilascio del software, ma anche un testing dinamico e, addirittura interattivo. Queste funzionalità si uniscono a quelle dei Web Application Firewall per costituire una nuova classe di soluzioni, chiamate RASP (Runtime

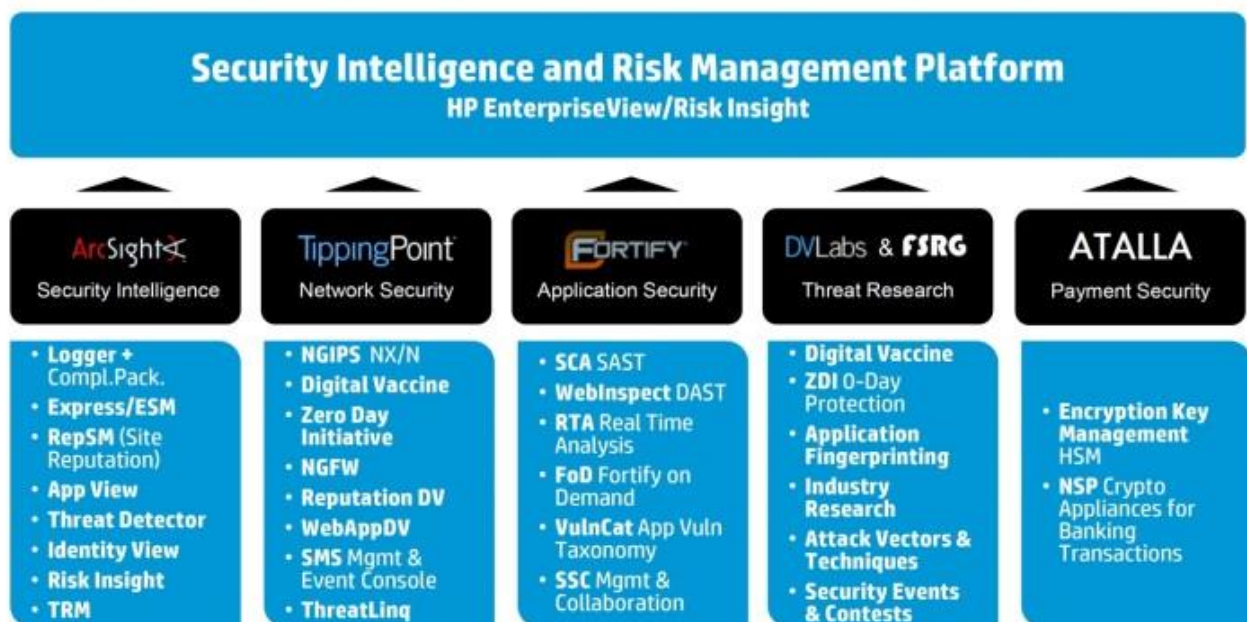
Application Self Protection), che si stanno rivelando fondamentali per una protezione in tempo reale delle applicazioni.

Di fatto, le applicazioni devono essere intrinsecamente sicure, a partire dal progetto e dalla fase di sviluppo. Questo non basta, però, perché solo in runtime è possibile verificare il funzionamento. Ricordiamo che l'applicazione è sviluppata per svolgere determinate funzioni e non è possibile immaginare tutti i possibili "abusi" di tali funzioni. Solo analisi durante la fase d'elaborazione, con i dati e le query reali, possono intercettare situazioni anomale. Proprio questo è l'ambito in cui operano le soluzioni RASP.

La sicurezza enterprise di HP

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.

Il linea con queste 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



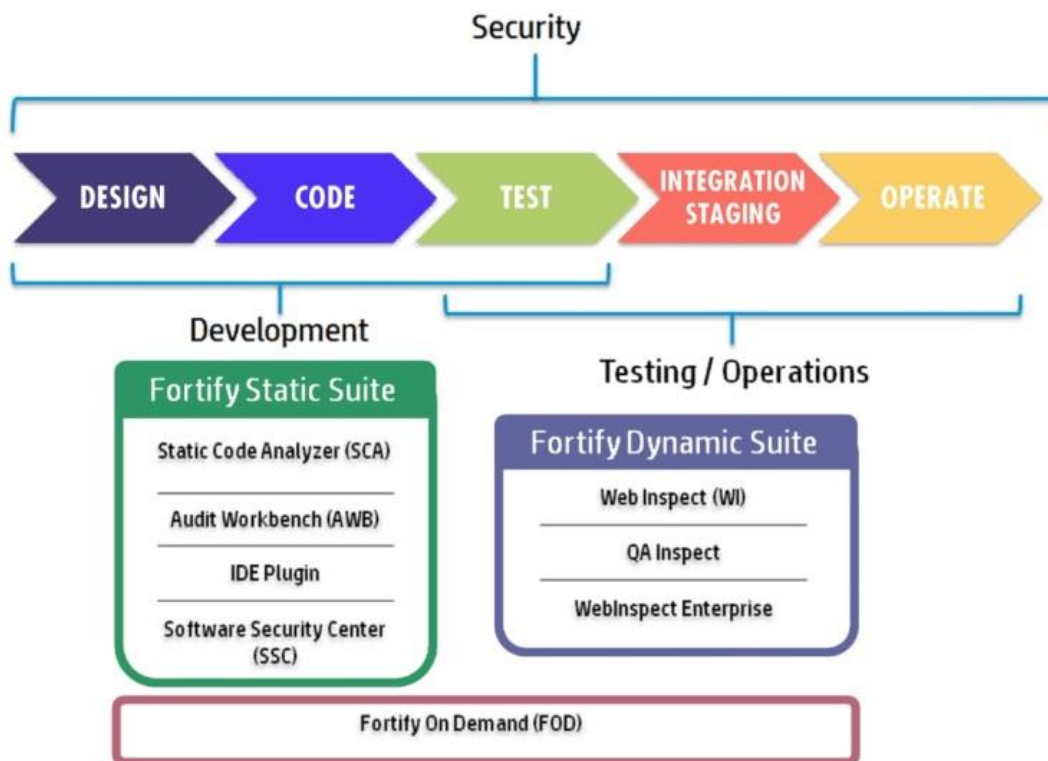
Le soluzioni che compongono la piattaforma di Security Intelligence e Risk Management di HP Enterprise Security Products

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 la cifratura dei dati e la gestione delle

chiavi, 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.



L'ambito d'intervento delle soluzioni HP Fortify

HP Fortify: la sicurezza nello sviluppo

All'interno dell'offerta Fortify, HP colloca la sua piattaforma di Security Intelligence and Risk Management adatta a effettuare test di sicurezza del codice di tipo statico, dinamico e in tempo reale.

HP Fortify predispone un approccio proattivo di Software Security Assurance per affrontare in modo sistematico il rischio di vulnerabilità nel software sulla base del principio che è più efficace e conveniente proteggere le applicazioni mentre sono in fase di sviluppo che farlo dopo che sono state rilasciate.

HP Fortify definisce quattro livelli di priorità per classificare la gravità delle vulnerabilità: critico, alto, medio e basso. I risultati delle valutazioni sono consegnati in un insieme di semplici grafici basati su un sistema coerente di valutazione a cinque stelle, che fornisce informazioni sulla probabilità che la vulnerabilità venga identificata e sfruttata da un outsider e sull'impatto in termini di danno potenziale che un malintenzionato potrebbe fare al patrimonio aziendale sotto forma di perdita finanziaria, violazione della conformità, perdita di reputazione del marchio, pubblicità negativa o altro.

HP Fortify Software Security Center

HP Fortify Software Security Center è una suite di soluzioni altamente integrate pensata per automatizzare e gestire la sicurezza applicativa e prevenire le vulnerabilità di sicurezza all'interno delle applicazioni.

La Suite HP Fortify Software Security Center automatizza e gestisce la sicurezza applicativa, mettendo le aziende in grado di testare la sicurezza delle applicazioni e di identificare le vulnerabilità, sia in modalità on-premises sia on-demand.

Questa suite svolge due attività fondamentali a supporto della gestione di sicurezza del software.

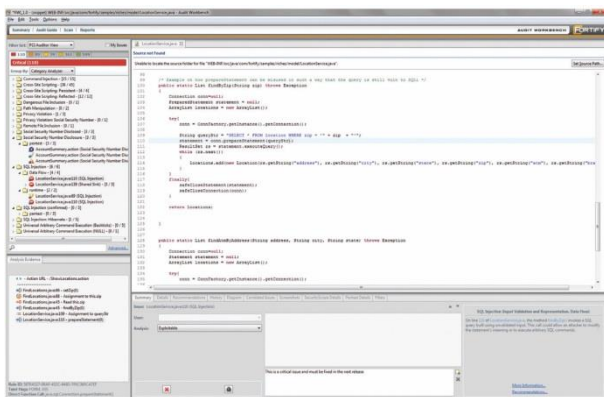
La prima è di mettere a disposizione funzioni di test di sicurezza per identificare le vulnerabilità lungo il ciclo di vita di un'applicazione, sia sviluppata internamente sia esternamente, attraverso tecnologie di test statico, dinamico e di analisi ibrida (statico-dinamica) in tempo reale.

La seconda attività riguarda l'analisi del ciclo di vita del processo di sviluppo attraverso funzioni di automazione di gestione, tracciamento, correzione e governance del rischio associato al software enterprise.

HP Fortify Static Code Analyzer

HP Fortify Static Code Analyzer (SCA) è la tecnologia sviluppata da HP per valutare il livello di sicurezza del software e rendere sicuro il codice legacy mentre questo viene sviluppato.

La soluzione proposta da HP utilizza diversi algoritmi e una base di conoscenza estesa di regole di codifica sicure per analizzare il codice sorgente di un'applicazione controllando ogni percorso che l'esecuzione e i dati possono seguire, per identificare ed eliminare le vulnerabilità che potrebbero essere sfruttate in applicazioni distribuite.



HP Fortify audit workbench

Fortify SCA ha la capacità di rilevare più di 500 tipi di vulnerabilità in 21 linguaggi di sviluppo e più di 700mila componenti a livello di API.

Per verificare che i problemi più gravi siano affrontati per primi, correla e

assegna una priorità ai risultati per fornire una classifica dei rischi e una guida dettagliata su come risolvere le vulnerabilità a livello di linea di codice.

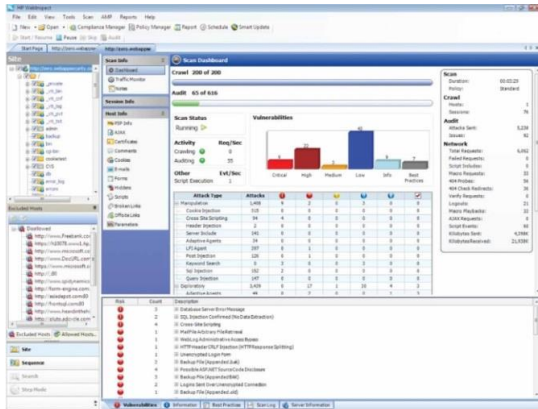
A partire dalla versione 4.0 HP Fortify SCA adotta un nuovo approccio basato sull'analisi di più thread di applicazioni software in parallelo, per migliorare le prestazioni di scansione e per velocizzare il rilevamento e la risoluzione delle vulnerabilità. In tal modo, è possibile effettuare test di sicurezza più frequenti, consentendo la scansione completa delle applicazioni senza impattare il processo di sviluppo.

Questo approccio consente di ottenere, secondo HP, anche una riduzione dei falsi positivi del 20% rispetto alle versioni precedenti del prodotto e mette a disposizione report di analisi della sicurezza software più dettagliati con classifiche di rischio per applicazioni mobili, Web, client e server.

HP Fortify SCA offre opzioni di implementazione flessibili con possibilità di accesso on-premises oppure on-demand.

HP WebInspect

HP WebInspect è uno strumento automatizzato e configurabile che effettua test dinamici sulla sicurezza delle applicazioni Web e test di penetrazione.



HP WebInspect

Imita le tecniche di hacking e gli attacchi, consentendo di analizzare a fondo le applicazioni e i servizi Web per individuare possibili vulnerabilità di sicurezza.

Consente di testare le applicazioni Web dallo sviluppo alla produzione, di gestire in modo efficiente i risultati dei test e favorisce la distribuzione di conoscenza sulla sicurezza all'interno dell'azienda.

HP Fortify on Demand: la sicurezza come servizio cloud

HP Fortify on Demand (FoD) è il servizio di tipo Software-as-a-Service di analisi del codice che consente alle aziende di testare la sicurezza del software in modo rapido e accurato. Fortify on Demand non richiede l'acquisto di alcun hardware né l'installazione di alcun software: è sufficiente caricare il codice e scegliere il tipo di test che si desidera effettuare per ottenere un report dettagliato.

HP FoD è disponibile per assessment sia statici sia dinamici e con diverse opzioni all'interno di ciascuna di queste categorie.

È possibile acquistare singole valutazioni o un abbonamento di un anno per valutazioni illimitate di una particolare applicazione. È possibile caricare i file e avviare una valutazione statica del codice oppure, se è stata acquistata una valutazione dinamica, è possibile verificare la URL. Questo servizio supporta Web, mobile e applicazioni thick-client, sia sviluppati internamente sia da terze parti.

Analisi di sicurezza statica

L'analisi statica di Fortify on Demand permette di valutare il livello di sicurezza del software e di rendere sicuro il codice legacy mentre questo viene sviluppato. L'utente carica il codice sorgente (byte o binario) di un'applicazione e riceve risultati recensiti manualmente solitamente in meno di 24 ore.

La soluzione proposta da HP utilizza diversi algoritmi e una base di conoscenza estesa di regole di codifica sicure per analizzare il codice sorgente di un'applicazione alla ricerca di vulnerabilità che potrebbero essere sfruttate in applicazioni distribuite.

Questa tecnica analizza ogni percorso che l'esecuzione e i dati possono seguire per identificare ed eliminare più di 500 categorie di vulnerabilità nel codice sorgente.

Analisi di sicurezza dinamica

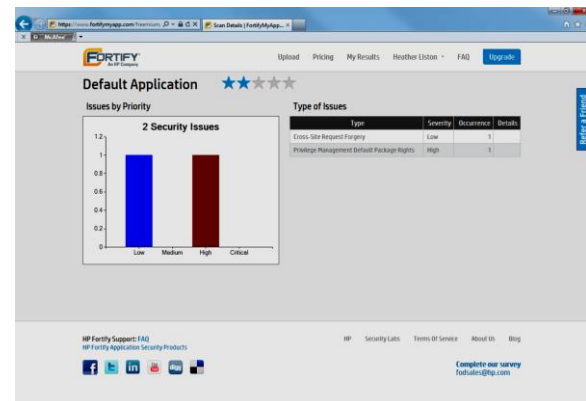
L'analisi di sicurezza di Fortify on Demand di tipo dinamico combina l'attività di test automatico con una metodologia di test manuale svolta da un gruppo di "application penetration tester" sull'applicazione Web. Questo tipo di test imita le tecniche di attacco dei cyber criminali, consentendo di analizzare a fondo le applicazioni e i servizi Web per individuare possibili vulnerabilità di sicurezza.

Analisi delle applicazioni mobile

L'approccio HP Fortify on Demand ai test delle applicazioni mobile prende in considerazione i tre livelli che costituiscono lo stack tecnologico: client, rete e server. Questo approccio fa in modo che le vulnerabilità presenti in un componente (il client, per esempio) possano essere utilizzate durante il test server per delineare un quadro più veritiero possibile del rischio legato all'applicazione mobile, in modo simile alla metodologia che potrebbe adottare un hacker. Il servizio prevede l'installazione iniziale di un'applicazione per poi eseguire un'analisi preliminare

sfruttando tutte le funzioni disponibili e permette di comprendere dove vengono richiesti i dati sensibili, come si spostano attraverso l'applicazione, come sono utilizzati e così via. Viene quindi costruito un diagramma di come questi componenti operano congiuntamente, che viene sfruttato per determinare la progressione della valutazione.

Il test viene eseguito sia su dispositivi mobili di prova sia utilizzando dispositivi simulati, a seconda del tipo di applicazione e delle sue funzionalità.



Fortify on Demand

Test delle applicazioni in produzione

Troppo frequentemente le applicazioni vengono rilasciate in produzione in modo frettoloso, con vulnerabilità non risolte. HP FoD risponde a questo problema fornendo un servizio per effettuare il test delle applicazioni Web in produzione senza causare interruzioni dell'attività. L'approccio seguito da HP parte dal presupposto che le applicazioni di produzione non dovrebbero essere

testate con lo stesso approccio aggressivo utilizzato nelle fasi di sviluppo (perché quando si è in produzione sono i dati reali che si espongono a un rischio). Per questo motivo Fortify on Demand offre quattro differenti opzioni metodologiche per la verifica delle applicazioni in produzione.

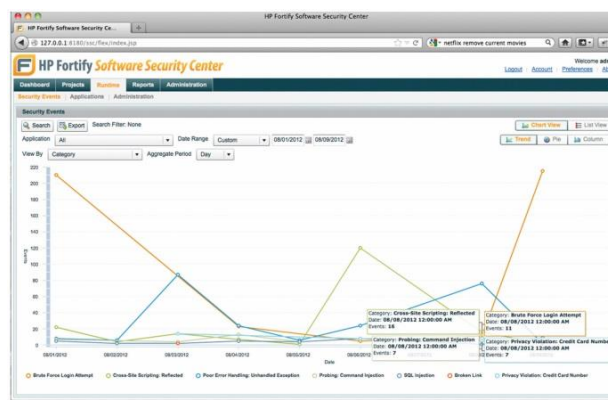
HP Fortify RunTime

Oltre alla suite di controllo della sicurezza delle applicazioni, HP Fortify è in grado di fornire anche una protezione attiva in tempo reale per le applicazioni Web con il componente Fortify RunTime (in precedenza RunTime Analyzer).

HP Fortify Runtime è integrato con HP Fortify Software Security Center per la gestione, con HP WebInspect per la convalida approfondita delle vulnerabilità e della protezione della sicurezza delle applicazioni al runtime (ovvero RASP) e con HP ArcSight ESM/Express via Application View per l'intelligence e la correlazione degli eventi di sicurezza.

Questo componente è un agent che si installa sui server che ospitano le applicazioni basate su Java o .Net e che, monitorando dall'interno l'esecuzione delle applicazioni stesse, è in grado di riconoscere quando le richieste fatte a quest'ultime siano lecite o possano contenere evidenze di un potenziale

comportamento illecito. Questo è possibile grazie alla particolare esecuzione dei due linguaggi fatta in ambienti virtuali (CLR per .Net e JVM per Java) che consente di vedere l'esecuzione dell'applicazione sequenzialmente: se a questo si aggiunge la capacità globale di HP Global Security Research di fornire l'intelligenza necessaria a distinguere quando nei processi di esecuzione dell'applicazione in atto qualche cosa disattende la normalità e manifesta una netta propensione al comportamento illecito, il potenziale della protezione esprimibile da questo connubio è evidente. Non esiste infatti un punto di osservazione più interno e più concreto di questo: dall'interno dell'applicazione poi è possibile non solo osservare ma anche bloccare questi comportamenti e generare allarmi che possono essere presi in carico da SIEM come HP ArcSight.



Visualizzazione dei trend in Fortify Runtime

HP Application Defender

Le tecniche di Runtime Application Self Protection (RASP) combinano funzionalità proprie dei Web Application Firewall con tecnologie per il test statico, dinamico e interattivo delle applicazioni.

HP ha introdotto questo tipo di tecnologia già da qualche tempo, per esempio nelle soluzioni HP WebInspect e HP ArcSight Application View. Soprattutto la tecnologia RASP chiamata HP Fortify RunTime è implementata come estensione di un debugger Java o di un profiler .NET, appunto a protezione delle applicazioni Java e .NET.

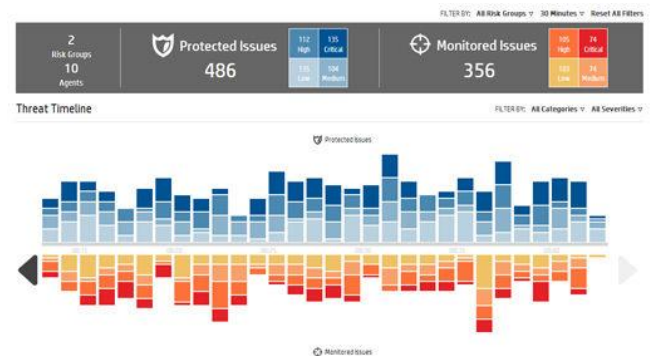
A queste si aggiungono altre funzioni inserite nei sistemi per il monitoraggio. L'esperienza maturata da HP in materia di tecnologie RASP è stata ulteriormente messa a frutto con il servizio per la protezione delle applicazioni in cloud denominato HP Application Defender.

Più precisamente, si tratta di un managed service per l'autoprotezione delle applicazioni, in risposta alla crescente pressione degli attacchi informatici ai servizi applicativi online.

Con l'aumentare del numero e della complessità delle applicazioni aziendali, la superficie esposta agli attacchi cresce considerevolmente e, come in precedenza osservato, i tradizionali metodi per proteggere le applicazioni

richiedono tempi lunghi, a cominciare dall'installazione delle patch, mentre le difese perimetrali sono una protezione indiretta.

Per questo, in HP hanno progettato un sistema di autoprotezione delle applicazioni, basato sull'analisi in tempo reale dell'esecuzione stessa del codice, monitorandone così l'attività per prevenire le aggressioni dall'interno dell'applicazione. Grazie al servizio di auto-protezione delle applicazioni, HP Application Defender consente alle aziende di identificare automaticamente le vulnerabilità del software e proteggersi in tempo reale.



Una dashboard di HP Application Defender: in blu le istanze protette, in rosso quelle monitorate

Dopo il processo di configurazione, la piattaforma cloud based consente ai professionisti della sicurezza d'individuare e bloccare le aggressioni senza cambiare codice o installare altri dispositivi sulla rete.

La soluzione permette di gestire e riportare i dati di sicurezza in tempo

reale, tramite dashboard interattive e alert che forniscono informazioni dettagliate sulla natura dell'attacco e sul punto in cui si è verificato. L'accuratezza è garantita dal fatto che HP Application Defender fornisce informazioni dall'interno dell'applicazione.

Questo aiuta gli sviluppatori a risolvere il problema in via permanente nel codice sorgente, mentre lo stesso viene risolto in maniera virtuale nell'ambiente di produzione.

HP ArcSight Application View

HP ArcSight Application View mette a disposizione una soluzione per la visibilità sugli eventi di sicurezza delle applicazioni, combinando le funzionalità delle soluzioni HP Fortify e della piattaforma integrata di Security Intelligence e Risk Management HP ArcSight ESM.

HP ArcSight è 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. Questa piattaforma fornisce visibilità sulle attività che interessano l'intera

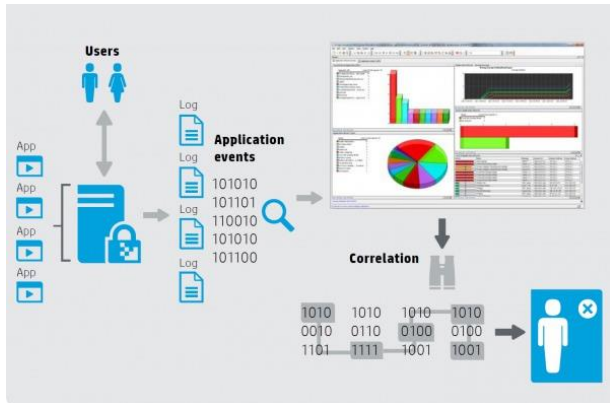
infrastruttura enterprise correlando log, ruoli dell'utente e flussi di rete per individuare eventi legati alla sicurezza in base ai quali definire priorità e predisporre risposte efficaci e preventive a minacce di vario tipo.

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.

HP ArcSight Application View 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 Runtime e rappresenta un agent a livello di Application Server, la cui implementazione non richiede di effettuare modifiche alle applicazioni.



HP ArcSight Application View

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 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.

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, attacchi spam.

HP ArcSight Application View rappresenta anche una soluzione complementare al software **HP ArcSight Identity View** focalizzato sul monitoraggio dell'identità degli utenti e pensato per proteggere le aziende enterprise da possibili minacce interne a cui, di fatto, può mettere a disposizione ulteriori dati legati alla sicurezza. Inoltre, consente di correlare le informazioni sugli eventi legati alle 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.



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*.

The logo for Reportec, featuring the word "Reportec" in a white, sans-serif font inside a dark blue rectangular box. The background of the entire page consists of diagonal stripes in shades of yellow and brown, with large, faint binary code (0s and 1s) overlaid.

Le soluzioni di HP ESP per la sicurezza applicativa
© 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.