Hewlett Packard Enterprise

Case study

# HPE Cyber Defense Center (CDC) salvaguarda le risorse ogni minuto di ogni giorno

## La più grande vetrina di tecnologie di sicurezza ed eccellenza operativa HPE

**Obiettivo**

Tutelare le risorse aziendali mondiali agendo, al tempo stesso, da modello di best practice operative per l'innovazione nel campo della sicurezza delle imprese.

**Approccio**

- Implementate i prodotti HPE ArcSight e integrate feed di dati provenienti dall'HPE TippingPoint Intrusion Prevention System (IPS) e da fonti di soggetti terzi.
- Analizzate fonti di big data per condurre funzionalità di analisi e allerte avanzate con HPE Vertica Analytics Platform.

**Argomenti IT**

- I prodotti ArcSight monitorano circa un miliardo di eventi al giorno, riducendone il flusso a un volume gestibile da un numero contenuto di analisti, un'attività che, se svolta manualmente, richiederebbe una schiera di oltre 30.000 analisti.
- Gli eventi sono correlati da circa 600 piattaforme TippingPoint IPS e dozzine di altre fonti, al fine di rilevare le minacce in modo proattivo. TippingPoint IPS rileva e blocca attivamente circa cinque milioni di attacchi al giorno.
- HPE Vertica Analytics Platform consente al CDC di correlare oltre due miliardi di dati registrati al giorno e consente al personale di effettuare interrogazioni in modo 50-1.000 volte più rapido rispetto a quanto possibile con i database tradizionali, utilizzando solo una frazione dell'hardware.

**Argomenti commerciali**

- I dati aziendali HPE sono protetti su scala globale per circa 250.000 dipendenti, con un personale di soli 22 professionisti della sicurezza.
- Il CDC funge da quadro per la sicurezza aziendale globale, al fine di mantenere le best practice di sicurezza HPE continuamente aggiornate e alla massima efficacia.
- Le innovazioni nelle pratiche di sicurezza CDC vengono trasferite nei prodotti e servizi di sicurezza HPE per mantenere i clienti in testa alle minacce informatiche.

Il HPE Cyber Defense Center (CDC) offre funzionalità di altissimo livello nei settori di operazioni, ingegneria, intelligence e gestione degli incidenti, per l'intera Hewlett Packard Enterprise (HPE). Il CDC ha implementato gran parte della famiglia di prodotti HPE ArcSight e dei feed di dati integrati da circa 600 piattaforme dei HPE TippingPoint Intrusion Prevention System ed effettua analisi complesse su enormi quantità di dati provenienti da Web e registri di sistema con HPE Vertica Analytics Platform, per analisi e allerte avanzate. Questo terreno di test sul campo non solo protegge l'infrastruttura IT globale di HPE, ma fornisce anche un quadro per aiutare i clienti HPE a rimanere in testa agli attacchi informatici e a condurre i propri affari in modo uniforme.

Dopo aver analizzato oltre 90 centri di operazioni di sicurezza dei clienti (SOC) in tutto il mondo e aver accumulato il maggiore set di dati nel suo genere, HPE ha preso le best practice di settore e gli insegnamenti appresi e li ha applicati al proprio Cyber Defense Center.

Il CDC dimostra non solo la capacità di HPE di ottenere una visione collettiva tridimensionale dell'intera impresa, ma funge anche da vetrina per l'innovazione in termini di sicurezza dell'impresa, tutelando una delle risorse più importanti dell'azienda: i dati.

Il CDC, inaugurato nell'autunno del 2013, sfrutta gli insegnamenti che HPE ha appreso dagli oltre 10 anni di implementazioni delle operazioni di sicurezza. È già uno degli SOC più grandi al mondo e tutela l'infrastruttura IT globale di HPE dagli attacchi informatici fornendo, al tempo stesso, un forum per mettere in evidenza le competenze di HPE in materia di sicurezza per clienti e partner. Ad esempio, protegge HPE da tipi di attacchi come Heartbleed e Shellshock, malware che potrebbero causare estreme vulnerabilità e intrusioni se non rilevati e corretti con patch.

In linea con la visione "HPE on HPE", secondo cui l'IT di HPE dovrebbe essere la vetrina più in vista dell'azienda, il team del CDC ha implementato la maggior parte dei prodotti all'interno della famiglia di prodotti HPE ArcSight e dei feed di dati integrati da circa 600 piattaforme dall'HPE TippingPoint Intrusion Prevention System implementate in tutto il mondo. Inoltre, HPE recupera registri dai server Web e altre fonti e conduce funzionalità di analisi e allerte avanzate con HPE Vertica Analytics Platform.

Questo terreno di test sul campo consente ad HPE di assicurare la propria infrastruttura IT e permette inoltre ad HPE di analizzare le minacce informatiche traducendo le informazioni in progressi futuri nei prodotti di sicurezza e nei servizi di consulenza HPE.

Rappresenta un importante traguardo nel campo dell'intelligence in materia di sicurezza su scala globale, dal momento che HPE conta attualmente:

- 20.000 dispositivi di rete
- 37.000 server
- 330.000 dipendenti
- 450.000 endpoint gestiti

## Correlazione di dati tra dozzine di piattaforme

La piattaforma TippingPoint IPS è implementata nelle sedi HPE di tutto il mondo e gestita a livello locale, con il CDC che funge da consumatore primario dei relativi eventi di prevenzione delle intrusioni. TippingPoint IPS fornisce protezione in linea e in tempo reale, grazie a una sicurezza proattiva della rete per il traffico di rete e i centri di dati HPE.

Le soluzioni ArcSight correlano a livello centrale i registri di TippingPoint e altre fonti, in modo che il CDC possa rilevare le minacce in modo proattivo. Tutte le piattaforme TippingPoint si affidano al servizio di abbonamento Vaccino digitale per le minacce HPE TippingPoint (HPE TippingPoint Threat Digital Vaccine, ThreatDV) che fornisce un pacchetto settimanale con filtro malware per aiutare le imprese a mettersi al sicuro dalle ultime minacce avanzate, intercettare e ostacolare le attività dei malware, tutelare dati sensibili e ottimizzare le prestazioni di rete.

Secondo Marcel Hoffmann, senior manager dell'HPE Cyber Defense Center: "In HPE, TippingPoint rileva e blocca attivamente circa cinque milioni di attacchi al giorno. Il nostro CDC gestisce il terzo impianto TippingPoint IPS per dimensioni al mondo e, quando rileva una minaccia seria, noi risaniamo il traffico e blocchiamo attivamente gli attacchi in questione".

Nonostante le dimensioni d'implementazione di TippingPoint, il CDC riceve un numero relativamente basso di allerte ad esso relative.

"Riceviamo elevati volumi di allerte dai firewall, ma molte di queste sono solo rumore di sfondo", spiega Hoffmann. "TippingPoint IPS fornisce un feed a basso volume e ad alta fedeltà di allerte fruibili su cui investighiamo attivamente".

Le piattaforme HPE ArcSight Enterprise Security Manager (ESM), HPE ArcSight Logger e HPE TippingPoint IPS lavorano insieme per creare un sistema di difesa informatica potente e completo. Ciascun elemento gioca un ruolo fondamentale nel garantire la sicurezza delle preziose risorse di informazioni HPE, che includono applicazioni aziendali, sistemi di informazioni dei clienti, risorse di proprietà intellettuale e tutte le risorse di informazioni cruciali disponibili sulla rete aziendale HPE.

TippingPoint IPS monitora e rileva le attività in rete, blocca le attività dannose a livello delle applicazioni e inserisce i dati relativi agli eventi in ArcSight ESM. ArcSight Logger classifica e archivia le informazioni relative agli eventi di TippingPoint e altre fonti.

ArcSight consente il monitoraggio dei registri di dozzine di piattaforme da una sola consolle ed effettua la correlazione avanzata di eventi da più fonti. Oltre a inglobare dati di registro dalle piattaforme TippingPoint IPS, ArcSight acquisisce anche i registri provenienti da firewall, Microsoft® Windows® Server Active Directory, HPE-UX, VMware, Microsoft.net e VPN, dispositivi e switch di rete, proxy Web, soluzioni open source e database. "Siamo in grado di catturare registri dalla maggior parte delle fonti utilizzando i connettori pronti all'uso di ArcSight e utilizziamo il framework HPE FlexConnector per costruire logiche di raccolta e contestualizzare i registri per tutte le altre", afferma Jorge Alzati, senior manager di ArcSight Engineering & Production Management.

> "Il CDC ha già rilevato e deviato migliaia di potenziali attacchi in meno di un anno. Il nostro programma di sicurezza informatica fornisce dati precisi di sicurezza, per aiutare i dirigenti a prendere decisioni basate sui fatti e aiutarci, al tempo stesso, a continuare a implementare una strategia di sicurezza predittiva".
>
> — Marcel Hoffmann, Senior Manager, Cyber Defense Center, Hewlett Packard Enterprise

ArcSight ESM filtra e correla i dati raccolti da TippingPoint IPS e altre fonti, offrendo agli analisti le informazioni solide e di alta qualità di cui hanno bisogno per effettuare analisi efficaci dell'intelligence di sicurezza. L'implementazione dei prodotti di sicurezza HPE ha seguito la metodologia di implementazione dei Servizi software professionali HPE (HPE Software Professional Services) e incorpora alta disponibilità, recupero a seguito di incidenti, tolleranza ai guasti e proprietà di bilanciamento dei carichi.

## Rilevamento e deviazione degli attacchi

Un'impresa delle dimensioni di HPE subisce attività di ricerca delle vulnerabilità e tentativi di sfruttamento delle vulnerabilità centinaia di volte al secondo. La soluzione HPE ArcSight elabora una media di un miliardo di eventi al giorno, riducendone il flusso a un volume gestibile da un numero contenuto di analisti attivi durante ciascun turno del CDC.

Tali analisti raffinano ulteriormente le allerte fino a 15-20 incidenti che vengono segnalati per azioni di follow-up e risanamento. Occorrerebbe una schiera di oltre 30.000 analisti per effettuare manualmente una funzione equivalente. Senza l'implementazione di ArcSight, tali analisi non verrebbero effettuate e quegli eventi non sarebbero esaminati, lasciando indisturbati gli attacchi in corso.

La soluzione ArcSight rileva modelli di attività, li correla e crea allerte sulla base delle regole dei casi d'uso. HPE gestisce un'enorme quantità di dati sensibili che devono essere tutelati, inclusi dati di sistemi, dipendenti e clienti.

ArcSight ESM offre al CDC un punto centralizzato per condurre tutte le attività di monitoraggio di sicurezza. Il CDC sfrutta ArcSight per rilevare le minacce in tempo reale, in modo che possano essere mitigate rapidamente, e utilizza ArcSight per raccogliere e correlare grandi quantità di dati di sicurezza, il che migliora enormemente la capacità degli analisti del CDC di individuare e contrastare le minacce reali.

"La soluzione ArcSight offre una visione unica del panorama delle minacce e ci aiuta a massimizzare le nostre risorse di sicurezza", afferma Hoffmann. "Il tempo e gli sforzi dei nostri analisti possono ora essere concentrati su eventi di sicurezza filtrati, indicanti minacce effettive, anziché sul filtraggio di enormi quantità di dati grezzi, provenienti da sistemi di monitoraggio separati".

L'analisi dei dati fornita da ArcSight supporta una mitigazione più rapida ed efficace e presenta un valido motivo di scelta da parte dei proprietari di risorse che hanno subito violazioni, il che è fondamentale per un risanamento veloce e valido. Quando viene rilevato un attacco, ArcSight aiuta gli analisti del CDC a documentare i fatti e a fornire le prove necessarie a coinvolgere in modo efficace i proprietari delle risorse e a ottenere il consenso all'acquisto di una soluzione.

I feed di dati sono correlati a livello centrale tra le unità aziendali e le aree geografiche, fornendo al CDC una visibilità unica sulle minacce informatiche.

"Le grandi imprese hanno bisogno della capacità di intercorrelare rapidamente i dati degli attacchi tra vari livelli, in modo da poter individuare in modo tempestivo le potenziali minacce che si verificano nell'intera società e che le unità o le regioni aziendali potrebbero non riconoscere", spiega Alzati.

Hoffmann aggiunge: "ArcSight offre un motore di correlazione altamente sofisticato e arricchisce i dati degli eventi, al fine di fornire analisi dei contenuti più rapide. Ciò consente ai nostri analisti di lavorare in modo più efficiente ed efficace e di intraprendere misure più rapide per la mitigazione delle minacce.

"Inoltre, ArcSight ci consente di rilevare le attività di ricognizione quando gli aggressori vanno in cerca di debolezze nei nostri sistemi, in modo da poter bloccare i potenziali attacchi prima che si verifichino".

Il CDC sfrutta costantemente le proprie esperienze, al fine di sviluppare casi d'uso per filtrare i feed di dati e affinare il processo di allerta. "È importante sviluppare casi d'uso in modo proattivo, per assicurarsi che il team del CDC riceva le giuste allerte automatizzate", afferma Alzati. "Il personale addetto alle operazioni revisiona i rapporti su base giornaliera, per garantire che siano implementati gli opportuni controlli e strumenti ma, una volta ottenuti i giusti casi d'uso, ArcSight funge da lastra di vetro unica, in grado di aiutare a interpretare tutte le informazioni di registro per comprendere lo stato della sicurezza dell'organizzazione".

La combinazione delle soluzioni ArcSight ESM e TippingPoint IPS aiuta gli analisti del CDC a rilevare e deviare migliaia di potenziali attacchi. Ad esempio, il CDC ha impedito proattivamente gli attacchi provenienti dall'exploit di Padding Oracle On Downgraded Legacy Encryption (Poodle).

Secondo Hoffmann: "Quando abbiamo sentito parlare per la prima volta della vulnerabilità Poodle, abbiamo scritto una regola dei casi d'uso in ArcSight per rilevare attività volte a cercare di sfruttare la vulnerabilità. Abbiamo inserito in una blacklist circa 250 indirizzi IP in base alle allerte di ArcSight derivanti dalla nuova regola, impedendo potenzialmente agli aggressori di sfruttare le vulnerabilità".

Poco dopo l'annuncio di Shellshock, in settembre 2014, TippingPoint ha informato gli analisti del CDC, mediante allerte visualizzate sui dashboard ArcSight ESM, del fatto che gli aggressori stavano scansionando i sistemi HPE in cerca di vulnerabilità. "ArcSight ci ha mostrato in tempo reale da dove provenivano le scansioni e qual era il loro obiettivo", afferma Hoffmann. "In un breve periodo di tempo, abbiamo potuto segnalare le vulnerabilità di HPE a Shellshock e promuovere la prioritizzazione delle patch di sistema per risanarle".

## Correlazione e analisi di big data

In partnership con HPE Labs, il CDC ha implementato dispositivi di registrazione dei server dei nomi di dominio (DNS) per raccogliere i registri di tutti e sei i cluster DNS interni che vengono poi inviati all'HPE Vertica Analytics Platform per funzionalità di analisi e allerte avanzate. HPE Vertica Analytics Platform gestisce enormi quantità di dati in modo rapido e affidabile, offrendo al CDC informazioni aziendali in tempo reale, per analisi avanzate dei big data.

**Case study**
HPE Cyber Defense Center

**Tecnologia**
di settore

## Sintesi di un cliente

**Soluzione di sicurezza HPE**

- HPE ArcSight Enterprise Security Manager
- HPE ArcSight Logger
- HPE TippingPoint Intrusion Prevention System
- Vaccino digitale per le minacce HPE TippingPoint
- HPE Vertica Analytics Platform

Con Vertica, il CDC è in grado di effettuare interrogazioni in modo 50-1.000 volte più rapido rispetto a quanto possibile con i database tradizionali, utilizzando solo una frazione dell'hardware. A differenza dei tradizionali database relazionali, progettati per l'elaborazione dei dati aziendali, Vertica è costruita dalle fondamenta specificamente per carichi di lavoro di analisi complessi ed è in grado di gestire con facilità la velocità e il volume dei dati raccolti in un SOC.

"Il CDC necessita di una piattaforma di analisi dei big data perché la tecnologia tradizionale non è in grado di tenere il passo con la velocità e le esigenze di accesso rapido ai dati necessarie per un'analisi tempestiva dei big data", afferma Lin Li, architetto aziendale di sicurezza informatica per HPE. "Ad esempio, il CDC analizza i file di registro provenienti da oltre 130 server Web interni. Con Vertica, possiamo archiviare e introdurre questi file come batch orari ed elaborarli in modo da consentire al CDC di condurre l'analisi".

I registri correlati di ArcSight vengono anch'essi inglobati in Vertica, permettendo al CDC di effettuare rapidamente analisi sofisticate dei big data, al fine di mitigare le minacce e impedire attacchi futuri. "Vertica consente al CDC di correlare oltre due miliardi di dati registrati al giorno, con file di registro provenienti da un'ampia varietà di formati", spiega Li. "Con Vertica, il CDC può normalizzare e ripulire i dati, nonché correlarli ad altri dati di riferimento. Ciò consente al CDC di comporre l'intero quadro, in modo che il team possa comprendere il traffico in arrivo nella rete globale HPE e mettere al sicuro le risorse aziendali in modo efficiente".

Li prosegue: "Dal momento che Vertica è di facile utilizzo e comprime i dati in modo ottimale, consente al CDC di archiviare i dati in modo conveniente e condurre analisi cronologiche di eventi passati. La maggior parte delle interrogazioni dettagliate su oltre 100 miliardi di dati di registro in Vertica vengono restituite entro un minuto. Ciò sarebbe stato impossibile con l'architettura precedente, dal momento che questo tipo di resa sarebbe semplicemente infattibile con un DBMS tradizionale di dimensioni paragonabili. Questo livello di analisi della cronologia consente al CDC di comprendere se gli utenti siano esposti a malware precedentemente sconosciuti e di attuare miglioramenti proattivi della sicurezza".

## Preparazione per il futuro

Il CDC rappresenta la prima di tre fasi della strategia di implementazione. La fase iniziale è stata incentrata sulla messa in sicurezza del perimetro, sfruttando le informazioni sulle minacce e riducendo la superficie di attacco. La fase 2 sarà incentrata sulla messa in sicurezza dell'applicazione, mentre la fase 3 su quella del business. La tabella di marcia del CDC prevede un'implementazione completa nell'intera impresa entro il 2017 e HPE continua a sviluppare best practice che possano essere sfruttate da altre grandi imprese.

"Bisogna iniziare in piccolo e non fare il passo più lungo della gamba", suggerisce Hoffmann. "È meglio implementare la sicurezza aziendale in fasi, soprattutto per le imprese di dimensioni molto grandi, con numerosi reparti. Prima dell'implementazione, individuate le risorse più cruciali, formate il vostro personale sui prodotti e sviluppate processi di risanamento maturi".

Il CDC sta inoltre programmando in termini di minacce della sicurezza emergenti, al fine di garantire di essere preparato a risolvere queste sfide future fin da oggi.

Con l'attenzione a un costante miglioramento, il CDC continua a evolversi fungendo, al tempo stesso, da terreno di test sul campo per i prodotti e i servizi HPE e da quadro per l'esecuzione di un SOC agile con personale relativamente contenuto di soli 22 professionisti della sicurezza.

Con la gestione di uno dei SOC di maggiori dimensioni al mondo, HPE sta imparando a ricavare ancora più valore da ogni dollaro speso per la sicurezza, in modo da poterlo trasferire ai clienti HPE.

Maggiori informazioni all'indirizzo
hpenterprisesecurity.com/

**Iscrivetevi per ricevere aggiornamenti**

★ Valutate questo documento

Hewlett Packard Enterprise

© Copyright 2015 Hewlett Packard Enterprise Development LP. Le informazioni contenute nel presente documento sono soggette a modifiche senza preavviso. Le uniche garanzie relative ai prodotti e i servizi Hewlett Packard Enterprise sono definite nelle esplicite dichiarazioni di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto qui dichiarato deve essere interpretato come garanzia aggiuntiva. Hewlett Packard Enterprise non è responsabile di errori tecnici o editoriali o di omissioni contenuti del presente documento.

Microsoft e Windows sono marchi registrati di Microsoft Corporation negli Stati Uniti.

4AA5-8767ITE, dicembre 2015, Rev. 1