Hewlett Packard Enterprise

HPE Cyber Defense Center protege los recursos globales cada minuto, cada día

La mayor exhibición de tecnologías para la seguridad y de excelencia operacional de HPE

Objetivo
Proteger los recursos de las empresas en todo el mundo y, al mismo tiempo, servir como modelo de las mejores prácticas operativas para la innovación en la seguridad de la empresa.

Enfoque
- Implementar los productos HPE ArcSight e integrar los sistemas de alimentación de datos de HPE TippingPoint Intrusion Prevention System y los recursos de otros fabricantes.
- Analizar grandes fuentes de datos para realizar procesos avanzados de análisis y alertas mediante HPE Vertica Analytics Platform.

La TI importa
- Los productos ArcSight supervisan unos mil millones de eventos al día, reduciendo el flujo de eventos a un volumen que puede ser gestionado por unos cuantos analistas —algo que requeriría un ejército de más de 30.000 analistas si se realizase manualmente.
- Los eventos tienen correlación con unas 600 plataformas de TippingPoint Intrusion Prevention System y decenas de recursos adicionales para detectar las amenazas con anticipación. La plataforma IPS TippingPoint detecta y bloquea unos cinco millones de ataques diarios.
- Gracias a HPE Vertica Analytics Platform, el Centro de Ciberdefensa puede correlacionar más de dos mil millones de registros diarios, y permite que el personal realice consultas entre 50 y 1000 veces más rápidas de lo que permiten las bases de datos tradicionales, usando una fracción del hardware.

Negocios
- Los datos empresariales de HPE de unos 250.000 empleados son protegidos a escala global con un personal de solo 22 profesionales de seguridad.
- Cyber Defense Center sirve como marco de la seguridad empresarial global para mantener las mejores prácticas actualizadas de forma continua y altamente eficientes.
- Las innovaciones en las prácticas de seguridad del CDC se trasladan a los productos y servicios de HPE para mantener a los clientes un paso por delante de las ciberamenazas.

HPE Cyber Defense Center ofrece capacidades de primera clase en operaciones, ingeniería, datos y gestión de incidentes para todo Hewlett Packard Enterprise (HPE). El CDC ha utilizado gran parte de la familia de productos HPE ArcSight y los sistemas de alimentación de datos integrados de unas 600 plataformas de HPE TippingPoint Intrusion Prevention System, y realiza complejos análisis de cantidades masivas de datos web y syslog con HPE Vertica Analytics Platform para ofrecer una capacidad avanzada de análisis y alertas. Este laboratorio de pruebas del mundo real no solo protege la infraestructura de IT global de HPE, sino que proporciona también un marco para ayudar a los clientes de HPE a permanecer pasos por delante de los ciberataques y a realizar sus negocios sin interrupciones.

Tras analizar más de 90 centros de operaciones de seguridad (COS) de clientes en todo el mundo y de acumular el mayor conjunto de datos de su clase, HPE ha utilizado las lecciones aprendidas y las mejores prácticas de la industria y las ha introducido en su propio Centro de Ciberdefensa.

El CDC no solo demuestra la capacidad de HPE para obtener una vista global en 3D de toda la empresa, sino que también sirve para mostrar la innovación en seguridad de la empresa, protegiendo uno de los activos más importantes de la compañía: los datos.

El CDC, que abrió en otoño de 2013, aprovecha las lecciones que HPE ha aprendido en más de 10 años de implementaciones de operaciones de seguridad. Ya es uno de los COS más grandes del mundo y protege la infraestructura de TI global de HPE de los ciberataques al tiempo que proporciona un foro para exhibir la experiencia de HPE en seguridad a los clientes y socios. Por ejemplo, ha protegido a HPE de ataques como los de Heartbleed y Shellshock, malwares que podrían haber provocado explotaciones y vulnerabilidades extremas en caso de no haberse detectado y aislado mediante parches.

En consonancia con la visión de «HPE on HPE» de que la tecnología de la información de HPE debe ser el escaparate principal de la compañía, el equipo de CDC ha utilizado la mayoría de productos de la familia HPE ArcSight y ha integrado sistemas de alimentación de datos de unas 600 plataformas de HPE TippingPoint Intrusion Prevention System en todo el mundo. HPE también reúne registros de servidores web y otras fuentes y realiza funciones avanzadas de análisis y alertas con HPE Vertica Analytics Platform.

Gracias a este laboratorio de pruebas del mundo real, HPE puede asegurar su propia infraestructura de TI y analizar también las ciberamenazas al tiempo que traduce sus conocimientos en avances futuros de productos de seguridad y servicios de consultoría HPE.

Representa un gran logro en cuanto a datos de seguridad a escala masiva, puesto que actualmente, HPE dispone de:

- 20.000 dispositivos de red
- 37.000 servidores
- 330.000 empleados
- 450.000 puntos de acceso gestionados

Correlación de datos con decenas de plataformas

La plataforma del IPS TippingPoint se utiliza en oficinas de HPE de todo el mundo y se gestiona a escala local, con el CDC como principal consumidor de sus eventos de prevención de intrusiones. El IPS TippingPoint ofrece protección en línea y en tiempo real proporcionando una seguridad de red proactiva para los centros de datos y el tráfico de red de HPE.

Las soluciones ArcSight correlacionan centralmente registros de TippingPoint y otros recursos para que el CDC pueda detectar amenazas con anticipación. Todas las plataformas de TippingPoint dependen del servicio de suscripción a vacunas digitales de protección frente a las amenazas (ThreatDV) de HPE TippingPoint, que ofrece un paquete semanal de filtros de malware para ayudar a las empresas a protegerse contra las últimas amenazas avanzadas, evitar e interrumpir la actividad del malware, proteger los datos sensibles y optimizar el rendimiento de la red.

Según Marcel Hoffmann, director senior del Centro de Ciberdefnsa de HPE, «en HPE, TippingPoint detecta y bloquea unos cinco millones de ataques diarios. Nuestro CDC dirige la tercera instalación de IPS TippingPoint más grande del mundo y cuando detecta una amenaza grave, saneamos el tráfico y bloqueamos esos ataques».

A pesar del tamaño de la implementación de TippingPoint, el CDC recibe relativamente pocas alertas de TippingPoint.

«Recibimos altos volúmenes de alertas de cortafuegos, pero muchas de ellas son ruido de fondo», explica Hoffmann. «El IPS TippingPoint proporciona un sistema de alimentación de bajo volumen y alta fidelidad de alertas que investigamos activamente».

Las plataformas HPE ArcSight Enterprise Security Manager (ESM), HPE ArcSight Logger y HPE TippingPoint IPS funcionan juntas para crear un sistema de ciberdefensa completo y poderoso. Cada elemento desempeña una función crítica en garantizar la seguridad de los valiosos activos de información de HPE, que incluye las aplicaciones de empresa, sistemas de información del cliente, activos de propiedad intelectual y todos los recursos de información crítica disponibles en la red empresarial de HPE.

El IPS TippingPoint supervisa y detecta la actividad en la red, bloquea la actividad maliciosa en la capa de la aplicación y alimenta datos de eventos al ArcSight ESM. ArcSight Logger clasifica y almacena la información de eventos de TippingPoint y otros recursos.

ArcSight permite supervisar registros de decenas de plataformas desde una sola consola y realiza una correlación avanzada de los eventos desde múltiples fuentes. Además de incorporar datos de registro de las plataformas IPS TippingPoint, ArcSight también incorpora registros de cortafuegos, Microsoft® Windows® Server Active Directory, HPE-UX, VMware, Microsoft.net y redes privadas virtuales, conmutadores y dispositivos de red, web proxys, soluciones de código abierto y bases de datos. «Podemos capturar registros de la mayoría de fuentes usando conectores listos para usar de ArcSight, y usamos la infraestructura de HPE FlexConnector para construir lógica de colección y contextualizar registros de las demás», dice Jorge Alzati, director senior de Dirección de Producción e Ingeniería de ArcSight.

«El CDC ya ha detectado y desviado miles de ataques potenciales en menos de un año. Nuestro programa de ciberseguridad proporciona datos de seguridad precisos que ayudan a los directivos a tomar decisiones basados en hechos y, al mismo tiempo, nos ayuda a nosotros a seguir implementando una estrategia de seguridad predictiva».

— Marcel Hoffmann, director senior, Cyber Defense Center, Hewlett Packard Enterprise

ArcSight ESM filtra y correlaciona los datos reunidos por el IPS TippingPoint y las otras fuentes, y proporciona a los analistas la información sólida y de alta calidad que necesitan para realizar análisis eficientes de datos de seguridad. La implementación de los productos de seguridad de HPE siguieron a la metodología de implementación de los servicios profesionales de software HPE e incorpora propiedades de equilibrio de carga, tolerancia a errores, recuperación de desastres y alta disponibilidad.

Detectando y desviando ataques

Una empresa del tamaño de HPE recibe sondeos de vulnerabilidades e intentos de aprovecharlas cientos de veces por segundo. La solución HPE ArcSight procesa una media de mil millones de eventos al día, reduciendo el flujo de eventos a un volumen que puede ser gestionado por los pocos analistas que están de servicio en cada turno del CDC.

Estos analistas reducen las alertas a 15-20 incidentes para realizar un seguimiento de ellas y tomar las medidas oportunas. Haría falta un ejército de más de 30.000 analistas si se realizase una función equivalente manualmente. Sin ArcSight, ese análisis no se realizaría, esos eventos hubieran quedado sin examinarse y los ataques en curso permanecerían sin detectarse.

La solución ArcSight detecta patrones de actividad, los correlaciona y crea alertas basadas en normas de caso de uso. HPE gestiona una enorme cantidad de datos sensibles que necesitan ser protegidos, incluidos los datos de sistemas, empleados y clientes.

ArcSight ESM ofrece al CdC un punto centralizado para realizar toda la supervisión de seguridad. El CdC aprovecha ArcSight para detectar amenazas en tiempo real de modo que puedan mitigarse rápidamente y también para reunir y correlacionar amplias cantidades de datos de seguridad que mejoran enormemente la capacidad de los analistas del CdC para localizar y desbaratar amenazas reales.

«La solución ArcSight proporciona una vista única al panorama de las amenazas y nos ayuda a maximizar nuestros recursos de seguridad», dice Hoffmann. «El tiempo y los esfuerzos de nuestros analistas puede dedicarse ahora a eventos de seguridad filtrados que indican amenazas reales, en lugar de a seleccionar ingentes volúmenes de datos sin procesar de distintos sistemas de supervisión».

Los análisis de datos proporcionados por ArcSight permiten una mitigación más rápida y eficiente, y presentan un fuerte argumento a favor para los propietarios de los activos afectados, lo cual es clave para encontrar remedios rápidos y eficaces. Cuando se detecta un ataque, ArcSight ayuda a los analistas del CdC a documentar los hechos y a proporcionar la prueba necesaria para involucrar eficazmente a los propietarios de los activos y a convencerlos sobre la solución.

Los sistemas de alimentación de datos están correlacionados centralmente en diferentes unidades de negocio y geografías, y proporcionan al CdC una visibilidad única sobre las ciberamenazas.

«Las empresas grandes necesitan la capacidad de correlacionar rápidamente los datos de los ataques entre múltiples planos para poder identificar rápidamente las posibles amenazas que se producen en toda la compañía y que algunas regiones o unidades de negocio podrían no reconocer», explica Alzati.

Hoffmann añade, «ArcSight ofrece un motor de correlación altamente sofisticado y enriquece los datos de los eventos para proporcionar un análisis de contexto más rápido. Gracias a ello, nuestros analistas pueden trabajar más eficientemente y se pueden tomar medidas más rápidas para mitigar las amenazas.

«ArcSight también nos permite detectar actividades de reconocimiento cuando los agresores busquen debilidades en nuestros sistemas para poder bloquear posibles ataques antes de que ocurran».

El CdC aprovecha continuamente sus experiencias para desarrollar casos de uso y filtrar los sistemas de alimentación de datos con el fin de mejorar el proceso de alerta. «Es importante tener iniciativa en el desarrollo de casos de uso para garantizar que el equipo del CdC reciba las alertas automatizadas apropiadas», comenta Alzati. «El personal de operaciones revisa informes a diario para asegurarse de que existe la instrumentación y los controles adecuados, pero una vez tienen los casos de uso apropiados, ArcSight sirve como pantalla única que les ayuda a comprender toda la información de registro y a entender el estado de la seguridad de la organización».

La combinación de las soluciones ArcSight ESM y TippingPoint IPS ha ayudado a los analistas de CdC a detectar y desviar miles de ataques potenciales. Por ejemplo, el CdC evitó proactivamente ataques del exploit POODLE (Padding Oracle On Downgraded Legacy Encryption).

Según Hoffmann, «la primera vez que oímos hablar de la vulnerabilidad ante el POODLE, escribimos una norma de caso de uso en ArcSight para detectar la actividad que intentaba aprovechar la vulnerabilidad. Creamos una lista negra de unas 250 direcciones IP basadas en alertas de ArcSight resultantes de la nueva norma, bloqueando potencialmente a los atacantes y evitando que se aprovecharan de las vulnerabilidades».

Al momento del anuncio de Shellshock en septiembre de 2014, TippingPoint informó a los analistas de CdC que los atacantes estaban escaneando los sistemas de HPE en busca de vulnerabilidades a través de las alertas mostradas en los paneles de ArcSight ESM. «ArcSight nos mostró en tiempo real de dónde procedían los escáneres y cuáles eran sus objetivos», dice Hoffmann. «En un breve plazo de tiempo, fuimos capaces de hacer un informe sobre las vulnerabilidades de HPE ante Shellshock y de impulsar la priorización de parches en el sistema para ponerles remedio».

Correlación y análisis de grandes datos

En colaboración con HPE Labs, el CdC implementó dispositivos de registro del servidor de nombres de dominio (DNS) para reunir registros de los seis clústeres de DNS internos, que a continuación se envían a HPE Vertica Analytics Platform para ofrecer una capacidad avanzada de análisis y alertas. HPE Vertica Analytics Platform gestiona cantidades masivas de datos de forma rápida y fiable, lo cual proporciona al CdC información sobre el negocio en tiempo real para ofrecer una capacidad avanzada de análisis de grandes datos.

Caso práctico
HPE Cyber Defense Center

Industria
Tecnología

El cliente de un vistazo

HPE Security Solution

- HPE ArcSight Enterprise Security Manager
- HPE ArcSight Logger
- HPE TippingPoint Intrusion Prevention System
- HPE TippingPoint Threat Digital Vaccine
- HPE Vertica Analytics Platform

Con Vertica, el CdC puede realizar consultas entre 50 y 1000 veces más rápido que con las bases de datos tradicionales, empleando una fracción del hardware. A diferencia de las bases de datos relacionales tradicionales diseñadas para el procesamiento de datos empresariales, Vertica está construida de principio a fin específicamente para complejas cargas de trabajo de análisis y puede admitir fácilmente la velocidad y el volumen de datos que se reúnen dentro de un COS.

«El CdC necesita una plataforma de análisis de grandes datos porque la tecnología tradicional no puede satisfacer los requisitos de velocidad y de rapidez en el acceso a los datos necesarios para analizar rápidamente grandes datos», dice Lin Li, arquitecto de ciberseguridad empresarial de HPE. «Por ejemplo, el CdC analiza archivos de registro de más de 130 servidores web internos. Con Vertica, podemos almacenar e inyectar estos archivos como lotes por hora y procesarlos de modo que el equipo de CdC pueda ejecutar los análisis».

Los registros correlacionados de ArcSight también se incorporan a Vertica y ello permite que el CdC realice rápidamente sofisticados análisis de grandes datos para mitigar las amenazas y evitar ataques futuros. «Gracias a Vertica, el CdC puede correlacionar más de dos mil millones de registros al día, con archivos de registro en una amplia variedad de formatos», explica Li. «Con Vertica, el CdC puede normalizar y limpiar los datos y correlacionarlos con otros datos de referencia. De esta manera, el CdC puede disponer de una idea general para que el equipo comprenda el tráfico que llega a la red global de HPE y así, asegurar eficientemente los recursos de la empresa».

Li continúa, «como Vertica es fácil de usar y comprime los datos muy bien, CDC puede almacenar los datos y realizar análisis históricos de eventos pasados con un coste eficiente. La mayoría de las consultas detalladas relacionadas con más cien mil millones de registros en Vertica se obtienen en menos de un minuto. Esto era imposible con la antigua arquitectura porque esta clase de rendimiento simplemente sería imposible con un sistema gestor de bases de datos convencional de una escala comparable. Este nivel de análisis histórico permite que el CdC comprenda si los usuarios pueden estar expuestos a malware desconocido anteriormente y realizar mejoras de seguridad con proactividad».

Preparándose para el futuro

El CdC está en la primera de las tres fases de una estrategia de implementación. La fase inicial se centra en asegurar el perímetro aprovechando la información sobre amenazas y reduciendo la superficie de ataque. La fase 2 se concentrará en asegurar la aplicación mientras que la fase 3 asegurará el negocio. La hoja de ruta del CdC exige una implementación completa en toda la empresa para 2017, y HPE continúa evolucionando mejores prácticas que puedan ser aprovechadas por otras grandes empresas.

«Empiece poco a poco, no intente hacer hervir el océano», advierte Hoffmann. «Es mejor implementar la seguridad empresarial en fases, especialmente para empresas muy grandes con múltiples divisiones. Antes de la implementación, identifique los activos más críticos, proporcione formación sobre los productos a su gente y desarrollo procesos maduros de remedio».

El CdC también está haciendo planes para las amenazas emergentes con el fin de asegurarse de estar bien preparado para abordar estos futuros desafíos —hoy.

Centrándose en una mejora continua, el CdC sigue evolucionando al tiempo que sirve como laboratorio de pruebas del mundo real para los productos y servicios de HPE y como infraestructura para dirigir un COS flexible con un personal relativamente corto de tan solo 22 profesionales de seguridad.

Al dirigir uno de los COS más grandes del mundo, HPE está aprendiendo a extraer incluso más valor de cada dólar en seguridad para que pueda trasladarse a los clientes de HPE.

Descubra más en hpenterprisesecurity.com/

Inscríbase para recibir actualizaciones

★ Valore este documento

Hewlett Packard Enterprise

4AA5-8767ESE, diciembre de 2015, Rev. 1