Hewlett Packard Enterprise

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

El mayor despliegue de exposición de excelencia operativa y de las tecnologías de seguridad de HPE

Objetivo
Proteger los recursos de la empresa en todo y ser, al mismo tiempo, un modelo de las mejores prácticas operativas para la innovación en seguridad empresarial

Enfoque
- Implementar los productos HPE ArcSight e integrar las fuentes de datos de HPE TippingPoint Intrusion Prevention System (IPS) y de orígenes de terceros
- Analizar los orígenes de macrodatos para efectuar un análisis avanzado y emitir alertas con HPE Vertica Analytics Platform

Asuntos de TI
- Los productos ArcSight supervisan aproximadamente mil millones de eventos al día, lo que reduce el flujo de eventos a un volumen que puede ser administrado por unos pocos analistas, algo que, si se realizara manualmente, requeriría el trabajo de más de 30 000 analistas.
- Los eventos se refieren desde aproximadamente 600 plataformas de TippingPoint Intrusion Prevention System y desde docenas de otras fuentes para detectar amenazas de manera preventiva. TippingPoint IPS detecta y bloquea activamente unos cinco millones de ataques al día.
- HPE Vertica Analytics Platform habilita al CDC a correlacionar más de 2000 millones de registros al día y permite al personal efectuar consultas de 50 a 1000 veces más rápido de lo que es posible con las bases de datos tradicionales, usando una fracción del hardware.

Asuntos del negocio
- Los datos empresariales de HPE se protegen a escala global para unos 250 000 empleados con un personal de solo 22 profesionales de seguridad.
- Cyber Defense Center actúa como un marco para la seguridad global de la empresa a fin de que las mejores prácticas de seguridad de HPE sigan siendo altamente eficaces y se mantengan actualizadas continuamente.
- Las innovaciones en las prácticas de seguridad del CDC se transfieren a los servicios y productos de seguridad de HPE para mantener a los clientes a la vanguardia de las amenazas cibernéticas.

HPE Cyber Defense Center ofrece capacidad de clase mundial en operaciones, ingeniería, inteligencia y gestión de incidentes para todos en Hewlett Packard Enterprise (HPE). El CDC implementó la mayor parte de la línea de productos HPE ArcSight e integró fuentes de datos de aproximadamente 600 plataformas de HPE TippingPoint Intrusion Prevention System (IPS) y realiza análisis complejos de cantidades exorbitantes de datos del sistema y de la red con HPE Vertica Analytics Platform para efectuar un análisis avanzado y emitir alertas. Esta base de pruebas del mundo real no solo protege la infraestructura de TI global de HPE, sino que además ofrece un contexto para ayudar a los clientes de HPE a mantenerse a la vanguardia de los ataques cibernéticos y llevar a cabo sus negocios de manera ininterrumpida.

Luego de analizar más de 90 centros de operaciones de seguridad (SOC) en todo el mundo y acumular el mayor conjunto de datos de su tipo, HPE ha tomado las mejores prácticas de la industria y las lecciones aprendidas y las ha aplicado a su propio Cyber Defense Center.

El CDC demuestra no solo la capacidad de HPE de lograr una visualización tridimensional colectiva de toda la empresa, sino que además sirve como ejemplo de la innovación en seguridad empresarial, ya que protege uno de los bienes más importantes de la compañía: la información.

El CDC, que abrió en el otoño de 2013, aprovecha las lecciones que HPE ha aprendido a lo largo de más de 10 años sobre las implementaciones de operaciones de seguridad. Ya es uno de los mayores SOC del mundo. Protege la infraestructura de TI global de HPE contra ataques cibernéticos y brinda, al mismo tiempo, un foro para demostrar la experiencia en seguridad de HPE a clientes y asociados. Por ejemplo, ha protegido a HPE de tipos de ataques tales como Heartbleed y Shellshock, software malicioso que podría haber ocasionado vulnerabilidad y explotación extremas de no haber sido detectado y solucionado.

En sintonía con la visión "HPE on HPE" de que la TI de HPE debe ser la presentación principal de la compañía, el equipo del CDC ha implementado la mayoría de los productos de la línea de productos HPE ArcSight y ha integrado fuentes de datos de aproximadamente 600 plataformas de HPE TippingPoint Intrusion Prevention System (IPS) implementadas en todo el mundo. HPE reúne además los registros de los servidores web y de otros orígenes y lleva a cabo análisis avanzados y emisión de alertas con HPE Vertica Analytics Platform.

Esta base de pruebas del mundo real permite a HPE proteger su propia infraestructura de TI y analizar las amenazas cibernéticas transformando la información en futuros avances para los servicios de asesoría y productos de seguridad de HPE.

Representa un logro mayor en inteligencia de seguridad a escala masiva ya que, actualmente, HPE cuenta con lo siguiente:

- 20 000 dispositivos de red
- 37 000 servidores
- 330 000 empleados
- 450 000 extremos administrados

Correlación de la información en docenas de plataformas

La plataforma de TippingPoint IPS se implementa en las instalaciones de HPE en todo el mundo y se administra localmente. El CDC actúa como el principal consumidor de sus eventos para la prevención de intrusiones. TippingPoint IPS ofrece protección en tiempo real y en línea brindando seguridad de red preventiva para los centros de datos y el tráfico de red de HPE.

Las soluciones de ArcSight correlacionan los registros de TippingPoint y de otros orígenes para que el CDC pueda detectar las amenazas de manera proactiva. Todas las plataformas de TippingPoint se basan en el servicio de suscripción HPE TippingPoint Threat Digital Vaccine (ThreatDV), el cual ofrece un paquete semanal para el filtro del malware que ayuda a las empresas a estar protegidas contra las amenazas avanzadas más actualizadas, a prevenir y a interrumpir la actividad del malware, a proteger información confidencial y a optimizar el desempeño de la red.

Según Marcel Hoffmann, gerente sénior del Cyber Defense Center de HPE: "En HPE, TippingPoint detecta y bloquea de manera activa aproximadamente cinco millones de ataques al día. Nuestro CDC opera la tercera instalación de TippingPoint IPS más grande del mundo y, cuando detecta una amenaza grave, saneamos el tráfico y bloqueamos esos ataques activamente".

A pesar del tamaño de la implementación de TippingPoint, el CDC recibe una cantidad relativamente baja de alertas de TippingPoint.

"Recibimos un volumen elevado de alertas de firewall pero muchos corresponden a ruido de fondo", explica Hoffmann. "TippingPoint IPS proporciona un flujo de alta fidelidad y bajo volumen de alertas que requieren acción y que investigamos activamente".

Las plataformas de HPE ArcSight Enterprise Security Manager (ESM), HPE ArcSight Logger y HPE TippingPoint IPS funcionan en conjunto para crear un sistema de defensa cibernética potente y exhaustivo. Cada elemento desempeña una función esencial en garantizar la seguridad de los valiosos activos de información de HPE, que incluyen aplicaciones de la empresa, sistemas de información del cliente, activos de propiedad intelectual y todos los recursos de información esencial disponibles en la red empresarial de HPE.

TippingPoint IPS supervisa y detecta la actividad en la red, bloquea la actividad malintencionada en la capa de la aplicación y envía la información del evento a ArcSight ESM. ArcSight Logger categoriza y almacena la información del evento de TippingPoint y de otros orígenes.

ArcSight habilita la supervisión de registros de docenas de plataformas desde una única consola y realiza la correlación avanzada de los eventos provenientes de varios orígenes. Además de utilizar datos del registro de las plataformas de TippingPoint IPS, ArcSight también aprovecha los registros de firewalls, Microsoft® Windows® Server Active Directory, HPE-UX, VMware, Microsoft.net y redes privadas virtuales, conmutadores y dispositivos de red, proxy web, soluciones de código abierto y bases de datos. "Tenemos la capacidad de capturar registros de la mayoría de los orígenes utilizando los conectores listos para usarse de ArcSight. También utilizamos el marco de trabajo HPE FlexConnector para generar la lógica de recolección y contextualizar los registros para terceros", indica Jorge Alzati, gerente sénior de Ingeniería de ArcSight y Gestión de la Producción.

"El CDC ya ha detectado y rechazado miles de ataques posibles en apenas menos de un año. Nuestro programa de seguridad cibernética ofrece información de seguridad precisa para ayudar a la administración a tomar decisiones basadas en hechos y, al mismo tiempo, a continuar con la implementación de una estrategia de seguridad predictiva".

— Marcel Hoffmann, gerente sénior, Cyber Defense Center, Hewlett Packard Enterprise

ArcSight ESM filtra y correlaciona la información obtenida por TippingPoint IPS y los otros orígenes, lo que le permite brindar a los analistas la información confiable y de alta calidad que necesitan para efectuar un análisis eficaz de la inteligencia de seguridad. La implementación de los productos de seguridad de HPE fue una extensión de la metodología de implementación de los servicios profesionales de software de HPE e incorpora la alta disponibilidad, la recuperación frente a desastres, la tolerancia de fallos y las propiedades de equilibrio de cargas.

Detección y rechazo de ataques

Una empresa de la envergadura de HPE recibe sondeos para detectar vulnerabilidades e intentos de explotar vulnerabilidades cientos de veces por segundo. La solución HPE ArcSight procesa un promedio de mil millones de eventos diariamente, lo que reduce el flujo de eventos a un volumen que puede ser administrado por los pocos analistas que están activos durante cada turno del CDC.

Esos analistas disminuyen más las alertas a entre 15 y 20 incidentes que se derivan para seguimiento y acción de corrección. Se necesitaría un ejército de más de 30 000 analistas para realizar una función equivalente manualmente. Sin ArcSight implementada, ese análisis no se realizaría y esos eventos no se analizarían, lo que dejaría los ataques en progreso sin detectar.

La solución ArcSight detecta patrones de actividad, los correlaciona y genera alertas en función de las reglas del caso de uso. HPE administra una enorme cantidad de información confidencial que necesita protegerse y que incluye información de los sistemas, de los empleados y de los clientes.

ArcSight ESM brinda al CDC un punto centralizado para llevar a cabo toda la supervisión de seguridad. El CDC aprovecha ArcSight para detectar amenazas en tiempo real a fin de que puedan mitigarse rápidamente. También utiliza ArcSight para reunir y correlacionar grandes cantidades de datos de seguridad, lo cual mejora ampliamente la capacidad de los analistas del CDC para localizar con precisión amenazas genuinas y frustrarlas.

"La solución ArcSight ofrece una vista única del entorno de la amenaza y nos ayuda a aprovechar al máximo nuestros recursos de seguridad", indica Hoffmann. "Ahora, el tiempo y los esfuerzos de nuestros analistas pueden enfocarse en eventos de seguridad filtrados que indiquen amenazas reales, en lugar de examinar grandes cantidades de datos sin procesar provenientes de sistemas de supervisión independientes".

El análisis de la información que ofrece ArcSight respalda una mitigación más rápida y más eficaz, y presenta un caso sólido a los propietarios con activos afectados, lo cual resulta clave para realizar correcciones rápidas y efectivas. Cuando se detecta un ataque, ArcSight ayuda a los analistas del CDC a documentar los hechos y proporciona la prueba necesaria para comprometer eficazmente a los propietarios de los activos y lograr su aceptación de una solución.

Las fuentes de datos se correlacionan de manera centralizada a través de todas las ubicaciones y unidades de negocios, lo cual brinda al CDC una visibilidad exclusiva de las amenazas cibernéticas.

"Las empresas grandes necesitan la capacidad de efectuar correlaciones cruzadas rápidamente a través de diversos planos para poder identificar con rapidez las posibles amenazas que se producen a través de la compañía y que las regiones o unidades de negocios individuales pueden no llegar a reconocer", explica Alzati.

Hoffmann agrega: "ArcSight ofrece un motor de correlación altamente sofisticado y enriquece la información del evento para brindar un análisis más rápido del contexto. Esto permite a nuestros analistas trabajar de manera más eficiente y efectiva y habilita acciones más rápidas para mitigar las amenazas".

"ArcSight nos permite, además, detectar las actividades de reconocimiento cuando los atacantes están buscando debilidades en nuestros sistemas para que podamos bloquear los posibles ataques antes de que puedan producirse".

El CDC aprovecha continuamente sus experiencias para desarrollar casos de uso para filtrar los suministros de datos y mejorar el proceso de emisión de alertas. "Es importante desarrollar casos de uso proactivamente para asegurarse de que el equipo del CDC reciba las alertas automáticas apropiadas", indica Alzati. "El personal de operaciones revisa los informes diariamente para garantizar la implementación de la instrumentación y los controles apropiados, pero, una vez que tienen los casos de uso adecuados, ArcSight actúa como panel único que los ayuda a dar sentido a toda la información del registro para entender el estado de seguridad de la organización".

La combinación de las soluciones ArcSight ESM y TippingPoint IPS ha ayudado a los analistas del CDC a detectar y rechazar miles de posibles ataques. Por ejemplo, el CDC evitó proactivamente los ataques provenientes de la explotación de ataques Padding Oracle On Downgraded Legacy Encryption (Poodle).

Según Hoffmann: "Cuando supimos por primera vez de la vulnerabilidad Poodle, escribimos la regla de caso de uso en ArcSight para detectar la actividad que intentara explotar la vulnerabilidad. Agregamos a la lista negra unas 250 direcciones IP en función de alertas de ArcSight derivadas de la regla nueva, lo que bloqueó potencialmente a los atacantes en sus intentos por explotar las vulnerabilidades".

A solo instantes del anuncio de Shellshock en septiembre de 2014, TippingPoint informó a los analistas del CDC que había atacantes explorando los sistemas de HPE para buscar vulnerabilidades mediante alertas que se mostraban en los paneles de ArcSight ESM. "ArcSight nos mostró en tiempo real de dónde provenían las exploraciones y cuáles eran sus objetivos", dice Hoffmann. "En un plazo corto, pudimos realizar un informe sobre las vulnerabilidades de HPE frente a Shellshock y dirigir las prioridades de las soluciones del sistema para corregirlas".

Análisis y correlación de macrodatos

Al asociarse con HPE Labs, el CDC implementó dispositivos para el inicio de sesión del servidor de nombres de dominio (DNS) para reunir registros de los seis clústeres de DNS internos, que luego se envían a HPE Vertica Analytics Platform para efectuar un análisis avanzado y emitir los alertas. HPE Vertica Analytics Platform administra grandes cantidades de información de manera rápida y confiable. Además, brinda al CDC inteligencia comercial en tiempo real para efectuar análisis avanzado de macrodatos.

El cliente a simple vista

Solución de seguridad de HPE

- 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 tiene la capacidad de efectuar consultas de 50 a 1000 veces más rápido de lo que lo que resulta posible con las bases de datos tradicionales, usando una fracción del hardware. A diferencia de las bases de datos relacionales tradicionales que están diseñadas para el procesamiento de datos comerciales, Vertica se construye desde el inicio específicamente para cargas de trabajo analíticas complejas y puede admitir con facilidad la velocidad y el volumen de los datos que se recopilan en un SOC.

"El CDC necesita una plataforma de análisis de macrodatos porque la tecnología tradicional no puede cumplir con las demandas de velocidad y de acceso rápido a la información que son necesarias para analizar velozmente grandes cantidades de datos", dice Lin Li, arquitecto de seguridad cibernética empresarial de HPE. "Por ejemplo, el CDC analiza los archivos de registro provenientes de más de 130 servidores web internos. Con Vertica, es posible almacenar e incorporar estos archivos como lotes por hora y procesarlos para que el equipo del CDC pueda ejecutar el análisis".

Los registros correlacionados desde ArcSight también se suministran a Vertica, lo cual permite al CDC realizar velozmente un análisis sofisticado de grandes cantidades de datos para atenuar amenazas y prevenir ataques futuros. "Vertica permite al CDC correlacionar más de dos mil millones de registros al día, con archivos de registros que ingresan con una amplia variedad de formatos", explica Li. "Con Vertica, el CDC puede normalizar y limpiar los datos y correlacionarlos con otros datos de referencia. Esto permite al CDC armar un panorama completo para que el equipo pueda entender el tráfico que ingresa a la red global de HPE y asegurar eficazmente los recursos de la empresa".

Li indicó además que "dado que Vertica resulta fácil utilizar y comprime muy bien los datos, esto permite al CDC almacenar la información de manera rentable y efectuar un análisis histórico de los eventos anteriores. La mayoría de las consultas detalladas contra más de cien mil millones de registros de Vertica regresan dentro de un minuto. Esto resultaba imposible con la arquitectura anterior porque este tipo de producción simplemente sería imposible con un sistema de gestión de bases de datos (DBMS) convencional de escala comparable. Este nivel de análisis histórico permite al CDC entender si los usuarios pueden llegar a estar expuestos a malware que antes no se conocía y realizar mejoras de seguridad proactivas".

Prepararse para el futuro

El CDC encabeza una estrategia de implementación de tres etapas. La etapa inicial se ha enfocado en asegurar el perímetro aprovechando la inteligencia de amenazas y reduciendo la superficie de ataque. La etapa dos se concentrará en asegurar la aplicación y la etapa tres protegerá el negocio. El plan de trabajo del CDC requiere una implementación completa en toda la empresa para el año 2017, y HPE continúa desarrollando mejores prácticas que otras grandes empresas pueden aprovechar.

"Empiece de a poco; no intente embarcarse en tareas imposibles", aconseja Hoffmann. "Es mejor implementar la seguridad empresarial en etapas, especialmente para empresas muy grandes con varias divisiones. Antes de la implementación, identifique los activos más esenciales, capacite a su personal y desarrolle procesos de corrección avanzados".

El CDC también está planificando para casos de amenazas de seguridad emergentes a fin de garantizar que esté bien preparado para tratar esos desafíos futuros en el presente.

Con un enfoque en la mejora continua, el CDC continúa desarrollándose y actuando como una base de pruebas del mundo real para los servicios y los productos de HPE y como estructura de trabajo para operar un SOC ágil con relativamente poco personal, tan solo 22 profesionales de la seguridad.

Operando uno de los SOC más grandes del mundo, HPE está aprendiendo a extraer incluso más valor de cada dólar invertido en la seguridad para poder transferirlo a los clientes de HPE.

Más información

hpenterprisesecurity.com/

Inscribirse para recibir actualizaciones

★ Califique este documento

Hewlett Packard Enterprise

4AA5-8767SPL diciembre de 2015, rev. 1