Publicado en Madrid el 30/01/2018

cClear se integra con Cisco Firepower para aumentar el análisis y las medidas preventivas en la red

Esta última colaboración impulsa la convergencia de NetOps y SecOps, y logra un objetivo común en el mantenimiento de infraestructuras de red seguras y de alto rendimiento

cPacket Networks, proveedor líder en soluciones de última generación de monitoreo de rendimiento de redes (NPM) y analíticas, anuncia la disponibilidad de una integración entre la plataforma cClear de cPacket y Firepower de Cisco. Como miembro del Programa de Partners de Soluciones de Cisco, cPacket puede trabajar con los clientes de Cisco para proporcionar una solución fiable que se integra perfectamente con Firepower de Cisco.

Como NPM de mayor distribución del sector, escalable y velocidad de cable en el mercado, cClear analiza cientos de miles de enlaces en tiempo real desde un panel de control centralizado, y permite el procesamiento del tráfico de red en el momento en que se observa, frente al enfoque del tipo 'captúralo ahora, procésalo más tarde' que ofrecen otras soluciones.

La combinación de cClear de cPacket, el panel de visualización y Firepower de Cisco, la plataforma de administración unificada, se conecta a la perfección para ofrecer a los clientes comunes los beneficios de un contexto más completo sobre los eventos de seguridad. La colaboración tiene como objetivo impulsar la convergencia de NetOps y SecOps, dos grupos dentro de la empresa que a menudo se encuentran aislados en gran parte, pero que comparten el objetivo común de mantener una infraestructura de red segura y de alto rendimiento a bajo coste y con la mayor de las eficiencias.

En un informe publicado en septiembre de 2017 y titulado: 'Align NetOps and SecOps Tool Objectives with Shared Use Cases', Gartner afirma que "debido a las divisiones históricas, existe poca coordinación entre los compradores de herramientas NetOps y SecOps, incluso si esas herramientas comparten puntos de instrumentación counes y casos de uso. Los equipos de NetOps y SecOps a menudo duplican esfuerzos y desperdician dinero, ya que las herramientas que utilizan comparten muchos puntos de instrumentación y algunos casos de uso, específicamente aquellos para el análisis de tráfico y automatización de redes. Para alinear estos esfuerzos y evitar la adquisición de múltiples herramientas para el mismo propósito, los responsables de I&O (Infraestructura y Operaciones) deben evaluar qué conjuntos de herramientas se utilizan en ambos equipos, identificar casos de uso superpuestos y explorar las posibilidades con la utilización de una herramienta común".

La alineación de NetOps y SecOps ya se está produciendo. Por ejemplo, los Network Packet Brokers (NPB) están alimentando cada vez más paquetes sin procesar y flujo de datos a herramientas de seguridad, como las que se usan para la Información de Seguridad y Gestión de Eventos (SIEM). Además, las empresas están aprovechando más las herramientas de monitoreo y diagnóstico del

rendimiento de redes (NPMD) por motivos de seguridad, como es el caso de la identificación de hosts infectados mediante el análisis de marcadores de ataques de malware, como los incidentes recientemente ocurridos con WannaCry y Heartbleed.

"A medida que evolucionan las redes y se vuelven más complejas, es fundamental que las empresas adopten un enfoque proactivo para garantizar una monitorización continua y constante que mitigue las amenazas en el tema de la seguridad", dice Brendan O'Flaherty, CEO de cPacket. "CPacket está bien posicionado para ofrecer una solución integral que ofrece informes y análisis en tiempo real que se consolidan en un tablero centralizado. El resultado es una mayor eficiencia de la red y una visibilidad total, así como un menor coste y riesgo de amenazas para NetOps y SecOps".

La integración cPacket/Cisco aprovecha el contexto del evento, así como la dirección IP del perpetrador, identificado por el Sistema de Prevención de Intrusión de Última Generación (NGIP) de Cisco Firepower para brindar un contexto inmediato a SecOps en forma de captura de paquetes (PCAP), con KPI de rendimiento de la red gracias a cClear.

Los indicadores clave de rendimiento de CClear en tiempo real y las funciones de búsqueda federada se pueden usar para identificar ataques DDos, escaneos de remediación posteriores y coincidencia de patrones en tiempo real, todos ellos con un sello de tiempo preciso para garantizar una correlación precisa. Con un contexto completo, los ingenieros de SecOps ahora pueden descubrir los detalles sobre un evento de seguridad, así como recopilar información importante sobre lo que condujo a tal evento, permitiendo el desarrollo de medidas preventivas para futuros intentos o ataques similares en la red.

Disponibilidad
La integración de la plataforma cClear de cPacket con Cisco Firepower ya está disponible. Para más información, visitar www.cpacket.com

Datos de contacto:
Axicom
671637795

Nota de prensa publicada en: Madrid

Categorías: Telecomunicaciones Hardware Software Ciberseguridad