splunk>

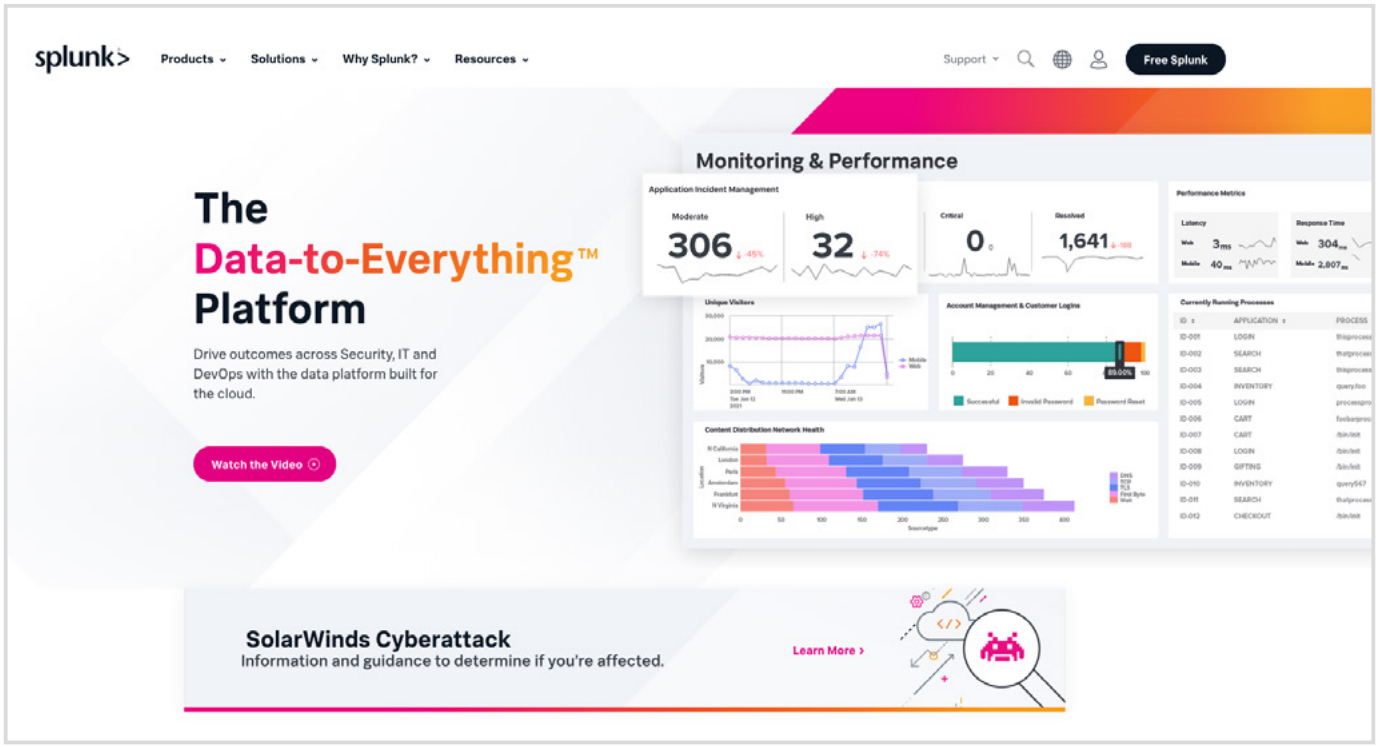
Splunk: el SIEM que resuelve los desafíos de seguridad del dato

Los cibercriminales se han agrupado en bandas organizadas que han hecho de la ciberdelincuencia un próspero negocio que no están dispuestos a abandonar. Situaciones extremas como la pandemia han propiciado el aumento de ataques, más sofisticados, impactando en mayor medida en el segmento empresarial. En 2020 fueron varias las compañías e instituciones que dieron la voz de alarma al verse atacadas. ¿Su máximo objetivo? El dato. Algo extremadamente peligroso si tenemos en cuenta que este es el principal activo de la empresa.

¿Qué necesitan las compañías para protegerse? Soluciones de gestión de eventos e información de seguridad, conocidas como SIEM, que ayuden a detectar, investigar y dar una respuesta temprana a los ataques, aseguran desde la consultora Gartner.

En su cuadrante mágico, Gartner destaca a los principales proveedores SIEM. La multinacional norteamericana Splunk tiene un papel destacado en el mismo. Nombrada por séptimo año consecutivo, en 2020, líder para la gestión de eventos e información de seguridad al conseguir la capacidad de ejecución más alta, evita el tiempo de inactividad de una compañía y detecta las vulnerabilidades antes de que surjan.

Forrester también nombró a Splunk líder en la plataforma de análisis de seguridad en "The Forrester Wave: Plataformas de análisis de seguridad", en el cuarto trimestre de 2020.



Tendencias SIEM

Splunk destaca la importancia que ha ido adquiriendo la tecnología de gestión de incidentes y eventos de seguridad (SIEM) desde hace una década, lo que la ha convertido en una plataforma de información con una gran demanda empresarial. Demanda que ha crecido durante el último año gracias a la gestión de amenazas. El Cuadrante Mágico de Gartner resalta, además, criterios como la supervisión basada en riesgos y la respuesta de la seguridad en la nube, por poner algunos ejemplos.

¿Cuáles van a ser las tendencias que van a girar en torno al SIEM en 2021? Un mayor enfoque en las alertas basadas en riesgos, pasando por la seguridad en la nube y las aplicaciones, la necesidad de los informes de cumplimiento o la visibilidad de amenazas, subrayan desde Splunk.

1) Si nos detenemos ante el alto número de alertas erróneas en un centro de operaciones de seguridad (SOC), los SIEM pueden mejorar exponencialmente la detección y respuesta ante infracciones y ataques dirigidos, gracias a la inteligencia y al análisis de ame-

nazas. Desde Splunk explican que las alertas basadas en riesgos son un enfoque relativamente nuevo a la hora de identificar amenazas, aunque consideran que libera tiempo y recursos a los SOC.

2) El SIEM también cobra protagonismo en torno a la seguridad en la nube. La migración hacia la misma no es fácil para todas las organizaciones. A medida que vayan avanzando en sus iniciativas digitales pasarán por alto algunos requisitos de seguridad, aumentando el riesgo, lo que, unido a una mayor superficie de ataque y a la falta de visibilidad, producirá una gran brecha de seguridad. Con una solución SIEM robusta la detección y respuesta a amenazas en entornos híbridos, en la nube y multinube será una realidad.

3) Por otro lado, el cumplimiento de la normativa es ineludible. Los informes de cumplimiento fortalecen la seguridad de una organización y los usuarios pueden documentar e informar de manera sencilla sobre incidentes, reduciendo la carga operativa y el tiempo de auditorías de seguridad.

4) Por último, la visibilidad de amenazas, más crítica que nunca, garantizando que la seguridad entre operaciones es fundamental durante su transición a la nube porque, como explican desde Splunk, el paso a la nube cambiará la forma en la que construimos, administramos e implementamos servicios.

Las organizaciones quieren llevar a cabo despliegues flexibles que se adapten a su infraestructura. Cuando se trata de una implementación SIEM hay varias opciones disponibles: para el despliegue *on-premise* los equipos de seguridad pueden "jugar" con los dispositivos físicos y virtuales, contenedores y despliegues en la nube privada o pública. También se puede llevar a cabo un despliegue por fases, empezando por un SIEM principal, expandiéndose a análisis de comportamiento de usuarios y entidades (UEBA) o una solución de orquestación, automatización y respuesta de seguridad (SOAR).

Desde Splunk comentan que se espera que los proveedores admitan versiones basadas en SaaS de su respectiva plataforma SIEM,

sin restricciones. Splunk Cloud es solo un ejemplo de cómo un SIEM puede combinar implementaciones locales, en la nube e híbridas para crear una solución SIEM basada en la nube que vaya más allá de la detección y la respuesta simples.

Splunk como SIEM en el día a día de las organizaciones

Splunk se adelanta a las tendencias al mejorar las operaciones de seguridad o contar con alertas basadas en riesgos. Esto hace que miles de organizaciones en el mundo usen Splunk como su SIEM para monitorizar la seguridad, detección avanzada de amenazas, investigación de incidentes y análisis forense, respuesta a incidentes, automatización de SOC, así como una amplia gama de análisis de seguridad y casos de uso de operaciones.

Su plataforma de datos, creada para la nube, incorpora varias soluciones de seguridad: Splunk Enterprise Security, Splunk UBA y Splunk Phantom.

La fuerza de una plataforma de datos

La importancia del dato es cada vez mayor en la denominada era de los datos. Y no es para menos si tenemos en cuenta que estos ayudan a las empresas a responder a cualquier pregunta. Pero ¿cómo sacar el mayor partido a los mismos?

Splunk pone a disposición de sus clientes la plataforma Data-to-Everything, con la que aporta datos a cada pregunta, decisión y acción. Una solución SIEM que permite monitorizar y analizar todos los datos, facilitando la toma de decisiones más apropiada. Porque, tal y como destacan desde Splunk, "los datos son valiosos si puedes actuar sobre ellos. Nuestra plataforma está diseñada para manejar datos de cualquier fuente, en cualquier estructura y escala de tiempo, permitiendo pasar de la investigación y el seguimiento, al análisis y la acción".

Splunk Enterprise Security ofrece la mayor parte del contenido de seguridad de Splunk, capacidades de monitoreo de eventos y respuesta ante incidentes, por poner algunos ejemplos.

Splunk UBA incluye analítica avanzada no supervisada, impulsada por *machine learning*.

Splunk Phantom, con capacidades SOAR (*Security Orchestration Automation and Response*) proporciona la corrección y mitigación automatizadas de incidentes de seguridad.

En definitiva, Splunk es un SIEM que combina soluciones de operaciones, análisis y datos para modernizar y optimizar las defensas cibernéticas de cualquier organización tanto en entornos locales como en múltiples nubes.