# SIEM: Hacia una nueva estrategia de ciberseguridad

POR MATÍAS DAVYT, SENIOR EN DELOITTE RISK ADVISORY – CIBERSEGURIDAD

En un mundo cada vez más interconectado y dependiente de la tecnología, los ataques informáticos se han vuelto cada vez más complejos y difíciles de detectar.

El número de dispositivos conectados ha aumentado drásticamente en los últimos años, y dado el número creciente de dispositivos IoT (*Internet of Things*) es esperable que esta realidad se mantenga. Desde servidores y *firewalls* hasta tabletas, teléfonos móviles y cámaras de videovigilancia, todo se encuentra conectado y, por tanto, expuesto a ataques informáticos. Más puntos de acceso implican una mayor dificultad en el control y detección de ataques, lo que aumenta la probabilidad de sufrir un incidente de ciberseguridad.

Se estima que tres de cada cuatro empresas han sufrido incidentes de seguridad en el último año, la mayoría de los cuales tardan semanas o meses en ser detectados. Es claro que la estrategia clásica de defensa mediante el agregado de capas de seguridad no es suficiente, se debe abordar esta problemática con un nuevo enfoque.

## LA NECESIDAD DE UNA NUEVA ESTRATEGIA

Típicamente las organizaciones responden a esta nueva realidad agregando más y más capas de seguridad. Herramientas como *firewalls*, sistemas de detección de intrusos, antivirus y *antispam* son cada vez más comunes en las empresas, así como controles operativos y procedimientos de seguridad. Estas medidas, si bien son necesarias, resultan en una complejidad adicional que es necesario atacar.

Todas estas herramientas generan una cantidad de información imposible de ser analizada por seres humanos, de este aumento de información surge la necesidad de distinguir los eventos normales de aquellos que presentan un riesgo para la organización.

Cada herramienta brinda una interfaz distinta, y genera información en formatos variados. A su vez, no existe un lugar central donde obtener la información necesaria en caso de ocurrir un incidente de ciberseguridad. Por otro lado, las auditorías requieren generar una gran cantidad de reportes, para los cuales se necesita consolidar información proveniente de múltiples fuentes de datos.

Las organizaciones han puesto gran énfasis en la prevención de ciberataques, sin tener en cuenta que la prevención no siempre es posible por más capas de seguridad que se agreguen. Hasta las más grandes empresas, que invierten una enorme cantidad de dinero en herramientas de seguridad, son víctimas de ataques en algún momento de su historia.

Estos ataques, una vez que ocurren, son difíciles de detectar. Teniendo en cuenta que el impacto de un incidente es proporcional al tiempo en que el mismo logra identificarse y resolverse, es clara la importancia de implementar mecanismos que permitan detectar estos incidentes a tiempo, mitigando así el daño ocasionado.

La mayoría de las organizaciones víctimas de ciberataques tienen evidencia del ataque en sus registros. La información necesaria para detectar estos ataques está disponible, y es mediante una estrategia de monitoreo permanente que se logra aprovechar y utilizar esta información de manera inteligente.

## ¿QUÉ ES UN SIEM?

Un SIEM (*Security Information and Event Management*) es un sistema que recibe información de múltiples fuentes de datos, la correlaciona y analiza en tiempo real buscando patrones de ataques conocidos y generando alertas tempranas que permitan responder a tiempo ante las amenazas. Además, esta información es luego almacenada para permitir su utilización en investigaciones y análisis forenses. Esto permite la coordinación de todos los dispositivos que juegan un rol en la seguridad de su organización, resultando en una mayor visibilidad sobre los comportamientos inusuales.

Existe una enorme cantidad de herramientas SIEM en el mercado, ninguna de las cuales es la solución más adecuada para todas las organizaciones. Además, ninguna de estas herramientas aporta valor a una organización si no es adaptada a sus necesidades particulares.

Las empresas deberían seleccionar la mejor herramienta para cada organización y adaptarla a sus necesidades, brindándole así una mayor visibilidad sobre el estado de su seguridad. Para esto es necesario contar con un equipo experto, que sea capaz de evolucionar para adaptarse a nuevos tipos de amenazas.

## CONCLUSIONES

Históricamente la defensa ante ciberataques ha estado enfocada en su prevención. Sin embargo, como se ha demostrado que no siempre es posible evitar estos ataques surge la necesidad de detectarlos a tiempo y tomar medidas mitigatorias.

La cantidad de herramientas utilizadas hoy en día por las organizaciones genera un gran volumen de información valiosa para la detección de ataques informáticos. Esta información está disponible, simplemente debe ser analizada y utilizada de forma inteligente. Un SIEM facilita el tratamiento de la información y su utilización para detectar ataques antes de que se conviertan en un incidente de seguridad mayor.