Tendencias en ciberseguridad

Gestión de Información de Eventos de Seguridad (SIEM)

La Gestión de Información de Eventos de Seguridad o Security Information and Event Management (SIEM) se basa en la detección de amenazas y respuesta a incidentes de seguridad a través de la obtención en tiempo real y **análisis histórico** de los eventos de seguridad, a partir de una amplia variedad de fuentes de eventos y datos contextuales. Esta gestión en tiempo real de información es factible en las grandes corporaciones, con multitud de **información de vulnerabilidades** o posibles ataques, como son las grandes entidades bancarias en las que el sistema recoge, analiza y prioriza los eventos de seguridad de la red.

ORIGEN DE LA TENDENCIA

- ECONÓMICO/EMPRESARIAL
- DEMANDA
- NORMATIVA
- TECNOLOGÍA

La tecnología SIEM ofrece análisis en tiempo real de alertas de seguridad generadas por las aplicaciones de la red. Los SIEM son ampliamente utilizados por empresas de todos los sectores, desde el transporte o la energía, hasta los seguros y las entidades bancarias. En este sentido, esta tecnología no constituye de por sí una tendencia. No obstante, el aumento del uso de la Infraestructura basada en la nube como servicio (IaaS) en las organizaciones se está convirtiendo en un importante impulsor del **SIEM como servicio**, ya que las organizaciones buscan simplificar la recopilación y análisis del registro de los eventos. Recientemente, la **UE pactó la directiva sobre ciberseguridad**, la primera norma de rango europeo que pretende reforzar la vigilancia de las redes informáticas que sostienen servicios esenciales como sanidad, energía o banca.

UBICACIÓN EN LA CADENA DE VALOR DE LA CIBERSEGURIDAD

Fabricación → Comercialización → **Servicios**

La tecnología **SIEM como servicio se encuadra en el último eslabón de la cadena de valor**, habiendo pasado de ser una herramienta on-premise a poder ser implementada, administrada y escalada en remoto. El SIEM podría estar alojado en el centro de datos del proveedor o en una servicio público cloud.

IMPACTO EN BENEFICIARIOS

USUARIO/PARTICULAR	EMPRESAS	ADMINISTRACIÓN PÚBLICA
Impacto en usuarios ●●○	Impacto en industria ●○○	Impacto en gobiernos ●●●
Los usuarios y clientes de entidades financieras, cuya banca cuenta con sistemas SIEM se benefician de una **mejor gestión** de sus datos e información personal y aseguran un **menor riesgo** en la gestión online de su cartera, fomentando la utilización de la banca online.	Los sistemas SIEM impactan en las entidades financieras aportando una gestión en tiempo real de incidencias y eventos en ciberseguridad que puedan poner en riesgo la cartera de sus clientes o su **información confidencial**. Este sistema aumenta la robustez y fiabilidad de la entidad financiera.	Con la incorporación de dichos sistemas SIEM, la administración asegura que las entidades bancarias, fundamentalmente, mantengan una **monitorización de los riesgos y amenazas** que sus clientes puedan sufrir. Esto aporta fiabilidad al sistema financiero nacional.

CLASIFICACIÓN DE LA TENDENCIA

- SOLUCIONES DE PREVENCIÓN
- **SOLUCIONES DE CONTROL**
- SOLUCIONES DE MITIGACIÓN

El SIEM como servicio gestiona los eventos o incidentes de ciberseguridad de manera que se puede **obtener información y ayudar a detectar las amenazas de forma rápida o identificar vulnerabilidades**. Además de ello se priorizan los eventos de seguridad de forma que sea posible tratar los incidentes de forma organizada con el fin de resolverlos en el menor tiempo posible y con las menores consecuencias.

CICLO DE VIDA DE LA TENDENCIA

- DESARROLLO
- **INTRODUCCIÓN**
- CRECIMIENTO
- MADUREZ

El término gestión de información de eventos de seguridad (SIEM), acuñado en 2005, hace referencia a la capacidad de **recopilar, analizar y presentar información** de la red y dispositivos de seguridad, a través de diversas aplicaciones de gestión de identidades, gestión de vulnerabilidades e instrumentos de política de cumplimiento, sistema operativo, bases de datos y registros de aplicaciones. La tecnología SIEM como Servicio es ofrecida por solo algunos proveedores, adaptándose a casos concretos con requisitos y presupuestos específicos.

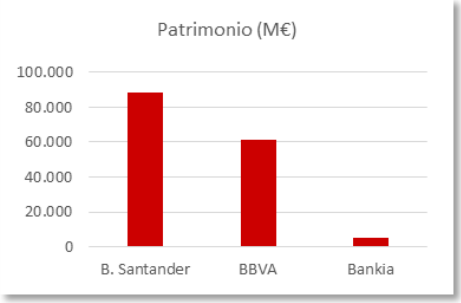
Tendencias en ciberseguridad

Gestión de Información de Eventos de Seguridad (SIEM)

ÁMBITO DE APLICACION

El ámbito de aplicación de la tendencias basada en los sistemas SIEM tiene mayor acogida entre **grandes empresas o** corporaciones cuyo negocio se asiente sobre la gestión de grandes cantidades de información como son aquellas basadas en el **asesoramiento en inversiones y la Banca transaccional en las entidades financieras**, siendo los principales sectores donde la gestión coordinada y segura de información resulta crítica para sus clientes.

CARACTERIZACIÓN DEL SECTOR DESTINATARIO



- Santander Private Banking experimentó en 2015 un crecimiento superior al 7 % en su patrimonio gestionado, hasta sobrepasar los 88.000 millones de euros. También aumentó en casi 4.000 nuevos clientes.
- BBVA, que cuenta con un patrimonio gestionado por banca privada que asciende a los 61.000 millones de euros, aumentó en 2015 un 7 % su número de clientes, que ascienden a 135.000
- Banca Privada de Bankia, volumen de negocio a cierre de 2015 ascendía a más de 5.000 millones de euros. Respecto a número de clientes de grandes patrimonios, cerró con más de 5.100 carteras, un 12 por ciento más que el año anterior.
- Kaspersky Lab publicó en su informe de amenazas correspondiente al primer trimestre del año 2015 que, respecto a las amenazas móviles, detectó 103.072 nuevos programas maliciosos para dispositivos móviles, un 6,6% menos que el año anterior, si bien el **volumen de nuevos troyanos de banca móvil creció un 29%.**
- En el tercer trimestre, sin embargo, las soluciones de Kaspersky Lab también bloquearon casi **626.000 programas maliciosos diseñados para robar dinero a través de acceso a las cuentas de banca online de los usuarios**. Este número es un 17,2% menor que la cifra registrada en el segundo trimestre del año, aunque es un 5,7% superior con respecto al año anterior.

PREVISIONES DE DEMANDA

CRECIMIENTO

- Durante el tercer trimestre de 2015, se produjeron 5,68 millones de notificaciones sobre infecciones de malware intentando robar dinero de los usuarios a través del **acceso online a las cuentas bancarias**, según Kaspersky.
- Según Gartner, durante 2014, el **mercado SIEM creció** de 1.500 M$ a aproximadamente 1.690 M$, alcanzando una tasa de crecimiento de **alrededor del 14%.**

CLIENTES

- Empresas, principalmente, con infraestructuras de cloud computing.
- Entidades financieras o de crédito.
- Empresas de predicción de mercado.
- Empresas de recaudación.
- Empresas con grandes sistemas de información y de gestión de datos.
- Gobierno y Administraciones Públicas.

MODELOS DE NEGOCIO

DIFERENCIACIÓN EN COSTE | DIFERENCIACIÓN EN PRESTACION DE SERVICIOS | DIFERENCIACIACIÓN EN VALOR AÑADIDO

CASO DE ÉXITO

splunk>

- La empresa SPLUNK ha desarrollado **SPLUNK Cloud**, un SIEM como servicio para el Orrstown Bank.
- Splunk Cloud ofrece al **Orrstown Bank** visibilidad centralizada de datos procedentes de más de 60 fuentes de datos únicos a través de todo su entorno TIC híbrido que incluye servidores de correo locales, servidores de Amazon Web Services y Microsoft Azure. Con la capacidad híbrida de analizar estos datos proporcionada por esta herramienta, el Orrstown Bank puede incrementar la **fiabilidad TIC de sus operaciones** y detectar rápidamente un comportamiento anómalo en todos sus registros de rendimiento, datos y aplicaciones de red.