NEWSLETTER

grupobeit.com

BLOG DEL CEO

La transformación digital ha redefinido por completo la forma en que operan las organizaciones. Hoy, las empresas conviven con entornos híbridos, infraestructuras distribuidas y una creciente integración entre IT y OT...

EDICIÓN 58

SIEM: La clave para una detección inteligente y respuesta oportuna

En un entorno donde las amenazas evolucionan constantemente, las organizaciones ya no pueden depender únicamente de soluciones aisladas de seguridad...

EVENTOS

Grupo BeIT y Arexdata presentes en la 14° Edición de Cybersecurity & Government

El día 14 de mayo tuvimos la oportunidad de asistir a la 14° Edición de Cybersecurity & Government, uno de los eventos más relevantes de ciberseguridad en la región....

Edición 58

SIEM: inteligencia que transforma la ciberseguridad en continuidad operativa

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

Un entorno donde la visibilidad lo es todo

La transformación digital ha redefinido por completo la forma en que operan las organizaciones. Hoy, las empresas conviven con entornos híbridos, infraestructuras distribuidas y una creciente integración entre IT y OT. Este nivel de conectividad ha traído eficiencia, pero también ha incrementado de manera exponencial la superficie de ataque.

En este contexto, el principal desafío ya no es únicamente proteger, sino entender en tiempo real lo que está ocurriendo dentro de la operación. La cantidad de información generada es tal que organizaciones globales procesan hasta 1.2 billones de eventos de seguridad al día, lo que hace imposible gestionar estos datos sin plataformas especializadas.

Es aquí donde el SIEM adquiere relevancia: no como una herramienta más, sino como un habilitador de visibilidad y control.

Un mercado que confirma su relevancia

La adopción del SIEM no es solo una tendencia tecnológica, sino una respuesta directa a la necesidad del mercado. Hoy, más del 82% de las grandes organizaciones ya utilizan SIEM como parte de su estrategia de seguridad.

Además, el crecimiento del sector refleja su importancia estratégica. Se proyecta que el mercado global alcanzará los 13.67 mil millones de dólares hacia 2031, impulsado principalmente por la adopción de modelos cloud y la creciente complejidad de los entornos digitales.

Este nivel de adopción confirma que el SIEM se ha consolidado como un estándar dentro de la operación moderna.

El núcleo del SOC moderno

El verdadero valor del SIEM se materializa en su rol dentro del SOC. Más allá de ser una herramienta de monitoreo, funciona como el cerebro que procesa, interpreta y prioriza la información de seguridad.

Al centralizar eventos de redes, aplicaciones, dispositivos y entornos industriales, el SIEM permite identificar correlaciones que no serían visibles de forma aislada. Esto habilita una detección más temprana de amenazas y una respuesta más efectiva.

Los resultados son claros. Organizaciones que implementan correctamente estas soluciones pueden reducir hasta en un 90% el tiempo de investigación de incidentes, además de disminuir significativamente su exposición al riesgo.

En este sentido, el SIEM no solo mejora la seguridad, sino que impacta directamente en la eficiencia operativa.

El desafío real: demasiada información, poco contexto

A pesar de contar con tecnologías avanzadas, muchas organizaciones enfrentan un problema crítico: la saturación de alertas. Los equipos de seguridad reciben más información de la que pueden procesar, lo que genera puntos ciegos operativos.

Se estima que los analistas apenas logran atender menos del 50% de las alertas generadas diariamente, dejando una gran cantidad de eventos sin análisis.

El SIEM moderno responde a este reto mediante el uso de inteligencia artificial y automatización, priorizando eventos relevantes y reduciendo falsos positivos. Este enfoque permite pasar de una gestión reactiva a una operación basada en contexto e inteligencia.

La nueva generación: SIEM inteligente y escalable

El avance hacia arquitecturas cloud ha transformado la forma en que se despliegan estas soluciones. Actualmente, más del 59% de los SIEM operan en modelos cloud, lo que facilita su escalabilidad y capacidad de procesamiento.

Además, la incorporación de tecnologías como machine learning y automatización ha permitido que estas plataformas evolucionen hacia modelos más avanzados, integrándose en estrategias de detección y respuesta extendida.

Este cambio posiciona al SIEM como una herramienta no solo de monitoreo, sino de anticipación.

La inteligencia como base de la resiliencia

En un entorno donde el tiempo de respuesta define el impacto de un incidente, la ciberseguridad debe evolucionar hacia modelos basados en inteligencia. La capacidad de anticiparse, contextualizar y actuar en tiempo real se ha convertido en un factor crítico de negocio.

El SIEM representa precisamente ese punto de convergencia entre datos, análisis y acción. Es la herramienta que permite transformar información en decisiones y decisiones en resiliencia.

En Grupo BeIT entendemos que proteger la operación no se trata solo de reaccionar, sino de anticipar, interpretar y responder con precisión. Y en ese camino, el SIEM no es solo una plataforma: es el cerebro que hace posible una ciberseguridad verdaderamente estratégica.

Contáctanos para un asesoría:

+52 56 5100 8613 admmarketing@buromc.com

Referencias:

- Security Information and Event Management (SIEM) Market Overview. (2026). Market Growth Reports. Recuperado de: Security Information and Event Management (SIEM) Market Size | Global Forecast To 2035
- Díaz, J. (2025). El aporte del SIEM en la búsqueda del SOC Autónomo. Recuperado de: El aporte del SIEM en la búsqueda del SOC Autónomo
- Security Information and Event Management Market. (2026). Markets and Markets. Recuperado de: Security Information and Event Management Market Growth Drivers & Opportunities | MarketsandMarkets
- IBM QRadar SIEM. (s.f.). IBM. Recuperado de: IBM QRadar SIEM
- IBM presenta un SIEM nativo en la nube diseñado para maximizar el tiempo y el talento de los equipos de seguridad. (2023). La Ecuación Digital. Recuperado de: IBM presenta un SIEM nativo en la nube diseñado para maximizar el tiempo y el talento de los equipos de seguridad

Edición 58

NEWSLETTER BeIT

SIEM: La clave para una detección inteligente y respuesta oportuna

En un entorno donde las amenazas evolucionan constantemente, las organizaciones ya no pueden depender únicamente de soluciones aisladas de seguridad. Hoy, la **visibilidad y correlación** de eventos en tiempo real se han convertido en elementos esenciales para prevenir incidentes críticos y responder oportunamente ante cualquier anomalía.

Aquí es donde entra el SIEM (Security Information and Event Management), una solución diseñada para centralizar, analizar y correlacionar logs y eventos de seguridad provenientes de toda la infraestructura tecnológica. Gracias a estas capacidades, las empresas pueden detectar amenazas en etapas tempranas, automatizar alertas y fortalecer su capacidad de respuesta ante incidentes.

Actualmente, las organizaciones enfrentan millones de eventos diarios de seguridad, haciendo prácticamente imposible gestionarlos manualmente. De acuerdo con IBM, el costo promedio global de una filtración de datos alcanzó los 4.88 millones de dólares en 2024, convirtiéndose en la cifra más alta registrada hasta ahora. Esto demuestra la necesidad de contar con plataformas que permitan una supervisión continua y una toma de decisiones más ágil y precisa.

Además, Gartner estima que las organizaciones que integran herramientas SIEM con automatización y analítica avanzada logran reducir significativamente los tiempos de detección y contención de amenazas. En un panorama donde cada segunda cuenta, el monitoreo centralizado se ha convertido en una necesidad estratégica para proteger la continuidad operativa, garantizar el cumplimiento normativo y mantener la confianza digital.

La evolución del SIEM también está siendo impulsada por inteligencia artificial y automatización avanzada. Nuevos estudios muestran cómo los modelos de IA comienzan a optimizar la generación de queries y la investigación de amenazas dentro de plataformas SIEM heterogéneas, permitiendo procesos de análisis más rápidos, eficientes y precisos.

Referencias:

- IBM. (s.f.). Cost of a Data Breach Report 2025. Recuperado de: https://www.ibm.com/reports/data-breach

- IBM. (s.f.). El aumento de las vulneraciones de datos eleva los costes a máximos históricos. Recuperado de: https://www.ibm.com/es-es/think/insights/whats-new-2024-cost-of-a-data-breach-report?utm_source=chatgpt.com

Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Hackeo a Canvas expone la vulnerabilidad de los entornos educativos digitales

NOTICIA BeIT

La plataforma educativa Canvas LMS, utilizada por miles de instituciones educativas alrededor del mundo, sufrió recientemente un ciberataque atribuido al grupo ShinyHunters, comprometiendo información de aproximadamente 275 millones de usuarios y afectando a cerca de 9,000 instituciones educativas. Entre los datos comprometidos se reportaron nombres, correos electrónicos, identificadores estudiantiles, mensajes privados e información académica sensible.

El ataque provocó interrupciones durante periodos de exámenes y actividades académicas críticas, evidenciando la dependencia que actualmente existe hacia plataformas digitales centralizadas y la importancia de fortalecer las estrategias de monitoreo, trazabilidad y respuesta ante incidentes.

Especialistas en ciberseguridad han advertido que este tipo de brechas incrementa considerablemente el riesgo de ataques de phishing dirigido, robo de identidad, ingeniería social y compromiso de credenciales. La magnitud del incidente vuelve a poner sobre la mesa la necesidad de contar con soluciones de monitoreo continuo, gestión de eventos y protección avanzada de datos para reducir riesgos y responder de forma más eficiente ante amenazas emergentes.

Este caso también refleja cómo sectores como educación, gobierno y empresas privadas enfrentan retos similares en materia de protección de la información, especialmente en un contexto donde los datos se han convertido en uno de los activos más valiosos para las organizaciones.

Contacto:

+52 56 5100 8613 admmarketing@buromc.com

Fuentes:

- Taylor, J. (2026). Canvas hack: is it ever a good idea to pay a ransom, and what happens to the data? The Guardian. Recuperado de: https://www.theguardian.com/technology/2026/may/17/canvas-hack-cyber-criminals-data-ransom-paid?utm_source=chatgpt.com

Grupo BeIT y Arexdata presentes en la 14° Edición de Cybersecurity & Government

AREXDATA
YOUR VALUE, YOUR DATA

El día 14 de mayo tuvimos la oportunidad de asistir a la 14° Edición de Cybersecurity & Government, uno de los eventos más relevantes de ciberseguridad en la región, acompañando a nuestro partner Arexdata, líder en trazabilidad y protección del dato.

Durante su participación, Arexdata presentó sus soluciones enfocadas en gobernanza de datos, protección de información confidencial, cumplimiento regulatorio y trazabilidad del dato, permitiendo a las organizaciones fortalecer la seguridad de la información y optimizar sus procesos de auditoría con menos esfuerzo y menor costo operativo.

En un contexto donde las organizaciones generan y almacenan cantidades masivas de información sensible, la visibilidad y control del dato se han convertido en pilares fundamentales para garantizar la continuidad operativa y la confianza digital. La colaboración entre aliados estratégicos permite impulsar soluciones más robustas que respondan a los desafíos actuales de ciberseguridad y cumplimiento.

Seguimos fortaleciendo alianzas que impulsan la innovación, la resiliencia digital y la confianza en la gestión de la información, contribuyendo a construir entornos tecnológicos más seguros para empresas e instituciones.