Grupo BeIT

NEWSLETTER

Blog CEO

El peligro latente de la persistencia en entornos cloud

Noticia BeIT

CloudFlare

Edición 49

Introducción a la detección de anomalías con XDR y SIEM

Servicios BeIT

Ethical Hacking

ELIT INFRASTRUCTURE SERVICES

BURÖMC SEGURIDAD INFORMÁTICA

Edición 49

El peligro latente de la persistencia en entornos cloud

Por: Elías Cedillo, Fundador y CEO GrupoBeIT

La migración hacia servicios en la nube como AWS, Microsoft Azure y Google Cloud ha transformado la operación empresarial, ofreciendo escalabilidad, flexibilidad y reducción de costos. Sin embargo, esta evolución también ha traído consigo un riesgo silencioso que muchas organizaciones subestiman: la persistencia del atacante en entornos cloud. Los ciberdelincuentes, además de robar datos, buscan establecerse de manera permanente dentro de la infraestructura para mantener el control y explotar recursos durante meses sin ser detectados.

Cuando un atacante compromete una cuenta en la nube, la exfiltración de datos suele ser el primer paso, pero los ataques más sofisticados van más allá. El verdadero objetivo es permanecer oculto incluso después de que la intrusión inicial haya sido aparentemente corregida. Esta persistencia se logra mediante tácticas avanzadas que aprovechan la complejidad y la falta de visibilidad en entornos multinube. Gartner advierte que la gestión de identidades y accesos (IAM) y la supervisión continua son esenciales para evitar que estas amenazas se consoliden, ya que la nube introduce un modelo de responsabilidad compartida donde el proveedor asegura la infraestructura física, pero la configuración y gestión de accesos recae en la empresa.

Los métodos más comunes para lograr persistencia incluyen la creación de usuarios fantasma con privilegios ocultos que no aparecen en auditorías superficiales, la instalación de backdoors en funciones serverless como AWS Lambda o Azure Functions para ejecutar código malicioso sin levantar sospechas, y la generación de llaves de API maliciosas que permiten acceso remoto incluso después de cambios de contraseñas. También es frecuente la manipulación de roles IAM, asignando permisos excesivos o creando políticas que facilitan el movimiento lateral dentro del entorno cloud. Estas técnicas son especialmente peligrosas porque se integran en la lógica interna de la infraestructura, donde las herramientas tradicionales no tienen visibilidad.

Este punto nos lleva a una realidad crítica: la seguridad tradicional basada en firewalls perimetrales es insuficiente. En la nube, el perímetro desaparece. Las aplicaciones, datos y usuarios están distribuidos globalmente, y las conexiones se realizan mediante APIs y servicios internos que no pasan por el firewall. Incluso los firewalls más avanzados no pueden inspeccionar la lógica interna de funciones serverless ni detectar credenciales maliciosas en IAM. Fortinet y otros líderes en ciberseguridad coinciden en que la solución pasa por adoptar un enfoque de confianza cero, que asume que ninguna conexión es segura por defecto y exige verificación continua de identidad y contexto.

A esta amenaza se suman tendencias alarmantes: según el **Informe 2025 de Tenable**, el 9 % del almacenamiento público en la nube contiene datos sensibles y el 97 % de ellos son confidenciales, lo que evidencia brechas graves en la gestión de accesos y configuraciones. Además, más del 50 % de las organizaciones almacenan secretos (claves, tokens) en definiciones de tareas de AWS ECS y servicios similares, creando vectores de ataque directos. Tenable también advierte sobre la "trilogía tóxica": cargas de trabajo expuestas públicamente, vulnerables y con privilegios elevados, presentes en el 29 % de las organizaciones, lo que facilita la persistencia y escalamiento de privilegios.

Por otro lado, las alertas de seguridad en la nube se han multiplicado por cinco en el último año, con un incremento del 116 % en eventos relacionados con IAM, como inicios de sesión imposibles y uso indebido de tokens en funciones serverless. Esto confirma que los atacantes están priorizando credenciales y exfiltración como tácticas principales. De hecho, **una de cada cuatro empresas sufrió al menos una exfiltración de datos en la nube en el último año,** y el 36 % experimentó múltiples filtraciones, impulsadas por configuraciones erróneas y falta de cifrado.

Las cadenas de suministro digitales y los entornos cloud también se perfilan como zonas críticas en 2025. Un solo proveedor comprometido puede abrir la puerta a múltiples organizaciones, amplificando el impacto del ataque. El costo global del cibercrimen superará los 10 billones de dólares este año, impulsado por el uso de IA para ataques más rápidos y sofisticados.

Finalmente, el **Informe Veeam 2025** revela que cerca del 70 % de las organizaciones siguen sufriendo ciberataques, a pesar de haber mejorado sus defensas. Lo más preocupante es que solo el 10 % logra recuperar más del 90 % de sus datos tras un incidente, mientras que el 57 % recupera menos del 50 %. Además, crecen los ataques centrados exclusivamente en exfiltración, que roban información sensible sin cifrarla ni bloquearla, dificultando su detección.

Acciones clave para mitigar este riesgo incluyen adoptar un modelo de confianza cero, realizar auditorías periódicas de IAM y roles para eliminar privilegios excesivos, implementar monitorización avanzada con herramientas como AWS GuardDuty, Microsoft Sentinel y soluciones CSPM (Cloud Security Posture Management) de Sophos para detectar anomalías y backdoors, y garantizar la automatización y visibilidad multinube mediante plataformas que correlacionen eventos y alertas en tiempo real. La nube no es insegura por naturaleza, pero su complejidad exige un cambio de mentalidad. La persistencia del atacante es una amenaza silenciosa que puede comprometer la continuidad del negocio, y para los líderes empresariales, invertir en seguridad adaptativa, visibilidad y gobernanza no es opcional: es la única forma de garantizar que la innovación en la nube no se convierta en un riesgo existencial.

Fuentes y referencias

- IBM – Arquitectura en la nube
- Fortinet – Firewall en la nube
- *Fortinet – Informe de seguridad en la nube 2024*
- Sophos – Cloud Optix
- Kaspersky – Amenazas avanzadas persistentes
- Bitdefender – Persistencia vía Hyper-V
- *Gartner – IAM en entornos multicloud*
- 17 riesgos de seguridad de la computación en la nube en 2025
- Informe 2025 de Tenable: Riesgos para la seguridad en la nube | Tenable®
- Amenazas de la Nube en Aumento: las Tendencias de Alertas Muestran que los Atacantes se Centran cada vez Más en IAM y Exfiltración
- Las cadenas de suministro y los entornos cloud serán zonas de especial peligro en 2025 | Endpoint | IT Digital Security
- *Un informe de Veeam revela que cerca del 70 % de las organizaciones siguen sufriendo ciberataques a pesar de las defensas mejoradas*

Panorama Global

CloudFlare

NOTICIA BeIT

El 18 de noviembre de 2025, Cloudflare experimentó una interrupción global que afectó a millones de usuarios y empresas en todo el mundo. El incidente comenzó alrededor de las 11:20 UTC y se prolongó por más de cinco horas, impactando servicios críticos como X (Twitter), ChatGPT, Canva, Uber, Spotify y plataformas de videojuegos como League of Legends. La causa no fue un ciberataque, sino un error interno derivado de un cambio en los permisos de una base de datos que generó entradas duplicadas en un archivo clave para la gestión de bots. Este archivo creció más de lo previsto, superando los límites del software encargado de enrutar el tráfico, lo que provocó fallos en cadena en la infraestructura global de Cloudflare. El impacto fue significativo porque la compañía gestiona cerca del 20% del tráfico mundial de Internet, lo que generó un efecto dominó que paralizó gran parte de la web, ocasionando pérdidas millonarias en comercio electrónico y publicidad, además de una caída del 5% en sus acciones.

Este evento pone en evidencia la dependencia crítica de las organizaciones en proveedores de infraestructura global y la necesidad de contar con planes de contingencia robustos. Como Grupo BeIT, podemos ofrecer soluciones estratégicas para mitigar riesgos ante incidentes similares. Primero, implementar arquitecturas multicloud y redundancia geográfica que permitan distribuir cargas entre diferentes proveedores, evitando puntos únicos de falla. Segundo, establecer sistemas de monitoreo avanzado con alertas proactivas que detecten anomalías en tiempo real y activen protocolos automáticos de conmutación por error. Tercero, diseñar planes de continuidad de negocio y recuperación ante desastres que incluyan pruebas periódicas y simulaciones para garantizar la resiliencia operativa. Además, podemos asesorar en la adopción de tecnologías edge y CDN híbridas que reduzcan la dependencia de un solo proveedor, así como en la integración de soluciones de seguridad que protejan la disponibilidad y la integridad de los servicios. Con estas medidas, se minimiza el impacto de una caída global y se fortalece la confianza y estabilidad de las operaciones digitales en entornos cada vez más interconectados.

Referencias

- https://www.cloudflarestatus.com/incidents/xyz
- https://techcrunch.com/2025/11/18/cloudflare-outage/
- https://www.theverge.com/2025/11/18/cloudflare-global-outage
- https://www.bleepingcomputer.com/news/security/cloudflare-outage-explained/
- https://downdetector.com/
- https://blog.cloudflare.com/
- https://www.reuters.com/technology/cloudflare-outage-impact-2025-11-18/
- https://www.cnbc.com/2025/11/18/cloudflare-outage-major-sites-down.html

Introducción a la detección de anomalías con XDR y SIEM

Los ciberdelincuentes evolucionan más rápido que la capacidad de respuesta tradicional, la detección de anomalías se ha convertido en un pilar estratégico para la resiliencia empresarial. Las organizaciones ya no pueden depender únicamente de sistemas reactivos; necesitan plataformas que integren visibilidad, inteligencia y automatización. Aquí es donde convergen dos tecnologías críticas: **Extended Detection and Response (XDR) y Security Information and Event Management (SIEM).**

XDR surge como una evolución natural del EDR, extendiendo la detección y respuesta a múltiples capas: endpoints, redes, correo electrónico, cargas en la nube y aplicaciones. IBM lo define como una arquitectura abierta que elimina brechas de visibilidad y permite flujos de trabajo optimizados para la investigación y respuesta a amenazas, integrando herramientas heterogéneas en una sola interfaz unificada. Fortinet refuerza esta visión con FortiXDR, que aplica inteligencia artificial para correlacionar eventos y ejecutar acciones automatizadas, reduciendo el tiempo medio de respuesta y mitigando riesgos hasta en un 99%.

Por su parte, SIEM, lejos de ser obsoleto, ha evolucionado hacia plataformas inteligentes que incorporan análisis de comportamiento (UEBA), machine learning y capacidades de orquestación. IBM QRadar SIEM, por ejemplo, permite reducir en un 90% el tiempo de investigación de incidentes y ofrece más de 700 integraciones prediseñadas para garantizar visibilidad completa del ecosistema de seguridad. Gartner confirma que los SIEM líderes en 2025 son cloud-native, integran IA y marketplaces ampliados, y se alinean con marcos como MITRE ATT&CK para mapear tácticas y técnicas avanzadas.

La interconexión entre XDR y SIEM no es opcional, sino estratégica. Mientras SIEM centraliza y correlaciona eventos para cumplir normativas y ofrecer trazabilidad, XDR añade contexto y capacidad de respuesta automatizada, reduciendo la fatiga de alertas y acelerando la contención. Dell Technologies, en alianza con CrowdStrike, ejemplifica esta tendencia al ofrecer servicios MDR basados en XDR para entornos multicloud, integrando telemetría y análisis predictivo para anticipar ataques sofisticados.

GrupoBeIT, con su propio SIEM para **TIER 1 y TIER 2,** y en alianza estratégica con **Cyberhawk para TIER 3,** apuesta por la convergencia SIEM-XDR como pilar fundamental para una ciberseguridad avanzada. Esta integración permite visibilidad completa del ecosistema digital, correlación inteligente de eventos y reducción significativa del MTTR (Mean Time to Respond). Incorporamos capacidades de análisis en tiempo real, detección proactiva de amenazas, y gestión integral de vulnerabilidades, complementadas con automatización de respuestas y flujos orquestados para incidentes críticos.

En este marco, nuestra propuesta de Ethical Hacking Modular se convierte en un complemento estratégico, no solo técnico. Ofrecemos a las empresas de México y del mercado internacional una visión desde la perspectiva del adversario, permitiendo a los líderes anticipar movimientos y responder con agilidad. La integración de análisis de vulnerabilidades, pentesting, revisión de código seguro y monitoreo de la Dark Web – Deep Web se conecta directamente con nuestro ecosistema SIEM-XDR, cerrando el ciclo entre detección, validación y remediación. Esto no solo fortalece la ciberdefensa, sino que posiciona a la organización como resiliente, proactiva y preparada para enfrentar los desafíos digitales del presente y del futuro.

Nuestra arquitectura está diseñada para escalar en entornos híbridos y multi-cloud, garantizando cumplimiento normativo (ISO 27001, GDPR) y resiliencia frente a ataques sofisticados como ransomware, APT y phishing avanzado. Con esta propuesta integral de GrupoBeIT protegemos, optimizamos la postura de seguridad de las organizaciones, alineando la defensa con los objetivos de negocio.

En la actualidad el mercado respalda esta transformación de SIEM y XDR: según Mordor Intelligence, el segmento SIEM crecerá de $9.61 mil millones en 2024 a más de $17 mil millones en 2029, impulsado por la integración con XDR y SOAR, mientras que XDR registra tasas de crecimiento superiores al 20% anual. Este dinamismo refleja una realidad ineludible: las empresas que no adopten estas tecnologías quedarán expuestas a riesgos operativos, regulatorios y reputacionales.

Para las empresas y sus líderes, el llamado a la acción es claro: **invertir en plataformas que combinen la capacidad analítica del SIEM con la respuesta inteligente del XDR**. No se trata solo de tecnología, sino de estrategia: reducir la complejidad, optimizar recursos y garantizar continuidad de negocio en un entorno donde cada segundo cuenta. La pregunta no es si su organización necesita XDR y SIEM, sino **cuándo y cómo los integrará para transformar su postura de seguridad en una ventaja competitiva**.

Referencias

- IBM: ¿Qué es XDR?
- IBM QRadar SIEM
- Fortinet: FortiXDR
- Gartner Magic Quadrant SIEM 2025
- Dell Technologies y CrowdStrike MDR
- Huawei HiSec Insight
- Cyberhawk SIEM XDR
- Mordor Intelligence: SIEM Market

BURÖMC SEGURIDAD INFORMÁTICA

Grupo BeIT

ELIT INFRASTRUCTURE SERVICES

ETHICAL HACKING MODULAR

¡La ciberseguridad hoy exige soluciones a la medida!

Por eso, lanzamos nuestra solución de Ethical Hacking Modular para IT, diseñada para adaptarse a los desafíos específicos de cada empresa e industria.

Con un enfoque flexible y escalable, puedes elegir los módulos que mejor se ajusten a tus necesidades de protección integral:

Análisis de Vulnerabilidades

Evaluación integral de cada sitio para identificar riesgos antes de que se conviertan en incidentes.

Pruebas de Penetración (Pentesting)

Simulación de ataques en modalidad caja blanca, gris o negra, según la realidad de tus sitios.

Monitoreo de Dark Web y Deep Web

Detección temprana de filtraciones y exposición de datos relacionados con tus sitios y assets críticos.

Análisis de Rendimiento con Smart Collector

Optimización del desempeño de tus dispositivos clave para mantener la continuidad operativa.

Análisis de Código

Revisión exhaustiva y segura de proyectos de código para prevenir vulnerabilidades desde su origen.

¡Agendemos una cita!

Contáctanos

Para más información o una propuesta a la medida, comunícate o contesta directamente a este correo.
Nota: Aplican términos y condiciones. Precio sujeto a dimensionamiento de cada proyecto.

+52 56 5100 8613

admmarketing@buromc.com