DIGISOC | rubrik | assured

WEBINAR → DATASHEET

RECUPERACIÓN DE IDENTIDADES EN TIEMPOS DE IA

TOP LATAM #07 MSSP Alert | FIRST | GLOBAL CYBER ALLIANCE

www.digisoc.net

CIBERSEGURIDAD MODERNA

Resiliencia en Tiempos de Inteligencia Artificial

La ciberseguridad se ha obsesionado con construir muros más altos. El panorama actual nos obliga a aceptar una nueva realidad: **Debemos prepararnos para la recuperación garantizada.**

Los atacantes ya no entran a la fuerza. **Hoy en día, los cibercriminales simplemente se loguean.**

LA IDENTIDAD ES EL NUEVO PERÍMETRO

El Nuevo Campo Batalla

La Exposición de la Identidad

Las identidades se han convertido en el vector de ataque más vulnerable y crítico. No son incidentes aislados; es el núcleo operativo de las organizaciones.

- **71% de los ataques en Latam** inician con una credencial comprometida.
- Más del **97% de los ataques** de identidad están basados en contraseñas.

- Las credenciales válidas se venden por pocos dólares en el mercado negro, permitiendo acceso directo.
- El crecimiento de identidades (humanas y no humanas) se multiplicará un 240% en los próximos meses.

Evolución **de las Amenazas con IA**

Password Spray

La IA permite probar contraseñas comunes (ej. "Password123") contra miles de usuarios simultáneamente. Al rotar usuarios, se evaden los mecanismos tradicionales de bloqueo de cuenta.

Phishing Sofisticado

Ya no hay errores ortográficos. Los atacantes utilizan infraestructura legítima, dominios confiables y aplicaciones con consentimientos válidos, haciendo el ataque indetectable para el usuario.

Robo de Tokens

La evolución más peligrosa. Al robar tokens de sesión activos, los atacantes ya no necesitan proporcionar contraseñas ni completar verificaciones MFA (Múltiple Factor de Autenticación).

Disponibilidad ≠ Recuperación

El Mito de la Nube Segura

Pensar **"está en la nube, no pasa nada" es un error crítico.** La alta disponibilidad (99.99%) garantiza que el servicio esté arriba, **pero no garantiza la recuperación** ante un ataque.

Casos recientes demuestran que un error humano o un ataque pueden eliminar entornos completos, incluyendo sus respaldos alojados en el mismo proveedor.

Responsabilidad Compartida: La recuperación de configuraciones, dependencias, políticas, grupos de identidad e integraciones (Active Directory, Entra ID) recae enteramente en la organización.

LA VELOCIDAD DE LA IA

27 Segundos

El Tiempo de Movimiento Lateral

Gracias a la automatización impulsada por la Inteligencia Artificial, el tiempo promedio que le toma a un atacante vulnerar un sistema inicial y realizar un movimiento lateral ha cambiado drásticamente.

Históricamente, el tiempo de latencia promedio era de **27 minutos**. Hoy, los ataques orquestados pueden expandirse y comprometer toda la red en solo **27 segundos**.

Anatomía de un Ataque a Identidades

Fase del Ataque	Vectores y Tácticas Clave	Impacto en la Organización
1. Riesgo Inicial	Errores humanos, cuentas obsoletas, contraseñas sin cambios y cuentas de servicio vulnerables.	Punto de entrada sigiloso. Miles de peticiones ocultas en el tráfico normal.
2. Exposición / Persistencia	Movimientos laterales, establecimiento de Backdoors e identidades con privilegios excesivos.	Compromiso profundo del sistema. Los EDR pueden ser vulnerados o apagados.
3. Interrupción Total	Cifrado de backups, inhabilitación de administradores y caída de Active Directory.	Operación ininterrumpida pero **sin capacidad de acceso**. Empresa paralizada.

28

DÍAS DE LATENCIA

El Costo del Tiempo de Inactividad

La Realidad de la Recuperación Manual

En un entorno tradicional, sin herramientas especializadas, simplemente reconfigurar un Active Directory y restablecer relaciones de confianza puede tomar entre **5 y 7 días**.

Encontrar una copia limpia libre de malware (evitando la reinfección) y restaurar todo el bosque de identidades puede paralizar las operaciones hasta por **28 días**.

PLATAFORMA RUBRIK

Ciber - Resiliencia Activa

Pasando de una postura reactiva y de prevención, **a una postura proactiva que garantiza la recuperación** de identidades, on-premise y en la nube.

Pilares **de las Resiliencias** de Identidades

Visibilidad Proactiva

Detección en tiempo real de anomalías (DSPM). Monitoreo de comportamientos, configuraciones incorrectas y comparación de entornos productivos vs. respaldos para detectar desviaciones maliciosas.

Protección Inmutable

Respaldo de identidades diseñado bajo un modelo Zero Trust. Datos inmutables, aislados lógicamente y cifrados. No pueden ser alterados, borrados ni cifrados por el atacante (Ransomware).

Recuperación Rápida

Restauración granular de objetos, dependencias o todo el bosque de identidades (Active Directory, Entra ID) en segundos. Recuperación automatizada sin fricción ni riesgo de reinfección.

Contexto Accionable Y Visión 360

Gestión Proactiva del Riesgo

La plataforma unifica la visibilidad de identidades, datos estructurados, no estructurados y aplicaciones SaaS, mapeados al framework MITRE ATT&CK.

- **Análisis de "Blast Radius":** Identifica exactamente qué alcance tuvo el ataque.
- **Análisis Forense:** Rastreo de quién tuvo acceso, a qué datos sensibles y con qué privilegios.

- **Correlación de Eventos:** Integración con SIEM y EDR (Palo Alto, CrowdStrike) para detectar movimientos laterales ocultos.
- **Flujos Automatizados:** Capacidad de deshabilitar o rotar identidades en riesgo inmediatamente.

DIGISOC | rubrik | assured

WEBINAR 22 DE JULIO

RECUPERACIÓN DE IDENTIDADES EN TIEMPOS DE IA

Regístrese y solicite un **Cyber Resiliency Assessment**

www.digisoc.net

DIGISOC

Gracias.

We protect.

www.digisoc.net