INSTITUTO DE CIBERSEGURIDAD E INTELIGENCIA DIGITAL

ICEID

BLUE TEAM
FIELD GUIDE

30 ESCENARIOS REALES DE RESPUESTA A INCIDENTES

GABRIEL GARCIA PÉREZ

Guía Maestra de Respuesta a Incidentes: Marco Operativo del SOC

1. Introducción y Propósito Operativo

La eficacia de un Centro de Operaciones de Seguridad (SOC) no se mide únicamente por su capacidad de detección, sino por la precisión y velocidad de su respuesta. En un ecosistema de amenazas donde el "tiempo de permanencia" (Dwell Time) del atacante determina la magnitud del impacto financiero y reputacional, la estandarización de procedimientos deja de ser una opción para convertirse en un imperativo estratégico.

Este documento compila 30 playbooks especializados, diseñados para transformar el caos intrínseco de un incidente de ciberseguridad en un proceso de defensa metódico, repetible y auditable. El objetivo es proporcionar al analista, desde niveles iniciales hasta especialistas en respuesta a incidentes (IR), una hoja de ruta táctica que minimice la incertidumbre y garantice la preservación de evidencia crítica en cada fase del ciclo de vida del ataque.

2. Fundamentos de la Metodología de Respuesta

Cada playbook contenido en esta guía se alinea con los marcos de trabajo internacionales NIST SP 800-61 y el modelo de fases de SANS Institute. No obstante, este manual va más allá de la teoría, enfocándose en la ejecución técnica bajo presión. Los procedimientos aquí descritos se rigen por tres principios fundamentales:

- **Rigor Forense**: Cada acción de contención debe considerar la integridad de la evidencia. El análisis debe preceder a la modificación del entorno siempre que la criticidad del negocio lo permita.
- **Reducción del MTTR (Mean Time To Respond):** La estructura lógica de estos playbooks está optimizada para que el analista identifique los Indicadores de Compromiso (IoC) y proceda al aislamiento del activo de forma inmediata.

- Adaptabilidad Táctica: Si bien los playbooks ofrecen una ruta definida, se insta al analista a mantener un pensamiento crítico. Los adversarios ajustan sus TTP (Técnicas, Tácticas y Procedimientos); por tanto, estas guías deben ser interpretadas como una base sólida que permite la improvisación informada.

3. Clasificación y Priorización de Incidentes

Para asegurar una asignación eficiente de recursos, el SOC utiliza una matriz de severidad basada en dos variables: el Impacto (grado de afectación a la confidencialidad, integridad o disponibilidad) y la Urgencia (velocidad con la que el incidente se propaga o causa daño).

Los escenarios incluidos en esta guía cubren las siguientes categorías de amenaza:

1. Vectores de Malware y Código Dañino.
2. Compromiso de Identidad y Acceso.
3. Explotación de Infraestructura y Aplicaciones.
4. Incidentes en Ecosistemas Cloud y Cadena de Suministro.
5. Amenazas Internas y Exfiltración de Datos.

4. Responsabilidad del Analista

El uso de estos playbooks conlleva la responsabilidad de documentar cada hallazgo en el sistema de gestión de casos (Ticketing/Case Management). La fase de "Lecciones Aprendidas" es el componente más valioso para la mejora continua del SOC; un incidente que no se documenta adecuadamente es una oportunidad perdida para fortalecer las defensas de la organización.

Este compendio constituye el estándar operativo de nuestra unidad de ciberdefensa. Su cumplimiento estricto garantiza que, independientemente de la complejidad del ataque, la respuesta de la organización sea coherente, profesional y técnica.

Estratégica y Táctica para la Ciberdefensa

Propósito del Documento

Este documento fundamental compila una serie integral y detallada de **Playbooks de Respuesta a Incidentes del SOC** (Centro de Operaciones de Seguridad). Su objetivo primordial es establecer una guía estructurada, táctica y de acción inmediata, asegurando una respuesta coherente, eficiente y estandarizada ante un amplio espectro de escenarios de ciberseguridad que puedan comprometer la integridad, confidencialidad y disponibilidad de los activos de información de la organización.

Estructura y Fases del Proceso de Respuesta

Cada *playbook* está meticulosamente diseñado siguiendo el marco de gestión de incidentes reconocido en la industria, dividiéndose en seis fases críticas. Este enfoque garantiza que cada etapa del ciclo de vida del incidente sea abordada con procedimientos claros y responsables definidos:

1. **Preparación (Preparation):** Establece los requisitos previos, incluyendo la revisión de políticas, la disponibilidad de herramientas forenses y de respuesta, la capacitación del equipo y la actualización de listas de contactos de escalamiento.
2. **Detección y Análisis (Detection & Analysis):** Se enfoca en el monitoreo de alertas de seguridad (SIEM, EDR), la confirmación de la naturaleza del incidente (verdadero positivo), la clasificación del incidente, y la recopilación inicial de datos para entender el alcance y la causa raíz.
3. **Contención (Containment):** Define las acciones inmediatas y estratégicas para limitar la propagación del ataque y detener el daño. Esto puede incluir el aislamiento de *hosts* comprometidos, la desactivación de cuentas o la implementación de reglas de *firewall* temporales.
4. **Erradicación (Eradication):** Detalla los pasos para eliminar completamente la amenaza del entorno. Esto incluye la limpieza de *malware*, la aplicación de parches, el cierre de la vulnerabilidad explotada y la rotación de credenciales comprometidas.
5. **Recuperación (Recovery):** Se centra en la restauración de los sistemas y

servicios afectados a su estado operativo normal (antes del incidente), la validación de la seguridad del entorno y la monitorización intensiva posterior al incidente.

6. **Lecciones Aprendidas (Lessons Learned):** Es la fase post-incidente donde se realiza un análisis retrospectivo para identificar qué funcionó, qué no y cómo mejorar los procesos, la tecnología y la preparación del equipo, actualizando los *playbooks* según sea necesario.

Clasificación del Incidente

Cada *playbook* incluye criterios específicos para la clasificación del incidente, lo cual es crucial para la asignación de recursos y la activación de los canales de comunicación apropiados:

- **Categoría:** Identifica el tipo de incidente (Ej: Intrusión, *Malware*, Denegación de Servicio, *Phishing*).
- **Severidad (Severity):** Mide el impacto técnico potencial en los activos de la organización (Ej: Bajo, Medio, Alto, Crítico).
- **Prioridad (Priority):** Determina la urgencia de la respuesta en función de la severidad y el impacto al negocio (Ej: P1-Inmediata, P2-Alta, P3-Media).

Escenarios Críticos Cubiertos

Los *playbooks* están diseñados para abordar los incidentes de ciberseguridad de mayor impacto potencial, detallando las acciones, los puntos de recopilación de evidencia y las herramientas típicas (EDR, SIEM, *Network Forensics*, *Cloud Security Tools*) a utilizar para los siguientes escenarios críticos:

- **Infección por Ransomware:** Procedimientos para el aislamiento rápido, identificación de la cepa, determinación del vector de infección y estrategias de recuperación sin pago.
- **Exfiltración de Datos por Amenaza Interna (*Insider Threat*):** Métodos de detección basados en comportamiento anómalo, monitoreo de acceso a datos sensibles y acciones legales/disciplinarias de contención.
- **Compromiso de Cuenta en la Nube (Cloud Account Compromise):** Pasos

para la revocación inmediata de tokens de sesión, análisis de registros de auditoría en la nube y verificación de cambios de configuración no autorizados.

- **Explotación de Aplicación Web (Web Application Exploitation):** Guía para el análisis de logs del WAF y del servidor web, identificación del *exploit* y aplicación de parches o mitigaciones temporales.
- **Ataque a la Cadena de Suministro (Supply Chain Attack):** Protocolos para la identificación de *software* comprometido de terceros, evaluación del alcance de la intrusión y colaboración con proveedores.
- **Infección por Malware a Través de Dispositivo USB:** Pasos forenses para el análisis del dispositivo, identificación de la carga útil del *malware* y barrido de la red para confirmar la no propagación.

Objetivo Estratégico

El objetivo general de estos *Playbooks* es crucial para la resiliencia operativa: **estandarizar los procedimientos**, asegurando que todos los analistas del SOC sigan una ruta predefinida y probada; **reducir el tiempo de respuesta** (MTTR - *Mean Time To Respond*), minimizando el "tiempo de permanencia" del atacante en el sistema; y, en última instancia, **mitigar el impacto** económico, operativo y reputacional de incidentes de seguridad, transformando una respuesta caótica en una defensa metódica y efectiva.

1-. Playbook 1: Infección por Ransomware

Escenario

Un endpoint o servidor muestra signos de actividad de ransomware, como cifrado de archivos, notas de rescate o alertas de herramientas EDR/XDR.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Malware - Ransomware
Severidad	Alta
Prioridad	Crítica (debido al impacto potencial en el negocio y la pérdida de datos)
Fuentes de Detección	EDR/XDR, SIEM, Reporte de Usuario, Antivirus, NDR

Fases y Acciones

1. Preparación (Configuración Previa al Incidente)

- **Estrategia de respaldo y recuperación:** Realizar copias de seguridad offline periódicas y pruebas de restauración.
- **Protección de endpoints:** Implementar EDR con detección de comportamiento y funciones de reversión (rollback).
- **Concienciación de usuarios:** Capacitación sobre el manejo seguro de correos electrónicos y medios USB.
- **Cobertura de registros (Logging):** Logs de Windows, Sysmon, registros de acceso a archivos y flujos de red.
- **Suscripciones a IOCs y feeds de amenazas:** Incluir indicadores específicos de ransomware.

2. Detección y Análisis

- **Confirmar actividad de ransomware:** Alerta de EDR, presencia de nota de rescate, extensiones de archivos cifrados.
- **Aislar el host afectado:** Desconectar de la red o usar la función de contención del EDR.
- **Identificar la cepa de ransomware:** Basado en la nota de rescate, hash del archivo o patrón del nombre de archivo.
- **Analizar logs y comportamiento:** Rastrear la fuente de ejecución, movimiento lateral, tareas programadas sospechosas o servicios.
- **Mapeo MITRE ATT&CK:** T1486 (Datos Cifrados para Impacto), T1059 (Ejecución de Comandos), T1021.002 (Movimiento Lateral SMB).

3. Contención

- **Aislar sistemas afectados:** Bloquear en el switch, firewall o vía EDR.
- **Deshabilitar cuentas infectadas:** Especialmente si se usan para movimiento lateral.
- **Bloquear comunicación externa:** Prevenir comunicación con C2 (Comando y Control) y el intercambio de claves por internet.
- **Snapshot de sistemas impactados:** Para análisis forense (si se requiere).

4. Erradicación

- **Eliminar artefactos de malware:** Borrar archivos de ransomware, scripts y tareas programadas.
- **Parchear vulnerabilidades:** Abordar vectores de ataque explotados como RDP, SMB o software desactualizado.

- **Realizar escaneo completo de Antivirus/EDR:** En todos los hosts dentro de la VLAN/subred afectada.
- **Validar eliminación:** Asegurar que no queden mecanismos de persistencia (claves de registro, elementos de inicio, servicios).

5. Recuperación

- **Restaurar desde respaldo limpio:** Confirmar que los respaldos no estén afectados antes de restaurar.
- **Reconstruir sistemas si es necesario:** Para sistemas sin respaldos limpios.
- **Monitorear sistemas restaurados:** Usar SIEM y EDR para asegurar que no ocurra reinfección.
- **Restablecer contraseñas:** Particularmente para usuarios privilegiados y afectados.

6. Lecciones Aprendidas e Informes

- **Realizar revisión post-incidente:** Analizar causa raíz, método de acceso inicial y eficiencia de la respuesta.
- **Actualizar reglas de detección:** Mejorar las reglas de correlación y disparadores en SIEM y EDR.
- **Documentar hallazgos:** Incluir indicadores, sistemas afectados y línea de tiempo.
- **Compartir IOCs:** Internamente y con comunidades de inteligencia de amenazas si está permitido.

Herramientas Típicas: SIEM (FortiSIEM, Google Chronicle), EDR/XDR (Kaspersky EDR,CrowdStrike, Cortex), Herramientas Forenses, Sistemas de Respaldo (Veeam, Rubrik).

2.- Playbook 2: Exfiltración de Datos por Insider (Amenaza Interna)

Escenario

Un empleado interno, contratista o usuario privilegiado intenta o logra exfiltrar datos sensibles a través de canales no autorizados como correo personal, almacenamiento en la nube, medios extraíbles o herramientas de transferencia de archivos.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Amenaza Interna - Exfiltración de Datos
Severidad	Alta (especialmente para datos regulados o confidenciales)
Prioridad	Alta a Crítica
Fuentes de Detección	DLP, SIEM, Logs de Proxy, CASB, EDR, Gateway de Correo

Fases y Acciones

1. Preparación

- **Definir categorías de datos sensibles:** Clasificar archivos: PII, datos financieros, secretos comerciales.
- **Implementación de DLP:** Establecer políticas de detección en endpoints, red y correo.
- **Monitoreo de actividad:** Registrar acceso de usuarios, transferencia de archivos y uso de aplicaciones en la nube.
- **Capacitación sobre riesgo interno:** Educar a los empleados sobre el manejo aceptable de datos.
- **Cumplimiento de control de acceso:** Acceso basado en roles, mínimo privilegio, segmentación.

2. Detección y Análisis

- **Disparar alerta de detección:** Violación de DLP, descargas anormales, adjuntos de correo grandes, subidas de archivos inusuales.
- **Analizar logs de acceso:** Buscar acceso a archivos, tiempos de transferencia y destinos.
- **Investigar comportamiento del usuario:** Verificar escalada de privilegios, anomalías en hora de inicio de sesión, intentos fallidos.
- **Confirmar intención o mala configuración:** Determinar si la acción fue maliciosa, accidental o una brecha en la política.
- **Mapeo MITRE ATT&CK:** T1020 (Exfiltración Automatizada), T1048 (Exfiltración sobre Protocolo Alternativo), T1537 (Transferir Datos a Cuenta en la Nube).

3. Contención

- **Suspender acceso del usuario:** Deshabilitar temporalmente la cuenta si el riesgo es alto.
- **Bloquear canales de exfiltración:** Revocar uso compartido en la nube, bloquear correo a dominios externos, deshabilitar puertos USB.
- **Aislar endpoints:** Si se sospecha de software malicioso en el dispositivo del usuario.
- **Preservar evidencia forense:** No apagar sistemas a menos que sea necesario; capturar datos volátiles si es posible.

4. Erradicación

- **Eliminar herramientas no autorizadas:** Ej. apps personales de transferencia de archivos, extensiones fraudulentas.
- **Aplicar políticas más estrictas:** Ajustar reglas DLP o firewall para bloquear intentos repetidos.
- **Corregir permisos mal configurados:** Reducir recursos compartidos sobreexpuestos, acceso a nivel de carpeta.

5. Recuperación

- **Restaurar acceso (si se justifica):** Después de confirmar que no hay amenaza continua.
- **Notificar a las partes interesadas:** Equipos legal, RRHH, cumplimiento y gestión.
- **Realizar evaluación de impacto:** Confirmar si los datos fueron realmente exfiltrados y su sensibilidad.

6. Lecciones Aprendidas e Informes

- **Documentar el incidente:** Línea de tiempo, tipos de datos, intención del actor, sistema utilizado.
- **Fortalecer el monitoreo:** Mejorar alertas sobre tipos de archivos específicos y métodos de transferencia.
- **Realizar capacitación de usuario o acción disciplinaria:** Si se confirma incidente malicioso o negligente.
- **Reportar a reguladores:** Si la ley lo requiere (ej. GDPR, leyes locales de protección de datos).

Playbook 3: Compromiso de Cuenta en la Nube

Escenario

Un atacante obtiene acceso no autorizado a la cuenta en la nube de un usuario, posiblemente a través de phishing, pulverización de contraseñas (password spraying), robo de tokens o abuso de OAuth. El atacante puede acceder al correo, almacenamiento o infraestructura.

Clasificación del Incidente

Categoría	**Detalles**

Tipo de Incidente	Compromiso de Identidad - Cuenta en la Nube
Severidad	Alta (especialmente si involucra cuenta privilegiada)
Prioridad	Crítica si se observa movimiento lateral o acceso a datos
Fuentes de Detección	SIEM, CASB, Logs nativos de la nube (AWS CloudTrail, Azure AD), Gateway de correo, EDR

Fases y Acciones

1. Preparación

- **Habilitar registro en la nube:** Usar AWS CloudTrail, Logs de inicio de sesión de Azure, logs de auditoría de Google Workspace.
- **Implementar MFA:** Hacerlo obligatorio para todos los usuarios.
- **Monitorear comportamiento:** Integrar logs de nube en SIEM, detección de anomalías.
- **Restricciones y alertas:** Alertar sobre viajes imposibles o accesos desde IPs desconocidas.

2. Detección y Análisis

- **Detectar anomalías de inicio de sesión:** Inicios fallidos, viajes imposibles, alertas de evasión de MFA.
- **Correlacionar con inteligencia de amenazas:** Coincidir IPs/User Agents con feeds de IOC.
- **Verificar logs de acceso:** Revisar actividad en buzón, almacenamiento, IAM o API.

- **Buscar escalada de privilegios:** Identificar creación de cuentas traseras (backdoor).
- **Mapeo MITRE ATT&CK:** T1078 (Cuentas Válidas), T1087.004 (Descubrimiento de Cuenta en Nube).

3. Contención

- **Revocar sesiones y tokens:** Invalidar todas las sesiones activas y tokens OAuth.
- **Restablecer contraseña:** Imponer contraseña fuerte y habilitar MFA.
- **Suspender cuenta:** Si se confirma compromiso de alto impacto.
- **Bloquear direcciones IP:** Si el atacante usó IPs maliciosas conocidas.

4. Erradicación

- **Eliminar reglas de bandeja de entrada maliciosas:** Limpiar reglas de reenvío o filtros ocultos.
- **Deshabilitar aplicaciones fraudulentas:** Revocar consentimiento para apps de terceros no autorizadas.
- **Revisar roles de administración:** Revertir acceso administrativo no autorizado.

5. Recuperación

- **Rehabilitar acceso:** Tras asegurar que se restableció el control total.
- **Notificar usuarios:** Especialmente si ocurrió compromiso de correo empresarial (BEC).
- **Monitorear anomalías post-recuperación:** Usar SIEM/CASB por 7-14 días.
- **Explotación de Aplicación Web:** Ataque vía vulnerabilidad web (SQLi, XSS, RCE) detectado por WAF/SIEM.

Playbook 4: Explotación de Aplicación Web

Escenario:

Se detecta un ataque exitoso o intento activo de explotación de una vulnerabilidad de aplicación web (por ejemplo, Inyección SQL, Cross-Site Scripting (XSS), Ejecución Remota de Código (RCE)) a través de un WAF (Web Application Firewall), un SIEM o logs de servidor web, afectando la disponibilidad o integridad de la aplicación y/o sus datos subyacentes.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Explotación de Aplicación - Vulnerabilidad Web
Severidad	Alta (especialmente si afecta a la lógica de negocio o datos sensibles)
Prioridad	Crítica (acción inmediata requerida para detener la explotación)
Fuentes de Detección	WAF, SIEM, Logs de Aplicación, Escáneres de Vulnerabilidades, Reporte de Usuario/Público

Fases y Acciones

1. Preparación

- **Inventario y Perfil:** Mantener un inventario actualizado de todas las aplicaciones web, sus componentes, versiones y sus flujos de datos sensibles.
- **Controles de Seguridad:** Implementar y mantener un WAF actualizado, y realizar escaneos de vulnerabilidades de forma periódica.
- **Logging Detallado:** Configurar logs de acceso y errores de la aplicación web, incluyendo parámetros de entrada y encabezados para análisis forense.
- **Planes de Backup:** Contar con imágenes y copias de seguridad de la

aplicación y la base de datos para restauraciones rápidas.

2. Detección y Análisis

- **Confirmar la Explotación:** Revisar logs del WAF y la aplicación en busca de payloads maliciosos, códigos de error atípicos o comandos del sistema no esperados.
- **Determinar el Vector de Ataque:** Identificar la vulnerabilidad específica (ej. ***GET /vulnerable.php?id=' OR '1'='1')*** y la función de la aplicación afectada.
- **Evaluar el Alcance y el Impacto:** Confirmar si el atacante logró acceso, modificó datos, o exfiltró información.
- **Captura de Tráfico:** Si es posible, capturar paquetes de red para un análisis más profundo de la sesión del atacante.
- **Mapeo MITRE ATT&CK:** T1190 (Explotación de Aplicación Web), T1505 (Ejecución de Cargas Web), T1078 (Cuentas Válidas).

3. Contención

- **Bloqueo en el WAF:** Aplicar una regla de bloqueo temporal y específica en el WAF o en el firewall perimetral para el vector de ataque o la IP de origen (si es viable).

- **Deshabilitar la Función:** Si el impacto es crítico y no se puede mitigar de inmediato, deshabilitar la funcionalidad o el endpoint web vulnerable.
- **Snapshot de la Máquina:** Crear una imagen del servidor (VM) para análisis forense si la explotación fue RCE o implicó el sistema operativo.
- **Desconexión de la Base de Datos:** Si hay actividad maliciosa directa en la base de datos (SQLi), aislar o limitar temporalmente su conectividad.

4. Erradicación

- **Parche de Código:** Aplicar inmediatamente el parche o corrección de código (hotfix) a la vulnerabilidad explotada, siguiendo un proceso de

desarrollo y pruebas seguro.

- **Análisis Post-Contención:** Escanear el código fuente y el servidor en busca de backdoors, web shells o archivos dejados por el atacante.
- **Limpieza de la Base de Datos:** Verificar y revertir cualquier cambio no autorizado de datos.
- **Refuerzo de la Configuración:** Ajustar permisos de archivos y directorios, y actualizar librerías de terceros a versiones seguras.

5. Recuperación

- **Restauración (si aplica):** Si la integridad de la aplicación está comprometida, restaurar la aplicación desde una imagen limpia y parchada.
- **Monitoreo Reforzado:** Poner la aplicación bajo un monitoreo intensivo de tráfico y logs (SIEM, WAF) después de la reactivación.
- **Validación de Funcionalidad:** Realizar pruebas de aceptación y pruebas de penetración enfocadas en la vulnerabilidad corregida para asegurar la solución.
- **Notificación al Público/Reguladores:** Evaluar la necesidad de notificación de violación de datos si se confirma la exposición de PII o datos regulados.

6. Lecciones Aprendidas e Informes

- **Revisión del Proceso:** Documentar la causa raíz de la vulnerabilidad y la eficacia de los controles de seguridad (WAF, escaneos, proceso de desarrollo seguro).
- **Mejora de SDLC:** Integrar pruebas de seguridad más robustas (SAST/DAST) en el ciclo de vida de desarrollo.
- **Actualización de Reglas:** Optimizar las reglas del WAF para prevenir variantes del ataque y mejorar la detección de patrones similares.
- **Capacitación:** Capacitar a los desarrolladores en prácticas de codificación segura (OWASP Top 10) y al equipo de respuesta sobre análisis de logs web.

Playbook 5: Ataque a la Cadena de Suministro

Escenario:

Se detecta un compromiso en un proveedor o socio de la cadena de suministro, cuyo software o acceso a la red de la organización es explotado para entregar código malicioso, robar datos o causar interrupción. Esto puede incluir el compromiso de un componente de software de terceros o un sistema de gestión de proveedores.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Compromiso de la Cadena de Suministro - Software de Terceros/Proveedor
Severidad	Crítica (el impacto puede ser amplio debido a la confianza en la fuente)
Prioridad	Crítica (acción inmediata para aislar la fuente de confianza comprometida)
Fuentes de Detección	SIEM, EDR/XDR, Análisis de Integridad de Archivos (FIM), Inteligencia de Amenazas, Notificación de Proveedor

Fases y Acciones

1. Preparación

- **Inventario de Proveedores/Software:** Mantener un inventario detallado de todos los proveedores críticos, software de terceros y sus dependencias.
- **Monitoreo de Confianza:** Implementar monitoreo de la integridad de los archivos y la reputación de los ejecutables y librerías de terceros.
- **Segmentación de Red:** Aislar o segmentar la red de sistemas que interactúan con proveedores o software de alto riesgo.
- **Pruebas de Seguridad de Proveedores:** Realizar evaluaciones de seguridad periódicas (auditorías, cuestionarios) a los proveedores críticos.

2. Detección y Análisis

- **Identificar el Componente Comprometido:** Determinar qué software, proveedor o canal de actualización fue explotado.
- **Revisar Logs de Integridad:** Buscar cambios no autorizados en archivos binarios o scripts de componentes de terceros.
- **Rastrear la Propagación:** Determinar cuántos sistemas se vieron afectados por el código o actualización maliciosa.
- **Correlación de Inteligencia:** Comparar indicadores de compromiso (IOCs) con alertas de inteligencia de amenazas sobre el ataque a la cadena de suministro.
- **Mapeo MITRE ATT&CK:** T1195 (Compromiso de Software de Terceros), T1547.001 (Persistencia vía Registro de Inicio), T1036.005 (Suplantación de Software Confiable).

3. Contención

- **Aislar Sistemas Afectados:** Desconectar o contener inmediatamente todos los sistemas que ejecutan el software o componente comprometido.
- **Bloqueo de Red:** Bloquear la comunicación de red (saliente y entrante) hacia o desde el proveedor o infraestructura comprometida.
- **Detener el Servicio/Actualización:** Si el vector es una actualización o servicio, deshabilitar temporalmente el mecanismo de distribución o revertir a una versión limpia.
- **Notificación al Proveedor:** Contactar al proveedor de software/servicio para validar el compromiso y coordinar la respuesta.

4. Erradicación

- **Eliminar el Software Malicioso:** Desinstalar o eliminar las versiones comprometidas del software y cualquier *web shell* o *backdoor* instalado.
- **Implementar Parche Verificado:** Solo implementar una versión o parche del proveedor que haya sido verificado por una fuente limpia y confiable.
- **Restablecer Contraseñas/Claves:** Cambiar todas las credenciales y claves

API que pudieran haber sido accedidas o expuestas por el componente comprometido.

- **Escaneo Exhaustivo:** Realizar un escaneo de seguridad en profundidad en todos los sistemas que estuvieron expuestos.

5. Recuperación

- **Restaurar Sistemas Limpios:** Restaurar los sistemas a un estado previo al compromiso (utilizando copias de seguridad limpias).
- **Validación Post-Restauración:** Confirmar la integridad de la aplicación y el componente de terceros antes de volver a la operación normal.
- **Monitoreo Cauteloso:** Mantener un monitoreo elevado en los sistemas restaurados y en los puntos de interacción con el proveedor afectado.
- **Comunicación con Partes Interesadas:** Informar a la dirección, cumplimiento y equipos legales sobre el estado del compromiso.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Determinar cómo el proveedor fue comprometido y por qué la detección falló inicialmente.
- **Revisión del Proceso de Adquisición:** Mejorar los procedimientos de diligencia debida y gestión de riesgos de terceros.

- **Reforzar Controles:** Implementar mejores controles de integridad de código y validación de actualizaciones de terceros.
- **Documentación y Reporte:** Documentar el incidente y sus implicaciones legales/regulatorias (si aplican).

4. **Malware vía Dispositivo USB:** Infección por medios físicos (autorun, ransomware en USB).

Playbook 6: Infección por Malware a Través de Dispositivo USB

Escenario:

Un usuario introduce un dispositivo USB infectado o desconocido, lo que resulta en la ejecución automática de código malicioso (como ransomware, spyware o un troyano) en un endpoint de la organización, o la transferencia de archivos maliciosos.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Malware - Infección vía Dispositivo USB
Severidad	Alta (riesgo de propagación lateral o cifrado de datos)
Prioridad	Crítica (debido a la fuente física de la infección y la necesidad de contención rápida)
Fuentes de Detección	EDR/XDR, Antivirus, Logs de Auditoría de Puertos USB (DLP), Reporte de Usuario

Fases y Acciones

1. Preparación

- **Control de Dispositivos:** Implementar políticas de control de puertos USB (DLP) que limiten el uso de medios extraíbles solo a dispositivos autorizados.
- **Deshabilitar *Autorun*:** Asegurar que la función de ejecución automática de medios extraíbles esté deshabilitada a nivel de política de grupo/SO.
- **Protección de Endpoints:** Configurar el EDR/Antivirus para detectar y bloquear la ejecución de archivos sospechosos desde unidades USB.
- **Concienciación de Usuarios:** Capacitación regular sobre la prohibición de conectar dispositivos USB desconocidos o no autorizados.

2. Detección y Análisis

- **Confirmar la Fuente:** Identificar que la actividad maliciosa comenzó tras la conexión de un dispositivo USB, a través de logs de auditoría de dispositivos o reportes de usuario.
- **Identificar el Malware:** Determinar el tipo de malware (ej. troyano, gusano, ransomware) mediante el análisis de archivos y el comportamiento del proceso en el EDR.
- **Evaluar el Alcance:** Verificar si el malware se ha propagado a otros sistemas en la red o si fue contenido.
- **Mapeo MITRE ATT&CK:** T1200 (Uso de Medios Extraíbles para Ejecución), T1566.004 (Phishing de Medios), T1059 (Ejecución de Comandos y Scripts).

3. Contención

- **Aislar el Endpoint:** Desconectar inmediatamente el host afectado de la red, o usar la función de contención del EDR/NDR.
- **Bloquear a Nivel de Red/Endpoint:** Aplicar reglas en el firewall, EDR o DLP para bloquear cualquier intento de replicación o comunicación del malware detectado.
- **Confiscar el Dispositivo Fuente:** Si el dispositivo USB aún está presente,debe ser incautado y puesto en cuarentena para un análisis forense seguro.
- **Notificar a Zonas de Alto Riesgo:** Alertar a equipos con alta interacción con medios físicos (ej. recepción, laboratorios).

4. Erradicación

- **Eliminar el Malware:** Borrar todos los archivos de malware, claves de registro, y mecanismos de persistencia.
- **Escaneo Exhaustivo:** Realizar un escaneo de seguridad en profundidad en el host afectado, idealmente desde un medio limpio/seguro.
- **Reforzar Controles:** Asegurar que los parches y las últimas firmas de seguridad se hayan aplicado en el host, y validar que la política de control de

USB esté en vigor.

5. Recuperación

- **Restaurar Sistemas:** Si la integridad está comprometida (ej. cifrado de archivos), restaurar el host desde una imagen limpia o copia de seguridad pre-incidente.
- **Restablecer Contraseñas:** Restablecer las contraseñas de las cuentas de usuario que iniciaron sesión o fueron utilizadas en el sistema comprometido.
- **Reconectar Monitoreado:** Reintegrar el sistema a la red, pero manteniéndolo bajo monitoreo intensivo por un período.

6. Lecciones Aprendidas e Informes

- **Análisis Post-Incidente:** Documentar la causa raíz (ej. qué política falló), el tipo de dispositivo USB y la efectividad de la contención.
- **Mejora de Políticas:** Revisar y fortalecer la política de control de dispositivos USB (DLP) y las herramientas de aplicación.
- **Reforzar Capacitación:** Ejecutar una campaña de capacitación de concienciación de seguridad específica sobre el riesgo de los medios extraíbles.
- **Actualizar Reglas:** Crear reglas específicas en el SIEM/EDR para detectar el patrón de comportamiento de este incidente en el futuro.

Playbook 7: Ataque DDoS (Denegación de Servicio Distribuido)

Escenario

Un servicio o infraestructura pública (sitio web, servidor DNS, aplicación en la nube) experimenta una sobrecarga masiva de tráfico proveniente de múltiples fuentes (una red de *bots*), lo que resulta en una degradación severa del rendimiento o una interrupción total del servicio para los usuarios legítimos.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Disponibilidad - Denegación de Servicio (DDoS)
Severidad	Crítica (debido al impacto directo en la continuidad del negocio y la experiencia del cliente)
Prioridad	Crítica (la acción inmediata es esencial para restaurar el servicio)
Fuentes de Detección	Monitoreo de Red, CDN/WAF, SIEM, Reporte de Usuarios/Público, Logs de Servidor/Balanceador de Carga

Fases y Acciones

1. Preparación

- **Contratación de Servicios de Mitigación:** Tener un servicio de protección DDoS externo (CDN, *scrubbing center*) en modo "siempre activo" o "a demanda".
- **Capacidad de Escalabilidad:** Asegurar que la infraestructura en la nube o los balanceadores de carga puedan escalar automáticamente.
- **Umbrales de Alerta:** Configurar alertas en el SIEM o en la plataforma de monitoreo de red para detectar picos de tráfico anómalos (alto RPS, latencia, conexiones).
- **Inventario de Activos Críticos:** Conocer las direcciones IP y DNS críticas que deben protegerse con prioridad.
- **Planes de Comunicación:** Establecer un protocolo de comunicación interna y externa (público, prensa) para notificar sobre la interrupción.

2. Detección y Análisis

- **Confirmar Ataque:** Verificar si la degradación del servicio se debe a una falla

interna o a una sobrecarga de tráfico externo.

- **Identificar Tipo de Ataque:** Determinar si es un ataque de volumen (UDP/ICMP Flood), de protocolo (SYN Flood) o de capa de aplicación (HTTP Flood), analizando el tráfico y los logs.
- **Determinar Origen y Objetivo:** Identificar las direcciones IP de origen (si es posible), puertos y el activo específico al que se dirige el ataque.
- **Medir Magnitud:** Cuantificar el volumen de tráfico malicioso (Gbps o PPS) para seleccionar la estrategia de mitigación adecuada.
- **Mapeo MITRE ATT&CK:** T1499 (Denegación de Servicio de Aplicación Web), T1498 (Denegación de Servicio de Red).

3. Contención

- **Activar Servicio de Mitigación:** Redirigir el tráfico del activo atacado a la plataforma de protección DDoS o CDN (*scrubbing center*).
- **Limitar Tasa (*Rate-Limiting*):** Aplicar límites temporales en *firewalls* o WAF a las IP que muestren patrones de ataque (ej. alto número de peticiones por segundo).
- **Bloqueo Geográfico/Por Protocolo:** Bloquear tráfico proveniente de regiones anómalas o protocolos que no deberían ser utilizados (si aplica).
- **Reducción de Superficie:** Deshabilitar temporalmente servicios o puertos no esenciales para ahorrar recursos del sistema.

4. Erradicación

- **Ajuste Fino de Reglas:** Optimizar las reglas del WAF/CDN durante el ataque para filtrar el tráfico malicioso específico del patrón detectado (ej. *User-Agents* o *Payloads*).
- **Depuración de Infraestructura:** Asegurar que todos los *firewalls* perimetrales y de la aplicación estén configurados correctamente y no contribuyan al problema.
- **Identificar Causa Raíz (si aplica):** Si el ataque fue posible por una mala configuración, corregirla.

5. Recuperación

- **Desactivar Mitigación (Gradual):** Retirar lentamente el tráfico del servicio de mitigación una vez que el volumen del ataque haya disminuido y se confirme la estabilidad.
- **Monitoreo Post-Ataque:** Mantener una vigilancia intensiva en los gráficos de tráfico y latencia para detectar posibles rebrotes o cambios en el vector de ataque.
- **Restauración Completa:** Asegurar que todos los servicios y funcionalidades deshabilitadas temporalmente se restablezcan y operen con normalidad.
- **Comunicación Externa:** Emitir una declaración de servicio restaurado a los usuarios/clientes afectados.

6. Lecciones Aprendidas e Informes

- **Revisión Post-Incidente:** Analizar el tiempo de detección, el tiempo de mitigación y la efectividad del servicio de protección DDoS.
- **Mejora de Capacidad:** Evaluar la necesidad de mayor capacidad de ancho de banda o de un plan de mitigación superior.
- **Documentar Metodología:** Documentar el vector de ataque utilizado, la *botnet* identificada (si es posible) y las *firmas* de tráfico malicioso.
- **Simulacros Periódicos:** Realizar simulacros de DDoS periódicos para probar la resiliencia de la infraestructura y la rapidez de la respuesta del equipo.

Herramientas Típicas: Servicios de Protección DDoS (Cloudflare, Akamai, AWS Shield, Google Cloud Armor, Azure DDoS Protection), WAF, Monitoreo de Red (*NetFlow*, *sFlow*), SIEM.

Playbook 8: Compromiso de Correo Empresarial (BEC)

Escenario

Un atacante obtiene acceso no autorizado a una cuenta de correo electrónico empresarial legítima (ej. a través de *phishing* o robo de credenciales) y la utiliza

para cometer fraude financiero, enviar correos maliciosos a otros empleados o socios, o exfiltrar información sensible, a menudo suplantando la identidad del usuario comprometido.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Compromiso de Identidad - Correo Empresarial (BEC)
Severidad	Crítica (riesgo de pérdida financiera directa o daño a la reputación)
Prioridad	Crítica (la detección temprana y la contención son vitales)
Fuentes de Detección	Gateway de Correo, SIEM, Logs de Auditoría de Correo, Reporte de Usuario/Receptor

Fases y Acciones

1. Preparación

- **Implementación de MFA:** Hacer que la autenticación multifactor (MFA) sea obligatoria para todas las cuentas, especialmente para ejecutivos y finanzas.
- **Detección de Suplantación (Spoofing):** Configurar y auditar políticas de DMARC, DKIM y SPF para prevenir la suplantación de dominio.
- **Monitoreo de Anomalías:** Configurar alertas en el SIEM o sistema de correo para detectar cambios anómalos (ej. creación de reglas de reenvío, inicios de sesión desde países atípicos, envío masivo).
- **Capacitación:** Entrenamiento de concienciación sobre *phishing*, estafas de transferencia bancaria y verificación de cambios en pagos.
- **Protocolos de Verificación:** Establecer un protocolo verbal o de canal secundario para verificar cualquier solicitud de pago o cambio de cuenta bancaria.

2. Detección y Análisis

- **Confirmar el Compromiso:** Verificar la autenticidad de la alerta (ej. correo de usuario comprometido reportado, alerta de inicio de sesión anómalo o creación de regla de bandeja de entrada).
- **Revisar Logs de Acceso:** Analizar el tiempo, la geolocalización y la dirección IP de los inicios de sesión sospechosos para identificar el acceso del atacante.
- **Buscar Artefactos Maliciosos:** Revisar la bandeja de entrada, la carpeta de elementos enviados y las reglas de bandeja de entrada en busca de reglas de reenvío, filtros ocultos o correos fraudulentos.
- **Analizar el Correo:** Determinar el alcance del ataque (a quién se le envió el correo fraudulento, si hubo transferencias de dinero solicitadas, etc.).
- **Mapeo MITRE ATT&CK:** T1078 (Cuentas Válidas), T1114.002 (Recolección de Correo – Reglas de Reenvío de Buzón).

3. Contención

- **Revocar Sesiones y Tokens:** Invalidar inmediatamente todas las sesiones de inicio de sesión activas para la cuenta comprometida.
- **Restablecer Contraseña/MFA:** Forzar el restablecimiento de la contraseña a una fuerte y asegurar que la configuración de MFA esté intacta o se vuelva a aplicar.
- **Bloquear IPs Sospechosas:** Bloquear a nivel de firewall o de servicio de correo las direcciones IP identificadas como las del atacante.
- **Alertar a Contactos:** Contactar de inmediato a los destinatarios internos y externos de los correos fraudulentos recientes.

4. Erradicación

- **Eliminar Reglas Maliciosas:** Borrar cualquier regla de reenvío, regla de bandeja de entrada oculta o configuración de *autorrespuesta* creadas por el atacante.
- **Limpiar Buzón:** Eliminar todos los correos electrónicos de *phishing* o fraude

enviados por el atacante.

- **Revisar Integraciones:** Revocar el acceso a aplicaciones de terceros (OAuth) o API que el atacante pudo haber comprometido o utilizado.
- **Escaneo de Endpoint:** Realizar un escaneo de malware en cualquier dispositivo que haya sido utilizado para el inicio de sesión anómalo.

5. Recuperación

- **Rehabilitar Acceso:** Restaurar el acceso normal del usuario solo después de confirmar que el control se ha restablecido y que la cuenta está segura con MFA.
- **Investigación Financiera:** Si se produjo una pérdida financiera, iniciar una investigación y coordinar con el departamento legal y bancario para intentar recuperar los fondos.
- **Comunicación con Socios:** Notificar a los socios/clientes si sus cuentas
- fueron el objetivo de correos fraudulentos provenientes de nuestra dirección.
- **Monitoreo Reforzado:** Mantener la cuenta y el *gateway* de correo bajo monitoreo intensivo por al menos 7 días.

6. Lecciones Aprendidas e Informes

- **Análisis Post-Incidente:** Determinar el vector de acceso inicial (ej. el correo de *phishing* exacto) y la eficacia del protocolo de respuesta.
- **Fortalecer Controles:** Mejorar las reglas de filtrado de correo y las alertas de comportamiento anómalo.

- **Acción Disciplinaria/Capacitación:** Determinar si se requiere capacitación adicional para el usuario o acción disciplinaria.
- **Documentación y Reporte:** Documentar la pérdida financiera (si aplica) y
- reportar el incidente a las autoridades regulatorias o policiales según sea necesario.

Playbook 9: Escalada de Privilegios No Autorizada

Escenario

Un usuario regular, una cuenta de servicio comprometida o un atacante que ha obtenido acceso a un sistema intenta o logra obtener permisos superiores a los que le corresponden (ej. de usuario estándar a administrador, *root* o System), explotando vulnerabilidades del sistema operativo, errores de configuración o credenciales robadas.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Compromiso de Identidad - Escalada de Privilegios
Severidad	Alta (acceso a datos sensibles, posibilidad de movimiento lateral/impacto a la continuidad)
Prioridad	Crítica (acción inmediata para detener el uso de privilegios elevados)
Fuentes de Detección	EDR/XDR, SIEM, Logs de Auditoría de SO, Sistemas de Control de Integridad de Archivos (FIM)

Fases y Acciones

1. Preparación

- **Principio de Mínimo Privilegio:** Asegurar que los usuarios y las cuentas de servicio solo tengan los permisos estrictamente necesarios para su función.
- **Gestión de Parches:** Mantener el sistema operativo, aplicaciones y bibliotecas actualizadas para mitigar vulnerabilidades de escalada.
- **Monitoreo de Comportamiento:** Configurar el EDR/SIEM para alertar sobre la ejecución de comandos o herramientas de escalada, o cambios inusuales de privilegios de procesos.

- **Control de Registros:** Habilitar logs detallados de eventos de seguridad (ej. creación de cuentas, adición a grupos de seguridad, cambios de permisos).

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de EDR o SIEM que indique un comportamiento de escalada (ej. ejecución de *exploits*, uso de herramientas como *Mimikatz* o *PowerSploit*).
- **Identificar el Vector:** Determinar cómo se intentó la escalada (ej. vulnerabilidad del SO, falla de configuración, credenciales en texto plano en memoria).
- **Evaluar el Alcance:** Confirmar si la escalada fue exitosa, si se crearon cuentas privilegiadas o se utilizó el acceso para otro propósito (ej. exfiltración).
- **Análisis de Proceso:** Rastrear el proceso padre y el binario que ejecutó la escalada.
- **Mapeo MITRE ATT&CK:** T1068 (Explotación de Vulnerabilidad), T1548 (Abuso de Control de Acceso y Permisos), T1003 (Acceso a Credenciales).

3. Contención

- **Aislar el Host:** Desconectar inmediatamente el endpoint donde se detectó la escalada, o aplicar la función de contención del EDR.
- **Revocar Credenciales:** Restablecer las contraseñas de la cuenta de usuario original y de cualquier cuenta privilegiada que haya sido creada o comprometida.
- **Suspender Cuentas:** Deshabilitar temporalmente las cuentas de alto privilegio que hayan estado involucradas en la actividad anómala.

- **Snapshot de Memoria/Disco:** Capturar una imagen de la memoria y/o el disco para análisis forense, especialmente si se utilizó un *exploit* de día cero.

4. Erradicación

- **Eliminar Artefactos:** Borrar cualquier *exploit*, *web shell*, *backdoor* o herramienta de ataque utilizada para la escalada.
- **Aplicar Parches:** Aplicar el parche de seguridad para la vulnerabilidad explotada o corregir la configuración errónea de inmediato.
- **Revertir Cambios:** Eliminar cuentas maliciosas creadas, revertir cambios de membresía de grupos o permisos de archivo.

5. Recuperación

- **Reinstalar/Restaurar:** Si la integridad del sistema no puede ser garantizada, reconstruir el host a partir de una imagen limpia o restaurar desde una copia de seguridad pre-incidente.
- **Validación de Privilegios:** Auditar y validar que todos los permisos en el sistema (usuarios, servicios) están correctamente configurados y se adhiere al mínimo privilegio.
- **Restablecer Acceso:** Rehabilitar el acceso del usuario y el host a la red después de la confirmación de la limpieza y corrección.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar la vulnerabilidad o la mala configuración específica que permitió la escalada.
- **Mejorar Hardening:** Reforzar la configuración de seguridad del sistema operativo y de las aplicaciones para prevenir futuras escaladas.
- **Actualizar Reglas:** Crear nuevas reglas de detección y correlación en el SIEM/EDR basadas en los patrones de ataque observados.
- **Capacitación:** Instruir a los administradores y desarrolladores sobre prácticas seguras de codificación y configuración para evitar este tipo de fallas.

Playbook 10: Exposición por Mala Configuración de Almacenamiento en la Nube

Escenario

Se detecta que un *bucket* de almacenamiento en la nube (ej. AWS S3, Azure Blob Storage, Google Cloud Storage) que contiene datos sensibles ha sido configurado erróneamente con acceso público (o un acceso excesivamente permisivo), lo que permite a usuarios no autenticados o no autorizados acceder, modificar o eliminar el contenido, resultando en una fuga o exposición de datos.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Exposición de Datos - Mala Configuración de Almacenamiento en la Nube
Severidad	Crítica (debido a la exposición potencial de PII, secretos comerciales o datos regulados)
Prioridad	Crítica (la acción inmediata para bloquear el acceso es vital)
Fuentes de Detección	CASB, Herramientas de Postura de Seguridad en la Nube (CSPM), Monitoreo de *Buckets*, Auditoría de Configuración, Reporte Público/Externo

Fases y Acciones

1. Preparación

- **Herramientas CSPM:** Implementar y configurar herramientas de Gestión de la Postura de Seguridad en la Nube (CSPM) para monitorear *buckets* y detectar configuraciones públicas de forma continua.
- **Revisión de Políticas:** Establecer una política de seguridad que prohíba el acceso público a *buckets* de datos sensibles y restringir quién puede modificar políticas de acceso (IAM).

- **Monitoreo de Logs:** Habilitar y auditar los logs de acceso a *buckets* para registrar quién y cuándo accede a los archivos.
- **Inventario de Datos:** Mantener un inventario actualizado de qué datos residen en cada *bucket* y su clasificación de sensibilidad.

2. Detección y Análisis

- **Confirmar la Exposición:** Validar la alerta de CSPM o del sistema de monitoreo sobre el acceso público o los permisos excesivos en el *bucket* afectado.
- **Determinar el Origen:** Identificar el cambio de configuración o la política de IAM que causó la exposición (ej. usuario, rol o *pipeline* que ejecutó el cambio).
- **Evaluar el Alcance:** Revisar los logs de acceso del *bucket* para determinar si terceros accedieron a los datos, qué archivos fueron leídos/descargados, y la criticidad de los datos expuestos.
- **Mapeo MITRE ATT&CK:** T1537 (Abuso de Política de la Nube), T1580 (Uso de Infraestructura de la Nube).

3. Contención

- **Remediación Inmediata:** Cambiar inmediatamente la configuración de acceso del *bucket* para revocar el acceso público o no autorizado (ej. bloquear todo acceso público, aplicar el principio de mínimo privilegio).
- **Auditoría de Políticas:** Bloquear o modificar cualquier política de IAM, ACL o política de *bucket* que haya permitido la exposición.
- **Rotación de Credenciales:** Si el cambio se hizo con credenciales
- comprometidas (ej. clave API), rotarlas de inmediato.
- **Bloqueo Geográfico/IP (Temporal):** Si la exposición se debe a acceso desde IPs específicas, bloquearlas temporalmente.

4. Erradicación

- **Corregir Causa Raíz:** Aplicar un control permanente para asegurar que la mala configuración no pueda ser revertida fácilmente (ej. bloqueo a nivel de la cuenta de nube).

- **Revisión Completa:** Escanear todos los *buckets* y recursos de almacenamiento de la organización para identificar otras configuraciones erróneas.
- **Eliminar Datos de *Cache* (Si Aplica):** Si se expuso contenido a través de CDN, invalidar el *cache* para remover cualquier dato sensible que haya sido almacenado temporalmente.

5. Recuperación

- **Validar el Acceso:** Confirmar que solo los usuarios y servicios autorizados tienen acceso al *bucket*.
- **Reanudar Operaciones:** Si alguna aplicación de negocio fue deshabilitada durante la contención, restaurar su acceso al *bucket* con los permisos corregidos.
- **Notificación:** Coordinar con el equipo legal y de cumplimiento para evaluar la necesidad de notificación a reguladores y a los individuos afectados si se confirmó la fuga de PII o datos regulados.
- **Monitoreo Post-Incidente:** Mantener un monitoreo elevado de logs de acceso al *bucket* por un período para detectar nuevos intentos de acceso anómalo.

6. Lecciones Aprendidas e Informes

- **Análisis Post-Incidente:** Documentar la causa raíz exacta de la mala configuración (ej. error humano, automatización defectuosa, política de *default* insegura).
- **Mejora del Proceso de Despliegue:** Integrar verificaciones de seguridad automatizadas (ej. *Shift-Left*) en los *pipelines* de CI/CD que gestionan la infraestructura en la nube.
- **Reforzar Entrenamiento:** Capacitar al personal de Ingeniería y operaciones sobre la seguridad de las políticas de IAM y las configuraciones de almacenamiento en la nube.
- **Documentación y Reporte:** Formalizar el informe del incidente y las lecciones aprendidas para actualizar la política de seguridad y el manual de

procedimientos.

Herramientas Típicas: CASB (Cloud Access Security Broker), CSPM (Cloud Security Posture Management, ej. Google Cloud Security Command Center, Wiz, Orca), Logs de Auditoría de la Nube (CloudTrail, Azure Activity Log), Herramientas de Infraestructura como Código (Terraform, CloudFormation) con escaneo de seguridad.

Playbook 11: Ataque de Relleno de Credenciales (*Credential Stuffing*)

Escenario

Un atacante utiliza listas de pares de nombre de usuario y contraseña (credenciales) robados o filtrados de brechas de datos de terceros para intentar iniciar sesión de forma masiva en las cuentas de los usuarios de la organización. Esto explota el hecho de que muchos usuarios reutilizan contraseñas. El objetivo es obtener acceso no autorizado a sistemas internos, aplicaciones o servicios en la nube.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Compromiso de Identidad - Ataque de Credenciales (*Credential Stuffing*)
Severidad	Media a Alta (depende de la cantidad de cuentas comprometidas y los sistemas afectados)
Prioridad	Alta (necesidad de detener el ataque en progreso y asegurar las cuentas vulnerables)

Fuentes de Detección	WAF/CDN, SIEM, Sistema de Gestión de Identidad y Acceso (IAM), Logs de Autenticación, CAPTCHA

Fases y Acciones

1. Preparación

- **Implementación de WAF/Bot Protection:** Usar servicios que puedan detectar y mitigar el tráfico automatizado de *bots*.
- **MFA Obligatorio:** Promover o hacer obligatoria la autenticación multifactor (MFA) para todas las cuentas.
- **Monitoreo de *Failed Logins*:** Configurar alertas en SIEM o IAM para detectar un número anómalo y masivo de intentos de inicio de sesión fallidos desde un pequeño conjunto de IPs o a un gran número de cuentas.
- **Detección de Reutilización:** Implementar una solución que compare hashes de contraseñas de usuarios contra listas de contraseñas filtradas (Pwned Passwords, etc.).
- **Bloqueo Inteligente:** Implementar políticas de bloqueo de cuentas o bloqueo temporal por IP después de un número reducido de intentos fallidos.

2. Detección y Análisis

- **Confirmar el Ataque:** Identificar un aumento exponencial en el volumen de solicitudes de inicio de sesión, especialmente fallidas, provenientes de IPs diversas.
- **Analizar Logs de Acceso Exitoso:** Revisar las cuentas que sí lograron iniciar sesión (éstas son las cuentas comprometidas) en busca de actividad
- anómala posterior (ej. cambio de configuración, exfiltración, movimiento lateral).
- **Determinar el Vector:** Confirmar que la fuente de las credenciales son listas públicas y no un *keylogger* o *phishing* interno.

- **Medir el Alcance:** Cuantificar el número total de intentos, el número de

cuentas válidas atacadas y el número de cuentas comprometidas.

- **Mapeo MITRE ATT&CK:** T1078 (Cuentas Válidas), T1110.004 (Fuerza Bruta de Credenciales: *Credential Stuffing*).

3. Contención

- **Bloqueo por Patrón:** Implementar reglas temporales en el WAF/Bot Protection para bloquear el patrón de tráfico o las IPs de origen más activas.
- **Forzar Restablecimiento de Contraseña:** Para todas las cuentas que se confirmen como comprometidas o atacadas con éxito, forzar un restablecimiento de contraseña inmediato.
- **Implementar CAPTCHA/Validación:** Activar medidas de validación humana (ej. CAPTCHA avanzado) en el punto de inicio de sesión para detener el tráfico automatizado.
- **Monitoreo de Sesiones Activas:** Cerrar cualquier sesión activa de las cuentas comprometidas para desalojar al atacante.

4. Erradicación

- **Validación de MFA:** Asegurar que la configuración de MFA se haya aplicado correctamente a todos los usuarios de alto riesgo.
- **Eliminar Artefactos:** Si el atacante dejó algún cambio o *backdoor* en las cuentas comprometidas (ej. reglas de reenvío de correo), revertir estos cambios.
- **Análisis de Impacto:** Determinar si el atacante logró exfiltrar o modificar datos durante el tiempo de compromiso y remediar ese impacto.
- **Mejora del Bloqueo:** Implementar soluciones permanentes de protección contra *bots* para evitar que el ataque se reanude.

5. Recuperación

- **Comunicación con Usuarios:** Notificar a todos los usuarios afectados sobre el incidente y guiarlos en el proceso de restablecimiento de contraseña y activación de MFA.

- **Revisión de Logs:** Continuar con una revisión intensiva de los logs de autenticación y de actividad de usuario por 7-14 días.
- **Monitorización de Tráfico:** Monitorear el tráfico de inicio de sesión para confirmar que los patrones de ataque de *bot* han cesado.
- **Auditoría de Políticas de Contraseña:** Revisar la robustez de las políticas de contraseña de la organización.

6. Lecciones Aprendidas e Informes

- **Análisis Post-Incidente:** Documentar la eficacia de la solución de *bot protection* y los *gaps* en la política de MFA.
- **Fortalecer Controles:** Priorizar la implementación de MFA en todos los sistemas y considerar la detección de contraseñas reutilizadas.
- **Capacitación Específica:** Realizar una campaña de concienciación a los usuarios sobre la no reutilización de contraseñas corporativas.
- **Documentación:** Documentar el origen del ataque (si fue posible) y los indicadores de compromiso utilizados.

Herramientas Típicas: WAF (Web Application Firewall), CDN (ej. Cloudflare, Akamai), SIEM, Herramientas de *Bot Management*, Sistema IAM (Identity and Access Management), Logs de Servidor de Autenticación.

Playbook 12: Acceso No Autorizado a Base de Datos Interna

Escenario

Se detecta un acceso no autorizado o malicioso a una base de datos (DB) interna que contiene datos sensibles (ej. PII, información financiera, secretos comerciales). El vector de ataque puede ser un empleado interno con abuso de privilegios (insider threat) o un sistema/aplicación comprometida que utiliza una cuenta de servicio de DB para el acceso.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Acceso No Autorizado - Base de Datos Interna / Abuso de Privilegios
Severidad	Crítica (riesgo de fuga masiva de datos y compromiso de la integridad/confidencialidad)
Prioridad	Crítica (la contención inmediata es vital para detener la lectura/modificación de datos)
Fuentes de Detección	Monitoreo de Actividad de Base de Datos (DAM), SIEM, Logs de Auditoría de DB, DLP, Reporte Interno

Fases y Acciones

1. Preparación

- **Principio de Mínimo Privilegio:** Limitar el acceso de usuarios y aplicaciones a solo los datos necesarios (acceso basado en roles).
- **Monitoreo de DB (DAM/SIEM):** Implementar herramientas para auditar y alertar sobre consultas anómalas (ej. consultas masivas a tablas sensibles, acceso fuera de horario).
- **Segmentación de Red:** Aislar la red de la base de datos de las redes de usuarios finales y de sistemas no esenciales.
- **Gestión de Cuentas de Servicio:** Uso de credenciales únicas y rotadas para aplicaciones, sin permisos excesivos.
- **Backups Cifrados:** Realizar copias de seguridad de la base de datos de forma regular y fuera de línea, asegurando el cifrado.

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de DAM/SIEM sobre consultas sospechosas, intentos de conexión fallidos o acceso de una cuenta de servicio en un contexto anómalo (ej. desde un servidor diferente).
- **Identificar el Usuario/Cuenta Comprometida:** Determinar qué credencial de usuario o cuenta de servicio fue utilizada para el acceso no autorizado.
- **Analizar Logs de Consultas:** Revisar el historial de comandos (SQL) ejecutados para determinar el alcance (qué datos se vieron, si se modificaron o eliminaron).
- **Rastrear el Origen:** Identificar la IP o el sistema desde donde se originó la conexión a la base de datos para ver si fue un insider o un sistema comprometido.
- **Mapeo MITRE ATT&CK:** T1552.001 (Descubrimiento de Credenciales: Almacenamiento en Archivos), T1580 (Uso de Infraestructura de la Nube - si la DB está en la nube).

3. Contención

- **Bloqueo de Acceso Inmediato:** Deshabilitar o bloquear temporalmente la cuenta de usuario/servicio comprometida a nivel de la base de datos o IAM.
- **Aislamiento de Origen:** Si se identificó el host de origen (ej. un servidor de aplicaciones comprometido), aislarlo de la red.
- **Bloqueo por IP/Regla:** Aplicar reglas en el Firewall de Base de Datos (DBF) o en el firewall de red para denegar el tráfico de la IP de origen maliciosa.
- **Snapshot Forense:** Crear una copia de la base de datos (o al menos de los logs) para análisis forense, manteniendo la integridad de la evidencia.

4. Erradicación

- **Rotación de Credenciales:** Restablecer la contraseña de la cuenta comprometida y de cualquier otra credencial que haya podido ser expuesta.
- **Parche/Corregir Vulnerabilidad:** Si la explotación fue a través de una aplicación o vulnerabilidad (ej. SQLi), aplicar el parche de código de inmediato.

- **Limpieza de Artefactos:** Eliminar cualquier *backdoor*, cuenta de base de

datos no autorizada o procedimiento almacenado malicioso que el atacante haya podido dejar.

- **Reforzar Controles DAM:** Ajustar las reglas de Monitoreo de Actividad de DB para detectar el patrón de ataque observado.

5. Recuperación

- **Validación de Integridad:** Verificar la integridad de los datos de la base de datos. Si hubo modificación o eliminación, restaurar las tablas o la DB completa desde un respaldo limpio pre-incidente.
- **Rehabilitación de Acceso:** Reestablecer el acceso a las aplicaciones/servicios utilizando las credenciales rotadas y validadas.
- **Notificación:** Informar a los equipos legales, de cumplimiento y a la dirección sobre el incidente y la potencial exposición de datos.
- **Monitoreo Cauteloso:** Mantener un monitoreo intensivo del servidor de DB y los logs de auditoría por un período de vigilancia extendido.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Determinar el *gap* exacto que permitió el acceso (ej. permisos excesivos, credencial en texto plano, falta de segmentación).
- **Mejorar Políticas:** Reforzar las políticas de control de acceso a la base de datos (modelo de menor privilegio) y mejorar el proceso de gestión de secretos (API keys, passwords).
- **Documentar:** Documentar el conjunto de datos exacto expuesto/afectado y la línea de tiempo del incidente.
- **Capacitación:** Instruir a los desarrolladores y DBAs sobre la seguridad de las bases de datos y la gestión de cuentas de servicio.

Herramientas Típicas: DAM (Database Activity Monitoring, ej. Imperva, IBM Guardium), SIEM, Logs de Auditoría Nativos de la DB (ej. Oracle Audit, SQL Server Audit), Firewalls de Base de Datos (DBF).

Playbook 13: Descubrimiento de Activos *Shadow IT*

Escenario

Se detecta la presencia de dispositivos, aplicaciones, servicios en la nube o infraestructura no autorizada, no soportada o desconocida (conocida como *Shadow IT*) siendo utilizada dentro del entorno corporativo. Estos activos no han pasado por el proceso de revisión y aprobación de seguridad, lo que representa un riesgo de vulnerabilidad o exposición de datos.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Riesgo - Uso de Activos No Autorizados (*Shadow IT*)
Severidad	Media a Alta (riesgo potencial de seguridad, cumplimiento y fuga de datos)
Prioridad	Alta (necesidad de evaluación y control o deshabilitación inmediata)
Fuentes de Detección	Escáneres de Red (NMAP), Logs de Proxy/DNS, CASB, Herramientas de Descubrimiento de Activos (ADM)

Fases y Acciones

1. Preparación

- **Inventario y Baseline:** Mantener un inventario actualizado de activos autorizados y un *baseline* de tráfico de red y comportamiento de aplicaciones.
- **Herramientas de Descubrimiento:** Implementar herramientas de Escaneo de Red, Monitoreo de DNS/Proxy y CASB para identificar aplicaciones y dispositivos desconocidos.

- **Política Clara:** Definir y comunicar una política clara sobre el uso de software, hardware y servicios en la nube no autorizados (política de uso aceptable).
- **Proceso de Aprobación:** Establecer un proceso claro para que los empleados soliciten y obtengan aprobación para nuevas herramientas tecnológicas.

2. Detección y Análisis

- **Confirmar el Hallazgo:** Investigar la alerta de la herramienta de descubrimiento (*Shadow IT* o dispositivo no autorizado) o el tráfico de red anómalo.
- **Identificar el Activo:** Determinar la función, el propietario, la ubicación y el tipo de datos que se están procesando en el activo no autorizado.
- **Evaluar el Riesgo:** Clasificar el riesgo del activo (*Shadow IT*): ¿Contiene datos sensibles? ¿Está parcheado? ¿Crea un canal de exfiltración?
- **Rastrear el Origen:** Identificar al usuario, departamento o proceso que introdujo el activo.
- **Mapeo MITRE ATT&CK:** T1568 (Acceso a Infraestructura Externa), T1583.003 (Recursos para Cuentas - Cloud).

3. Contención

- **Aislamiento de Dispositivo:** Si es un dispositivo no autorizado o de alto riesgo, aislarlo de la red corporativa.
- **Bloqueo de Acceso:** Si es una aplicación/servicio en la nube, bloquear el acceso a través de DNS, Proxy o Firewall a la URL/IP del servicio.
- **Compromiso de la Fuente:** Si el activo fue instalado a través de un sistema comprometido, aplicar las medidas de contención del *playbook* de sistema comprometido (ej. parcheo, aislamiento).
- **Contacto con Propietario:** Contactar al propietario del activo para notificar la violación de la política y comenzar el proceso de remediación.

4. Erradicación

- **Desinstalación:** Desinstalar o eliminar la aplicación, el servicio o el dispositivo no autorizado de la red o del *endpoint*.
- **Revisión de Datos:** Asegurar que todos los datos corporativos almacenados en el activo *Shadow IT* sean recuperados y eliminados de forma segura de la aplicación no autorizada.
- **Corregir Causa Raíz:** Abordar la razón por la cual el activo se introdujo (ej. si el proceso interno es demasiado lento o la herramienta corporativa es inadecuada).

5. Recuperación

- **Reintegración o Alternativa:** Si el activo *Shadow IT* es legítimo y necesario, iniciar el proceso formal de aprobación para su uso o implementar una alternativa corporativa autorizada que cumpla con los estándares de seguridad.
- **Monitoreo Reforzado:** Poner al usuario/departamento identificado bajo un monitoreo temporal reforzado para asegurar el cumplimiento de las políticas.
- **Capacitación Correctiva:** Proporcionar capacitación de cumplimiento de políticas al personal involucrado.

6. Lecciones Aprendidas e Informes

- **Análisis Post-Incidente:** Documentar la naturaleza del activo *Shadow IT* (por qué se usó y por qué la detección falló inicialmente).
- **Mejora del Proceso:** Revisar el proceso de adquisición y aprobación de tecnología para satisfacer las necesidades del negocio de manera más eficiente y segura.
- **Actualizar Herramientas:** Ajustar las reglas de detección de las herramientas (CASB, Proxy, ADM) para incluir el patrón de este activo y sus variantes.
- **Campaña de Concienciación:** Lanzar una campaña de comunicación a toda la organización sobre los riesgos y las políticas de *Shadow IT*.

Herramientas Típicas: CASB (Cloud Access Security Broker), Soluciones de

Descubrimiento de Activos (ADM), Logs de Proxy/DNS, Escáneres de Red, Herramientas DLP.

Playbook 14: Ataque de Fuerza Bruta RDP (Protocolo de Escritorio Remoto)

Escenario

Se detecta un volumen masivo y anómalo de intentos de inicio de sesión fallidos dirigidos a endpoints o servidores que exponen el Protocolo de Escritorio Remoto (RDP) a Internet o a través de la red interna. El atacante utiliza herramientas automatizadas para probar numerosas contraseñas contra cuentas válidas o comunes, buscando un acceso inicial para la persistencia y el movimiento lateral.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Compromiso de Identidad - Fuerza Bruta / Acceso Inicial (RDP)
Severidad	Media a Crítica (si el ataque es exitoso, conduce a un compromiso completo del sistema)
Prioridad	Crítica (la acción inmediata es crucial para prevenir un acceso exitoso)
Fuentes de Detección	Logs de Seguridad de Windows (Evento 4625), SIEM, Firewall, IPS/IDS, EDR/XDR, Monitoreo de Red

Fases y Acciones

1. Preparación

- **Exposición Limitada:** Limitar el acceso RDP solo a IPs confiables (VPN o *jump servers*). Evitar la exposición directa a Internet.
- **MFA en RDP/VPN:** Implementar la autenticación multifactor (MFA) para

todas las conexiones RDP.

- **Política de Bloqueo de Cuentas:** Configurar una política de bloqueo de cuentas de SO después de un número reducido de intentos fallidos.
- **Monitoreo de *Failed Logins*:** Configurar alertas en el SIEM para detectar picos anómalos en el ID de Evento 4625 (falla de inicio de sesión).
- **Cambio de Puerto:** Cambiar el puerto RDP por defecto (3389) a un puerto no estándar (una medida de seguridad superficial, pero útil).

2. Detección y Análisis

- **Confirmar el Ataque:** Analizar el SIEM o los logs de Windows (Eventos 4625 y 4624) para validar el alto volumen de intentos fallidos.
- **Identificar Origen:** Determinar las direcciones IP de origen del ataque (suelen ser numerosas y distribuidas).
- **Identificar Cuentas Atacadas:** Confirmar qué cuentas están siendo objetivo (ej. Administrator, User, cuentas comunes).
- **Verificar Acceso Exitoso:** Revisar si el ataque ya logró un inicio de sesión exitoso (ID de Evento 4624) en medio de los intentos fallidos. **Esto eleva la severidad a Crítica.**
- **Mapeo MITRE ATT&CK:** T1110.003 (Fuerza Bruta de Credenciales: RDP), T1078 (Cuentas Válidas).

3. Contención

- **Bloqueo a Nivel de Firewall:** Aplicar reglas en el firewall perimetral o de host para bloquear de inmediato las IPs de origen identificadas.
- **Deshabilitar RDP Temporalmente:** Si el ataque es masivo y no se puede bloquear por IP de manera efectiva, deshabilitar temporalmente el servicio RDP del host atacado.
- **Forzar Bloqueo de Cuentas:** Si el ataque se dirige a una cuenta específica de alto valor, bloquear la cuenta hasta que se pueda proteger con MFA/contraseña fuerte.
- **Aislar Host (si hay compromiso):** Si se detectó un acceso exitoso, aislar el host inmediatamente para detener el movimiento lateral.

4. Erradicación

- **Rotación de Credenciales:** Restablecer las contraseñas de las cuentas atacadas y, especialmente, de cualquier cuenta que haya sido comprometida con éxito.
- **Implementar o Reforzar MFA:** Asegurar que la MFA esté implementada y configurada correctamente en el punto de acceso RDP.
- **Revisar Políticas de Bloqueo:** Ajustar la política de bloqueo de cuentas para que sea más agresiva y efectiva contra futuros ataques de fuerza bruta.
- **Análisis de Sistema Comprometido:** Si hubo un acceso exitoso, ejecutar el *playbook* de *Malware* o *Compromiso de Cuenta* para buscar artefactos.

5. Recuperación

- **Rehabilitar RDP (con controles):** Volver a habilitar el acceso RDP, asegurándose de que todas las conexiones pasen a través de VPN/MFA y que las IPs maliciosas permanezcan bloqueadas.
- **Revisar *Gaps* de Firewall:** Auditar las reglas del firewall para asegurar que solo las IPs necesarias puedan acceder al puerto RDP.
- **Validación de Cuentas:** Auditar las cuentas de usuario para asegurar que no se hayan creado cuentas fraudulentas o modificado permisos.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar por qué el RDP estaba expuesto de forma inadecuada o por qué las contraseñas eran débiles.
- **Fortalecer Defensas:** Priorizar la adopción de un *gateway* de VPN o una solución RDP con protección avanzada contra la fuerza bruta.
- **Actualizar Reglas:** Crear reglas específicas en el Firewall/IDS/SIEM para detectar y bloquear proactivamente este tipo de escaneo masivo en el futuro.
- **Capacitación:** Instruir a los administradores sobre las mejores prácticas para asegurar los servicios de acceso remoto.

Herramientas Típicas: Firewall (Network & Host), SIEM, EDR/XDR, IDS/IPS, Sistema de Gestión de Identidad y Acceso (IAM), Herramientas de Gestión de Acceso

Privilegiado (PAM).

Playbook 15: Acceso No Autorizado a Entornos de Desarrollo

Escenario

Un atacante, que puede ser un empleado comprometido o una amenaza externa, obtiene acceso no autorizado a sistemas críticos del ciclo de vida de desarrollo de software (SDLC), como repositorios de código (Git), servidores de integración continua/despliegue continuo (CI/CD como Jenkins, GitLab, Azure DevOps) o *artifact repositories*. El objetivo suele ser inyectar código malicioso (*backdoor*), robar propiedad intelectual o manipular la cadena de suministro de software.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Compromiso de Acceso/Cadena de Suministro - Entornos de Desarrollo
Severidad	Crítica (impacto directo en el producto, la propiedad intelectual y la confianza del cliente)
Prioridad	Crítica (acción inmediata para detener la manipulación del código y la automatización del *build*)
Fuentes de Detección	Logs de Auditoría de Git, Logs de Servidor CI/CD (Jenkins, GitLab), SIEM, EDR/XDR, Reporte de Dev

Fases y Acciones

1. Preparación

- **Autenticación Fuerte:** Implementar MFA obligatorio y claves SSH (en lugar de contraseñas) para el acceso a Git y CI/CD.
- **Principio de Mínimo Privilegio:** Limitar estrictamente los permisos en repositorios y sistemas CI/CD (quién puede aprobar, hacer *merge* o ejecutar *jobs*).
- **Segmentación de Red:** Aislar los servidores CI/CD, especialmente los *runners* o *agents* que ejecutan el código, del resto de la red corporativa.
- **Monitoreo de Logs:** Habilitar y auditar logs detallados para cambios en *jobs* de CI/CD, nuevos *webhooks*, adición de claves SSH y actividad de usuarios privilegiados.
- **Revisiones de Código:** Hacer obligatorias las revisiones de código de pares (*peer reviews*) para todos los *merges*.

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar *commits* no firmados o anómalos, cambios en *pipelines* de CI/CD, creación de nuevas cuentas o claves SSH desconocidas.
- **Identificar el Vector:** Determinar si el compromiso fue por una credencial de usuario, una clave de API filtrada, una vulnerabilidad en el servidor CI/CD o un *web shell*.
- **Evaluar el Alcance:** Revisar cuántos repositorios, ramas y *jobs* de CI/CD se vieron afectados o fueron manipulados. Confirmar si se liberó código malicioso.
- **Análisis Forense:** Si un servidor fue comprometido, realizar un *snapshot* del mismo para análisis forense.
- **Mapeo MITRE ATT&CK:** T1568 (Acceso a Infraestructura Externa), T1583 (Obtención de Recursos), T1526 (Control de Recursos de Nube/Infraestructura).

3. Contención

- **Revocar Credenciales:** Revocar de inmediato las claves SSH, tokens de acceso personal (PAT) y contraseñas de la cuenta comprometida.

- **Suspender Acceso:** Suspender temporalmente las cuentas de usuario y de servicio que fueron utilizadas en el ataque.
- **Detener Pipelines CI/CD:** Deshabilitar o pausar todos los *jobs* de CI/CD potencialmente afectados para evitar la inyección o el despliegue de código malicioso.
- **Bloqueo a Nivel de Repositorio:** Cambiar temporalmente las ramas principales a modo de solo lectura o forzar la aprobación de *merge* de un administrador de seguridad.

4. Erradicación

- **Revertir Código:** Identificar y revertir todos los *commits* y modificaciones maliciosas en el repositorio a un estado limpio y verificado.
- **Eliminar Artefactos:** Borrar cualquier clave SSH, token de acceso, *hook* o *script* que el atacante haya agregado a los sistemas CI/CD/Git.
- **Reconstruir Servidores:** Si el servidor CI/CD o los *runners* fueron comprometidos, reconstruirlos desde una imagen limpia y parchada.
- **Parchear Vulnerabilidades:** Aplicar parches de seguridad para cualquier vulnerabilidad (ej. en Jenkins o Gitlab) que haya sido explotada.

5. Recuperación

- **Validación de Integridad:** Verificar que todo el código y los binarios de las últimas versiones (*builds*) estén libres de código malicioso.
- **Restablecer Acceso:** Rehabilitar el acceso de las cuentas de usuario solo después de un restablecimiento de credenciales seguro (con MFA y/o nuevas claves SSH).
- **Reanudar Operaciones:** Reanudar la ejecución de los *jobs* de CI/CD y liberar las ramas para desarrollo normal, manteniendo la supervisión.
- **Auditoría Post-Incidente:** Ejecutar una auditoría de seguridad automatizada en todos los repositorios críticos para detectar cualquier artefacto restante.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar el vector de acceso inicial y los *gaps* de configuración que permitieron la manipulación del SDLC.
- **Mejorar Seguridad del SDLC:** Implementar procesos de escaneo de secretos y escaneo de vulnerabilidades (SAST/DAST) en el *pipeline* de CI/CD.
- **Fortalecer Secrets Management:** Mover las credenciales de servicio fuera de los archivos de configuración y hacia una solución de gestión de secretos dedicada (ej. HashiCorp Vault, AWS Secrets Manager).
- **Capacitación:** Instruir a los desarrolladores sobre prácticas de seguridad de Git, revisión de código y la importancia de la MFA.

Herramientas Típicas: SIEM, Soluciones de Seguridad de la Cadena de Suministro de Software (SSCS), Logs de Auditoría de Git/CI/CD, Soluciones SAST/DAST, EDR/XDR.

Playbook 16: Abuso de Integraciones OAuth (*Phishing* de Consentimiento)

Escenario

Un usuario es engañado mediante una campaña de *phishing* de consentimiento para autorizar una aplicación de terceros maliciosa o ilegítima a acceder a datos sensibles de su cuenta en la nube (ej. Google Workspace, Microsoft 365, Slack). El atacante utiliza el acceso delegado del token OAuth (ej. leer correos, acceder a archivos, enviar mensajes) para la exfiltración de datos o el movimiento lateral.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Compromiso de Identidad - OAuth / *Phishing* de Consentimiento

Severidad	Alta (acceso delegado a datos por un atacante que opera bajo una aplicación "legítima")
Prioridad	Crítica (la acción inmediata para revocar el token es vital para detener el abuso delegado)
Fuentes de Detección	CASB, Logs de Auditoría de Identidad (Azure AD, Google Workspace), Gateway de Correo, Reporte de Usuario

Fases y Acciones

1. Preparación

- **Monitoreo de Aplicaciones:** Utilizar un CASB (Cloud Access Security Broker) o herramientas de auditoría nativas para monitorear nuevas aplicaciones de terceros con permisos excesivos.
- **Restricción de Consentimiento:** Implementar políticas que limiten el consentimiento de aplicaciones solo a administradores o a una lista blanca de aplicaciones verificadas.
- **Concienciación:** Capacitación específica a los usuarios sobre los riesgos del *phishing* de consentimiento (revisar los permisos solicitados por la aplicación).
- **Revisión de Aplicaciones:** Auditoría periódica de las aplicaciones de terceros autorizadas y los permisos que tienen.
- **Alertas de CASB:** Configurar alertas para cuando una aplicación solicite un conjunto de permisos de alto riesgo (ej. acceso de lectura/escritura a todos los correos).

2. Detección y Análisis

- **Confirmar el Abuso:** Investigar la alerta de CASB o del Gateway de Correo que indica que una aplicación no aprobada recibió consentimiento.

- **Identificar la Aplicación:** Determinar el nombre, el ID del cliente y los permisos que le fueron concedidos a la aplicación.
- **Evaluar el Alcance:** Revisar los logs de auditoría de la plataforma de identidad para ver la actividad que la aplicación ha realizado (ej. ¿Se leyeron correos? ¿Se accedió a archivos específicos?).
- **Determinar el Origen:** Rastrear si el usuario fue atacado a través de un correo de *phishing* o por otro medio.
- **Mapeo MITRE ATT&CK:** T1526 (Control de Recursos de Nube/Infraestructura), T1566.002 (*Phishing*: Ataque de Consentimiento de Servicios de Confianza), T1078 (Cuentas Válidas).

3. Contención

- **Revocar el Token OAuth:** Revocar de inmediato el consentimiento y el token de acceso de la aplicación maliciosa para la cuenta del usuario.
- **Eliminar la Aplicación:** Bloquear o eliminar la aplicación de la lista de aplicaciones permitidas a nivel de la organización para evitar que otros usuarios la autoricen.
- **Restablecer Contraseña (Preferencia):** Aunque el token sea delegado, restablecer la contraseña del usuario y forzar una nueva autenticación con MFA.
- **Auditoría de Cuentas Adicionales:** Escanear proactivamente el entorno para identificar cualquier otro usuario que también haya autorizado la misma aplicación maliciosa.

4. Erradicación

- **Limpiar Artefactos:** Si la aplicación utilizó el acceso para establecer un mecanismo de persistencia (ej. crear reglas de reenvío en el correo), eliminar esos artefactos.
- **Análisis de Impacto:** Determinar si los datos fueron efectivamente exfiltrados y, si es así, iniciar la respuesta según el *playbook* de "Exfiltración de Datos".
- **Bloqueo a Nivel de Firewall/Proxy:** Bloquear cualquier comunicación de

red conocida o URL asociada con la aplicación maliciosa.

5. Recuperación

- **Restaurar el Acceso:** Asegurar que el usuario pueda iniciar sesión y acceder a sus recursos de forma normal y segura (con MFA).
- **Comunicación de *Lecciones Aprendidas*:** Notificar al equipo y al usuario la naturaleza del ataque para que puedan identificar futuros intentos.
- **Auditoría de Permisos:** Realizar una auditoría completa de las aplicaciones de terceros que el usuario tiene autorizadas para asegurarse de que no haya otras *apps* sospechosas.

6. Lecciones Aprendidas e Informes

- **Análisis Post-Incidente:** Documentar la URL de *phishing* utilizada, el ID de la aplicación y la eficacia de la herramienta CASB/Auditoría.
- **Fortalecer Controles:** Reforzar la política de restricción de consentimiento de OAuth, idealmente permitiendo solo aplicaciones aprobadas por IT.
- **Campaña de Concienciación:** Realizar una campaña de *phishing* simulado de consentimiento para evaluar la resiliencia de los usuarios y educarlos.
- **Documentación:** Reportar la aplicación maliciosa a la plataforma de identidad correspondiente (ej. Google, Microsoft) si es un tercero externo.

Herramientas Típicas: CASB (Cloud Access Security Broker), Logs de Auditoría de Plataformas de Identidad (ej. Azure AD Audit, Google Workspace Audit), Herramientas de Correo/Filtrado (para detectar el *phishing* inicial).

Playbook 17: Exfiltración de Datos vía Túnel DNS

Escenario

Un atacante ha comprometido un host interno y está utilizando el Protocolo de Nombres de Dominio (DNS) para establecer un canal de comando y control (C2)

encubierto y exfiltrar datos sensibles. El ataque se logra codificando la información binaria o de texto dentro de las consultas DNS (subdominios) y recibiendo comandos en las respuestas DNS, lo que permite un movimiento de datos lento pero sigiloso a través de un protocolo que a menudo se monitorea de forma deficiente.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Exfiltración de Datos - Túnel DNS / C2 Encubierto
Severidad	Alta (riesgo de fuga de datos sensible y control persistente del host)
Prioridad	Crítica (la contención inmediata es vital para detener el flujo de datos)
Fuentes de Detección	Logs de Servidor DNS, Monitoreo de Red (NDR), SIEM, Análisis de Tráfico (Pcap), EDR/XDR

Fases y Acciones

1. Preparación

- **Monitoreo de DNS:** Habilitar el registro y la recolección centralizada de logs de DNS (consultas y respuestas) en el SIEM/NDR.
- **Detección de Anomalías:** Configurar alertas para patrones anómalos de DNS (ej. número inusualmente alto de consultas DNS por host, longitud excesiva de consultas, consultas a dominios con baja reputación).
- **Bloqueo Saliente:** Implementar reglas de firewall para que solo los servidores DNS internos autorizados puedan realizar consultas salientes a Internet.
- **Inspección Profunda:** Utilizar NDR o *Deep Packet Inspection* (DPI) en los

gateways para analizar el contenido del *payload* de las consultas DNS.

2. Detección y Análisis

- **Confirmar el Túnel:** Investigar la alerta de logs de DNS/SIEM sobre consultas de gran longitud o repetitivas a un dominio malicioso conocido (Túnel C2).
- **Analizar el Tráfico:** Usar herramientas de análisis de paquetes (*Wireshark*, etc.) o la plataforma NDR para inspeccionar los datos codificados en las consultas DNS.
- **Identificar el Host/Proceso:** Determinar qué host y, específicamente, qué proceso en el endpoint está generando las consultas maliciosas.
- **Medir la Magnitud:** Estimar la cantidad de datos que se han exfiltrado y la sensibilidad de los mismos.
- **Mapeo MITRE ATT&CK:** T1071.002 (Protocolos de Aplicación: DNS), T1572 (Túneles de Protocolo), T1048 (Exfiltración sobre Protocolo Alternativo).

3. Contención

- **Aislar el Host:** Desconectar inmediatamente el endpoint comprometido de la red (o usar la función de contención del EDR).
- **Bloquear el Dominio C2:** Agregar el dominio malicioso y las IPs del servidor DNS del atacante a las listas de bloqueo del firewall y del servidor DNS interno (sinkhole).
- **Bloqueo por Patrón:** Si es posible, aplicar una regla de IPS/Firewall para bloquear cualquier consulta DNS saliente con una longitud de *query* superior a un umbral razonable (ej. 150 caracteres).
- **Anunciar Nuevo DNS:** Si el servidor DNS interno fue comprometido, forzar a todos los hosts a usar un servidor DNS limpio o alternativo.

4. Erradicación

- **Eliminar Artefactos:** Borrar el *malware* o el *script* que está ejecutando el *túnel DNS* en el host comprometido.
- **Restablecer Cuentas:** Si el ataque utilizó una cuenta de usuario o servicio

comprometida, restablecer las credenciales y asegurar MFA.

- **Parchear Vulnerabilidades:** Si el túnel fue el resultado de una vulnerabilidad, aplicar el parche correspondiente.
- **Análisis de Persistencia:** Revisar el host aislado en busca de mecanismos de persistencia utilizados por el *malware*.

5. Recuperación

- **Restaurar Sistemas:** Si el host no puede ser desinfectado de manera confiable, reconstruirlo desde una imagen limpia.
- **Monitoreo Reforzado:** Reintegrar el host y la red bajo un monitoreo intensivo, con especial atención a los logs de DNS y las alertas de túnel.
- **Notificación y Cumplimiento:** Coordinar con los equipos legales y de cumplimiento si la exfiltración de datos sensibles se confirma.

6. Lecciones Aprendidas e Informes

- **Análisis Post-Incidente:** Documentar la técnica de codificación, el dominio C2 utilizado y el punto de falla en la monitorización de DNS.
- **Mejorar Políticas de DNS:** Implementar o reforzar el uso de un DNS seguro (*DNS over HTTPS/TLS*) y servicios de inteligencia de amenazas de DNS.
- **Fortalecer NDR/SIEM:** Ajustar los umbrales de alerta del NDR y SIEM para detectar patrones de tunelización más sutiles.
- **Capacitación:** Instruir al equipo del SOC en las técnicas de tunelización de DNS y las herramientas para decodificar los *payloads*.

Herramientas Típicas: Servidores DNS (Bind, Windows Server), Logs de DNS, SIEM, NDR (Network Detection and Response), IDS/IPS, Analizadores de Paquetes (ej. Wireshark), Herramientas de Descodificación de DNS.

Playbook 18: Inyección de JavaScript en Sitios Públicos (*Skimming/Magecart*)

Escenario

Un atacante ha logrado inyectar código JavaScript malicioso (conocido como *web skimming* o ataque *Magecart*) en una página web pública de la organización, típicamente en una página de pago o de recolección de datos. Este código se ejecuta en el navegador del usuario final y roba información sensible (ej. números de tarjetas de crédito, PII, credenciales de inicio de sesión) justo antes de que se envíe al servidor legítimo.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Fraude/Exfiltración de Datos - *Skimming* / Manipulación de Web Pública
Severidad	Crítica (impacto directo en el cliente, pérdida financiera, daño a la reputación y cumplimiento PCI DSS)
Prioridad	Crítica (la acción inmediata es esencial para detener el robo continuo de datos)
Fuentes de Detección	Monitoreo de Integridad de la Web (WIM), WAF, Detección de Cambios en la CDN, Reporte Público/Externo

Fases y Acciones

1. Preparación

- **Monitoreo de Integridad (WIM/SRI):** Implementar herramientas de Monitoreo de Integridad Web (WIM) para alertar sobre cambios no autorizados en archivos JS, bibliotecas de terceros y páginas de pago.
- **Uso de *Subresource Integrity* (SRI):** Implementar SRI para el *hashing* de bibliotecas JavaScript de terceros en las páginas críticas.
- **Segmentación de Pago:** Aislar las plataformas de pago y limitar los servicios

de terceros que se ejecutan en esas páginas.

- **WAF y CSP:** Configurar el WAF para bloquear patrones de inyección conocidos y definir una Política de Seguridad de Contenido (CSP) estricta.
- **Monitoreo de DNS:** Alertar sobre cualquier nueva consulta DNS de la página de pago que se dirija a un dominio de terceros desconocido.

2. Detección y Análisis

- **Confirmar la Inyección:** Investigar la alerta del WIM o del WAF que indica la presencia de código JS no autorizado.
- **Analizar el Código Malicioso:** Obtener una muestra del *script* inyectado para determinar su función, el tipo de datos que roba y el dominio C2 al que los envía.
- **Determinar el Vector:** Identificar cómo el atacante logró inyectar el código (ej. compromiso de una biblioteca de terceros, vulnerabilidad XSS almacenada, compromiso del servidor web/CMS).
- **Evaluar el Alcance:** Determinar cuántas páginas (ej. página de *checkout*, página de *login*) están afectadas y durante cuánto tiempo ha estado activo el *skimmer*.
- **Mapeo MITRE ATT&CK:** T1574.004 (Abuso de Cargador de Componente: *Hijack* de Bibliotecas), T1584.007 (*Compromise Infrastructure*: *Web Skimmer*).

3. Contención

- **Eliminación Inmediata:** Despliegue de inmediato de una versión limpia y verificada del código/archivo afectado para eliminar el *script* inyectado.
- **Bloqueo a Nivel de WAF/CDN:** Aplicar una regla de bloqueo específico en el WAF o CDN para la URL/IP del servidor C2 del atacante y para el patrón de la inyección.
- **Deshabilitar Temporalmente:** Si la eliminación es compleja o el riesgo es crítico, deshabilitar temporalmente la funcionalidad web afectada (ej. deshabilitar los pagos en línea) hasta que la limpieza esté garantizada.
- **Rotación de Credenciales:** Si el vector fue el compromiso de un servidor,

restablecer todas las credenciales asociadas con ese servidor (ej. claves de despliegue, acceso de FTP).

4. Erradicación

- **Corregir Causa Raíz:** Aplicar un parche de seguridad a la vulnerabilidad explotada o limpiar el servidor/CMS comprometido para asegurar que la inyección no se repita.
- **Revisión de Código:** Escaneo exhaustivo de todo el código de la aplicación web y sus dependencias en busca de otras inyecciones o *backdoors*.
- **Limpieza de Servidores:** Reconstruir o limpiar los servidores web y de bases de datos para eliminar cualquier persistencia del atacante.

5. Recuperación

- **Validación de Código:** Confirmar a través de WIM o SRI que todos los archivos críticos han sido restaurados a su estado íntegro.
- **Notificación y Cumplimiento:** Notificar de inmediato a los socios bancarios, procesadores de pago y, si aplica, a los reguladores de privacidad de datos (ej. GDPR, leyes locales).
- **Comunicación con Clientes:** Preparar y emitir una comunicación a los clientes potencialmente afectados sobre el incidente.
- **Reanudar Operaciones:** Restaurar la funcionalidad web, manteniendo un monitoreo de tráfico intensivo.

6. Lecciones Aprendidas e Informes

- **Análisis Post-Incidente:** Documentar el vector de inyección exacto, la duración del compromiso y el número de clientes/registros afectados.
- **Fortalecer WAF y CSP:** Ajustar la Política de Seguridad de Contenido (CSP) para restringir el origen de los *scripts* y mejorar las reglas del WAF.
- **Mejora del SDLC:** Integrar escaneo de seguridad (SAST/DAST) para prevenir vulnerabilidades de inyección en el código.
- **Documentación:** Formalizar el informe del incidente y las medidas tomadas para el cumplimiento de PCI DSS (si aplica).

Herramientas Típicas: WAF (Web Application Firewall), CDN (con capacidad de inspección), WIM (Web Integrity Monitoring), CSP (Content Security Policy), Escáneres de Vulnerabilidades Web, Escaneo de *Malware* de Servidor.

Playbook 19: Explotación de Endpoint de API Inseguro

Escenario

Un atacante abusa de un *endpoint* de una Interfaz de Programación de Aplicaciones (API) expuesta públicamente o internamente debido a fallas en la configuración de seguridad, como la ausencia de autenticación (Auth), autorización (AuthZ) o limitación de tasa (*rate-limiting*). El atacante explota estas vulnerabilidades para acceder a datos sensibles, realizar acciones no autorizadas o causar una Denegación de Servicio (DoS) a través de un uso excesivo.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Explotación de Aplicación - API Insegura / Denegación de Servicio
Severidad	Alta a Crítica (depende del tipo de datos expuestos o del impacto en la disponibilidad)
Prioridad	Crítica (la acción inmediata es esencial para detener el abuso en curso)
Fuentes de Detección	Logs de Servidor API, API Gateway, WAF, SIEM, Monitoreo de Rendimiento de Aplicación (APM), NDR

Fases y Acciones

1. Preparación

- **API Gateway:** Implementar una API Gateway o un WAF enfocado en APIs para aplicar políticas de AuthN, AuthZ y *rate-limiting*.

- **Pruebas de Seguridad:** Realizar pruebas de penetración (pen-testing) y escaneos DAST/SAST enfocados en el *Top 10* de vulnerabilidades de APIs de OWASP (ej. BOLA, Broken Access Control).
- **Logging Detallado:** Configurar el *logging* en el servidor de la API y el *gateway* para registrar todas las solicitudes (incluyendo parámetros) y respuestas.
- **Umbrales de Alerta:** Configurar alertas de SIEM/APM para detectar picos anómalos de tráfico a *endpoints* específicos o un alto número de respuestas de error (4xx/5xx).

2. Detección y Análisis

- **Confirmar el Abuso:** Investigar la alerta de *rate-limiting* o los picos de tráfico en un *endpoint* que indican un uso automatizado.
- **Identificar la Vulnerabilidad:** Determinar el *endpoint* específico explotado y el *gap* de seguridad (ej. falta de token, falla de AuthZ, falta de *rate-limiting*).
- **Evaluar el Alcance y el Impacto:** Confirmar si el atacante logró acceder a datos no autorizados, modificó registros (si la falla es de AuthZ) o si solo causó una Denegación de Servicio.
- **Analizar el Tráfico:** Revisar los logs de la API para identificar el patrón de las solicitudes maliciosas (ej. múltiples IDs de usuario en una solicitud, patrones de *scripting*).
- **Mapeo MITRE ATT&CK:** T1499 (Denegación de Servicio de Aplicación Web), T1505 (Ejecución de Cargas Web), T1078 (Cuentas Válidas).

3. Contención

- **Bloqueo de IPs/Tokens:** Aplicar reglas de bloqueo inmediato en el API Gateway o WAF para las IPs de origen o los tokens maliciosos.
- **Implementar *Rate-Limiting* de Emergencia:** Aplicar o reducir el límite de tasa en el *endpoint* explotado a un umbral muy bajo (ej. 1 solicitud por segundo).

- **Deshabilitar *Endpoint* Temporalmente:** Si el riesgo es crítico (ej. fuga de datos en curso) y no se puede mitigar de inmediato, deshabilitar o poner fuera de línea el *endpoint* vulnerable.

- **Rotación de Claves:** Si se sospecha del compromiso de una clave de API, rotarla inmediatamente.

4. Erradicación

- **Parche de Código/Configuración:** Corregir el código de la API para imponer la Autenticación, la Autorización (AuthZ) y la limitación de tasa (*rate-limiting*) correctas.
- **Refuerzo de API Gateway:** Asegurar que las políticas del *API Gateway* sean coherentes con los requisitos de seguridad.
- **Revisar *Payloads*:** Escanear la base de datos o el sistema subyacente para asegurarse de que no se hayan inyectado datos maliciosos o alterado la configuración.

5. Recuperación

- **Validación de Parche:** Desplegar el parche en un entorno de pruebas y validarlo con pruebas de penetración enfocadas antes de ir a producción.
- **Rehabilitar *Endpoint*:** Restaurar el *endpoint* al servicio normal después de confirmar que las mitigaciones están en su lugar y son efectivas.
- **Monitoreo Reforzado:** Poner el *endpoint* bajo un monitoreo intensivo de tráfico, AuthN/Z y *rate-limiting* durante la primera semana.
- **Notificación:** Si hubo fuga de datos, iniciar el proceso de notificación y cumplimiento.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar la falla exacta de diseño o configuración que expuso la API (ej. falta de verificación de ID de objeto, variable no inicializada, *default* inseguro).
- **Mejora del SDLC:** Integrar las pruebas de seguridad de API (fuzzing,

validación de esquemas) como un paso obligatorio en el proceso de CI/CD.

- **Fortalecer Controles:** Crear una lista de control (checklist) de seguridad de API para el equipo de desarrollo/DevOps.
- **Capacitación:** Instruir a los desarrolladores sobre las vulnerabilidades de API (OWASP API Security Top 10) y las prácticas de codificación segura.

Herramientas Típicas: API Gateway (ej. Apigee, AWS API Gateway), WAF, SIEM, APM (Application Performance Monitoring), Pruebas de Penetración de APIs (ej. Postman, Burp Suite), Logs de Acceso.

Playbook 20: Robo y Mal Uso de Credenciales por Insider

Escenario

Un empleado actual o ex-empleado utiliza sus credenciales de acceso legítimas (nombre de usuario y contraseña) a las que tiene acceso autorizado para realizar acciones maliciosas o no autorizadas, como la exfiltración de datos, sabotaje de sistemas, fraude financiero o la descarga masiva de información sensible. La dificultad radica en que el actor está operando dentro del perímetro de confianza.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Amenaza Interna - Abuso de Acceso Legítimo / Robo de Propiedad Intelectual
Severidad	Crítica (impacto directo, persistente y difícil de detectar con controles perimetrales)
Prioridad	Crítica (la acción inmediata es esencial

	para suspender el acceso y preservar la evidencia)
Fuentes de Detección	Monitoreo de Comportamiento de Usuarios (UEBA), DLP, SIEM, Logs de Acceso a Archivos, Reporte HR

Fases y Acciones

1. Preparación

- **UEBA/Monitoreo de Comportamiento:** Implementar herramientas que establezcan una línea base del comportamiento normal de los usuarios y alerten sobre desviaciones (ej. accesos a archivos fuera del patrón, inicios de sesión atípicos, descargas masivas).
- **DLP y Control de Acceso:** Reforzar las políticas de DLP en endpoints y red, y aplicar estrictamente el principio de mínimo privilegio (acceso solo a lo necesario para la función).
- **Gestión de Privilegios:** Uso de soluciones de Gestión de Acceso Privilegiado (PAM) para monitorear y grabar sesiones de usuarios con acceso elevado.
- **Proceso HR/Legal:** Definir un protocolo de respuesta y coordinación legal-forense con el departamento de Recursos Humanos y Legal para el manejo de la evidencia y las acciones disciplinarias.

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de UEBA sobre actividad anómala, violaciones de DLP (ej. intento de imprimir o copiar archivos sensibles) o una notificación de RRHH.
- **Analizar Logs de Acceso:** Revisar los logs de acceso a archivos/bases de datos para identificar el volumen y el tipo de datos accedidos o copiados.
- **Rastrear la Intención:** Correlacionar la actividad con el perfil del usuario (ej. ¿El usuario ha sido despedido o está en revisión de desempeño?).
- **Identificar el Canal:** Determinar la ruta de exfiltración (ej. correo personal, USB, almacenamiento en la nube no autorizado, impresión).

- **Mapeo MITRE ATT&CK:** T1078 (Cuentas Válidas), T1133 (Acceso a Servicios Externos), T1020 (Exfiltración Automatizada).

3. Contención

- **Suspender/Revocar Acceso:** Deshabilitar la cuenta del usuario de inmediato a nivel de red, correo, sistemas y VPN. Esto debe ser coordinado con Legal/HR.

- **Aislar Endpoints:** Aislar de la red cualquier dispositivo que el empleado haya utilizado recientemente para acceder a los datos sensibles.
- **Bloquear Canales de Exfiltración:** Si es viable, bloquear temporalmente los canales de salida sospechosos (ej. subir archivos a la nube, dominios de correo personal).
- **Preservar Evidencia:** NO apagar los sistemas. Capturar una imagen del disco duro y una copia de la memoria (RAM) para análisis forense.

4. Erradicación

- **Revisión de Cambios:** Auditar todos los cambios realizados por el usuario en sistemas de administración (ej. creación de cuentas de *backdoor*, modificación de configuraciones) y revertirlos.
- **Reclamar Activos:** Recuperar cualquier activo físico de la empresa (laptops, teléfonos, tokens de hardware).
- **Revisar Permisos:** Corregir cualquier sobre-privilegio que haya permitido al usuario acceder a datos o sistemas fuera de su ámbito normal.

5. Recuperación

- **Validar la Integridad:** Confirmar que no se haya comprometido la integridad de los datos o la configuración del sistema.
- **Restaurar Accesos:** Si el acceso tuvo un impacto en las operaciones de un departamento, restaurar el acceso a otros usuarios legítimos.
- **Evaluación de Impacto Legal:** Determinar la obligación de notificación a reguladores o a los afectados basándose en la sensibilidad de los datos

comprometidos.

- **Comunicación con Empleados:** Manejar la comunicación interna de manera controlada y en coordinación con RRHH para evitar pánico.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar el *gap* en los controles que permitió el acceso o la exfiltración (ej. falta de DLP, demasiados privilegios, falta de UEBA).

- **Fortalecer Controles:** Reforzar el monitoreo UEBA, endurecer las políticas de DLP y revisar los procesos de baja de empleados (offboarding).
- **Revisión de Roles:** Realizar una auditoría de roles y permisos para asegurar que se cumpla rigurosamente el principio de mínimo privilegio en toda la organización.
- **Documentación y Reporte:** Formalizar el informe del incidente para fines legales y disciplinarios.

Herramientas Típicas: UEBA (User and Entity Behavior Analytics), DLP (Data Loss Prevention), SIEM, PAM (Privileged Access Management), Herramientas Forenses (FTK Imager, EnCase), Logs de Directorio Activo/IAM.

Playbook 21: Mala Configuración de Identidad en la Nube (Roles IAM Excesivos Explotados)

Escenario

Un atacante externo, o una cuenta de servicio o un usuario interno comprometido, explota un rol o una política de Gestión de Identidad y Acceso (IAM) que ha sido configurada con permisos excesivos (*over-privileged*). Esta explotación permite al atacante escalar privilegios, acceder a recursos que no debería (ej. bases de datos, almacenamiento) o manipular la infraestructura en la nube, lo que lleva a un compromiso de la plataforma y potencialmente a una fuga de datos.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Compromiso de Identidad - Mala Configuración de IAM / Escalada de Privilegios en la Nube
Severidad	Crítica (el atacante tiene las "llaves del reino" debido a los permisos excesivos)
Prioridad	Crítica (la acción inmediata es esencial para revocar los permisos abusivos)
Fuentes de Detección	Logs de Auditoría de IAM (CloudTrail, Azure AD, Logs de Google Cloud), CSPM, SIEM, Monitoreo de Comportamiento

Fases y Acciones

1. Preparación

- **Principio de Mínimo Privilegio (IAM):** Aplicar rigurosamente el principio
- del mínimo privilegio a todos los usuarios, roles y cuentas de servicio.
- **Revisión Periódica de Roles:** Implementar herramientas de Gestión de la Postura de Seguridad en la Nube (CSPM) para auditar y alertar sobre roles con permisos *Wildcard* (*) o privilegios sin usar.
- **MFA para Privilegiados:** Hacer obligatoria la autenticación multifactor (MFA) para todas las cuentas con privilegios de administrador o de alto riesgo.
- **Monitoreo de Logs de IAM:** Configurar el SIEM para detectar actividad anómala de roles y cuentas de servicio (ej. cambios en políticas IAM, creación de claves de acceso, acceso a recursos fuera de su patrón).

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de CSPM o SIEM sobre el uso anómalo de un rol privilegiado (ej. un rol de solo lectura intentando hacer un cambio, un rol de una región accediendo a recursos de otra).
- **Identificar el Rol/Cuenta:** Determinar qué rol o cuenta de servicio fue explotado y cuáles son exactamente sus permisos excesivos.
- **Evaluar el Alcance:** Revisar los logs de auditoría para determinar qué acciones realizó el atacante (ej. acceso a almacenamiento, modificación de permisos, creación de infraestructura maliciosa).

- **Determinar el Vector:** Rastrear si la explotación fue a través de una credencial de cuenta de servicio comprometida o un usuario que abusó de un permiso que no necesitaba.
- **Mapeo MITRE ATT&CK:** T1078 (Cuentas Válidas), T1537 (Abuso de Política de la Nube), T1098.005 (Cuenta Compromiso: Creación de Cuenta de Nube).

3. Contención

- **Revocar Claves y Tokens:** Revocar de inmediato todas las claves de acceso y tokens de sesión para la cuenta de servicio o el rol IAM comprometido.
- **Modificar Política *Inline*:** Aplicar una política de denegación *inline* temporal al rol explotado para revocar el permiso específico que se está abusando.
- **Suspender Cuenta:** Si el compromiso fue a través de una cuenta de usuario, suspender la cuenta hasta que se restablezcan las credenciales y el MFA.
- **Aislar Recursos:** Si la explotación llevó a la creación de infraestructura maliciosa (ej. una VM para minería), aislarla o eliminarla inmediatamente.

4. Erradicación

- **Corregir Política IAM:** Modificar la política de IAM comprometida para adherirse al mínimo privilegio, eliminando cualquier permiso excesivo (*wildcard*) o innecesario.
- **Eliminar Artefactos:** Borrar cualquier recurso (VMs, *buckets*, cuentas de usuario) creado por el atacante.
- **Auditoría de Acceso:** Ejecutar una auditoría automatizada en todos los roles similares para prevenir el mismo tipo de explotación.

- **Rotación Masiva:** Considerar la rotación de claves de acceso de otras cuentas de servicio en el mismo entorno por precaución.

5. Recuperación

- **Validación de Roles:** Confirmar que los roles corregidos tienen los permisos mínimos necesarios y que las aplicaciones dependientes funcionan correctamente.
- **Reanudar Operaciones:** Reintegrar los sistemas o el tráfico que fue suspendido durante la contención.
- **Monitoreo Post-Incidente:** Mantener un monitoreo intensivo de los logs de IAM y CSPM para asegurar que no ocurran nuevos abusos.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar la justificación original (y errónea) del rol con privilegios excesivos y quién lo creó.
- **Mejora del Proceso de Creación de Roles:** Implementar un proceso de revisión y aprobación obligatorio para la creación de nuevos roles con privilegios elevados.
- **Fortalecer CSPM:** Ajustar las reglas del CSPM para detectar inmediatamente cualquier desviación de la política de mínimo privilegio.
- **Capacitación:** Instruir al personal de DevOps y de la Nube sobre la importancia de las políticas de IAM y las mejores prácticas de seguridad en la nube.

Herramientas Típicas: CSPM (Cloud Security Posture Management, ej. Wiz, Orca, Cloud Security Command Center), Logs de Auditoría de Plataformas de Nube (AWS CloudTrail, Azure Monitor, Google Cloud Logging), SIEM, Herramientas de Automatización (para la remediación rápida).

Playbook 22: Explotación de Pipeline CI/CD (Inyección de Código Malicioso)

Escenario

Un atacante ha comprometido una etapa del *pipeline* de Integración Continua/Despliegue Continuo (CI/CD) —ya sea a través de un servidor *build* inseguro, un repositorio de código comprometido o una dependencia maliciosa. El objetivo es inyectar código en el proceso automatizado de compilación o despliegue para distribuir *backdoors* en el producto final o en la infraestructura de producción/servidores *build*.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Compromiso de la Cadena de Suministro - Pipeline CI/CD / Inyección de Código
Severidad	Crítica (impacto directo en el producto final, riesgo de *supply chain attack*)
Prioridad	Crítica (la acción inmediata es esencial para detener el *build* y la distribución del código)
Fuentes de Detección	Monitoreo de Integridad (FIM), Logs de Servidor CI/CD, SIEM, Escaneo de *Software Composition Analysis*

Fases y Acciones

1. Preparación

- **Principio de Mínimo Privilegio:** Aplicar el mínimo privilegio a las cuentas de servicio y a los *runners* del CI/CD.
- **Segmentación:** Aislar los entornos de CI/CD del resto de la red. Los *runners* no deben tener acceso a Internet sin un proxy estricto.
- **Monitoreo de Integridad (FIM):** Implementar FIM en los servidores CI/CD para detectar cambios no autorizados en ejecutables y scripts del *pipeline*.

- **Seguridad en *Builds*:** Utilizar análisis de Composición de Software (SCA) y de Vulnerabilidades (SAST/DAST) como puertas de calidad en el *pipeline*.
- **Auditoría de Logs:** Recolección centralizada y alerta en SIEM sobre comandos inusuales o fallos en el proceso de *build*.

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de FIM o SIEM que indica una modificación en los scripts de *build*, un comando inesperado o un proceso desconocido en el servidor CI/CD.
- **Analizar el *Payload*:** Determinar el código malicioso inyectado y su objetivo (ej. *backdoor*, *web shell*, exfiltración de credenciales).
- **Identificar el Vector:** Determinar cómo se inyectó el código (ej. compromiso de credenciales de Git, abuso de un *plugin* de Jenkins, compromiso del servidor *build*).
- **Evaluar el Alcance:** Confirmar si el código malicioso ya fue compilado o desplegado en entornos superiores (QA, Producción).
- **Mapeo MITRE ATT&CK:** T1547.001 (Persistencia: Registro de Inicio/Servicios), T1195 (Compromiso de Software de Terceros), T1059 (Ejecución de Comandos).

3. Contención

- **Detener el *Pipeline* Inmediatamente:** Pausar o deshabilitar todos los *jobs* de CI/CD en todos los entornos.
- **Aislar Servidores *Build*:** Desconectar inmediatamente los servidores de *build* comprometidos de la red.
- **Revocar Credenciales:** Invalidar todas las claves de acceso, tokens y claves SSH asociadas con los servidores *build* y las cuentas de servicio de CI/CD.
- **Bloqueo de Artefactos:** Si el atacante inyectó artefactos maliciosos en un repositorio (ej. Nexus, Artifactory), ponerlos en cuarentena o eliminarlos.

4. Erradicación

- **Revertir Código/Configuración:** Identificar y revertir cualquier cambio malicioso en los *scripts* de *pipeline* (YAML, Groovy, etc.) y en el código del repositorio.
- **Reconstruir Servidores:** Destruir y reconstruir los servidores *build*/runners a partir de imágenes base limpias y verificadas.
- **Parchear Vulnerabilidades:** Aplicar parches de seguridad para cualquier vulnerabilidad del servidor CI/CD explotada (ej. versión de Jenkins, *plugin* vulnerable).
- **Limpieza de Persistencia:** Revisar los servidores reconstruidos y los *pipelines* en busca de cualquier mecanismo de persistencia remanente.

5. Recuperación

- **Revisión de Seguridad:** Ejecutar una revisión de seguridad completa del *pipeline* y el código base por parte del equipo de seguridad.
- **Reanudar *Builds* Controlados:** Reanudar el *pipeline* gradualmente, verificando la integridad de la compilación en cada etapa.
- **Validación del Producto:** Si el código fue desplegado, realizar un escaneo de seguridad en el producto o entorno de producción.
- **Notificación (si Aplica):** Si el producto comprometido fue distribuido a clientes, iniciar el proceso de notificación y respuesta del *playbook* de "Ataque a la Cadena de Suministro".

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar el punto exacto de compromiso (ej. credencial filtrada, servidor expuesto, dependencia no segura).
- **Fortalecer Pruebas:** Reforzar las pruebas de seguridad del *pipeline* (ej. *Git hooks* para verificar claves, escaneo de secretos).
- **Implementar Inmutabilidad:** Adoptar un enfoque de infraestructura inmutable para los *runners* de CI/CD (desechables después de cada *build*).
- **Capacitación:** Instruir a los desarrolladores y equipos de DevOps en las técnicas de ataque a la cadena de suministro y la protección de entornos CI/CD.

Herramientas Típicas: SIEM, FIM (File Integrity Monitoring), Soluciones SSCS (*Software Supply Chain Security*), SCA (*Software Composition Analysis*), EDR/XDR, Plataformas CI/CD (Jenkins, GitLab, GitHub Actions).

Playbook 23: Uso No Autorizado de IA Generativa

Escenario

Un empleado interactúa con una herramienta de Inteligencia Artificial Generativa pública y no autorizada (ej. ChatGPT, Bard, Copilot, etc.) e introduce o "pega" datos sensibles, confidenciales o regulados de la empresa. Esto constituye una violación de la política de seguridad de datos, ya que expone información propietaria a un tercero y potencialmente la entrena en su modelo, resultando en una fuga o pérdida de propiedad intelectual y cumplimiento normativo.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Exposición de Datos - Uso No Autorizado de IA Generativa / Violación de Política
Severidad	Media a Crítica (depende de la sensibilidad de los datos expuestos, ej. secretos comerciales)
Prioridad	Alta (necesidad de detener el acceso y evaluar la magnitud de la exposición)
Fuentes de Detección	DLP, Logs de Proxy/DNS, CASB, Monitoreo de Red, Reporte de Usuario/Departamento

Fases y Acciones

1. Preparación

- **Política Clara:** Establecer una política de uso de IA Generativa que prohíba estrictamente la introducción de datos sensibles en plataformas no autorizadas.
- **Bloqueo/Restricción de Red:** Implementar reglas de Proxy/Firewall/DLP para bloquear o, al menos, monitorear el acceso a URLs de IA Generativa populares.
- **DLP Contextual:** Configurar reglas de DLP que busquen patrones de datos sensibles (ej. PII, números de tarjetas, código fuente) intentando ser pegados en campos de texto de las URL de IA.
- **Capacitación:** Campañas de concienciación a los usuarios sobre el riesgo de la "fuga de datos por *prompt*" y las consecuencias.

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de DLP o Proxy que indica que un usuario accedió a una plataforma de IA y transfirió un gran volumen de texto o texto con patrones sensibles.
- **Identificar al Usuario y el Dato:** Determinar el empleado, el sistema desde donde se realizó la acción y el tipo exacto de dato sensible que fue expuesto.
- **Rastrear la Intención:** Entrevistar al usuario (en coordinación con RRHH/Legal) para determinar si la acción fue maliciosa, accidental o por desconocimiento de la política.
- **Evaluar el Alcance:** Determinar la cantidad y criticidad de los datos subidos y si esto viola alguna regulación (ej. HIPAA, GDPR, etc.).
- **Mapeo MITRE ATT&CK:** T1048.003 (Exfiltración sobre Protocolo Alternativo: Transferencia a la Nube), T1537 (Abuso de Política de la Nube).

3. Contención

- **Bloqueo Inmediato:** Reforzar las reglas de Proxy/Firewall para bloquear inmediatamente todas las plataformas de IA generativa no aprobadas para

el usuario o sistema afectado.

- **Aislamiento de Dispositivo:** Aislar el dispositivo del usuario (si la acción fue causada por un *exploit* o *malware*). Si es un abuso de credenciales legítimas, no es necesario el aislamiento.
- **Comunicación con Proveedor (si aplica):** Si la organización tiene un acuerdo con la plataforma de IA, solicitar la eliminación de los datos o el historial.

4. Erradicación

- **Eliminar el Acceso:** Asegurar que el usuario no pueda volver a acceder a la plataforma de IA no autorizada.
- **Limpieza de Dispositivo:** Asegurar que no queden copias de los datos sensibles en el portapapeles o historial de navegación del dispositivo.
- **Revisión de Políticas:** Si la violación fue masiva, revisar y ajustar las políticas de DLP para una detección más robusta en el futuro.

5. Recuperación

- **Capacitación Correctiva:** Proporcionar una capacitación intensiva y obligatoria al usuario sobre el manejo de información sensible y la política de IA.
- **Notificación y Cumplimiento:** Coordinar con Legal y Cumplimiento para evaluar las obligaciones de notificación a reguladores y clientes debido a la exposición de datos.
- **Monitoreo Reforzado:** Poner al usuario bajo un monitoreo intensivo por un período para asegurar el cumplimiento de la política.
- **Evaluación de Solución:** Si la necesidad del usuario era legítima, evaluar y desplegar una solución de IA aprobada y segura internamente.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar la razón por la que el usuario recurrió a la IA no autorizada (ej. falta de una herramienta interna, desconocimiento,

ineficiencia del proceso).

- **Fortalecer Controles:** Mejorar la implementación técnica del DLP en los navegadores y *endpoints* para prevenir el copiado de datos sensibles en general.
- **Actualizar Política:** Actualizar el manual de incidentes de seguridad y la política de uso aceptable con una sección detallada sobre la IA generativa.
- **Acción Disciplinaria:** Documentar las acciones disciplinarias tomadas (si aplica) en coordinación con RRHH y Legal.

Herramientas Típicas: DLP (Data Loss Prevention), Proxy/Firewall de Próxima Generación (para filtrado de URL), CASB (para monitoreo de servicios en la nube no autorizados), SIEM.

Playbook 24: Abuso de Replay de Token OAuth

Escenario

Un atacante logra interceptar y robar un *token* de acceso OAuth válido emitido para una aplicación o un usuario. El atacante reutiliza este *token* (*replay*) antes de que expire o sea revocado para suplantar la identidad del usuario o de la aplicación de confianza, obteniendo acceso temporal a los recursos protegidos del usuario sin necesidad de sus credenciales.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Compromiso de Identidad - Robo / *Replay* de Token de Acceso (OAuth)
Severidad	Alta (acceso no autorizado y sigiloso a datos y recursos)

Prioridad	Crítica (la acción inmediata es esencial para invalidar el *token* robado)
Fuentes de Detección	Logs de Servidor de Autorización OAuth, SIEM, CASB, Logs de Servidor de Recursos, Detección UEBA

Fases y Acciones

1. Preparación

- **Cifrado Fuerte:** Asegurar que todos los canales de comunicación por donde se transmiten *tokens* (ej. TLS/HTTPS) estén correctamente configurados y se prohíban versiones débiles.
- **Vida Útil Corta del *Token*:** Configurar *tokens* de acceso con una vida útil (TTL) muy corta y utilizar *refresh tokens* solo con los más altos estándares de seguridad.
- **Detección de Reutilización:** Implementar validación en el Servidor de Recursos (API) para detectar el uso simultáneo de un mismo *token* desde ubicaciones o dispositivos muy distantes (*impossible travel*).
- **Revisión de Flujos OAuth:** Auditar periódicamente los flujos de OAuth de las aplicaciones internas para asegurar que los *tokens* no se almacenen de forma insegura.
- **MFA para Revocación:** Exigir MFA para cualquier acción de alto privilegio, como la revocación o la gestión de *refresh tokens*.

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de SIEM/CASB sobre el uso anómalo de un *token* de acceso (ej. mismo *token* usado por dos IPs geográficamente distantes, uso de un *token* después de una actividad sospechosa).
- **Identificar el *Token*:** Determinar el *token* específico, el usuario/aplicación al que pertenece y el *scope* (permisos) que otorga.

- **Rastrear el Origen:** Analizar los logs de acceso al Servidor de Recursos para ver qué acciones realizó el atacante con el *token* reutilizado.
- **Determinar el Vector de Robo:** Investigar cómo el *token* fue interceptado (ej. *man-in-the-middle*, *cross-site scripting*, almacenamiento inseguro en un *log*).

- **Mapeo MITRE ATT&CK:** T1078 (Cuentas Válidas), T1539 (Abuso de *Tokens* de Acceso de Aplicación), T1552.004 (Credenciales en Tránsito).

3. Contención

- **Revocar el *Token* de Acceso:** Revocar de inmediato el *token* de acceso y el *refresh token* asociado en el Servidor de Autorización OAuth.
- **Forzar Cierre de Sesión:** Forzar el cierre de todas las sesiones activas para el usuario/aplicación afectada.
- **Bloqueo Geográfico/IP:** Si es posible, bloquear las direcciones IP de origen desde donde se detectó el *replay* malicioso.
- **Aislamiento de la Aplicación (si aplica):** Si el problema es la aplicación que emite el *token* de forma insegura, deshabilitarla temporalmente.

4. Erradicación

- **Corregir Vulnerabilidad:** Si el robo del *token* fue causado por una vulnerabilidad (ej. un problema de código que lo expuso), corregir el código o la configuración de inmediato.
- **Reforzar Cifrado:** Asegurar que los *cookies* y *headers* que contienen *tokens* tengan las banderas de seguridad (ej. *HttpOnly*, *Secure*).
- **Actualizar Flujo OAuth:** Si el flujo es inseguro (ej. *Implicit Grant*), migrar a un flujo más seguro (ej. *Authorization Code with PKCE*).
- **Escaneo de *Malware*:** Escanear el dispositivo del usuario afectado si se sospecha de un robo de *token* local (*malware*).

5. Recuperación

- **Reautenticación:** Solicitar al usuario/aplicación que se reautentique para

obtener un nuevo *token* válido.

- **Monitoreo Cauteloso:** Mantener el Servidor de Autorización y los Servidores de Recursos bajo monitoreo intensivo para detectar nuevos *tokens* comprometidos o intentos de *replay*.
- **Notificación y Cumplimiento:** Informar a los equipos legales y de cumplimiento si el acceso no autorizado expuso datos sensibles.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar el método exacto utilizado para robar el *token* y la razón por la que la detección de *replay* falló o fue lenta.
- **Fortalecer Políticas:** Implementar medidas como *Proof Key for Code Exchange* (PKCE) si no se utiliza y reducir aún más la vida útil de los *tokens* de acceso.
- **Actualizar Reglas:** Crear reglas específicas de UEBA/SIEM para correlacionar la actividad del *token* con la geolocalización y el comportamiento del usuario.
- **Capacitación:** Instruir a los desarrolladores sobre la seguridad de OAuth 2.0 y la protección de *tokens* en tránsito y en reposo.

Herramientas Típicas: Servidor de Autorización OAuth (ej. Okta, Azure AD), CASB, SIEM/UEBA, WAF, Logs de Auditoría de la Nube, Herramientas de Análisis de Red.

Playbook 25: Exposición por Mala Configuración de Almacenamiento en la Nube

Escenario

Se detecta que un *bucket* de almacenamiento en la nube (ej. AWS S3, Azure Blob Storage, Google Cloud Storage) que contiene datos sensibles ha sido configurado erróneamente con acceso público (o un acceso excesivamente permisivo), lo que permite a usuarios no autenticados o no autorizados acceder, modificar o eliminar el contenido, resultando en una fuga o exposición de datos.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Exposición de Datos - Mala Configuración de Almacenamiento en la Nube
Severidad	Crítica (debido a la exposición potencial de PII, secretos comerciales o datos regulados)
Prioridad	Crítica (la acción inmediata para bloquear el acceso es vital)
Fuentes de Detección	CASB, Herramientas de Postura de Seguridad en la Nube (CSPM), Monitoreo de *Buckets*, Auditoría de Configuración, Reporte Público/Externo

Fases y Acciones

1. Preparación

- **Herramientas CSPM:** Implementar y configurar herramientas de Gestión de la Postura de Seguridad en la Nube (CSPM) para monitorear *buckets* y detectar configuraciones públicas de forma continua.
- **Revisión de Políticas:** Establecer una política de seguridad que prohíba el acceso público a *buckets* de datos sensibles y restringir quién puede modificar políticas de acceso (IAM).
- **Monitoreo de Logs:** Habilitar y auditar los logs de acceso a *buckets* para registrar quién y cuándo accede a los archivos.
- **Inventario de Datos:** Mantener un inventario actualizado de qué datos residen en cada *bucket* y su clasificación de sensibilidad.

2. Detección y Análisis

- **Confirmar la Exposición:** Validar la alerta de CSPM o del sistema de monitoreo sobre el acceso público o los permisos excesivos en el *bucket* afectado.
- **Determinar el Origen:** Identificar el cambio de configuración o la política de IAM que causó la exposición (ej. usuario, rol o *pipeline* que ejecutó el cambio).
- **Evaluar el Alcance:** Revisar los logs de acceso del *bucket* para determinar si terceros accedieron a los datos, qué archivos fueron leídos/descargados, y la criticidad de los datos expuestos.
- **Mapeo MITRE ATT&CK:** T1537 (Abuso de Política de la Nube), T1580 (Uso de Infraestructura de la Nube).

3. Contención

- **Remediación Inmediata:** Cambiar inmediatamente la configuración de acceso del *bucket* para revocar el acceso público o no autorizado (ej. bloquear todo acceso público, aplicar el principio de mínimo privilegio).
- **Auditoría de Políticas:** Bloquear o modificar cualquier política de IAM, ACL o política de *bucket* que haya permitido la exposición.
- **Rotación de Credenciales:** Si el cambio se hizo con credenciales comprometidas (ej. clave API), rotarlas de inmediato.
- **Bloqueo Geográfico/IP (Temporal):** Si la exposición se debe a acceso desde IPs específicas, bloquearlas temporalmente.

4. Erradicación

- **Corregir Causa Raíz:** Aplicar un control permanente para asegurar que la mala configuración no pueda ser revertida fácilmente (ej. bloqueo a nivel de la cuenta de nube).
- **Revisión Completa:** Escanear todos los *buckets* y recursos de almacenamiento de la organización para identificar otras configuraciones

erróneas.

- **Eliminar Datos de *Cache* (Si Aplica):** Si se expuso contenido a través de CDN, invalidar el *cache* para remover cualquier dato sensible que haya sido almacenado temporalmente.

5. Recuperación

- **Validación de Acceso:** Confirmar que solo los usuarios y servicios autorizados tienen acceso al *bucket*.
- **Reanudar Operaciones:** Si alguna aplicación de negocio fue deshabilitada durante la contención, restaurar su acceso al *bucket* con los permisos corregidos.
- **Notificación:** Coordinar con el equipo legal y de cumplimiento para evaluar las obligaciones de notificación a reguladores y a los individuos afectados si se confirmó la fuga de PII o datos regulados.
- **Monitoreo Post-Incidente:** Mantener un monitoreo elevado de logs de acceso al *bucket* por un período para detectar nuevos intentos de acceso anómalo.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar la causa raíz exacta de la mala configuración (ej. error humano, automatización defectuosa, política de *default* insegura).
- **Mejora del Proceso de Despliegue:** Integrar verificaciones de seguridad automatizadas (ej. *Shift-Left*) en los *pipelines* de CI/CD que gestionan la infraestructura en la nube.
- **Reforzar Entrenamiento:** Capacitar al personal de Ingeniería y Operaciones sobre la seguridad de las políticas de IAM y las configuraciones de almacenamiento en la nube.
- **Documentación y Reporte:** Formalizar el informe del incidente y las lecciones aprendidas para actualizar la política de seguridad y el manual de procedimientos.

Herramientas Típicas: CASB (Cloud Access Security Broker), CSPM (Cloud Security Posture Management, ej. Google Cloud Security Command Center, Wiz, Orca), Logs de Auditoría de la Nube (CloudTrail, Azure Activity Log), Herramientas de Infraestructura como Código (Terraform, CloudFormation) con escaneo de seguridad.

Playbook 26: Movimiento Lateral en Cargas de Trabajo en la Nube

Escenario

Un atacante ha comprometido un recurso inicial en un entorno de nube (ej. una Máquina Virtual, un Pod de Kubernetes o un Contenedor) y utiliza ese acceso para saltar hacia otros recursos dentro de la misma red o plataforma de nube. Esto se logra abusando de credenciales de servicio, configuraciones de red débiles, o *exploits* de vulnerabilidades en las cargas de trabajo vecinas, escalando su impacto dentro del entorno cloud.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Movimiento Lateral - Cargas de Trabajo en la Nube / *Container Breakout*
Severidad	Crítica (la propagación permite acceder a múltiples entornos y servicios críticos)
Prioridad	Crítica (la contención inmediata es vital para evitar el compromiso total de la plataforma en la nube)
Fuentes de Detección	Monitoreo de Red en la Nube (VPC Flow Logs), EDR/XDR para Contenedores, SIEM/UEBA, Logs de Auditoría de la Nube

Fases y Acciones

1. Preparación

- **Microsegmentación:** Implementar políticas de red estrictas y de mínimo privilegio entre las cargas de trabajo (VMs, contenedores, funciones sin servidor).

- **Gestión de Identidad de Cargas (IAM):** Asignar roles IAM con el mínimo privilegio a las cargas de trabajo (ej. *service accounts*) y evitar el uso de credenciales fijas.
- **Monitoreo de *Flow Logs*:** Habilitar y analizar los logs de flujo de red (VPC Flow Logs, etc.) en el SIEM para detectar conexiones inusuales entre cargas de trabajo.
- **Seguridad en *Runtime*:** Utilizar herramientas de seguridad para contenedores que detecten la ejecución de comandos inesperados o la creación de conexiones salientes anómalas.

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de EDR/SIEM sobre intentos de conexión anómalos o *logins* a máquinas vecinas desde un host comprometido.
- **Analizar el Tráfico:** Revisar los *Flow Logs* y los logs de la plataforma en la nube para identificar el patrón de salto (ej. uso de SSH/RDP inesperado, acceso a API de nube).
- **Identificar el Vector:** Determinar cómo se logró el salto (ej. abuso de *service account* con permisos excesivos, explotación de una vulnerabilidad de red, robo de claves SSH).
- **Evaluar el Alcance:** Confirmar qué otras VMs, contenedores o servicios se vieron afectados y qué datos se accedieron.
- **Mapeo MITRE ATT&CK:** T1021.001 (Movimiento Lateral: SSH), T1580 (Uso de Infraestructura de la Nube), T1552.001 (Credenciales en Archivos).

3. Contención

- **Aislar Carga de Trabajo Inicial:** Desconectar o aislar inmediatamente la

carga de trabajo (VM/Contenedor) que fue el punto de entrada inicial.

- **Revocar Credenciales de Servicio:** Revocar todas las credenciales o *tokens* de las cuentas de servicio asociadas con la carga de trabajo comprometida que puedan ser utilizadas para el movimiento lateral.

- **Bloqueo de Red:** Aplicar reglas de firewall de forma inmediata para denegar la comunicación desde la carga de trabajo inicial hacia los activos críticos.
- **Forzar *Rolling Update*:** Para entornos de contenedores, forzar una actualización (*rolling update*) de los *pods* potencialmente comprometidos.

4. Erradicación

- **Eliminar *Malware/Backdoor*:** Borrar cualquier artefacto de *malware* o *backdoor* que el atacante haya instalado para establecer la persistencia.
- **Corregir Política IAM:** Modificar el rol IAM de la carga de trabajo inicial para adherirse al mínimo privilegio, eliminando el exceso de permisos que facilitó el movimiento.
- **Parchear Vulnerabilidades:** Aplicar parches a las vulnerabilidades explotadas en el sistema operativo o en el software de la aplicación para evitar la re-explotación.
- **Restablecer Configuraciones:** Revertir cualquier cambio de configuración que haya creado *gaps* de red o *firewalls* internos.

5. Recuperación

- **Reconstruir Cargas de Trabajo:** Si la integridad no puede garantizarse, reconstruir la carga de trabajo a partir de una imagen limpia y verificada.
- **Validación de Segmentación:** Realizar pruebas de conectividad para confirmar que las reglas de microsegmentación están en vigor y son efectivas.
- **Monitoreo Reforzado:** Mantener un monitoreo intensivo de los *Flow Logs* y la actividad de la cuenta de servicio por un período de tiempo prolongado.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar el vector de entrada inicial y la configuración errónea (IAM, Red, OS) que facilitó el movimiento lateral.
- **Mejorar Seguridad *Cloud Native*:** Fortalecer la seguridad del plano de control de la nube y de los orquestadores (Kubernetes).

- **Reforzar Políticas de IAM:** Implementar auditorías automáticas de políticas IAM para evitar que las cargas de trabajo obtengan privilegios excesivos.
- **Capacitación:** Instruir a los equipos de DevOps/Nube sobre los riesgos de las credenciales de servicio y la microsegmentación.

Herramientas Típicas: Logs de Flujo de VPC/VNet (AWS/Azure/GCP), EDR/XDR (con foco en la nube/contenedores), CSPM, SIEM/UEBA, Plataformas de Orquestación (Kubernetes).

Playbook 27: Exportaciones No Autorizadas de *Snapshots* de BD

Escenario

Un atacante o un empleado interno comprometido explota permisos de acceso excesivos o insuficientemente monitoreados dentro de la plataforma de nube para crear una copia no autorizada (*snapshot*) de una base de datos (ej. AWS RDS, Azure SQL, Google Cloud SQL) y la comparte con una cuenta externa, o la copia a una ubicación de almacenamiento accesible públicamente, lo que resulta en una fuga masiva de datos estructurados.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Exposición de Datos - Exportación No Autorizada / Abuso de Acceso a Base de Datos

Severidad	Crítica (la exposición del *snapshot* implica una fuga de la base de datos completa)
Prioridad	Crítica (la acción inmediata es vital para eliminar el *snapshot* externo y revocar el acceso)
Fuentes de Detección	Logs de Auditoría de la Nube (CloudTrail, Azure/GCP Logging), CSPM, Monitoreo de Uso de *Snapshots*, SIEM/UEBA

Fases y Acciones

1. Preparación

- **Mínimo Privilegio (IAM):** Restringir rigurosamente quién puede crear, modificar o, especialmente, COMPARTIR *snapshots* de bases de datos.
- **Detección de Configuración:** Utilizar CSPM para auditar y alertar sobre cualquier *snapshot* que se comparta con cuentas externas o se haga público.
- **Monitoreo de Logs:** Configurar alertas en el SIEM para las llamadas de API específicas de la nube relacionadas con la creación o modificación de políticas de *snapshot* (ej. ModifyDBSnapshotAttribute en AWS).
- **Cifrado de *Snapshots*:** Asegurar que todos los *snapshots* estén cifrados y que el acceso a las claves de cifrado esté estrictamente controlado.

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de CSPM o SIEM que indica una operación de compartición de *snapshot* a una cuenta externa desconocida o no autorizada.
- **Identificar el Rol/Usuario:** Determinar qué identidad (usuario, rol o cuenta de servicio) ejecutó la API para crear y/o compartir el *snapshot*.
- **Evaluar la Sensibilidad:** Determinar la sensibilidad de los datos contenidos

en la base de datos de origen (ej. PII, datos financieros, secretos).

- **Rastrear el Destino:** Identificar la cuenta externa o el *bucket* de almacenamiento donde se exportó o compartió el *snapshot*.
- **Mapeo MITRE ATT&CK:** T1537 (Abuso de Política de la Nube), T1078 (Cuentas Válidas), T1567 (Exfiltración a Servicio de Nube Propio).

3. Contención

- **Revocar el Acceso/Compartición:** Eliminar inmediatamente la política de compartición externa del *snapshot* y hacerla privada.
- **Eliminar *Snapshot* Malicioso:** Si el *snapshot* fue copiado a un *bucket* de almacenamiento, eliminar el archivo tan pronto como se obtenga una copia para análisis forense.
- **Revocar Credenciales:** Revocar de inmediato las claves de acceso de la identidad (rol/usuario) que ejecutó la acción.
- **Bloqueo a Nivel de IAM:** Aplicar una política de denegación *inline* temporal para todas las acciones relacionadas con *snapshots* de DB en el entorno.

4. Erradicación

- **Corregir Política IAM:** Modificar la política del rol/usuario comprometido para eliminar el permiso de compartir o copiar *snapshots* (ej. rds:CopyDBSnapshot).
- **Auditoría de Roles:** Realizar una auditoría de todos los roles con privilegios de *snapshot* para asegurar que se adhieran al mínimo privilegio.
- **Borrar Artefactos:** Asegurar que no existan otros *snapshots* creados por el atacante en el entorno y que las cuentas de destino (si son internas) estén limpias.

5. Recuperación

- **Validación de Roles:** Confirmar que los roles corregidos permiten las operaciones legítimas de *backup* y restauración, pero no la compartición externa.
- **Notificación y Cumplimiento:** Coordinar con Legal y Cumplimiento para

determinar las obligaciones de notificación a reguladores y clientes, ya que se confirmó una fuga de datos.

- **Restablecer Credenciales:** Restablecer las credenciales del usuario/rol afectado y revalidar el MFA (si aplica).

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar el origen del privilegio excesivo (ej. rol preexistente, error en el script de aprovisionamiento, falta de revisión).
- **Mejorar Automatización:** Implementar validaciones en los scripts de infraestructura como código (IaC) que aprueban los *snapshots* solo para cuentas internas.
- **Fortalecer CSPM:** Ajustar las reglas del CSPM para que las alertas de compartición de *snapshots* sean la prioridad más alta.
- **Capacitación:** Instruir al personal de base de datos y de la nube sobre las implicaciones de seguridad de los metadatos y los *snapshots*.

Herramientas Típicas: Logs de Auditoría de la Nube (CloudTrail, etc.), CSPM (Cloud Security Posture Management), IAM (Identity and Access Management), SIEM.

Playbook 28: Intento de Escape de Contenedor (*Container Breakout*)

Escenario

Un atacante explota una vulnerabilidad en el motor de contenedores (ej. Docker, containerd, CRI-O), una mala configuración de permisos (ej. capacidades excesivas, volumen *root* montado) o una falla del núcleo del host para "escapar" del entorno aislado del contenedor y obtener acceso al sistema operativo subyacente (*host*). Esto representa una escalada de privilegios crítica y la anulación de la principal barrera de seguridad del entorno de contenedores.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Escalada de Privilegios - Escape de Contenedor / Compromiso de Host
Severidad	Crítica (el atacante tiene acceso al host, a todos los contenedores y a la red del clúster)
Prioridad	Crítica (la acción inmediata es esencial para aislar el host y detener la propagación)
Fuentes de Detección	EDR/XDR para Contenedores, Plataforma de Seguridad de Contenedores (*Runtime Security*), SIEM/UEBA

Fases y Acciones

1. Preparación

- **Principio de Mínimo Privilegio:** Limitar estrictamente las capacidades de los contenedores y las *service accounts* de Kubernetes. Evitar contenedores ejecutándose como *root*.
- **Parcheo de Host/Kernel:** Mantener el sistema operativo del host y el motor de contenedores (Docker/K8s) con los últimos parches de seguridad.
- **Seguridad en *Runtime*:** Implementar herramientas de seguridad que monitoreen la actividad del contenedor y del host para detectar llamadas al sistema inusuales o ejecución de comandos fuera de la línea base.
- **Monitoreo de Configuración:** Utilizar *Admission Controllers* en Kubernetes (ej. Gatekeeper, Kyverno) para prohibir la ejecución de contenedores inseguros (ej. *Privileged* o montando *hostPath*).

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de *Runtime Security* o EDR/XDR sobre una actividad inusual en el host proveniente de un proceso dentro del contenedor (ej. montaje de sistemas de archivos, uso de herramientas de red en el host, manipulación de *namespaces*).
- **Identificar el Vector:** Determinar la vulnerabilidad exacta que permitió el escape (ej. CVE de Docker, mala configuración de *capability*, *Exploit* de Kernel).

- **Identificar el Contenedor/Pod:** Determinar el nombre del contenedor y el *pod* de origen, el *namespace* y el *cluster* de Kubernetes afectado.
- **Evaluar el Alcance:** Revisar los logs del host para ver si el atacante logró establecer persistencia o realizar movimiento lateral a otros contenedores/VMs.
- **Mapeo MITRE ATT&CK:** T1611 (Escape de Contenedor), T1580 (Uso de Infraestructura de la Nube).

3. Contención

- **Aislar el Nodo/Host:** Desconectar inmediatamente el nodo de Kubernetes o el host que ejecuta el contenedor comprometido de la red principal.
- **Detener el Contenedor:** Forzar el cierre inmediato del contenedor y eliminar el *pod* (o el contenedor) malicioso para detener la actividad en el host.
- **Revocar Credenciales:** Revocar cualquier *service account token* o credencial que pudiera haber sido robada del host.
- **Bloqueo a Nivel de Firewall:** Aplicar reglas de *firewall* de red (o políticas de red de K8s) para aislar el host o el *namespace* afectado.

4. Erradicación

- **Parchear/Actualizar:** Aplicar el parche de seguridad necesario al host y/o al motor de contenedores para la vulnerabilidad explotada.
- **Corregir Configuración:** Modificar el manifiesto del contenedor o la política de K8s para eliminar la configuración insegura que permitió el escape.
- **Reconstruir la Imagen:** Crear una nueva imagen de contenedor limpia y

segura (si la imagen original fue el vector).

- **Limpieza de Artefactos:** Borrar cualquier artefacto malicioso, clave SSH o *backdoor* que el atacante haya dejado en el sistema de archivos del host.

5. Recuperación

- **Reconstruir el Host:** Desaprovisionar y reconstruir el nodo/host comprometido desde cero con una imagen base verificada.
- **Redespliegue Seguro:** Desplegar la carga de trabajo en un nodo limpio, asegurándose de que la configuración de seguridad de *runtime* (ej. Seccomp, AppArmor) esté en su lugar.
- **Monitoreo Reforzado:** Mantener el nuevo host bajo monitoreo intensivo por 7-14 días.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar la versión exacta del software y la configuración que permitió el *breakout* y el *exploit* específico utilizado.
- **Mejorar Hardening:** Reforzar la configuración de seguridad del host y los *runtime profiles* (ej. SELinux, AppArmor, Seccomp) para los contenedores.
- **Fortalecer Políticas:** Implementar políticas de seguridad que bloqueen la creación de contenedores con capacidades peligrosas o montajes de host críticos.
- **Documentación:** Reportar la brecha a los equipos de desarrollo y *site reliability* (SRE) para asegurar la prevención en futuros despliegues.

Herramientas Típicas: Plataformas de Seguridad de Contenedores (ej. Falco, Aqua Security), EDR/XDR, Logs de Auditoría de K8s, Monitoreo de Host (Syslog), SIEM.

Playbook 29: Uso de SaaS *Shadow IT* y Exposición de Datos

Escenario

Un empleado utiliza servicios de almacenamiento en la nube personales y no autorizados (ej. Dropbox, Google Drive personal, OneDrive personal, WeTransfer)

para almacenar, compartir o transferir datos corporativos sensibles. Esto crea un riesgo de exposición y pérdida de control sobre la información, ya que los datos se mueven fuera del perímetro de seguridad, las políticas de cumplimiento y el monitoreo de la organización.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Exposición de Datos - *Shadow IT* / Transferencia No Autorizada de Archivos
Severidad	Alta (riesgo potencial de seguridad, cumplimiento, y fuga de datos persistente)
Prioridad	Alta (necesidad de detener el flujo de datos y recuperar la información expuesta)
Fuentes de Detección	DLP (Data Loss Prevention), Logs de Proxy/Firewall, CASB, EDR, Monitoreo de Red Saliente, UEBA

Fases y Acciones

1. Preparación

- **DLP en *Endpoint* y Red:** Configurar el DLP para detectar y bloquear la transferencia de archivos con alto contenido sensible (ej. PII, secretos, código fuente) a servicios de almacenamiento en la nube no autorizados.
- **Políticas de Uso Aceptable:** Establecer una política clara que prohíba el uso de cuentas personales o de terceros para el almacenamiento y transferencia de datos corporativos.
- **Bloqueo/Monitorización de URLs:** Utilizar el firewall/proxy para bloquear o

monitorear activamente el tráfico hacia servicios *Shadow IT* conocidos.

- **Promoción de Servicios Seguros:** Asegurar que los empleados tengan acceso fácil y bien soportado a las herramientas corporativas de almacenamiento seguro (ej. Google Drive/OneDrive corporativo).
- **Capacitación:** Instruir a los empleados sobre los riesgos de los servicios personales en la nube y los mecanismos de protección de datos de la empresa.

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de DLP que indica un intento exitoso o fallido de subir un archivo sensible a un dominio personal o no autorizado.
- **Identificar al Usuario y el Dato:** Determinar el empleado responsable, el tipo de dato (ej. lista de clientes, plan de negocio) y el volumen de la transferencia.
- **Rastrear el Destino:** Determinar a qué servicio específico (ej. Dropbox, Box, Google Drive personal) se subió el archivo.
- **Evaluar el Riesgo:** Clasificar si el dato es solo sensible o también está sujeto a regulaciones estrictas (ej. GDPR, HIPAA).
- **Mapeo MITRE ATT&CK:** T1048.003 (Exfiltración sobre Protocolo Alternativo: Transferencia a la Nube), T1567 (Exfiltración a Servicio de Nube Propio).

3. Contención

- **Acción Inmediata de DLP:** Si la transferencia está en curso, forzar el bloqueo inmediato en el *endpoint* o en el *gateway*.
- **Entrevista con RRHH/Legal:** Iniciar el protocolo de manejo de incidentes internos, contactando al usuario en presencia de Recursos Humanos o Legal.
- **Aislamiento de Dispositivo:** Aislar temporalmente el *endpoint* del usuario para asegurar que no se estén realizando otras transferencias no autorizadas.
- **Cierre de Sesiones de Navegador:** Si es un dispositivo corporativo, limpiar el caché y el historial para eliminar cualquier persistencia o *login* a servicios

no autorizados.

4. Erradicación

- **Eliminar el Acceso a Servicios:** Si la cuenta personal del empleado fue utilizada a través de un dispositivo corporativo, desinstalar cualquier aplicación cliente (*sync client*) de ese servicio *Shadow IT*.
- **Eliminar Datos (Si Es Posible):** Si el dato se subió a una cuenta que la empresa puede controlar, o si el empleado coopera, gestionar la eliminación del archivo del servicio en la nube no autorizado.
- **Reforzar DLP:** Ajustar las reglas de DLP con el patrón de transferencia o la huella digital del archivo específico que se expuso.

5. Recuperación

- **Auditoría Forense:** Realizar un análisis forense al dispositivo del usuario para asegurar que no haya otros artefactos de exfiltración.
- **Notificación y Cumplimiento:** Coordinar con Legal y Cumplimiento para evaluar si la exposición de los datos requiere notificación a reguladores o a los clientes afectados.
- **Capacitación Correctiva:** Proporcionar una capacitación de seguridad de datos específica y documentada al usuario.
- **Restablecer el Acceso:** Restaurar el acceso normal del usuario después de la confirmación de la erradicación y la acción disciplinaria (si aplica).

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar la razón por la que el empleado eligió el *Shadow IT* (ej. limitación del tamaño de archivo en el Drive corporativo, falta de función de compartición externa, ineficiencia).
- **Mejorar Herramientas:** Invertir en la mejora de las herramientas corporativas para que sean tan eficientes como los servicios de consumo,

reduciendo el incentivo para usar *Shadow IT*.

- **Fortalecer Controles DLP:** Revisar y optimizar la cobertura de DLP para nuevos servicios en la nube no autorizados.
- **Documentación y Acción Disciplinaria:** Formalizar el informe del incidente y documentar la acción disciplinaria tomada en coordinación con RRHH.

Herramientas Típicas: DLP (Data Loss Prevention - Endpoint y Network), CASB (Cloud Access Security Broker), Firewall/Proxy, UEBA (User and Entity Behavior Analytics), EDR/XDR.

Playbook 30: Fuga de Claves API vía GitHub Público

Escenario

Un desarrollador, accidentalmente o por descuido, incluye credenciales sensibles como Claves API, *tokens* de acceso, contraseñas o claves privadas dentro de un repositorio de código que es público o accesible externamente (ej. GitHub, GitLab, Bitbucket). Esto expone los secretos a cualquier persona, incluido un atacante automatizado que realiza un *scaneado* continuo de repositorios en busca de credenciales activas, lo que puede llevar al compromiso de servicios en la nube o de aplicaciones.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Exposición de Datos - Fuga de Claves API / Compromiso de Repositorio
Severidad	Crítica (acceso directo a servicios sensibles, potencial pérdida financiera o de datos)

Prioridad	Crítica (la acción inmediata es esencial para revocar la clave y evitar la explotación)
Fuentes de Detección	Herramientas de Escaneo de Secretos (Gitleaks, TruffleHog), Plataforma de Nube, Reporte Externo

Fases y Acciones

1. Preparación

- **Escaneo de Secretos:** Implementar escaneo de secretos automatizado en pre-commit (*hooks* locales) y en el *pipeline* de CI/CD para detectar secretos antes de que lleguen al repositorio.
- **Gestión de Secretos:** Utilizar soluciones dedicadas (ej. HashiCorp Vault, AWS Secrets Manager) para inyectar secretos de forma dinámica, evitando que sean almacenados en el código.
- **Monitoreo de Uso de Claves:** Configurar alertas en la plataforma de nube (ej. AWS CloudTrail) sobre el uso inusual de las claves que podrían ser expuestas.
- **Políticas de Repositorio:** Aplicar políticas para prohibir la creación de repositorios públicos no autorizados.
- **Capacitación:** Instruir a los desarrolladores sobre la importancia de las variables de entorno y los riesgos de subir secretos.

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta del escáner de secretos o de la plataforma de nube que indica una clave de acceso o *token* en un repositorio público.
- **Identificar el Secreto:** Determinar el tipo de secreto (ej. AWS Access Key, Token de GitHub, Credencial de DB) y el servicio al que otorga acceso.

- **Evaluar el Uso:** Revisar los logs de la plataforma comprometida para determinar si la clave expuesta ha sido utilizada por un tercero desde su exposición.
- **Identificar el *Commit*:** Rastrear el *commit*, el autor y el archivo exacto donde se filtró la clave.
- **Mapeo MITRE ATT&CK:** T1552.001 (Descubrimiento de Credenciales: Almacenamiento en Archivos), T1580 (Uso de Infraestructura de la Nube).

3. Contención

- **Revocación Inmediata:** Revocar o deshabilitar inmediatamente el secreto/clave API expuesta en el servicio de destino (ej. AWS IAM, Stripe Dashboard). **Esta es la acción de máxima prioridad.**
- **Bloqueo de Repositorio:** Si es posible, hacer privado el repositorio comprometido o eliminar el archivo que contiene la clave (aunque no borra el historial de Git).
- **Notificación:** Contactar al equipo de desarrollo y al propietario del secreto/servicio para informar sobre la revocación y la brecha.

4. Erradicación

- **Eliminar del Historial de Git:** Utilizar herramientas de reescritura de historial (ej. git filter-repo, BFG Repo-Cleaner) para eliminar permanentemente la clave del historial del repositorio.
- **Validación:** Asegurar que la clave ha sido eliminada del repositorio, y que el *commit* limpio ha sido forzado al repositorio.
- **Revisar *Commits* Adicionales:** Escanear el historial de otros repositorios del mismo usuario para detectar más secretos filtrados.
- **Reemplazo Seguro:** Emitir un nuevo secreto y asegurar que solo se almacene en la bóveda de secretos o se inyecte de forma segura.

5. Recuperación

- **Restaurar Servicio:** Restaurar el servicio o la aplicación afectada con la nueva clave API.

- **Monitoreo Reforzado:** Mantener un monitoreo de alto nivel en el servicio al que daba acceso la clave por un período para detectar cualquier actividad anómala residual.
- **Validación del *Pipeline*:** Asegurar que el escáner de secretos ahora está integrado y funcionando correctamente en el *pipeline* del desarrollador.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar el error específico (ej. falta de uso de variables de entorno, *pre-commit hook* deshabilitado).
- **Fortalecer Automatización:** Hacer obligatorio el escaneo de secretos en CI/CD y automatizar la revocación de claves que se detecten en repositorios públicos.
- **Mejorar Gestión de Secretos:** Reforzar el uso de *service roles* (en lugar de claves estáticas) siempre que sea posible.
- **Capacitación:** Implementar una sesión de capacitación obligatoria para desarrolladores sobre "Seguridad de Secretos" y el uso correcto de Git.

Herramientas Típicas: Gitleaks, TruffleHog, Git filter-repo, BFG Repo-Cleaner, Soluciones de Gestión de Secretos (HashiCorp Vault, AWS Secrets Manager), Logs de Auditoría de Servicios en la Nube (CloudTrail, etc.).

Playbook 31: Acceso No Autorizado a Secretos CI/CD

Escenario

Un atacante (interno o externo) obtiene acceso a las credenciales, claves API, *tokens* o variables de entorno sensibles que están almacenadas o inyectadas en un *pipeline* de Integración Continua/Despliegue Continuo (CI/CD) (ej. Jenkins, GitHub Actions, GitLab CI). El objetivo es robar estos secretos para escalar privilegios o acceder a entornos de producción, bases de datos o servicios de la nube a los que el *pipeline* tiene acceso legítimo.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Compromiso de Identidad - Robo de Secretos / Ataque a la Cadena de Suministro
Severidad	Crítica (acceso directo a credenciales de alto privilegio y entornos de producción)
Prioridad	Crítica (la acción inmediata es esencial para revocar los secretos expuestos)
Fuentes de Detección	Logs de Auditoría de Plataformas CI/CD, Logs de Acceso a *Vaults* de Secretos, SIEM, Monitoreo de Red

Fases y Acciones

1. Preparación

- **Uso de *Secrets Vault*:** Almacenar todos los secretos en una solución de gestión de secretos dedicada (ej. HashiCorp Vault, AWS/Azure/GCP Secrets Manager), no en variables de entorno sin cifrar.
- **Inyección Temporal:** Utilizar la inyección dinámica de secretos en el *pipeline* para que sean válidos solo durante el tiempo de ejecución del *job*.
- **Mínimo Privilegio de *Pipeline*:** Configurar las cuentas de servicio (*runners*) del CI/CD con la menor cantidad de permisos necesarios para la tarea.
- **Auditoría de Logs:** Monitorear y alertar sobre intentos de acceder al *vault* de secretos desde ubicaciones inesperadas o por parte de un *job* inusual.
- **Rotación Automática:** Implementar la rotación automática de los secretos para reducir la ventana de oportunidad de una clave filtrada.

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de SIEM o del *Secrets Vault* sobre

acceso a secretos con credenciales de *pipeline* desde IPs externas o patrones anómalos.

- **Identificar el Secreto Expuesto:** Determinar el nombre, el valor y el alcance (ej. credenciales de producción, clave de despliegue) del secreto comprometido.
- **Rastrear el Vector:** Determinar cómo se filtró el secreto (ej. *log* no cifrado, vulnerabilidad en un *plugin* de CI/CD, *exploit* en el servidor *build*).
- **Evaluar el Impacto:** Revisar los logs de los servicios a los que el secreto otorga acceso para ver si ya fue utilizado por el atacante.
- **Mapeo MITRE ATT&CK:** T1552.001 (Descubrimiento de Credenciales: Almacenamiento en Archivos), T1580 (Uso de Infraestructura de la Nube).

3. Contención

- **Revocación Inmediata del Secreto:** Revocar de inmediato el secreto comprometido en el *Secrets Vault* y en cualquier servicio al que dé acceso. **Esta es la acción de máxima prioridad.**
- **Detener el *Pipeline*:** Pausar o deshabilitar todos los *jobs* de CI/CD que utilicen el secreto comprometido o que se ejecuten en la plataforma explotada.
- **Aislar Servidor *Build*:** Aislar de la red el servidor *build* o el *runner* del *pipeline* si se sospecha que el servidor fue el punto de compromiso.
- **Invalidar Sesiones:** Invalidar todas las sesiones activas y *tokens* asociados con la cuenta de servicio del *pipeline*.

4. Erradicación

- **Eliminar el Vector:** Corregir la vulnerabilidad (ej. parchear el servidor, actualizar el *plugin*, asegurar el código de despliegue) que permitió la filtración del secreto.
- **Rotación de Secretos Afectados:** Generar un nuevo secreto limpio para reemplazar el valor comprometido.

- **Purgar Logs:** Eliminar o asegurar todos los logs y artefactos de *build* para asegurarse de que el secreto no esté almacenado en texto plano en ningún lugar.
- **Refuerzo de *Vault*:** Auditar y reforzar la política de acceso del *Secrets Vault* para el *pipeline* afectado.

5. Recuperación

- **Validación del Nuevo Secreto:** Insertar el nuevo secreto de forma segura en el *Secrets Vault* y confirmar que el *pipeline* puede acceder correctamente para un *job* de prueba.

- **Reanudar Operaciones:** Restaurar la funcionalidad completa del *pipeline* de CI/CD.
- **Monitoreo Reforzado:** Mantener un monitoreo intensivo del *pipeline* y el *Secrets Vault* por un período para detectar cualquier intento de reutilización del secreto revocado o un nuevo compromiso.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar el error de configuración (ej. secretos en un archivo .env, log de depuración activado) o la vulnerabilidad que expuso el secreto.
- **Fortalecer Controles:** Implementar la inyección de secretos directamente en memoria a través del *Secrets Vault* en lugar de variables de entorno.
- **Mejorar Políticas:** Reforzar las políticas de seguridad en la plataforma CI/CD (ej. prohibir ciertos *plugins* o comandos inseguros).
- **Capacitación:** Instruir a los desarrolladores y equipos de DevOps en el uso correcto de la bóveda de secretos y las prácticas de "código limpio" para variables.

Herramientas Típicas: *Secrets Vault* (HashiCorp Vault, etc.), Logs de Auditoría de CI/CD, SIEM, Escaneo de Secretos (Gitleaks, TruffleHog), Plataformas de Nube (para revocar claves).

Playbook 32: Explotación de Día Cero (*Zero-Day*) en Librerías

Escenario

Se detecta la explotación activa de una vulnerabilidad de Día Cero (*Zero-Day*) en una librería, un componente o un *framework* de software ampliamente utilizado (ej. Log4j, Spring4Shell) que está integrado en múltiples aplicaciones internas o de cara al público. Dado que no existe un parche oficial disponible de inmediato, la organización debe actuar bajo una alta incertidumbre para mitigar el riesgo.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Explotación - Vulnerabilidad de Día Cero en Librería / Compromiso Masivo
Severidad	Crítica (la vulnerabilidad afecta a numerosos sistemas y el impacto puede ser total)
Prioridad	Crítica (la acción inmediata es esencial, a menudo con la necesidad de implementar mitigaciones temporales)
Fuentes de Detección	Inteligencia de Amenazas (Vendor/Comunidad), Logs de WAF/IDS/IPS, Escaneo de Vulnerabilidades (DAST/SAST)

Fases y Acciones

1. Preparación

- **Inventario de Componentes (SBOM):** Mantener un inventario de Material de Software (SBOM) para identificar rápidamente qué activos utilizan la librería/componente afectado.

- **Detección de Exploit:** Configurar el WAF, IDS/IPS y EDR/XDR con reglas heurísticas o de emergencia para detectar patrones de explotación del *Zero-Day* (incluso si no hay firma oficial).
- **Aislamiento de Emergencia:** Preparar planes de contingencia para desconectar rápidamente la infraestructura crítica que utilice la librería vulnerable.
- **Proceso de Parcheo Rápido:** Tener un proceso ágil para aplicar parches o mitigaciones *out-of-band* tan pronto como sean liberados.

2. Detección y Análisis

- **Confirmar la Explotación:** Validar los reportes de inteligencia o las alertas internas sobre la explotación activa del *Zero-Day*.
- **Identificar Activos Afectados:** Utilizar el SBOM y escáneres de vulnerabilidades para determinar todos los sistemas (servidores, contenedores, funciones) que contienen la librería vulnerable.
- **Analizar Logs:** Revisar los logs de la aplicación, WAF y IDS en busca de patrones de *payloads* o secuencias de explotación del atacante.
- **Evaluar el Impacto:** Determinar si el ataque ha sido exitoso en alguno de los activos y si se ha logrado acceso o movimiento lateral (lo que activa el *playbook* de "Compromiso de Host").
- **Mapeo MITRE ATT&CK:** T1068 (Explotación de Vulnerabilidad), T1562.007 (Evasión de Defensa: Manipulación de *Runtime*), T1059 (Ejecución de Comandos).

3. Contención

- **Implementar Mitigación Temporal:** Aplicar la mitigación temporal inmediata recomendada por el proveedor o la comunidad de seguridad (ej. desactivar una función vulnerable, remover clases Java específicas, aplicar una regla WAF estricta).
- **Aislamiento de Infraestructura Crítica:** Desconectar o segmentar de la red la infraestructura de alto valor que no pueda ser mitigada de forma inmediata.

- **Bloqueo Perimetral:** Implementar reglas de *blocking* en el WAF/IDS/IPS para todos los patrones de *exploit* conocidos.
- **Rotación de Credenciales:** Asumir que el atacante pudo haber robado credenciales de cualquier sistema afectado y rotarlas de inmediato.

4. Erradicación

- **Aplicación del Parche (Hotfix):** Tan pronto como esté disponible, aplicar el parche o la actualización del componente afectado en todos los activos.
- **Limpieza de Artefactos:** Si se confirmó el compromiso, eliminar cualquier *web shell*, *backdoor* o archivo malicioso que el atacante haya dejado en los sistemas.

- **Análisis de Binarios:** Escanear los binarios y los procesos de ejecución para asegurar que la librería vulnerable haya sido eliminada o parcheada correctamente.
- **Restricciones de Código:** Si no hay parche, forzar una versión anterior y no vulnerable o eliminar temporalmente la funcionalidad dependiente.

5. Recuperación

- **Validación del Parche:** Realizar escaneos de vulnerabilidad intensivos post-parche para confirmar que la vulnerabilidad ya no es explotable.
- **Restauración de Sistemas Comprometidos:** Reconstruir o restaurar desde una copia de seguridad limpia cualquier sistema que se haya confirmado como comprometido antes de volver a la red.
- **Monitoreo Reforzado:** Mantener un monitoreo intensivo durante al menos 7 días después del parcheo para detectar cualquier actividad lateral tardía del atacante.
- **Rehabilitación de Servicios:** Reintegrar los servicios que fueron desconectados durante la fase de contención.

6. Lecciones Aprendidas e Informes

- **Análisis Post-Incidente:** Documentar la línea de tiempo, las decisiones de

mitigación tomadas y la eficacia de la respuesta bajo la presión del *Zero-Day*.

- **Mejorar SBOM:** Utilizar este incidente para verificar y mejorar el proceso de mantenimiento del Inventario de Software (SBOM).
- **Fortalecer Defensas:** Desarrollar un plan para implementar *Virtual Patching* (parcheo virtual) y herramientas de seguridad de *runtime* más robustas.
- **Comunicación con Clientes:** Si el producto de la organización estaba afectado, gestionar la comunicación con los clientes sobre el parche de seguridad y el impacto.

Herramientas Típicas: WAF (Web Application Firewall), IDS/IPS, EDR/XDR, Herramientas de Escaneo de Vulnerabilidades (ej. Nessus, Qualys), Escáneres de Composición de Software (SCA), Plataformas de Seguridad de *Runtime*.

Playbook 33: Abuso de *Tokens* de Sesión Robados en SaaS (Secuestro de Sesión)

Escenario

Un atacante obtiene el *token* de sesión (ej. *cookie* de sesión) de un usuario legítimo a través de un ataque de *Cross-Site Scripting* (XSS), un ataque *Man-in-the-Middle* (MitM) o un *malware* en el *endpoint*. El atacante reutiliza este *token* en su propio navegador para suplantar la identidad del usuario y tomar el control de su sesión activa en una aplicación SaaS (Software as a Service) o una plataforma web, logrando acceso no autorizado sin necesidad de credenciales de inicio de sesión.

Clasificación del Incidente

Categoría	Detalles
Tipo de Incidente	Compromiso de Identidad - Secuestro de Sesión / Robo de *Token*

Severidad	Alta (acceso a los datos del usuario en la sesión, eludiendo MFA)
Prioridad	Crítica (la acción inmediata es esencial para terminar la sesión secuestrada)
Fuentes de Detección	Logs de Aplicación SaaS, SIEM/UEBA, Logs de Acceso de IDP, Monitoreo de Red, EDR/XDR, WAF/IDS/IPS

Fases y Acciones

1. Preparación

- **Protección de *Cookies*:** Asegurar que las *cookies* de sesión estén configuradas con banderas de seguridad (ej. HttpOnly, Secure, SameSite) para prevenir XSS y ataques de red.
- **Vida Útil Corta de Sesión:** Configurar un tiempo de vida (TTL) corto para los *tokens* de sesión y forzar la reautenticación después de inactividad o un período.
- **Monitoreo de Sesiones:** Implementar monitoreo en el IDP (Proveedor de Identidad) o la aplicación SaaS para detectar el uso simultáneo del mismo *token* desde ubicaciones o User Agents muy disímiles (*impossible travel*).
- **Detección de XSS:** Utilizar WAF y herramientas de escaneo de vulnerabilidades para prevenir la inyección de código XSS, un vector común para el robo de *cookies*.

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de UEBA/SIEM sobre actividad anómala dentro de una sesión activa (ej. cambios de configuración, descargas masivas, *impossible travel*).
- **Identificar el *Token*:** Determinar el ID de la sesión y el *token* que está siendo

abusado.

- **Rastrear la Fuente:** Analizar los logs de acceso de la aplicación para ver la geolocalización y los dispositivos utilizados por el usuario legítimo y el atacante (suplantador).
- **Determinar el Vector de Robo:** Investigar cómo el *token* fue interceptado (ej. *malware* en el *endpoint*, un ataque MitM en una red no segura, *phishing* de sesión).
- **Evaluar el Alcance:** Confirmar qué acciones maliciosas se realizaron durante el secuestro (ej. exfiltración de datos, modificación de configuraciones, envío de correos).

- **Mapeo MITRE ATT&CK:** T1539 (Abuso de *Tokens* de Acceso de Aplicación), T1550.001 (*Use Alternate Authentication: Application Access Token*), T1566 (Phishing).

3. Contención

- **Terminar la Sesión (Logout):** Revocar o invalidar de inmediato el *token* de sesión secuestrado y cerrar forzosamente todas las sesiones activas del usuario afectado. **Esta es la acción de máxima prioridad.**
- **Revocar Credenciales (Opcional):** Forzar el restablecimiento de la contraseña del usuario y asegurar que el MFA esté activo.
- **Aislar el *Endpoint*:** Si el vector fue el *malware* en el *endpoint*, aislar inmediatamente el dispositivo del usuario de la red.
- **Bloqueo Geográfico/IP:** Si la IP del atacante es conocida, bloquearla temporalmente a nivel perimetral.

4. Erradicación

- **Eliminar *Malware/Exploit*:** Si se confirmó *malware* o *exploit* en el *endpoint* o la aplicación, eliminar la causa raíz.
- **Limpieza de *Backdoors*:** Revisar la cuenta secuestrada en busca de reglas de reenvío de correo, cambios en la configuración o *backdoors* de

persistencia que el atacante haya podido dejar.

- **Parchear Vulnerabilidad XSS:** Si el vector fue un XSS, aplicar un parche de código o una mitigación a nivel de WAF para prevenir futuras inyecciones.
- **Reforzar Banderas:** Asegurar que las *cookies* de sesión usen HttpOnly y Secure en todas las aplicaciones críticas.

5. Recuperación

- **Validación del Usuario:** Solicitar al usuario que se reautentique con su nueva contraseña y MFA.
- **Restauración de Configuración:** Revertir cualquier cambio no autorizado en la configuración del servicio SaaS realizado por el atacante.
- **Monitoreo Reforzado:** Mantener un monitoreo intensivo del patrón de inicio de sesión y la actividad del usuario afectado por un período.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar el método exacto utilizado para robar el *token* (ej. librería vulnerable, *endpoint* XSS, *malware* de info-stealer).
- **Fortalecer Controles:** Reforzar las políticas de seguridad de la aplicación (CSP, XSS *hardening*) y el uso de EDR/XDR en los *endpoints* para detectar *malware* de robo de sesión.
- **Mejorar Políticas de Sesión:** Implementar políticas de cierre de sesión más agresivas y utilizar mecanismos de enlace de sesión (ej. *token binding*) si es compatible con la aplicación.
- **Capacitación:** Instruir a los usuarios sobre cómo verificar las URL y los riesgos de utilizar redes Wi-Fi públicas para acceder a información sensible.

Herramientas Típicas: WAF/IDS/IPS, EDR/XDR, SIEM/UEBA, Plataformas de Gestión de Identidad (IDP), Logs de Servidor Web/SaaS.

Playbook 34: Ransomware Nativo de la Nube en Almacenamiento de Objetos

Escenario

Un atacante, que ha comprometido una clave de acceso API o un rol IAM de una cuenta de servicio, utiliza ese acceso privilegiado para cifrar o eliminar objetos de forma masiva en *buckets* de almacenamiento en la nube (ej. AWS S3, Azure Blob Storage, Google Cloud Storage). Esto resulta en la pérdida de disponibilidad de los datos y, a menudo, la aparición de una nota de rescate en el *bucket* o en un recurso asociado.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Malware - Ransomware en la Nube / Disponibilidad y Confidencialidad
Severidad	Crítica (impacto directo en la continuidad del negocio y la pérdida de datos a escala)
Prioridad	Crítica (la acción inmediata es esencial para detener el proceso de cifrado)
Fuentes de Detección	Logs de Auditoría de la Nube (CloudTrail, etc.), SIEM/UEBA, CASB, Monitoreo de Almacenamiento (ej. S3 *Events*)

Fases y Acciones

1. Preparación

- **Inmutabilidad y Versionado:** Habilitar el *Object Lock* y el *Versionado* en los *buckets* críticos para prevenir la eliminación o sobrescritura de objetos.
- **Mínimo Privilegio (IAM):** Aplicar estrictamente el mínimo privilegio a roles

y cuentas de servicio, especialmente a las que pueden escribir o eliminar en *buckets*.

- **Monitoreo de *API Calls*:** Configurar alertas en el SIEM para detectar picos anómalos de llamadas de API de escritura/eliminación, ejemplo:

s3:PutObject

s3:DeleteObject

desde una sola identidad.

- **Separación de Cuentas:** Utilizar cuentas o proyectos separados para la administración del almacenamiento y el uso de la aplicación.
- **Copias de Seguridad (Cross-Region):** Replicar copias de seguridad a una cuenta diferente o a una región distinta con acceso estrictamente restringido.

2. Detección y Análisis

- **Confirmar el Ataque:** Investigar la alerta de logs de la nube o SIEM que indica una tasa de eliminación/cifrado de objetos inusualmente alta.
- **Identificar la Identidad:** Determinar la clave de acceso, el rol IAM o la cuenta de servicio exacta que está realizando las operaciones maliciosas.
- **Analizar Logs de Acceso:** Revisar los logs de auditoría para determinar qué objetos fueron afectados (cifrados/eliminados) y el patrón de las operaciones.
- **Rastrear el Origen:** Identificar la IP o el recurso desde donde se originan las llamadas de API maliciosas.
- **Evaluar el Alcance:** Determinar el número de *buckets* y la sensibilidad de los datos afectados.
- **Mapeo MITRE ATT&CK:** T1486 (Datos Cifrados para Impacto), T1537 (Abuso de Política de la Nube), T1078 (Cuentas Válidas).

3. Contención

- **Revocación Inmediata:** Revocar o deshabilitar inmediatamente la clave de

acceso o el rol IAM que está siendo abusado. **Esta es la acción de máxima prioridad para detener el cifrado.**

- **Bloqueo de *Bucket*:** Aplicar una política de denegación *inline* temporal a los *buckets* afectados para impedir cualquier nueva escritura o eliminación de objetos , ejemplo:
  Deny: s3:*

- **Aislamiento de Origen:** Si el atacante está operando desde una VM o un recurso interno, aislar ese recurso de la red.
- **Deshabilitar API:** Si es necesario y el riesgo es crítico, deshabilitar temporalmente las API de *Object Write/Delete* en la cuenta afectada.

4. Erradicación

- **Eliminar el Vector:** Asegurar que la causa raíz del compromiso de la credencial (ej. código fuente con clave *hardcodeada*, *phishing* de desarrollador) haya sido eliminada.
- **Auditoría de Roles:** Realizar una auditoría de todos los roles similares para prevenir el mismo error de configuración.
- **Borrar Objetos Cifrados:** Si los objetos cifrados son irreversibles, eliminarlos del *bucket* y del sistema de versionado, manteniendo solo las versiones limpias.
- **Rotación de Credenciales:** Implementar una rotación masiva de credenciales para todas las identidades de servicio de alto riesgo.

5. Recuperación

- **Restauración de Versiones Limpias:** Utilizar el mecanismo de *Versionado* o *Object Lock* para restaurar los objetos a la última versión limpia conocida (pre-cifrado).
- **Validación de Integridad:** Confirmar que los datos restaurados son íntegros y no fueron alterados previamente al cifrado.
- **Monitoreo Reforzado:** Mantener el monitoreo de las API y los *buckets* afectados a un nivel Crítico por un período.
- **Notificación y Cumplimiento:** Coordinar con Legal y Cumplimiento para

evaluar las obligaciones de notificación y documentar la pérdida de datos.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar cómo se comprometió la credencial de alto privilegio y por qué fallaron los controles de mínimo privilegio.
- **Fortalecer Políticas de IAM:** Reforzar las políticas de IAM para limitar las operaciones de escritura/eliminación solo a los recursos que las necesitan.
- **Mejorar Configuraciones:** Asegurar que el *Object Lock* o la *Inmutabilidad* estén habilitados por defecto en todos los *buckets* críticos.
- **Capacitación:** Instruir a los desarrolladores y equipos de DevOps en las implicaciones de seguridad de las claves de acceso IAM y la gestión de secretos.

Herramientas Típicas: Logs de Auditoría de la Nube (CloudTrail, etc.), CSPM, SIEM/UEBA, CASB, Plataformas de Orquestación (para automatizar la revocación de claves).

Playbook 35: Insider Malicioso Preparando Datos (*Staging*)

Escenario

Un empleado interno con intención maliciosa, utilizando su acceso legítimo, acumula y organiza datos sensibles, secretos comerciales o PII de la organización. El objetivo es "preparar el terreno" moviendo estos datos desde sus ubicaciones normales (ej. bases de datos, repositorios) a una zona de tránsito temporal o personal (ej. carpeta local cifrada, almacenamiento en la nube personal, servidor interno poco monitoreado) antes de la exfiltración final y masiva.

Clasificación del Incidente

Categoría	Detalles

Tipo de Incidente	Amenaza Interna - *Staging* de Datos / Preparación para Exfiltración
Severidad	Alta (la amenaza está activa y la fuga de datos es inminente)
Prioridad	Crítica (la detección y contención temprana son vitales para prevenir la fuga masiva)
Fuentes de Detección	DLP (Data Loss Prevention), UEBA, Logs de Acceso a Archivos, EDR/XDR, Logs de Transferencia de Red

Fases y Acciones

1. Preparación

- **UEBA y *Baseline*:** Establecer una línea base del comportamiento normal de acceso a archivos y carpetas de cada usuario para detectar desviaciones (ej. acceso nocturno, descarga inusual de documentos, acceso a archivos no relacionados con su trabajo).
- **DLP y Control de Archivos:** Configurar el DLP para alertar sobre transferencias masivas de archivos, cambios de nombre sospechosos o el cifrado de carpetas locales.
- **Monitoreo de Red:** Monitorear el tráfico saliente y las conexiones a servicios de almacenamiento personal en la nube.
- **Gestión de Privilegios:** Implementar el mínimo privilegio y el monitoreo de usuarios con acceso a repositorios masivos de datos.

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de UEBA o DLP sobre actividades de acumulación (ej. acceso secuencial a miles de archivos, creación de archivos ZIP/RAR con etiquetas sensibles).
- **Identificar el Dato:** Determinar el tipo, volumen y sensibilidad de los datos

que están siendo preparados (ej. código fuente completo, todos los registros de clientes).

- **Rastrear el *Staging Area*:** Identificar la ubicación de tránsito (ej. carpeta TEMP, *bucket* personal, VM interna poco monitoreada) donde el actor está acumulando los datos.
- **Correlación de Eventos:** Correlacionar la actividad de *staging* con otros eventos (ej. renuncias, evaluaciones de desempeño, actividad fuera de horario).

- **Mapeo MITRE ATT&CK:** T1074.001 (*Data Staged: Local Data Staging*), T1020 (Exfiltración Automatizada), T1537 (Transferir Datos a Cuenta en la Nube).

3. Contención

- **Congelar la Actividad:** Si es viable, bloquear la capacidad del usuario de escribir o modificar archivos en el *staging area* sin suspender su cuenta. Esto detiene la acumulación sin alertar al actor.
- **Suspender Acceso (Coordinado):** Coordinar con RRHH y Legal para deshabilitar o revocar la cuenta del usuario de inmediato si se determina que la fuga es inminente.
- **Bloquear Canales de Exfiltración:** Si el *staging area* es un servicio en la nube personal, bloquear el acceso a esa URL a nivel de proxy/firewall/DLP.
- **Preservar Evidencia:** Capturar una imagen forense del *staging area* (disco duro local, *snapshot* de la VM, logs del servicio en la nube) antes de la eliminación.

4. Erradicación

- **Eliminar los Datos Acumulados:** Borrar de forma segura todos los archivos *staged* del sistema de la organización (el disco local, la VM, la carpeta de red).
- **Borrar Artefactos:** Eliminar cualquier herramienta que el actor haya utilizado para el *staging* (ej. *scripts* de compresión, *software* de sincronización no autorizado).
- **Rotación de Credenciales:** Restablecer la contraseña del usuario y revocar cualquier *token* o clave que pudiera haber sido robada.

5. Recuperación

- **Notificación y Cumplimiento:** Coordinar con Legal para determinar si la actividad de *staging* ya constituyó una violación de datos que requiere notificación.
- **Auditoría de Activos:** Realizar una auditoría completa en todos los activos a los que el actor tenía acceso para asegurar que no se hayan dejado *backdoors* o cambios de persistencia.
- **Restaurar el Acceso:** Restablecer el acceso para el resto del equipo, si la contención afectó a los recursos compartidos.

6. Lecciones Aprendidas e Informes

- **Análisis de Causa Raíz:** Documentar el patrón de comportamiento que alertó sobre el *staging* y por qué el DLP no detuvo el movimiento inicial de los datos a la zona de tránsito.
- **Fortalecer UEBA:** Ajustar los umbrales de UEBA para que la actividad de *staging* (ej. compresión de archivos) sea de mayor prioridad de alerta.
- **Mejorar Monitoreo:** Fortalecer el monitoreo de volúmenes de almacenamiento no convencionales y servicios de sincronización no aprobados.
- **Documentación y Acción Disciplinaria:** Formalizar el informe del incidente y documentar la acción disciplinaria tomada en coordinación con RRHH/Legal.

Herramientas Típicas: UEBA (User and Entity Behavior Analytics), DLP (Data Loss Prevention), Logs de Auditoría de Sistemas de Archivos (FIM), Logs de Red, EDR/XDR, Herramientas Forenses.

Playbook 36: Integración No Autorizada de App SaaS OAuth (*Phishing* de Consentimiento)

Escenario

Un empleado interactúa con una aplicación de terceros maliciosa o no autorizada y, por medio de un engaño (*phishing* de consentimiento) o descuido, autoriza a dicha aplicación a acceder a los datos de su cuenta en la nube (ej. Google Workspace, Microsoft 365, Slack). La aplicación recibe permisos excesivos (*scopes*) para leer correos, acceder a archivos o realizar otras acciones sensibles, lo que resulta en un acceso delegado y no autorizado a los datos corporativos.

Clasificación del Incidente

Categoría	**Detalles**
Tipo de Incidente	Compromiso de Identidad - OAuth / *Phishing* de Consentimiento
Severidad	Alta (acceso delegado a datos por un atacante que opera bajo una aplicación "legítima")
Prioridad	Crítica (la acción inmediata para revocar el *token* es vital para detener el abuso delegado)
Fuentes de Detección	CASB, Logs de Auditoría de Identidad (Azure AD, Google Workspace), Gateway de Correo, Reporte de Usuario

Fases y Acciones

1. Preparación

- **Monitoreo de Aplicaciones:** Utilizar un CASB (Cloud Access Security Broker) o herramientas de auditoría nativas para monitorear nuevas aplicaciones de terceros con permisos excesivos.

- **Restricción de Consentimiento:** Implementar políticas que limiten el consentimiento de aplicaciones solo a administradores o a una lista blanca de aplicaciones verificadas.
- **Concienciación:** Capacitación específica a los usuarios sobre los riesgos del *phishing* de consentimiento (revisar los permisos solicitados por la aplicación).
- **Revisión de Aplicaciones:** Auditoría periódica de las aplicaciones de terceros autorizadas y los permisos que tienen.
- **Alertas de CASB:** Configurar alertas para cuando una aplicación solicite un conjunto de permisos de alto riesgo (ej. acceso de lectura/escritura a todos los correos).

2. Detección y Análisis

- **Confirmar la Alerta:** Investigar la alerta de CASB o del Gateway de Correo que indica que una aplicación no aprobada recibió consentimiento.
- **Identificar la Aplicación:** Determinar el nombre, el ID del cliente y los permisos que le fueron concedidos a la aplicación.
- **Evaluar el Alcance:** Revisar los logs de auditoría de la plataforma de identidad para ver la actividad que la aplicación ha realizado (ej. ¿Se leyeron correos? ¿Se accedió a archivos específicos?).
- **Determinar el Vector:** Rastrear si el usuario fue atacado a través de un correo de *phishing* o por otro medio.
- **Mapeo MITRE ATT&CK:** T1526 (Control de Recursos de Nube/Infraestructura), T1566.002 (*Phishing*: Ataque de Consentimiento de Servicios de Confianza), T1078 (Cuentas Válidas).

3. Contención

- **Revocar el *Token* OAuth:** Revocar de inmediato el consentimiento y el *token* de acceso de la aplicación maliciosa para la cuenta del usuario. **Esta**

es la acción de máxima prioridad.

- **Eliminar la Aplicación:** Bloquear o eliminar la aplicación de la lista de aplicaciones permitidas a nivel de la organización para evitar que otros usuarios la autoricen.

- **Restablecer Contraseña (Preferible):** Aunque el *token* sea delegado, restablecer la contraseña del usuario y forzar una nueva autenticación con MFA.
- **Auditoría de Cuentas Adicionales:** Escanear proactivamente el entorno para identificar cualquier otro usuario que también haya autorizado la misma aplicación maliciosa.

4. Erradicación

- **Eliminar Reglas de Persistencia:** Si la aplicación utilizó el acceso para establecer un mecanismo de persistencia (ej. crear reglas de reenvío en el correo), eliminar esos artefactos.
- **Análisis de Impacto:** Determinar si los datos fueron efectivamente exfiltrados y, si es así, iniciar la respuesta según el *playbook* de "Exfiltración de Datos".
- **Bloqueo de Comunicación:** Bloquear cualquier comunicación de red conocida o URL asociada con la aplicación maliciosa.

5. Recuperación

- **Rehabilitar Acceso:** Asegurar que el usuario pueda iniciar sesión y acceder a sus recursos de forma normal y segura (con MFA).
- **Comunicación de *Lecciones Aprendidas*:** Notificar al equipo y al usuario la naturaleza del ataque para que puedan identificar futuros intentos.
- **Auditoría de Permisos:** Realizar una auditoría completa de las aplicaciones de terceros que el usuario tiene autorizadas para asegurarse de que no haya otras *apps* sospechosas.

6. Lecciones Aprendidas e Informes

- **Análisis Post-Incidente:** Documentar la URL de *phishing* utilizada, el ID de la aplicación y la eficacia de la herramienta CASB/Auditoría.
- **Fortalecer Controles:** Reforzar la política de restricción de consentimiento de OAuth, idealmente permitiendo solo aplicaciones aprobadas por IT.
- **Campaña de Concienciación:** Realizar una campaña de *phishing* simulado de consentimiento para evaluar la resiliencia de los usuarios y educarlos.
- **Documentación:** Reportar la aplicación maliciosa a la plataforma de identidad correspondiente (ej. Google, Microsoft) si es un tercero externo.

Herramientas Típicas: CASB (Cloud Access Security Broker), Logs de Auditoría de Plataformas de Identidad (ej. Azure AD Audit, Google Workspace Audit), Herramientas de Correo/Filtrado (para detectar el *phishing* inicial).