Módulo 4. De la alerta al caso

CÓRDOBA CREA FUTURO

1. Investigación mínima

En los entornos de monitoreo de seguridad, una alerta generada por un sistema SIEM constituye una señal inicial que requiere interpretación. El hecho de que una regla de detección se active indica que determinados eventos cumplen con un patrón previamente definido, pero esto no implica necesariamente que se haya producido un incidente de seguridad real. En consecuencia, el trabajo del analista consiste en transformar esa señal técnica en una comprensión contextual del evento detectado.

Dentro de los centros de operaciones de seguridad (SOC), este proceso inicial suele denominarse investigación mínima o investigación preliminar. Su objetivo consiste en reunir la información esencial que permita determinar si una alerta debe tratarse como un incidente confirmado, si corresponde a un falso positivo o si requiere un análisis más profundo por parte de analistas especializados. Esta etapa forma parte del proceso de análisis dentro del ciclo de respuesta a incidentes descrito en los modelos de gestión de incidentes utilizados en ciberseguridad (Cynet, s. f.).

La investigación mínima busca responder preguntas básicas que orientan el proceso de análisis. Entre estas preguntas se encuentran: qué ocurrió dentro del sistema, cuándo sucedió, qué activos pudieron verse afectados y qué acciones se registraron durante el evento. Para responder estas cuestiones, los analistas utilizan información proveniente de registros del sistema, herramientas de monitoreo, datos de red y otras fuentes disponibles dentro de la infraestructura tecnológica.

En la práctica operativa, esta investigación se organiza a partir de cuatro componentes principales. El primero corresponde a la reconstrucción de la línea temporal de los eventos, que permite comprender la secuencia de acciones registradas en los sistemas. El segundo consiste en la formulación de hipótesis explicativas, que ayudan a interpretar los datos recopilados. El tercer componente se relaciona con la recopilación de evidencias digitales, que permiten respaldar las conclusiones obtenidas durante el análisis. Finalmente, los resultados de la investigación se documentan mediante un informe de incidente, que registra de manera estructurada la información obtenida.

Estos elementos permiten transformar registros técnicos dispersos en una interpretación coherente del evento investigado. A través de este proceso, el analista SOC puede determinar si la alerta representa un comportamiento legítimo del sistema o si corresponde a una actividad potencialmente maliciosa que requiere acciones adicionales.

La investigación mínima cumple además una función organizacional importante dentro de los procesos de seguridad. Al establecer un procedimiento estructurado para analizar las alertas generadas por los sistemas de monitoreo, se evita que los analistas tomen decisiones basadas únicamente en interpretaciones aisladas de los eventos. En su lugar, el análisis se basa en la recopilación sistemática de información y en la construcción progresiva de una explicación fundamentada del evento.

En este marco, la investigación mínima actúa como un puente entre la detección automática realizada por las herramientas de monitoreo y el análisis humano realizado por los equipos de seguridad. Este proceso permite transformar grandes volúmenes de eventos registrados en los sistemas en casos investigables que pueden ser comprendidos dentro del contexto operativo de la organización.

Timeline

El análisis de **timeline** o reconstrucción de línea temporal constituye una de las herramientas más utilizadas en la investigación de incidentes de seguridad. Su propósito consiste en organizar cronológicamente los eventos registrados por los sistemas informáticos para comprender cómo se desarrolló una actividad determinada dentro de la infraestructura tecnológica.

Los sistemas digitales generan continuamente registros de actividad, conocidos como *logs*, que documentan acciones realizadas en distintos componentes de la infraestructura. Estos registros pueden provenir de sistemas operativos, aplicaciones, servidores, dispositivos de red, herramientas de seguridad o plataformas de monitoreo. Cada registro contiene información

temporal que permite identificar el momento exacto en que ocurrió una determinada acción dentro del sistema (ScienceDirect, s. f.).

El análisis de *timeline* utiliza estos registros para reconstruir la secuencia de eventos asociados a un incidente. En lugar de observar los eventos de manera aislada, el analista organiza la información en orden cronológico para comprender la relación entre las distintas actividades registradas. Este enfoque permite identificar patrones de comportamiento que podrían pasar desapercibidos cuando los eventos se analizan de forma individual.

Dentro del análisis forense digital, la reconstrucción de líneas temporales permite observar cómo evolucionó un incidente desde su inicio hasta su detección. Por ejemplo, un evento de autenticación fallida puede preceder a un acceso exitoso desde la misma dirección IP, seguido por cambios en la configuración del sistema o transferencias de información. Cuando estos eventos se analizan de forma cronológica, es posible identificar la secuencia completa de acciones realizadas dentro del sistema (Belkasoft, s. f.).

La construcción de una línea temporal también permite identificar el momento inicial del incidente, lo que en muchos casos se conoce como punto de compromiso inicial. Determinar cuándo comenzó la actividad sospechosa resulta fundamental para comprender cuánto tiempo permaneció el incidente dentro del sistema antes de ser detectado. Este período puede ofrecer información valiosa sobre el alcance del evento y sobre las acciones que pudieron haberse realizado durante ese tiempo.

Además de facilitar la comprensión del incidente, el análisis de timeline permite identificar correlaciones entre eventos registrados en diferentes sistemas. En infraestructuras complejas, los incidentes suelen involucrar múltiples componentes tecnológicos. Por esta razón, los analistas deben integrar registros provenientes de distintas fuentes para construir una visión completa del comportamiento observado.

Las metodologías de análisis forense digital destacan que el timeline permite transformar grandes volúmenes de registros técnicos en una representación estructurada del incidente investigado. Al organizar los eventos en una secuencia temporal coherente, los analistas pueden identificar relaciones entre acciones aparentemente independientes y comprender cómo se desarrolló la actividad dentro del sistema (Cyber Engage, s. f.).

Este enfoque también contribuye a mejorar la comunicación de los resultados de la investigación. Una línea temporal clara permite explicar de manera comprensible cómo se desarrolló el incidente y qué acciones se registraron en cada etapa del proceso. De esta forma, el timeline no solo cumple una función analítica, sino también una función documental dentro del proceso de investigación de incidentes.

En el contexto de las operaciones de seguridad, la reconstrucción temporal se convierte así en una herramienta central para transformar los registros generados por los sistemas en una explicación estructurada del evento investigado. A partir de esta secuencia temporal, los analistas pueden continuar el proceso de investigación formulando hipótesis que permitan interpretar el comportamiento observado.

Hipótesis

Una vez reconstruida la secuencia temporal de los eventos registrados en el sistema, el proceso de investigación avanza hacia la formulación de **hipótesis que expliquen el comportamiento observado.** Las hipótesis representan interpretaciones preliminares que buscan dar sentido a los registros analizados y orientar el proceso de investigación hacia posibles explicaciones del incidente.

En el contexto de la respuesta a incidentes de seguridad, los analistas SOC utilizan las hipótesis como herramientas de análisis que permiten transformar una serie de eventos técnicos en una narrativa explicativa. En lugar de limitarse a observar registros aislados, el analista intenta

comprender cómo esos eventos se relacionan entre sí y qué tipo de actividad podrían representar.

El proceso de formulación de hipótesis comienza generalmente a partir de la información obtenida durante el análisis de timeline. Cuando los eventos se organizan cronológicamente, el analista puede identificar patrones que sugieren determinadas interpretaciones. Por ejemplo, una serie de intentos de autenticación seguidos por un acceso exitoso y cambios en los privilegios de usuario puede sugerir un posible compromiso de credenciales.

Las hipótesis permiten estructurar el proceso de investigación. En lugar de analizar todos los registros disponibles de forma indiscriminada, el analista puede orientar su búsqueda hacia aquellos datos que permitan confirmar o descartar la explicación planteada. Este enfoque facilita la organización del trabajo analítico y permite concentrar la atención en los elementos más relevantes del incidente.

Dentro de las investigaciones de seguridad digital, las hipótesis suelen construirse a partir de tres componentes principales: los eventos observados, el contexto del sistema afectado y el conocimiento previo sobre patrones de ataque o comportamientos anómalos. Estos elementos permiten construir explicaciones plausibles que luego serán contrastadas con las evidencias disponibles.

La formulación de hipótesis también cumple una función importante en la identificación de información adicional necesaria para el análisis. Cuando el analista plantea una posible explicación del incidente, puede identificar qué tipos de registros o evidencias serían necesarios para validar esa interpretación. Por ejemplo, si la hipótesis sugiere un acceso no autorizado a una cuenta privilegiada, el analista puede buscar registros adicionales relacionados con autenticaciones, cambios de configuración o accesos remotos.

En este sentido, las hipótesis actúan como guías para el proceso de investigación. A medida que se recopilan nuevas evidencias, las hipótesis iniciales pueden confirmarse, modificarse o descartarse. Este proceso iterativo permite avanzar progresivamente hacia una comprensión más precisa del incidente.

Además, la formulación de hipótesis contribuye a evitar interpretaciones apresuradas de los eventos registrados. En los entornos de monitoreo de seguridad, muchos eventos pueden tener explicaciones legítimas relacionadas con el funcionamiento normal del sistema. Por esta razón, el analista debe considerar múltiples posibles explicaciones antes de concluir que se trata de un incidente de seguridad.

A través de este enfoque analítico, el proceso de investigación avanza desde la simple observación de registros técnicos hacia la construcción de una explicación fundamentada del evento detectado. Una vez formuladas las hipótesis iniciales, el siguiente paso consiste en recopilar las **evidencias digitales** que permitan confirmar o refutar estas interpretaciones.

Evidencias

La recopilación de **evidencias digitales** constituye una etapa fundamental dentro del proceso de investigación de incidentes de seguridad. Las evidencias permiten respaldar las conclusiones obtenidas durante el análisis y ofrecen información verificable sobre las actividades registradas en los sistemas. En el contexto de la respuesta a incidentes, la evidencia digital representa cualquier dato que permita reconstruir o demostrar qué acciones se realizaron dentro de la infraestructura tecnológica.

Las evidencias pueden provenir de múltiples fuentes dentro del entorno informático. Entre las más comunes se encuentran los registros del sistema operativo, los registros de autenticación, los archivos de configuración, los registros de tráfico de red, los datos generados por herramientas de monitoreo y la información almacenada en dispositivos o servidores.

Cada una de estas fuentes puede aportar información relevante para comprender el comportamiento observado durante el incidente.

Tabla 1. Tipos de evidencias utilizadas en investigaciones de incidentes

Tipo de evidencia	Fuente de obtención	Información que aporta
Registros de autenticación	Servidores de identidad o sistemas operativos	Permiten identificar accesos de usuarios y posibles intentos de autenticación indebidos
***Logs* del sistema**	Sistemas operativos y aplicaciones	Registran actividades realizadas en el sistema durante el incidente
Registros de red	*Firewalls*, IDS/IPS o dispositivos de red	Permiten observar conexiones sospechosas o transferencias de datos
Archivos del sistema	Servidores o estaciones de trabajo	Pueden contener modificaciones o artefactos asociados a la actividad investigada
Datos del SIEM	Plataforma de monitoreo de seguridad	Permiten correlacionar eventos provenientes de distintas fuentes

Fuente: elaboración propia.

En las investigaciones de seguridad digital, el valor de la evidencia radica en su capacidad para documentar hechos verificables. Mientras que el análisis de timeline permite ordenar los eventos y las hipótesis ofrecen posibles interpretaciones, las evidencias proporcionan los datos concretos que sustentan el análisis realizado por el equipo de seguridad.

Las guías de respuesta a incidentes recomiendan integrar técnicas de análisis forense dentro del proceso de investigación para asegurar la correcta preservación y manejo de la información recopilada. Este enfoque busca garantizar que los datos obtenidos durante el análisis mantengan su integridad y puedan utilizarse posteriormente para auditorías o investigaciones adicionales (National Institute of Standards and Technology, 2006).

Uno de los principios fundamentales en la gestión de evidencias digitales consiste en **preservar la información original.** Durante el proceso de recopilación, los analistas deben evitar alterar los datos almacenados en los sistemas, ya que cualquier modificación podría afectar la validez de la evidencia o dificultar el análisis posterior. Por esta razón, las metodologías forenses recomiendan realizar copias controladas de los datos antes de proceder con su análisis.

Otro aspecto importante en la gestión de evidencias es la **trazabilidad del proceso de investigación**. A medida que los analistas recopilan información, deben registrar qué datos fueron obtenidos, en qué momento se recopilaron y qué herramientas se utilizaron para su análisis. Esta documentación permite mantener un registro claro del proceso de investigación y facilita la revisión posterior del incidente.

Las evidencias digitales también cumplen un papel central en la comunicación de los resultados de la investigación. Cuando el equipo de seguridad presenta sus conclusiones, las evidencias permiten demostrar cómo se llegó a determinadas interpretaciones del incidente. De esta forma, el análisis no se basa únicamente en suposiciones o interpretaciones, sino en datos verificables que respaldan las conclusiones obtenidas.

En los entornos organizacionales, la correcta gestión de evidencias contribuye además a fortalecer los procesos de seguridad. Al conservar registros claros de los incidentes investigados, las organizaciones pueden analizar eventos anteriores, identificar patrones de comportamiento y mejorar sus mecanismos de detección y respuesta.

Una vez recopiladas y analizadas las evidencias disponibles, el proceso de investigación continúa con la elaboración de un **informe de incidente**, que permite documentar de manera estructurada los hallazgos obtenidos durante el análisis.

Informe

Una vez finalizada la fase inicial de análisis del incidente, los resultados obtenidos deben organizarse y documentarse mediante la elaboración de un **informe de incidente.** Este documento cumple una función central dentro del proceso de respuesta a incidentes, ya que permite registrar de manera estructurada la información recopilada durante la investigación y comunicar los hallazgos a otras áreas de la organización.

El informe de incidente transforma el análisis técnico realizado por el equipo de seguridad en un documento comprensible que puede ser utilizado por responsables de gestión, equipos técnicos y, en algunos casos, organismos reguladores. A través de este documento se presenta una descripción clara del evento detectado, las acciones realizadas durante la investigación y las conclusiones obtenidas a partir del análisis de los datos disponibles.

Dentro de los procesos de gestión de incidentes, la elaboración de informes permite mantener un registro sistemático de los eventos de seguridad que afectan a la organización. Esta documentación facilita el seguimiento de incidentes, la revisión de los procedimientos utilizados durante la respuesta y el análisis posterior de los eventos registrados.

Los lineamientos de notificación de incidentes utilizados en organismos gubernamentales destacan la importancia de documentar adecuadamente la información relacionada con los eventos de seguridad. La documentación estructurada de los incidentes permite mejorar la coordinación entre los equipos responsables de la gestión de la seguridad informática y facilita la comunicación con otras entidades cuando es necesario reportar el incidente (Cybersecurity and Infrastructure Security Agency, 2015).

Un informe de incidente suele incluir diferentes tipos de información. Entre los elementos más comunes se encuentran la descripción del evento detectado, el momento en que se identificó la alerta, los sistemas afectados, las evidencias recopiladas durante la investigación y las acciones realizadas para contener o mitigar el incidente. También pueden incorporarse recomendaciones destinadas a prevenir situaciones similares en el futuro.

En algunos sectores regulados, la elaboración de informes de incidentes forma parte de los requisitos de cumplimiento normativo. Las organizaciones pueden estar obligadas a reportar determinados eventos de seguridad dentro de plazos establecidos por las autoridades regulatorias. En estos casos, los informes permiten documentar el incidente y cumplir con los procedimientos de notificación correspondientes (BPI, s. f.).

Además de su función administrativa y regulatoria, los informes de incidentes cumplen un papel importante en la gestión del conocimiento dentro de la organización. Al registrar de manera sistemática la información obtenida durante las investigaciones, las organizaciones pueden construir un historial de incidentes que facilite el análisis de patrones de ataque y la mejora de los mecanismos de seguridad.

De esta forma, el informe de incidente representa el cierre de la fase de investigación mínima. A partir de la documentación del evento y de las conclusiones obtenidas, el proceso de gestión de incidentes puede continuar hacia las etapas de cierre, análisis posterior y mejora de los procesos de seguridad, que se desarrollan en la siguiente unidad.

Tips para redactar un informe de incidente

- Describir qué ocurrió y cuándo se detectó el evento.
- Identificar los sistemas o usuarios involucrados.
- Incluir las evidencias relevantes del análisis.
- Explicar las acciones realizadas durante la respuesta.

- Registrar las conclusiones y posibles recomendaciones.

CONTINUAR

2. Cierre, post-incidente y mejora

La gestión de incidentes de seguridad no concluye cuando el evento ha sido contenido o cuando el análisis inicial ha finalizado. Una vez que el incidente ha sido investigado y documentado, las organizaciones deben analizar lo ocurrido para comprender sus causas, evaluar la eficacia de la respuesta y fortalecer los mecanismos de prevención. Esta etapa posterior al incidente permite transformar la experiencia obtenida durante la investigación en conocimiento útil para mejorar los procesos de seguridad.

Los modelos de gestión de incidentes destacan que la respuesta a incidentes debe integrarse dentro de un proceso de mejora continua. En este enfoque, cada incidente analizado proporciona información valiosa sobre el funcionamiento de los sistemas, la eficacia de los controles de seguridad y la capacidad de respuesta del equipo responsable de la gestión de incidentes. El análisis posterior permite identificar debilidades en los procesos existentes y establecer medidas que reduzcan la probabilidad de que situaciones similares vuelvan a ocurrir (ISO, 2023).

Dentro de esta etapa posterior al incidente suelen desarrollarse varias actividades complementarias. Entre ellas se encuentran el análisis de lecciones aprendidas, la implementación de acciones correctivas, la evaluación de métricas de respuesta a incidentes y la integración de estos resultados dentro de un ciclo de mejora organizacional. Estos elementos permiten consolidar el aprendizaje derivado del incidente y fortalecer progresivamente las capacidades de seguridad de la organización.

Lecciones aprendidas

El análisis de **lecciones aprendidas** constituye una práctica ampliamente utilizada en los procesos de gestión de incidentes de seguridad. Su objetivo consiste en revisar lo ocurrido durante el incidente y evaluar la eficacia de las acciones realizadas durante su detección, análisis y respuesta. A través de este proceso, las organizaciones pueden identificar tanto las fortalezas como las debilidades de sus procedimientos de seguridad.

Durante esta etapa, el equipo responsable de la gestión del incidente revisa los distintos momentos del proceso de respuesta. Esto incluye el momento en que se detectó el evento, el tiempo requerido para analizar la alerta, las decisiones tomadas durante la investigación y las medidas implementadas para contener o mitigar el incidente. Este análisis permite evaluar si los procedimientos existentes resultaron adecuados o si es necesario introducir mejoras en los procesos de seguridad.

Las normas de gestión de incidentes de seguridad recomiendan incorporar sesiones formales de revisión posterior al incidente. Estas sesiones permiten analizar lo ocurrido desde una perspectiva organizacional y facilitan la identificación de aspectos que pueden optimizarse en futuras situaciones similares (ISO, 2023).

El proceso de análisis de lecciones aprendidas también permite mejorar la coordinación entre las diferentes áreas involucradas en la respuesta a incidentes. En muchos casos, la gestión de incidentes requiere la colaboración entre equipos técnicos, responsables de seguridad, áreas de gestión y, en determinados contextos, autoridades externas. La revisión posterior permite identificar posibles dificultades en la comunicación o en la coordinación entre estos actores.

Además, las lecciones aprendidas pueden contribuir a mejorar los mecanismos de detección utilizados por las herramientas de monitoreo. Si durante la investigación se identifica que un incidente no fue detectado oportunamente o que generó múltiples alertas irrelevantes, el equipo de seguridad puede ajustar las reglas de detección o los umbrales configurados en el sistema SIEM.

De esta forma, el análisis de lecciones aprendidas permite transformar cada incidente en una oportunidad de aprendizaje para la organización. Al documentar y analizar la experiencia obtenida durante la gestión del incidente, las organizaciones pueden fortalecer sus procesos de seguridad y mejorar su capacidad de respuesta ante eventos futuros.

Acciones correctivas

Las **acciones correctivas** representan las medidas que se implementan después de la resolución de un incidente con el objetivo de reducir la probabilidad de que situaciones similares vuelvan a ocurrir. Mientras que el análisis de lecciones aprendidas permite comprender qué ocurrió durante el incidente, las acciones correctivas se orientan a introducir cambios concretos en los sistemas, procesos o políticas de seguridad.

En los procesos de gestión de incidentes, las acciones correctivas suelen derivarse directamente del análisis posterior al incidente. Cuando se identifican debilidades en los controles de seguridad, en los procedimientos operativos o en las configuraciones de los sistemas, el equipo responsable de la seguridad puede proponer medidas destinadas a corregir esas condiciones. Estas acciones pueden incluir modificaciones técnicas, ajustes en los procedimientos operativos o la incorporación de nuevos controles de seguridad.

Dentro de los entornos de monitoreo de seguridad, una de las acciones correctivas más frecuentes consiste en revisar las reglas de detección utilizadas por los sistemas SIEM. Si durante la investigación del incidente se observa que la alerta se generó demasiado tarde o que el sistema produjo un número elevado de falsos positivos, el equipo de seguridad puede ajustar los parámetros de detección para mejorar la eficacia del monitoreo.

Las acciones correctivas también pueden involucrar cambios en la configuración de los sistemas afectados. Por ejemplo, si el incidente estuvo relacionado con un acceso indebido a una cuenta de usuario, la organización puede revisar sus políticas de autenticación, reforzar los

mecanismos de control de acceso o implementar medidas adicionales como la autenticación multifactor.

El enfoque de gestión proactiva de incidentes destaca que las organizaciones deben utilizar los incidentes como oportunidades para fortalecer sus controles de seguridad. En lugar de considerar el incidente únicamente como un evento aislado, el análisis posterior permite identificar condiciones estructurales que podrían facilitar incidentes similares en el futuro (Prysmex, s. f.).

Además de las medidas técnicas, las acciones correctivas también pueden involucrar mejoras en los procesos organizacionales. Por ejemplo, una organización puede actualizar sus procedimientos de respuesta a incidentes, mejorar la capacitación del personal o fortalecer los mecanismos de comunicación entre los equipos responsables de la gestión de incidentes.

La implementación de acciones correctivas permite transformar el conocimiento obtenido durante la investigación en mejoras concretas para la seguridad de la organización. De esta forma, cada incidente analizado contribuye a fortalecer los mecanismos de prevención y a mejorar la capacidad de respuesta frente a eventos futuros.

Métricas

La gestión de incidentes de seguridad requiere mecanismos que permitan evaluar el desempeño de los procesos de detección, análisis y respuesta. Para lograrlo, las organizaciones utilizan **métricas de respuesta a incidentes**, que funcionan como indicadores cuantitativos destinados a medir la eficacia de los procedimientos de seguridad implementados.

Las métricas permiten transformar la experiencia operativa del equipo de seguridad en información medible. A partir de estos indicadores, las organizaciones pueden analizar cómo se comportan sus procesos de monitoreo y respuesta, identificar posibles demoras en la gestión de incidentes y detectar oportunidades de mejora en sus procedimientos de seguridad (Cortex, s. f.).

Entre las métricas más utilizadas en los procesos de respuesta a incidentes se encuentran aquellas relacionadas con el tiempo requerido para detectar, analizar y resolver un incidente. Estos indicadores permiten comprender qué tan rápido la organización identifica eventos de seguridad y qué tan eficiente resulta el proceso de investigación.

Una de las métricas más conocidas es el **tiempo medio de detección del incidente**, que mide el intervalo entre el momento en que ocurre una actividad maliciosa y el momento en que el sistema o el equipo de seguridad identifica la alerta correspondiente. Este indicador permite evaluar la eficacia de los mecanismos de monitoreo y detección utilizados dentro de la organización.

Otra métrica ampliamente utilizada es el **tiempo medio de respuesta,** que representa el tiempo necesario para analizar la alerta, investigar el incidente y aplicar las medidas necesarias para contener o mitigar el evento. Este indicador permite evaluar la eficiencia del equipo de respuesta a incidentes y la eficacia de los procedimientos utilizados durante el análisis.

Además de los indicadores relacionados con el tiempo, las organizaciones también utilizan métricas vinculadas con la calidad del proceso de detección. Entre estas métricas se incluyen el

número de incidentes detectados en un período determinado, el porcentaje de falsos positivos generados por el sistema de monitoreo y la proporción de incidentes que requieren escalamiento a niveles de análisis más avanzados.

Las métricas de respuesta a incidentes cumplen una función importante dentro de los procesos de gestión de seguridad, ya que permiten identificar tendencias a lo largo del tiempo. Al analizar estos indicadores de manera periódica, las organizaciones pueden evaluar si sus procesos de seguridad están mejorando o si existen áreas que requieren ajustes adicionales.

En este sentido, las métricas no solo permiten evaluar el desempeño actual de los sistemas de seguridad, sino que también ofrecen información valiosa para la toma de decisiones estratégicas. A partir de estos indicadores, los responsables de seguridad pueden identificar necesidades de capacitación, ajustar los procedimientos de monitoreo o incorporar nuevas herramientas destinadas a mejorar la capacidad de detección y respuesta frente a incidentes.

De esta manera, las métricas se convierten en una herramienta clave para transformar la experiencia obtenida durante la gestión de incidentes en información útil para mejorar los procesos de seguridad de la organización.

Figura 1. Métricas de respuesta a incidentes

Fuente: elaboración propia.

Ciclo de mejora

La gestión de incidentes de seguridad se integra dentro de un proceso organizacional más amplio orientado a la **mejora continua de los mecanismos de protección y respuesta.** Cada incidente investigado proporciona información valiosa sobre el funcionamiento de los sistemas, la eficacia de los controles implementados y la capacidad de la organización para detectar y responder ante actividades anómalas. Por esta razón, los procesos de respuesta a incidentes suelen incorporarse dentro de un ciclo de aprendizaje que permite fortalecer progresivamente las capacidades de seguridad.

Los modelos de gestión de incidentes describen este proceso como un ciclo continuo en el que cada etapa de respuesta genera información que puede utilizarse para mejorar los procedimientos existentes. Este enfoque permite que la organización aprenda de los incidentes ocurridos y utilice ese conocimiento para reforzar sus mecanismos de detección, análisis y mitigación (Sygnia, s. f.).

Dentro de este ciclo, la experiencia obtenida durante la investigación del incidente se transforma en insumos para mejorar diferentes aspectos de la seguridad organizacional. Por ejemplo, los resultados del análisis pueden utilizarse para ajustar reglas de detección en los sistemas SIEM, mejorar los procedimientos de respuesta o fortalecer los controles de acceso en los sistemas afectados.

El ciclo de mejora también se relaciona con el análisis de las métricas obtenidas durante la gestión de incidentes. Los indicadores de desempeño permiten evaluar si los tiempos de detección y respuesta están mejorando o si existen áreas del proceso que requieren ajustes. A partir de esta información, los responsables de seguridad pueden introducir cambios destinados a optimizar los procedimientos de monitoreo y respuesta.

En muchos casos, este proceso de mejora incluye la actualización de políticas de seguridad, la revisión de configuraciones en los sistemas tecnológicos y la capacitación del personal encargado de la gestión de incidentes. Estas acciones permiten fortalecer la preparación de la organización frente a futuros eventos de seguridad.

El enfoque de mejora continua también promueve la revisión periódica de los procedimientos de respuesta a incidentes. A medida que las organizaciones enfrentan nuevos tipos de amenazas o incorporan nuevas tecnologías, resulta necesario actualizar los procesos de seguridad para adaptarlos a los cambios del entorno tecnológico.

De esta manera, el ciclo de mejora conecta todas las etapas del proceso de gestión de incidentes. La detección inicial de una alerta conduce a la investigación del evento, el análisis posterior permite identificar oportunidades de mejora y las acciones correctivas introducen cambios que fortalecen los mecanismos de seguridad de la organización.

En consecuencia, la gestión de incidentes se convierte en un proceso dinámico que evoluciona a medida que la organización aprende de los eventos experimentados. Cada incidente investigado contribuye a mejorar la

capacidad de detección, análisis y respuesta, consolidando así un enfoque de seguridad basado en el aprendizaje continuo.

CONTINUAR

Referencias

Belkasoft. (s. f.). *Digital forensic timeline analysis.* https://belkasoft.com/digital-forensic-timeline-analysis

BPI. (s. f.). *Cyber incident reporting requirements: Notification timelines for financial institutions.* https://bpi.com/cyber-incident-reporting-requirements-notification-timelines-for-financial-institutions/

Cortex. (s. f.). *Your guide to incident response metrics.* https://www.cortex.io/post/your-guide-to-incident-response-metrics

Cyber Engage. (s. f.). *Understanding timeline analysis in digital forensics. Medium.* https://medium.com/@cyberengage.org/understanding-timeline-analysis-in-digital-forensics-eb84bb297fc7

Cybersecurity and Infrastructure Security Agency. (2015). *Federal incident notification guidelines.* https://www.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines_2015.pdf

Cynet. (s. f.). *NIST incident response: 4-step life cycle, templates and tips.* https://www.cynet.com/incident-response/nist-incident-response/

International Organization for Standardization. (2023). *ISO/IEC 27035-1:2023 Information security incident management – Part 1: Principles of incident management*. https://cdn.standards.iteh.ai/samples/78973/38e0e742e02741ba856510f74aa9f23b/ISO-IEC-27035-1-2023.pdf

National Institute of Standards and Technology. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Prysmex. (s. f.). *Gestión proactiva de incidentes en calidad y seguridad.* https://www.prysmex.com/blog/gestion-proactiva-de-incidentes-en-calidad-y-seguridad

ScienceDirect. (s. f.). *Timeline analysis*. https://www.sciencedirect.com/topics/computer-science/timeline-analysis

Sygnia. (s. f.). *What is incident response? Process, plan and complete guide*. https://www.sygnia.co/blog/what-is-incident-response-process-plan-and-complete-guide/

CONTINUAR