Módulo 4. Integración SIEM + SOAR/SIRP (Wazuh/Graylog/OpenSearch + TheHive/Cortex/Shuffle)

CÓRDOBA CREA FUTURO

Introducción

La integración entre plataformas SIEM y soluciones SOAR/SIRP constituye hoy un componente central de los programas avanzados de detección y respuesta en redes. En el marco del enfoque de gestión del riesgo promovido por el NIST SP 800-61r3, la detección, el análisis y la respuesta a incidentes deben articularse como procesos continuos y coordinados (Nelson et al., 2025). Las capacidades de recolección, normalización y análisis de logs, como las desarrolladas por Wazuh, junto con las funcionalidades de visualización y reporte de Graylog, permiten consolidar la fase de detección. Su integración con herramientas de orquestación y gestión de casos habilita una respuesta estructurada, medible y alineada con la mejora continua.

Unidad 1. Herramientas SIEM – Wazuh / Graylog / OpenSearch

Unidad 2. Herramientas SOAR. Orquestación / Cases

Unidad 1. Herramientas SIEM – Wazuh / Graylog / OpenSearch

Parsers / normalización.

En los sistemas SIEM modernos, la normalización de eventos constituye el fundamento técnico que permite transformar registros heterogéneos en información estructurada y correlacionable. La diversidad de fuentes —sistemas operativos, dispositivos de red, servicios cloud, aplicaciones y herramientas de seguridad— genera formatos disímiles que requieren procesos sistemáticos de decodificación y estandarización antes de ser analizados. La literatura técnica coincide en que la efectividad de la detección depende directamente de la calidad del parsing inicial, ya que errores en esta etapa impactan en la correlación, la priorización y la respuesta posterior (Nelson et al., 2025).

Wazuh implementa este proceso mediante un modelo compuesto por **decoders y rules**, que operan en etapas sucesivas. De acuerdo con su documentación oficial, los decoders son responsables de analizar los logs crudos y

convertirlos en estructuras normalizadas que permiten identificar campos relevantes como marca temporal, dirección IP de origen, usuario, proceso o severidad. Este mecanismo resulta esencial cuando se integran fuentes tan diversas como syslog, Windows Event Channel, macOS ULS o registros provenientes de proveedores cloud.

El proceso de normalización en Wazuh incluye una fase de predecodificación, decodificación y posterior coincidencia con reglas. Los decoders pueden ser predefinidos o personalizados, lo que permite adaptar el SIEM a entornos específicos con formatos propietarios o herramientas de terceros. La documentación señala explícitamente que los decoders convierten formatos heterogéneos en un formato unificado que el sistema puede procesar eficientemente. Esta arquitectura es coherente con las buenas prácticas de ingeniería de seguridad, donde la estandarización previa es condición necesaria para la correlación avanzada.

En entornos distribuidos, el almacenamiento estructurado también es determinante. El indexador de Wazuh, basado en

un motor distribuido de búsqueda y análisis en tiempo real, almacena los eventos en formato JSON, garantizando escalabilidad y redundancia mediante el uso de shards y nodos múltiples. Esta arquitectura no solo optimiza la consulta sino que sostiene la continuidad operativa ante fallas de hardware o ataques.

La normalización no cumple únicamente una función técnica; constituye además un requisito organizacional dentro del ciclo de gestión de incidentes. El NIST SP 800-61r3 establece que la capacidad de análisis efectivo depende de la disponibilidad de información consistente y contextualizada (Nelson et al., 2025). En este sentido, el parsing adecuado permite enriquecer eventos con metadatos como técnicas MITRE ATT&CK o referencias a controles regulatorios, mejorando la capacidad de priorización y clasificación.

Complementariamente, la visualización desempeña un rol central en la interpretación de datos normalizados. El Wazuh dashboard proporciona capacidades de consulta y visualización que permiten aplicar filtros, explorar eventos en tiempo real y construir paneles personalizados. Estas funcionalidades se alinean con el enfoque de Graylog, donde dashboards y widgets convierten consultas estructuradas en representaciones gráficas accionables, facilitando el monitoreo continuo y la generación de reportes (Graylog, 2026).

Desde una perspectiva sistémica, la normalización representa el punto de convergencia entre recolección y análisis. Sin una estructura homogénea de datos, la correlación multi-fuente pierde consistencia, la detección genera falsos positivos y la respuesta se retrasa. En consecuencia, los parsers y mecanismos de estandarización constituyen la base técnica sobre la cual se edifica la integración SIEM con herramientas de orquestación posteriores.

Correlación con red y endpoint

La correlación constituye el núcleo analítico de un sistema SIEM, ya que permite transformar eventos aislados en patrones significativos de comportamiento. Mientras que la normalización estructura los datos, la correlación articula relaciones temporales, contextuales y técnicas entre múltiples fuentes. En el marco de la gestión de incidentes, el NIST SP 800-61r3 subraya que la capacidad de identificar eventos relacionados y agruparlos en incidentes es esencial para reducir el tiempo de detección y mejorar la priorización (Nelson et al., 2025).

En entornos híbridos, la correlación eficaz requiere integrar información proveniente tanto de endpoints como de dispositivos de red y servicios en la nube. Wazuh recopila registros desde agentes instalados en sistemas Linux,

Windows y macOS, así como desde dispositivos que envían eventos vía syslog o mediante integraciones con proveedores cloud (Wazuh, 2026a). Esta diversidad de fuentes permite construir una visión transversal del entorno, combinando telemetría de sistema operativo, eventos de autenticación, integridad de archivos, actividad de procesos y eventos de infraestructura.

La correlación se implementa en Wazuh a través de su ruleset, donde las reglas definen condiciones sobre campos específicos, patrones o valores que, al cumplirse, generan alertas con niveles de prioridad determinados (Wazuh, 2026a). Estas reglas pueden incorporar identificadores de técnicas del marco MITRE ATT&CK, lo que permite contextualizar los eventos dentro de tácticas adversarias reconocidas. Esta capacidad resulta particularmente relevante cuando se combinan indicadores provenientes de red y endpoint, por ejemplo, autenticaciones exitosas seguidas de conexiones externas inusuales.

Desde el punto de vista técnico, la correlación puede ser de tipo simple o compuesta. En el primer caso, una regla detecta un patrón específico en un único evento. En el segundo, múltiples eventos en una ventana temporal determinada se asocian para producir una alerta de mayor relevancia. La documentación de Wazuh señala que las reglas pueden encadenarse mediante identificadores previos, permitiendo detectar secuencias relacionadas (Wazuh, 2026a). Este mecanismo habilita la detección de comportamientos progresivos, como escalamiento de privilegios o movimientos laterales.

La integración con índices diferenciados también fortalece la correlación. Wazuh almacena alertas, eventos archivados, información de monitoreo de agentes y estadísticas de desempeño en índices específicos, lo que permite consultas estructuradas sobre diferentes dimensiones operativas (Wazuh, 2026a). Esta segmentación facilita el cruce entre eventos de seguridad y estado del agente, aportando contexto adicional para la evaluación de incidentes.

Desde la perspectiva del análisis visual, la correlación se vuelve operativamente significativa cuando puede representarse en dashboards dinámicos. El Wazuh dashboard permite explorar eventos en tiempo real, aplicar filtros y realizar consultas complejas para identificar tendencias y anomalías (Wazuh,

2026b). De manera complementaria, Graylog destaca que los dashboards configurables y los widgets permiten visualizar agregaciones, métricas y distribuciones temporales que apoyan la identificación de patrones anómalos (Graylog, 2026). La representación gráfica de correlaciones reduce la carga cognitiva del analista y facilita la toma de decisiones.

En términos estratégicos, la correlación multi-fuente disminuye el ruido operativo al consolidar múltiples señales en un único evento contextualizado. Esto se alinea con las recomendaciones del NIST respecto de la consolidación y clasificación sistemática de eventos para optimizar la fase de análisis (Nelson et al., 2025). Sin correlación adecuada, el SIEM produce alertas fragmentadas que incrementan el volumen sin aumentar la calidad de la detección.

La convergencia entre telemetría de red y endpoint resulta especialmente relevante en escenarios NDR. La combinación de registros de autenticación, actividad de procesos, tráfico de red y cambios en la configuración del sistema permite construir narrativas completas de ataque. Esta visión integrada constituye el punto de transición hacia el segundo bloque del módulo, donde la

orquestación y gestión de casos automatiza y estructura la respuesta a partir de las detecciones generadas.

Tableros y KPIs de detección

En un sistema SIEM, la detección no se agota en la generación de alertas; requiere mecanismos de visualización y medición que permitan interpretar el estado de seguridad en tiempo real y evaluar su evolución. Los tableros constituyen el punto de interacción entre los datos estructurados y la toma de decisiones analítica. Su función no es meramente estética, sino estratégica: traducen grandes volúmenes de eventos en indicadores comprensibles y accionables.

El Wazuh dashboard se define como una interfaz web flexible que permite visualizar, analizar y gestionar datos de seguridad recolectados por agentes y dispositivos monitoreados (Wazuh, 2026b). Esta interfaz integra capacidades de consulta, filtrado y visualización en tiempo real, lo que facilita la exploración de eventos específicos, tendencias y anomalías. Además, incorpora paneles orientados a casos de uso como detección de malware, monitoreo de integridad de archivos, cumplimiento normativo y threat hunting, lo que evidencia un diseño orientado a escenarios operativos concretos (Wazuh, 2026b).

La construcción de KPIs en un entorno SIEM debe responder a objetivos definidos dentro del programa de gestión de incidentes. El NIST SP 800-61r3 enfatiza que las organizaciones deben establecer métricas que permitan evaluar la efectividad de la detección y la respuesta, incluyendo tiempos de identificación, clasificación y contención (Nelson et al., 2025). En el contexto del Bloque 1, los KPIs de detección pueden incluir:

- Volumen de alertas por severidad.
- Distribución temporal de eventos críticos.
- Tasa de falsos positivos.
- Eventos asociados a técnicas MITRE ATT&CK específicas.
- Estado de conectividad de agentes.

Wazuh permite crear dashboards personalizados donde múltiples visualizaciones —como gráficos de líneas, gráficos circulares o mapas de calor— se integran en una única vista consolidada (Wazuh, 2026a). Esta capacidad

facilita la observación simultánea de indicadores técnicos y operativos, proporcionando una visión holística del entorno. Por ejemplo, un tablero puede mostrar la evolución de intentos fallidos de autenticación junto con el estado de los agentes y la distribución geográfica de direcciones IP sospechosas.

Desde la perspectiva de Graylog, los dashboards están compuestos por widgets basados en búsquedas guardadas o consultas dinámicas, capaces de agregar, transformar y filtrar datos en tiempo real (Graylog, 2026). La posibilidad de programar reportes periódicos permite trasladar la información técnica a niveles ejecutivos o de cumplimiento, integrando la dimensión estratégica con la operativa.

Un aspecto relevante en la definición de KPIs es la diferenciación entre indicadores de actividad y de calidad. El volumen de alertas refleja actividad, pero no necesariamente eficacia. En cambio, métricas como la proporción de alertas que derivan en incidentes confirmados aportan información sobre precisión de detección. Esta distinción es coherente con el enfoque de mejora continua recomendado por el NIST, donde las métricas deben servir para ajustar procesos y reducir brechas (Nelson et al., 2025).

Asimismo, los índices diferenciados en Wazuh —como los destinados a alertas, eventos archivados y monitoreo de agentes— permiten segmentar métricas técnicas y operativas (Wazuh, 2026a). Esta arquitectura posibilita medir tanto la actividad de seguridad como la salud del propio SIEM, incluyendo rendimiento del servidor o conectividad de endpoints.

En entornos NDR, los tableros cumplen además una función de correlación visual. La superposición temporal de eventos de red y endpoint permite identificar patrones complejos que podrían pasar desapercibidos en registros individuales. La visualización se convierte así en una herramienta cognitiva que reduce la fragmentación analítica y mejora la capacidad de interpretación contextual.

La consolidación de KPIs dentro de dashboards personalizados constituye el puente entre la fase de detección y la fase de respuesta. Solo cuando los indicadores son claros, medibles y alineados con los objetivos organizacionales puede establecerse una transición eficaz hacia mecanismos de orquestación automatizada.

Ruido vs. señal

En entornos SIEM, uno de los desafíos estructurales más relevantes es la distinción entre ruido y señal. La acumulación masiva de eventos puede generar saturación analítica si no existen mecanismos adecuados de filtrado, priorización y correlación. El NIST SP 800-61r3 enfatiza que la clasificación y priorización efectiva de eventos es determinante para evitar la sobrecarga del equipo de respuesta y mejorar la capacidad de detección real (Nelson et al., 2025).

En sistemas como Wazuh, donde se recolectan logs de endpoints, dispositivos de red y servicios cloud (Wazuh, 2026a), la generación de eventos puede ser constante y volumétrica. Por ello, la correcta configuración de reglas, niveles de severidad y dashboards resulta crítica para transformar datos masivos en información accionable.

Algunos conceptos principales que debemos tener en cuenta son:

1. Ruido operacional:

El ruido operacional refiere al conjunto de eventos que, aunque técnicamente válidos, no aportan valor analítico inmediato. Puede incluir registros repetitivos, eventos de bajo impacto o actividades legítimas que disparan reglas genéricas. En entornos donde se monitorean múltiples sistemas operativos y servicios, como ocurre con Wazuh (2026a), el volumen de eventos puede incrementarse exponencialmente. Si no se ajustan adecuadamente las reglas y umbrales de severidad, el sistema genera alertas que saturan la capacidad del analista. El ruido no implica ausencia de datos relevantes, sino falta de discriminación contextual, lo que dificulta la identificación de incidentes prioritarios.

2. Señal significativa:

La señal representa aquellos eventos o correlaciones que evidencian comportamientos anómalos o potencialmente maliciosos. A diferencia del ruido, la señal está contextualizada, priorizada y asociada a indicadores claros. Las reglas en Wazuh permiten asignar niveles de prioridad y enriquecer eventos con referencias a técnicas de ataque (Wazuh, 2026a), lo que facilita distinguir patrones críticos. Desde la perspectiva del NIST, la capacidad de identificar eventos que requieren acción inmediata es un componente esencial del análisis de incidentes (Nelson et al., 2025). La señal no es simplemente un evento aislado, sino un evento interpretado dentro de un marco analítico estructurado.

3. Falsos positivos:

Los falsos positivos son alertas generadas por el SIEM que no corresponden a un incidente real. Aunque forman parte inevitable de cualquier sistema de detección, su acumulación excesiva deteriora la eficiencia operativa. Una tasa elevada de falsos positivos puede desincentivar la atención del equipo y retrasar la identificación de amenazas reales. El ajuste fino de reglas y la personalización de decoders, como permite la plataforma Wazuh (2026a), son estrategias clave para reducir este fenómeno. La literatura en gestión de incidentes indica que la calidad de

detección debe evaluarse no solo por la cantidad de alertas, sino por su precisión y relevancia (Nelson et al., 2025).

4. Falsos negativos:

El falso negativo ocurre cuando una actividad maliciosa no es detectada por el sistema. Este escenario es particularmente crítico, ya que genera una falsa sensación de seguridad. Puede originarse por reglas insuficientes, parsing incompleto o correlación inadecuada entre eventos de red y endpoint. La correcta normalización de logs y la capacidad de consulta avanzada en dashboards (Wazuh, 2026b) permiten revisar eventos históricos y ajustar mecanismos de detección. En términos estratégicos, el equilibrio entre reducción de falsos positivos y minimización de falsos negativos constituye un desafío permanente en los sistemas SIEM.

5. Afinamiento de reglas y priorización:

El afinamiento continuo de reglas es el mecanismo principal para transformar ruido en señal. Implica revisar patrones de coincidencia, ajustar niveles de severidad y adaptar configuraciones al contexto organizacional. El Wazuh dashboard incorpora herramientas para probar reglas y decoders, facilitando su validación técnica (Wazuh, 2026b). Este proceso se alinea con el enfoque de mejora continua promovido por el NIST, donde las métricas y revisiones periódicas permiten optimizar la detección y reducir la sobrecarga operativa (Nelson et al., 2025). La madurez de un SIEM no depende del volumen de datos recolectados, sino de la capacidad de filtrarlos inteligentemente.

La distinción entre ruido y señal no es un problema meramente técnico, sino organizacional y estratégico. Un SIEM eficaz no es aquel que genera más alertas, sino el que produce alertas relevantes, contextualizadas y priorizadas. La combinación de normalización adecuada, reglas bien configuradas y visualización estructurada

permite reducir la saturación analítica y fortalecer la capacidad de respuesta. En este sentido, la calidad de detección constituye el punto de madurez que habilita la transición hacia mecanismos de orquestación automatizada abordados en el siguiente bloque.

CONTINUAR

Unidad 2. Herramientas SOAR. Orquestación / Cases

Plataforma de respuesta a incidentes de seguridad (SIRP) y de análisis de inteligencia de amenazas TheHive / Cortex / Shuffle (OSS)

Una plataforma SIRP orientada a operaciones de respuesta organiza el trabajo del equipo en torno a entidades estructuradas como alertas, casos, tareas, observables y registros de actividad. Este enfoque no es simplemente una decisión de diseño técnico, sino una necesidad organizacional vinculada con la gobernanza del proceso de respuesta. El National Institute of Standards and Technology establece que los procedimientos de manejo de incidentes deben definir claramente roles, responsabilidades, autoridades y criterios de documentación, con el fin de asegurar consistencia y trazabilidad operativa (Cichonski et al., 2012). En su revisión más reciente, el NIST enfatiza que la respuesta a incidentes debe integrarse dentro del marco más amplio de gestión del

riesgo organizacional, incorporando mecanismos de mejora continua y aprendizaje institucional (Nelson et al., 2025).

En este contexto, TheHive opera como una plataforma que formaliza el ciclo de respuesta mediante la estructuración de casos y la automatización controlada de acciones. Un componente central de TheHive 5 es el mecanismo denominado “functions”, definido como bloques de código JavaScript que se ejecutan dentro de un entorno controlado y con permisos explícitos, lo que limita su alcance operativo y reduce riesgos asociados a automatización no gobernada (TheHive Project, 2024a). Esta arquitectura responde al principio de que toda capacidad de automatización debe estar sujeta a controles formales, en coherencia con las recomendaciones del NIST respecto de la necesidad de procedimientos documentados y controles de acceso adecuados (Cichonski et al., 2012).

Las functions pueden exponer endpoints públicos a través de la API de la plataforma, permitiendo que sistemas externos disparen flujos automatizados mediante solicitudes HTTP (TheHive Project, 2024a). Asimismo, acceden a objetos estructurados que representan alertas, casos, observables y tareas,

posibilitando la creación, actualización o enriquecimiento automático de entidades dentro del sistema. Esta capacidad es particularmente relevante cuando se integra un SIEM con una SIRP, ya que permite transformar alertas técnicas en casos formalmente gestionados.

La documentación de TheHive distingue diferentes tipos de functions según su forma de activación: invocadas por API externa, disparadas como notificaciones ante eventos internos, ejecutadas manualmente sobre casos o alertas, o utilizadas como “feeders” para transformar datos externos antes de su incorporación al sistema (TheHive Project, 2024b). Esta diferenciación habilita diseños de orquestación donde no todas las acciones se automatizan de la misma manera ni con el mismo nivel de autonomía, preservando el equilibrio entre eficiencia y control.

Desde el punto de vista operativo, la plataforma incorpora un modo de ejecución “dry-run” que permite probar funciones sin modificar entidades reales, lo que reduce el riesgo de errores durante la configuración inicial (TheHive Project, 2024b). Este mecanismo se alinea con las prácticas recomendadas por el NIST en cuanto a la necesidad de validar procedimientos y

asegurar que los procesos técnicos puedan ejecutarse correctamente antes de aplicarlos en entornos productivos (Cichonski et al., 2012).

La integración con Cortex amplía las capacidades de análisis y acción sobre observables asociados a un caso. Las notas de versión de TheHive 5.2 documentan mejoras en la integración con Cortex Responders, incluyendo su disponibilidad dentro del contexto de tareas y registros, lo que fortalece la coherencia entre análisis técnico y documentación formal del incidente (TheHive Project, 2024c). Asimismo, se reportan mejoras en la estabilidad del conector y en la validación de configuraciones, lo que evidencia un enfoque orientado a confiabilidad operativa.

En conjunto, la articulación entre TheHive y Cortex permite ejecutar análisis automatizados sobre observables y registrar sus resultados dentro del caso correspondiente, integrando inteligencia técnica con trazabilidad documental. Este modelo responde al principio establecido por el NIST de que las organizaciones deben mantener registros adecuados de las actividades realizadas durante la respuesta a incidentes, tanto para fines operativos como para auditoría y aprendizaje posterior (Nelson et al., 2025).

De esta manera, la plataforma SIRP no se limita a almacenar información, sino que estructura el proceso completo de gestión de incidentes, integrando automatización controlada, análisis técnico y gobernanza organizacional dentro de un marco coherente de gestión del riesgo.

Playbooks: apertura, enriquecimiento y cierre

La formalización de playbooks constituye uno de los pilares de una plataforma SOAR, ya que transforma el conocimiento operativo en procedimientos estructurados, repetibles y auditables. Desde la perspectiva metodológica, el NIST establece que los equipos de respuesta deben contar con procedimientos documentados que describan cómo ejecutar acciones técnicas y organizacionales durante el ciclo de vida del incidente (Cichonski et al., 2012). En la revisión más reciente, se refuerza la necesidad de integrar estos procedimientos dentro de una gestión del riesgo más amplia, asegurando que la respuesta no sea improvisada sino sistemática (Nelson et al., 2025). En este marco, los playbooks operan como guías estructuradas que estandarizan las acciones en las fases de apertura, análisis y cierre.

La etapa de apertura implica transformar una alerta en un caso formalmente gestionado. En una plataforma como TheHive, esta transición puede automatizarse mediante functions invocadas por API o disparadas por eventos internos, permitiendo que una alerta recibida desde un SIEM sea convertida en un caso con tareas predefinidas y campos estructurados (TheHive Project, 2024a). La apertura estructurada reduce la variabilidad operativa, asegura que se asignen responsables desde el inicio y establece un marco documental coherente. De acuerdo con NIST, la fase de detección y análisis debe incluir clasificación inicial y determinación de alcance, lo que requiere mecanismos formales de registro y priorización (Cichonski et al., 2012).

El enriquecimiento constituye la segunda etapa del playbook. Aquí se incorporan análisis adicionales, correlación con inteligencia de amenazas y verificación de observables. La integración con Cortex permite ejecutar analizadores y responders directamente sobre observables asociados a un caso, registrando los resultados en el contexto de tareas o registros del incidente (TheHive Project, 2024c). Este diseño fortalece la coherencia entre análisis técnico y documentación formal, evitando que los resultados queden dispersos en herramientas externas. El NIST enfatiza que el análisis debe basarse en información suficiente y contextualizada para determinar el impacto real del incidente (Nelson et al., 2025), lo

que justifica la automatización de consultas, validaciones y enriquecimientos que aporten evidencia adicional antes de decidir acciones de contención.

La fase de cierre representa la consolidación formal del proceso. Un playbook maduro no se limita a resolver técnicamente el incidente, sino que incluye documentación completa de acciones realizadas, evidencias recolectadas y decisiones adoptadas. Según el NIST, las actividades posteriores al incidente son esenciales para capturar lecciones aprendidas y mejorar procedimientos futuros (Cichonski et al., 2012). En una SIRP, el cierre implica marcar el estado del caso, asegurar que todas las tareas estén completadas y que la información relevante quede registrada para auditoría y análisis posterior. Las mejoras de indexación y rendimiento en TheHive facilitan la consulta y análisis histórico de casos cerrados, fortaleciendo la capacidad de revisión estratégica (TheHive Project, 2024c).

Es importante destacar que los playbooks no son estáticos. Deben evolucionar conforme cambian las amenazas, se incorporan nuevas fuentes de detección o se identifican debilidades en procesos previos. El enfoque de gestión del riesgo descrito por Nelson et al.

(2025) subraya que la mejora continua es parte integral del ciclo de respuesta. En consecuencia, la automatización debe ser gobernada y revisada periódicamente para evitar la cristalización de procedimientos obsoletos o ineficientes.

En síntesis, los playbooks estructuran la transición desde la detección hacia la resolución documentada del incidente. Al integrar apertura automatizada, enriquecimiento técnico y cierre formal, la plataforma SOAR convierte la respuesta en un proceso controlado, medible y alineado con estándares internacionales. Esta sistematización constituye la base para evaluar métricas de desempeño y consolidar una postura de seguridad madura.

Métricas de respuesta

La madurez de un programa de respuesta a incidentes no puede evaluarse únicamente por la existencia de herramientas o procedimientos formales. Requiere métricas que permitan medir desempeño, identificar cuellos de botella y orientar decisiones estratégicas. El NIST establece que las organizaciones deben definir indicadores que evalúen la efectividad y eficiencia del proceso de respuesta,

integrándolos dentro del marco general de gestión del riesgo (Cichonski et al., 2012; Nelson et al., 2025).

En el contexto de una plataforma SOAR/SIRP como TheHive, las métricas se construyen a partir de datos estructurados de casos, tareas, tiempos de transición y estados. La disponibilidad de esta información convierte a la plataforma no solo en un sistema operativo, sino también en una fuente de análisis organizacional.

1. Tiempo medio de detección (MTTD):

El tiempo medio de detección mide el intervalo entre la ocurrencia del evento y su identificación como incidente relevante. Este indicador refleja la capacidad de los mecanismos de monitoreo y análisis para identificar señales significativas dentro de grandes volúmenes de datos. El NIST señala que reducir el tiempo de identificación es esencial para limitar el impacto operativo de un incidente (Cichonski et al., 2012). En un entorno integrado SIEM–SIRP, el MTTD depende tanto de la calidad de correlación inicial como de la automatización en la apertura de casos. Una reducción sostenida de este indicador sugiere mejora en reglas de detección y procesos de triage.

2. Tiempo medio de respuesta (MTTR):

El tiempo medio de respuesta representa el período transcurrido entre la apertura del caso y la implementación efectiva de acciones de contención o remediación. Según Nelson et al. (2025), la rapidez en la respuesta debe equilibrarse con precisión y documentación adecuada. En una plataforma como TheHive, el MTTR puede medirse mediante la comparación de marcas temporales asociadas a creación de casos, ejecución de tareas y cierre. Un MTTR elevado puede indicar deficiencias en asignación de responsabilidades, sobrecarga del equipo o playbooks poco optimizados.

3. Tasa de escalamiento:

La tasa de escalamiento mide el porcentaje de casos que requieren intervención de niveles superiores o equipos especializados. Este indicador permite evaluar si los procedimientos de triage inicial están correctamente definidos. De acuerdo con el NIST, la clasificación adecuada en fases tempranas es fundamental para asignar recursos apropiados (Cichonski et al., 2012). Un escalamiento excesivo puede reflejar falta de capacitación o automatización insuficiente, mientras que un escalamiento demasiado bajo podría indicar subestimación de riesgos.

4. Porcentaje de automatización efectiva:

Este indicador mide qué proporción de tareas dentro de los casos se ejecuta mediante automatización frente a intervención manual. Las functions y la integración con analizadores externos permiten ejecutar acciones de forma controlada (TheHive Project, 2024a). Sin embargo, la automatización debe evaluarse no solo por cantidad, sino por impacto en reducción de tiempos y errores. El NIST enfatiza que los procesos deben revisarse periódicamente para asegurar que continúan siendo efectivos (Nelson et al., 2025). Una automatización mal calibrada puede generar decisiones prematuras o inconsistentes.

5. Tasa de reincidencia de incidentes:

La reincidencia mide la frecuencia con la que un tipo de incidente vuelve a ocurrir después de haber sido cerrado previamente. Este indicador refleja la calidad de las acciones correctivas implementadas durante el cierre. El NIST destaca la importancia de actividades posteriores al incidente para identificar causas raíz y fortalecer controles preventivos (Cichonski et al., 2012). Una alta reincidencia sugiere que el proceso de erradicación fue incompleto o que las lecciones aprendidas no se incorporaron adecuadamente en los controles organizacionales.

Las métricas de respuesta convierten la gestión de incidentes en un proceso evaluable y optimizable. Sin

indicadores claros, la respuesta se limita a una actividad reactiva sin capacidad de aprendizaje estructurado. En una plataforma SOAR/SIRP, la disponibilidad de datos temporales y estructurales permite construir métricas objetivas que orienten decisiones estratégicas. La medición sistemática, alineada con estándares internacionales, constituye el fundamento para la mejora continua y prepara el terreno para la consolidación de lecciones aprendidas y backlog operativo, que serán abordados en el siguiente apartado.

Lecciones y backlog

La fase posterior al incidente constituye uno de los componentes más estratégicos del ciclo de respuesta, aunque con frecuencia es subestimada en la práctica operativa. Tanto la versión clásica como la revisión reciente de la guía del NIST coinciden en que las actividades posteriores al incidente son esenciales para consolidar aprendizajes, identificar debilidades y fortalecer controles organizacionales (Cichonski et al., 2012; Nelson et al., 2025). La respuesta no finaliza con la contención técnica ni con el cierre administrativo del caso; se completa cuando la organización incorpora mejoras estructurales derivadas del análisis del evento.

Las lecciones aprendidas permiten transformar la experiencia reactiva en conocimiento institucional. Este proceso implica revisar la secuencia completa del incidente: cómo fue detectado, cómo se clasificó, qué decisiones se tomaron, qué tiempos se registraron y qué impacto operativo tuvo. El NIST establece que estas revisiones deben ser sistemáticas y documentadas, y que deben involucrar tanto a equipos técnicos como a responsables organizacionales relevantes (Cichonski et al., 2012). De esta manera, el incidente se convierte en una fuente de retroalimentación para políticas, procedimientos y controles.

En el contexto de una plataforma SIRP como TheHive, la disponibilidad de información estructurada facilita este análisis retrospectivo. La existencia de registros temporales, tareas asignadas, observables asociados y estados de transición permite reconstruir con precisión el ciclo de vida del caso. Las mejoras de indexación y rendimiento reportadas en versiones recientes de la plataforma fortalecen la capacidad de consulta histórica, optimizando el acceso a casos similares o relacionados (TheHive Project, 2024c). Esta capacidad es

fundamental para identificar patrones recurrentes y determinar si ciertos tipos de incidentes están aumentando en frecuencia o complejidad.

El concepto de backlog se vincula directamente con este proceso de mejora continua. El backlog no debe entenderse únicamente como una lista de tareas pendientes, sino como un repositorio estructurado de mejoras identificadas a partir de incidentes anteriores. Puede incluir ajustes en reglas de detección, actualización de playbooks, incorporación de nuevos analizadores o modificaciones en controles preventivos. Nelson et al. (2025) enfatizan que la gestión del riesgo requiere retroalimentación constante entre eventos observados y controles implementados, lo que convierte al backlog en un mecanismo formal de evolución organizacional.

Asimismo, la integración con marcos como MITRE ATT&CK permite identificar brechas en cobertura defensiva. Si múltiples incidentes revelan exposición repetida a una misma técnica adversaria, el backlog debe incluir acciones orientadas a fortalecer controles específicos asociados a esa técnica. Esta articulación entre análisis retrospectivo y planificación estratégica reduce la probabilidad de reincidencia y mejora la resiliencia organizacional.

Es relevante destacar que el backlog debe priorizarse en función de impacto y riesgo. No todas las lecciones requieren la misma urgencia ni asignación de recursos. El NIST propone que las decisiones de mejora se integren dentro de un marco más amplio de gestión de riesgos, considerando probabilidad, impacto y costos asociados (Nelson et al., 2025). De este modo, el proceso de aprendizaje posterior al incidente no se convierte en una acumulación desordenada de tareas, sino en una estrategia organizada de fortalecimiento continuo.

En síntesis, las lecciones aprendidas y la gestión estructurada del backlog transforman la respuesta a incidentes en un proceso evolutivo. Una plataforma SOAR/SIRP madura no solo organiza el presente del incidente, sino que alimenta el futuro de la postura de seguridad. Esta capacidad de aprendizaje institucional cierra el ciclo operativo iniciado con la detección y consolida una cultura de mejora permanente.

CONTINUAR

Preguntas de repaso

Las actividades posteriores al incidente deben limitarse a la documentación administrativa del caso cerrado, sin necesidad de revisión estratégica adicional.

- ◯ Verdadero
- ◯ Falso

SUBMIT

La gestión estructurada de lecciones aprendidas y backlog permite reducir la reincidencia de incidentes mediante la incorporación de mejoras en procesos y controles.

- ◯ Verdadero

Falso

SUBMIT

CONTINUAR

Conclusión

La integración entre plataformas SIEM y soluciones SOAR/SIRP representa un salto cualitativo en la madurez de los programas de detección y respuesta en redes. Mientras el SIEM estructura, normaliza y correlaciona grandes volúmenes de eventos, la SIRP formaliza la gestión de casos, automatiza acciones y consolida la trazabilidad operativa. Este modelo articulado se alinea con el enfoque de gestión del riesgo propuesto por el NIST, donde la detección, la respuesta y las actividades posteriores forman parte de un ciclo continuo de mejora.

La eficacia del sistema no depende exclusivamente de la capacidad tecnológica, sino de la coherencia entre procesos documentados, métricas de desempeño y aprendizaje institucional. La reducción de ruido, la estandarización mediante playbooks y la incorporación sistemática de lecciones aprendidas permiten

transformar la respuesta reactiva en un proceso estratégico, medible y evolutivo.

CONTINUAR

Referencias

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide* (NIST Special Publication 800-61 Revision 2). National Institute of Standards and Technology.

Graylog. (2026). *Visualize and report log data*. Graylog Documentation.

Graylog. (2026). *Dashboards*. Graylog Documentation.

Nelson, M., et al. (2025). *Computer Security Incident Handling Guide (NIST Special Publication* 800-61 Revision 3). National Institute of Standards and Technology.

TheHive Project. (2024a). About functions – *TheHive 5 Documentation*. StrangeBee.

TheHive Project. (2024b). *SOAR – TheHive Project*. StrangeBee.

TheHive Project. (2024c). *Release Notes for Version 5.2 – TheHive 5 Documentation*. StrangeBee.

Wazuh. (2026a). *Log data analysis – Use cases. Wazuh Documentation.*

Wazuh. (2026b). *Wazuh dashboard – Components. Wazuh Documentation.*

Wazuh. (2026c). *Log data collection – Capabilities. Wazuh Documentation.*

CONTINUAR