Módulo 3. Alertas y KPIs

1. Severidad / SLAs

En los entornos de monitoreo de seguridad, los sistemas SIEM generan grandes volúmenes de alertas provenientes de múltiples fuentes de información. Registros de autenticación, tráfico de red, actividad de aplicaciones, eventos del sistema operativo y datos de sensores de seguridad forman parte de un flujo constante de información que debe ser procesado por los equipos de seguridad.

El desafío principal en estos entornos no consiste únicamente en detectar eventos potencialmente maliciosos, sino en **organizar y priorizar las alertas generadas** para que puedan ser analizadas de manera efectiva por los analistas de seguridad. Sin mecanismos de priorización adecuados, un centro de operaciones de seguridad puede verse rápidamente saturado por la cantidad de alertas generadas.

Para enfrentar este desafío, las operaciones de monitoreo utilizan tres mecanismos operativos principales: el triage de alertas, la definición de umbrales de detección y la gestión de incidentes mediante colas de trabajo y objetivos de nivel de servicio. Estos elementos permiten transformar grandes volúmenes de

datos en un flujo de incidentes gestionables, donde cada alerta recibe un nivel de prioridad y un tiempo esperado de respuesta.

A continuación, analizaremos cómo funcionan estos mecanismos dentro del ciclo de gestión de incidentes. En particular, veremos cómo se clasifican las alertas según su severidad, cómo se establecen los límites que determinan cuándo una alerta debe generarse y cómo se organizan los tiempos de respuesta mediante indicadores operativos como los **Service Level Objectives (SLOs).**

Triage y prioridad

El **triage de alertas** representa una de las primeras etapas del proceso de gestión de incidentes dentro de un centro de operaciones de seguridad (SOC). Su objetivo consiste en analizar rápidamente las alertas generadas por el sistema SIEM para determinar cuáles requieren investigación inmediata y cuáles pueden tratarse con menor urgencia.

El concepto de *triage* proviene del ámbito médico, donde se utiliza para clasificar pacientes según la gravedad de su estado y asignar recursos de atención de manera eficiente. En el contexto de la seguridad informática, este enfoque se adapta para clasificar incidentes potenciales en función de su impacto y su probabilidad de representar una amenaza real.

Los sistemas SIEM pueden generar miles de alertas por día, muchas de las cuales corresponden a comportamientos legítimos dentro de la infraestructura tecnológica. Actividades como actualizaciones automáticas, accesos remotos autorizados o cambios de configuración pueden activar reglas de detección sin representar necesariamente un incidente de seguridad. Por esta razón, el proceso de *triage* permite separar las alertas relevantes de aquellas que corresponden a eventos benignos.

Los marcos de trabajo para equipos de respuesta a incidentes, como el CSIRT Services Framework desarrollado por FIRST, establecen que la clasificación inicial de incidentes debe considerar múltiples factores. Entre ellos se encuentran el tipo de evento detectado, la criticidad del sistema afectado, el alcance potencial del incidente y el impacto que podría tener sobre la organización (FIRST, 2023).

Estos criterios permiten asignar **niveles de severidad** que orientan la prioridad de respuesta. Un intento de acceso no autorizado a un servidor que contiene información sensible puede recibir una prioridad mayor que un evento similar ocurrido en un equipo de usuario con privilegios limitados. De esta forma, el contexto operativo del sistema afectado influye directamente en la clasificación de la alerta.

Durante el *triage* también se realizan tareas de validación destinadas a identificar **falsos positivos**. Muchas reglas de detección utilizan patrones estadísticos o correlaciones entre eventos que requieren verificación adicional. En esta etapa, el analista SOC revisa información contextual como direcciones IP, historial de activida del usuario, ubicación geográfica del acceso o comportamiento previo del sistema (Radiant Security, 2024).

Tabla 1. Niveles de prioridad en el triage de alertas SOC

Nivel de prioridad	Características del evento	Ejemplo de alerta	Acción esperada
Crítica	Evento con impacto directo en activos críticos o evidencia clara de compromiso	Acceso no autorizado a servidor crítico	Investigación inmediata y escalamiento
Alta	Actividad sospechosa con alto potencial de riesgo	Múltiples intentos de autenticación fallida desde una misma IP	Análisis prioritario por analista SOC
Media	Evento anómalo que requiere validación	Actividad inusual de usuario fuera del horario habitual	Revisión contextual y verificación
Baja	Evento informativo o comportamiento	Cambios de configuración	Registro y monitoreo

	esperado	programados	

Fuente: elaboración propia con base en FIRST (2023) y Radiant Security (2024).

Este proceso de análisis preliminar permite reducir significativamente el volumen de alertas que requieren investigación profunda. Al concentrar los recursos de análisis en incidentes potencialmente críticos, el triage contribuye a mejorar la eficiencia operativa del SOC.

Además, la correcta implementación de procesos de triage facilita el establecimiento de métricas operativas. Indicadores como el tiempo promedio de clasificación de alertas o el porcentaje de falsos positivos identificados permiten evaluar el desempeño del proceso de monitoreo y ajustar las reglas de detección cuando sea necesario.

Umbrales

Los **umbrales de alerta** constituyen uno de los mecanismos más utilizados para controlar cuándo un sistema de monitoreo debe generar una alerta. En los sistemas SIEM, estos umbrales permiten distinguir entre actividades normales del sistema y comportamientos que pueden indicar una posible anomalía.

En términos operativos, un umbral representa un valor límite asociado a una métrica o a un conjunto de eventos. Cuando el comportamiento observado supera ese límite, el sistema genera una alerta para indicar que se ha producido una desviación respecto del comportamiento esperado (Wazuh, 2024).

Este enfoque resulta especialmente útil en entornos donde ciertos eventos son habituales pero pueden volverse sospechosos cuando ocurren con una frecuencia inusual. Por ejemplo, un intento fallido de autenticación puede considerarse un evento normal. Sin embargo, múltiples intentos fallidos en un intervalo de tiempo reducido pueden indicar un posible ataque de fuerza bruta.

Las plataformas SIEM utilizan sistemas de clasificación de reglas que asignan diferentes niveles de severidad según la naturaleza del evento detectado. Herramientas de monitoreo como Wazuh, por ejemplo, clasifican las alertas en distintos niveles de gravedad que permiten priorizar su análisis.

La definición adecuada de estos umbrales requiere comprender el comportamiento normal de la infraestructura tecnológica. Cada sistema presenta patrones específicos de uso que dependen del tipo

de actividad que realiza la organización. Por esta razón, los umbrales suelen definirse a partir del análisis histórico de eventos.

Cuando los umbrales se establecen demasiado bajos, el sistema puede generar una gran cantidad de alertas innecesarias. Este fenómeno se conoce como **fatiga de alertas** y puede dificultar la identificación de incidentes reales. Por el contrario, umbrales demasiado altos pueden impedir la detección temprana de actividades maliciosas.

Para evitar estos problemas, muchas organizaciones utilizan un proceso de ajuste progresivo de las reglas de detección. A medida que se analizan los eventos generados por el sistema, los umbrales se recalibran para mejorar el equilibrio entre sensibilidad de detección y reducción de falsos positivos.

Los umbrales también se utilizan para monitorear indicadores operativos del SOC. En estos casos, los límites se aplican a métricas como el tiempo promedio de resolución de incidentes o el número de alertas pendientes de análisis. Cuando estos indicadores superan los valores definidos, el sistema puede generar alertas que advierten sobre posibles problemas operativos (Intrafocus, 2018).

De esta manera, los umbrales cumplen una doble función dentro de los sistemas de monitoreo: permiten detectar anomalías de seguridad y, al mismo tiempo, evaluar el desempeño del proceso de gestión de incidentes.

Encolado

Una vez que las alertas han sido clasificadas y priorizadas mediante el proceso de *triage*, es necesario organizar su tratamiento dentro del flujo de trabajo del centro de operaciones de seguridad. Este proceso se gestiona mediante sistemas de **encolado de incidentes**, que permiten registrar y ordenar las alertas pendientes de análisis.

En los entornos de seguridad, cada alerta relevante se transforma en un **caso o ticket de incidente**. Este registro incluye información sobre el evento detectado, el nivel de severidad asignado, la fuente de los datos y el estado actual de la investigación. De esta forma, cada incidente queda documentado dentro de un sistema que permite realizar su seguimiento a lo largo del proceso de respuesta.

El uso de colas de trabajo permite organizar las tareas del equipo SOC de manera estructurada. Las alertas se ordenan según su prioridad, lo que facilita que los incidentes más críticos reciban atención inmediata. Este mecanismo también permite distribuir el trabajo entre diferentes analistas de seguridad.

En muchos centros de operaciones se utilizan modelos de trabajo escalonados. Los analistas de nivel 1 realizan una revisión inicial de las alertas para confirmar su

relevancia. Cuando un incidente requiere un análisis más profundo, se escala a analistas de nivel 2 o nivel 3, quienes cuentan con mayor experiencia técnica y acceso a herramientas avanzadas de investigación.

El sistema de colas también permite registrar el estado de cada incidente dentro del proceso de respuesta. Entre los estados más comunes se encuentran abierto, en investigación, escalado, resuelto o cerrado. Esta clasificación facilita el seguimiento del progreso de cada caso y permite mantener una trazabilidad completa de las acciones realizadas.

Además, el análisis de las colas de incidentes puede revelar información valiosa sobre el funcionamiento del SOC. Por ejemplo, un aumento sostenido en el número de alertas pendientes puede indicar que el volumen de eventos supera la capacidad operativa del equipo. En estos casos, puede ser necesario ajustar las reglas de detección o incorporar nuevos recursos de análisis.

El encolado de incidentes también permite generar métricas operativas que ayudan a evaluar el desempeño del equipo de seguridad. Indicadores como el tiempo promedio de resolución de incidentes o la cantidad de alertas procesadas por analista permiten identificar oportunidades de mejora en los procesos de monitoreo.

Objetivos de Nivel de Servicio (SLOs)

Los **Service Level Objectives (SLOs)** representan metas cuantificables que permiten medir el desempeño de un servicio tecnológico. En el contexto de las operaciones de seguridad, estos objetivos se utilizan para definir tiempos esperados de respuesta y resolución frente a incidentes detectados por el sistema de monitoreo (Beyer et al., 2016).

El enfoque de SLO se desarrolla ampliamente en el libro **Site Reliability Engineering** publicado por Google, donde se describe cómo las organizaciones pueden utilizar métricas operativas para evaluar la calidad de sus servicios tecnológicos. En este marco, los SLOs establecen valores objetivo que permiten determinar si el servicio está funcionando dentro de los niveles de desempeño esperados.

En los centros de operaciones de seguridad, los SLOs suelen definirse a partir de métricas relacionadas con la gestión de incidentes. Entre los ejemplos más comunes se encuentran el tiempo máximo para analizar una alerta crítica, el tiempo promedio de resolución de incidentes o el porcentaje de alertas investigadas dentro de un período determinado.

Por ejemplo, una organización puede establecer como objetivo que las alertas clasificadas con severidad alta sean analizadas en un plazo máximo de quince minutos desde su detección. Este tipo de métricas permite garantizar que los incidentes críticos reciban atención prioritaria.

Los SLOs forman parte de un sistema más amplio de medición del desempeño que incluye los Service Level Indicators (SLIs) y los Service Level Agreements (SLAs). Los SLIs representan las métricas utilizadas para medir el desempeño del servicio, mientras que los SLAs establecen compromisos formales entre proveedores y clientes respecto de esos niveles de servicio.

Esta relación puede entenderse como una cadena de medición. Los indicadores (SLI) permiten observar el desempeño del sistema, los objetivos (SLO) establecen el nivel esperado y los acuerdos (SLA) formalizan las responsabilidades asociadas a ese desempeño (Atlassian, 2023).

El seguimiento de estos indicadores permite evaluar la eficiencia operativa del SOC y detectar posibles desviaciones en los procesos de respuesta a incidentes. Si los tiempos de análisis superan los valores definidos en los SLOs, puede ser necesario revisar los procedimientos operativos o ajustar la asignación de recursos.

Además, el uso de SLOs facilita la generación de reportes de desempeño que permiten comunicar el estado de las operaciones de seguridad a otros sectores de la organización. Estos reportes contribuyen a mantener la transparencia del proceso de monitoreo y a justificar decisiones relacionadas con la inversión en herramientas o personal especializado.

CONTINUAR

2. Casos, duplicados y ruido vs señal

Los sistemas SIEM operan en entornos donde la generación de eventos es constante y masiva. Cada actividad realizada dentro de una infraestructura tecnológica puede producir registros que posteriormente son analizados por motores de correlación. A partir de estos registros, las reglas de detección generan alertas que indican posibles comportamientos anómalos o incidentes de seguridad.

Este flujo continuo de información plantea un desafío operativo para los centros de operaciones de seguridad (SOC): **distinguir entre señales relevantes y ruido operativo**. Muchas alertas generadas por los sistemas de monitoreo corresponden a eventos repetidos, correlaciones redundantes o comportamientos legítimos que coinciden con patrones de detección. Cuando estos eventos se acumulan sin mecanismos de control adecuados, pueden saturar los procesos de análisis y dificultar la identificación de incidentes reales.

En este contexto, los procesos de gestión de incidentes incorporan mecanismos específicos para reducir la redundancia de alertas, enriquecer la información disponible para el análisis y organizar el flujo de trabajo

del equipo de seguridad. Estas prácticas incluyen técnicas de deduplicación de eventos, procesos de enriquecimiento de información, mecanismos de asignación de casos a analistas y procedimientos formales de cierre de incidentes.

El objetivo de estos procesos consiste en transformar grandes volúmenes de alertas en un conjunto estructurado de casos investigables. De esta forma, los analistas SOC pueden concentrar sus esfuerzos en eventos con mayor relevancia para la seguridad de la organización.

Protección Dinámica del Usuario (Dynamic User Protection o De-dup)

Uno de los problemas más frecuentes en los sistemas SIEM es la generación de **alertas duplicadas o altamente similares.** Cuando múltiples eventos activan la misma regla de detección en un período corto de tiempo, el sistema puede generar numerosas alertas que describen esencialmente el mismo comportamiento.

Este fenómeno se observa, por ejemplo, cuando un atacante realiza múltiples intentos de acceso a un sistema o cuando una aplicación produce repetidamente el mismo tipo de evento de error. Si cada evento genera una alerta independiente, el volumen de incidentes registrados puede aumentar rápidamente, dificultando el trabajo del equipo de seguridad.

Para abordar este problema, los sistemas de monitoreo utilizan técnicas de **deduplicación de alertas**, también conocidas como *de-duplication* o *de-dup*. Estas técnicas permiten identificar eventos repetidos y agruparlos dentro de un mismo caso de incidente.

Las plataformas de gestión de incidentes, como las documentadas en entornos de seguridad empresarial, implementan mecanismos que permiten correlacionar eventos similares y consolidarlos en un único registro de incidente. En lugar de generar múltiples alertas separadas, el sistema agrupa los eventos y actualiza el caso existente con nueva información (IBM, 2023).

Este proceso permite mantener una representación más clara del incidente en curso. En lugar de analizar decenas de alertas independientes, el analista SOC puede revisar un único caso que resume la actividad observada. Esto facilita la comprensión del comportamiento detectado y reduce la carga operativa del equipo de monitoreo.

La deduplicación también contribuye a mejorar la visibilidad de los incidentes críticos. Cuando el sistema elimina o agrupa alertas redundantes, los analistas pueden identificar con mayor facilidad

aquellas alertas que representan eventos realmente nuevos o inesperados.

Además de reducir el volumen de alertas, la deduplicación permite generar métricas más representativas del comportamiento del sistema. En lugar de contar cada evento individual como un incidente independiente, los sistemas de monitoreo pueden registrar un solo caso que refleje la actividad completa asociada al evento.

De esta manera, las técnicas de de-dup contribuyen a mejorar la eficiencia del análisis de seguridad y permiten que los equipos SOC se concentren en incidentes que requieren una investigación real.

Enriquecimiento

El **enriquecimiento de alertas** es un proceso mediante el cual se agrega información adicional a los eventos detectados por el sistema SIEM para facilitar su análisis. Cuando una alerta se genera a partir de una regla de detección, suele contener únicamente los datos básicos asociados al evento original.

Estos datos pueden incluir elementos como direcciones IP, identificadores de usuario, nombres de host o marcas de tiempo. Si

bien esta información permite identificar el evento detectado, muchas veces resulta insuficiente para comprender su contexto completo.

El enriquecimiento busca ampliar esa información incorporando datos provenientes de otras fuentes. Entre estas fuentes se encuentran bases de datos de inteligencia de amenazas, inventarios de activos, sistemas de gestión de identidades y registros históricos de actividad (ThreatConnect, 2019).

Los procesos de Threat Intelligence Enrichment descritos en la literatura sobre integración de inteligencia de amenazas en SIEM permiten complementar las alertas con información contextual relevante. Por ejemplo, una dirección IP detectada en una alerta puede compararse con listas de direcciones asociadas a actividades maliciosas conocidas.

De esta forma, el sistema puede indicar si la dirección IP pertenece a una red previamente identificada como fuente de ataques. Esta información adicional ayuda al analista SOC a determinar con mayor rapidez la gravedad del incidente.

El enriquecimiento también puede incluir información sobre los activos involucrados en el evento. Si el sistema detecta actividad sospechosa en un servidor crítico, el SIEM puede incorporar datos provenientes del

inventario de activos para indicar el rol del sistema dentro de la infraestructura tecnológica.

Esta contextualización permite comprender mejor el impacto potencial del incidente. Un evento detectado en un servidor que almacena información sensible puede requerir una respuesta más inmediata que un evento similar en un equipo de pruebas.

El enriquecimiento también facilita la automatización de procesos de análisis. Cuando las alertas contienen información contextual suficiente, es posible implementar reglas que clasifiquen automáticamente ciertos tipos de incidentes o que asignen prioridades basadas en el riesgo asociado.

De esta manera, el enriquecimiento transforma las alertas técnicas en información más completa y comprensible, lo que permite mejorar la calidad del análisis y acelerar la respuesta a incidentes.

En la práctica operativa de un SOC, la gestión de alertas requiere aplicar criterios consistentes para reducir el ruido y priorizar incidentes relevantes. Veamos algunas de estas prácticas en la siguiente tabla, que distingue entre **acciones recomendadas** y **errores frecuentes** durante el análisis de alertas:

Tabla 2. Buenas prácticas en la gestión de alertas SIEM

Qué hacer	Qué evitar
Analizar el contexto de la alerta antes de clasificarla	Asumir que todas las alertas representan incidentes reales
Utilizar información enriquecida (inteligencia de amenazas, inventario de activos) para validar eventos	Investigar eventos sin contexto o sin revisar fuentes adicionales
Agrupar eventos repetidos mediante mecanismos de deduplicación	Tratar cada alerta duplicada como un incidente independiente
Priorizar incidentes según su impacto en activos críticos	Priorizar únicamente según el volumen de alertas generadas
Documentar las acciones realizadas durante la investigación	Resolver incidentes sin registrar el proceso de análisis
Revisar y ajustar periódicamente las reglas y umbrales del SIEM	Mantener reglas de detección sin revisión durante largos períodos

Fuente: elaboración propia.

Asignación

Una vez que una alerta ha sido validada y enriquecida con información contextual, el siguiente paso dentro del proceso de gestión de

incidentes consiste en **asignar el caso a un analista responsable de su investigación**. Este proceso forma parte del flujo operativo que permite gestionar incidentes de manera organizada dentro de un SOC.

Los marcos de referencia para la gestión de incidentes, como el **NIST SP 800-61 Incident Handling Guide**, describen la importancia de establecer procedimientos claros para la asignación de responsabilidades durante el análisis de incidentes. Esta práctica permite asegurar que cada caso sea investigado por personal capacitado y dentro de los tiempos definidos por los procesos operativos.

En muchos centros de operaciones de seguridad se utiliza un modelo escalonado de análisis. Los analistas de **nivel 1** suelen encargarse de revisar las alertas iniciales y confirmar si corresponden a incidentes reales o a falsos positivos. Este proceso incluye la revisión de registros, la validación de la actividad detectada y la recopilación de información adicional.

Si el incidente requiere un análisis más profundo, el caso puede escalarse a analistas de nivel 2 o nivel 3, quienes poseen mayor experiencia técnica y acceso a herramientas avanzadas de investigación. Estos analistas pueden realizar tareas como análisis forense de registros, correlación de eventos en múltiples sistemas o investigación de actividad maliciosa avanzada.

La asignación de casos también permite mantener un registro claro de las acciones realizadas durante la investigación. Cada analista responsable documenta los pasos seguidos, las herramientas utilizadas y las conclusiones obtenidas. Esta documentación resulta fundamental para mantener la trazabilidad del proceso de respuesta a incidentes (ThreatConnect, 2019).

Además, la asignación estructurada de casos permite distribuir el trabajo de manera equilibrada entre los miembros del equipo SOC. Cuando el volumen de alertas aumenta, los sistemas de gestión de incidentes pueden asignar casos automáticamente según criterios como disponibilidad del analista o especialización técnica.

Este mecanismo contribuye a mantener la eficiencia operativa del equipo de seguridad y permite asegurar que los incidentes se analicen dentro de los tiempos establecidos por los objetivos de servicio definidos por la organización.

Cierre

El **cierre de incidentes** representa la etapa final del proceso de gestión de incidentes dentro de un centro de operaciones de seguridad. Una vez que el análisis ha concluido y se han tomado las acciones necesarias para mitigar o resolver el incidente, el caso puede registrarse como finalizado dentro del sistema de gestión de incidentes.

El proceso de cierre no implica únicamente marcar el incidente como resuelto. Según las recomendaciones del **NIST SP 800-61**, esta etapa también incluye la documentación de las acciones realizadas, la evaluación del impacto del incidente y la identificación de posibles mejoras en los procesos de seguridad.

Durante el cierre del incidente, los analistas suelen registrar información sobre la causa del evento, los sistemas afectados, las medidas de mitigación implementadas y las lecciones aprendidas durante la investigación. Esta información permite construir una base de conocimiento que puede utilizarse en incidentes futuros.

El análisis posterior a los incidentes también puede revelar oportunidades para mejorar las reglas de detección o los procedimientos de respuesta. Por ejemplo, si un incidente fue detectado con retraso debido a una configuración inadecuada de las reglas SIEM, el equipo de seguridad puede ajustar los parámetros de monitoreo para mejorar la detección temprana.

El cierre de incidentes también contribuye a generar métricas operativas que permiten evaluar el desempeño del SOC. Indicadores como el tiempo promedio de resolución, el número de incidentes investigados o la proporción de falsos positivos pueden utilizarse para medir la eficiencia de los procesos de monitoreo (Cichonski et al., 2012).

Además, mantener un registro completo de incidentes cerrados permite analizar tendencias a largo plazo. Al revisar el historial de incidentes, las organizaciones pueden identificar patrones recurrentes de actividad maliciosa y fortalecer sus estrategias de defensa.

De esta forma, el cierre de incidentes no representa simplemente el final de una investigación, sino una oportunidad para consolidar el aprendizaje organizacional y mejorar continuamente los procesos de seguridad.

Tabla 3. Cierre de incidentes SOC

Buenas prácticas	Errores frecuentes
Documentar claramente las acciones realizadas durante la investigación	Cerrar incidentes sin registrar el análisis realizado

Registrar las causas del incidente y las medidas de mitigación aplicadas	Limitar el cierre a marcar el ticket como resuelto
Revisar si es necesario ajustar reglas o umbrales del SIEM	Ignorar oportunidades de mejora en los mecanismos de detección
Incorporar las lecciones aprendidas al conocimiento del equipo SOC	Resolver incidentes sin compartir aprendizajes con el equipo
Verificar que el incidente esté completamente contenido antes del cierre	Cerrar casos mientras el evento aún está activo

Fuente: elaboración propia con base en Cichonski et al. (2012).

CONTINUAR

Referencias

Atlassian. (2023). *SLA vs SLO vs SLI: Understanding the difference*. https://www.atlassian.com/es/incident-management/kpis/sla-vs-slo-vs-sli

Beyer, B., Jones, C., Petoff, J., & Murphy, N. (2016). *Site reliability engineering: How Google runs production systems*. O'Reilly Media. https://sre.google/sre-book/service-level-objectives/

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide* (NIST SP 800-61 Rev. 2). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

FIRST. (2023). *CSIRT services framework version 2.1*. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

IBM. (2023). *Managing duplicate offenses*. https://www.ibm.com/docs/es/i/7.4.0?topic=protection-mirrored-concepts

Intrafocus. (2018). *Understanding KPI targets*. https://www.intrafocus.com/2018/08/understanding-kpi-targets/

Radiant Security. (2024). *SOC alert triage*. https://radiantsecurity.ai/learn/soc-alert-triage/

ThreatConnect. (2019). *Threat intelligence enriched SIEM*. https://threatconnect.com/wp-content/uploads/ThreatConnect-SIEM-Threat-Intelligence-Whitepaper.pdf

Wazuh. (2024). *Rules classification and alert levels*. https://documentation.wazuh.com/current/user-manual/ruleset/rules-classification.html

CONTINUAR