Módulo 4. Monitoreo liviano

CÓRDOBA CREA FUTURO

Introducción

En primer lugar, conviene establecer la definición de lo que se entiende por incidente de ciberseguridad.

Se puede definir como cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de una empresa. Algunos ejemplos son la infección por *malware*, los ataques de denegación de servicio o el robo de datos.

Un incidente de ciberseguridad se transforma en una crisis cuando los daños ocasionados superan la capacidad de respuesta de la entidad afectada. Esto ocurre cuando los recursos y procedimientos habituales no resultan suficientes para abordar el incidente, lo que provoca una escalada en la gravedad y el alcance del problema. Mientras que un incidente puede resolverse de forma estructurada dentro de una organización, una situación de crisis compromete gravemente su operación normal.

Por lo general, una crisis se desencadena ante un incidente clasificado, según su peligrosidad o impacto, como crítico, muy alto o alto. Es

fundamental que las organizaciones estén preparadas para enfrentar ambos escenarios y dispongan de planes de acción adecuados que permitan mitigar los riesgos y reducir las consecuencias de cada situación.

Las diferencias entre un incidente y una crisis incluyen la naturaleza del evento, el impacto, la duración y persistencia, así como la afectación en términos de reputación y confianza. Mientras que un incidente puede gestionarse de forma interna —generalmente por el equipo de TI— y resolverse en un tiempo relativamente breve, una crisis requiere, además de una respuesta técnica, una intervención a nivel ejecutivo y organizativo. Esto implica la movilización de recursos adicionales y la adopción de decisiones estratégicas para mitigar el impacto y restablecer la normalidad operativa. En caso de que no se logre una gestión adecuada, recuperar la confianza perdida puede demandar un esfuerzo considerable y sostenido en el tiempo.

Comprender las diferencias entre ambas situaciones permite implementar estrategias de respuesta más eficaces, optimizar la gestión de recursos y reducir al mínimo el impacto ocasionado.

El monitoreo liviano constituye una estrategia útil para pequeñas y medianas empresas (pyme) con recursos limitados. Consiste en recolectar y analizar información de seguridad de redes y *endpoints* sin recurrir a soluciones costosas, utilizando herramientas de código abierto.

En este módulo, se presenta Wazuh, una plataforma *open source* que integra diversas capacidades:

- Funciones de SIEM (gestión de eventos e información de seguridad),
- Funciones de XDR (detección extendida con respuesta activa), y
- Herramientas para el proceso de *triage*, que permiten priorizar, escalar y documentar incidentes en entornos pyme.

Wazuh permite desplegar agentes livianos en cada equipo y centralizar registros, alertas e informes en un único panel, lo que facilita la detección de amenazas con un costo mínimo.

CONTINUAR

Unidad 1. Wazuh

Figura 1. Wazuh

Fuente: Grabolosa, 2024, https://goo.su/xRsdmV

Antes de avanzar, es necesario definir los conceptos introducidos en el título para comprender el marco de trabajo de Wazuh: SIEM y XDR.

Un sistema de gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés) combina la gestión de la información de seguridad (SIM) con la gestión de eventos de seguridad (SEM) en una solución integral orientada a la detección de amenazas y al cumplimiento normativo. En

términos generales, una SIM recopila, analiza y gestiona los registros y eventos de sistemas o aplicaciones anfitrionas, mientras que un SEM se encarga de supervisar y analizar, en tiempo real, los eventos relacionados con la seguridad.

El sistema SIEM recopila, analiza y correlaciona datos provenientes de diversas fuentes en tiempo real para identificar y responder ante amenazas. Estas fuentes pueden incluir registros de sistemas, aplicaciones, dispositivos de red o equipos finales. Para ello, utiliza técnicas de análisis y correlación que permiten detectar patrones de comportamiento malicioso y generar alertas ante actividades sospechosas. Además, incorpora funciones para la elaboración de informes y la representación visual de los datos.

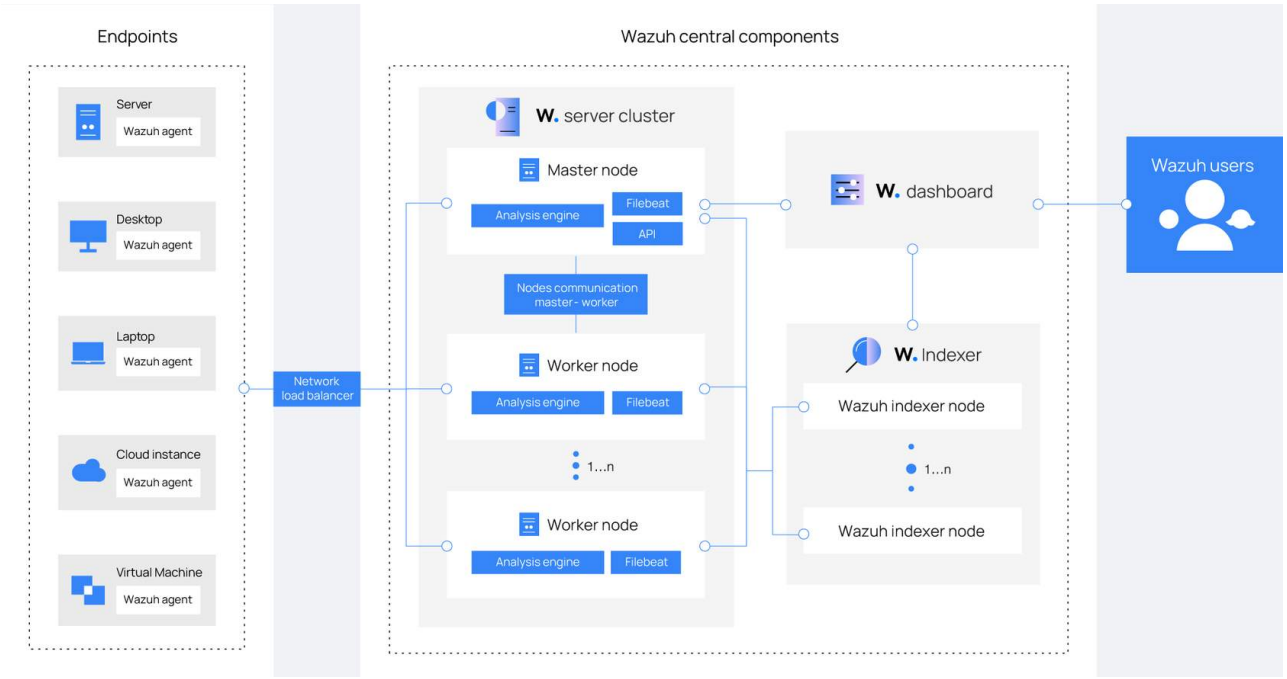
Por su parte, XDR (detección y respuesta extendidas) amplía el alcance del monitoreo, abarcando una gama más amplia de dispositivos o servicios. A diferencia del enfoque pasivo de algunas soluciones, XDR también incorpora mecanismos de respuesta activa automatizada que permiten actuar ante la detección de comportamientos maliciosos.

Wazuh reúne una serie de características que le permiten funcionar como una solución integrada de SIEM y XDR. No obstante, conviene revisar primero su arquitectura.

Wazuh es una plataforma de seguridad gratuita y de código abierto, diseñada incluso para entornos empresariales pequeños. Integra módulos de SIEM, EDR, búsqueda de

amenazas (*threat hunting*), análisis de vulnerabilidades y evaluación de configuraciones. En la siguiente figura se presenta su arquitectura básica: cada *endpoint* (servidor o estación de trabajo) ejecuta un agente que envía eventos al servidor central de Wazuh, donde los datos son procesados. Luego, se visualizan mediante un panel web que presenta alertas, gráficos e informes. Además, Wazuh puede escalar horizontalmente mediante un clúster de indexadores para mejorar su rendimiento.

Figura 2. Arquitectura general de Wazuh



Fuente: Grabolosa, 2024, https://goo.su/xRsdmV

Agentes y registro —

Los agentes de Wazuh se instalan en cada dispositivo final —como estaciones de trabajo, servidores, máquinas virtuales o entornos en la nube— y capturan eventos locales. Tienen la capacidad de recolectar registros del sistema operativo, aplicaciones, cortafuegos y otros dispositivos; además, Wazuh ofrece soporte *agentless* para recopilar datos mediante SNMP o desde cortafuegos externos.

Por ejemplo, en una pyme pueden desplegarse agentes en sistemas Windows y Linux para monitorear inicios de sesión, modificaciones en archivos críticos, eventos de firewall o escaneos de red. Estos agentes envían los registros de forma cifrada al servidor de Wazuh, donde se analizan y correlacionan a través de un sistema de reglas. De este modo, los eventos relevantes se transforman en alertas de seguridad.

Wazuh proporciona agentes compatibles con Windows, Linux, macOS, entre otros sistemas. Su instalación es sencilla, mediante paquetes o scripts, lo que resulta adecuado para organizaciones sin equipos técnicos especializados.

En cuanto al registro, los agentes recopilan eventos desde múltiples fuentes, como directorios (mediante monitoreo de integridad de archivos, FIM), registros de seguridad de Windows o *syslog* en Linux. Toda la información se indexa en formato JSON en el servidor, lo que permite conservar un historial completo de eventos de seguridad, útil para auditorías y análisis posteriores.

En la práctica, una pyme del sector gastronómico —por ejemplo, una pizzería— podría contar con un agente de Wazuh instalado en su servidor de facturación con Windows y otro en su *router* con Linux. Entre los datos recolectados estarían los registros de conexiones bloqueadas por el cortafuegos, intentos fallidos de inicio de sesión y modificaciones en archivos sensibles, como la configuración del

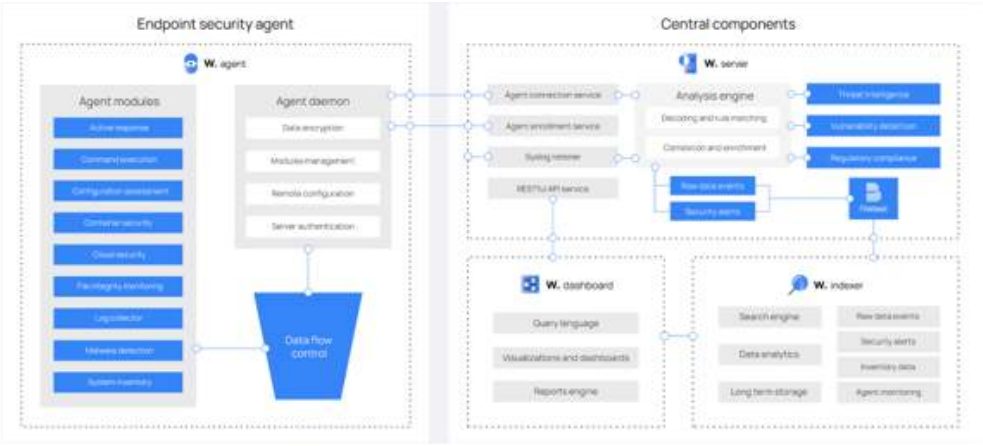
sistema de cobro. Toda esta información se enviaría al servidor de Wazuh para su análisis y generación de alertas.

El despliegue por agentes es flexible —

Wazuh permite construir clústeres de alta disponibilidad en caso de que la organización escale, aunque también puede ejecutarse en una única máquina, lo que resulta adecuado para empresas pequeñas. En todos los casos, no se requiere el pago de licencias por agente, una ventaja relevante para pymes con presupuestos limitados.

La solución se basa en la instalación de un agente en cada dispositivo final (*endpoint*) que se desea monitorear, junto con tres componentes centrales: el indexador, el servidor y el panel de control (*dashboard*). Esta infraestructura puede desplegarse en uno o varios nodos, permitiendo la conformación de un clúster que mejora el rendimiento, la seguridad y la disponibilidad del sistema. A continuación, se presentan los componentes necesarios para el funcionamiento de Wazuh.

Figura 3. Componentes de Wazuh



Fuente: Grabolosa, 2024, https://goo.su/xRsdmV

Reglas iniciales

Wazuh incluye un conjunto de reglas predefinidas y decodificadores que permiten identificar patrones en los registros. El servidor aplica estas reglas al flujo de eventos recibido desde los agentes, utilizando inteligencia de amenazas —como la base de MITRE ATT&CK— para reconocer indicadores maliciosos. Cada evento registrado pasa primero por un decodificador, que extrae los campos clave; luego, se comparan con las reglas disponibles. Si se detecta una coincidencia con un patrón de interés —por ejemplo, un intento de explotación o la presencia de un *malware* conocido—, se genera una alerta de seguridad.

Las **reglas por defecto** abarcan eventos comunes, como intentos fallidos de inicio de sesión, cambios de usuarios, ejecución de comandos sensibles, detección de *malware* mediante huellas hash, o anomalías en servicios. Estas cubren distintas áreas, incluyendo seguridad en Windows y Linux, cortafuegos, auditoría de configuraciones, vulnerabilidades (CVE) y cumplimiento normativo.

En cuanto a la **inteligencia asociada**, Wazuh correlaciona los eventos detectados con bases como MITRE y CVE. Por ejemplo, ante un comportamiento compatible con *ransomware* o la ejecución de un script malicioso, se activa la regla correspondiente con su referencia asociada.

Tras la **instalación**, se recomienda revisar las reglas de mayor nivel (del 0 al 10) para comprender qué tipo de alertas generan. En entornos pyme, se puede comenzar con el conjunto estándar e ir deshabilitando aquellas reglas que no resulten aplicables, como aquellas específicas de sectores financieros si no corresponde.

La **configuración inicial** requiere un esfuerzo mínimo. Wazuh carga automáticamente los archivos de reglas en el directorio «/var/ossec/ruleset/». A partir de allí, es posible ajustar el conjunto de reglas según las necesidades del entorno, por ejemplo, modificando umbrales o excluyendo direcciones IP internas. En resumen, Wazuh incluye un conjunto completo de reglas listas para detectar comportamientos sospechosos, lo que facilita y agiliza su implementación en una pyme.

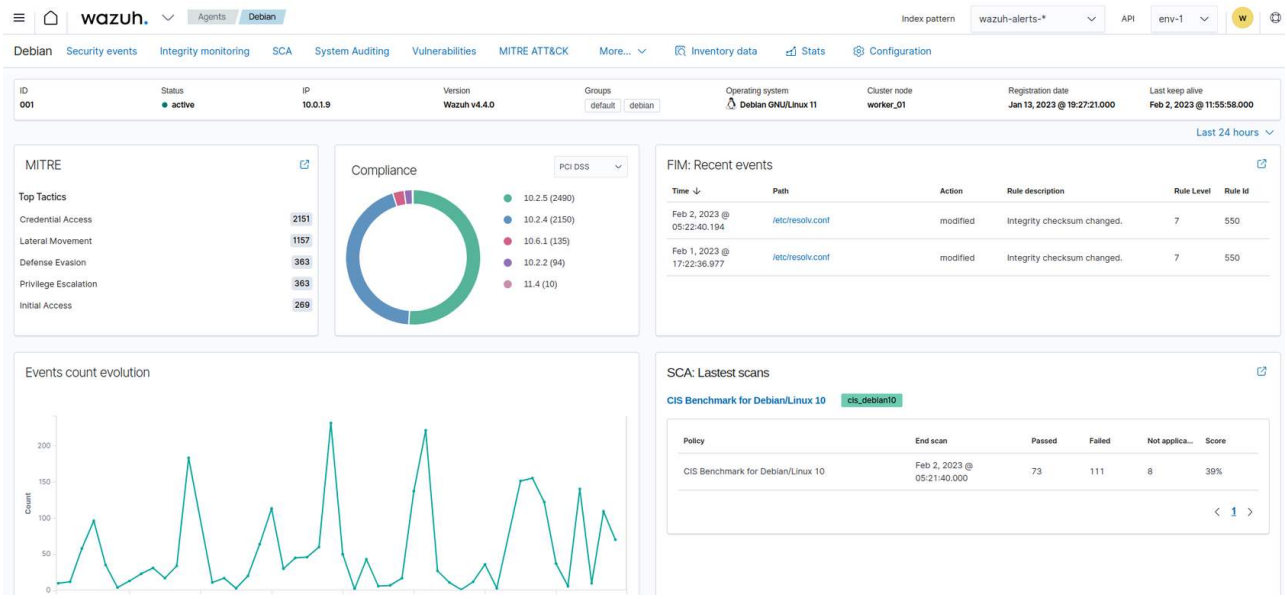
Dashboards y búsquedas

El panel de control (*dashboard*) constituye la interfaz web desde la cual se visualizan los datos recolectados, junto con el análisis de eventos y las alertas de seguridad generadas. Este entorno incorpora diversas funcionalidades que se detallarán más adelante.

Wazuh ofrece un panel unificado —integrado con Kibana o OpenSearch Dashboards— para la visualización centralizada de información. En este se despliegan *widgets* con datos relevantes, como tácticas detectadas según el marco MITRE ATT&CK, cumplimiento normativo (SCA, HIDS), monitoreo de integridad de archivos (FIM) y gráficas que muestran la evolución temporal de los eventos, entre otros.

En la imagen que se presenta a continuación, se observa un ejemplo real del panel de Wazuh: a la izquierda, se muestran métricas relacionadas con MITRE y cumplimiento, mientras que a la derecha se visualizan gráficos vinculados a eventos y alertas —como detección de *malware* o actividad anómala—.

Figura 4. Captura de *dashboard* de Wazuh (Wazuh App en Kibana) con paneles de tácticas MITRE, cumplimiento, integridad de archivos y eventos por hora



Fuente: Grabolosa, 2024, https://goo.su/xRsdmV

Los agentes se instalan en dispositivos finales, como computadoras de escritorio, servidores, instancias en la nube o máquinas virtuales. Permiten prevenir, detectar y responder a amenazas, con compatibilidad para operar en distintos sistemas operativos.

Un aspecto destacable de Wazuh es que, si bien los dispositivos finales requieren la instalación de un agente, también es posible monitorear equipos sin agente (*agentless*), como cortafuegos, *switches*, *routers* o sistemas de detección de intrusiones en red (NIDS).

Además, la plataforma permite realizar búsquedas y consultas sobre los registros indexados. Es posible filtrar eventos por equipo, tipo de alerta o

palabra clave (como nombre de usuario, dirección IP o huella hash), lo que facilita la investigación de incidentes. Ante una alerta, se puede acceder rápidamente al contexto y detalles del evento en el equipo afectado.

La interfaz de Wazuh incluye dos módulos principales para esta tarea: «Discover», que permite realizar consultas libres sobre los registros, y «Dashboard / Threat Hunting», orientado a análisis preconfigurados. A través de estos módulos, es posible realizar búsquedas detalladas y acceder a representaciones gráficas que simplifican la interpretación de la información, incluso para personal sin formación técnica especializada. Por ejemplo, un analista en una pyme puede consultar todos los intentos fallidos de acceso por SSH registrados en el último día o identificar qué regla específica generó una alerta determinada. Las visualizaciones predefinidas —en forma de gráficos o tablas— facilitan la comprensión del estado de seguridad de los sistemas monitoreados.

Funcionalidades y casos de uso de Wazuh —

Wazuh ofrece un conjunto de funcionalidades que permiten supervisar, detectar, analizar y responder a incidentes de seguridad, así como cumplir con normativas vigentes. A continuación, se describen sus principales capacidades:

- **Security Configuration Assessment (SCA).** Supervisa la configuración de sistemas y aplicaciones para verificar el cumplimiento de normas y políticas de

seguridad. Los agentes realizan escaneos periódicos que permiten detectar errores de configuración o vulnerabilidades. Estos controles pueden ajustarse según las necesidades de la organización.

- **Detección de *malware*:** identifica actividad maliciosa y genera indicadores de compromiso asociados a infecciones o ciberataques en dispositivos finales.
- **Monitoreo de integridad de archivos (FIM):** analiza cambios en el contenido, permisos, propiedad o atributos de archivos definidos como críticos.
- **Detección de amenazas:** ofrece visibilidad completa sobre los dispositivos monitorizados. Incluye funciones de conservación, indexación y consulta de registros que permiten investigar amenazas que hayan eludido controles previos.
- **Análisis de registros:** recopila eventos del sistema operativo y aplicaciones, que se envían al servidor de forma segura para su análisis y correlación mediante reglas.
- **Detección de vulnerabilidades:** obtiene datos del inventario de software instalado y los cruza con bases de datos CVE actualizadas para identificar software vulnerable.
- **Respuesta a incidentes:** incluye mecanismos de respuesta activa preconfigurados que permiten aplicar contramedidas ante amenazas en curso.
- **Cumplimiento normativo:** contribuye a satisfacer requisitos de normativas como GDPR, NIST, TSC e HIPAA, especialmente mediante sus funciones SCA y FIM.
- **Higiene de TI:** mantiene un inventario actualizado de los dispositivos monitorizados, lo que mejora la visibilidad de los activos y facilita su gestión.

- **Seguridad en contenedores:** brinda monitoreo y detección de amenazas, vulnerabilidades y anomalías en hosts y contenedores Docker.
- **Protección del entorno laboral e integración con terceros:** se integra con plataformas en la nube como AWS, Microsoft Azure, GCP, Microsoft 365 y GitHub. Esto permite supervisar servicios, máquinas virtuales y actividades, y generar alertas ante riesgos o incumplimientos normativos.

Alertas y tuning

Wazuh transforma los eventos relevantes en alertas que se presentan en el panel de control (*dashboard*) y que pueden reenviarse mediante distintos canales, como correo electrónico, Slack u otras integraciones. Cada regla está asociada a un nivel de severidad (de 0 a 10) y a un identificador único. Es responsabilidad del operador validar estas alertas: en algunos casos son informativas, mientras que en otros reflejan amenazas reales.

Para evitar una sobrecarga de notificaciones irrelevantes, es fundamental realizar un ajuste adecuado de la configuración (*tuning*). A continuación, se describen algunas prácticas:

Revisión de reglas: se ajustan aquellas que generan alertas frecuentes sin relevancia. Por ejemplo, si una aplicación legítima genera constantemente una alerta por ejecución de comandos, se puede desactivar esa regla o establecer una excepción.

- **Umbrales y frecuencia.** Para eventos voluminosos, como múltiples accesos fallidos, es posible elevar el umbral o aplicar correlación por dirección IP o usuario. De este modo, la alerta solo se activará tras un número determinado de intentos dentro de un intervalo de tiempo específico.

- **Listas de ignorados:** se pueden configurar archivos de exclusión con patrones o direcciones IP internas que serán omitidas. Esto permite eliminar alertas conocidas que no representan una amenaza, como escaneos internos rutinarios.
- **Respuestas activas:** como plataforma con capacidades de XDR, Wazuh permite ejecutar acciones automáticas ante determinadas alertas, como activar un cortafuegos o bloquear un usuario. Estas respuestas deben configurarse con cautela, especialmente en entornos de producción.

Un sistema de monitoreo sin una configuración adecuada puede generar una cantidad excesiva de alertas, lo que deriva en fatiga operativa.

Para evitarlo, es importante priorizar los eventos con mayor probabilidad de representar un riesgo. Separar lo probable de lo posible, en función del contexto, permite enfocar la atención en las alertas verdaderamente relevantes.En resumen, Wazuh proporciona el motor de generación de alertas, pero corresponde al usuario refinar las reglas para asegurar que las alertas activas tengan un valor crítico para el negocio.Para facilitar una toma de decisiones más eficiente, se recomienda seguir los cinco pasos que se describen a continuación.

1. **Priorizar desde el inicio.**

Separar lo probable de lo posible, a partir del contexto disponible, permite distinguir las alertas con mayor nivel de prioridad. Este enfoque no se limita únicamente a la respuesta a incidentes, sino que resulta aplicable a la gestión de todas las alertas relevantes. La capacidad de establecer prioridades otorga a los analistas margen operativo para concentrarse en aquellas situaciones que requieren atención inmediata.

2. **Obtener el contexto adecuado**

El triaje de alertas contribuye a reducir la fatiga operativa y facilita su priorización en función del riesgo asociado. Esto se logra incorporando información contextual suficiente. Una de las formas más efectivas de obtener este contexto consiste en agregar y validar indicadores de seguridad internos —como indicadores de compromiso y datos de eventos— junto con inteligencia de amenazas externa.En muchos entornos, la inteligencia de amenazas se incorpora después de clasificar un evento como sospechoso, lo que supone una pérdida de oportunidad, ya que este tipo de información puede aportar contexto relevante en etapas mucho más tempranas del análisis.

El contexto adecuado permite a los equipos de SOC y de respuesta a incidentes diferenciar lo posible de lo probable. Por ejemplo, una alerta por actividad saliente anómala desde un servidor de desarrollo de una entidad financiera puede resultar preocupante y justificar una investigación adicional, aun cuando no se haya confirmado un comportamiento malicioso.

En cambio, si la inteligencia de amenazas indica que las direcciones IP involucradas corresponden a servidores de comando y control dirigidos específicamente a organizaciones del sector financiero, la alerta adquiere una mayor probabilidad de representar una amenaza real y requiere una acción inmediata, como el bloqueo y la activación del proceso de respuesta a incidentes.

3. **Concentrarse en tomar mejores decisiones**

Reducir el volumen de alertas irrelevantes y distinguir entre eventos de alta y baja prioridad permite a los analistas tomar decisiones más acertadas. En este contexto, la coordinación del equipo es fundamental: todos los integrantes deben contar con la misma información respecto a la situación, los riesgos asociados, el impacto potencial y los pasos a seguir.

Uno de los principales desafíos en la gestión de seguridad y riesgos es justamente la orquestación efectiva de los equipos. Para enfrentarlo, algunas organizaciones han comenzado a incorporar manuales operativos —conocidos como *playbooks*— en sus procesos de seguridad y respuesta a incidentes (SOC e IR). Estos documentos definen pasos repetibles desde la detección de un evento sospechoso hasta su clasificación, análisis y resolución. Sirven como guías para mapear o incluso automatizar varias etapas del proceso de respuesta.Sin embargo, aunque útiles, estos manuales suelen ser estáticos y limitados en su capacidad de influir directamente en la toma de decisiones, ya que carecen de un componente clave: la inteligencia situacional en tiempo real.

4. **Aumentar la eficacia mediante la inteligencia situacional**

Existe una diferencia entre compartir información general y asegurar que cada integrante del equipo reciba los datos específicos que necesita para cumplir su función. Por ejemplo, un analista de amenazas buscará información sobre actores maliciosos, amenazas activas contra la organización e indicadores únicos asociados al comportamiento del atacante, poniendo el foco en las primeras etapas de la cadena de ataque (*cyber kill chain*), como reconocimiento, preparación, entrega y explotación.

En cambio, un analista de respuesta a incidentes se centrará en los indicadores de compromiso vinculados a etapas posteriores, como la instalación del *malware*, la comunicación con servidores de comando y control (C&C) y las acciones realizadas sobre los sistemas comprometidos. Aunque ambos profesionales trabajan sobre el mismo incidente, sus necesidades de información son distintas, aunque complementarias.

La inteligencia situacional consiste en entregar la información adecuada, a la persona correcta y en el momento oportuno. Para lograrlo, es necesario integrar

los datos provenientes de diversas fuentes —como SIEM, IDS/IPS, *endpoints*, HIDS o cortafuegos— con inteligencia de amenazas.

Esto permite que cada integrante del equipo acceda a información relevante para su función específica, mejorando la eficacia del trabajo colaborativo.Cuando todos los miembros del equipo reciben información precisa en tiempo real y operan con un objetivo común, se alcanza lo que se denomina un entendimiento compartido, condición fundamental para una respuesta eficaz y coordinada.

5. **Colaborar para tomar mejores decisiones, más rápido**

En esta etapa, un espacio de trabajo colaborativo para la investigación permite llevar el concepto de *playbook* a un plano dinámico, reflejando la toma de decisiones del equipo en tiempo real y operativizándolo mediante procesos automatizados. El marco y el flujo de trabajo se construyen en función de las acciones e interacciones del equipo conforme ocurren. Un entorno de colaboración fluido favorece decisiones más rápidas y eficaces, y permite incorporar las siguientes capacidades:

- **Visión global.** Proporciona una perspectiva unificada que muestra todos los equipos y personas involucradas en la investigación, así como sus actividades dentro de la organización, organizadas por región o área de especialización.
- **Conocimiento centrado:** mantiene una visión de conjunto compartida por todo el equipo, sin perder la capacidad de concentrarse en aspectos específicos según el rol o función de cada integrante.
- **Iteración práctica:** permite que los miembros del equipo trabajen de forma paralela con distintas hipótesis, prueben sus teorías y, posteriormente, compartan los hallazgos con el resto del grupo, lo que optimiza el proceso de análisis y toma de decisiones.

CONTINUAR

Unidad 2. Evaluar, priorizar y clasificar alertas e incidentes de seguridad (triage)

El término *triage* no es exclusivo del ámbito informático. Su origen se remonta a la medicina militar del siglo XVIII, donde era necesario decidir con rapidez qué soldados podían recibir atención. Para ello, los médicos clasificaban a los heridos en tres categorías: imposibles de salvar, urgentes y leves.

En el campo de la ciberseguridad, el concepto conserva su esencia. En lugar de soldados, se clasifican incidentes; y en lugar de heridas físicas, se evalúan los daños potenciales a sistemas y datos. La definición técnica aparece en la guía del *National Institute of Standards and Technology* (NIST), que establece:

"Triage es el proceso llevado a cabo para analizar, clasificar y priorizar eventos de seguridad según su gravedad, impacto y urgencia, con el fin de decidir rápidamente qué incidentes requieren atención inmediata y cuáles pueden esperar" (National Institute of Standards and Technology, 2024, https://goo.su/ypMEyn).

Este proceso es ejecutado, en la mayoría de las organizaciones, por los equipos de respuesta a incidentes, conocidos como CSIRT (*computer security incident response teams*). Su función es comparable a la de un equipo médico de urgencias: reciben alertas, realizan un diagnóstico preliminar y determinan si el incidente es real y cuál es su nivel de gravedad (leve, grave o crítico).

La capacidad del CSIRT para realizar un buen proceso de *triage* puede marcar la diferencia entre contener una amenaza a tiempo o enfrentar una brecha de seguridad con consecuencias importantes.

El *triage* cumple una función doble:

- **Reducir el tiempo de exposición.** Cuanto antes se identifique y clasifique un evento crítico, más rápido se podrá activar la respuesta correspondiente y limitar el impacto.

- **Optimizar los recursos.** Dado que en la mayoría de los entornos no hay un exceso de personal, el proceso de *triage* permite asignar cada alerta al nivel de atención adecuado, liberando a los perfiles más especializados para que se concentren en incidentes complejos.

No se trata solo de clasificar eventos, sino de responder preguntas clave: ¿qué ocurrió? ¿Cómo, cuándo y dónde sucedió? ¿Cuál fue el origen y la

causa probable? Para ello, se recolectan datos específicos del sistema que ayuden a comprender el incidente y activar la respuesta apropiada.

Una vez configurado Wazuh, el paso siguiente consiste en gestionar las alertas e incidentes que se generen. El proceso de *triage* implica analizar, categorizar y priorizar cada evento de seguridad en cuanto se detecta. Esta etapa resulta especialmente crítica en entornos con recursos limitados, como las pymes, donde un mismo analista o un equipo reducido debe tomar decisiones rápidas respecto al nivel de urgencia de cada alerta. El objetivo es responder preguntas como: ¿El evento constituye un incidente real? ¿Qué daños puede causar? ¿Cuál es la urgencia de la respuesta?

Priorización por severidad

Una regla fundamental del proceso de *triage* es clasificar el impacto potencial de los incidentes. Para ello, se emplean niveles de criticidad —por ejemplo: crítico, alto, medio y bajo— que permiten asignar prioridades de forma estructurada.

Se consideran incidentes críticos (P1) aquellos que afectan directamente la confidencialidad, integridad o disponibilidad de sistemas esenciales. Ejemplos típicos son la detección de *ransomware* cifrando archivos o el acceso no autorizado a cuentas privilegiadas, situaciones que pueden interrumpir la operación del negocio de forma inmediata. Tal como señala la Agencia de la Unión Europea para la Ciberseguridad (ENISA), estos son eventos que afectan activos esenciales y requieren acción inmediata, 24/7 (ENISA, 2021).

En cambio, eventos con menor impacto —como escaneos de red sin intrusión o intentos fallidos de inicio de sesión sin señales de exfiltración— se ubican en

niveles inferiores (P2/P3). La mayoría de los marcos de gestión de incidentes asigna prioridades como las siguientes:

- **P2 (alto).** Incidentes graves que no comprometen servicios críticos, pero exigen atención pronta.
- **P3 (medio):** eventos relevantes pero limitados en alcance o impacto.
- **P4 (bajo):** notificaciones informativas que no representan un riesgo inmediato.

Por ejemplo, si Wazuh reporta múltiples intentos fallidos de conexión SSH desde una IP externa hacia un servidor de desarrollo, podría clasificarse como P3. En cambio, la detección de un *exploit* conocido ejecutándose en un servidor de producción requerirá atención inmediata y se categorizará como P1.

Para una asignación de prioridades más precisa, conviene incorporar el contexto: momento del evento (por ejemplo, si ocurrió durante un turno crítico o fin de semana), usuarios implicados, presencia de datos sensibles, entre otros factores.

Cuanto antes se detecte y clasifique un evento crítico, más rápido se activará la respuesta y se reducirá el impacto. Por ello, se recomienda asignar inicialmente una prioridad alta y ajustarla posteriormente tras una evaluación más detallada; es preferible reducir la severidad tras un análisis que subestimar un incidente relevante. Esta práctica permite a los equipos —especialmente en entornos con recursos limitados, como las pymes— concentrarse en las alertas que verdaderamente representan una amenaza para la continuidad del negocio.

Flujo de escalado —

Una vez clasificado un incidente, es necesario escalarlo de forma adecuada para garantizar una respuesta proporcional a su gravedad. En el caso de incidentes P1 o

de severidad alta, el escalamiento debe realizarse de manera inmediata al nivel jerárquico o técnico correspondiente. A continuación, se describe un posible esquema de escalamiento:

1. **Nivel inicial (analista o responsable local de TI).** Se detecta la alerta en Wazuh, se valida su relevancia y se aplican medidas básicas, como el aislamiento del dispositivo afectado.
2. **Escalamiento técnico:** si el incidente supera la capacidad de resolución local —por ejemplo, involucra múltiples sistemas o software malicioso avanzado—, debe derivarse al responsable de TI de la organización o a un equipo especializado externo, como un proveedor de servicios de seguridad.
3. **Escalamiento gerencial:** en situaciones críticas, como la filtración de datos sensibles, se notifica a la gerencia y se activa un comité interno que puede incluir áreas de seguridad, legales y de comunicación, encargado de coordinar la respuesta integral.

Este flujo puede documentarse en un procedimiento interno o *playbook*, que trace los pasos críticos desde la detección hasta la contención. Una práctica recomendada consiste en establecer criterios de escalamiento claros: por ejemplo, todo incidente clasificado como P1 debe notificarse de inmediato al responsable de seguridad (CISO o equivalente) y activar al equipo de respuesta correspondiente. En el contexto de una pyme, esto puede implicar contactar al gerente de TI y registrar el incidente en un informe formal.

Lo fundamental es que cada alerta grave recorra con agilidad la cadena de responsabilidad adecuada, evitando demoras que puedan amplificar el daño.

Comunicación con IT —

La comunicación efectiva es una parte esencial del proceso de ***triage***. El analista debe informar de forma clara y oportuna al personal de tecnología involucrado, y, si corresponde, a otras áreas como gerencia o legal, sobre el incidente detectado. Es recomendable utilizar canales formales, como sistemas de tickets (por ejemplo, JIRA o ServiceNow), correos electrónicos corporativos, plataformas de mensajería como Slack o Teams, o llamadas telefónicas en casos críticos. Lo fundamental es que exista un registro de la comunicación —incluyendo fecha, hora y destinatarios — y que se transmita toda la información relevante: qué ocurrió, qué sistemas se vieron afectados y qué acciones se llevaron a cabo.

Por ejemplo, si Wazuh emite una alerta por un posible acceso no autorizado, el analista puede enviar de inmediato un correo detallando el evento (dirección IP de origen, usuario afectado, hora de ocurrencia) al equipo de redes y al responsable de TI. Asimismo, puede generar un ticket con un enlace directo al evento en Wazuh para facilitar el seguimiento. Esto permite que todas las partes involucradas cuenten con el contexto necesario para actuar de forma coordinada.

Una comunicación deficiente puede derivar en acciones duplicadas, demoras innecesarias o en la falta de respuesta ante un incidente real. Por ello, es importante garantizar que la información llegue a la persona adecuada, de forma completa y en el momento oportuno.

Documentación y cierre —

Una vez resuelto el incidente, se realiza el cierre (o clausura formal). Esto incluye documentar todo el proceso: qué ocurrió, cómo se investigó, qué medidas se tomaron y qué resultados tuvo la respuesta. Se debe elaborar un informe breve (o un ticket cerrado) que contenga, por ejemplo, la línea de tiempo del incidente, evidencias recopiladas (*logs*, capturas de pantalla) y las decisiones de escalada.

Además, se recomienda recopilar *lessons learned* para mejorar procedimientos. Por ejemplo, si una alerta resultó ser un falso positivo de un script interno, se anotará para ajustar esa regla y así evitarlo en el futuro.

Según la guía de INCIBE (2024), al cierre de una crisis "la desactivación de la crisis no termina con la mitigación de la amenaza, sino que se debe realizar una auditoría detallada de cada uno de los procesos" (https://goo.su/4NDWv). Esto implica verificar que el incidente fue contenido (por ejemplo, *malware* eliminado), que no hay puertas traseras abiertas y que se restauró la seguridad del sistema. También conviene comunicar a todos los *stakeholders* relevantes que el incidente ha concluido satisfactoriamente, indicando el impacto final (idealmente «cero» en caso de éxito).

Finalmente, el registro del incidente queda archivado en la documentación interna. Para pymes con certificaciones ISO 27001 o políticas internas, este reporte servirá como evidencia de respuesta adecuada. En cualquier caso, el objetivo es aprender de la experiencia: «comunicarse de manera oportuna con todas las partes y aprender de experiencias pasadas para mejorar la respuesta futura». Cada incidente documentado permite ajustar las reglas de Wazuh, los *playbooks* de *triage* y las prácticas de la empresa.

A continuación, se presenta un resumen de las fases de gestión de crisis de ciberseguridad:

Tabla 1. Fases de gestión de una crisis de ciberseguridad

FASES	DESCRIPCIÓN Y ACCIONES
Fase 0: Preparación	En esta etapa se realizan planes y medidas preventivas para mitigar los posibles riesgos y daños que pueda ocasionar la crisis de ciberseguridad, antes de que esta suceda. Esto incluye la definición de roles y responsabilidades, gestión de stakeholders, definición de planes de continuidad de negocio y planes de recuperación ante desastres, realización de inventariado de activos y análisis de riesgos y ejecución de simulacros.
Fase 1: Identificación y análisis	Una vez identificado un incidente, deberá de ser notificado internamente y, además, deberá llevarse a cabo un análisis que permita determinar si cumple con los requisitos para tratar la situación como una crisis. En caso afirmativo, deberá convocarse el Comité de Crisis.
Fase 2: Respuesta y comunicación	Con la información recopilada, el Comité de Crisis tomará la decisión de activar el plan de gestión de crisis de ciberseguridad, en caso de que cumpla con los criterios previamente definidos. En este momento, se determinarán las primeras acciones de contención que permitan minimizar el impacto para, posteriormente, erradicar el incidente y recuperar los sistemas afectados. Mientras se llevan a cabo estas acciones, se debe mantener en todo momento una comunicación clara y transparente con todos los stakeholders identificados.
Fase 3: Cierre	Una vez que la crisis ha sido controlada y resuelta, el comité tomará la decisión de desactivar la situación de crisis. En este punto es importante analizar lo sucedido, identificar las áreas de mejora y extraer lecciones que puedan ser aplicadas en el futuro, mejorando la respuesta ante futuras crisis.

Fuente: INCIBE, 2024, https://goo.su/4NDWv

La desactivación del plan de gestión de crisis de ciberseguridad es el punto de cierre del proceso de gestión de la crisis, cuya decisión es competencia del Comité de Crisis. En esta fase, y con el objetivo de ayudar a esta toma de decisiones, también se debe realizar una revisión del estado actual de las amenazas de ciberseguridad (previo informe del grupo técnico y/o responsable) para valorar si el incidente efectivamente ha sido solucionado. Si la amenaza ha sido

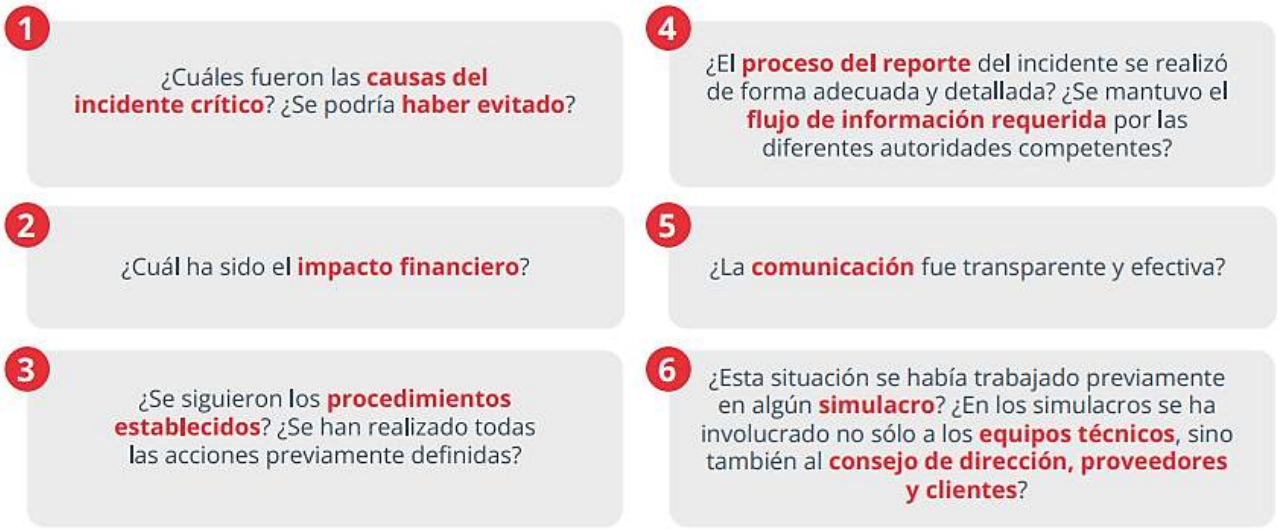
mitigada y la empresa puede volver a desarrollar sus funciones y actividades correctamente, se procederá formalmente al cierre de la crisis. Es importante resaltar que la desactivación de la crisis debe ser comunicada ante todos los *stakeholders* y las autoridades competentes, a través de los canales que hayan sido anteriormente definidos y con las pautas desarrolladas en el apartado de comunicación.

Lecciones aprendidas

Es necesario precisar que el cierre de la crisis de ciberseguridad no termina con la mitigación de la amenaza, sino que se debe realizar una auditoría detallada de cada una de las etapas, las acciones realizadas y los grupos involucrados, con el objetivo de identificar mejoras aplicables tanto en las medidas de seguridad de la empresa como en el procedimiento seguido. Se deben documentar aquellas prácticas que funcionaron correctamente —y que, por tanto, pueden mantenerse—, así como los puntos que requieren mejoras significativas.

Con toda esta información, se puede desarrollar un plan de mejora que establezca prioridades y plazos para la implementación de los cambios. También es conveniente solicitar *feedback* por parte del equipo encargado de responder al incidente, así como de las personas afectadas, para incorporar distintas perspectivas.

Figura 5. Preguntas para el análisis posterior a un incidente crítico



Fuente: INCIBE, 2024, https://goo.su/4NDWv

Laboratorio guiado (opcional) —

A continuación, se propone un laboratorio práctico que puede ser realizado sin costo por pymes que deseen experimentar con la plataforma Wazuh utilizando herramientas libres y entornos controlados. Este ejercicio permite validar el funcionamiento del sistema, comprender su arquitectura y observar alertas reales generadas en condiciones simuladas.

1. **Preparar el entorno.** Necesitarás dos máquinas virtuales (puedes usar VirtualBox, VMware o alguna nube gratuita como Oracle Cloud o AWS Free Tier). Una será el servidor Wazuh (se recomienda Ubuntu 22.04 LTS) y la otra actuará como endpoint (Windows 10 o Linux). Asegúrate de que ambas estén en la misma red interna.
2. **Instalar Wazuh Server.** Sigue la documentación oficial para instalar Wazuh Manager en la máquina del servidor. Asegúrate de incluir OpenSearch (o Elasticsearch OSS) y OpenSearch Dashboards, que te van a servir para ver los datos desde el navegador. Todo el software es libre y gratuito.

3. **Configurar el agente.** En la máquina cliente, instala el agente de Wazuh correspondiente (.deb en Linux o .msi en Windows). Después, regístralo en el servidor y configura qué logs debe recolectar (por ejemplo, syslog para Linux o Event Viewer para Windows). Reinicia el servicio de Wazuh en ambas máquinas para activar todo.
4. **Generar *logs* simulados.** Provoca eventos que generen actividad sospechosa. Por ejemplo:

    - En Linux, intenta acceder a archivos restringidos (`sudo cat /etc/shadow`), modifica archivos de configuración o lanza comandos de red.
    - En Windows, haz intentos fallidos de inicio de sesión o cambia configuraciones del sistema.

5. **Observar los resultados en el *dashboard*.** Ingresa a OpenSearch Dashboards desde tu navegador. Allí, verás *widgets* con alertas recientes, tácticas MITRE ATT&CK, cumplimiento normativo, actividad por hora, etc. Usa la sección «Threat Hunting» para buscar eventos por IP, host o palabra clave.
6. **Configurar alertas y reportes.** Puedes personalizar reglas en `/var/ossec/ruleset/rules` para que Wazuh genere alertas específicas (por ejemplo, si hay más de cinco intentos de login fallidos en cinco minutos). También puedes activar respuestas automáticas o configurar notificaciones por correo. Finalmente, genera un reporte con las alertas recientes desde la sección «Reports».

Este laboratorio enseña a desplegar y verificar rápidamente un SIEM básico con Wazuh, sin necesidad de inversión monetaria. Se recomienda realizarlo primero en un entorno de prueba —preferentemente *air-gapped*— para familiarizarte con la

herramienta. La documentación oficial de Wazuh y los foros comunitarios en español pueden guiarte en cada paso.

CONTINUAR

Referencias

European Union Agency for Cybersecurity [ENISA]. (2021). *Incident classification for the EU CSIRTs network*. https://www.enisa.europa.eu/publications/incident-classification-for-the-eu-csirts-network

Grabolosa, P. (2024). *Wazuh – Una plataforma de Código Abierto que unifica SIEM y XDR*. InLab. https://inlab.fib.upc.edu/es/articulos/wazuh-una-plataforma-de-codigo-abierto-que-unifica-siem-y-xdr

INCIBE. (2024). *Guía de gestión de crisis de ciberseguridad en empresas*. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_gestion_de_crisis.pdf

National Institute of Standards and Technology. (2024). *Computer Security Incident Handling Guide* (NIST Special Publication 800-61 Rev. 3). https://doi.org/10.6028/NIST.SP.800-61r3

Referencias bibliográficas de referencia

Oliva, D. (2025). *Triage informático: Guía práctica para priorizar incidentes*. OpenWebinars. https://openwebinars.net/blog/triage-informatico-guia-practica-para-priorizar-incidentes/

ThreatQuotient. (2021, 31 de marzo). *Fatiga por alertas de seguridad: Cinco pasos para tomar mejores decisiones, más rápido*. Digital Biz Magazine. https://www.digitalbizmagazine.com/fatiga-por-alertas-de-seguridad/

Se incorporaron recomendaciones datos de informes de Kaspersky sobre incidentes en pymes.

https://www.itwarelatam.com/2025/02/11/segun-kaspersky-las-pymes-enfrentaron-un-promedio-de-16-incidentes-de-ciberseguridad-durante-2024/

Se consultó la guía de INCIBE sobre gestión de crisis para enfatizar la comunicación y documentación en incidentes

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_gestion_de_crisis.pdf

CONTINUAR