APUNTES 05

DETECCIÓN Y DOCUMENTACIÓN DE INCIDENTES DE CIBERSEGURIDAD

INCIDENTES DE CIBERSEGURIDAD

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

La Importancia de la Detección de Incidentes

La detección de incidentes es clave en cualquier ámbito y además es fundamental que se efectúe en tiempo y forma.

En su día, un incidente no detectado a tiempo en uno de bastiones más famosos de la Historia, cambió la concepción del mundo entero y dio lugar al orden internacional tal y como lo conocemos hoy: la caída de Constantinopla en manos de los otomanos.

"Espantoso eco encuentra la noticia en Roma, en Génova, en Venecia. Como el retumbar del trueno se extiende a Francia, a Alemania, y Europa ve, conturbada, que por culpa de su ciega indiferencia ha penetrado por la Kerkaporta, la malhadada y olvidada puerta, una nefasta y devastadora potencia que debilitará sus fuerzas por espacio de siglos. Pero en la Historia, como en la vida humana, el deplorar lo sucedido no hace retroceder el tiempo, y no bastan mil años para recuperar lo que se perdió en una sola hora" (Stefan Zweig)

Constantinopla era una ciudad prácticamente inexpugnable. Era la capital de un imperio de más de 1000 años, protegida por murallas triples con foso, y cerrado su puerto natural, el Cuerno de Oro, con una enorme cadena de hierro. Además, sus navíos estaban equipados con un arma cuya fórmula aún hoy no se conoce del todo: el fuego griego. El fuego griego era una sustancia líquida que se lanzaba con cañones y que ardía en contacto con el agua, haciendo naufragar a las naves enemigas.

El asedio fue increíble, con artillería, con navíos transportados por tierra, con bombardeos de enormes cañones de bronce, con innumerables tropas, pero Constantinopla no cayó por todo esto. Constantinopla se perdió por no detectar a tiempo un incidente: ¡la Kerkaporta noroeste se dejó entreabierta! La kerkaporta era una pequeña puerta de servicio para tránsito de peatones y avituallamiento en tiempos de paz, que se dejó abierta por un descuido. Un pequeño número de jenízaros penetraron por ella, se situaron tras las filas de los defensores y proclamaron a voces que la ciudad estaba tomada. Esto provocó la desbandada de la soldadesca y la caída de la ciudad, que habría podido esperar un poco más a la escuadra veneciana que venía de camino en su auxilio, pero el incidente pasó desapercibido a los guardianes de las torres cercanas.

Y así, una ciudad que había resistido con éxito 22 asedios a lo largo de la Historia fue saqueada con saña. De haberse detectado a tiempo el incidente no habría ocurrido nada reseñable, pues esta puerta sólo permitía el paso de personas de una en una y el número de invasores que engañaron a los guardias fue, en realidad, muy reducido.

En esta unidad se revisarán los procedimientos de notificación de incidentes, interna y externamente, priorizando la notificación obligatoria por los cauces oficiales.

Estos procedimientos contendrán indicaciones relativas a la apertura del incidente, el detalle a informar acerca del mismo, las ventanas temporales de reporte, las entidades destinatarias de la información y, finalmente, las condiciones que se tendrán que dar para el cierre del incidente.

1.- DESARROLLAR PROCEDIMIENTOS DE ACTUACIÓN PARA LA NOTIFICACIÓN DE INCIDENTES.

El Concepto de CSIRT

Un Equipo de Respuesta a Incidentes de Seguridad es una organización que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad.

Estos procedimientos recopilan la información relativa a la notificación para enviarla a la autoridad competente o CSIRT de referencia, con objeto de que quede registrado el incidente de ciberseguridad.

Estos procedimientos deberán contemplar la secuencia de notificación, así como los criterios empleados y las tablas a consultar para asignar los niveles de peligrosidad e impacto correspondientes en cada caso.

Para saber más: El Consejo Nacional de Ciberseguridad edita y mantiene la Guía Nacional de Notificación y Gestión de Ciberincidentes, que contiene las pautas oficiales a seguir en cada caso.

Dichas pautas se resumen en este apartado, no obstante, se puede disponer del detalle completo de las mismas descargando la Guía desde el siguiente enlace: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

1.1.- CRITERIOS PARA LA NOTIFICACIÓN.

Para la notificación de los incidentes de ciberseguridad se utilizará como criterio de referencia el Nivel de Peligrosidad que se asigne a un incidente, sin perjuicio de que a lo largo del desarrollo, mitigación o resolución del mismo, se categorice con un determinado Nivel de Impacto (según el Esquema Nacional de Seguridad) que haga aconsejable la comunicación del incidente a la autoridad competente o CSIRT de referencia.

En todo caso, cuando un determinado suceso pueda asociarse a más de un tipo de incidente contenido en la Tabla de Clasificación/Taxonomía de los ciberincidentes debido a sus características potenciales, éste se asociará a aquel que tenga un Nivel de peligrosidad superior de acuerdo con los criterios correspondientes.

1.1.1.- NIVEL DE PELIGROSIDAD DEL CIBERINCIDENTE.

El indicador de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en los sistemas de información o comunicación del ente afectado, así como para los servicios prestados o la continuidad de negocio en caso de haberla. Este indicador se fundamenta en las características intrínsecas a la tipología de amenaza y su comportamiento.

En la Guía Oficial se incluye la Tabla de Criterios de determinación del nivel de peligrosidad de un ciberincidente. Mediante la consulta de esta tabla, las entidades notificadoras de información podrán asignar un determinado nivel de peligrosidad a un incidente. A grandes rasgos, los niveles de peligrosidad son los siguientes:

Bajo

- Spam
- Scanning o sniffing

Medio

- Discurso de odio
- Ingeniería Social
- Intrusión o Intento de Intrusión

- Uso no autorizado de recursos
- Fraude
- Denegación de servicio
- Revelación de información

Alto

- Pornografía infantil, contenido sexual, violencia
- Infección por código dañino
- Compromiso de aplicaciones y cuentas
- Denegación de servicio distribuida
- Compromiso de la información
- Phishing

Muy Alto

- Distribución y configuración de malware
- Robo y sabotaje
- Interrupciones

Crítico

- Amenazas Persistentes Avanzadas

1.1.2.- NIVEL DE IMPACTO DEL CIBERINCIDENTE.

El indicador de impacto de un ciberincidente se determinará evaluando las consecuencias de éste en las funciones y actividades de la organización afectada, en sus activos o en los individuos afectados. De acuerdo con ello, se tienen en cuenta aspectos como las consecuencias potenciales o materializadas que provoca una determinada amenaza en un sistema de información y/o comunicación, así como en la propia entidad afectada (organismos públicos o privados, y particulares).
Los criterios empleados para la determinación del nivel de impacto asociado a un ciberincidente atienden a los siguientes parámetros:

- Impacto en la Seguridad Nacional o en la Seguridad Ciudadana.
- Efectos en la prestación de un servicio esencial o en una infraestructura crítica.
- Tipología de la información o sistemas afectados.
- Grado de afectación a las instalaciones de la organización.
- Posible interrupción en la prestación del servicio normal de la organización.
- Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.
- Pérdidas económicas.
- Extensión geográfica afectada.
- Daños reputacionales asociados.

Los incidentes se asociarán a alguno de los siguientes niveles de impacto: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO o SIN IMPACTO.
En la Guía Oficial se incluye la Tabla de Criterios de determinación del nivel de impacto de un ciberincidente. Mediante la consulta de esta tabla, las entidades notificadoras de información podrán asignar un determinado nivel de impacto a un incidente en concreto.

1.1.3.- NIVELES CON NOTIFICACIÓN OBLIGATORIA ASOCIADA.

Los incidentes se asociarán a uno de los niveles de peligrosidad e impacto establecidos en la Guía Oficial, teniendo en cuenta la obligatoriedad de notificación de todos aquellos que se categoricen con un nivel CRÍTICO, MUY ALTO O ALTO para todos aquellos sujetos obligados a los que les sea aplicable normativa específica de acuerdo con lo contemplado en dicha Guía, en función de su naturaleza.
En ese caso, deberán comunicar, en tiempo y forma, los incidentes que registren en sus redes y sistemas de información y estén obligados a notificar por superar los umbrales de impacto o peligrosidad establecidos en la Guía.

1.2.- INTERACCIÓN CON EL CSIRT DE REFERENCIA.

Los CSIRT de referencia disponen de herramientas de notificación y ticketing de incidentes para lograr una mejor gestión y seguimiento del incidente con los usuarios. Cada CSIRT puede proporcionar diversos métodos de interacción con estas herramientas para facilitar la interacción durante todo el ciclo de vida del incidente.
No obstante, en caso de no disponer de las herramientas proporcionadas por los CSIRT de referencia, se considera válido el uso de correo electrónico.

1.3.- APERTURA DEL INCIDENTE.

Siempre que el CSIRT de referencia recibe una notificación sobre un posible ciberincidente, el equipo técnico realiza un análisis inicial que determinará si el caso es susceptible de ser gestionado por el mismo. Esta apertura puede producirse por un reporte del afectado, por una detección del CSIRT como parte de las labores de detección que realizan o por un tercero que reporta al CSIRT un incidente que afecta a su comunidad de referencia.

Si aplica la gestión del ciberincidente por parte del CSIRT, se registrará la información reportada y se asignarán una clasificación y unos valores iniciales de peligrosidad e impacto que serán comunicados al remitente, iniciándose posteriormente las acciones necesarias para la resolución del ciberincidente.

Durante el registro de un ciberincidente, el CSIRT asignará a cada caso un identificador único que estará presente durante todas las comunicaciones relacionadas con el incidente. Si las comunicaciones se realizan por correo electrónico, este identificador aparecerá en el campo “asunto” y no deberá modificarse o eliminarse ya que esto ralentizaría la gestión y la resolución final del ciberincidente.

A lo largo del proceso de gestión del ciberincidente, el CSIRT podrá comunicarse con el remitente o con terceras partes para solicitar o intercambiar información adicional que agilice la resolución del problema.

Asimismo, las autoridades competentes podrán establecer canales de comunicación oportunos según se desarrolle reglamentariamente.

1.4.- INFORMACIÓN A NOTIFICAR.

Para una correcta gestión y tratamiento de incidente registrado, se hace necesario disponer de datos e informaciones precisas acerca del mismo.

La Guía Oficial incluye una tabla que reseña la información a notificar en un ciberincidente, a modo de orientación para la entidad afectada por el ciberincidente en su comunicación a la autoridad competente o CSIRT de referencia.

Todos aquellos sujetos obligados a los que les sea aplicable normativa específica de acuerdo con lo contemplado en la Guía Oficial, deberán comunicar en tiempo y forma toda aquella información relativa al incidente registrado que les sea exigible.

El sujeto obligado comunicará en la notificación inicial todos aquellos campos de la tabla acerca de los que tenga conocimiento en ese momento, siendo posteriormente perceptiva la cumplimentación del resto de los campos, que se resumen a continuación:

- Asunto
- Operador de Servicios Esenciales o Proveedor de Servicios Digitales
- Sector Estratégico
- Fecha y hora del incidente
- Fecha y hora de detección del incidente
- Descripción
- Recursos tecnológicos afectados
- Origen del incidente
- Taxonomía
- Nivel de peligrosidad
- Nivel de impacto
- Impacto transfronterizo
- Plan de acción y contramedidas
- Afectación
- Medios necesarios para la resolución
- Impacto económico estimado
- Extensión geográfica
- Daños reputacionales
- Adjuntos
- Regulación afectada
- Requerimiento de actuación de las Fuerzas y Cuerpos de Seguridad del Estado

1.5.- VENTANA TEMPORAL DE REPORTE.

Todos aquellos sujetos obligados que se vean afectados por un incidente de notificación también obligatoria a la autoridad competente, a través del CSIRT de referencia, remitirán, en tiempo y forma, aquellas notificaciones inicial, intermedia y final requeridas de acuerdo con la Tabla de Ventana temporal de reporte para sujetos obligados que figura en la Guía Oficial.

- La notificación inicial es una comunicación consistente en poner en conocimiento y alertar de la existencia de un incidente.

- La notificación intermedia es una comunicación mediante la que se actualizarán los datos disponibles en ese momento relativos al incidente comunicado.

- La notificación final es una comunicación final mediante la que se amplían y confirman los datos definitivos relativos al incidente comunicado.

Además, se aportarán todas aquellas notificaciones adicionales intermedias o posteriores que se consideren necesarias.

La comunicación se realizará siempre por escrito mediante el uso de correo electrónico o sistema proporcionado por el CSIRT de referencia del operador, enviando la Tabla de Información a notificar en un ciberincidente a la autoridad competente que figura en la Guía Oficial.

1.6.- ESTADOS Y VALORES DE CIERRE.

Durante las distintas fases de gestión de un ciberincidente, el CSIRT de referencia mantendrá el incidente en estado abierto, realizando en coordinación con el afectado las acciones necesarias y los seguimientos adecuados.
Una solución y el cierre del ciberincidente asociado no suponen siempre una resolución satisfactoria del problema. En algunos casos no es posible alcanzar una solución adecuada por diferentes razones, como pueden ser la falta de respuesta por parte de algún implicado o la ausencia de evidencias que permitan identificar el origen del problema.
En la Guía Oficial se detalla la Tabla de Estados de los ciberincidentes, que muestra los diferentes estados que puede tener un ciberincidente en un instante dado, a saber:

- Cerrado.
    - Resuelto y con respuesta por parte del organismo afectado.
    - Resuelto y sin respuesta por parte del organismo afectado.
    - Sin impacto
    - Falso positivo
    - Sin Resolución y con respuesta por parte del organismo afectado.
    - Sin Resolución y sin respuesta por parte del organismo afectado.
- Abierto

En la Guía Oficial se indican asimismo los días tras los que se cerrará un ciberincidente sin respuesta, en función de su nivel de peligrosidad o impacto.

2.- NOTIFICACIÓN INTERNA DE INCIDENTES.

Caso práctico
Se denomina Notificación Interna de Incidentes al conjunto de mecanismos, procedimientos, reglas y sistemas de Registro y Notificación propios de cada organización privada.
Según esto, no hay un estándar genérico para estos mecanismos de notificación, no obstante, sí que suele haber estándares de facto internos a cada una de las organizaciones.

La definición del flujo de notificación interna tiene lugar en el ámbito de cada empresa, compañía o corporación empresarial, y tiene por objeto protocolizar el registro de datos del incidente con detalle suficiente y notificarlo de forma normalizada a la jerarquía de la empresa. A partir de dicha notificación, la organización tomará las medidas internas adecuadas, e incluso desencadenará las correspondientes notificaciones oficiales, en caso de que procedan.
Por lo general, el flujo de notificación interna se implementa mediante un sistema ad hoc, que se basa en la información registrada automáticamente en un SIEM, complementada con los datos adicionales recogidos por los técnicos en el momento de detección del incidente.

3.- NOTIFICACIÓN DE INCIDENTES A QUIENES CORRESPONDA.

Sistema de Ventanilla Única
Mediante el sistema de ventanilla única se informa de un incidente. La información solicitada en cada caso, en función de la naturaleza del afectado, deberá ser remitida de acuerdo con el cauce establecido por su autoridad competente o CSIRT de referencia.

Funcionamiento del sistema de ventanilla única:
Primero. El sujeto afectado enviará un correo electrónico (o ticket) al CSIRT de referencia (INCIBE-CERT o CCN-CERT) notificando el incidente.
Segundo. El CSIRT de referencia, dependiendo del incidente, pondrá en conocimiento del mismo al organismo receptor implicado o la autoridad nacional competente:

- Si afecta a la Defensa Nacional, al ESP-DEF-CERT
- Si afecta a Infraestructura Crítica de la Ley PIC 8/2011, al CNPIC
- Si afecta al RGPD, a la AEPD.
- Si es un incidente de AAPP bajo el ENS de peligrosidad MUY ALTA o CRÍTICA, al CCN-CERT
- Si es un incidente de obligatorio reporte según el RD Ley 12/2018, a la autoridad nacional competente correspondiente:
    - RGPD: se remite la URL del portal de la AEPD.
    - BDE: se remite la plantilla de notificación .XLS del BDE.
    - PIC: se remite la plantilla de notificación .XLS del CNPIC.
    - ENS: se remite la plantilla de notificación .DOC a CCN-CERT.
    - NIS: se remite la plantilla de notificación de la autoridad nacional competente.

Tercero. El Organismo receptor implicado o autoridad nacional competente se pone en contacto con el sujeto afectado para recabar datos del incidente.
Cuarto. El sujeto afectado comunica los datos necesarios al organismo receptor implicado o autoridad nacional competente.

Quinto. Si procede, desde la Oficina de Coordinación Cibernética (CNPIC) se pone la información a disposición de las Fuerzas y Cuerpos de Seguridad del Estado y Ministerio Fiscal para iniciar la investigación policial y judicial (art. 14.3 RD Ley 12/2018).

Autoevaluación I

De los siguientes criterios, marcar el que no se utiliza para la determinación del nivel de impacto asociado a un incidente:

a) Tipología de la información o sistemas afectados.
b) Grado de afectación a las instalaciones de la organización.
c) Nivel de impacto reglado para el malware documentado
d) Posible interrupción en la prestación del servicio normal de la organización.

Autoevaluación II

¿Cuál de los siguientes campos pueden cumplimentarse a posteriori tras la notificación inicial? Multirespuesta

a) Fecha y hora del incidente
b) Nivel de impacto
c) Descripción
d) Plan de acción y contramedidas

Autoevaluación III

¿Cómo se efectuará la notificación al CSIRT de referencia?

a) Siempre por escrito, utilizando sólo correo electrónico
b) Siempre por escrito, utilizando sólo el sistema proporcionado por el CSIRT de referencia
c) Siempre por escrito, utilizando correo electrónico o el sistema proporcionado por el CSIRT de referencia
d) En caso de emergencia máxima, se puede notificar el incidente por teléfono

Autoevaluación IV

¿Qué empresas deben tener un flujo de notificación interna de incidentes?

a) Las grandes corporaciones
b) Las PYMEs
c) Todas las empresas, sin distinción

Autoevaluación V

¿Cómo se actúa en la notificación urgente de incidentes a las autoridades competentes?

a) Se envía una notificación al CSIRT de referencia, INCIBE-CERT o CCN-CERT, que actúa como Ventanilla Única y lo remite a su vez al organismo receptor implicado en cada caso
b) Cuando se trata de una notificación realmente urgente, se puede obviar la comunicación a la Ventanilla Única y se puede acceder directamente al organismo receptor (ESP-DEF-CERT, CNPIC, AEPD, BDE)

TEST I

1- ¿Qué Nivel de Peligrosidad tiene la "Denegación de Servicio Distribuida"?

a) Muy Alto.
b) Bajo.
c) Medio.
d) Alto.
e) Crítico.

2- ¿Cómo se actúa cuando un determinado suceso puede asociarse a más de un tipo de incidente contenido en la Tabla de Clasificación?:

a) Se recopilará más información y se volverá a analizar el incidente, hasta que quede suficientemente clara la categoría a la que se debe asociar.
b) Se asociará a aquel tipo que tenga un Nivel de peligrosidad superior, de acuerdo con los criterios correspondientes.
c) Se asociará a todos los tipos de incidentes relacionados con él.

3- ¿Qué Nivel de Peligrosidad tiene el "Fraude"?

a) Muy Alto.
b) Bajo.
c) Medio.
d) Alto.
e) Crítico.

4- Para la notificación de los incidentes de ciberseguridad se utiliza como referencia:

a) La Taxonomía de Referencia.
b) El Nivel de Impacto.
c) Los datos recopilados por los sistemas de alerta temprana.
d) El Nivel de Peligrosidad.

5- Un ciberincidente sin respuesta se cerrará tras:

a) 10 días.
b) Un número de días que depende de su nivel de peligrosidad o impacto.
c) 15 días.
d) 20 días.

6- ¿Qué contiene, entre otras cosas, el ENS?:
   a) Los Niveles de Impacto de los incidentes.
   b) Nada de lo anterior.
   c) Los Niveles de Peligrosidad de los incidentes.
   d) La relación entre Niveles de Peligrosidad y Niveles de Impacto.
7- ¿Qué Nivel de Peligrosidad tiene el "Scanning o Sniffing"?
   a) Alto.
   b) Medio.
   c) Crítico.
   d) Muy Alto.
   e) Bajo.
8- ¿Cuál es la misión de un Equipo de Respuesta a Incidentes de Seguridad?:
   a) Notificar los incidentes a las Administraciones Públicas.
   b) Es el SOC de una empresa privada.
   c) Evaluar el impacto de un incidente sobre una empresa privada.
   d) Recibir, revisar y responder a informes y actividad sobre incidentes de seguridad.
9- ¿Qué Nivel de Peligrosidad tiene el "Discurso de Odio"?
   a) Medio.
   b) Muy Alto.
   c) Bajo.
   d) Alto.
   e) Crítico.
10- ¿Qué Nivel de Peligrosidad tiene el "Contenido Sexual o Violento"?
   a) Crítico.
   b) Muy Alto.
   c) Medio.
   d) Alto.
   e) Bajo.

TEST II

1- ¿Qué Nivel de Peligrosidad tiene el "Phishing"?
   a) Crítico.
   b) Muy Alto.
   c) Alto.
   d) Medio.
   e) Bajo.
2- ¿Qué Nivel de Peligrosidad tiene el "Spam"?
   a) Muy Alto.
   b) Crítico.
   c) Bajo.
   d) Alto.
   e) Medio.
3- ¿Qué Nivel de Peligrosidad tiene el "Uso No Autorizado de Recursos"?
   a) Bajo.
   b) Muy Alto.
   c) Crítico.
   d) Alto.
   e) Medio.
4- ¿Qué Nivel de Peligrosidad tiene la "Intrusión o Intento de Intrusión"?
   a) Crítico.
   b) Alto.
   c) Bajo.
   d) Muy Alto.
   e) Medio.
5- ¿Qué Nivel de Peligrosidad tiene la "Ingeniería Social"?
   a) Bajo.
   b) Medio.
   c) Crítico.
   d) Muy Alto.
   e) Alto.
6- ¿Qué Nivel de Peligrosidad tiene la "Denegación de Servicio"?
   a) Bajo.

b) Muy Alto.
c) Medio.
d) Alto.
e) Crítico.

7- ¿Qué organismo edita y mantiene la Guía Nacional de Notificación y Gestión de Ciberincidentes?:
a) El INCIBE.
b) El Consejo Nacional de Ciberseguridad.
c) El Esquema Nacional de Seguridad.

8- Si un incidente afecta a una infraestructura crítica, se debe notificar a:
a) ESP-DEF-CERT.
b) CCN-CERT.
c) CNPIC.
d) INCIBE-CERT.

9- ¿Qué Nivel de Peligrosidad tiene la "Distribución y Configuración de Malware"?
a) Bajo.
b) Critico.
c) Medio.
d) Alto.
e) Muy Alto.

10- Señalar cuál de los siguientes incidentes tiene un nivel de peligrosidad Critico:
a) Infección por Código Dañino.
b) Amenaza Persistente Avanzada.
c) Scanning o Sniffing.
d) Revelación de Información.

Respuesta
Autoevaluación I: c)
Autoevaluación II: a) c)
Autoevaluación III: c)
Autoevaluación IV: c)
Autoevaluación V: a)
TEST I 9/10: 1), 2), 3), 4), 5), 6), 7), 8), 9), 10)
TEST II 10/10: 1), 2), 3), 4), 5), 6), 7), 8), 9), 10)

Blue Team (Let's defend)
El equipo azul (blue team) en ciberseguridad se refiere a un equipo dedicado a la defensa de una organización contra posibles amenazas de seguridad cibernética. El blue team lleva a cabo actividades como la detección y respuesta a incidentes, la evaluación continua de la seguridad y la implementación de medidas de seguridad proactivas para prevenir futuros ataques. El objetivo del blue team es proteger los sistemas y datos de la organización, manteniendo un alto nivel de seguridad y disponibilidad.

La web "https://letsdefend.io/" es una plataforma que ofrece soluciones y servicios en el ámbito de la ciberseguridad, como la formación y el entrenamiento en habilidades técnicas para la defensa cibernética, así como pruebas de penetración y evaluaciones de seguridad para empresas y organizaciones.

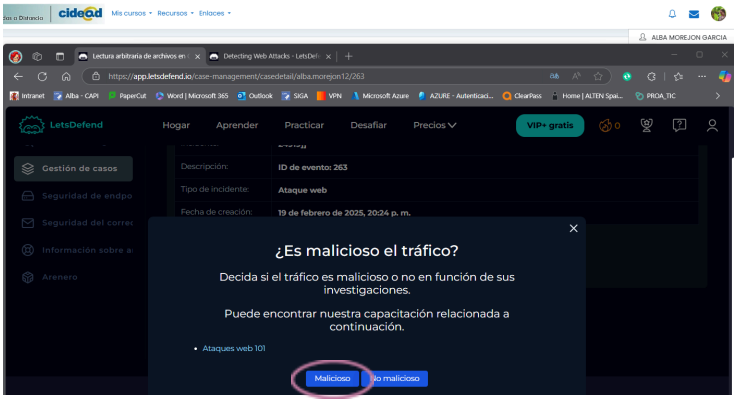
Introducción: Descripción del caso práctico.
"Eres parte del equipo de ciberseguridad de la sede ministerial de Justicia en Andalucía. Todo parece estar funcionando de manera normal hasta que un día recibes una llamada urgente del responsable del departamento de TI. Algo va mal en los sistemas y hay un posible ciberataque en curso.
Rápidamente te diriges a la oficina y comienzas a investigar. Descubres a través del SIEM que existe un patrón de actividad sospechosa que indica un posible ataque. Inmediatamente, comienzas a investigar con tu equipo y a profundizar en los detalles del incidente. Descubrís que se ha producido una brecha en la seguridad y que los datos confidenciales están en riesgo…"

La plataforma "https://letsdefend.io" tiene una sección de simulación de productos SIEM como IBM Qradar, ArcSight ESM, etc. Como analista de SOC, una de tus tareas principales puede ser monitorear y analizar las alertas mostradas en un SIEM.
Elige una de las actividades sospechosas de la sección "Practice - Monitoring", simulando que puede ser uno de los posibles ataques recibidos en el anterior relato ficticio. Para este "evento" elegido se debe realizar un análisis (write-up) con el resultado de la investigación realizada.
Además, se debe indicar las distintas comunicaciones que deberían realizarse en caso de confirmarse un incidente de ciberseguridad en los sistemas.

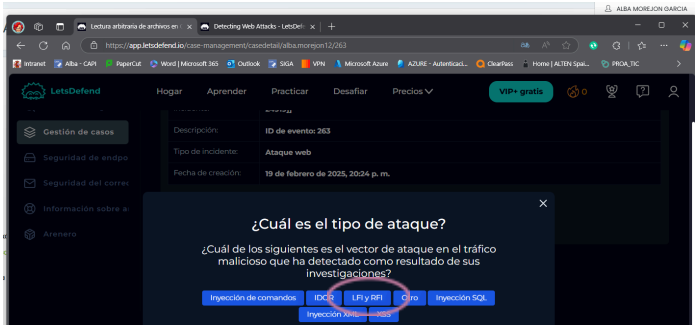
Apartado 1: Write-up de un incidente.
Elige un incidente con categoría “High” o “Critical” del “SIEM” de “Letsfend.io” y redacta un documento con la investigación realizada y con los resultados obtenidos.
He seleccionado la siguiente incidencia:
High Web Attack, EventID: 263 - [SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919]]

Write-Up: explicación del proceso de investigación que llevas a cabo para determinar si la alerta se trata de un falso positivo o si realmente es un incidente.
El incidente elegido es un ataque web en el que alguien intentó acceder a un archivo importante llamado /etc/passwd, que contiene información sobre los usuarios del sistema. El atacante logró navegar a través de las carpetas del sistema con alguna herramienta, y el sistema no bloqueó el intento, por lo que pudo acceder a dicho archivo.
Al investigar, se identificó un comportamiento sospechoso en el tráfico. Se reconoció un intento de acceso a un archivo sensible (/etc/passwd) desde la dirección IP 203.160.68.12 con un navegador Firefox utilizando un sistema operativo MacOS, lo que sugiere que el ataque vino desde fuera de la red de la empresa. El host afectado lleva el nombre de CP-Sark-Gateway-01 y la dirección IP 172.16.20.146.
La alerta se disparó debido a un patrón de explotación de una vulnerabilidad conocida (CVE-2024-24919), que permite a los atacantes acceder a archivos del sistema, debido a un problema de seguridad en el sistema.
El ataque fue exitoso y no se trata de un falso positivo, esto significa que un atacante pudo acceder al archivo sensible y no fue un error del sistema.
A continuación, realizaremos el playbook que nos ofrece la página “letsdefend.io” sobre este incidente, en el que seguiremos una guía o modo de proceder para un tipo de ataque genérico, donde responderemos a diferentes preguntas para recopilar los datos importantes.

1- ¿Es malicioso el tráfico? Decida si el tráfico es malicioso o no en función de sus investigaciones.
La solicitud HTTP contiene un intento de acceder al archivo /etc/password. Coincide con un patrón característico de un intento de explotación de la vulnerabilidad (Zero Day) CVE-2024-24919 para la lectura de archivos restringidos. La solicitud HTTP POST seguramente contenga información maliciosa para hackear el acceso, junto con la dirección IP externa indican que es un comportamiento sospechoso.
Respuesta: Malicioso



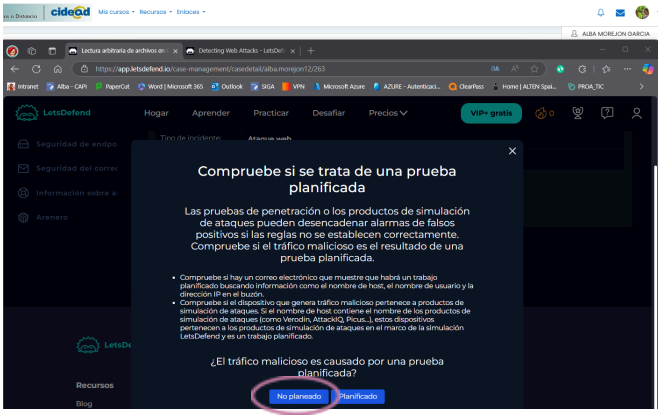
2- ¿Cuál es el tipo de ataque? ¿Cuál de los siguientes es el vector de ataque en el tráfico malicioso que ha detectado como resultado de sus investigaciones?
LFI (Local file Inclusion), permite a un atacante incluir archivos en un servidor web manipulando parámetros en las solicitudes HTTP. El tipo de ataque es una Lectura Arbitraria de Archivos (LFI) , el vector de ataque en el tráfico detectado coincide con el descrito, el atacante accedió a la carpeta sensible utilizando una técnica de transversal de archivos.
Respuesta: LFI y RFI



3- Compruebe si se trata de una prueba planificada. ¿El tráfico malicioso es causado por una prueba planificada?

No se encontró ningún correo electrónico que indique un trabajo planificado relacionado con la dirección 203.160.68.12 o el host CP-Sark-Gateway-01, que tampoco coincide con ningún nombre que coincida con los productos de simulación de ataques.

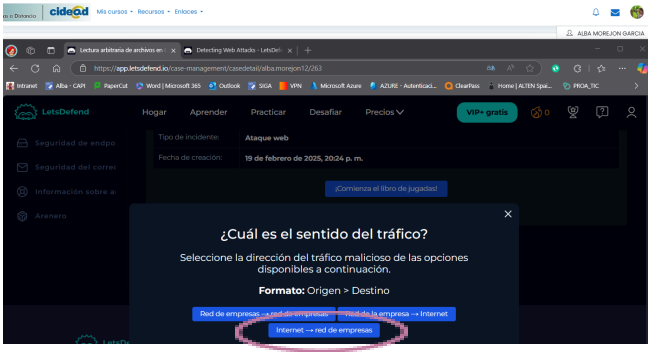
Respuesta: No planificado



4- ¿Cuál es el sentido del tráfico? Seleccione la dirección del tráfico malicioso de las opciones disponibles a continuación. Formato: Origen > Destino

El tráfico se origina desde una dirección de origen externo a la red (Internet) y la dirección de destino pertenece a la red interna de la empresa.

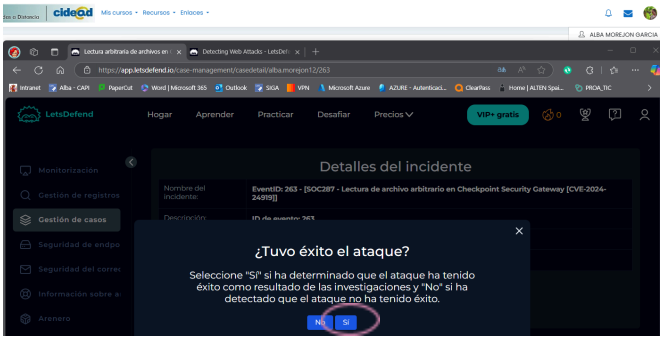
Respuesta: Internet -> Red de empresas



5- ¿Tuvo éxito el ataque? Seleccione "Sí" si ha determinado que el ataque ha tenido éxito como resultado de las investigaciones y "No" si ha detectado que el ataque no ha tenido éxito.

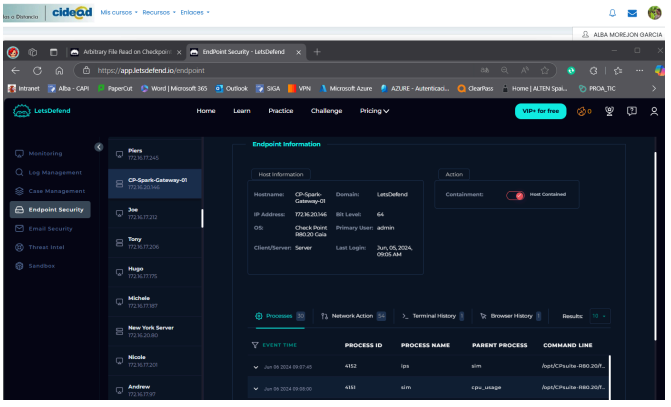
La investigación reveló que el atacante logró acceder al archivo /etc/passwd, lo que indica que la vulnerabilidad fue explotada con éxito. Se hizo un acceso no autorizado a información sensible.

Respuesta: Sí



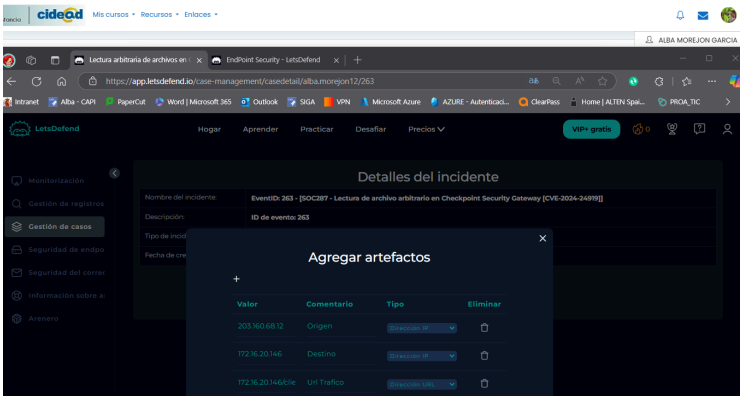
En el apartado de “Endpoint Security” encontramos el nombre del host involucrado en este incidente: “CP-Sark-Gateway-01” y siguiendo las indicaciones activamos el “Host contained”.

En esta página podemos visualizar los procesos y las acciones en la red.



6- Agregar artefactos

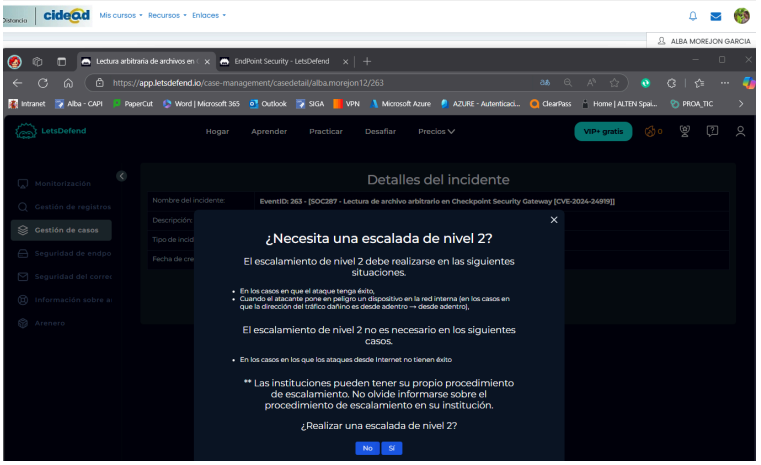
Continuamos con el análisis y añadimos los artefactos identificados, la dirección IP origen, la dirección IP destino y la URL de solicitud.



7- ¿Necesita una escalada de nivel 2?

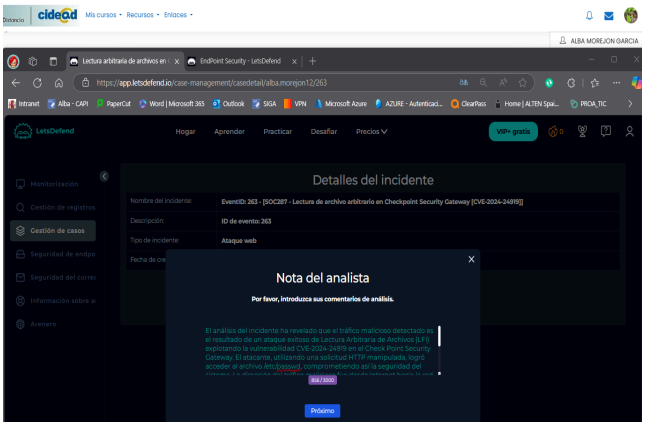
El ataque tuvo éxito y un dispositivo de la red interna se ha visto afectado.

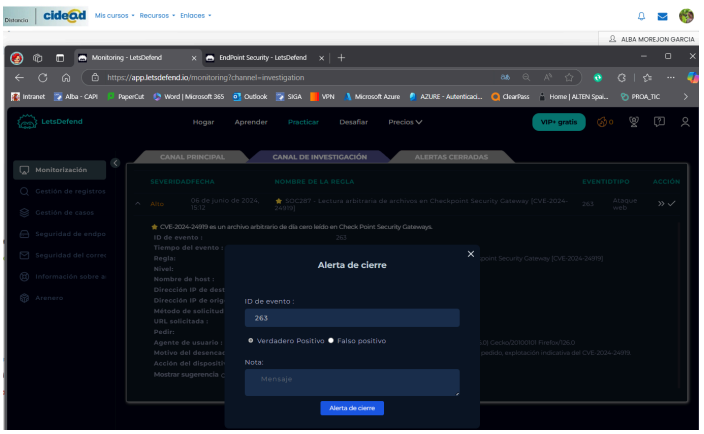
Respuesta: Sí



8- Nota del analista

El análisis del incidente ha revelado que el tráfico malicioso detectado es el resultado de un ataque exitoso de Lectura Arbitraria de Archivos (LFI) explotando la vulnerabilidad CVE-2024-24919 en el Check Point Security Gateway. El atacante, utilizando una solicitud HTTP manipulada, logró acceder al archivo /etc/passwd, comprometiendo la seguridad del sistema. La dirección del tráfico malicioso fue desde Internet hacia la red interna, lo que justifica una escalada de nivel 2 para una respuesta más detallada y efectiva. Se han identificado y documentado los artefactos relevantes, y se ha confirmado que el tráfico no es parte de una prueba planificada. Es importante aplicar medidas de mitigación y mantener una comunicación clara con todas las partes involucradas para minimizar el impacto y prevenir futuros incidentes similares.

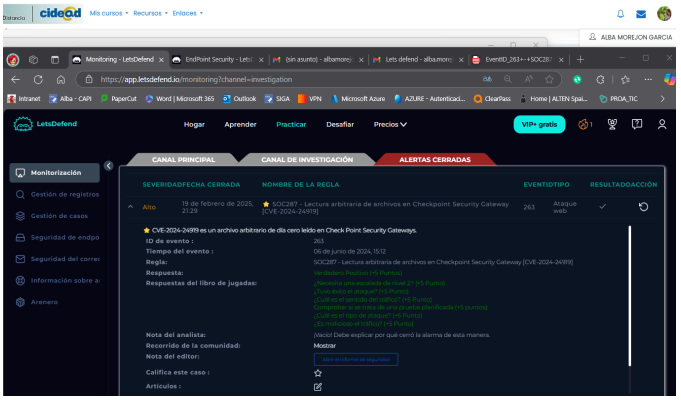


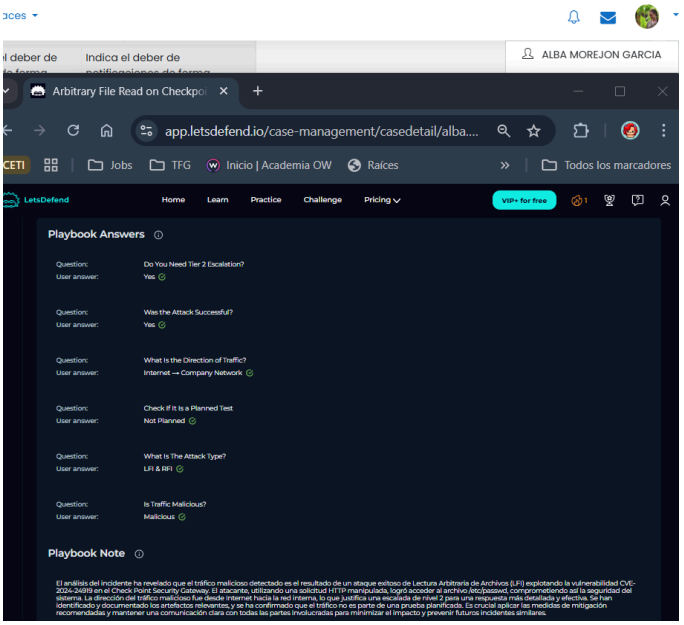


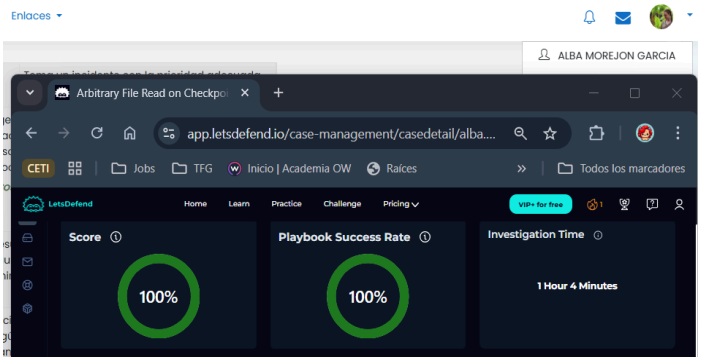
9- Alerta de cierre

Declaramos que ha sido un verdadero positivo

Resultado:







Apartado 2: Comunicaciones de incidentes.
Según el caso práctico planteado con datos ficticios iniciales y del incidente seleccionado se debe realizar la documentación de la notificación y gestión del incidente. Además, se puede añadir toda la información ficticia que se considere necesaria para poder determinar de forma concreta el ciber incidente.
Para la realización de los siguientes apartados se puede consultar la "Guía Nacional de Notificación y Gestión de Ciber Incidentes" en sus apartados 5 y 6.

Deberás efectuar la siguiente tarea:
1. Realizar una clasificación justificada del incidente según la taxonomía oficial.
Categoría del incidente: Ataque web
Subcategoría: Lectura arbitraria de archivos (LFI)
El incidente se clasifica como un ataque web debido a la explotación de la vulnerabilidad CVE-2024-24919 que permite la lectura arbitraria de archivos en los Checkpoint Security Gateways. El atacante utilizó una solicitud HTTP manipulada para acceder al archivo sensible /ect/passwd, comprometiendo la seguridad del sistema.

2. Determinar el nivel de peligrosidad del incidente.
Nivel de peligrosidad: Alto
La vulnerabilidad a la que hemos hecho referencia, es una vulnerabilidad Day Zero que permite a un atacante leer archivos en el sistema afectado. Esto puede llevar a la exposición de información sensible y potencialmente permitir movimientos laterales y escalada de privilegios dentro de la red. La naturaleza crítica del archivo accedido, que contiene información sensible sobre los usuarios del sistema y el hecho de que haya sido permitido y no bloqueado por el sistema, aumenta la peligrosidad del incidente. La explotación de esta vulnerabilidad compromete la integridad y confidencialidad de los datos

3. Determinar el nivel de impacto del ciber incidente.
Nivel de impacto: Crítico
La explotación de la vulnerabilidad CVE-2024-24919 puede comprometer datos confidenciales y afectar la integridad y confidencialidad de la información en los sistemas (sede ministerial de Justicia en Andalucía). Además, puede tener repercusiones legales y de reputación significativas. La capacidad del atacante para acceder al archivo sugiere que la seguridad del sistema ha sido gravemente comprometida.

4. Indicar la posible obligación de notificar al CSIRT correspondiente.
Obligación de notificación: si
Según la Guía Nacional de Notificación y Gestión de Ciberincidentes, los incidentes que comprometen la seguridad de la información en entidades públicas deben ser notificados al CSIRT correspondiente. Dado el nivel de peligrosidad y el impacto de este incidente, es obligatorio notificar al INCIBE-CERT (Instituto Nacional de Ciberseguridad de España) para coordinar la respuesta y la mitigación, ya que el incidente involucra una brecha de seguridad significativo que afecta a una entidad pública.

5. Rellenar una tabla con la información que se enviaría al CSIRT.

CAMPO	DETALLE
Fecha y hora del incidente	06 de junio de 2024, 03:12 pm
Nombre del incidente	Lectura arbitraria de archivos en Checkpoint Security Gateway (CVE-2024-24919)
Descripción del incidente	Explotación de una vulnerabilidad de día cero que permite la lectura arbitraria de los archivos, accediendo al archivo /etc/passwd mediante una solicitud HTTP POST con payload malicioso
Nivel de peligrosidad	Alto
Nivel de impacto	Crítico
IP de origen	203.160. 68,12
IP de destino	172.16.20.146
Nombre del host	CP-Sark-Gateway-01
Modo de ataque	Solicitud HTTP POST con payload malicioso para leer el archivo /etc/password
Impacto	Compromiso de datos confidenciales y posible escalada de privilegios
Medidas tomadas	Contención del host, análisis de artefactos, escalada a nivel 2, aplicación del hotfix proporcionado por Check Point, monitoreo continuo del sistema…
Contacto	Nombre del responsable de seguridad, email y teléfono

6. Explicar cuantas notificaciones son requeridas y con qué frecuencia. (No hay que crear las notificaciones)

Número de notificaciones requeridas: Múltiples, para asegurar una gestión efectiva del incidente.

Frecuencia:

- Inicial: notificación inmediata al detectar y confirmar el incidente. Se deben proporcionar detalles clave sobre el incidente, para alertar al CSIRT y coordinar una respuesta rápida.
- Actualización: notificaciones periódicas cada 24 horas o según el progreso del incidente, hasta la resolución completa. Deben incluir cualquier cambio significativo en el estado del incidente, nuevas evidencias, medidas adicionales y el progreso para la mitigación del ataque. La frecuencia de las actualizaciones se ajustará según las indicaciones del CSIRT y la gravedad del incidente.
- Final: notificación de cierre, una vez que el incidente ha sido mitigado y resuelto. Se debe resumir todas las acciones tomadas, los resultados obtenidos y cualquier aportación útil para futuros incidentes (lecciones aprendidas).

Este proceso de notificación asegura que todas las partes involucradas estén informadas y que se tomen las medidas adecuadas para proteger la seguridad de la red y los datos de la organización.

7. Rellenar la información con el estado del cierre del incidente.

Estado del cierre: cerrado

El incidente se cerrará una vez que se hayan completado todas las acciones de mitigación y se haya confirmado que no hay más amenazas activas. En este caso, el incidente ha sido mitigado mediante la contención del host afectado y la implementación de medidas de seguridad adicionales (aplicación de hotfix). Se ha realizado un monitoreo exhaustivo para asegurar que no haya más intentos de explotación de la vulnerabilidad. Todo el proceso ha sido documentado, incluyendo las lecciones aprendidas y las recomendaciones para prevenir futuros incidentes similares. La información se ha desarrollado según las indicaciones de la Guía Nacional de Notificaciones y Gestión De Incidentes.