Ciclo de respuesta

1.1. Clasifica los siguientes eventos en precursores o indicadores

# Evento Precursor o Indicador

### **1. Clasificación de eventos en precursores o indicadores**

1. **Aparición de interlocutores desconocidos o que no deberían estar en la conversación (CC y CCO en hilos de email) - Indicador**
   * **Razonamiento:** Este evento sugiere que alguien no autorizado está monitoreando o participando en la conversación, indicando un posible compromiso de seguridad.
2. **Identificación de un amplio número de conexiones provenientes de una misma máquina de la organización hacia otros sistemas de la misma - Indicador**
   * **Razonamiento:** Este comportamiento es anómalo y puede indicar que la máquina está comprometida y siendo utilizada para escanear o atacar otros sistemas dentro de la organización.
3. **Amenazas por parte de terceros (internos o externos) - Precursor**
   * **Razonamiento:** Las amenazas son advertencias de posibles ataques futuros. Aunque no indican un compromiso actual, sí sugieren la posibilidad de futuros incidentes.
4. **Recepción de correos no deseados provenientes de dominios no identificados o de escasa reputación en respuesta a hilos de conversación legítimos ya existentes - Indicador**
   * **Razonamiento:** Este evento sugiere que los atacantes tienen acceso a los hilos de conversación legítimos y están intentando intervenir, lo que indica un compromiso activo.
5. **Cambios en la configuración de las máquinas que puedan permitir el acceso de malware, como detectar el firewall deshabilitado - Indicador**
   * **Razonamiento:** Cambios no autorizados en la configuración de seguridad indican que las máquinas pueden haber sido comprometidas y preparadas para la instalación de malware.
6. **Identificación de información confidencial de la organización en medios externos (Deep web, redes sociales, webs públicas, medios de comunicación, etc.) - Indicador**
   * **Razonamiento:** La aparición de información confidencial en lugares públicos o la deep web indica que ha habido una fuga de datos.
7. **Múltiples intentos de acceso fallidos a la base de datos o servidores - Indicador**
   * **Razonamiento:** Intentos repetidos y fallidos de acceso son típicos de un ataque de fuerza bruta o intentos de acceso no autorizado, indicando un posible ataque en curso.
8. **Notificación de usuarios por identificación de la misma extensión inusual en varios ficheros ya existentes previamente en el equipo - Indicador**
   * **Razonamiento:** La aparición de extensiones inusuales puede ser una señal de que los archivos han sido manipulados o afectados por malware.
9. **Tráfico de red elevado relacionado con servicios de mensajería electrónica o dominios de almacenamiento en la nube - Indicador**
   * **Razonamiento:** Un incremento anómalo en el tráfico de red hacia ciertos servicios puede indicar actividades maliciosas como exfiltración de datos.
10. **Recepción de mensajes inesperados que instan a cambiar o revelar las credenciales de plataformas corporativas - Precursor**
    * **Razonamiento:** Este tipo de mensajes son típicos de intentos de phishing y sugieren que los atacantes están preparando un intento de obtener acceso a las credenciales.
11. **Presencia de dispositivos y equipos no corporativos en la red - Precursor**
    * **Razonamiento:** La presencia de dispositivos no autorizados puede indicar una vulnerabilidad en las políticas de seguridad que podría ser explotada en el futuro.
12. **Identificación de un gran número de ficheros con fecha de última modificación simultánea y de madrugada - Indicador**
    * **Razonamiento:** Modificaciones masivas y simultáneas de archivos son una señal de actividad sospechosa, como un ataque automatizado o una infección de malware.
13. **Degradación de la experiencia de usuario (incremento en el tiempo de respuesta de los servidores, ralentización de la navegación, etc.) - Indicador**
    * **Razonamiento:** La degradación del rendimiento puede ser un signo de un ataque en curso, como un ataque de denegación de servicio o la actividad de malware que consume recursos.
14. **Existencia de campañas de denegación de servicios activas que afectan a otras compañías del sector - Precursor**
    * **Razonamiento:** La existencia de campañas DDoS en el sector sugiere que la organización podría ser un próximo objetivo, aunque no se haya observado un ataque aún.
15. **Alerta en los sistemas de monitorización de la organización por la ejecución simultánea de un proceso con el mismo nombre en varias máquinas del mismo segmento de red y ubicado en rutas temporales (como C:\Users\Administrador\AppData\Local\Temp) - Indicador**
    * **Razonamiento:** La ejecución simultánea de un proceso inusual puede indicar la propagación de malware o un ataque coordinado dentro de la red.

1.1. [DDoS] Completa la siguiente tabla con eventos que permitirían

identificar que se podría estar produciendo un potencial

incidente de denegación de servicios.

# Evento

**1- Incremento significativo en el tráfico de red hacia los servidores públicos.**

* **Razonamiento:** Un aumento abrupto del tráfico es un indicador común de un ataque DDoS, ya que los atacantes inundan el servidor con solicitudes.

**2- Reducción notable en el rendimiento de los servicios web.**

* **Razonamiento:** Un ataque DDoS puede consumir recursos del servidor, causando lentitud o inoperatividad de los servicios.

**3-Recepción de alertas de sobrecarga en dispositivos de red como routers y firewalls.**

* **Razonamiento:** Los dispositivos de red pueden detectar y alertar sobre tráfico anormalmente alto, indicando un posible DDoS.

**4-Identificación de múltiples solicitudes desde una gran cantidad de direcciones IP.**

* **Razonamiento:** Los ataques DDoS generalmente utilizan múltiples IPs para inundar el objetivo, haciéndolo difícil de bloquear.

**5-Reportes de indisponibilidad o lentitud por parte de los usuarios.**

* **Razonamiento:** Los usuarios pueden experimentar problemas de acceso cuando los servidores están siendo atacados por DDoS.

**6-Detención del tráfico en segmentos críticos de la red.**

* **Razonamiento:** Un ataque DDoS puede ser tan severo que detiene completamente el tráfico en ciertas partes de la red.

**7-Log de eventos de denegación de servicio en sistemas de monitoreo.**

* **Razonamiento:** Los sistemas de monitoreo pueden detectar patrones típicos de DDoS y registrar estos eventos.

**8-Alertas de sobrecarga en el servidor de aplicaciones.**

* **Razonamiento:** Los servidores de aplicaciones bajo ataque DDoS mostrarán signos de sobrecarga debido a la cantidad de solicitudes procesadas.

1.2. [Defacement] Completa la siguiente tabla con eventos que

permitirían identificar que se podría estar produciendo un

potencial incidente de defacement

# Evento

**1-Modificación no autorizada del contenido visible en el sitio web.**

* **Razonamiento:** La alteración del contenido web es el principal síntoma de un ataque de defacement.

**2-Reportes de usuarios sobre contenido inapropiado o mensajes no esperados.**

* **Razonamiento:** Los usuarios pueden notar y reportar cambios inesperados, como mensajes ofensivos o imágenes no autorizadas.

**3-Aparición de mensajes de hackeo o defacement en la página principal del sitio.**

* **Razonamiento:** Los atacantes a menudo dejan mensajes para anunciar el defacement, lo cual es una señal clara del ataque.

**4-Cambios en los archivos de configuración del servidor web.**

* **Razonamiento:** Los atacantes pueden modificar archivos de configuración para redirigir el contenido o mantener el acceso.

1.3. [Ransomware] Completa la siguiente tabla con eventos que

permitirían identificar que se podría estar produciendo un

potencial incidente de infección por ransomware

# Evento

**1-Cifrado de archivos y aparición de notas de rescate.**

* **Razonamiento:** El ransomware cifra los archivos y deja una nota solicitando un rescate para la recuperación.

**2-Bloqueo de acceso a sistemas críticos con mensajes solicitando pago.**

* **Razonamiento:** El ransomware puede impedir el acceso a sistemas completos hasta que se pague el rescate.

**3-Detección de actividad anómala en los logs de acceso.**

* **Razonamiento:** Los registros pueden mostrar comportamientos anómalos que indican la presencia y actividad del ransomware.

**4-Incremento de los tiempos de respuesta en el acceso a datos.**

* **Razonamiento:** El cifrado de archivos puede ralentizar el acceso a los datos, lo que puede ser un signo de un ataque en curso.

**5-Alerta de actividad sospechosa por parte de soluciones de seguridad.**

* **Razonamiento:** Los sistemas de seguridad pueden detectar y alertar sobre la actividad relacionada con el ransomware antes de que se complete el cifrado.

Página 5 de 12

1.4. [Fraude en transferencia] Completa la siguiente tabla con

eventos que permitirían identificar que se podría estar

produciendo un potencial incidente de fraude en transferencia

# Evento

1. **Cambios sospechosos en las instrucciones de pago recibidas por correo.**
   * **Razonamiento:** Las solicitudes de cambiar las instrucciones de pago pueden ser indicativos de un intento de fraude.
2. **Solicitudes urgentes y fuera de lo común para realizar transferencias.**
   * **Razonamiento:** Los estafadores a menudo crean un sentido de urgencia para que las víctimas no verifiquen la autenticidad de las solicitudes.
3. **Notificación de pagos a cuentas no habituales.**
   * **Razonamiento:** El envío de fondos a cuentas desconocidas o no habituales puede indicar un fraude en curso.
4. **Aparición de correos con remitentes falsificados.**
   * **Razonamiento:** Los correos de suplantación de identidad a menudo contienen direcciones de remitente que parecen legítimas, pero no lo son.
5. **Alertas de transacciones no reconocidas por los sistemas bancarios.**
   * **Razonamiento:** Los sistemas bancarios pueden detectar y alertar sobre transacciones inusuales que podrían ser fraudulentas.

1.5. Identifica la criticidad para los siguientes incidentes con apoyo

de una matriz de categorización

Inicialmente, sin hacer uso de la matriz adjunta, identifica y argumenta qué nivel de

criticidad se considera que tendrían los siguientes escenarios:

1.1.1. Escenario #1

La constructora Ladrillo Rojo S.L., la cual dispone de unos ingresos anuales totales por

valor de 10M, notifica que todos los equipos de la organización se han visto cifrados. Según

indica poseían un total de:

15 equipos de usuario. No se realizan copias de seguridad para estos equipos.

2 servidores (1 de ellos alberga la herramienta ERP). Realizan copias de seguridad

diarias almacenadas en cloud, las cuales no se han visto afectadas.

Junto a esto, añaden que durante las semanas anteriores a dicho incidente recibieron una

fuerte campaña de spam y que los usuarios emplean sus dispositivos corporativos para el

desempeño de acciones personales, como consultas a sus cuentas bancarias.

Se indican que los correos recibidos durante esta campaña presentaban documentos

Word adjuntos y hacía referencia a proveedores de la organización, aunque el Display

Name de estos no coincidía con el correo desde el que procedían (dicho patrón resulta

similar al identificado por la campaña de distribución del malware Emotet).

Asimismo, indican que uno de los empleados afirma haber interactuado con uno de los

archivos adjuntos recibidos durante la campaña pasada. Dado que las infecciones por

Emotet suelen presentar una segunda fase en la que se lleva a cabo la descarga de otras

piezas de malware, las cuales suelen ser infostealers, podrían haberse visto afectados

datos de carácter personal.

**Criticidad: Alta**

* **Razonamiento:** Todos los equipos de usuario están cifrados y no hay copias de seguridad. La pérdida de acceso a los datos puede detener completamente las operaciones de la empresa, lo que tiene un impacto severo en la operativa y productividad.

1.1.2. Escenario #2

El bufete de abogados Senordal comunica haber realizado un pago de forma fraudulenta.

Según indica, iniciaron una conversación con uno de sus proveedores a día 29 de febrero

de 2020 en relación a una factura pendiente.

El día 3 de marzo, por parte del proveedor se le transmite que, debido a una auditoría en

curso, el pago pendiente debe de ser realizado a un número de cuenta distinto al

empleado de forma habitual para las transacciones llevadas a cabo entre ambos. Pese a

ello, el cliente indica haber procedido con el pago.

Desde el cliente se trasmite que, tras comprobar el remitente de dicho correo electrónico

en el cual se indica la modificación de los datos bancarios, identifica que el dominio de

correo no coincide con el legítimo de su proveedor.

**Criticidad: Alta**

* **Razonamiento:** Realizar un pago fraudulento puede resultar en pérdidas financieras significativas y potenciales repercusiones legales, afectando la estabilidad financiera de la organización.

Página 7 de 12

1.1.3. Escenario #3

La empresa de fabricación y distribución textil Inditox S.A., la cual obtiene una gran parte

de sus beneficios gracias a su servicio online, indica que está sufriendo una

indisponibilidad de su servicio online desde las 19:00 (actualmente son las 20:30),

impidiendo así a sus clientes el acceso a éste.

Posteriormente, esta empresa transmite que su facturación anual es de 2.628M, de los

cuales un 30% de estos depende de su servicio online, puesto que dicho servicio aporta a

la hora 90.000€. Adicionalmente, se indica que poseen de un equipo de IT y una figura de

gestión que pueden llevar a cabo las acciones que les sean indicadas.

**Criticidad: Crítica**

* **Razonamiento:** La indisponibilidad del servicio online, que representa el 30% de la facturación, tiene un impacto directo y significativo en los ingresos y la reputación de la empresa, pudiendo causar pérdidas financieras a largo plazo.

1.1.4. Escenario #4

La empresa Devilaim, que da servicio únicamente en España, indica tener sospechas sobre

una fuga de información. Dicha empresa cuenta con una facturación superior a 101M

anuales.

Desde la compañía se indica que, por parte de su equipo de IT, se ha revisado el tráfico de

salida a internet y durante dicho análisis el director de IT indica haber identificado ciertas

comunicaciones con servicios online de alojamiento de archivos desde direcciones IP

asociadas a equipos de empleados, así como un acceso recurrente por parte de un becario

a una dirección URL asociada a una clínica veterinaria que finaliza en news.php y cuya

dirección IP asociada se encuentra geolocalizada en Holanda.

Adicionalmente, se traslada que no cuentan con una política de caducidad de credenciales

para altos cargos de la organización y que la política de caducidad de credenciales para los

empleados regulares es de 6 meses. Conocen que muchos de los miembros de la empresa

emplean credenciales similares a las empleadas en el entorno laboral en sus servicios y

que no se comprueba, al realizar el cambio de claves semejanzas con credenciales

anteriores.

Junto a ello, indican que su CEO (92 años) les ha trasladado que hace unos días le llegó un

correo en inglés de DinLinke.com en el que le indicaban que había recibido un documento

y necesitaba introducir las credenciales de su cuenta para acceder a este. Finalmente,

indican que no disponen de copias de seguridad para los equipos de los empleados y que

en ellos se almacena información necesaria para el desarrollo de la operativa.

**Criticidad: Alta**

* **Razonamiento:** La sospecha de fuga de información y accesos no autorizados a datos críticos puede comprometer la integridad y confidencialidad de la información, afectando la confianza de los clientes y la reputación de la empresa.

Una vez completado el análisis cualitativo inicial de la criticidad de los distintos escenarios

presentados, verifica de forma cuantitativa la adecuación del nivel identificado empleando

la siguiente matriz de categorización:

Página 8 de 12

Formulario de triaje

v1.0.xlsx

1.6. Clasifica los siguientes eventos en la fase correspondiente de la

Cyber Kill Chain

# Evento Fase Medida de seguridad

**Enlace web a un portal falso de acceso a Google en un correo de phishing - Reconocimiento**

* **Razonamiento:** El reconocimiento implica recopilar información sobre el objetivo. Un enlace de phishing intenta obtener credenciales para acceder a sistemas de la organización.
* **Medida de seguridad:** Formación y concienciación de empleados para reconocer y reportar correos de phishing.

**Detección de varios procesos WMIC en equipos corporativos conectados al mismo segmento de red - Comando y Control**

* **Razonamiento:** El uso de WMIC en varios equipos puede indicar que un atacante está controlando las máquinas de forma remota.
* **Medida de seguridad:** Monitoreo de procesos anómalos y restringir el uso de herramientas administrativas.

**Escaneo de todos los subdominios y direcciones IP asociadas al dominio principal de la organización - Reconocimiento**

* **Razonamiento:** El escaneo de subdominios y direcciones IP es una técnica de reconocimiento para mapear la infraestructura del objetivo.
* **Medida de seguridad:** Implementar mecanismos de detección de escaneo y limitar la exposición de la infraestructura.

**Incremento en el volumen de tráfico desde el segmento de servidores ERP y de gestión hacia direcciones IP desconocidas - Exfiltración**

* **Razonamiento:** El aumento del tráfico hacia IPs desconocidas puede indicar que datos están siendo extraídos.
* **Medida de seguridad:** Monitoreo de tráfico de red, análisis de comportamiento y bloquear direcciones IP sospechosas.

**Identificación de peticiones hacia direcciones IP calificadas como C&C en horas de madrugada durante los últimos 15 días - Comando y Control**

* **Razonamiento:** Las peticiones a direcciones IP de Comando y Control indican que el atacante está gestionando el malware de forma remota.
* **Medida de seguridad:** Bloquear direcciones IP maliciosas y revisar el tráfico de red fuera del horario laboral.

**Cifrado de todos los servidores en el mismo segmento de red por medio de ransomware - Acciones en el Objetivo**

* **Razonamiento:** El cifrado de servidores es una acción final de los atacantes para extorsionar a la organización.
* **Medida de seguridad:** Implementar soluciones de backup y recuperación, y segmentar la red para limitar la propagación del ransomware.

**Borrado de todos los logs de eventos (EVTX) de los servidores y equipos corporativos donde se detectó la presencia de Trickbot - Cobertura**

* **Razonamiento:** Los atacantes borran los logs para cubrir sus huellas y evitar la detección.
* **Medida de seguridad:** Asegurar los logs y utilizar sistemas de gestión de información y eventos de seguridad (SIEM) para mantener registros centralizados e inmutables.

**Alto número de intentos de inicio de sesión con la cuenta de administrador local de madrugada y en un rango de pocos minutos - Reconocimiento**

* **Razonamiento:** Múltiples intentos de inicio de sesión pueden ser un ataque de fuerza bruta para obtener acceso no autorizado.
* **Medida de seguridad:** Implementar autenticación multifactor (MFA) y políticas de contraseñas fuertes.

**Instalación de Trickbot en todos los equipos del mismo segmento de red - Instalación**

* **Razonamiento:** La instalación de malware en múltiples equipos indica que el ataque ha progresado a la etapa de despliegue del software malicioso.
* **Medida de seguridad:** Utilizar soluciones de seguridad en endpoints y monitorear continuamente para detectar y detener la propagación de malware.

**Detección de una versión del malware Emotet en varios equipos, no identificado por el antivirus - Entrega**

* **Razonamiento:** La detección de Emotet en varios equipos indica que el malware ha sido entregado y ejecutado en la red.
* **Medida de seguridad:** Mantener el software antivirus actualizado, implementar soluciones avanzadas de detección y respuesta de endpoints (EDR).

