Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Incidentes de Ciberseguridad

UD05. Documentación y comunicación de un incidente.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

Blue Team (Let's defend)

INCIBE. Ventanillas Únicas (CC0)

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.

¿Qué te pedimos que hagas?

- ✓ **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 "letsdefend" 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. Esta sección está en "Practice - Monitoring".

  Con el uso de la plataforma de entrenamiento de "https://letsdefend.io/", elige una de las actividades sospechosas de la sección "Practise" - 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.**

  Deberás efectuar la siguiente tarea:

  - ➢ 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.

    Accedemos al sitio web de **`LetsDefend`**, y como indican desde el enunciado, vamos a seleccionar un incidente del listado que nos ofrecen desde el apartado **`Practice/Monitoring`**.

Voy a elegir para este apartado la vulnerabilidad **"Ejecución de Código Remoto Detectada en Splunk Enterprise"**.

Ya nos ofrece desde un primer momento información que nos puede ser muy útil, por lo que vamos a ir tomando nota de ella.

Rule: SOC239 - Remote Code Execution Detected in Splunk Enterprise

Level: Security Analyst

Source IP Address: 180.101.88.240

Destination IP Address: 172.16.20.13

Hostname: Splunk Enterprise

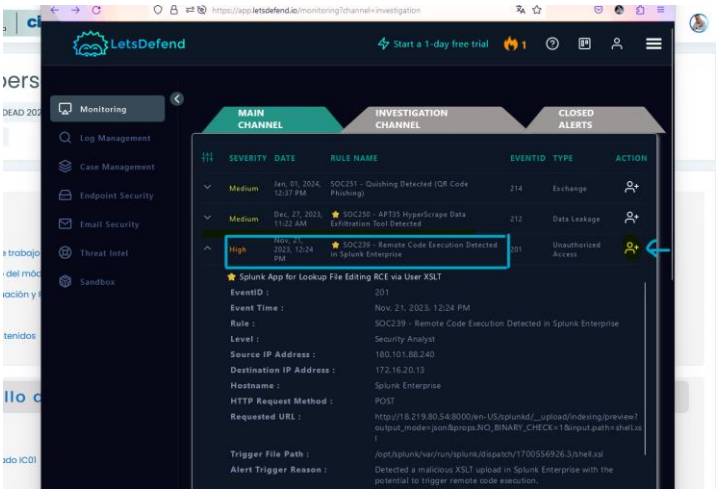
HTTP Request Method: POST

Requested URL: http://18.219.80.54:8000/en-US/splunkd/__upload/indexing/preview?output_mode=json&props.NO_BINARY_CHECK=1&input.path=shell.xsl

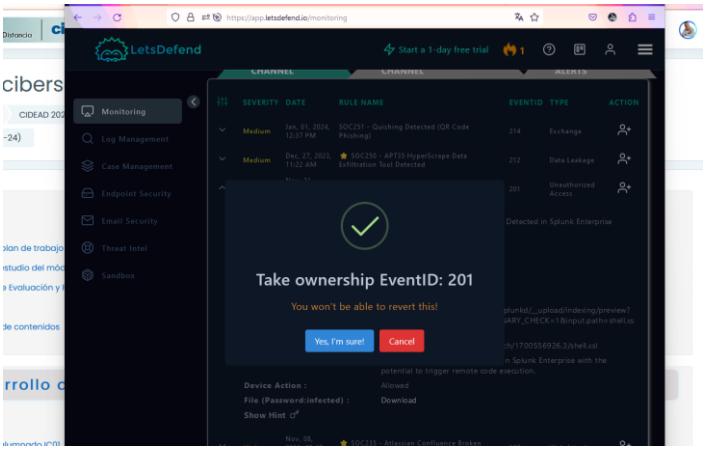
Trigger File Path: /opt/splunk/var/run/splunk/dispatch/1700556926.3/shell.xsl

Alert Trigger Reason: Detected a malicious XSLT upload in Splunk Enterprise with the potential to trigger remote code execution.

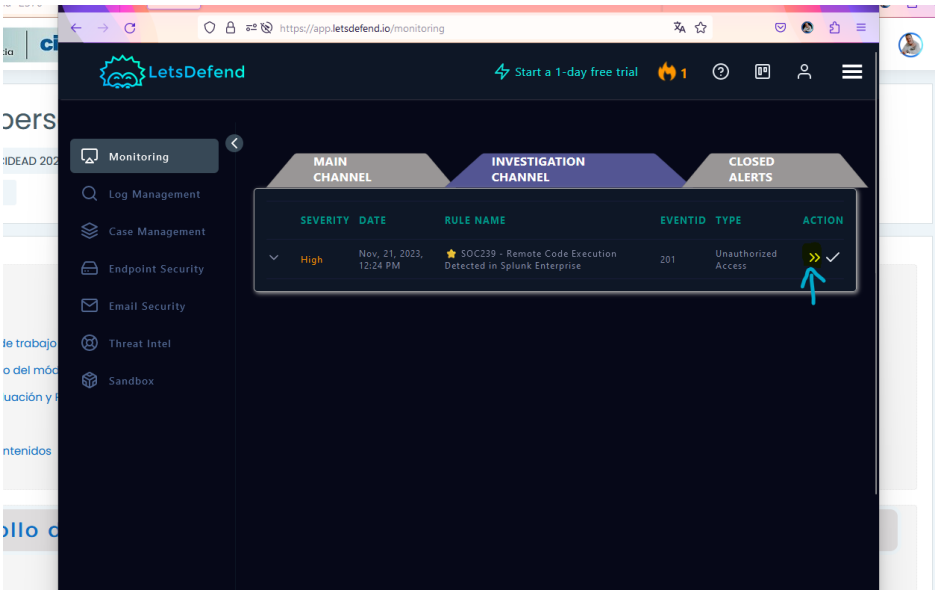
Accedemos a crear un nuevo caso pulsando sobre el icono de usuario que aparece a la derecha de la vulnerabilidad.

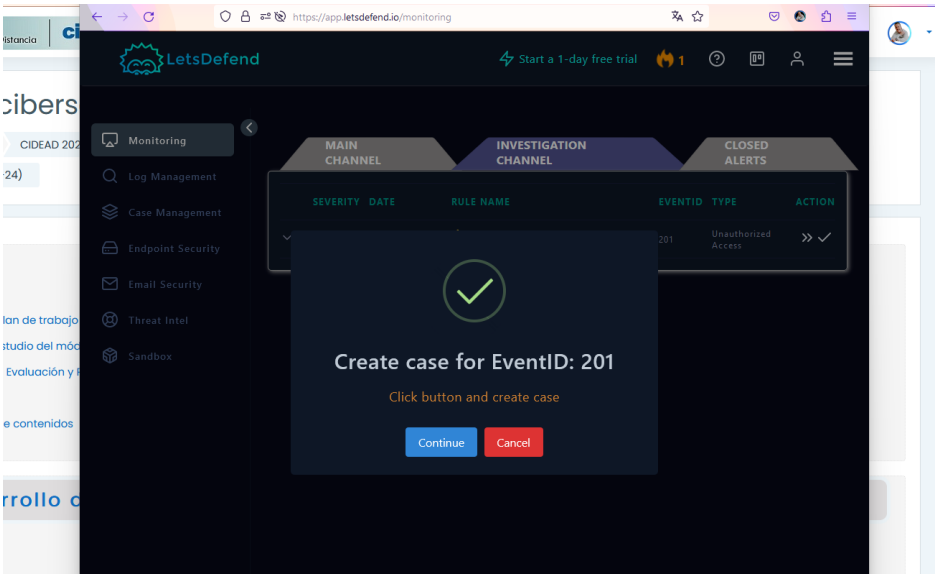


Aceptamos:

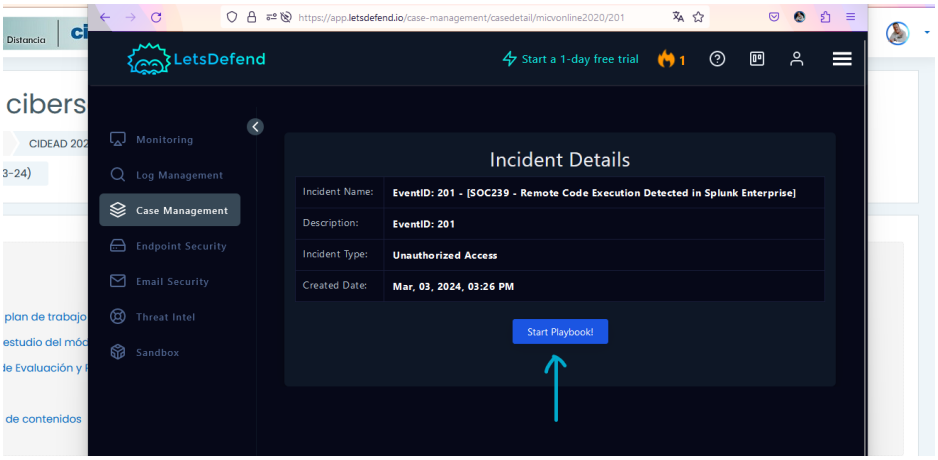


Creamos un nuevo caso de estudio:

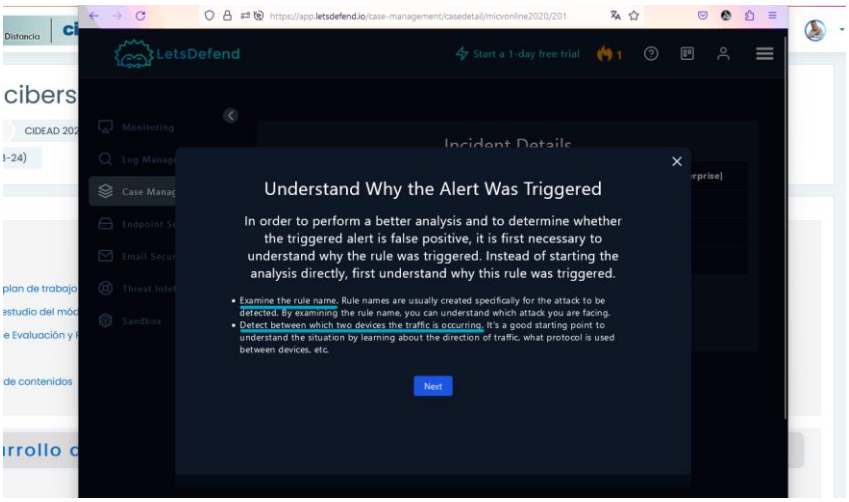




Creamos un nuevo **`Playbook`**:



El siguiente paso, nos da pistas sobre qué buscar:

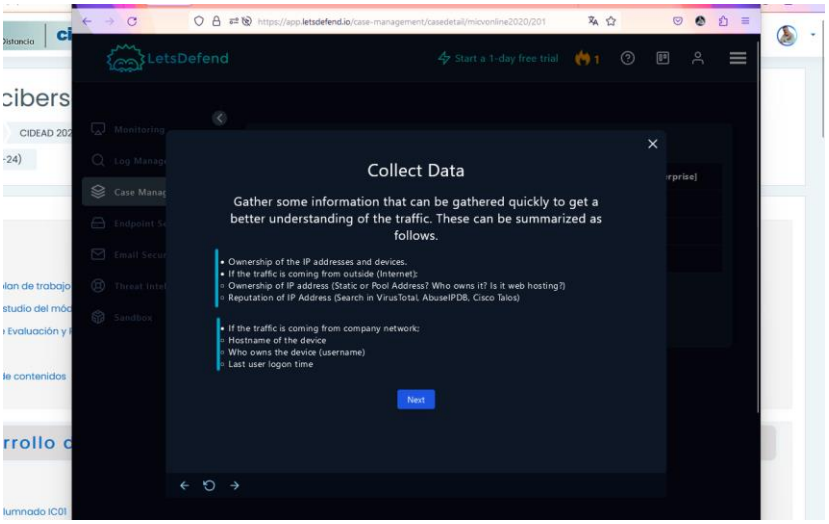


Si examinamos el nombre de la regla, podemos ver que está relacionada con la vulnerabilidad **`CVE-2023-46214`**. Estamos según su descripción ante el peligro de ejecución remota de código.

La información original también da pistas sobre los dispositivos en los que se produce el tráfico, y el resto lo recopilaremos en los siguientes pasos.

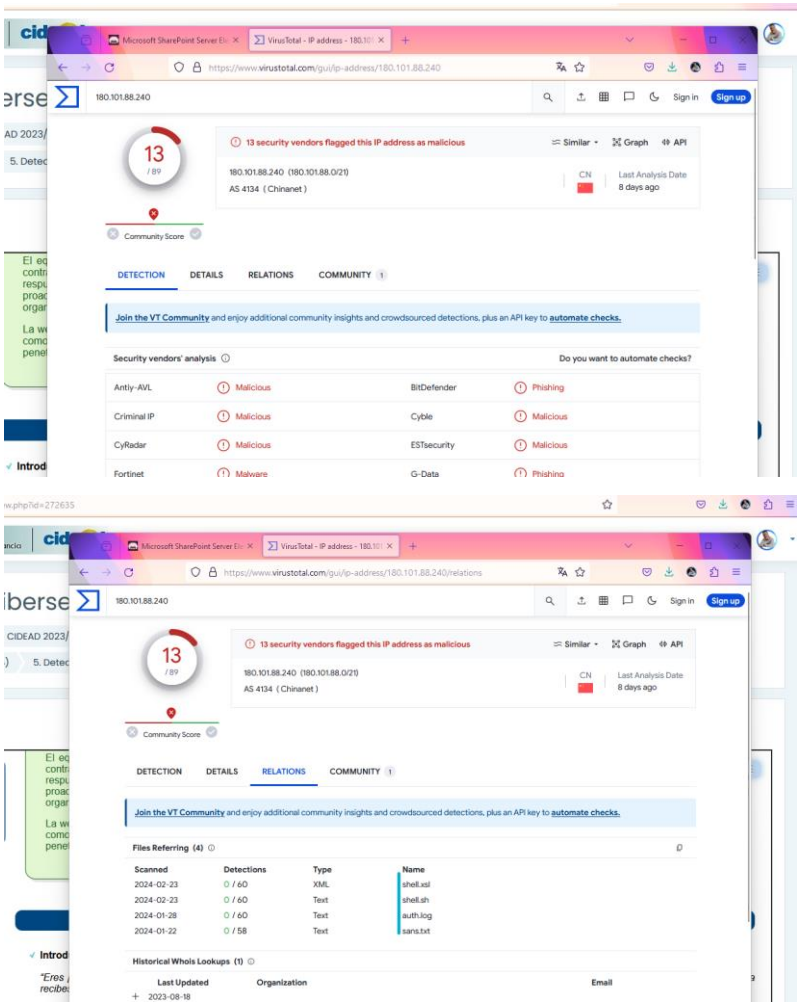
El siguiente paso nos informa sobre la recogida de determinados datos.

La mayoría, como **`IP's`**, **`hostname`** o puerto de destino ya hemos podido verlas antes, aunque podremos obtener algunos datos más revisando luego los **`logs`**.

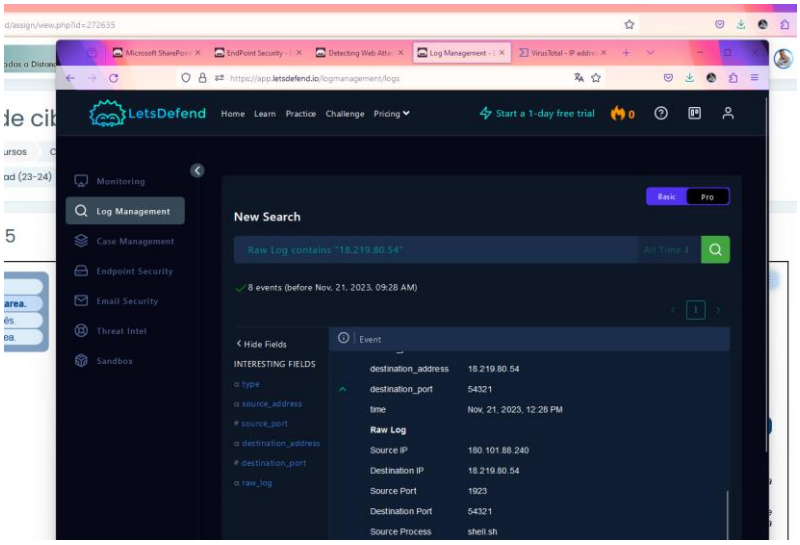


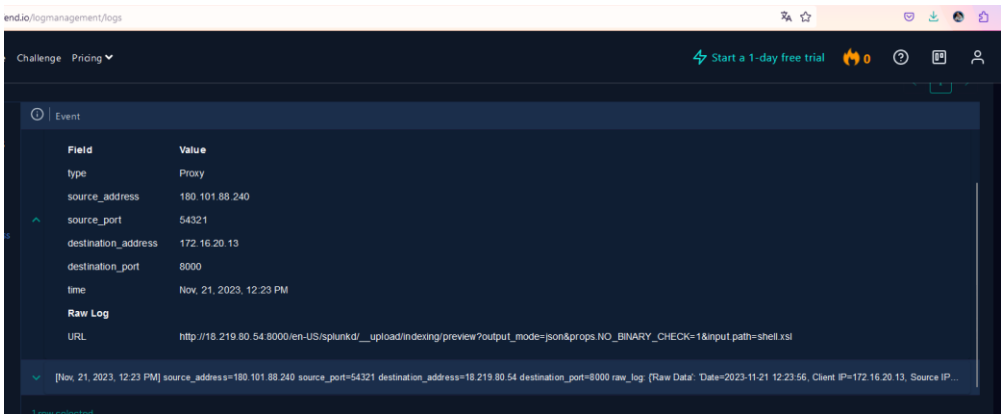
Analizando ya parte de esta información podemos ver, que, si pasamos la **IP** de origen en **Virustotal**, nos informará que es maliciosa.

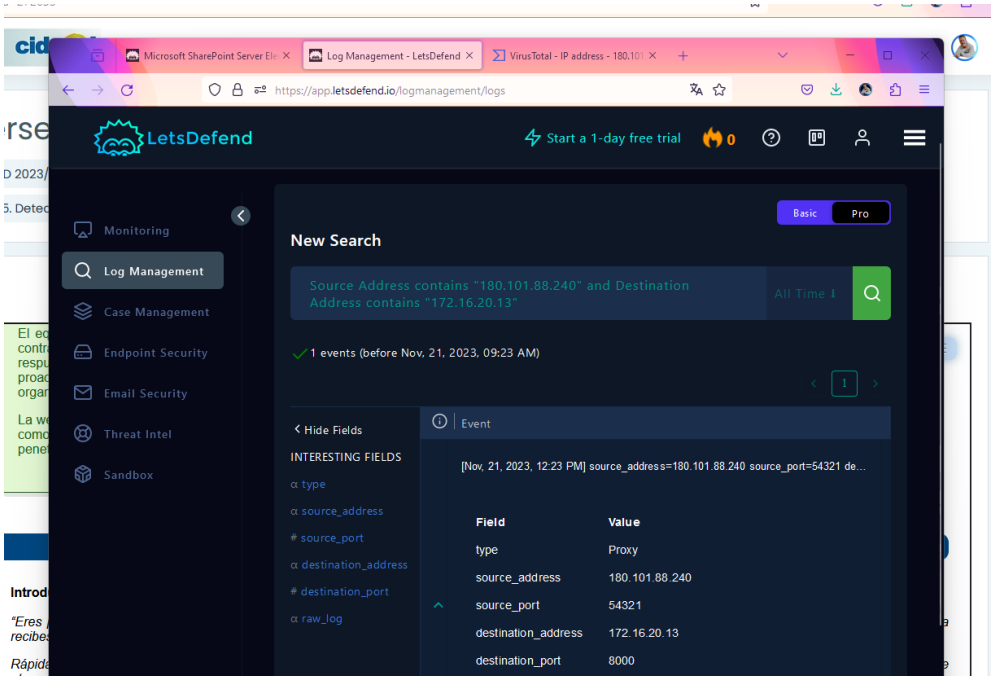
Nos muestra detalles como el origen y entidad propietaria, así como los ficheros relacionados con la actividad ilícita.



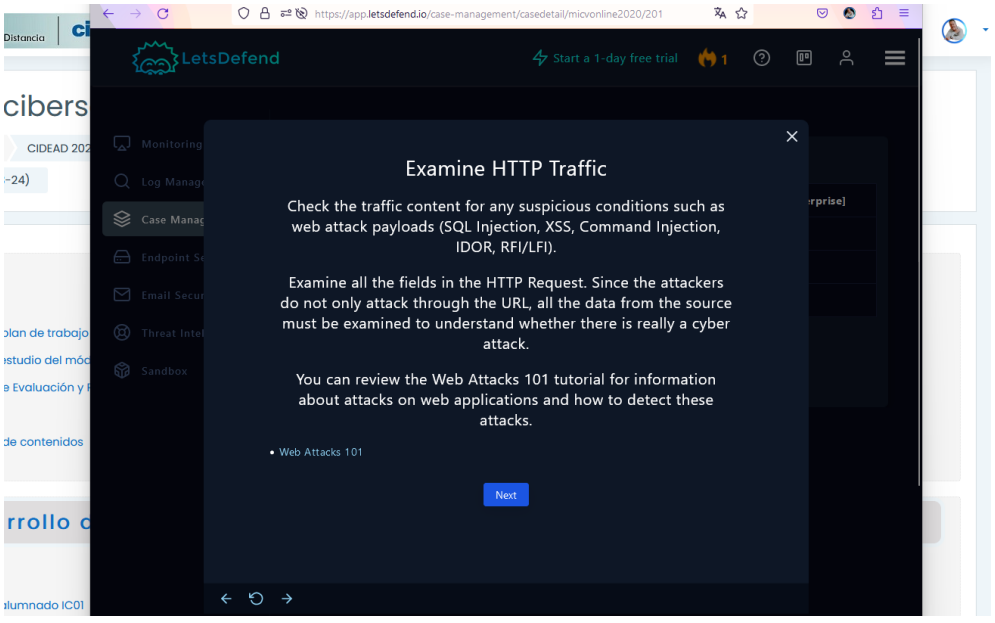
Si abrimos una segunda pestaña, podemos ir viendo más información sobre los registros.



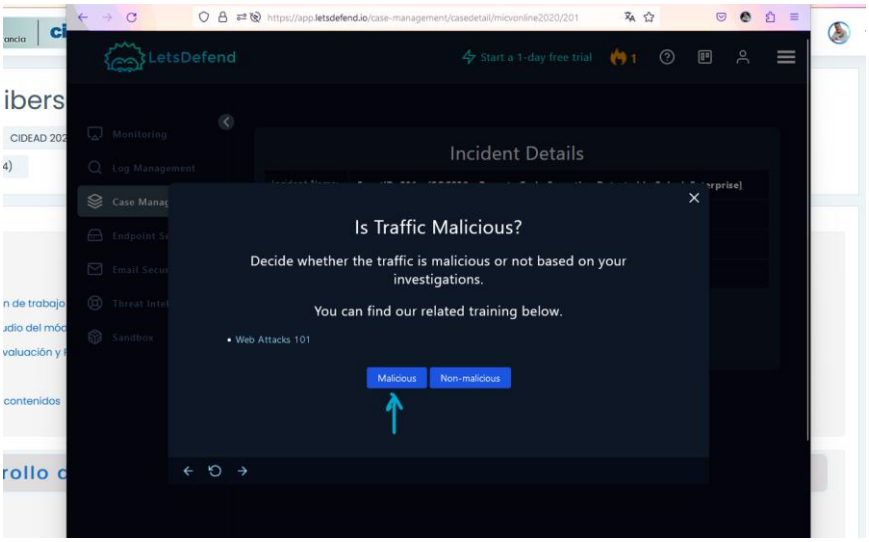




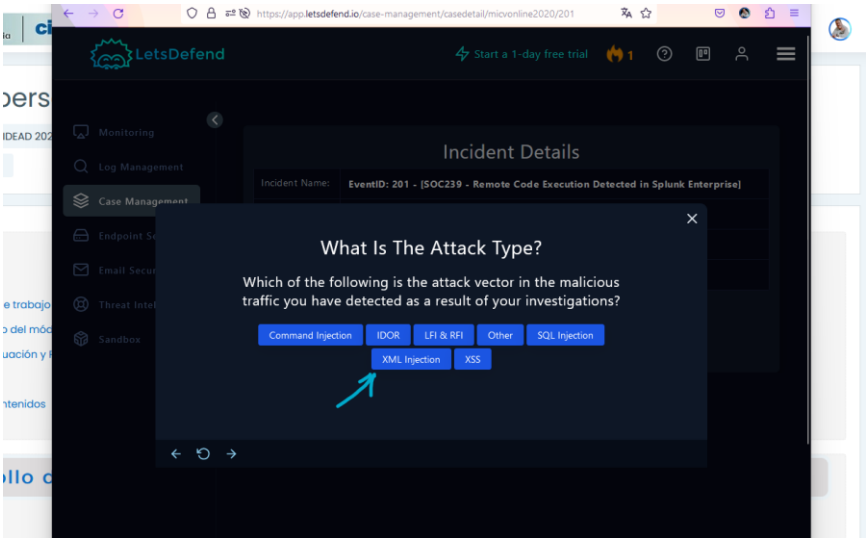
Tras recopilar esos datos, proseguimos con los pasos en la ventana principal:



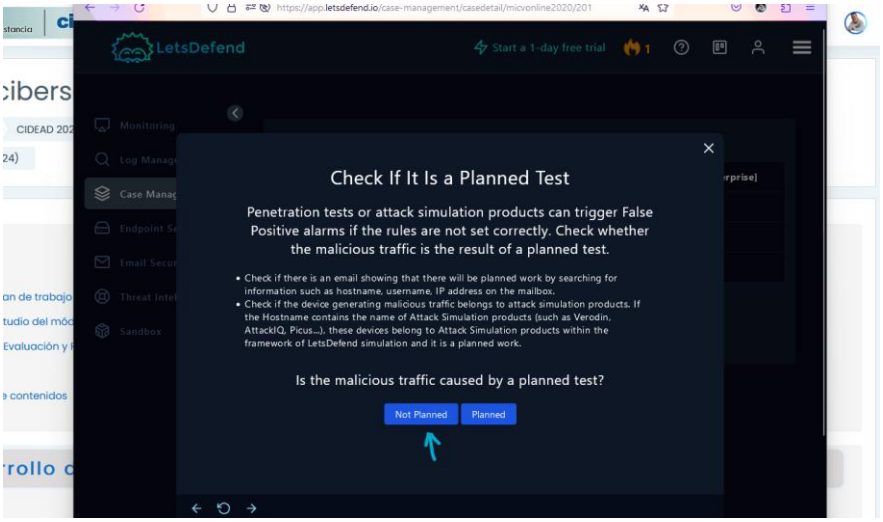
Vistos los resultados anteriores, podemos asegurar que el tráfico es malicioso.



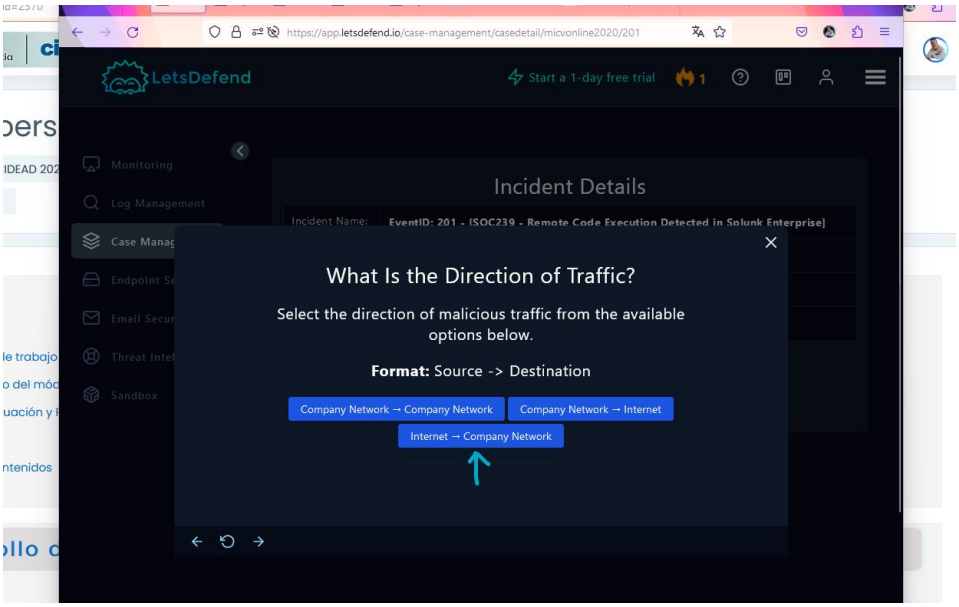
Con los datos referidos de los archivos involucrados, podemos indicar que se trata de un ataque de **`Inyección XML`**.



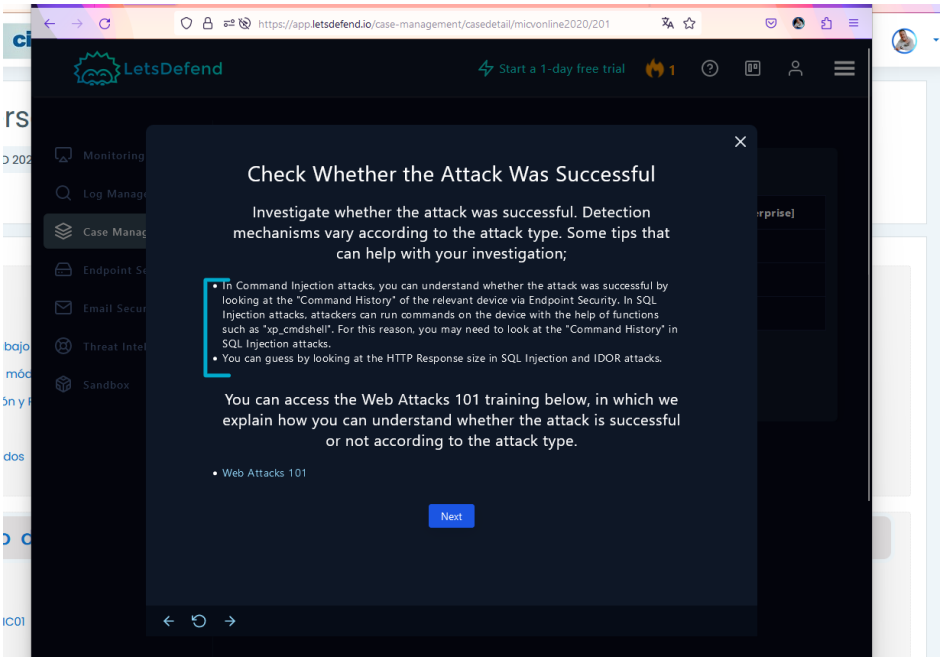
Tras la revisión de **`logs`**, y visto el tráfico registrado y las conexiones, no creo que podamos determinar que sea un ataque planeado.



La dirección de origen pertenece a la **IP** de la empresa China (**180.101.80.240**) y la de destino es la interna del servidor **Splunk** (**172.16.20.13**), por lo que podemos concretar que la dirección del tráfico es desde Internet a la Red de la Empresa.



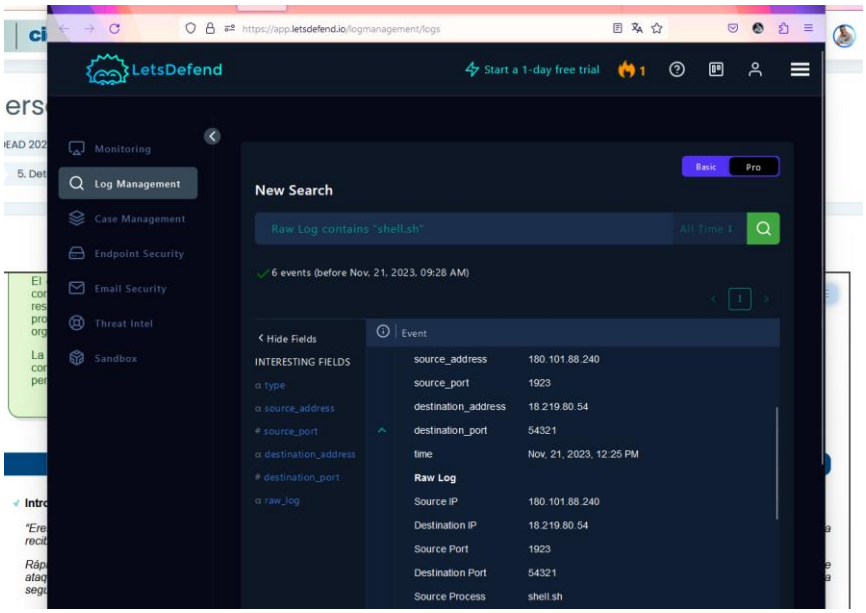
Otra indicación donde buscar información nos aparece en la nueva ventana, donde nos sugiere que busquemos más datos, por ejemplo, en el historial de comandos.

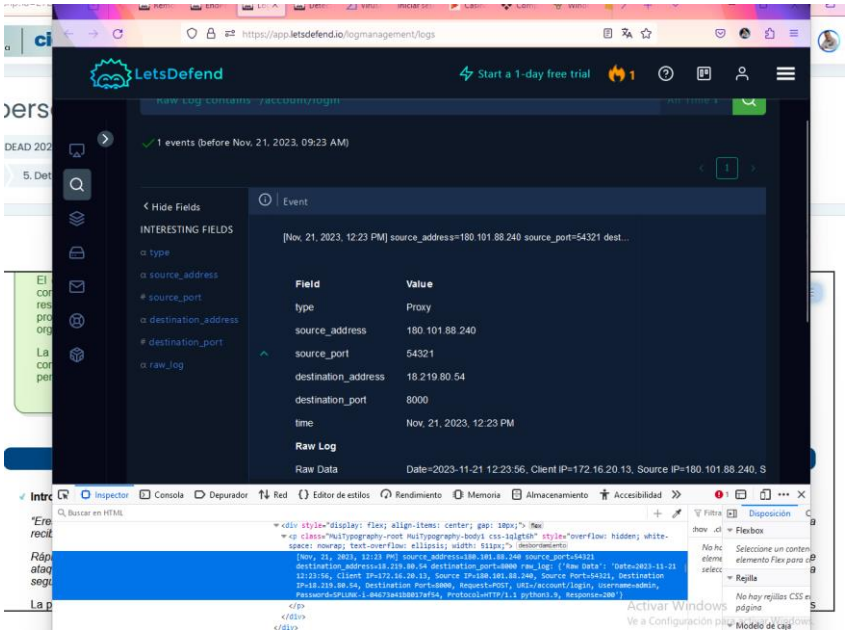


Con los indicios anteriores, podemos hacer varias búsquedas relativas a los archivos incluidos en la alerta y en el tráfico.

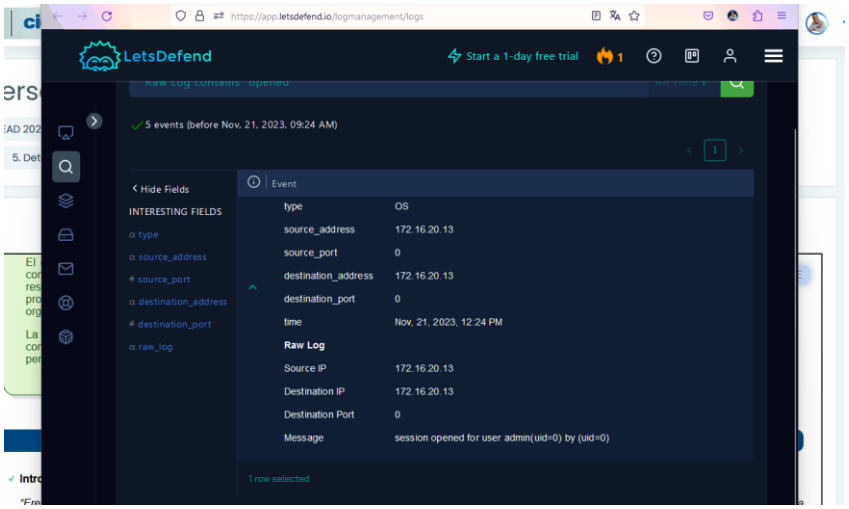
Podemos encontrar, incluso sin descargarlos, valiosa información en la red sobre ambos archivos (disponible más información en el apartado de webgrafía), por lo que no le dedicaremos más tiempo, y nos enfocamos en aprovechar esa información para seguir buscando.

Se puede observar como el atacante ha ejecutado exitosamente el archivo **shell.sh** y cargado **shell.xsl**.

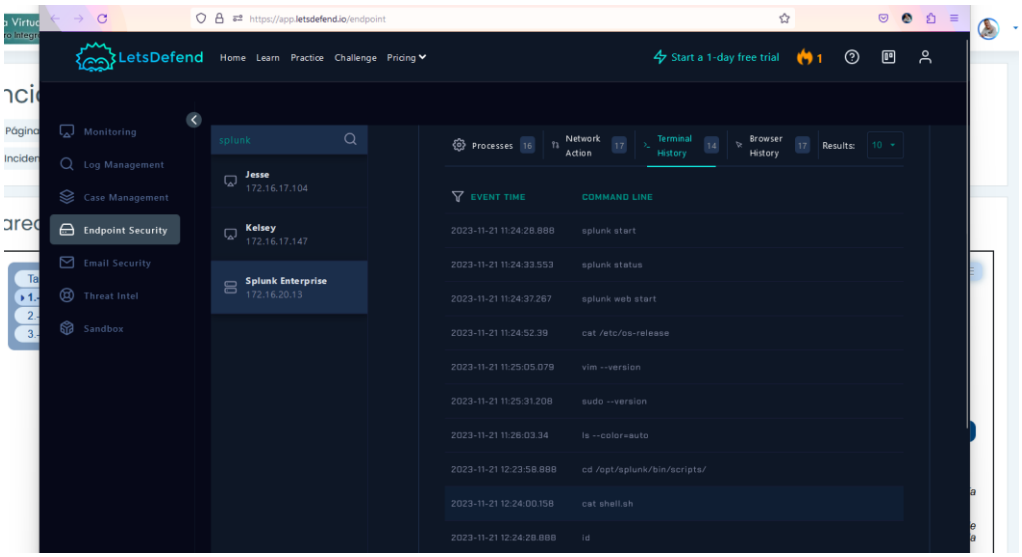


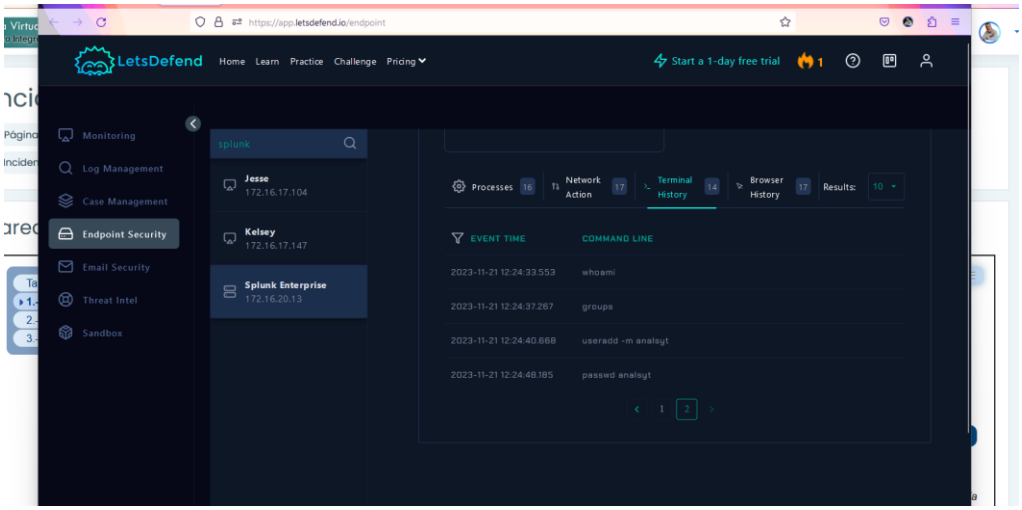


Además, ha creado una cuenta de usuario administrador y ha creado un nuevo usuario para generar persistencia.

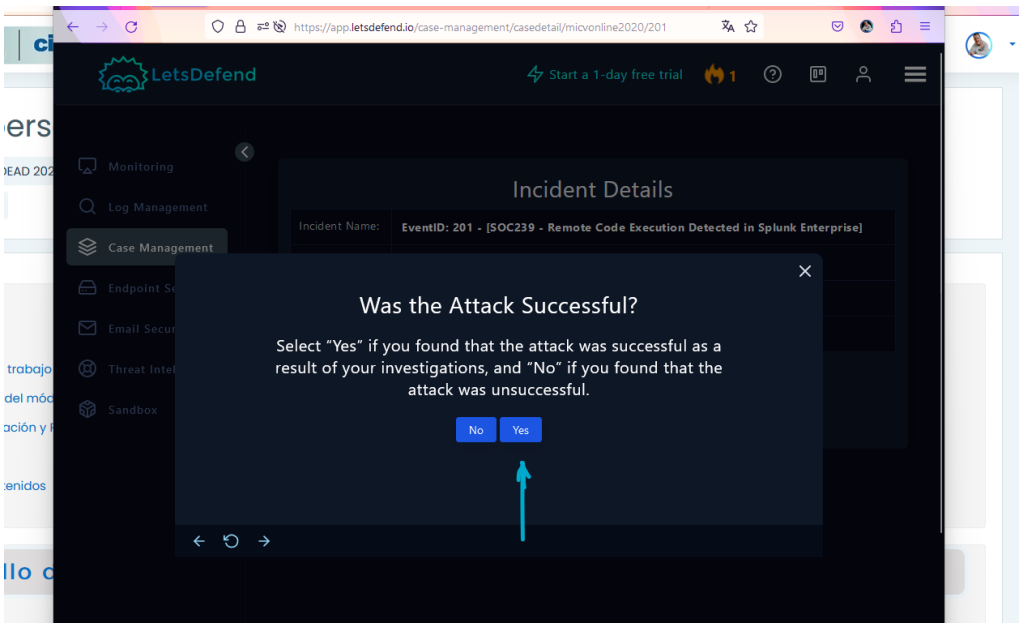


Repasamos el historial de comandos.

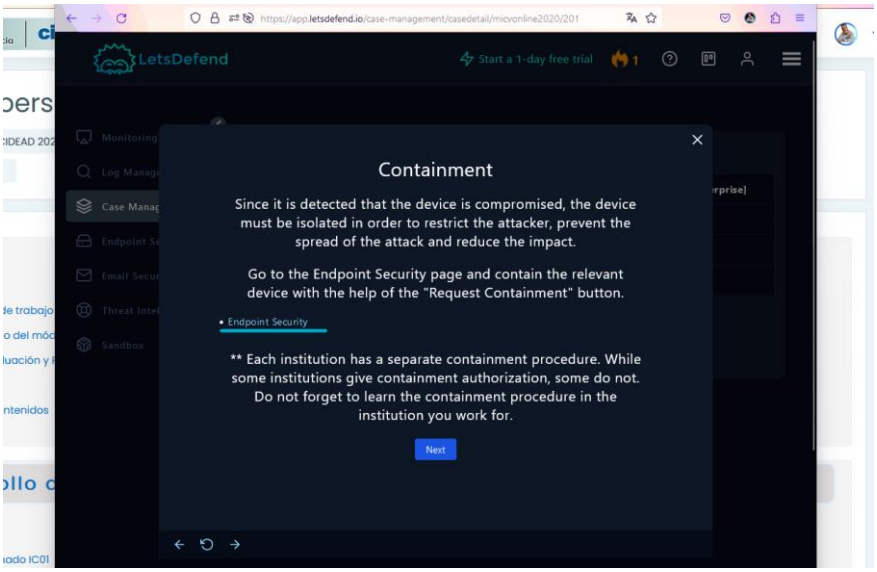




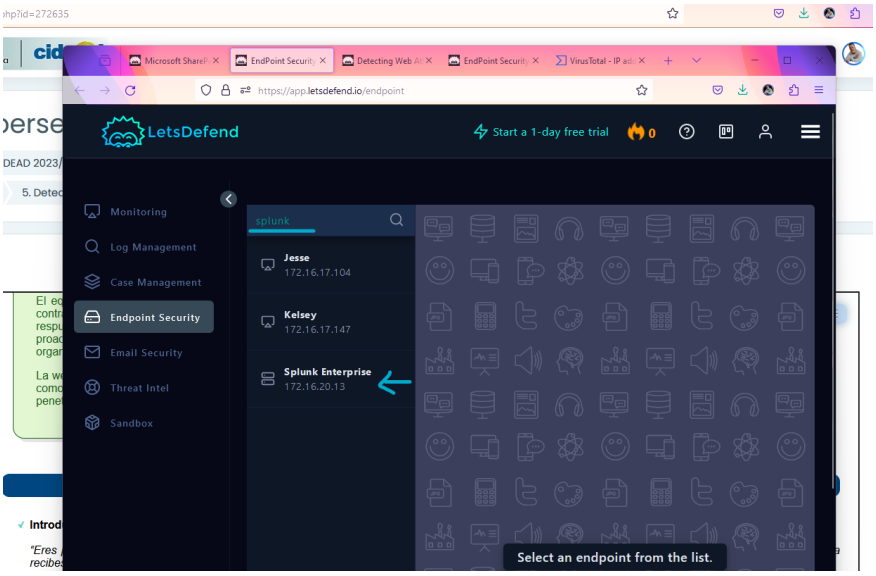
Como ha sido un acción permitida y el ataque ha resultado exitoso, lo señalamos así en el siguiente paso.

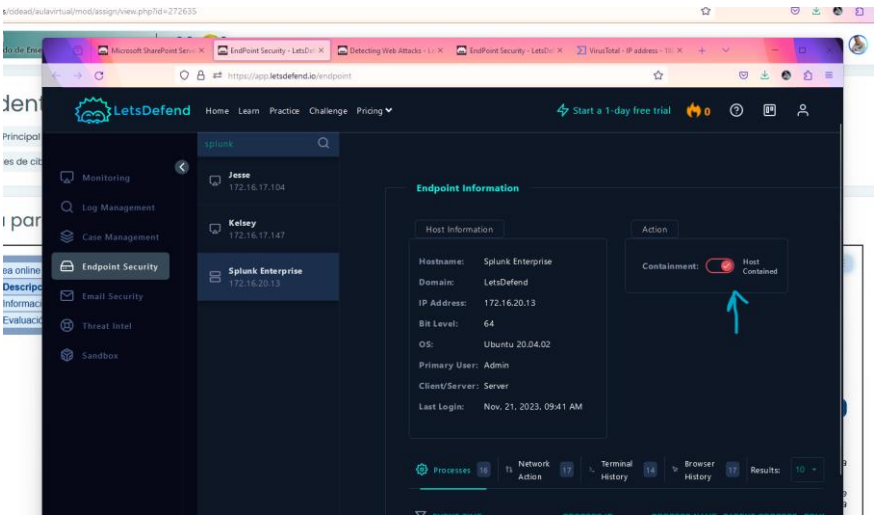


Vamos con el apartado de contención. Nos indica que el dispositivo de debe estar aislado, para restringir otras opciones de ataque.

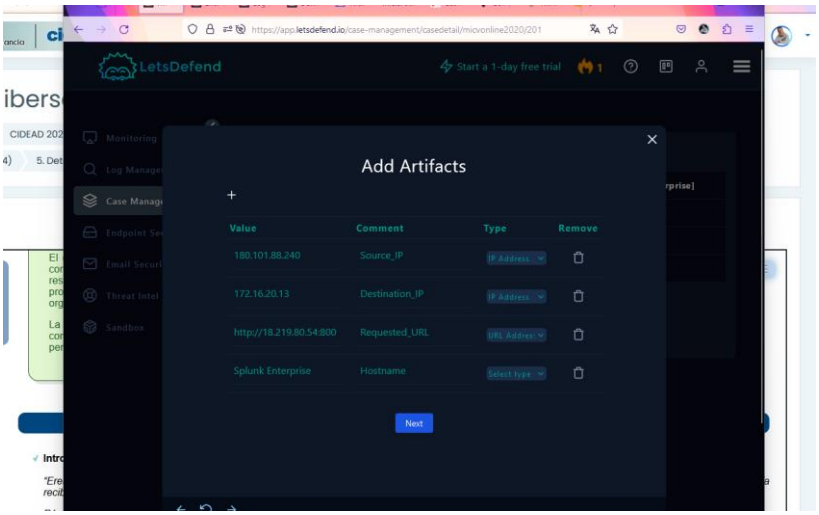


Accedemos desde una nueva ventana al apartado **"Endpoint Security"**, y buscamos **"Splunk"**. Dentro, activamos la contención.

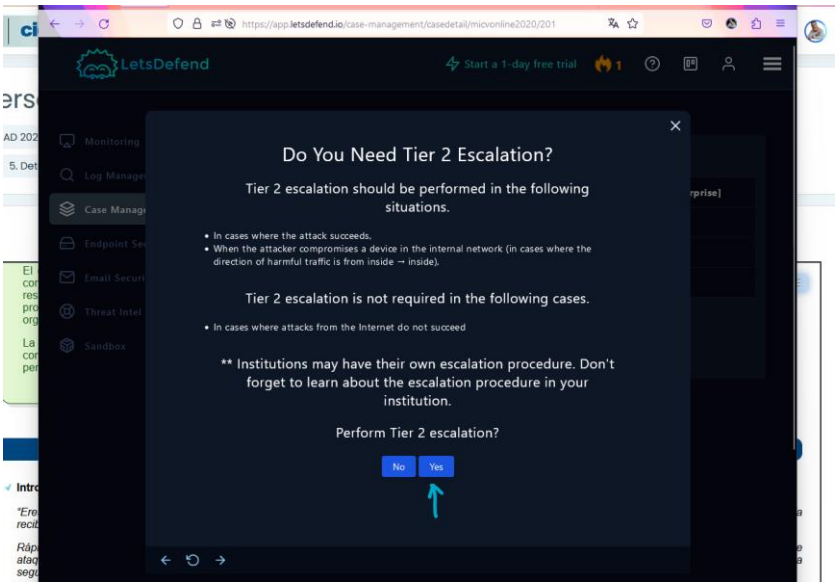




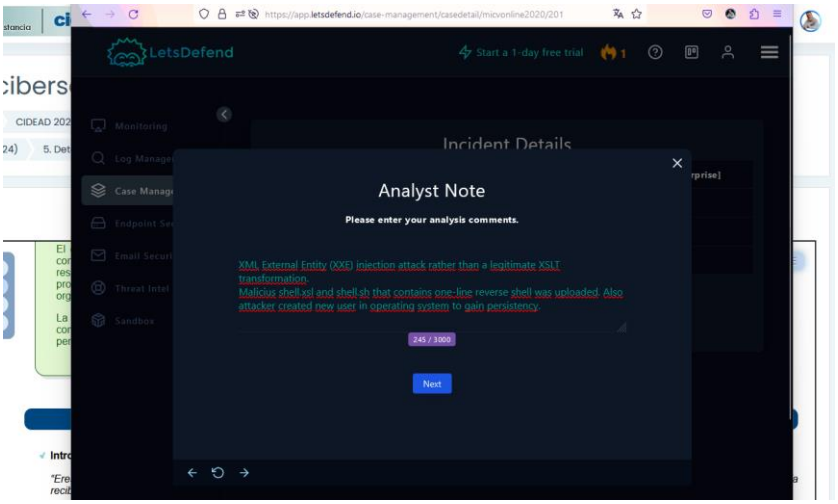
Nos pide añadir los artefactos encontrados. Completamos los campos con ellos.



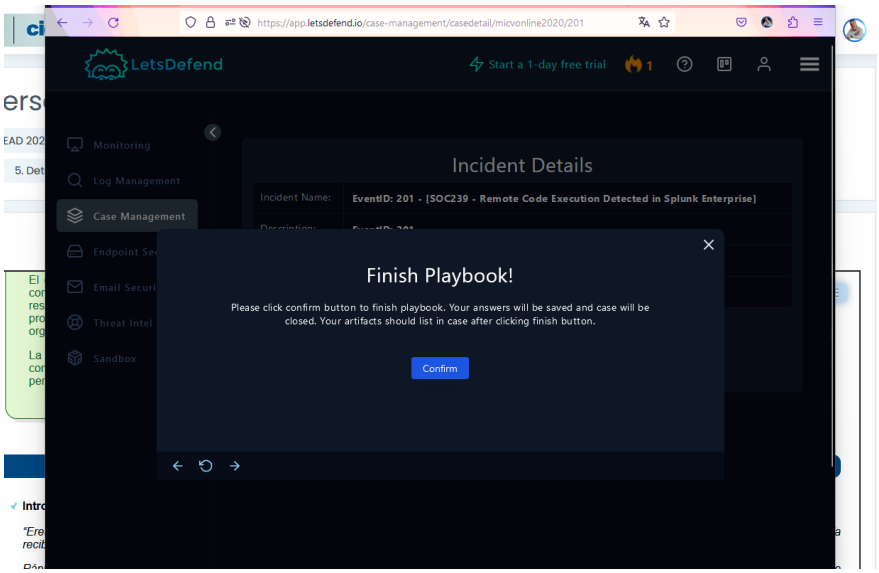
En el siguiente paso, vemos por su descripción de situaciones que debemos escalar a **`Nivel 2`**.

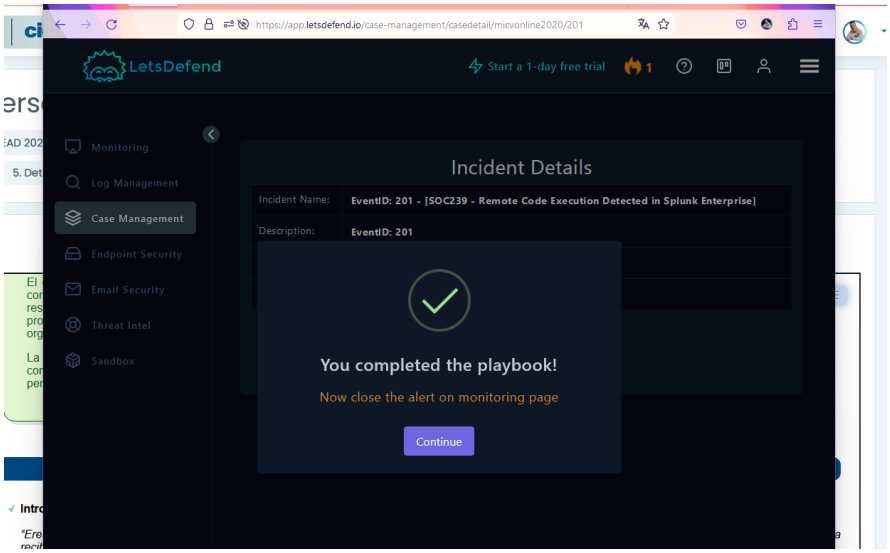


Nos permite añadir un texto explicativo sobre el análisis, por lo que aprovechamos para dejar una explicación somera.

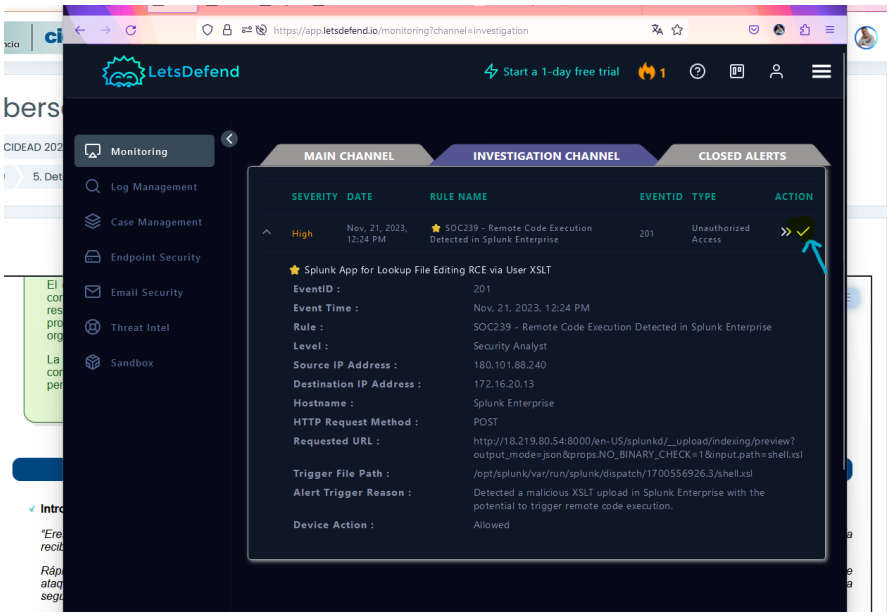


Con ello, terminamos el **`Playbook`**.

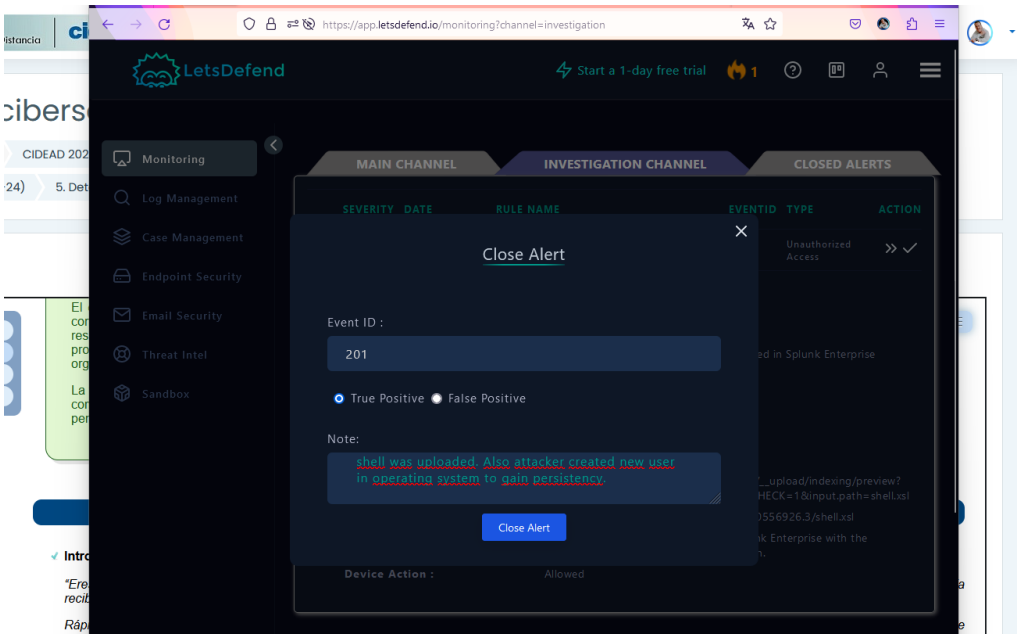




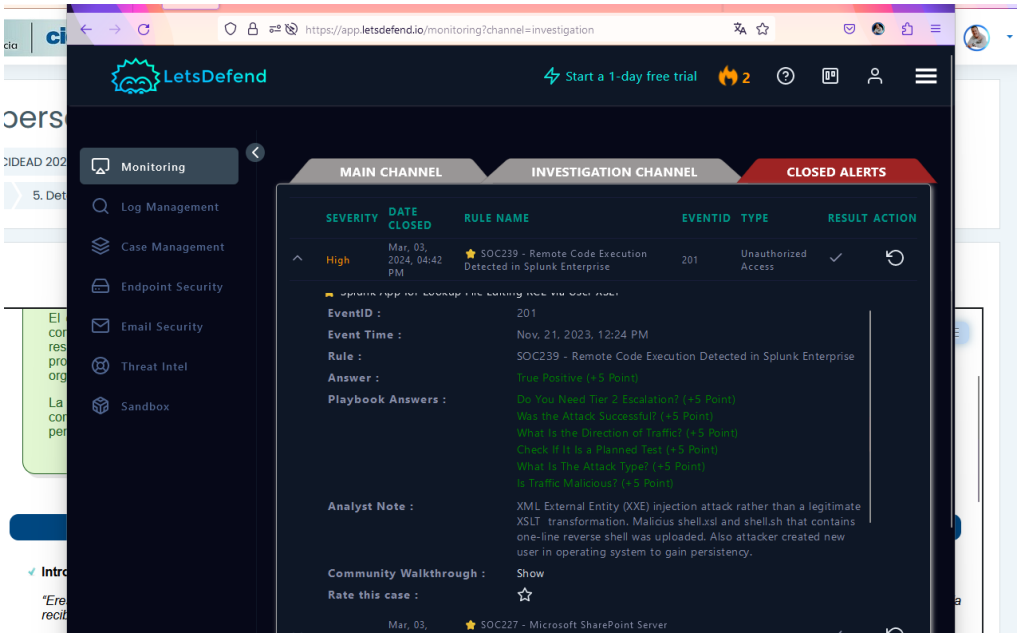
Podemos ahora cerrar el caso de estudio creado.



Al cerrar, nos pedirá añadir una nota explicativa sobre la alerta estudiada.



Al cerrarlo, podemos ver el resumen y en el supuesto de haber errado en algo, nos lo indicarán en la puntuación (apartado en verde).



✓ **Apartado 2: Comunicaciones de incidente.**

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 ciberincidente.

Para la realización de los siguientes apartados se puede consultar la “Guía Nacional de Notificación y Gestión de Ciberincidentes” en sus apartados 5 y 6. Hay un enlace a esta guía en la siguiente sección.

Deberás efectuar la siguiente tarea:

- Realices una clasificación justificada del incidente según la taxonomía oficial.

Intrusión	Compromiso de cuenta con privilegios	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegios.

Aplicando a la tabla 3 de la guía, los datos conseguidos durante el estudio del caso, y viendo que el ataque fue exitoso, se puede concluir que se trata de una intrusión con compromiso de cuenta con privilegios.

- Determines el nivel de peligrosidad del incidente.

ALTO	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Código dañino	Sistema infectado
		Servidor C&C (Mando y Control)
	Intrusión	Compromiso de aplicaciones
		Compromiso de cuentas con privilegios
	Intento de intrusión	Ataque desconocido
	Disponibilidad	DoS (Denegación de servicio)
		DDoS (Denegación distribuida de servicio)
	Compromiso de la información	Acceso no autorizado a información
		Modificación no autorizada de información
		Pérdida de datos
	Fraude	Phishing

El nivel de peligrosidad según la tabla es: **Alto**.

- Determines el nivel de impacto del ciberincidente.

Considerando los criterios mencionados en la guía, el nivel de impacto de la alerta CVE-2023-46214 puede clasificarse como **Alto**, por la coincidencia con los siguientes parámetros:

- **Tipología de la información o sistemas afectados:** La vulnerabilidad afecta a un software de gestión de logs y eventos muy utilizado, implicando que podría ser utilizada para el acceso a información sensible de las organizaciones.
- **Grado de afectación a las instalaciones de la organización:** La explotación exitosa de la vulnerabilidad, como apuntamos antes, podría permitir la ejecución de código remoto en el sistema afectado, con un impacto importante en las operaciones de la organización afectada.
- **Posible interrupción en la prestación del servicio normal de la organización:** La explotación de la vulnerabilidad podría provocar la interrupción del servicio de Splunk Enterprise, afectando entonces a la capacidad de monitorización y gestión de sus sistemas.

- **Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones:** La recuperación de un ataque tras explotar esta vulnerabilidad podría requerir un tiempo considerable y recursos adicionales, implicando un impacto económico significativo.
- **Pérdidas económicas:** La explotación de la vulnerabilidad podría provocar la pérdida de datos confidenciales, que acabarían significando multas y daños en la reputación de la organización.

He valorado la posibilidad de escalarlo, por el posible Impacto en la Seguridad (al depender del departamento de Justicia), pero al concebirlo como contenido en los momentos siguientes a la detección, he decidido dejarlo con esa clasificación.

➢ Indicar la posible obligación de notificar al CSIRT correspondiente.

El ámbito de aplicación de uso de Splunk, abarca mayoritariamente a grandes empresas de sectores como las telecomunicaciones, banca y finanzas, organismos gubernamentales (como es el caso) y educativos.

Por ello, al clasificarlo como de nivel Alto, desde el apartado 6.1.6 de la guía nos indican que es obligatorio notificar el incidente al CSIRT correspondiente (CCN-CERT).

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

Qué notificar	Descripción
Asunto	Notificación de incidente de seguridad - CVE-2023-46214
OSE/PSD	Equipo Ciberseguridad Sede Ministerial de Justicia en Andalucia.
Sector estratégico	Justicia
Fecha y hora del incidente	21/11/2023 12:24PM
Fecha y hora de detección del incidente	21/11/2023 14:24PM
Descripción	Se ha detectado una explotación de la vulnerabilidad CVE-2023-46214 en Splunk Enterprise. Esta vulnerabilidad permite la ejecución de código remoto en el sistema afectado.
Recursos tecnológicos afectados	Servidor Splunk Enterprise
Origen del incidente	Internet
Taxonomía	Intrusión. Compromiso cuenta con privilegios.
Nivel de Peligrosidad	Alto
Nivel de Impacto	Alto
Impacto transfronterizo	No
Plan de acción y contramedidas	Actualización a Splunk Enterprise 9.0.7 o 9.12. Implementación de medidas de mitigación internas temporales.
Afectación	Interrupción del servicio Splunk. Pérdida de datos.
Medios necesarios para la resolución	Actualización de software. Monitorización de sistemas. Análisis forense.

Impacto económico estimado	No cuantificado
Daños reputacionales	No cuantificados
Extensión geográfica	Andalucia.
Adjuntos	Informe previo. Datos iniciales. Logs. Capturas de pantalla.
Regulación afectada	RGPD
Se requiere actuación de FFCCSE	No
Que notificar	**Descripción**

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

Al haber sido detectado de forma temprana, se efectuarán tres notificaciones:

- Una **notificación inicial** poniendo en conocimiento y alertando de la existencia del incidente.
- Una **notificación intermedia** actualizando, tras asegurar la contención, con los datos disponibles relativos al incidente comunicado.
- Una **notificación final** ampliando y confirmando los datos definitivos relativos al incidente comunicado.

La frecuencia, dado el nivel alto debe ser: inmediata para la inicial, y para las otras en el mismo momento en que se puedan reunir los datos.

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

Fecha:	20/12/2023 9:32PM
Responsable:	Juan A. García Muelas
Resumen del estado:	El incidente de seguridad relacionado con la vulnerabilidad CVE-2023-46214 ha sido cerrado. Se han implementado las siguientes medidas para mitigar el riesgo: • Actualización de Splunk Enterprise a la versión 9.0.7 o 9.1.2: Se han actualizado todos los servidores de Splunk Enterprise a una versión no vulnerable. • Implementación de medidas de mitigación temporales: Se han implementado medidas de mitigación temporales en los servidores que no se han podido actualizar de inmediato. • Monitorización de sistemas: Se está monitorizando de forma continua los sistemas para detectar cualquier actividad anómala que pueda indicar la explotación de la vulnerabilidad.
Conclusiones:	Incidente cerrado con éxito tras mitigación del riesgo y no detectarse nuevas incidencias relacionadas. Notificado a CCN-CERT.
Anexos:	Informe final.

Webgrafía.

https://www.incibe.es/incibe-cert/guias-y-estudios/guias/guia-nacional-de-notificacion-y-gestion-de-ciberincidentes

https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2023-46214

https://advisory.splunk.com/advisories/SVD-2023-1104

https://www.uptycs.com/blog/splunk-vulnerability-cve-2023-46214