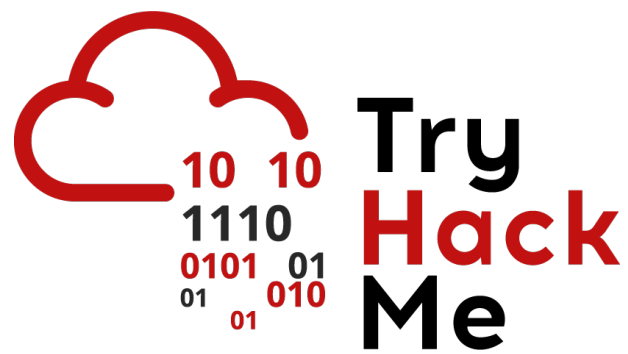


Writeup: Sala *Junior Security Analyst Intro*

Autor: Ismaeldevs
Plataforma: TryHackMe
4 de julio de 2025



Índice

1. Introducción	2
2. Sala	2
2.1. Tarea 1 – Una carrera como analista de seguridad junior	2
2.2. Tarea 2 - Centro de Operaciones de Seguridad (SOC)	2
2.3. Tarea 3 - Un día en la vida de un analista de seguridad junior	2
3. Conclusión sobre la Sala	7

1. Introducción

En esta sala aprenderemos sobre el rol de un **Analista de Seguridad** de nivel inicial dentro de un SOC (Security Operations Center). Se aprende sobre las funciones clave de este puesto, el funcionamiento interno de un SOC, y se exploran las herramientas, procesos y habilidades que se emplean en la investigación y respuesta a incidentes de seguridad.

2. Sala

2.1. Tarea 1 – Una carrera como analista de seguridad junior

En esta primera tarea descubriremos el papel de un analista de seguridad junior (también llamado Triage Specialist o analista Tier 1), responsable de filtrar y gestionar alertas en un SOC operativo las 24 horas. Se enfoca en monitorear logs, configurar herramientas de seguridad y escalar incidentes a niveles superiores cuando es necesario.

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.2. Tarea 2 - Centro de Operaciones de Seguridad (SOC)

Aprenderemos sobre la función y estructura de un SOC: un centro 24/7 que descubre, previene y responde a incidentes cibernéticos. Se detallan sus tres principales actividades:

1. **Preparación/Prevenir** (inteligencia de amenazas, firmas IDS, mantenimiento de herramientas)
2. **Monitoreo/Investigación** (uso de SIEM/EDR para priorizar alertas)
3. **Respuesta** (contención y remediación de hosts comprometidos)

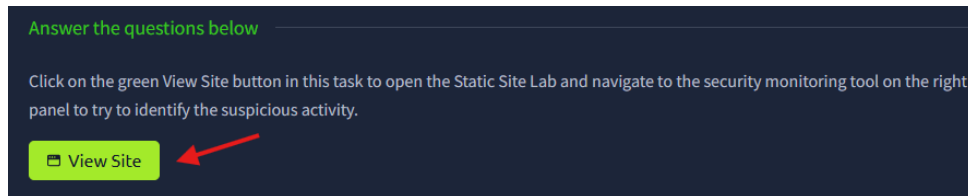
Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.3. Tarea 3 - Un día en la vida de un analista de seguridad junior

Vamos a conocer un vistazo práctico a una jornada típica en un SOC: revisar tickets de alertas, investigar eventos sospechosos (como IPS/IDS, correos o tráfico malicioso), bloquear IPs maliciosas y extraer evidencia forense.

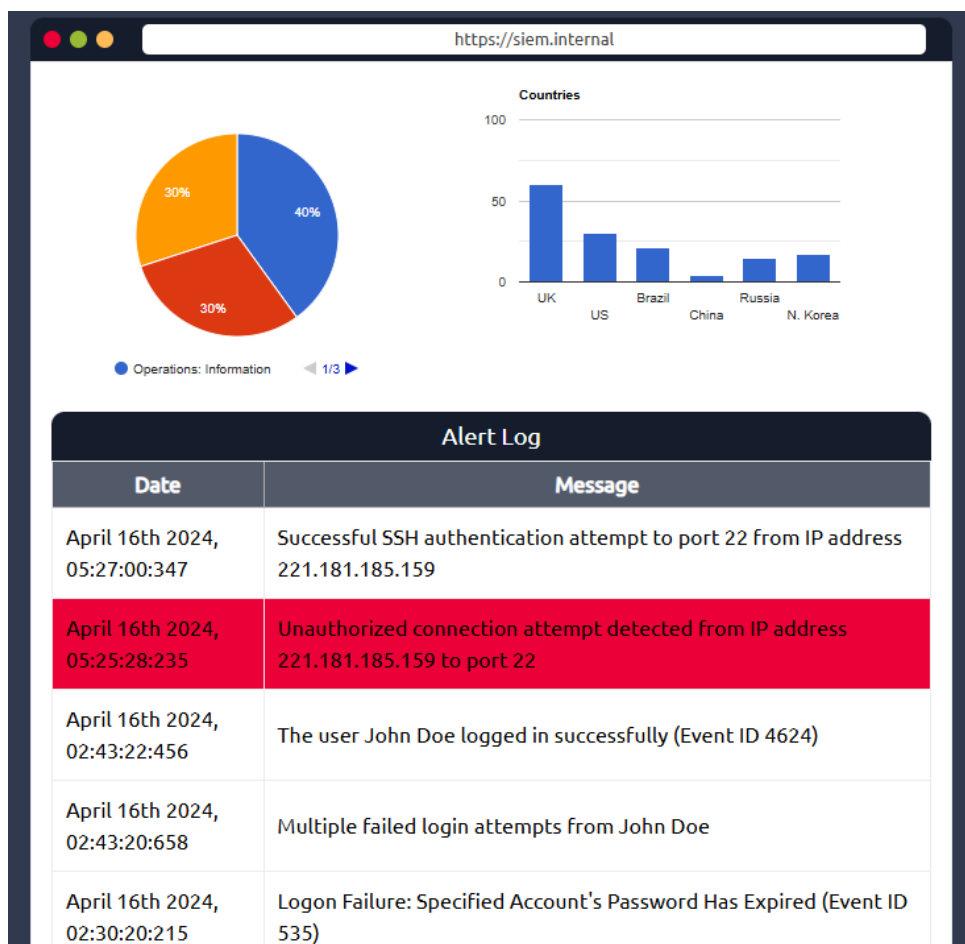
También se muestra la reacción ante incidentes reales: escalar, contener, eliminar procesos maliciosos y asegurar sistemas.

Ahora, para completar la tarea debemos desplegar el sitio de práctica e ir respondiendo las siguientes preguntas.



Pregunta: What was the malicious IP address in the alerts?

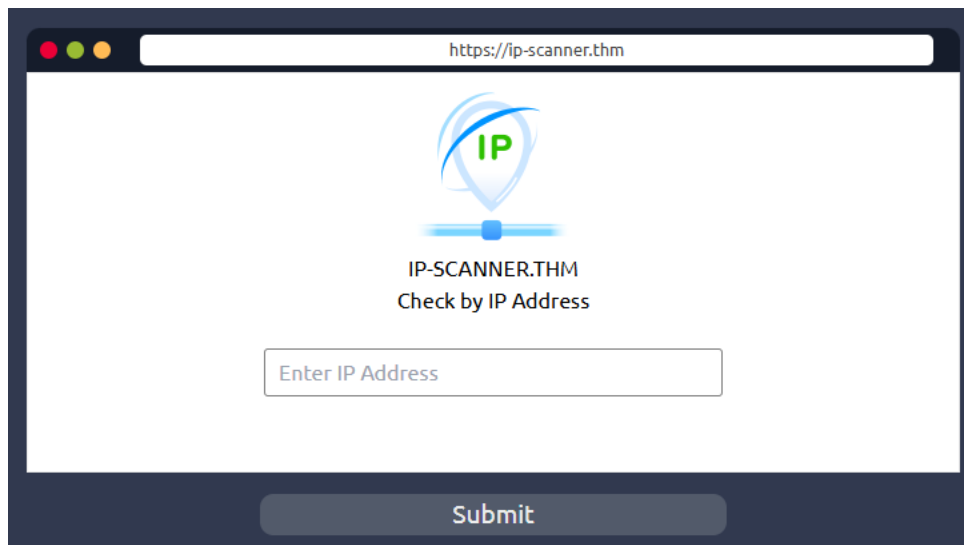
Para responder a la pregunta, simplemente debemos revisar las alertas de logs e identificar la IP maliciosa.



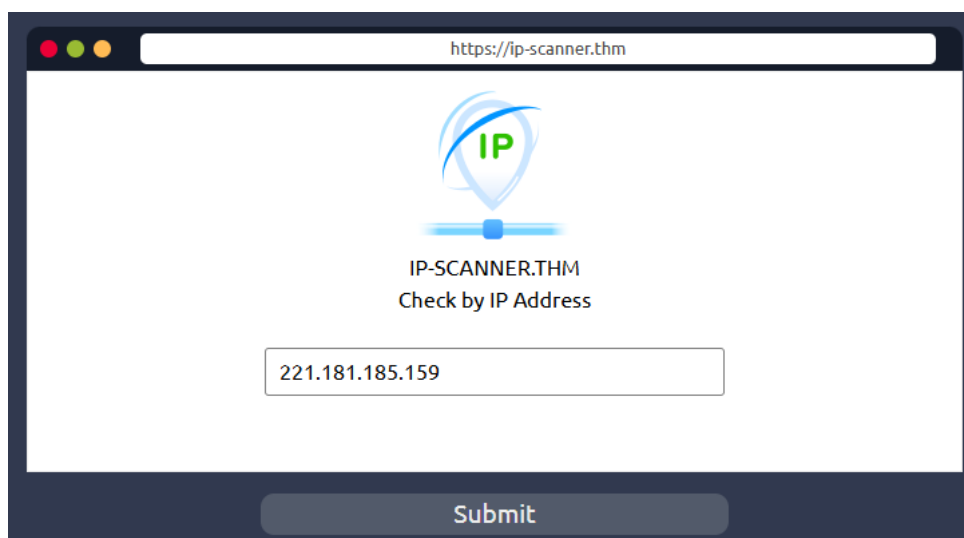
Respuesta: 221.181.185.159

Pregunta: To whom did you escalate the event associated with the malicious IP address?

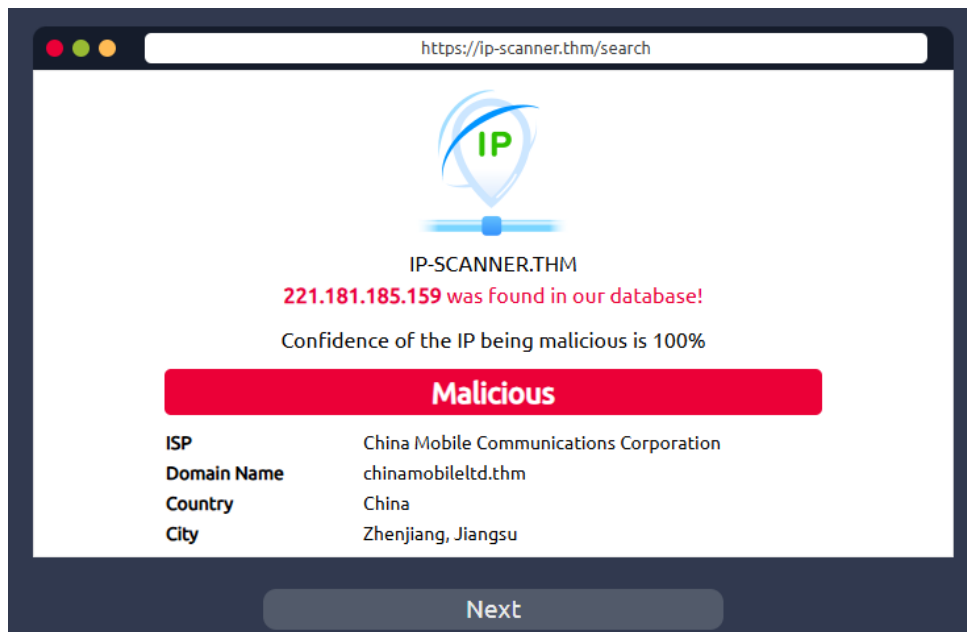
Una vez hecho eso, haremos clic en la IP y pasaremos a la siguiente sección, posterior a eso, introduciremos la IP para obtener más información sobre ella y haremos clic en Submit.



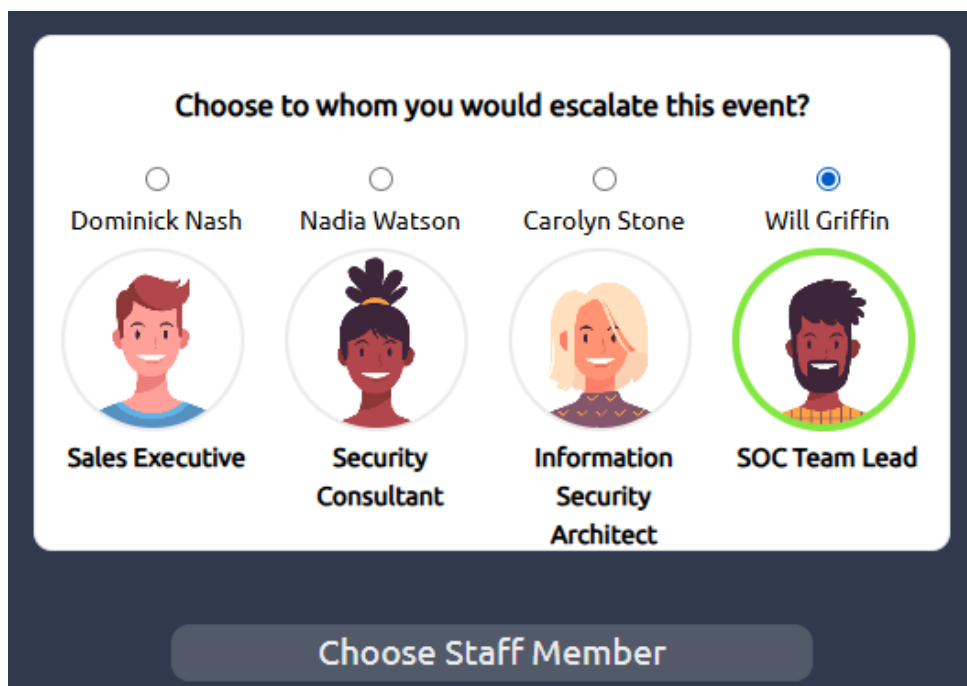
A screenshot of a web browser window displaying the IP-Scanner.THM interface. The address bar shows `https://ip-scanner.thm`. The page features a logo with a blue shield and a green 'IP' inside. Below the logo, the text 'IP-SCANNER.THM' and 'Check by IP Address' is displayed. A text input field contains the placeholder text 'Enter IP Address'. At the bottom, there is a dark blue 'Submit' button.



A second screenshot of the same IP-Scanner.THM web interface. The text input field now contains the IP address '221.181.185.159'. The 'Submit' button remains at the bottom.



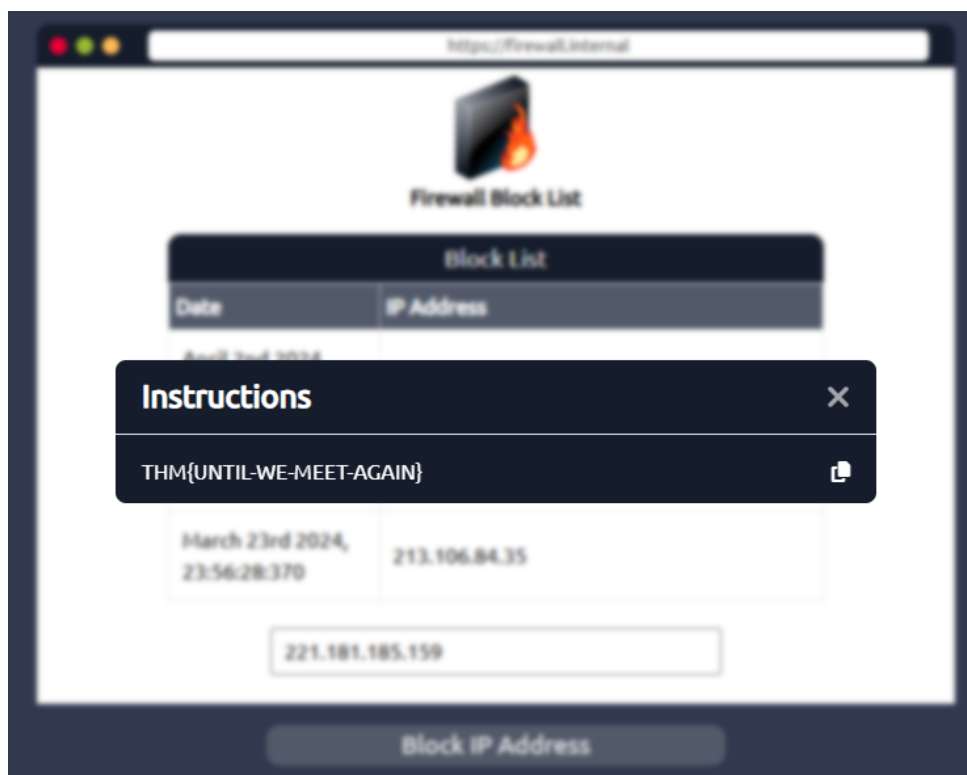
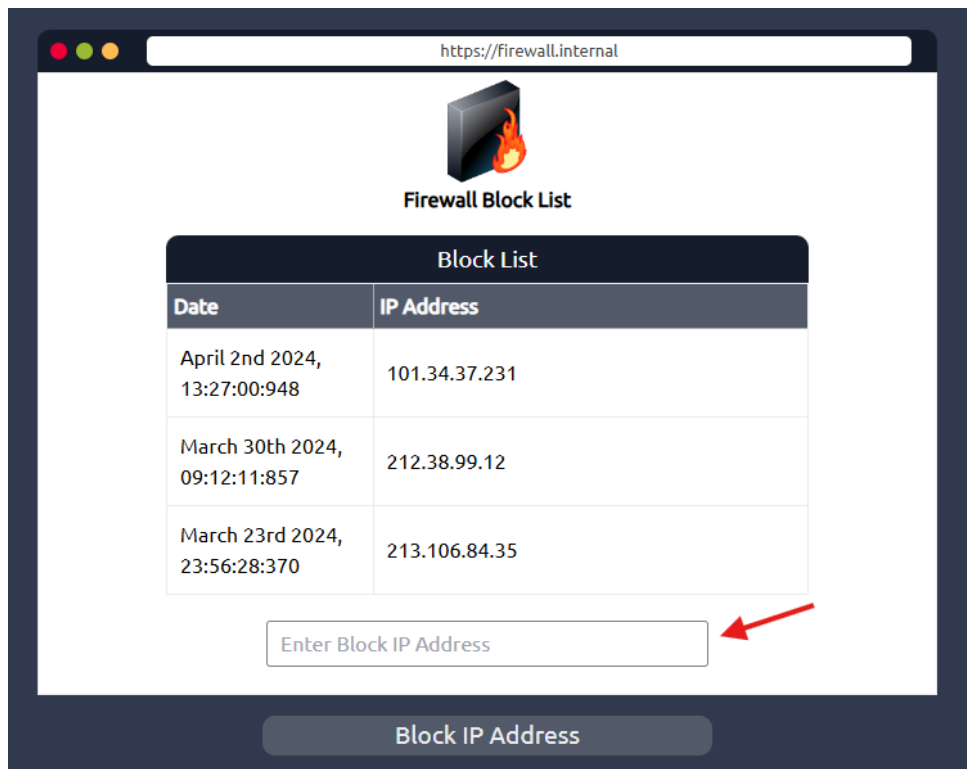
Después de obtener más información sobre la IP, debemos darle a Next y seleccionar al Staff adecuado que debe escalar este tipo de eventos.



Respuesta: Will Griffin

Pregunta: After blocking the malicious IP address on the firewall, what message did the malicious actor leave for you?

Ahora que ya seleccionamos al staff correspondiente, debemos bloquear esta IP, para ello, introduciremos la IP correcta y procederemos a darle en **Block IP Address**.



Respuesta: **THM{UNTIL-WE-MEET-AGAIN}**

3. Conclusión sobre la Sala

Al finalizar la sala hemos logrado comprender en profundidad el rol de un **Junior Security Analyst**, cómo opera un SOC y qué tareas diarias enfrentan los analistas de primer nivel. Además, aprendimos otros conceptos como el análisis de alertas, escalamiento de incidentes, uso de herramientas como SIEM o EDR, y la importancia de la colaboración en equipo.