

Introducción al analista de seguridad junior



Tarea 1: Una carrera como analista de seguridad junior (asociado)

En el puesto de Analista de Seguridad Junior, serás Especialista en Triage. Dedicarás mucho tiempo a la clasificación y supervisión de los registros de eventos y alertas.

Las responsabilidades de un analista de seguridad junior o un analista SOC de nivel 1 incluyen:

- Supervisar e investigar las alertas (la mayoría de las veces, es un entorno de operaciones SOC 24x7)
- Configurar y administrar las herramientas de seguridad
- Desarrollar e implementar firmas básicas de IDS (sistema de detección de intrusiones)
- Participar en grupos de trabajo y reuniones del SOC
- Crear tickets y escalar los incidentes de seguridad al Nivel 2 y al Líder del Equipo si es necesario

Cualificaciones requeridas (más comunes):

- 0-2 años de experiencia en Operaciones de Seguridad
- Comprensión básica de redes (modelo OSI (modelo de interconexión de sistemas abiertos) o modelo TCP /IP (protocolo de control de transmisión/modelo de protocolo de Internet)), sistemas operativos (Windows,

Linux), aplicaciones web. Para obtener más información sobre los modelos OSI y TCP /IP, consulte la Sala de introducción a las redes .

- Las habilidades de scripting/programación son una ventaja.

Certificación deseada:

- CompTIA Security+

A medida que prograses y mejores tus habilidades como analista de seguridad junior, eventualmente ascenderás al nivel 2 y al nivel 3.

P: ¿Cuál será tu papel como Analista de Seguridad Junior?

R: Triage Specialist

Tarea 2: Centro de Operaciones de Seguridad (SOC)

P: Lea lo anterior.

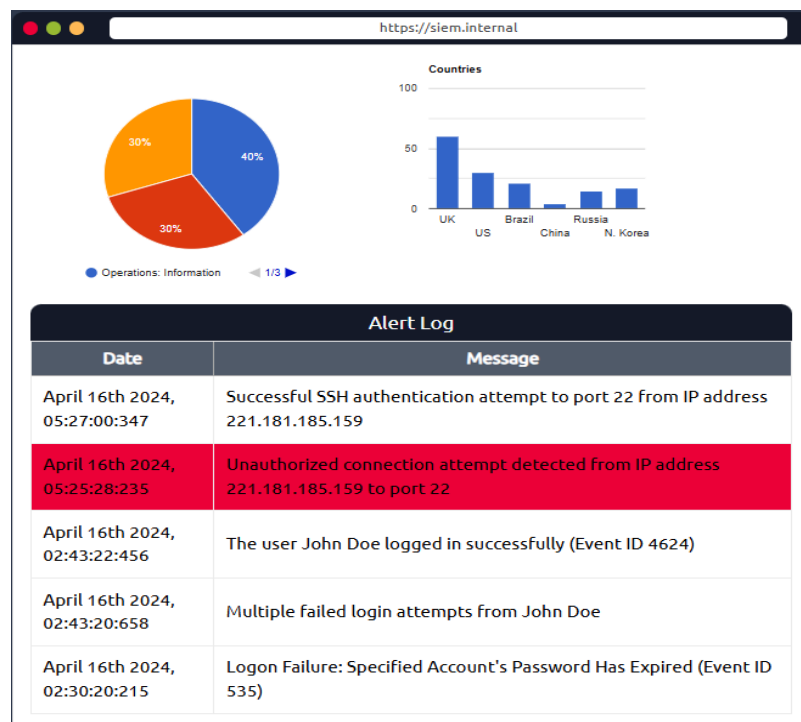
R: No se necesita respuesta

Tarea 3: Un día en la vida de un analista de seguridad junior (asociado)

P1: Haga clic en el botón verde Ver sitio en esta tarea para abrir el Laboratorio del sitio estático y navegar a la herramienta de monitoreo de seguridad en el panel derecho para intentar identificar la actividad sospechosa.

R1: No se necesita respuesta


P2: ¿Cuál era la dirección IP maliciosa en las alertas?



R2: 221.181.185.159


P3: ¿A quién le escaló el evento asociado con la dirección IP maliciosa?

https://ip-scanner.thm


IP-SCANNER.THM
Check by IP Address

Submit

https://ip-scanner.thm/search


IP-SCANNER.THM
221.181.185.159 was found in our database!
Confidence of the IP being malicious is 100%

Malicious


ISP	China Mobile Communications Corporation
Domain Name	chinamobiletd.thm
Country	China
City	Zhenjiang, Jiangsu

Next

Choose to whom you would escalate this event?

☐


Dominick Nash



Sales Executive

☐


Nadia Watson



Security Consultant

☐


Carolyn Stone



Information Security Architect

☒

Will Griffin

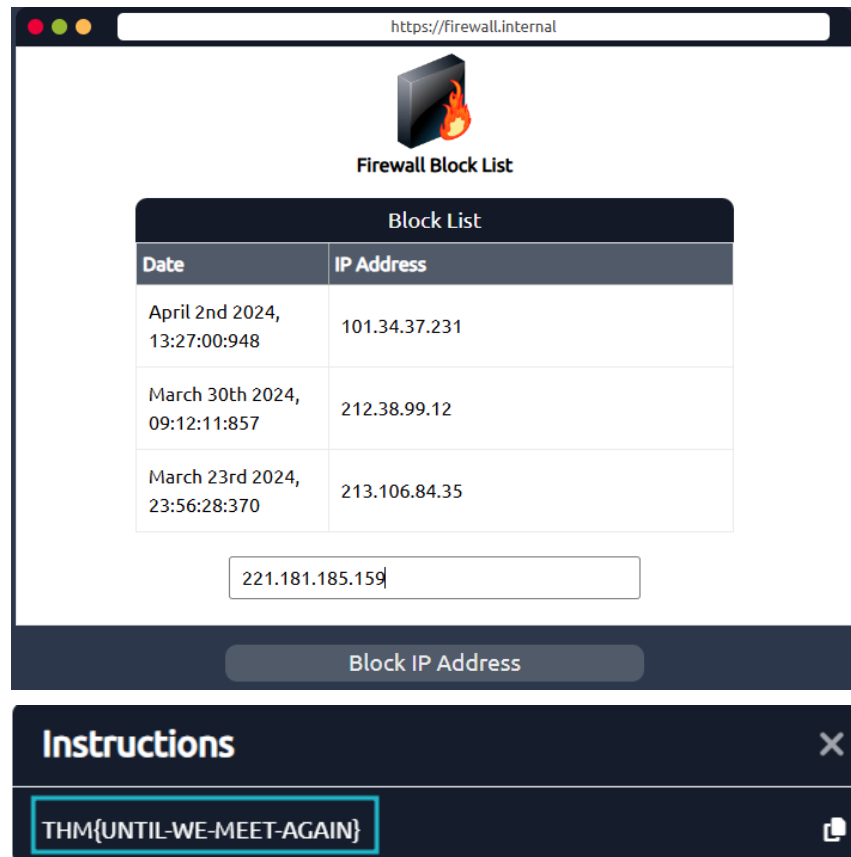


SOC Team Lead

Choose Staff Member

R3: Will Griffin

P4: Después de bloquear la dirección IP maliciosa en el firewall, ¿qué mensaje le dejó el actor malicioso?



R4: THM{UNTIL-WE-MEET-AGAIN}

 **LinkedIn:** <https://www.linkedin.com/in/mateo-rodr%C3%ADguez-suar-202695249/>

 **GitHub:** <https://github.com/MaateoSuar>