Writeup: Sala *Intro to Detection Engineering*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025

Índice

1. Introducción

En esta sala conoceremos sobre los fundamentos y metodologías clave de la ingeniería de detecciones dentro del ámbito de la ciberseguridad. Además, aprenderemos cómo identificar amenazas utilizando datos de logs, comportamientos maliciosos y marcos de referencia ampliamente utilizados como MITRE ATT&CK, Cyber Kill Chain y el ADS Framework.

2. Sala

2.1. Tarea 1 – Introducción

En esta primera tarea vamos a conocer el rol del **Detection Engineering** dentro del área de ciberseguridad. Aprendemos cómo un ingeniero de detección diseña procesos que permiten identificar amenazas, elaborar reglas de detección y hacer ajustes continuos frente a la evolución del entorno y los atacantes.

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

2.2. Tarea 2 - ¿Qué es la ingeniería de detección?

Aprenderemos la defínción de **Detection Engineering** como un proceso continuo para construir y operar análisis basados en inteligencia de amenazas, enfocados en detectar actividades maliciosas o malas configuraciones. Se detallan cuatro tipos principales de detección:

- **Basada en configuración:** detectar desalineaciones en infraestructuras.
- **Basada en modelado:** identificación de anomalías frente a un comportamiento base.
- **Indicadores:** uso de IOCs (IP, hashes, etc).
- **Comportamiento del atacante:** detección a partir de TTPs

Una vez que comprendimos sobre la ingeniería de detección, procedemos a responder las siguientes preguntas.

Pregunta: Which detection type focuses on misalignments within the current infrastructure?

Respuesta: **Configuration**

Pregunta: Which detection approach involves building an asset or activity baseline profile for detection?

Respuesta: **Modelling**

Pregunta: Which type of detection integrates with defensive playbooks?

Respuesta: **Threat Behaviour**

2.3. Tarea 3 - Metodologías de ingeniería de detección

En esta tarea vamos a conocer el ciclo metodológico típico:

1. **Análisis de brechas de detección**
2. **Identificación de fuentes de datos y recolección de logs**
3. **Creación de líneas base del comportamiento normal**
4. **Redacción de reglas (Sigma, Snort, YARA, etc)**
5. **Despliegue, automatización y afinamiento permanente de detecciones**

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

2.4. Tarea 4 - Marcos de ingeniería de detección 1

Nos introduciremos en aprender algunos marcos de referencia usados en ingeniería de detección:

- **MITRE ATT&CK y CAR:** para mapear TTPs adversarios.
- **Pyramid of Pain:** evalúa cuán costoso es para el atacante cambiar indicadores.
- **Cyber Kill Chain y Unified Kill Chain:** fases de un ataque, con una versión extendida de 18 etapas

Ahora que comprendemos algunos marcos, pasamos a responder las siguientes preguntas.

Pregunta: Which framework looks at how to make it difficult for an adversary to change their approach when detected?

Respuesta: **Pyramid of Pain**

Pregunta: What is the improved Cyber Kill Chain framework called?

Respuesta: **The Unified Kill Chain**

Pregunta: How many phases are in the improved kill chain?

Respuesta: **18**

2.5. Tarea 5 - Marcos de ingeniería de detección 2

Ahora aprenderemos sobre el **Alerting and Detection Strategy (ADS) Framework** de Palantir, guía la creación efectiva de alertas:

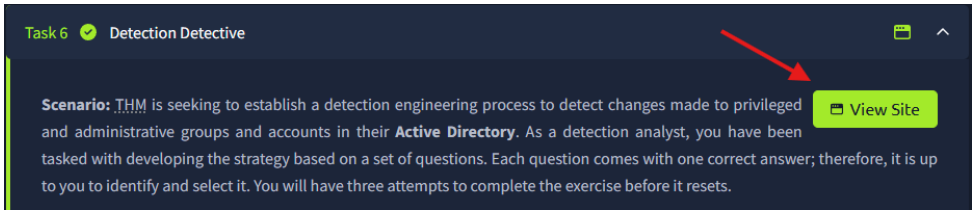
- **Define objetivos**
- **Categorización según ATT&CK**
- **Resumen estratégico**
- **efinición de fuentes de datos**
- **Metodologías de reducción de falsos positivos**

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

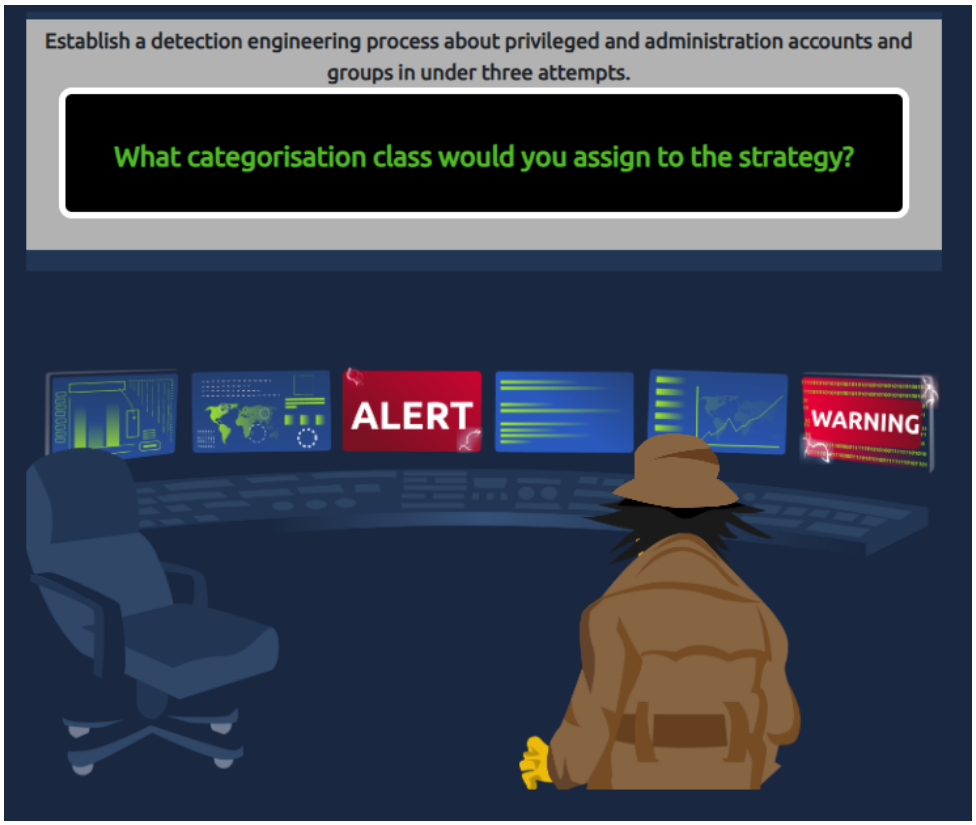
2.6. Tarea 6 - Detective de detección

Ahora nos introduciremos en un escenario práctico donde el objetivo es construir un proceso de detección en Active Directory para cambios en grupos privilegiados.

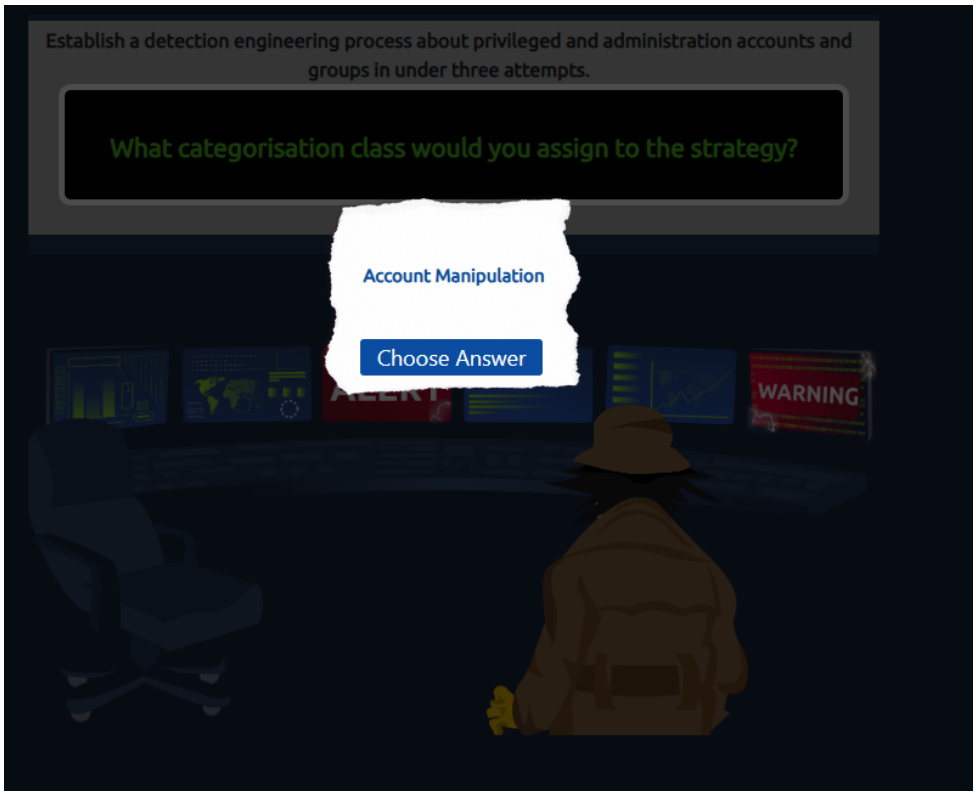
Para comenzar vamos a ir al lado superior de la tarea y haremos clic en **View Site**.



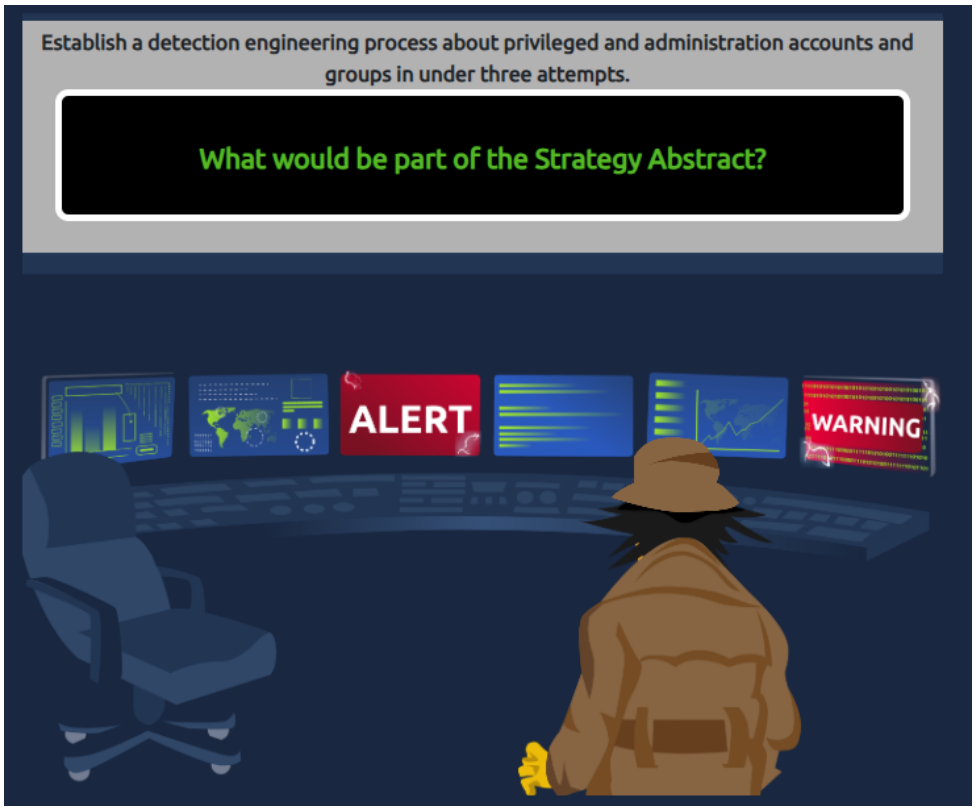
Se nos desplegara el sitio y vamos a comenzar a construir el proceso de detección respondiendo a las preguntas en pantalla.

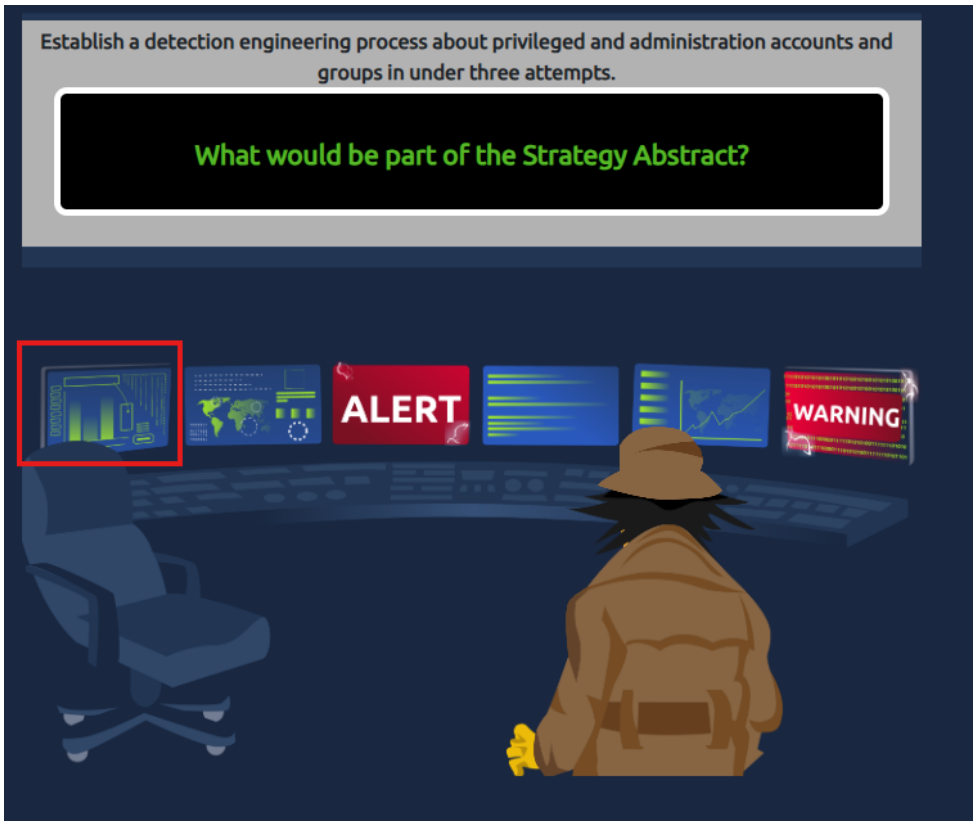


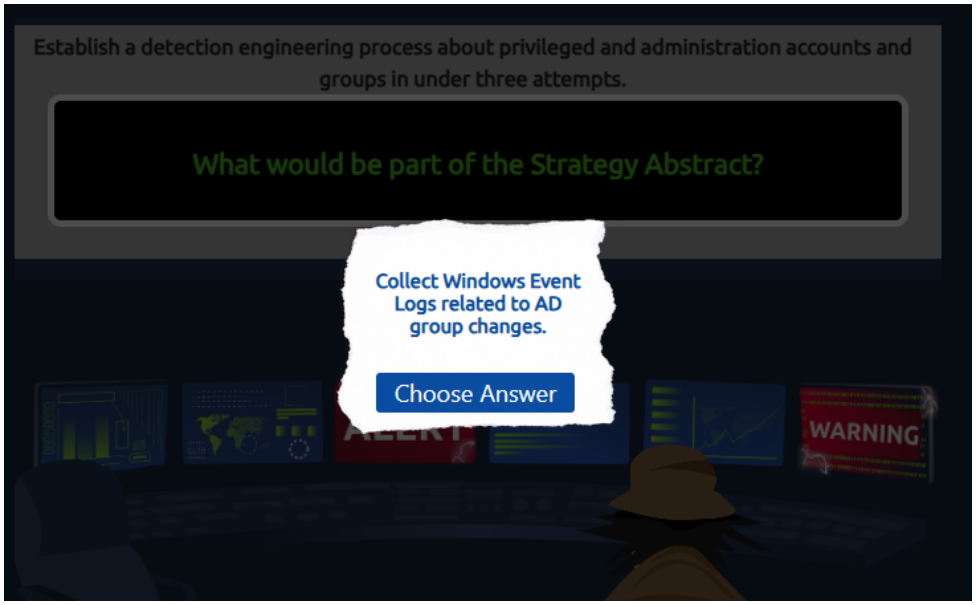
Para responder a la pregunta, debemos hacer clic en los diferentes monitores y analizar las respuestas para seleccionar la correcta.



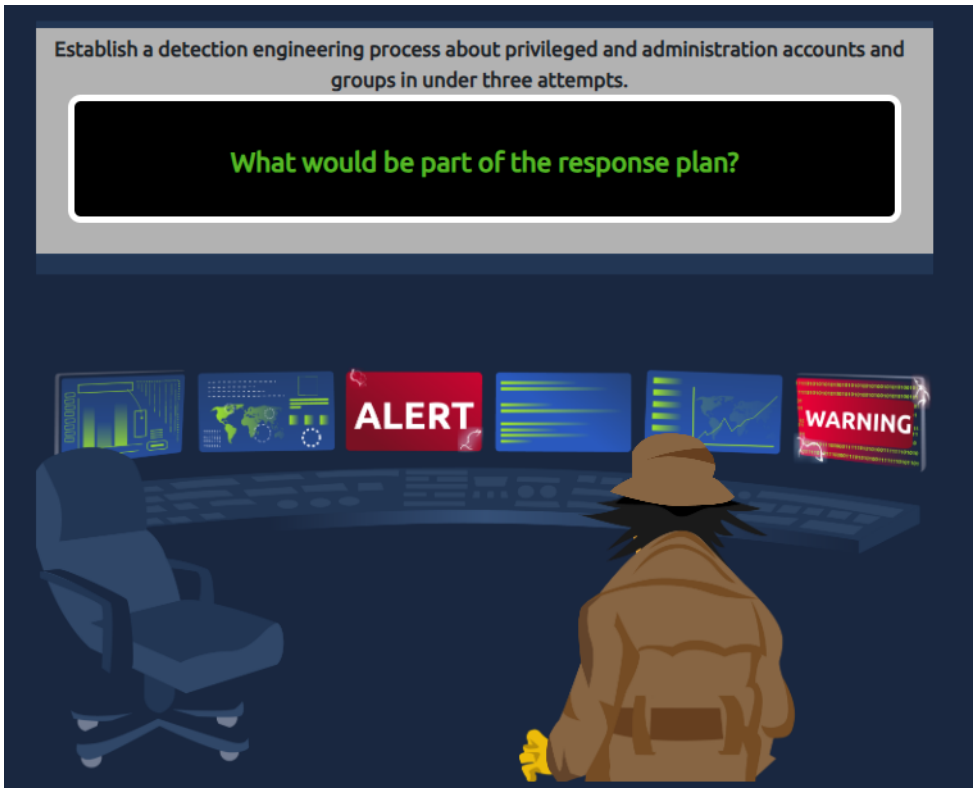
Una vez que logramos encontrar la respuesta haremos clic en **Choose Answer**, posterior a eso, continuaremos a responder las siguientes preguntas.

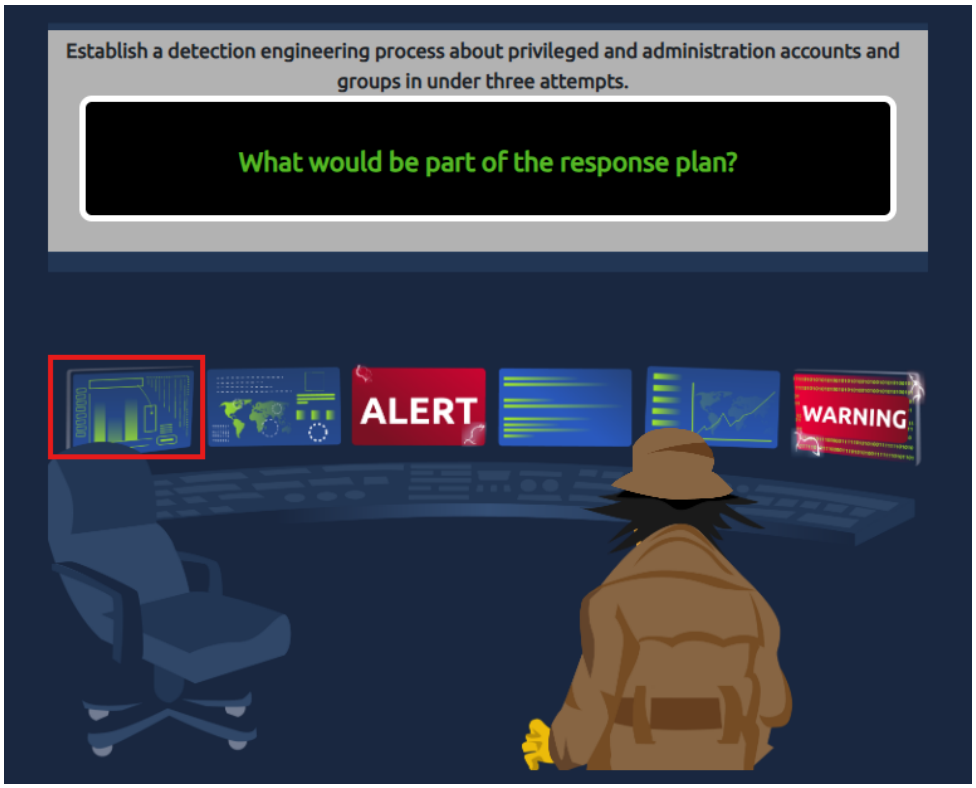


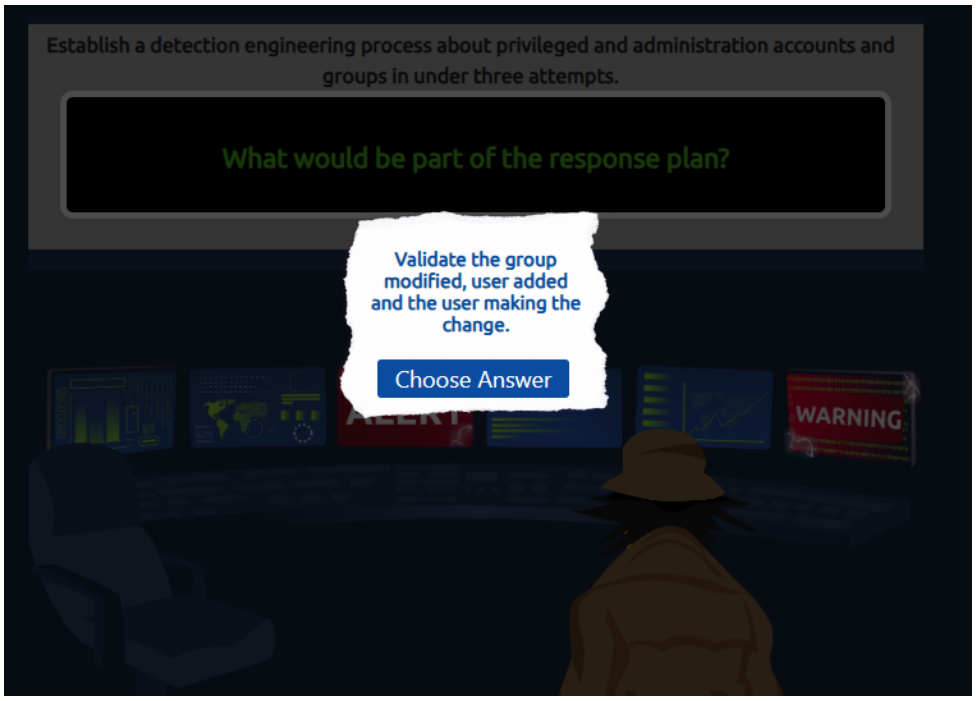




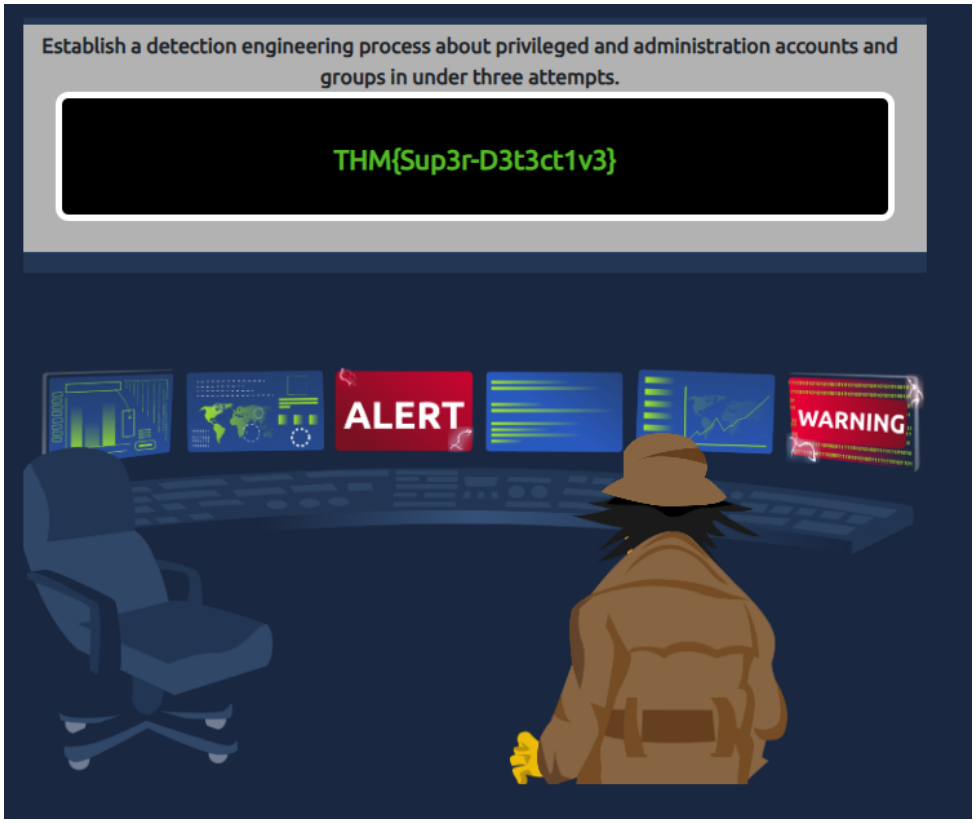
Después de encontrar la respuesta, pasamos a seleccionar la siguiente respuesta.


Establish a detection engineering process about privileged and administration accounts and groups in under three attempts.
What would be part of the response plan?
ALERT
WARNING


Establish a detection engineering process about privileged and administration accounts and groups in under three attempts.
What would be part of the response plan?
ALERT
WARNING



Al finalizar, nos mostrara la flag para completar la tarea.



Respuesta: THM{Sup3r-D3t3ct1v3}

3. Conclusión sobre la Sala

Una vez que finalizamos la sala, hemos logrado aprender los principios esenciales de la ingeniería de detección, incluyendo los distintos tipos de detección, metodologías para desarrollarlas y los marcos conceptuales que permiten estructurar y categorizar amenazas de manera efectiva.