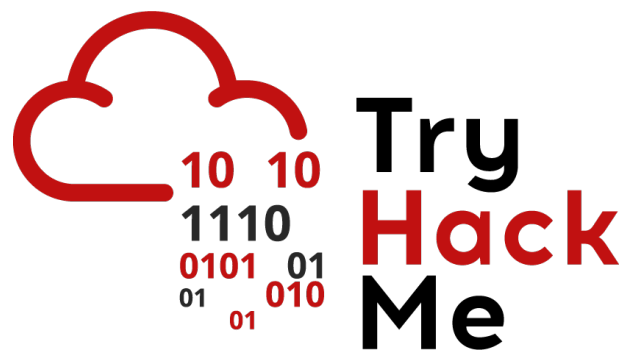


Writeup: Sala *Introduction to SIEM*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción	2
2. Sala	2
2.1. Tarea 1 – Introducción	2
2.2. Tarea 2 - Visibilidad de la red a través del SIEM	2
2.3. Tarea 3 - Fuentes de registro e ingestión de registros	3
2.4. Tarea 4 - ¿Por qué SIEM?	3
2.5. Tarea 5 - Análisis de registros y alertas	3
2.6. Tarea 6 - Trabajo de Laboratorio	4
2.7. Tarea 7 - Conclusión	8
3. Conclusión sobre la Sala	8

1. Introducción

Esta sala está orientada a quienes inician en el uso del **SIEM (Security Information and Event Management)**, fundamental para la detección y gestión de incidentes en entornos corporativos. Aprenderemos qué es un SIEM, cómo se obtiene visibilidad de red mediante logs, de dónde provienen esos registros, cómo se procesan y se analizan mediante reglas de correlación.

2. Sala

2.1. Tarea 1 – Introducción

Aprenderemos que es **SIEM (Security Information and Event Management)**, la cual es una plataforma que centraliza, normaliza y correlaciona eventos y registros provenientes de distintos sistemas para detectar amenazas en tiempo real.

Una vez entendemos que es el SIEM, podemos pasar a responder la siguiente pregunta.

Pregunta: What does SIEM stand for?

Respuesta: **Security Information and Event Management system**

2.2. Tarea 2 - Visibilidad de la red a través del SIEM

Conoceremos la importancia de la visibilidad de red, diferenciando entre fuentes host-centradas (logs de sistema, procesos, PowerShell, Sysmon, etc.) y network-centradas (tráfico SSH, HTTP(S), VPN, FTP). También, se destaca cómo la correlación de ambas mejora del monitoreo y la detección.

Después de comprender este punto, podemos pasar a responder las siguientes preguntas:

Pregunta: Is Registry-related activity host-centric or network-centric?

Respuesta: **host-centric**

Pregunta: Is VPN related activity host-centric or network-centric?

Respuesta: **network-centric**

2.3. Tarea 3 - Fuentes de registro e ingestión de registros

En esta tarea vamos a aprender como se detallan los dispositivos que generan logs (Windows con Event Viewer, Linux en /var/log/..., servidores web) y los métodos de ingestión hacia el SIEM como agentes/forwarders, syslog, carga manual y escucha por puerto

Ahora que logramos comprender el tema de los registros, procedemos a responder la siguiente pregunta.

Pregunta: In which location within a Linux environment are HTTP logs stored?

Respuesta: `/var/log/httpd`

2.4. Tarea 4 - ¿Por qué SIEM?

Aprenderemos sobre el rol esencial del SIEM en correlacionar eventos de múltiples fuentes para detectar comportamiento anómalo, generar alertas y facilitar una respuesta rápida, posicionándose como componente crucial en un SOC.

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

2.5. Tarea 5 - Análisis de registros y alertas

Vamos a aprender cómo el SIEM aplica reglas de correlación para generar alertas. Se presenta el uso de paneles (dashboards) para monitoreo, y se describe el flujo típico de investigación por un analista SOC:

- **Evaluación de event**
- **Clasificación (falso positivo o incidente real)**
- **Ajuste de reglas**
- **Activación de medidas de respuesta**

Después de entender el análisis de registros y alertas, pasamos a responder las siguientes preguntas.

Pregunta: Which Event ID is generated when event logs are removed?

Respuesta: **104**

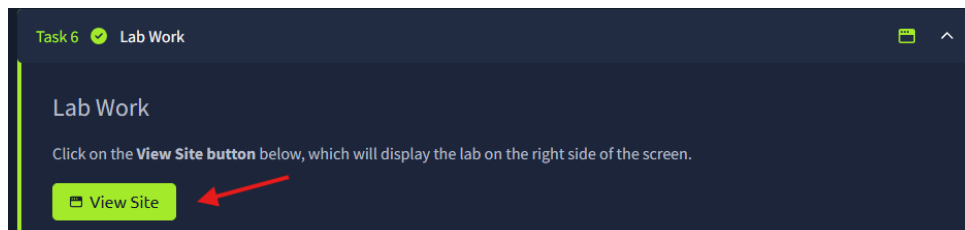
Pregunta: What type of alert may require tuning?

Respuesta: **False Alarm**

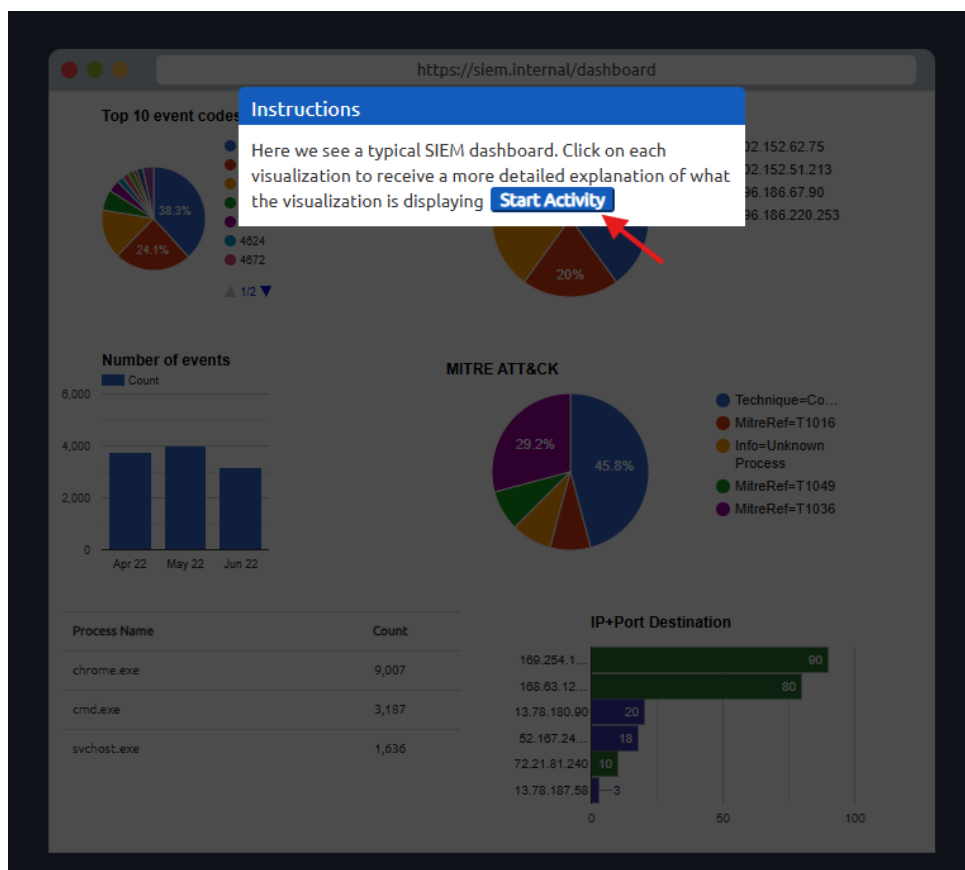
2.6. Tarea 6 - Trabajo de Laboratorio

Ahora llevaremos a cabo un laboratorio práctico donde debemos identificar qué proceso generó una alerta, investigar el usuario y el host implicado, determinar si es falso o verdadero positivo, y extraer la flag correspondiente en base al análisis realizado.

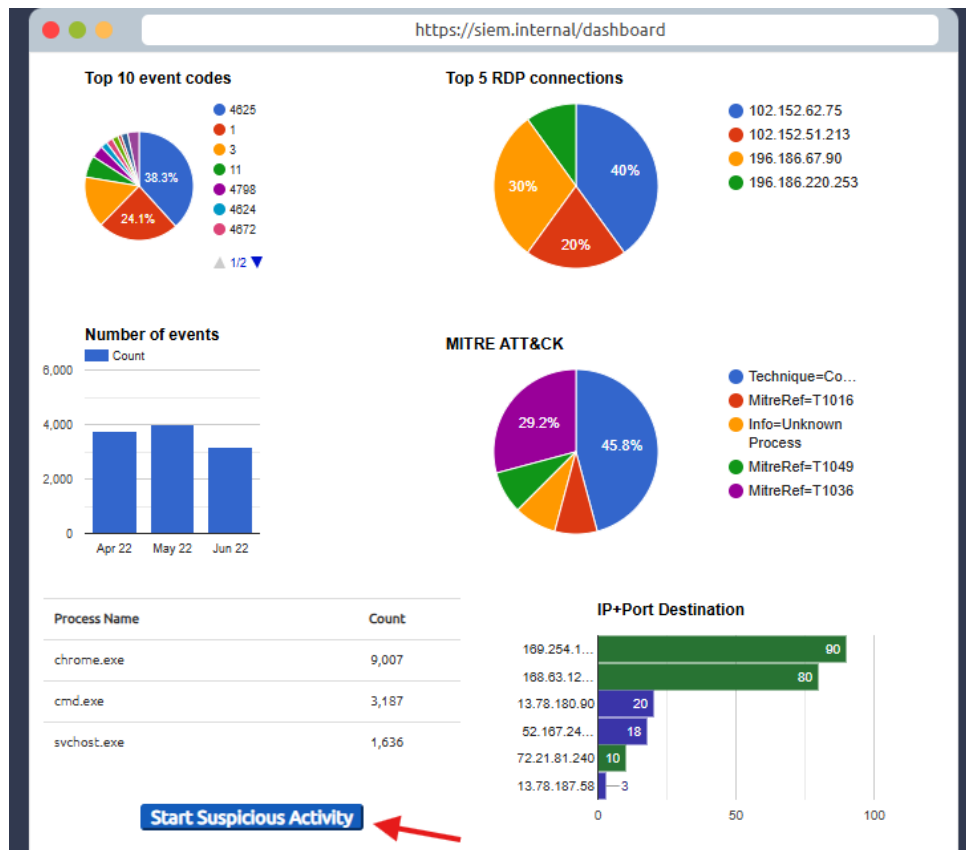
Para empezar, debemos desplegar el sitio donde realizaremos la práctica, para ello, vamos al lado superior del sitio y haremos clic en **View Site**.



Una vez desplegado el sitio, haremos clic en **Start Activity**



Después, haremos clic en **Start Suspicious Activity**



Pregunta: Click on Start Suspicious Activity, which process caused the alert?

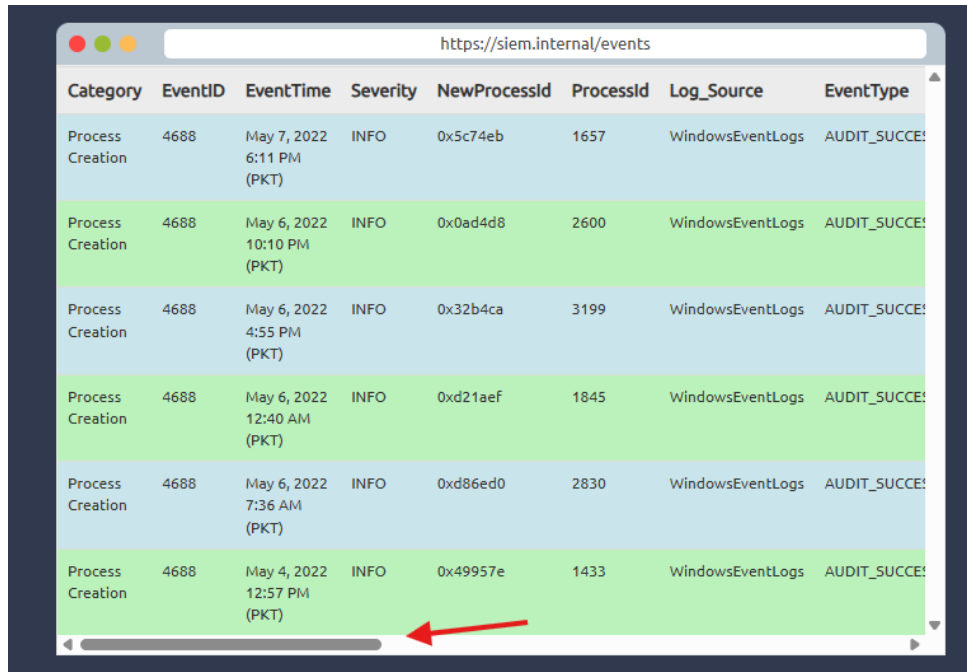
Simplemente echaremos un vistazo a los nombres de los procesos y nos daremos cuenta cual es el proceso que esta causando la alerta.

Process Name	Count
chrome.exe	9,007
cmd.exe	3,187
svchost.exe	1,636
cudominer.exe	1

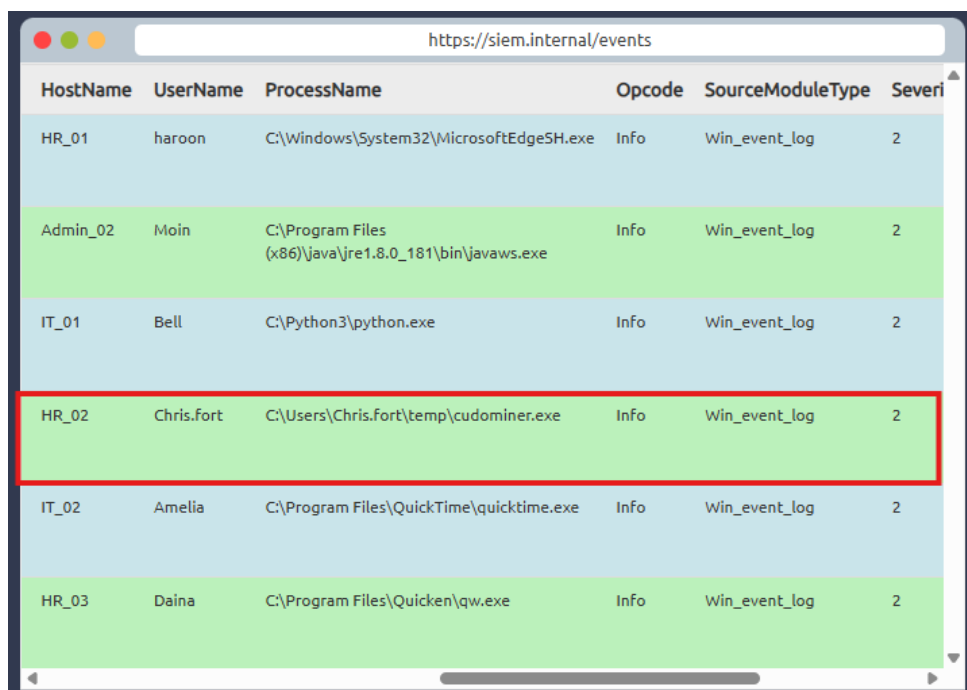
Respuesta: cudominer.exe

Pregunta: Find the event that caused the alert, which user was responsible for the process execution?

A continuación, haremos clic en el proceso que nos alerta y pasaremos al siguiente escenario donde vamos a buscar al responsable de la ejecución del proceso. Una vez en el nuevo escenario, vamos a utilizar el scroll lateral para ubicarnos en la sección de **UserName** y encontrar al responsable.



Category	EventID	EventTime	Severity	NewProcessId	ProcessId	Log_Source	EventType
Process Creation	4688	May 7, 2022 6:11 PM (PKT)	INFO	0x5c74eb	1657	WindowsEventLogs	AUDIT_SUCCE
Process Creation	4688	May 6, 2022 10:10 PM (PKT)	INFO	0x0ad4d8	2600	WindowsEventLogs	AUDIT_SUCCE
Process Creation	4688	May 6, 2022 4:55 PM (PKT)	INFO	0x32b4ca	3199	WindowsEventLogs	AUDIT_SUCCE
Process Creation	4688	May 6, 2022 12:40 AM (PKT)	INFO	0xd21aef	1845	WindowsEventLogs	AUDIT_SUCCE
Process Creation	4688	May 6, 2022 7:36 AM (PKT)	INFO	0xd86ed0	2830	WindowsEventLogs	AUDIT_SUCCE
Process Creation	4688	May 4, 2022 12:57 PM (PKT)	INFO	0x49957e	1433	WindowsEventLogs	AUDIT_SUCCE



HostName	UserName	ProcessName	Opcode	SourceModuleType	Severi
HR_01	haroon	C:\Windows\System32\MicrosoftEdgeSH.exe	Info	Win_event_log	2
Admin_02	Moin	C:\Program Files (x86)\java\jre1.8.0_181\bin\javaws.exe	Info	Win_event_log	2
IT_01	Bell	C:\Python3\python.exe	Info	Win_event_log	2
HR_02	Chris.fort	C:\Users\Chris.fort\temp\cudominer.exe	Info	Win_event_log	2
IT_02	Amelia	C:\Program Files\QuickTime\quicktime.exe	Info	Win_event_log	2
HR_03	Daina	C:\Program Files\Quicken\qw.exe	Info	Win_event_log	2

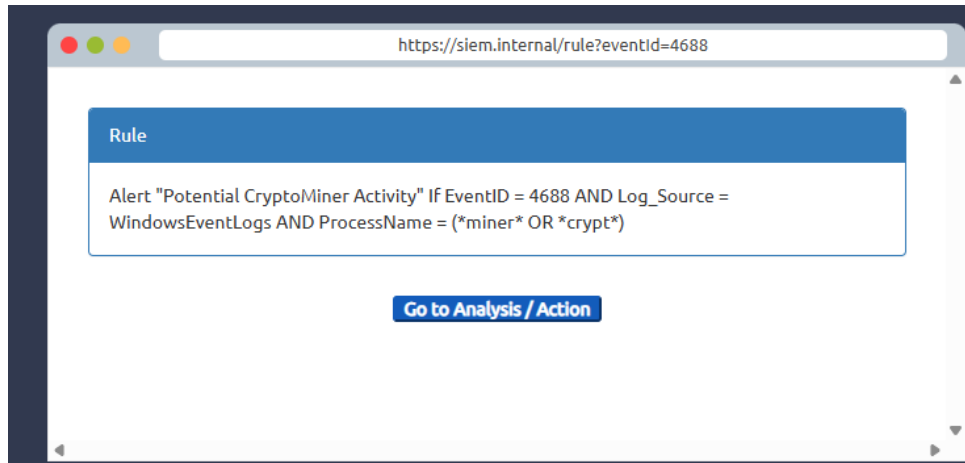
Respuesta: **chris.fort**

Pregunta: What is the hostname of the suspect user?

Respuesta: **HR_02**

Pregunta: Examine the rule and the suspicious process; which term matched the rule that caused the alert?

Haremos clic en el proceso de Chris.fort para continuar y poder averiguar el término que coincidió con la regla que salto la alerta.

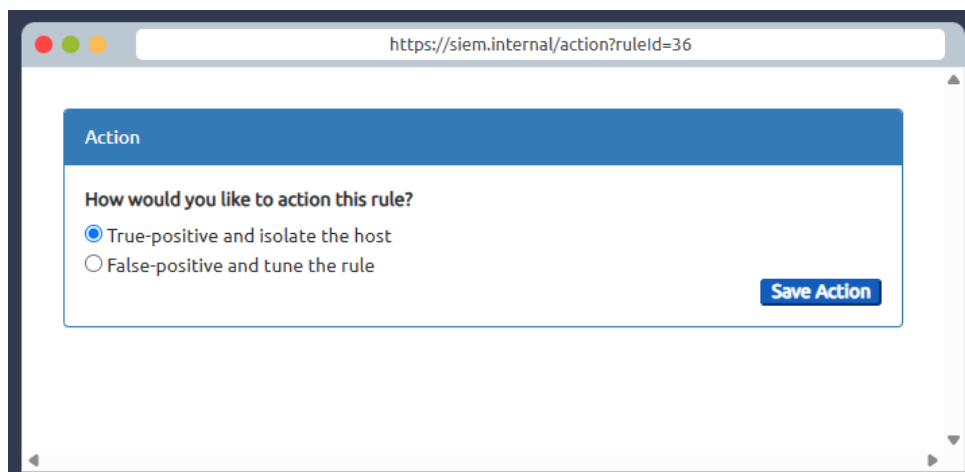


Respuesta: miner

Pregunta: What is the best option that represents the event? Choose from the following:

- False-Positive
- True-Positive

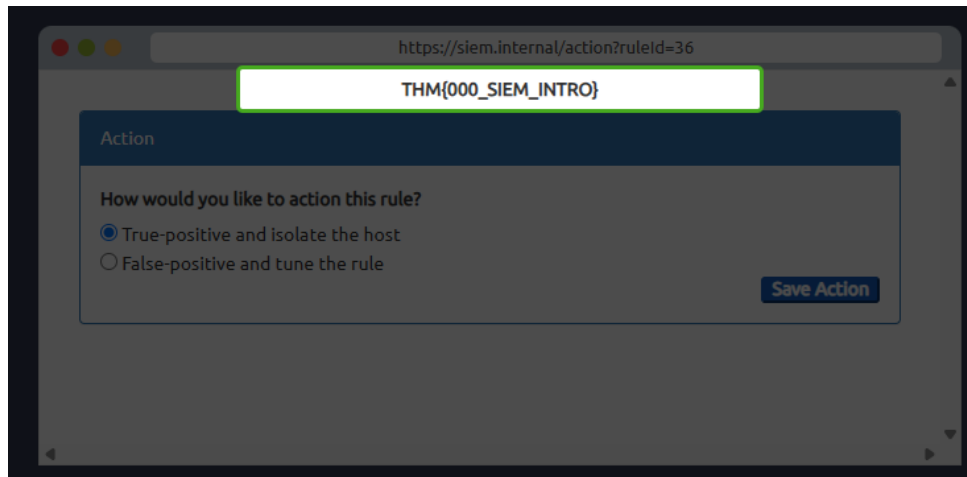
Haremos clic en [Go to Analyst / Action](#) para continuar y seleccionaremos la mejor opción que representa este evento.



Respuesta: True-Positive

Pregunta: Selecting the right ACTION will display the FLAG. What is the FLAG?

Ahora haremos clic en [Save Action](#) y lograremos obtener la flag para completar la tarea.



Respuesta: **THM{000_SIEM_INTRO}**

2.7. Tarea 7 - Conclusión

Esta última tarea nos comenta sobre esta introducción sólida al SIEM donde aprendimos qué es, cómo recoge y correlaciona logs, por qué es fundamental, cómo analizar alertas y cómo aplicar estos conocimientos con un ejercicio práctico.

3. Conclusión sobre la Sala

Al finalizar logramos comprender la utilidad del SIEM en la seguridad empresarial, sabiendo cómo se recopilan, almacenan y analizan los eventos del sistema y la red para detectar actividades sospechosas. Además, exploramos sus componentes principales, las fuentes de datos y el papel que cumple un analista al investigar alertas.