



CREACIÓN LABORATORIO SIEM

José Luis Torres Arana

Introducción a los SIEM

Un **SIEM** (Security Information and Event Management) es una solución de seguridad que ayuda a las organizaciones a reconocer y gestionar posibles amenazas y vulnerabilidades antes de que perturben su actividad.

Un **SOC** (Security Operation Center) es un equipo de profesionales de seguridad dedicados a monitorizar toda la infraestructura informática de una organización. Su misión es la de detectar, analizar y responder a incidentes de seguridad en tiempo real.

Hoy en día, los SIEM se han convertido en un componente esencial de los SOC (Security Operation Center)

Todas las soluciones SIEM realizan algún tipo de agregación, consolidación y clasificación de datos para identificar amenazas y cumplir requisitos de conformidad de datos.

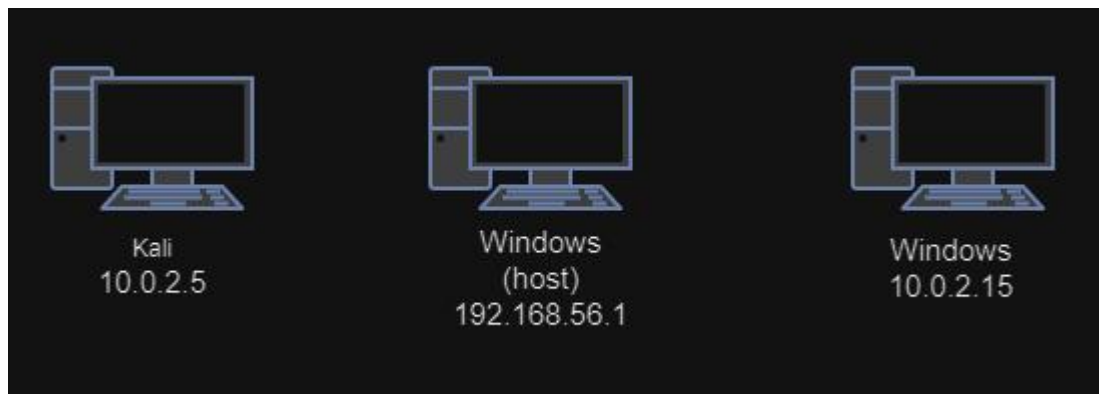
Con el uso de SIEM, podemos destacar como **ventajas**:

Vista centralizada de amenazas
Capacidad de aplicar inteligencia avanzada sobre amenazas
Reconocimiento de amenazas en tiempo real
Mejora de la eficiencia organizativa
Evaluación e informes de cumplimiento normativo
Detección de amenazas avanzadas y desconocidas
Mayor transparencia a la hora de la supervisión de una organización
Automatización
Investigaciones digitales
Supervisión de usuarios y aplicaciones

Explicación laboratorio

Para esta simulación de SIEM, aprovecharemos el free trial del servicio SIEM de Elastic.

Primero, configuramos una máquina virtual Kali, con IP 10.0.2.5, una máquina Windows, con IP 10.0.2.15 y, por último, también configuraremos la máquina host (Windows), que cuenta con la IP 192.168.56.1.



Estos tres equipos que componen nuestra red han sido configurados dentro de la misma **Política de Agentes (Agent policy)**.

Una política de agentes es una colección de entradas y configuraciones mediante las cuales configuramos los datos que queremos que sean recolectados por un agente. De manera que, al estar los 3 equipos bajo la misma política, todas las reglas que configuremos se aplicarán a todos por igual.

El uso de una política de agentes tiene varias ventajas, como por ejemplo:

- Aplicar configuraciones a un determinado conjunto de hosts.
- Permite mantener la flexibilidad en grandes implantaciones ya que los cambios pueden ser probados rápidamente antes de ser implantados.
- Proporciona una forma de agrupar y gestionar grandes infraestructuras.

Algunos ejemplos de usos de políticas podría ser agrupar los diferentes hosts según el sistema operativo que tengan (por ejemplo una política para los equipos Windows, otra para los Linux...). También se podría agrupar según la función que cumpla el host (como work-stations, servidores...).

El agente de Elastic se encarga de añadir supervisión de registros, métricas y otros tipos de datos a un host. También añade protección frente a amenazas de seguridad, consulta datos de los sistemas operativos, reenvía datos de servicios... Cada agente que instalemos solo puede tener una política de agentes.

Para añadir los equipos del laboratorio a la política, debemos primero instalar el agente en cada uno.

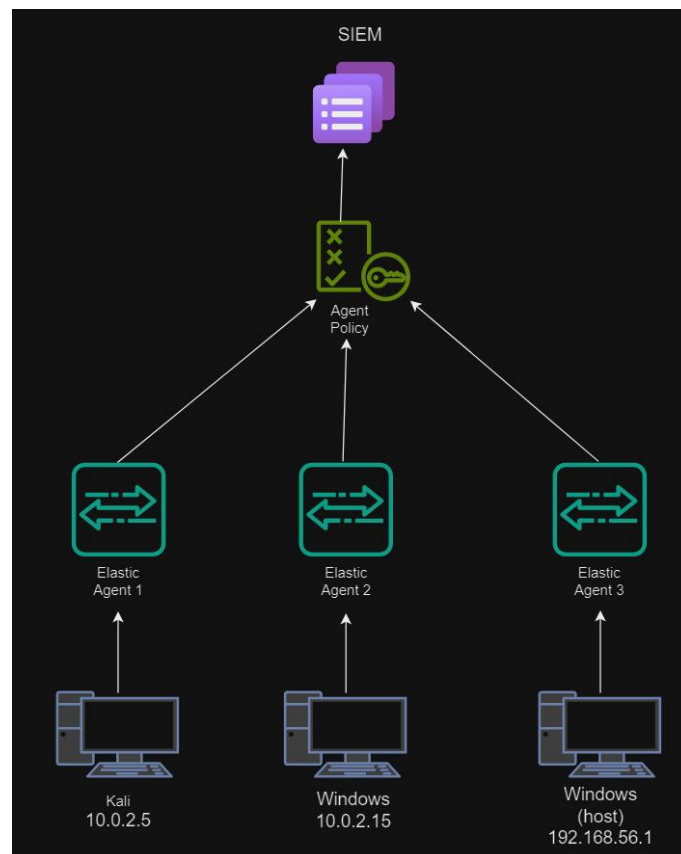
En el caso de la máquina Kali, usaremos la siguiente sintaxis para instalar el agente:

```
~ curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.15.4-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.15.4-linux-x86_64.tar.gz
cd elastic-agent-8.15.4-linux-x86_64
sudo ./elastic-agent install --url=https://f5ed97a074764f1bbafc6c375eb7aec8.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=Tk4zTUhKTUJoaVlTeHEyNVJHThg6RDRQanBwR0VUOWEyZ1k3REstX2pHQQ==
```

Luego, en el caso de las dos máquinas windows, la sintaxis que usaremos para instalarlo será:

```
PS C:\WINDOWS\system32> $ProgressPreference = 'SilentlyContinue'
>> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.15.4-windows-x86_64.zip -OutFile elastic-agent-8.15.4-windows-x86_64.zip
>> Expand-Archive .\elastic-agent-8.15.4-windows-x86_64.zip -DestinationPath .
>> cd elastic-agent-8.15.4-windows-x86_64
>> .\elastic-agent.exe install --url=https://f5ed97a074764f1bbafc6c375eb7aec8.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=Tk4zTUhKTUJoaVlTeHEyNVJHThg6RDRQanBwR0VUOWEyZ1k3REstX2pHQQ==
```

La red quedaría configurada de la siguiente forma:



Showing 3 agents [Clear filters](#) ● Healthy 2 ● Unhealthy 0 ● Updating 0 ● Offline 1 ● Inactive 0 ● Unenrolled 0

<input type="checkbox"/>	Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
<input type="checkbox"/>	Offline	DESKTOP-JCEFOM4	Agent policy test rev. 3	N/A	N/A	last week	8.15.4	...
<input type="checkbox"/>	Healthy	PC-Selu	Agent policy test rev. 3	0.14 %	201 MB	12 seconds ago	8.15.4	...
<input type="checkbox"/>	Healthy	kali	Agent policy test rev. 3	0.87 %	209 MB	11 seconds ago	8.15.4	...

Una vez tenemos las 3 máquinas configuradas y conectadas, el siguiente paso es comprobar que las máquinas pueden conectarse correctamente con el SIEM.

Para ello nos iremos al apartado Logs dentro del menú Observability. En este apartado, veremos un historial de los logs (o registros) que ha ido recolectando el agente que hemos instalado.

En este caso, para simplificar, nos centraremos en la máquina Kali. Así que el siguiente paso será filtrar los logs para que solo nos muestre los que nos interesan. Lo conseguiremos con la condición *"host.name: kali"*

actions	@timestamp	resource	content
<input type="checkbox"/>	Nov 18, 2024 @ 20:15:09.663	kali	Endpoint process event
<input type="checkbox"/>	Nov 18, 2024 @ 20:15:09.659	kali	Endpoint process event
<input type="checkbox"/>	Nov 18, 2024 @ 20:15:09.650	kali	Endpoint process event
<input type="checkbox"/>	Nov 18, 2024 @ 20:15:08.885	kali	Endpoint process event
<input type="checkbox"/>	Nov 18, 2024 @ 20:15:08.885	kali	Endpoint process event
<input type="checkbox"/>	Nov 18, 2024 @ 20:15:08.885	kali	Endpoint process event
<input type="checkbox"/>	Nov 18, 2024 @ 20:15:08.884	kali	Endpoint process event
<input type="checkbox"/>	Nov 18, 2024 @ 20:15:08.884	kali	Endpoint process event
<input type="checkbox"/>	Nov 18, 2024 @ 20:15:08.881	kali	Endpoint process event
<input type="checkbox"/>	Nov 18, 2024 @ 20:15:08.880	kali	Endpoint process event
<input type="checkbox"/>	Nov 18, 2024 @ 20:15:08.877	kali	Endpoint process event
<input type="checkbox"/>	Nov 18, 2024 @ 20:15:08.875	kali	Endpoint process event
<input type="checkbox"/>	Nov 18, 2024 @ 20:15:08.874	kali	Endpoint process event

Podemos observar que, sin realizar ninguna acción en la máquina, se nos han creado varias entradas. En cada una de ellas tenemos las siguientes columnas:

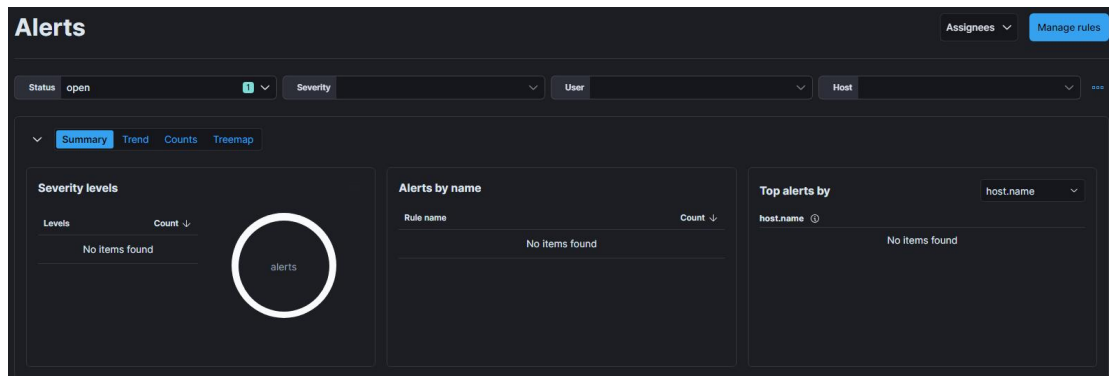
- **Actions:** nos indica distintas acciones que podemos realizar con el log seleccionado.

Si le damos a la primera opción, se nos abrirá otra ventana que nos da una información más detallada del registro. En esta nueva ventana nos sale información sobre el evento en cuestión (id del evento, id del agente que ha capturado el evento, versión del agente, tipo de evento...), información sobre la máquina (sistema operativo, IP, arquitectura...) e información sobre el proceso que se está llevando a cabo en el evento.

- **Timestamp:** esta columna representa la fecha y hora en las que el evento ha ocurrido.
- **Resource:** nos muestra diferente información acerca de la fuente de la que proviene el evento (host.name, service.name, cloud.instance.id...).
- **Content:** representa el log.level y el mensaje del evento que está ocurriendo.

Una vez hayamos comprobado que tenemos los 3 equipos bien conectados al SIEM, el siguiente paso será crear las **alertas**.

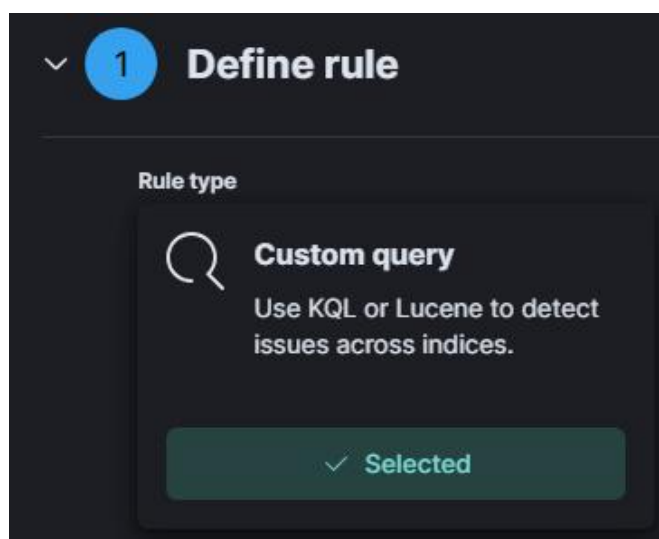
Para crearlas, lo primero que tenemos que hacer es irnos al apartado de alertas de Elastic:

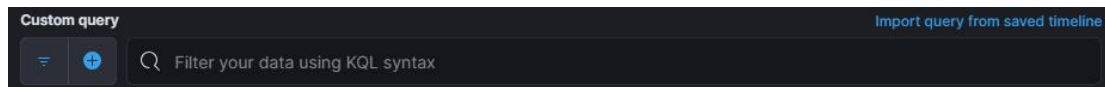


Este panel proviene de Kibana, la cual es una herramienta diseñada para explorar, visualizar y crear un panel de control sobre los datos de registros almacenados por Elasticsearch.

Le damos a “Manage rules” y a crear una nueva regla, la cual determinará qué condiciones se tendrán que dar para que salte la alerta de dicha regla.

El primer paso será definir qué tipo de regla vamos a configurar, en nuestro caso elegiremos “Custom query”, lo que nos permitirá personalizar la regla completamente.





En este apartado, deberemos indicar mediante qué campo y qué valor saltará la alerta.

La primera alerta que crearemos será un detector de ejecución de comando “**whoami**”. Este comando está tanto en Linux como en Windows, y sirve para indicar qué usuario ha iniciado sesión en ese momento en ese equipo.

Este comando hay que tenerlo muy en cuenta porque suele ser el primer comando que se ejecuta una vez un atacante consigue acceso a una máquina, para hacer un reconocimiento del sistema.

La sintaxis usada en la custom query será:

process.args: “whoami”

En este caso el campo seleccionado sería *process.args* y el valor que buscamos sería *whoami*

El siguiente paso será rellenar información adicional sobre la regla. En este paso debemos ser claros para que otros usuarios del SIEM comprendan correctamente la función de la regla.

En este laboratorio no tiene mucha importancia ya que yo soy el único usuario. Pero en una organización con más usuarios que tengan acceso es importante que todo el mundo comprenda la regla.

2 About rule

Name
Whoami Command Detection

Description
This rule detects the execution of the whoami command on a monitored system.

Default severity
Select a severity level for all alerts generated by this rule.
Low

☐ Severity override
Use source event values to override the default severity.

Default risk score
Select a risk score for all alerts generated by this rule.
0 25 50 75 100 21

☐ Risk score override
Use a source event value to override the default risk score.

Tags
whoami × detection ×

Optional

Otro aspecto clave que podemos incluir en las alertas son las tácticas y las técnicas de **MITRE ATT&CK**.

El marco MITRE ATT&CK es una base de conocimientos, actualizada continuamente y accesible para todo el mundo, que es utilizada para modelar, detectar, prevenir y combatir amenazas de ciberseguridad basándose en el comportamiento conocido de los ciberdelicuentes.

Dentro de este marco, nos encontramos con tácticas y con técnicas.

- Las tácticas representan un objetivo concreto, algo que el atacante quiere conseguir. Suelen corresponder con las fases de un ataque.
- Las técnicas en cambio representan la forma en que intentan lograrlo.

Tácticas	
Reconocimiento	Desarrollo de recursos
Acceso inicial	Ejecución
Persistencia	Aumento de privilegios
Evasión de defensa	Acceso con credenciales
Descubrimiento	Movimiento lateral
Recopilación	Comando y Control
Exfiltración	Impacto

En el caso de la alerta que estamos creando para la ejecución del comando whoami, podemos llegar a la conclusión de que pertenece a la táctica de Descubrimiento (Discovery).

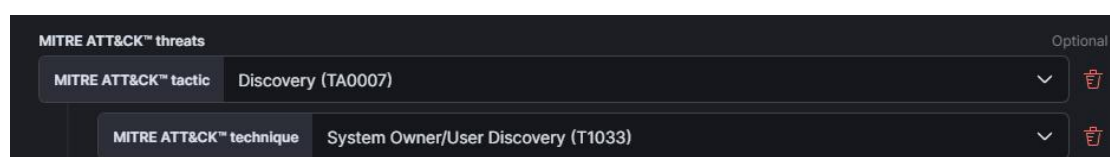
Si investigamos en la propia página de MITRE, veremos que esta consiste en técnicas que un atacante o adversario puede utilizar para obtener conocimiento sobre el sistema y/o sobre la red interna.

Es una parte importante porque es la que les ayuda a orientarse para decidir cómo actuar.

Como técnica, si acudimos a la página del MITRE vemos una lista con diferentes técnicas.

Atendiendo a todas las descripciones de las técnicas, elegiremos:

T1033	System Owner/User Discovery	Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using OS Credential Dumping . The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from System Owner/User Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
-------	--------------------------------	--



El siguiente paso es determinar cada cuanto se ejecutará la regla. En este caso, el periodo de tiempo que le marquemos será el tiempo en el que se detectarán alertas. Para whoami lo establecemos en 5 minutos.

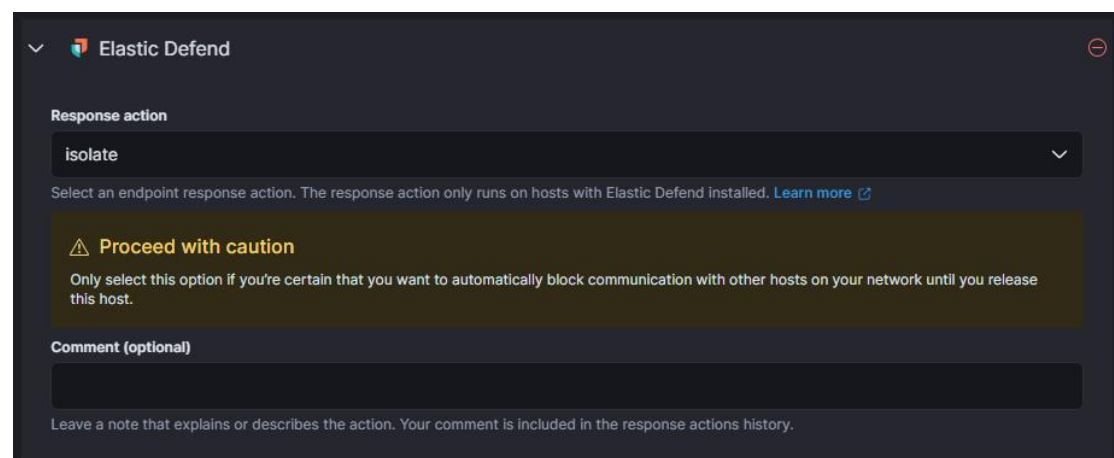
Por último, tenemos que indicar la acción que se llevará a cabo cuando se detecte la alerta.

Estableceremos que, cada vez que ocurra la alerta, se le notifique al administrador vía email.

El cuerpo que pondremos en el mensaje será: *Rule “Whoami Command Detection” generated {{state.signals_count}} alerts.*

El argumento que le estamos indicando se sustituirá con el número de alertas cuando se genere el mensaje.

Otra acción que se llevará a cabo será el aislamiento del host en el que ha ocurrido la alerta. Este aislamiento se llevará a cabo mediante la integración Elastic Defend, y su objetivo es que se bloqueen las comunicaciones entre el host afectado y el resto de la red interna.



Response action

isolate

Select an endpoint response action. The response action only runs on hosts with Elastic Defend installed. [Learn more](#)

⚠ Proceed with caution

Only select this option if you're certain that you want to automatically block communication with other hosts on your network until you release this host.

Comment (optional)

Leave a note that explains or describes the action. Your comment is included in the response actions history.

Una vez hemos configurado todos los campos, le daremos a guardar configuración y a activar regla.

A partir de ahora, cada vez que se ejecute el comando, nos aparecerá una alerta en nuestro dashboard.

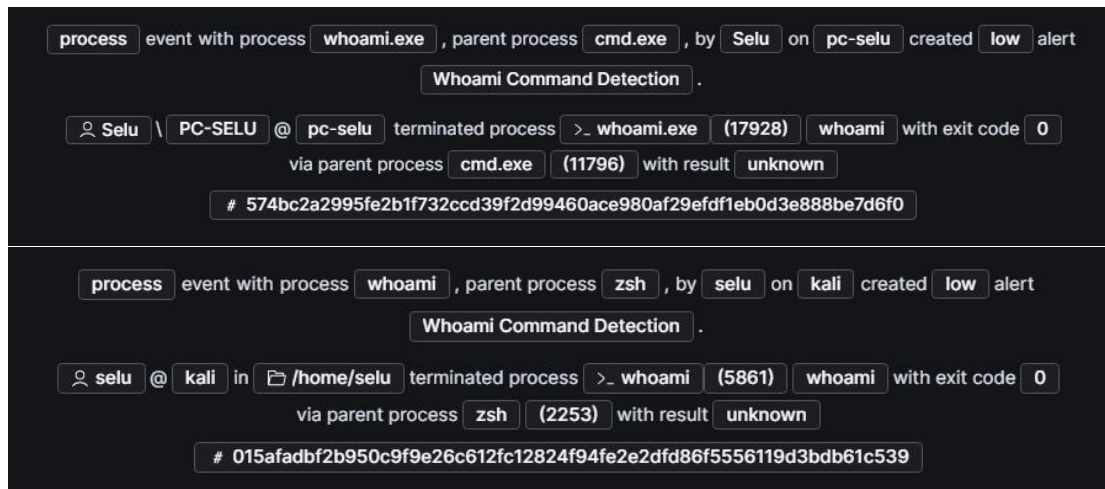
Ahora, pondremos a prueba la alerta creada ejecutando el whoami tanto en una de las máquinas windows y en la kali.

Una vez ejecutados ambos, podemos comprobar que se ha creado una alerta en el dashboard:

Rule name	Last alert	Alert count
Whoami Command Detection	4 seconds ago	4

En ella, se nos indica que han saltado 4 alertas en total de la regla que acabamos de crear.

En los detalles de cada alerta aparece:



La primera de las imágenes corresponde al mensaje que nos ha dado el equipo con sistema operativo Windows, mientras que la segunda imagen corresponde al equipo con Linux.

Podemos observar ciertas diferencias entre ambas, como por ejemplo el “parent process”. En windows, el proceso proviene del “cmd.exe” mientras que en Linux proviene de “zsh”, ambos intérpretes de comandos de windows y de linux, respectivamente.

Como respuesta y mitigación, tomaremos las siguientes medidas:

- Revisión de logs: para comprobar si el comando fue ejecutado en combinación con otros comandos (como *id*, *net user*, *hostname...*) para identificar si forma parte de un posible reconocimiento.
- Correlación de eventos: analizando si hay otros indicadores de compromiso (IoC) en el sistema, como intentos de escala de privilegios, creación o modificación de cuentas o conexiones remotas sospechosas.
- Restricción de comandos: para limitar el uso de comandos innecesarios en entornos críticos o incluso deshabilitar el acceso a shells interactivos para cuentas sin privilegios administrativos.

Otra alerta que podemos configurar es para los **intentos fallidos de inicio de sesión**. La regla que utilizaremos en este caso será del tipo “Threshold”. Este tipo de regla se basa en un número de logs que se reciben de una fuente de datos en un período de tiempo determinado.

Custom query	event.code:4625
Rule type	Threshold
Timeline template	None
Threshold	Results aggregated by user.name >= 3

Como query utilizaremos: *event.code:4625*.

El código 4625 documenta todo intento fallido de inicio de sesión en el equipo local. En cambio, el 4624 es el que documenta los intentos exitosos de inicio de sesión. Esta alerta solo nos servirá para el equipo con sistema operativo Windows.

En el apartado Threshold, estamos indicando que se deben filtrar los logs que contengan el código de evento 4625 y que filtre dichos logs con el nombre de usuario. Establecemos que, si dicho nombre de usuario se repite 3 o más veces, se activará la alerta.

Esta alerta puede tener varios falsos positivos, como pueden ser:

- Autenticación mal configurada o credenciales obsoletas.
- La contraseña de la cuenta de servicios puede estar caducada y dar error.
- Problemas de infraestructura caída.

En esta regla habría que tener en cuenta que, según la cuenta que esté afectada por esta alerta, hay que darle una mayor o menor importancia. Puede que la cuenta que ha activado la alerta sea una cuenta con privilegios administrativos o que sea crítica. Otro aspecto a investigar sería el de si los intentos son desde internet, o son de manera local.

Al igual que en la regla anterior, configuraremos que, cada vez que se genere una alerta, se envíe un email al administrador indicando las veces que se ha generado la alerta.

En cuanto al MITRE ATT&CK, esta regla queda recogida en la táctica: **Credential Access (TA0006)**.

Esta táctica recoge diferentes técnicas para robar credenciales (nombres de usuario y contraseñas).

De entre las técnicas, este caso sería una **Brute Force (T1110)**.

La fuerza bruta consiste en, sistemáticamente, intentar adivinar la contraseña utilizando un mecanismo repetitivo o iterativo. Básicamente el atacante va comprobando una serie de contraseñas que tenga en una base de datos o diccionario con el usuario que haya descubierto.

Al ser un procedimiento repetitivo, es fácil que se genere esta alerta en cuanto comienza la fuerza bruta.

Como subtécnica, hemos indicado:

- **T1110.001 Password Guessing.**
- **T1110.003 Password Spraying.**

About

Detects if a user makes 3 failed attempts to login into the system.

Severity	● Low
Risk score	47
Reference URLs	<ul style="list-style-type: none"> • https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4625 • https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4624 • https://serverfault.com/questions/379092/remote-desktop-failed-logon-event-4625-not-logging-ip-address-on-2008-terminal-s/403638#403638
MITRE ATT&CK™	Credential Access (TA0006) <ul style="list-style-type: none"> └ Brute Force (T1110) <ul style="list-style-type: none"> └ Password Guessing (T1110.001) └ Password Spraying (T1110.003)
Max alerts per run	100

Como respuesta y mitigación estableceremos las siguientes medidas:

- Aislar el host afectado para prevenir vulnerabilidades posteriores.
- Si el equipo está expuesto a internet con RDP (Remot Desktop Protocol) o algún otro servicio, restringir el acceso a dicho activo. Si no fuera posible, habría que limitar el acceso al servicio para algunas direcciones IP en concreto, mediante firewall.
- Investigar qué credenciales se han podido exponer o han sido utilizadas por el atacante para asegurar todas las cuentas que han podido ser comprometidas. Estas contraseñas habría que reestablecerlas.
- Ejecutar un análisis completo en busca de malware, para comprobar que no se ha dejado ningún mecanismo de persistencia en el sistema.
- Por último, actualizar las políticas de registro y auditoría para mejorar el MTDD (Tiempo medio de detección) y el MTTR (Tiempo medio de respuesta).

En conclusión, una vez hemos comprobado que estas dos reglas funcionan, ya tendríamos el SIEM creado y funcionando con los 3 equipos de nuestra red local. Los siguientes pasos que debemos tomar sería crear otras reglas para detectar las máximas amenazas posibles y remediar las diferentes alertas que se vayan generando.