

# SOC (Security Operations Center)

## Módulo 5 – Herramientas



### SIEM - Ejercicios

Sheila Fernández Cisneros – 02/07/2024

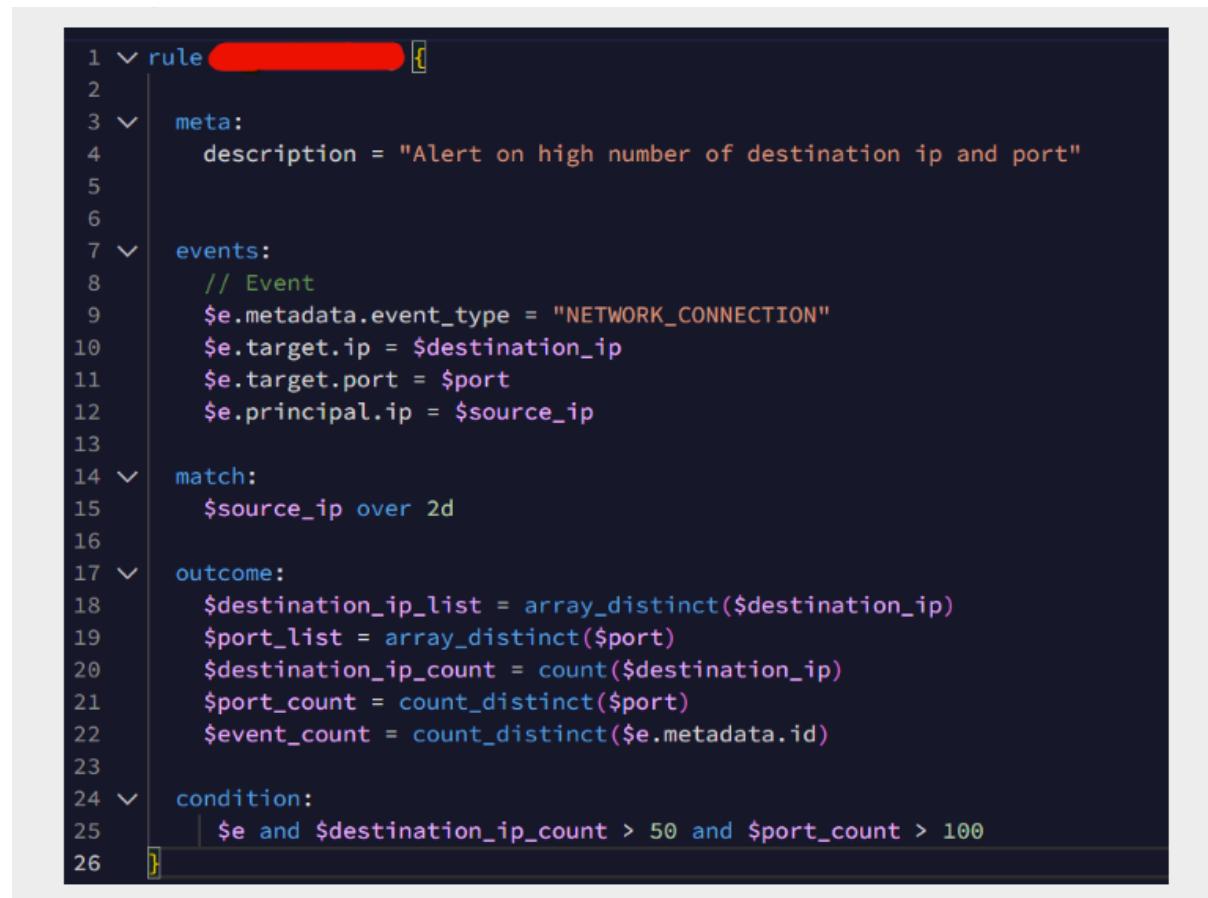
# Ejercicios SIEM ("Security Information and Event Management")

Para poder acceder a los links de los ejercicios es importante tener abierta la demo.<https://demo.backstory.chronicle.security/?warstory=> ó <http://goo.gle/chroniclelab>

## Tarea 1:

En los cursos de SIEM se ha podido observar cómo es el SIEM aportado por Google Chronicle. Estos SIEM (Security Information and Event Management), monitorizan incidentes de seguridad en base a unas determinadas reglas, las cuales, en este caso (Chronicle) están escritas en Yara. Una buena tarea de toma de contacto será echar un ojo a una de las reglas para comprender un poco su funcionamiento.

- ¿Para qué crees que sirve la siguiente regla? Describela a grandes rasgos. Pista: presta especial atención a la ‘condition’.



```
1 ✓ rule [REDACTED] [
2
3   ✓ meta:
4     description = "Alert on high number of destination ip and port"
5
6   ✓ events:
7     // Event
8     $e.metadata.event_type = "NETWORK_CONNECTION"
9     $e.target.ip = $destination_ip
10    $e.target.port = $port
11    $e.principal.ip = $source_ip
12
13   ✓ match:
14     $source_ip over 2d
15
16   ✓ outcome:
17     $destination_ip_list = array_distinct($destination_ip)
18     $port_list = array_distinct($port)
19     $destination_ip_count = count($destination_ip)
20     $port_count = count_distinct($port)
21     $event_count = count_distinct($e.metadata.id)
22
23   ✓ condition:
24     | $e and $destination_ip_count > 50 and $port_count > 100
25
26 ]
```

Construcción de Reglas según la documentación oficial de Chronicle

La regla se construye con hasta 4 secciones clave:

- **meta**
  - Utiliza pares clave-valor arbitrarios para describir la regla.
  - Valores clave para el autor y la severidad están codificados para aparecer en el panel de reglas.
  - Otros valores clave se pueden definir según las necesidades de tu negocio.
- **events**
  - Condiciones de filtro de eventos, similar a una cláusula WHERE.
- **match (opcional)**
  - Describe la ventana de tiempo para una coincidencia, requerida cuando se ejecuta la correlación de múltiples eventos.
- **condition**
  - Describe los eventos que deben coincidir y cualquier agregado.

### Estructura de la regla

Para YARA-L 2.0, se debe especificar las declaraciones de variables, definiciones y usos en el siguiente orden:

- meta
- events
- match (opcional)
- outcome (opcional)
- condition
- options (opcional)

En el caso de que se omita la sección opcional match, la regla puede coincidir con un solo

### Descripción de la regla del ejercicio:

1. **Meta:** permite incluir metadatos adicionales sobre una regla.
  - **description = “Alert on high number of destination ip and port”:** Este campo describe detalles de lo que hace la regla. En este caso significa que la regla está diseñada para generar una alerta cuando se detecta un alto número de conexiones a direcciones IP de destino y puertos. Esto puede ser indicativo de actividades sospechosas o maliciosas, como un escaneo de puertos o intentos de comunicación con muchos servidores diferentes, lo que podría sugerir la presencia de malware o actividad malintencionada en la red.
2. **Events Section:** Esta sección define las condiciones que un evento debe cumplir para ser considerado por la regla. En este caso:

- **\$e.metadata.event\_type** = “NETWORK\_CONNECTION”: Indica que la regla se utiliza para eventos de conexión de red.
- **\$e.target.ip** = \$destination\_ip: La IP destino se almacena en esta variable.
- **\$e.target.port** = \$port: Define el puerto de destino del evento.
- **\$e.principal.ip** = \$source\_ip: Define que la IP de origen del evento.

\$e indica evento.

### 3. Match:

- **\$source\_ip over 2d:** significa que la regla está diseñada para detectar si la dirección IP de origen ha aparecido repetidamente en eventos durante un período de 2 días.

### 4. Outcome:

- **\$destination\_ip\_list** = array\_distinct(\$destination\_ip): “array\_distinct” elimina las Ip duplicadas almacenadas en la variable “destination\_ip”. Con este calculo se almacenan las IP de destino únicas que se han observado en los eventos.
- **\$port\_list** = array\_distinct(\$port): Se eliminan los duplicados de los puertos, almacenándose los valores de puertos únicos.
- **\$destination\_ip\_count** = count(\$destination\_ip): “count” se usa para contar, en este caso el número de IPs destino. Proporciona el número total de veces que las direcciones IP de destino han aparecido.
- **\$port\_count** = count\_distinct(\$port): “count\_distinct” cuenta valores únicos, en este caso, cuenta el número de puertos únicos que se han observado en los eventos.
- **\$event\_count** = count\_distinct(\$e.metadata.id): proporciona el número de eventos distintos basándose en un identificador único de evento.

### 5. Condition:

- **\$e and \$destination\_ip\_count > 50 and \$port\_count > 100:** Esta condición significa que la regla se activará si hay eventos (\$e) y si el número de direcciones IP de destino únicas (\$destination\_ip\_count) es mayor a 50 y el número de puertos únicos (\$port\_count) es mayor a 100.

La sección “outcome” y la sección “condition” utilizan las variables \$e definidas en la sección “events” para realizar cálculos y verificaciones adicionales.

## Conclusión

Esta regla detecta eventos de conexión de red en los que se observan más de 50 direcciones IP de destino y más de 100 puertos únicos en un período de 2 días.

## Propósito de la Regla

Esta regla está diseñada para identificar patrones de tráfico de red que podrían indicar actividad maliciosa o anómala. Específicamente, la regla se centra en detectar conexiones a un gran número de direcciones IP de destino y a una variedad de puertos diferentes dentro de un período de 2 días.

## Tarea 2:

**Análisis de una regla Yara para detección de malware. Para finalizar con el análisis de reglas de este tipo, se presenta la siguiente regla basada en la detección de un determinado tipo de malware en base a las características de un archivo:**

```
rule DetectMalwareSample
{
    meta:
        description = "Detects a specific malware sample based on its file characteristics"
        author = "Tu Nombre"
        date = "2024-06-21"
        hash = "d41d8cd98f00b204e9800998ecf8427e"

    strings:
        $str1 = "malicious_function"
        $str2 = "suspicious_behavior"
        $str3 = { E8 ?? ?? ?? ?? 83 C4 04 }

    condition:
        uint16(0) == 0x5A4D and
        filesize < 200KB and
        ($str1 or $str2 or $str3)
}
```

**¿Cómo debe de ser ese archivo para que sea detectado por la regla? De nuevo fíjate bien en la “condition” e intenta deducir cuáles son estas características.**

Para que un archivo sea detectado por la regla, debe cumplir con las siguientes características.

**Desglose de la “condition”:**

**1. Firma de cabecera:**

- **uint16(0) == 0x5A4D:** Esto comprueba si los primeros 2 bytes del archivo (en la posición 0) contienen el valor hexadecimal 0x5A4D, que corresponde a la firma

“MZ”. Esta firma indica que el archivo es un ejecutable de Windows (formato PE ejecutable). “uint16(offset)” es una función que se utiliza en Yara que siempre lee 2 bytes a partir del offset especificado.

## 2. Tamaño del archivo:

- **filesize < 200KB**: Esto asegura que el tamaño del archivo sea menor de 200 kilobytes.

## 3. Cadenas de caracteres (strings):

- **(\$str1 or \$str2 or \$str3)**: Al menos una de las siguientes cadenas debe estar presente en el archivo:
  - \$str1 = “malicious\_function”
  - \$str2 = “suspicious\_behavior”
  - \$str3 = { E8 ?? ?? ?? ?? 83 C4 04 }: Esta es una secuencia de bytes específica que puede representar una llamada a una función seguida de la instrucción add esp, 4 en ensamblador x86, que es común en ciertos tipos de malware.

## Conclusión

Para que un archivo sea detectado por esta regla Yara, debe cumplir con las siguientes condiciones:

- Debe ser un ejecutable de Windows (que tenga la firma “MZ”).
- Debe tener un tamaño menor de 200 kilobytes.
- Debe contener al menos una de las cadenas o secuencias de bytes especificadas:
  - La cadena "malicious\_function".
  - La cadena "suspicious\_behavior".
  - La secuencia de bytes { E8 ?? ?? ?? ?? 83 C4 04 }.

Si el archivo cumple con todas estas condiciones, la regla Yara lo detectará como un posible malware.

## Explicación Adicional Extra

Personalmente, tengo predilección por el análisis de malware, es por tanto que he investigado esta parte mas en profundidad.

### **uint16(0) == 0x5A4D**

- **uint16(0):**
  - uint16 es una función de Yara que lee un valor de 16 bits (2 bytes) del archivo.

- El parámetro 0 dentro de los paréntesis indica el desplazamiento (offset) desde el inicio del archivo. En este caso, 0 significa que está leyendo desde el byte 0 del archivo.
- **0x5A4D:**
  - 0x5A4D es un valor hexadecimal.
  - Los valores hexadecimales 5A y 4D corresponden a los caracteres ASCII “M” y “Z”, respectivamente.

La secuencia de bytes especificada por \$str3 en la regla Yara se relaciona con instrucciones en ensamblador x86.

### **Secuencia de bytes:**

- $\$str3 = \{ E8 ?? ?? ?? ?? 83 C4 04 \}$
1. **E8:** Esta es la instrucción de llamada a función en ensamblador x86 (CALL).
    - La instrucción CALL en x86 se utiliza para llamar a una función.
    - E8 es el opcode para CALL con un desplazamiento relativo de 32 bits.
  2. **?? ?? ?? ??:** Estos son cuatro bytes comodín (wildcards).
    - Los comodines ?? indican que cualquier valor puede ocupar estos cuatro bytes.
    - En el contexto de la instrucción CALL, estos cuatro bytes representan el desplazamiento relativo de la dirección a la que se está llamando.
  3. **83 C4 04:** Esta es una secuencia de instrucciones que sigue a la llamada.
    - 83 C4 04 en ensamblador x86 se traduce a ADD ESP, 4.
      - 83 es el opcode para una operación de ajuste (ADD) con un valor inmediato.
      - C4 indica que el registro ESP (stack pointer) es el operando.
      - 04 es el valor inmediato que se suma a ESP.

### **Explicación de la secuencia en el contexto de malware:**

- **CALL y ADD ESP, 4:**
  - Cuando el programa ejecuta CALL, guarda la dirección de retorno en la pila (stack) y salta a la dirección especificada por el desplazamiento relativo de 32 bits.
  - Despues de la llamada, ADD ESP, 4 ajusta el puntero de la pila (ESP) incrementándolo en 4 bytes.
  - Este patrón es común en ciertas funciones de malware, ya que los programas maliciosos a menudo manipulan el puntero de la pila para ocultar sus intenciones o gestionar la memoria de maneras específicas.

### **Relación con el malware:**

La secuencia de bytes E8 ?? ?? ?? ?? 83 C4 04 especificada en la regla YARA es una firma de comportamiento que indica una llamada a una función (CALL) con un desplazamiento relativo

de 32 bits, seguida de una instrucción para ajustar el puntero de la pila (ADD ESP, 4). Este patrón es significativo en la detección de malware porque implica operaciones típicamente usadas para eludir la detección, esconder llamadas a funciones maliciosas, o manejar la memoria de manera específica. Los análisis de malware buscan estos patrones, ya que representan comportamientos comunes en programas maliciosos que manipulan el flujo de ejecución y la pila para sus propios fines.

## Tarea 3:

Se ha detectado una alerta de seguridad en el sistema a través de Google Chronicle. El evento se refiere al lanzamiento de un proceso sospechoso desde un archivo de script.bat ubicado en un directorio temporal de un usuario. Los detalles de la alerta son los siguientes en el enlace: [https://demo.backstory.chronicle.security/alerts/de\\_69de214c-6f5d-d8d4-e797-ad5c85b5aee0/overview](https://demo.backstory.chronicle.security/alerts/de_69de214c-6f5d-d8d4-e797-ad5c85b5aee0/overview).

- Verificar la Legitimidad del Archivo:

- Investiga como analizarías el archivo vSRtdUK.bat para determinar su origen y si es legítimo.

- Analizar el Hash MD5:

- Consulta bases de datos de amenazas conocidas utilizando el hash MD5 (10af8616d121c6427d904f3efcad37b2) del archivo para ver si coincide con archivos maliciosos conocidos.
  - Registra cualquier coincidencia y toma las medidas necesarias para aislar y eliminar el archivo si se confirma que es malicioso.

- Documentar las Conclusiones:

- Proporciona recomendaciones sobre las acciones a tomar para mitigar la amenaza y prevenir futuros incidentes similares.

The screenshot shows the Google SecOps interface with the following details:

- Alert Summary:** info.bat - vSRtdUK.bat (CUSTOM RULE ALERT)
- Tags:** [n/a]
- Detection Rule:** info.bat
- Detection window:** [n/a]
- Detection time:** 2024-06-24T14:46:04.341
- Rule Description:** Detects batch files which are created or executed. [View Other Alerts From This Rule](#)
- Events:** A table showing one event entry:

TIMESTAMP	EVENT	USER	HOSTNAME	PROCESS NAME
2024-06-24T14:46:04.341	PROCESS_LAUNCH vSRtdUK.bat	[Unknown]	nancy-newman-windows-pc.corp.local	vSRtdUK.bat

The screenshot shows a 'DETECTION SUMMARY' page. On the left, there's a sidebar with sections for 'Assets' (listing IP addresses like 10.3.94.126 and MAC addresses like de:5d:89:ff:f7:aa) and 'File Hashes' (listing a hash like 10af8616d121c6427d904f3efcad37b2). The main area has tabs for 'DETECTION' and 'INVESTIGATION'. Under 'DETECTION', it shows 'Detection window' (2024-06-24T14:46:04.341), 'Detection time' (2024-06-24T14:46:04.341), and 'Rule Description' (Detects batch files which are created or executed). A 'View Other Alerts From This Rule' link is also present. At the bottom, there are buttons for 'WRAP TEXT', 'COLUMNS', and a menu icon. A specific event is highlighted with a blue box: 'PROCESS\_LAUNCH' for 'vSRtdUK.bat'.

## Detalles de la alerta

- **Creada:** 2024-06-24T09:17:54.228
- **Severidad:** baja
- **Prioridad:** baja
- **Riesgo:** 40 bajo riesgo

## Resumen de detección

- **Nombre de la regla:** info\_bat
- **Tiempo de detección:** 2024-06-24T09:16:04.341
- **Descripción de la regla:** “Detects batch files which are created or executed”

## Eventos:

- **Timestamp:** 2024-06-24T09:16:04.341
- **Evento:** Process\_Launch vSRtdUK.bat
- **Hostname:** nancy-newman-windows-pc.corp.local
- **Nombre de proceso:** vSRtdUK.bat

## Contexto teórico

Un archivo BAT (batch file) es un archivo de script utilizado en sistemas operativos DOS y Windows. Los archivos BAT contienen una serie de comandos que se ejecutan en secuencia para automatizar tareas repetitivas en la línea de comandos. El término “batch” se refiere a la ejecución por lotes, lo que significa que múltiples comandos se agrupan en un solo archivo y se ejecutan uno tras otro automáticamente.

## Características de los Archivos BAT

1. **Extensión del Archivo:** Los archivos BAT tienen la extensión .bat.
2. **Contenido:** Contienen comandos de la línea de comandos de Windows (CMD), como copiar archivos, mover directorios, y ejecutar programas.
3. **Ejecutables:** Al ejecutar un archivo BAT, cada comando en el archivo se ejecuta en el orden en que aparece.

4. **Automatización:** Son útiles para automatizar tareas repetitivas, como la copia de seguridad de archivos, la configuración de entornos, o la ejecución de múltiples programas en una secuencia específica.

En la descripción de la alerta se puede ver que se refiere a detectar archivos batch, veamos que diferencia hay entre archivos batch y archivos bat.

- **Batch:** En un sentido más amplio, “batch processing” (procesamiento por lotes) se refiere a la ejecución de una serie de programas o comandos en un sistema sin intervención manual. Esto puede aplicarse a diferentes tipos de archivos de script, no solo a los archivos BAT.
- **Archivos BAT:** Específicamente se refiere a los archivos con la extensión .bat que contienen comandos ejecutables en la línea de comandos de Windows.

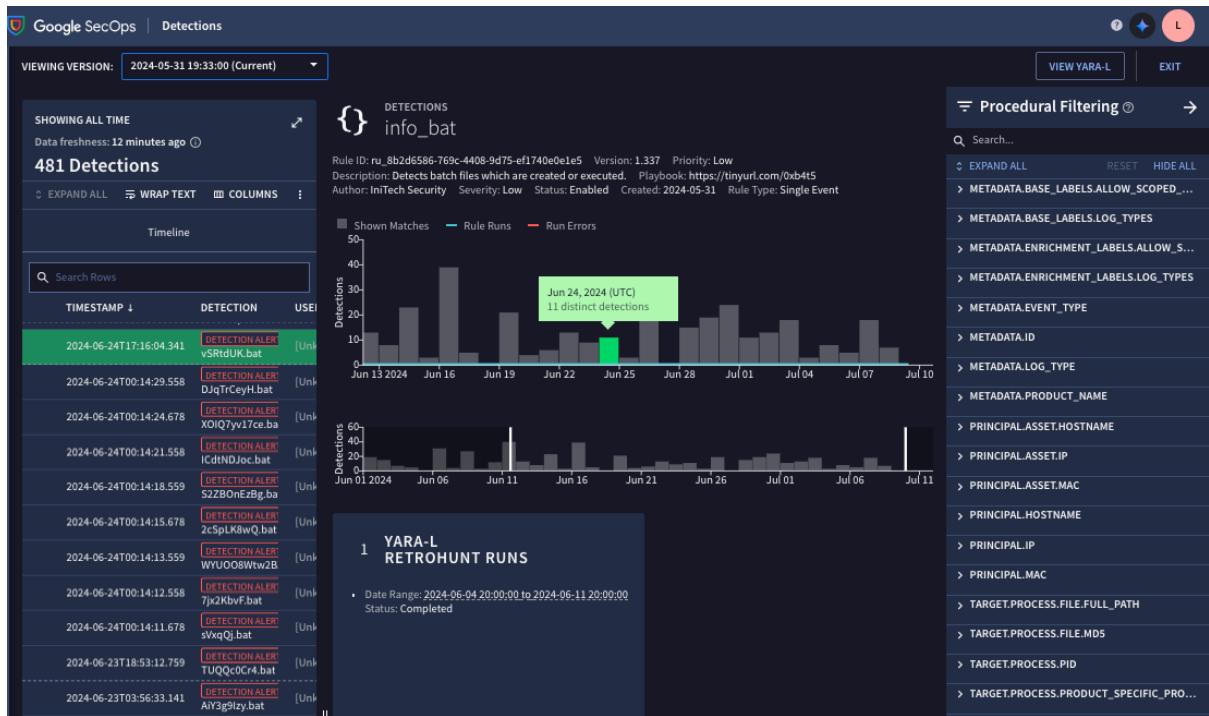
## Resolución del ejercicio

Según la información obtenida en el enunciado entendemos que lo que ha ocurrido es que se ha identificado un posible incidente de seguridad donde un archivo .bat en un directorio temporal del sistema ha iniciado un proceso, es decir, que el script del archivo .bat ha comenzado a ejecutarse. Este tipo de evento es sospechoso porque los directorios temporales suelen ser utilizados por malware para ejecutar actividades maliciosas sin ser detectados fácilmente.

Para realizar la verificación de la legitimidad del archivo vSRtdUK.bat, incluyendo el análisis del hash MD5 y la documentación de las conclusiones, lo primero que debemos hacer es investigar y obtener mas detalles de la alerta, del archivo, del usuario y del host desde donde ha sido ejecutado.

## Recopilación de información y Análisis de la legitimidad el archivo incluído el análisis del hash

Desde el overview, al seleccionar la regla info\_bat podemos obtener mas detalles relevantes de la misma como son el ID, Playbook y la severidad.



Conocemos el usuario y el host desde donde se ha ejecutado el proceso, son Nancy Newman desde un pc Windows cuya IP es 10.3.94.126 y dirección Mac es de:5d:89:ff:f7:aa. Esta información se puede obtener desde el “graph summary” de la alerta.

Google SecOps | Alerts & IOCs

## ⚠️ info\_bat - vSRtdUK.bat

CUSTOM RULE ALERT

This alert is managed in the SIEM. You can update or close the alert directly here.

**OVERVIEW**   **GRAPH**   **ALERT HISTORY**

**Graph Summary**

**INFO\_BAT**

- Status: New
- Severity: Low
- Priority: Low
- Risk Score: 40 ALERT RISK - LOW
- Detected: 2024-06-24T09:16:04.341
- Created: 2024-06-24T09:17:54.228
- Last Seen: --
- Updated: --
- Rule: [info\\_bat](#)
- Description: Detects batch files which are created or executed.

**NANCY-NEWMAN-WINDOWS-PC.COR P.LOCAL**

- Hostname: nancy-newman-windows-pc.corp.local
- First time seen: 2024-06-24T09:16:04.341
- Last time seen: 2024-06-24T09:16:04.341
- IP addresses: 10.3.94.126
- Mac addresses: de:5d:89:ff:f7:aa
- Entity Risk: 4
- Score:

**MD5 10AF8616D121C6427D904F3EF CAD37B2**

- Hash type: Md5
- First time seen: 2024-03-17T21:17:06.034
- Last time seen: 2024-06-24T09:16:04.341
- Entity Risk: [n/a]
- Score:

**GRAPH**

**GRAPH OPTIONS**

```

graph TD
    Alert((info_bat)) --- FileHash[10af8616d121c6427...]
    Alert --- Host[nancy-newman-wind...]
    FileHash --- Host
    FileHash --- Alert
    Host --- Alert
    FileHash --- FileHash2[info_bat]
    FileHash2 --- Alert
    
```

The graph shows a central alert node (info\_bat) connected to a host node (nancy-newman-wind...) and a file hash node (10af8616d121c6427...). The file hash node is also connected to the host node and itself, indicating a self-loop relationship.

A partir de esta sección, podemos seleccionar mas detalles de la regla info\_bat y obtener más información relevante.

The screenshot shows the Google SecOps Detections interface. On the left, a timeline view displays 477 detections from June 2024. A specific event for 'PROCESS\_LAUNCH' on June 24, 2024, at 09:16:04 is selected. The main panel shows the raw log and a detailed UDM Event pane. The UDM Event pane contains a large JSON object with fields such as '\_access', '\_id', 'target\_process', and various metadata keys. To the right, a 'Procedural Filtering' sidebar lists many metadata keys, including 'EXPAND ALL', 'RESET', 'HIDE ALL', and numerous specific keys like 'METADATA.BASE\_LABELS\_ALLOW\_SCOPED', 'METADATA.ENRICHMENT\_LABELS\_ALLOW\_SCOPE', etc.

En primer lugar, observamos que es un evento de tipo process\_launch lo que indica que la alerta se debe a que un proceso se ha ejecutado. Además, observamos que el product\_name es interno lo que nos indica que el evento ha tenido lugar de forma interna, como ya sabíamos desde el usuario y host indicado anteriormente. Podemos ver la localización del archivo causante de la ejecución del proceso: C:\Users\AppBarData\local\Temp\vSRtdUK.bat y su hash MD5: 10af8616d121c6427d904f3efcad37b2.

Con este hash nos podemos dirigir a diferentes feeds de inteligencia para obtener información acerca de la legitimidad del archivo, nos dirigimos a virusTotal y no obtenemos ningún resultado. A continuación, buscamos en bases de datos como la de malware bazaar y tampoco lo encontramos.

Además, en el Raw, podemos ver el ID del proceso que se ha ejecutado, el 43208. Al no obtener información acerca del archivo en los feeds de inteligencia, seguimos investigando. Seleccionmos el hash que nos lleva a la siguiente sección.

The screenshot shows the Google SecOps search interface. At the top, there's a search bar with the query: `target.process.file.md5 = "0xa0f8616d121c6427d994f3efcad37b2"`. Below the search bar, the timeline shows a single event at approximately 16:46 on June 24, 2024. The event details are as follows:

Timestamp	Event	User	Hostname	Process Name
2024-06-24T17:16:04.341	<span style="color:red">ALERT</span> PROCESS_LAUNCH	(Unknown)	nancy-newman-windows-oc.corp.local	vSRdUk.bat

The left sidebar shows various aggregation fields like `process_id`, `file_path`, `hash`, `hostname`, and `ip`. The right sidebar includes the **EVENT VIEWER** and **UDM FIELDS** sections, which provide detailed information about the event.

Desde aquí obtenemos también el pid del proceso ejecutado: 43208, conociendo este dato se puede conocer si aún está en ejecución e identificar que acción realiza en el sistema.

Al haber sido ejecutado en Windows, nos podríamos dirigir al task manager o usar el comando tasklist en la terminal cmd, para ver si aún está en ejecución: `tasklist /FI "PID eq <PID>"` y obtener detalles del proceso con: `wmic process where "ProcessId=<PID>" get Name, ExecutablePath, CommandLine, CreationDate`.

Además, podríamos identificar acciones del proceso usando resource monitor para ver los recursos que el proceso está utilizando y event viewer para ver eventos relacionados.

De este modo, se puede evaluar la gravedad y aislar el proceso si parece sospechoso o malicioso, aislando el sistema afectado de la red para evitar la propagación de cualquier potencial amenaza. Si hay indicios claros de actividad sospechosa, y el proceso está en ejecución, se detiene inmediatamente el proceso para mitigar cualquier daño potencial.

Antes de detener el proceso, si es seguro hacerlo, se tomaría una captura de la memoria y se recolectaría cualquier archivo asociado para un análisis forense posterior.

Si el proceso no presenta una amenaza inmediata y permite tiempo para una investigación mas detallada, se podría monitorear para comprender mejor sus acciones con herramientas como Procmon.

Se realizaría en cualquier caso una verificación adicional ejecutando un análisis antivirus o antimalware en el archivo y el sistema y se revisarían los logs y eventos en el event viewer relacionados con el proceso.

Si se tiene acceso al archivo, analizarlo en un sandbox.

Investigar actividades recientes del usuario y sus acciones:

- Revisar registros de inicio/cierre de sesión.
- Verificar accesos inusuales a sistemas/archivos.
- Examinar correos electrónicos y comunicaciones.
- Revisar historial de comandos y aplicaciones ejecutadas.
- Confirmar cumplimiento de políticas de seguridad.
- Entrevistar al usuario para obtener contexto adicional.

En el host, revisar:

- Logs del sistema para eventos relacionados.
- Realizar un escaneo completo de malware.
- Analizar conexiones de red activas y tráfico sospechoso.
- Verificar la integridad de archivos del sistema.

Todas estas acciones serían documentadas detallando las acciones tomadas y los hallazgos obtenidos.

## **Toma las medidas necesarias para aislar y eliminar el archivo si se confirma que es malicioso**

Si el archivo se confirma como malicioso:

- **Aislar el Archivo:**
  - Desconectar el sistema afectado de la red.
  - Mover el archivo a un entorno seguro o sandbox.
- **Eliminar el Archivo:**
  - Utilizar software antivirus o antimalware.
  - Eliminar manualmente el archivo y sus rastros si es necesario.
- **Análisis Adicional y Mitigación:**
  - Realizar un escaneo completo del sistema.
  - Examinar los logs del sistema para actividades relacionadas.
  - Aplicar parches y actualizaciones de seguridad.

## **Documentar las Conclusiones**

### **1. Introducción:**

- **Descripción del Incidente:** Se detectó un proceso sospechoso iniciado por un archivo de script.bat en un directorio temporal de un usuario, lo que generó una alerta de seguridad en Google Chronicle.

### **2. Análisis del Archivo:**

- **Contenido del Archivo:** En caso de tener el archivo se detallaría aquí su contenido.
- **Hash MD5:** El hash MD5 del archivo es 10af8616d121c6427d904f3efcad37b2.
- **Resultado de la Búsqueda de Hash:** No se encontraron coincidencias en bases de datos de amenazas conocidas (VirusTotal, MalwareBazaar).

### **3. Acciones Tomadas (en caso de tener el archivo):**

- **Aislamiento del Archivo:**
  - El sistema afectado fue desconectado de la red para evitar la propagación del malware.
  - El archivo fue movido a un entorno seguro para análisis adicional.
- **Eliminación del Archivo:**
  - Se utilizó software antivirus para eliminar el archivo.
  - Se realizó una eliminación manual de los rastros del archivo.
- **Análisis Adicional:**
  - Se realizó un escaneo completo del sistema para asegurar la eliminación de otros archivos maliciosos.
  - Se revisaron los logs del sistema para identificar actividades relacionadas.
  - Se aplicaron parches y actualizaciones de seguridad.

### **4. Investigación del Usuario y Host:**

- **Actividades del Usuario:**
  - Revisados los registros de inicio/cierre de sesión.
  - Verificados accesos inusuales a sistemas y archivos.
  - Examinados correos electrónicos y comunicaciones del usuario.
  - Revisado historial de comandos y aplicaciones ejecutadas.
  - Entrevista con el Usuario.
- **Revisión del Host:**
  - Examinados los logs del sistema, red y archivos.
  - Realizado análisis de malware con herramientas avanzadas.
  - Revisadas conexiones de red activas y tráfico sospechoso.
  - Verificada la integridad de los archivos del sistema.

### **5. Recomendaciones:**

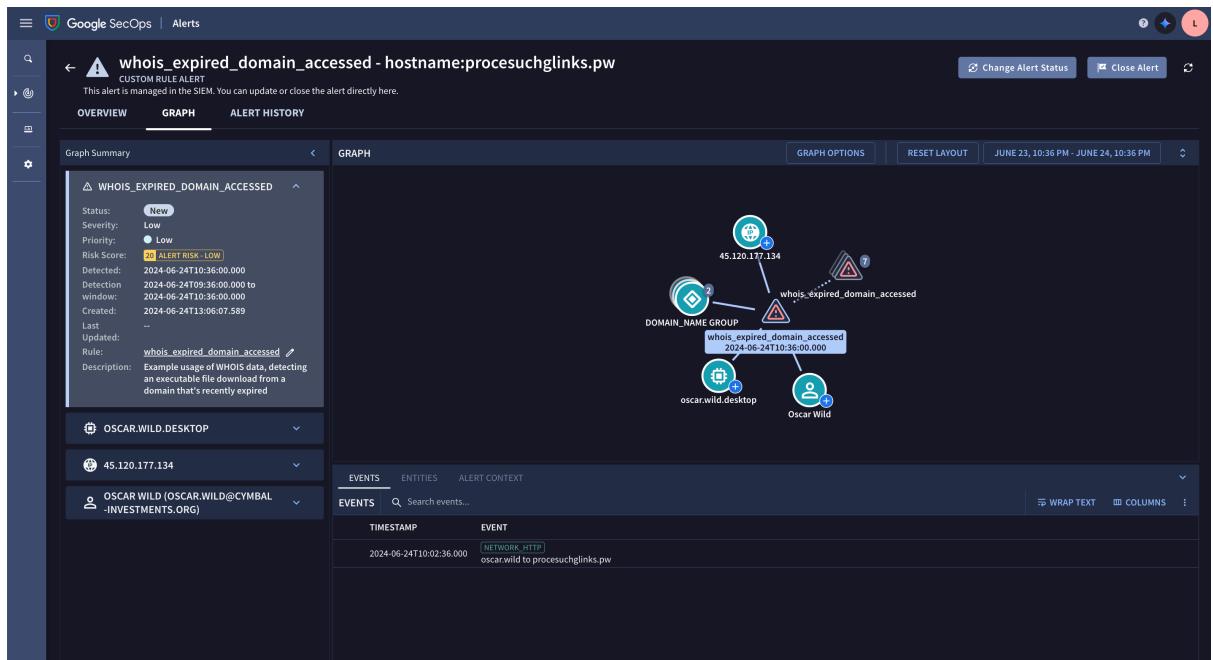
- **Mitigación de la Amenaza:**
  - Actualizar todas las firmas de antivirus y aplicar controles de acceso más estrictos.
  - Implementar monitorización continua para detectar actividades sospechosas.
- **Prevención de Futuros Incidentes:**
  - Capacitar a los usuarios sobre buenas prácticas de seguridad.
  - Refinar las reglas de detección en Google Chronicle para identificar mejor los comportamientos maliciosos.

## 6. Conclusión:

Siguiendo estos pasos, se realizó un análisis exhaustivo del archivo vSRtdUK.bat, determinando su origen y tomando las acciones necesarias para mitigar cualquier amenaza identificada.

## Tarea 4:

**Se ha detectado una alerta de seguridad en el sistema a través de Google Chronicle. La alerta es la que se encuentra en el siguiente link:** [https://demo.backstory.chronicle.security/alerts/de\\_980b1f65-2004-cb73-17a6-3c67b0ab707a/graph](https://demo.backstory.chronicle.security/alerts/de_980b1f65-2004-cb73-17a6-3c67b0ab707a/graph)





TIMESTAMP	DETECTION	USER	HOSTNAME	PROCESS NAME
2024-06-24T13:06:00.000	<span style="background-color: red; color: white; padding: 2px 5px;">DETECTION ALERT</span> hostname:procesuchglinks.pw	oscar.wild	procesuchglinks.pw	[Unknown]
ENTITIES (1)				
2023-05-09T20:33:13.000	<span style="background-color: red; color: white; padding: 2px 5px;">DOMAIN</span> procesuchglinks.pw	[Unknown]	[Unknown]	[Unknown]
EVENTS (1)				
2024-06-24T12:32:36.000	<span style="background-color: red; color: white; padding: 2px 5px;">NETWORK_HTTP</span> oscar.wild to procesuchglinks.pw	oscar.wild	oscar.wild.desktop	[Unknown]

1 target.ip = "45.120.177.134"

The screenshot shows a log analysis interface with the following details:

Top navigation: History, UDM Lookup, Lists, Generated Query, etc.

Section tabs: OVERVIEW, EVENTS (1), ALERTS (2).

Sub-section tabs: Trend over time, Prevalence.

Aggregations sidebar:

- Search field: Search fields or values...
- Grouped Fields:
  - hostname (2): oscar.wild.desktop, procesuchlinks.pw
  - ip (2): 10.19.6.24, 45.120.177.134
  - user (2): Oscar Wild, oscar.wild
  - domain (1): procesuchlinks.pw
  - email (1): oscar.wild@cymbal-investments.org

Events table:

EVENTS	PIVOT	Search events...	
TIMESTAMP	EVENT	USER	HOSTNAME
2024-07-09T12:32:45.000	[ALERT] [NETWORK_HTTP] oscar.wild to procesuchlinks.pw	oscar.wild	oscar.wild.desktop

AGGREGATIONS	
<input type="text"/> Search fields or values...	
▼ GROUPED FIELDS ⓘ	
▼ hostname (2)	1
Combined values for 8 fields ⓘ	
oscar.wild.desktop	1
procesuchglinks.pw	1
▼ ip (2)	1
Combined values for 11 fields ⓘ	
10.19.6.24	1
45.120.177.134	1
▼ user (2)	1
Combined values for 9 fields ⓘ	
Oscar Wild	1
oscar.wild	1
▼ domain (1)	1
Combined values for 10 fields ⓘ	
procesuchglinks.pw	1
▼ email (1)	1
Combined values for 6 fields ⓘ	
oscar.wild@cymbal-investments.org	1
▼ UDM FIELDS	
▼ principal.user.attribute.labels.key (1)	1
lastLogin	1
> additional.fields.key (3)	1
> additional.fields.value.string_value (3)	1
> metadata.enrichment_labels.log_types (2)	1
▼ principal.user.department (2)	1
Default Department	1
Office of the CISO	1



file_path	(14)	18
Combined values for 6 fields ⓘ		
C:\Users\oscar.wild\Desktop\Update.exe		7
C:\Windows\explorer.exe		7
C:\Users\oscar.wild\AppData\Local\51e3b645-cd3e-4087-8175-9451ecd98863\software.exe		1
C:\Users\oscar.wild\AppData\Local\Temp\2210231586.exe		1
C:\Users\oscar.wild\AppData\Local\Temp\4848.exe		1
C:\Users\oscar.wild\AppData\Local\Temp\Avl.exe		1
C:\Users\oscar.wild\AppData\Local\Temp\F20B.exe		1
C:\Users\oscar.wild\AppData\Local\Temp\myfile.exe		1
C:\Users\oscar.wild\AppData\Local\Temp\sonic.exe		1
C:\Users\oscar.wild\Desktop\program.exe		1
C:\Users\oscar.wild\Downloads\123.dll		1
C:\Users\oscar.wild\Downloads\TactXCI.dll		1
C:\Users\oscar.wild\Downloads\intl.dll		1
C:\Windows\SysWOW64\cmd.exe		1

process_id	(34)	15
hash	(33)	11
Combined values for 13 fields ⓘ		
0000a30f08a3bc2d09c7a03a12a03c85bc6f01f264652170c49826dd944dc018		1
0084698bf5926c0673a745833521fc5d050cd30feb03eb6c00e0b92826245066		1
0098039069d7dd188ea52042b095b5588e2fcf7c7cb407246432d776d2f37d80		1
01153cfef9fe9f1c3460e02d254bbe49b7b07c343061b7630234d95948d8f6106		1
027cc450cef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745		1
05d6b2f8a9c4c319ca23e571b9bd77142f3c880524a67b6f6783550af620374b		1
0d6518769e10895cc1880040fb0680520cb179d37624bd2685368414b4a6e4eb		1
2b248e9302a441c389c30a85534c0cc2		1
317c1da3d49d534fdde575395da84879		1
34f917aabaa5684fbe56d3c57d48ef2a1aa7cf06d		1
SHOW 10 MORE...		
email	(1)	26
Combined values for 6 fields ⓘ		
oscar.wild@cymbal-investments.org		26

i principal.hostname = "oscar.wild.desktop" nocase

History UDM Lookup Lists

OVERVIEW EVENTS (26) ALERTS (28)

### Gemini Summary

#### Events

There are 26 NETWORK\_HTTP, PROCESS\_LAUNCH, NETWORK\_CONNECTION, and SCAN\_FILE events from Microsoft, Zscaler, and Google.

There are 3 users present:

- Most common:  
I. Oscar Wild (100%)  
II. oscar.wild (100%)
- Least common: S-1-5-18 (58%)

There are 9 hostnames present:

- Most common: oscar.wild.desktop (100%)
- Least common:  
I. againandagainmorder.ru (4%)  
II. procesuchlinks.pw (4%)  
III. sempersim.su (4%)

There are 16 IP addresses present:

- Most common: 10.19.6.24 (100%)
- Least common:  
I. 103.111.55.218 (4%)  
II. 45.141.84.223 (4%)  
III. 85.143.223.246 (4%)

#### Alerts

There are 28 alerts. 11% of the alerts have PRIORITY\_CRITICAL priority and 50% of the alerts have Critical severity.

There are 8 rules:

- Most common: gcti\_malicious\_file\_process\_launch (29%)
- Least common:  
I. google\_safefrowsing\_file\_process\_creation (4%)  
II. malware\_win\_lokibot\_c2 (4%)

[Ask Gemini](#)

**Note:** We updated some Search views. Go to Legacy View for old views.

#### Entity summary

**Asset**  
**oscar.wild.desktop**

First time seen	Last time seen	IP addresses	Mac addresses
8 months ago	10 hours ago	10.19.6.24	b4:22:2b:49:3a:2b

[View More](#)

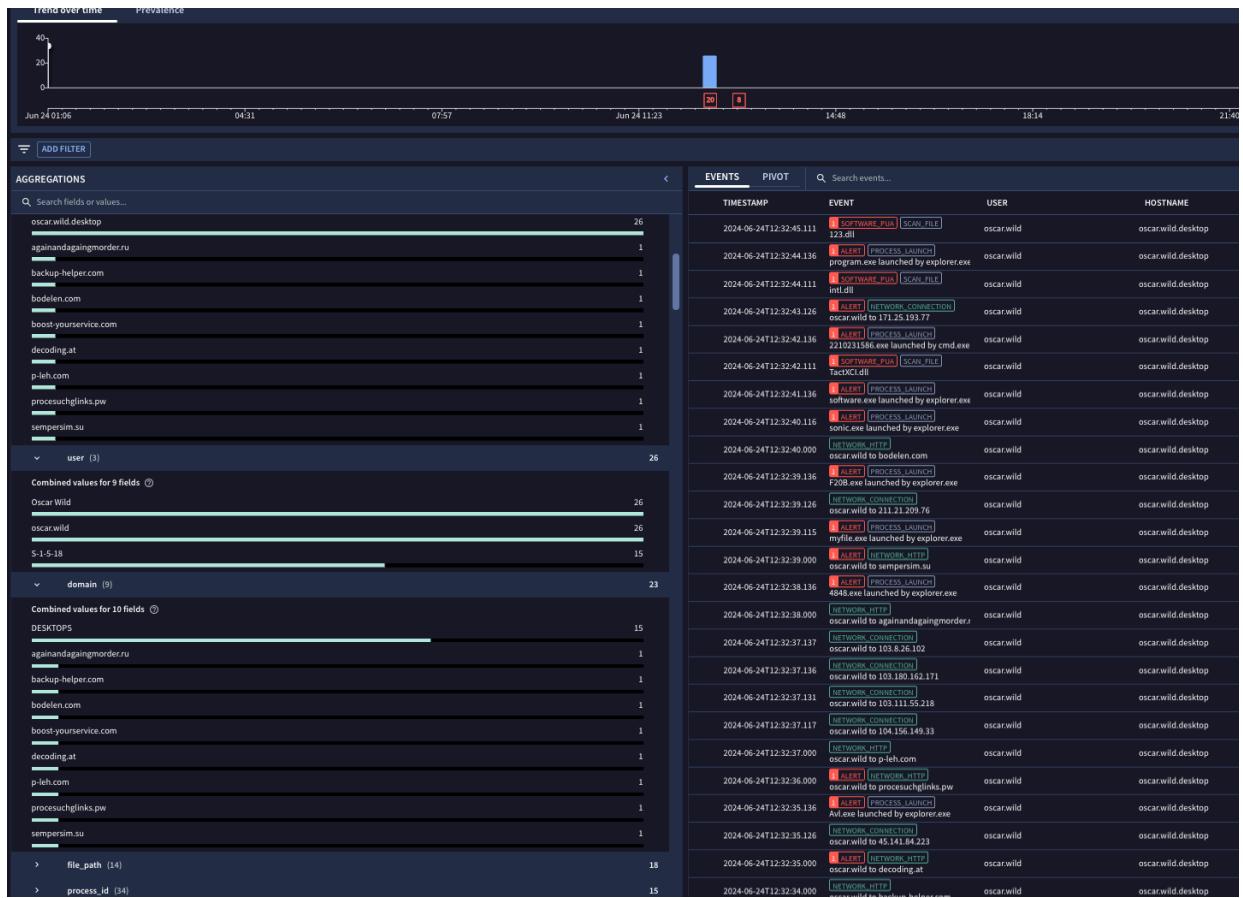
**28 alerts**

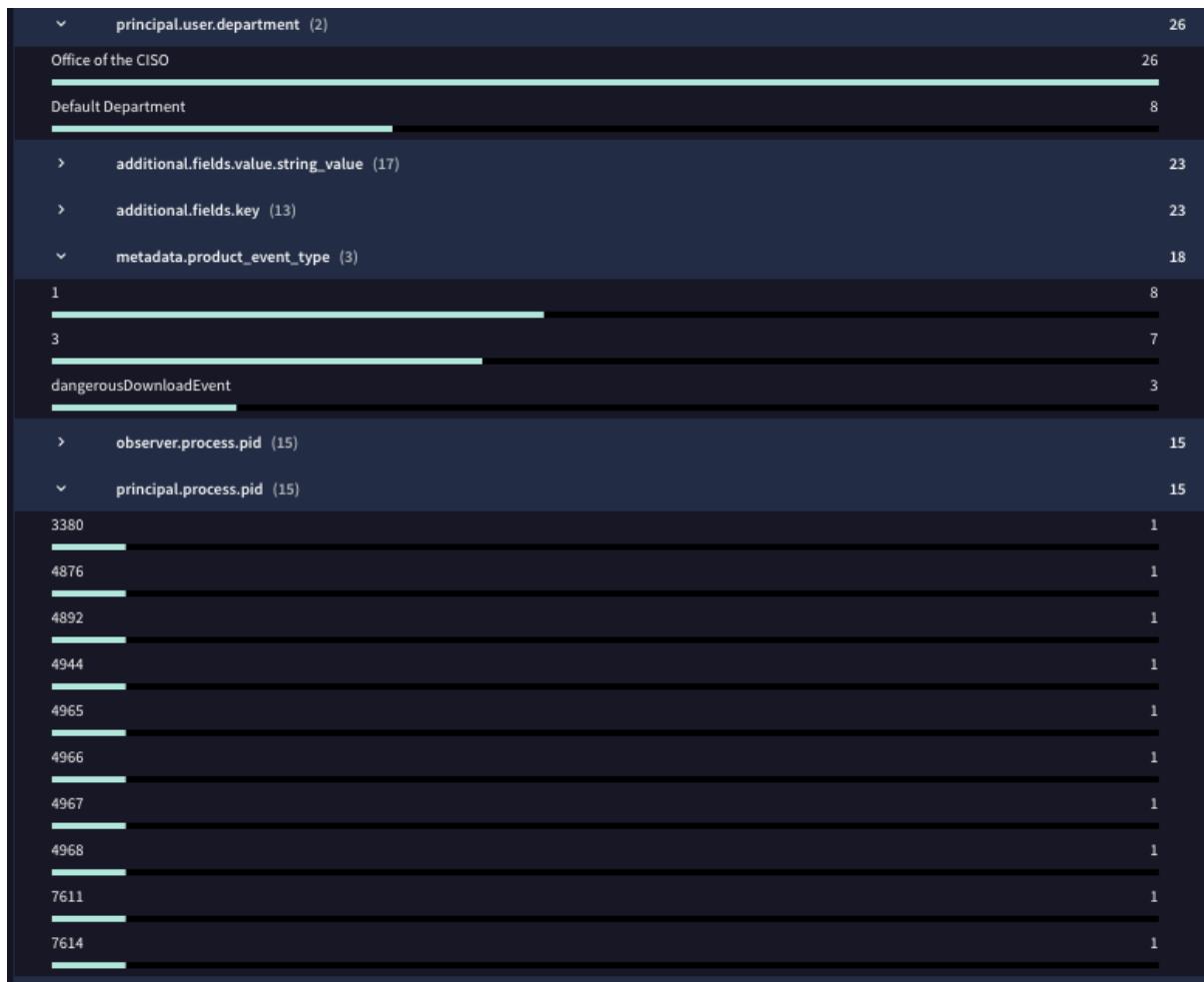
**Highest alert count by Rule:**

- gcti\_malicious\_file\_process\_launch (8)
- Applied Threat Intelligence IOC Match Rule [Active Breach Priority Host Indicators] (5)
- google\_safefrowsing\_with\_prevalence (5)
- whois\_expired\_domain\_accessed (4)
- sw\_malware\_win\_lokibot\_c2 (2)

01:00 AM June 24 03:00 AM June 24 05:00 AM June 24 07:00 AM June 24 09:00 AM June 24 11:00 AM June 24 01:00 PM June 24 03:00 PM June 24 05:00 PM June 24 07:00 PM June 24 09:00 PM June 24 11:00 PM June 24 01:00 AM June 25

[Open Alerts & IOCs](#) [View in Alerts Tab](#)





**Analiza la alerta para poder conocer:**

- **La acción realizada que ha hecho saltar la regla.**

La acción que ha hecho saltar la regla es el acceso a un dominio cuyo registro ha expirado recientemente, detectando la descarga de un archivo ejecutable desde dicho dominio.

El acceso ha sido mediante GET desde un protocolo HTTPS a través del usuario oscar.wild, el cual ha sido asociado con 26 eventos y se ha detectado que hay dos registros con el mismo nombre: Oscar.Wild y oscar.wild.

- **La dirección IP desde la que ha accedido el usuario.**

IP: 10.19.6.24

- **La dirección IP del servidor en el que se encuentra el dominio al que se ha accedido, además del nombre de dicho dominio.**

IP: 45.120.177.134

Nombre del dominio: procesuchglinks.pw

- **El nombre de la regla que ha saltado con esta acción.**

Nombre de la regla: whois\_expired\_domain\_accessed

- **¿Con qué empresa habría que contactar para indicar el incidente producido? ¿Qué preguntas/recomendaciones habría que hacerles?**

El departamento del usuario causante de la alerta es del departamento CISO y su email corporativo es: oscar.wild@cymbal-investments.org, por tanto, se debería contactar con la empresa Cymbal Investments.

La IP del servidor de la descarga ha sido asociado con actividades maliciosas de malware por 4 vendors en virusTotal y el dominio con 2 vendors en virusTotal.

### **Preguntas/Recomendaciones para la empresa:**

#### **Preguntas:**

- ¿Cuál es el propósito del acceso al dominio procesuchglinks.pw?
- ¿El archivo ejecutable descargado ha sido verificado y autorizado por el equipo de seguridad?
- ¿El usuario Oscar Wild tiene conocimiento de haber accedido a este dominio y descargado dicho archivo?
- ¿El archivo descargado ha sido ejecutado o manipulado por el usuario, y si es así, qué resultados se obtuvieron?
- ¿Se ha detectado alguna actividad inusual en otros dispositivos de la red desde que se produjo este incidente?
- ¿Qué medidas de seguridad adicionales se están tomando para proteger la red contra accesos a dominios maliciosos?

#### **Recomendaciones:**

Dado que algunos proveedores han marcado el dominio como malicioso, se deben tomar las siguientes acciones:

- **Aislamiento y Análisis:**
  - Aislar el equipo para reducir posibles daños y propagación.
  - Aislar el archivo ejecutable descargado en un entorno seguro para un análisis más profundo y verificar si contiene malware.
  - Realizar un análisis forense en el dispositivo de Oscar Wild para identificar cualquier indicio de compromiso.
  - Monitorear las actividades del usuario Oscar Wild para identificar posibles accesos no autorizados.
- **Bloqueo del Dominio:** Bloquear el acceso al dominio procesuchglinks.pw en la red corporativa para evitar futuros incidentes.
- **Revisar los registros de actividad (logs) y el tráfico de red** en torno al tiempo de la alerta para identificar cualquier comportamiento anómalo o adicional relacionado con este incidente.

- **Comunicaciones Internas:** Informar al equipo de IT y a todos los empleados sobre los riesgos asociados con el dominio y recordarles las mejores prácticas para evitar accesos a dominios sospechosos.
- **Contactar a los Proveedores de Seguridad:** Contactar a los proveedores de seguridad que han marcado el dominio como malicioso para obtener más detalles sobre la naturaleza de la amenaza detectada.
- **Actualizar las políticas de acceso** y descargas para evitar conexiones a dominios.
- **Considerar la implementación de alertas adicionales** para mejorar la detección temprana de accesos potencialmente peligrosos ya que se ha comprobado la existencia de 14 rutas de descarga de archivos ejecutables muchos de los cuales en directorios temporales que puede ser sospechoso y 33 hash de archivos descargados.
- Utilizar **herramientas de análisis de comportamiento** para detectar accesos y actividades inusuales en tiempo real.

The screenshot shows a detailed analysis of the domain `procesuchglinks.pw`. At the top, it indicates that 2/92 security vendors flagged the domain as malicious. The domain itself is listed as `unknown`. Below this, the registrar is shown as `Stichting Registrar of Last Resort Foundation`, with creation and last analysis dates from 1 year ago and 4 months ago respectively. The interface includes tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. A prominent call-to-action button says "Join our Community". The "Security vendors' analysis" section lists various vendors and their findings, such as CRDF (Malicious), Abusix (Clean), and BitDefender (Clean). A "Do you want to automate checks?" section is also present.

## Tarea 5:

Una de las posibilidades que ofrece el SIEM de Chronicle es analizar directamente los IoCs (Indicadores de Compromiso), como se puede apreciar en el siguiente enlace: <https://demo.backstory.chronicle.security/breach-analytics?startTime=2024-06-22T10:15:22.081Z&endTime=2024-06-25T10:15:22.081Z>. En este ejercicio se pide:

- Encontrar cual es la campaña que más IoC tiene asociados.

APT 33 Campaign.

- ¿Qué tipo de IoC son los que se han detectado para esa campaña? ¿Cuáles son esos IoC?  
manygoodnews.com categorizado como Spyware and malware, Malicious y Web applications.
- ¿A qué asociaciones/grupos criminales se atribuyen esos IoC?  
Hackers Espías iraníes.
- Una de las posibilidades que ofrece este SIEM es la integración de VirusTotal. Para alguno de los IoC, accede al menú “VT Context” y comenta la información que ofrece VirusTotal acerca de ese indicador de compromiso.

### Análisis del IoC “manygoodnews.com”

#### Información de VirusTotal:

- **Detección:** 8 de 92 vendors han detectado el dominio como malicioso.
- **Proveedores que detectaron:**
  - Antiy-AVL: Malicious
  - CyRadar: Malicious
  - Kaspersky: Malware
  - Seclookup: Malicious
  - Bfore.Ai PreCrime: Malicious
  - Fortinet: Malware
  - Lionic: Malicious
  - Sphos: Malware

#### Categorías:

- Sophos: spyware and malware
- alphaMountain.ai: Malicious
- Xcitium Verdict Cloud: web applications
- Forcepoint ThreatSeeker: alternative journals

#### Información de la Entidad “manygoodnews.com”

- **Ciudad Administrativa:** Kita-ku Osaka-shi
- **País Administrativo:** Japón
- **Correo Administrativo:** 4ef0947320e8e498s@value-domain.com
- **Estado Administrativo:** Osaka
- **Fecha de Creación:** 2023-08-22
- **Fecha de actualización:** 2023-08-23
- **Registrador del Dominio:** <http://www.onamae.com>
- **Servidores de Nombres:**
  - ns11.value-domain.com
  - ns12.value-domain.com
  - ns13.value-domain.com

- **Fuentes:** Indicator was published in publicly available sources: [intezer.com](https://intezer.com). [www.securityweek.com](https://www.securityweek.com)
- **Severidad:** Medium

## Último Certificado HTTPS:

- **Fecha de Validez:**
  - Not Before: 2015-11-30
  - Not After: 2025-11-27
- **Algoritmo de Clave Pública:** RSA

IOC	Type	Status	GCTP Priority	Categories	Sources	Assets	Severity	Associations	Campaigns	First Seen	Last Seen	VT Context
192.0.78.24	IP	Match	[Unspecified]	Blocked	ESET Threat... viviana-ell...	High	--	--	2018-01-09T08:05:4...	2024-06-25T10:38:4...	<a href="#">VT Context (0/92)</a>	
manygoodnews.com	DOMAIN	Match	[Unspecified]	Indicator was pu...	Mandiant O...	10.205.11...	Medium	--	2020-02-22T02:59:5...	2024-07-09T16:42:4...	<a href="#">VT Context (8/92)</a>	
76.223.105.230	IP	Match	[Unspecified]	Unwanted	ESET Threat...	larabaker-pc	Medium	--	2023-02-22T17:34:3...	2023-10-16T12:31:4...	<a href="#">VT Context (0/92)</a>	
54.225.121.9	IP	Match	[Unspecified]	Unwanted	ESET Threat....	george-sc...	Medium	--	2018-01-09T08:29:4...	2024-06-24T21:42:0...	<a href="#">VT Context (0/92)</a>	

Detections | IoCs | Graph | Attribution

VT Augment by VIRUSTOTAL

You are not signed in to virustotal.com or you have to allow VT Augment to read your VT cookies. If you have a VT ENTERPRISE license, make sure you sign in to view advanced threat reputation and context.

Sign In

8 / 92

8 security vendors flagged this domain as malicious  
manygoodnews.com

Registrar: - Creation Date: 10 months ago Last Updated: 10 months ago

Full report

Similar domains

VT Graph

**SECURITY VENDORS SCANNING RESULTS**

Anti-AVL: malicious  
CyRadar: malicious  
Kaspersky: malware

Bfore.Ai PreCrime: malicious  
Fortinet: malware

**WHOIS LOOKUP**

Administrative city: Kita-ku Osaka-shi  
Administrative country: Japan  
Administrative email: 4ef0947320e8e498s@value-domain.com  
Administrative state: Osaka  
Create date: 2023-08-22 00:00:00  
Domain name: manygoodnews.com  
Domain registrar id: 49  
Domain registrar url: http://www.onamae.com  
Expiry date: 2024-08-22 00:00:00  
Name server 1: ns1.value-domain.com  
Name server 2: ns12.value-domain.com  
Name server 3: ns13.value-domain.com  
Query time: 2023-08-23 10:12:49

manygoodnews.com

Community Score: 8 / 92

8/92 security vendors flagged this domain as malicious

Creation Date: 10 months ago | Last Analysis Date: 2 hours ago

spyware and malware | Malicious | web applications

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Contained in Graphs (1)

citreno | manygoodnews APT 33 Campaign | 2023-10-07 00:21:15

Comments

ATT&CKcon 5.0 returns October 22-23, 2024 in McLean, VA. Stay tuned for regi

[Home](#) > [Groups](#) > [APT33](#)

## APT33

APT33 is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.<sup>[1][2]</sup>

Threat Intelligence

## Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware

September 20, 2017

Mandiant

Written by: Jacqueline O'Leary, Josiah Kimble, Kelli Vanderlee, Nalani Fraser

When discussing suspected Middle Eastern hacker groups with destructive capabilities, many automatically think of the suspected Iranian group that previously used SHAMOON – aka [Disttrack](#) – to target organizations in the Persian Gulf. However, over the past few years, we have been tracking a separate, less widely known suspected Iranian group with potential destructive capabilities, whom we call APT33. Our analysis reveals that APT33 is a capable group that has carried out cyber espionage operations since at least 2013. We assess APT33 works at the behest of the Iranian government.

Recent investigations by FireEye's [Mandiant incident response](#) consultants combined with FireEye iSIGHT Threat Intelligence analysis have given us a more complete picture of APT33's operations, capabilities, and potential motivations. This blog highlights some of our analysis. Our detailed report on FireEye Threat Intelligence contains a more thorough review of our supporting evidence and analysis. We will also be discussing this threat group further during our [webinar](#) on Sept. 21 at 8 a.m. ET.

### Targeting

APT33 has targeted organizations – spanning multiple industries – headquartered in the United States, Saudi Arabia and South Korea. APT33 has shown particular interest in organizations in the aviation sector involved in both military and commercial capacities, as well as organizations in the energy sector with ties to petrochemical production.

SEARCH

Enter any question here, for example "Find externally shared documents with confidential in the title"

1 target.hostname = "manygoodnews.com"

Generated Query  Case Sensitivity Off JUNE 22, 03:45 PM - JUNE 25, 03:45 PM Run Search

History UDM Lookup Lists OVERVIEW EVENTS (42) ALERTS (45)

Entity summary

**Domain** manygoodnews.com

First time seen: 4 years ago | Last time seen: 5 hours ago | WHOIS for: manygoodnews.com | Registrar: GMO Internet Group, Inc. d/b/a Onamae.com

Company: Whois Privacy Protection Service by VALUE-DOMAIN | Country: JAPAN | Contact email: whoisproxy@value-domain.com | Created: 10 months ago

Last updated: 10 months ago | Expires: in 2 months

View More

VT Context (8/92)

45 alerts

Highest alert count by Rule:

- suspicious\_download\_office (18)
- Applied Threat Intelligence IOC Match Rule [High Priority Host Indicators] (12)
- vt\_relationships\_file\_contacts\_domain (12)
- high\_risk\_user\_download\_executable\_from\_macro (3)

03:45 PM June 22 09:30 PM June 22 05:30 AM June 23 01:30 PM June 23 09:30 PM June 23 05:30 AM June 24 01:30 PM June 24 09:30 PM June 24 05:30 AM June 25 01:30 PM June 25

Open Alerts & IOCs View in Alerts Tab

Relevant IOCs

IOC	Categories	Sources	Assets	Confidence	Severity
manygoodnews.com	Indicator was published in publicly available sources	Mandiant Open Source Intelligence	10.205.11.20, steve-watson-pc, dominikjtzs-pc, 10.20.20.73, javier's-pc, alice-benjamin-pc, betty-decaro-pc, mikerosz-pc, 10.10.149.177, 10.1.12.24, 10.0.30.228.adablaclk-pc	Medium	Medium

OVERVIEW EVENTS (42) ALERTS (45)

10.0.30.228.adablaclk-pc

loc ingest time: 2024-05-24T16:38:40.970Z | FirstSeen: 2020-02-21T18:59:51Z | LastSeen: 2024-07-03T08:42:44.688Z | Confidence Score: 73 | Feed Name: MANDIANT | Active Time Start: 1970-01-01T00:00:01Z

Active Time End: 9999-12-31T23:59:59Z | Description: [n/a]

View in IOCs List

Prevalence of Assets

## Tarea 6:

AWS GuardDuty ha detectado una actividad sospechosa en una instancia de EC2. La instancia ha realizado una consulta DNS a un dominio conocido por estar asociado con actividades maliciosas, como el almacenamiento de credenciales robadas y otros datos capturados por malware: [https://demo.backstory.chronicle.security/alerts/de\\_721e9a2d-56cc-061f-2a6c-7f7ab380b97f/overview](https://demo.backstory.chronicle.security/alerts/de_721e9a2d-56cc-061f-2a6c-7f7ab380b97f/overview)

- ¿Qué es AWS GuardDuty y cuál es su función en la seguridad de AWS?
- ¿Cuál es la implicación de que una instancia de EC2 realice consultas a un dominio conocido por actividades maliciosas?
- ¿Qué información puedes obtener de la dirección IP 52.91.61.68 y su ubicación en Virginia, Estados Unidos?
- ¿Qué significa que la acción de seguridad sea “ALLOW” en el contexto de esta alerta?

- ¿Por qué es relevante el protocolo DNS en este tipo de alertas de seguridad?
- ¿Qué pasos seguirías para investigar más a fondo esta alerta y determinar si es una amenaza real?
- ¿Qué medidas de mitigación podrías implementar para prevenir futuras consultas a dominios maliciosos por parte de instancias de EC2?
- ¿Cómo afecta la severidad 'media' de esta alerta a la priorización de la respuesta por parte del SOC?
- ¿Qué rol juegan las tácticas de 'Command and Control' y las técnicas de 'Application Layer Protocol' en este tipo de incidentes?
- ¿Qué otras herramientas y servicios de AWS podrías utilizar para complementar la investigación de esta alerta de GuardDuty?

The screenshot shows the Google SecOps Alerts interface. The alert details are as follows:

- RUNDLL32 EXECUTE LONG FILENAME.**
- MANDIANT INTEL EMERGING THREATS**
- Status:** New
- Created:** 2024-06-24T13:23:27.422
- Severity:** Medium
- Priority:** Unspecified
- Risk score:** 65 - MED RISK
- Last updated:** 2024-06-24T13:23:27.422
- Tags:** TAG005, T1218.011
- Detection Rule:** Rundll32 execute long filename.
- Rule Set:** Mandiant Intel Emerging Threats
- Detection window:** 2024-06-24T10:04:00.000 to 2024-06-24T10:09:00.000
- Detection time:** 2024-06-24T10:09:00.000
- Rule Description:** Detects RUNDLL32 executing very long file name.

**DETECTION SUMMARY**

Detection Rule	Rule Set:	Detection window	Detection time	Rule Description
Rundll32 execute long filename.	Mandiant Intel Emerging Threats	2024-06-24T10:04:00.000 to 2024-06-24T10:09:00.000	2024-06-24T10:09:00.000	Detects RUNDLL32 executing very long file name.

**EVENTS**

TIMESTAMP	EVENT
2024-06-24T10:08:46.000	PROCESS_LAUNCH rundll32.exe launched by powershell.exe

The screenshot shows the Google SecOps Alerts & IOCs interface. The alert details are identical to the first screenshot. The graph visualization shows the following entities and their relationships:

- ASSET GROUP** (represented by a blue circle icon)
- USER GROUP** (represented by a green circle icon)
- RUNDLL32 EXECUTE LONG FILENAME.** (represented by a red triangle icon)
- Process Launch Event** (represented by a blue square icon)

The graph shows a flow from the Asset Group to the User Group, which then triggers the RUNDLL32 EXECUTE LONG FILENAME event, which in turn triggered the Process Launch event.

**GRAPH**

**EVENTS**

TIMESTAMP	EVENT	USER	HOSTNAME	PROCESS NAME
2024-06-24T10:08:46.000	PROCESS_LAUNCH rundll32.exe launched by powershell.exe	lisawalker	wins-d19	powershell.exe

## 1. ¿Qué es AWS GuardDuty y cuál es su función en la seguridad de AWS?

Amazon GuardDuty es un servicio de detección de amenazas que monitorea continuamente su

entorno de AWS para detectar posibles riesgos de seguridad. Analiza y procesa orígenes de datos fundamentales, como eventos de AWS CloudTrail administración, registros de AWS CloudTrail eventos, registros de flujo de VPC (de instancias de Amazon EC2) y registros de DNS.

## Funcionalidades

- Monitorea la actividad de las instancias de Amazon EC2 y cargas de trabajo de contenedores para detectar patrones inusuales de eventos de inicio de sesión y actividades maliciosas.
- Supervisa el comportamiento de acceso a las cuentas de AWS para detectar indicios de posibles riesgos, como despliegues de infraestructura no autorizados o llamadas inusuales a la API.
- Combina el machine learning y la inteligencia de amenazas integrada de AWS y de terceros líderes para ayudar a proteger las cuentas, las cargas de trabajo y los datos de AWS ante amenazas.
- Genera hallazgos detallados de seguridad para su visibilidad y corrección.
- Permite configurar alertas vía SNS ante hallazgos críticos.
- Ofrece una página para verificar el uso actual y estimar el uso futuro.

## Beneficios

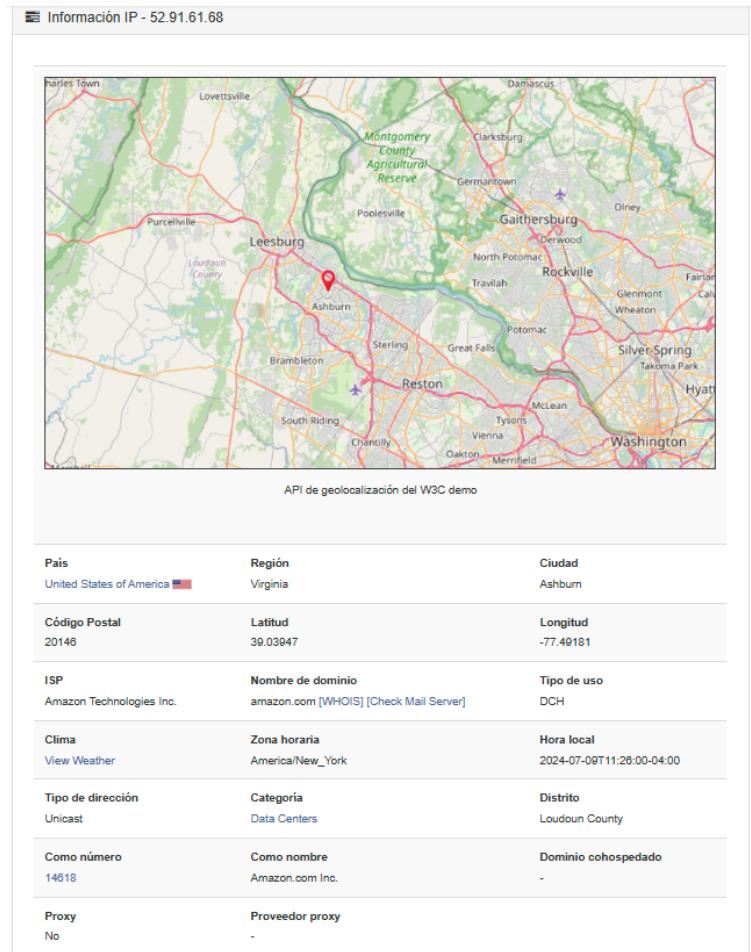
- Protege las cuentas, datos y recursos en varios tipos de cómputo de AWS, incluyendo Amazon Elastic Compute Cloud (Amazon EC2), cargas de trabajo sin servidor y cargas de trabajo en contenedores.
- Ayuda a identificar problemas en la red de AWS, como ataques cibernéticos u otras actividades no autorizadas.
- Permite localizar e identificar más fácilmente los problemas cibernéticos en el ecosistema de la nube.
- Ofrece una integración con Site24x7 para acceder a una prueba gratuita de 30 días.

### 2. ¿Cuál es la implicación de que una instancia de EC2 realice consultas a un dominio conocido por actividades maliciosas?

Si una instancia de EC2 realiza consultas DNS a un dominio conocido por actividades maliciosas, puede implicar que la instancia ha sido comprometida y está participando en una red de Command and Control (C2). Esto sugiere que la instancia puede estar exfiltrando datos, descargando malware adicional o siendo controlada remotamente por atacantes.

### 3. ¿Qué información puedes obtener de la dirección IP 52.91.61.68 y su ubicación en Virginia, Estados Unidos?

La dirección IP 52.91.61.68 es una dirección de AWS en la región de Virginia, Estados Unidos. Esta información indica que la instancia afectada está operando en uno de los centros de datos de AWS en esa región, lo que puede ayudar a localizar y manejar la instancia comprometida.



#### **4. ¿Qué significa que la acción de seguridad sea “ALLOW” en el contexto de esta alerta?**

En el contexto de esta alerta, que la acción de seguridad sea “ALLOW” significa que el tráfico no ha sido bloqueado y las comunicaciones entre la instancia EC2 y el dominio malicioso han sido permitidas. Esto puede ocurrir si no hay reglas de firewall o políticas de seguridad que restrinjan este tipo de tráfico.

#### **5. ¿Por qué es relevante el protocolo DNS en este tipo de alertas de seguridad?**

El protocolo DNS es relevante porque a menudo se utiliza por malware para resolver nombres de dominio y comunicarse con servidores C2. Las consultas DNS a dominios maliciosos pueden ser un indicador temprano de un compromiso de seguridad y pueden ayudar a identificar y detener actividades maliciosas antes de que causen más daño.

#### **6. ¿Qué pasos seguirías para investigar más a fondo esta alerta y determinar si es una amenaza real?**

**Pasos de investigación:**

1. **Identificar la instancia EC2 afectada:** Obtener detalles como el ID de la instancia, la cuenta de AWS y la región.
2. **Revisar los registros:** Analizar los registros de flujo de VPC, CloudTrail y CloudWatch Logs para identificar actividades sospechosas.
3. **Realizar un análisis forense:** Conectarse a la instancia (si es seguro) y analizar los procesos en ejecución, archivos sospechosos y configuraciones del sistema.
4. **Comprobar la integridad del sistema:** Verificar si hay cambios no autorizados en el sistema operativo y aplicaciones.
5. **Correlacionar con otras alertas:** Ver si hay alertas similares o relacionadas en GuardDuty u otros sistemas de monitoreo.

## 7. ¿Qué medidas de mitigación podrías implementar para prevenir futuras consultas a dominios maliciosos por parte de instancias de EC2?

### Medidas de mitigación:

- **Actualizar las reglas de seguridad:** Configurar grupos de seguridad y listas de control de acceso (ACL) para bloquear dominios y direcciones IP maliciosas.
- **Implementar listas negras de DNS:** Utilizar servicios de DNS seguros que bloquen automáticamente dominios maliciosos conocidos.
- **Aplicar parches de seguridad:** Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
- **Monitorización continua:** Configurar alertas y monitoreo continuo para detectar y responder a actividades sospechosas.
- **Segmentación de red:** Aislar las instancias críticas y limitar sus accesos a solo lo necesario.

## 8. ¿Cómo afecta la severidad “media” de esta alerta a la priorización de la respuesta por parte del SOC?

Una alerta de severidad “media” indica que la amenaza es potencialmente dañina pero no crítica. El SOC (Centro de Operaciones de Seguridad) debe priorizar estas alertas después de las alertas de alta severidad. Sin embargo, es importante no ignorarlas y realizar una investigación adecuada para prevenir un posible escalamiento de la amenaza.

## 9. ¿Qué rol juegan las tácticas de “Command and Control” y las técnicas de “Application Layer Protocol” en este tipo de incidentes?

**Tácticas de “Command and Control” (C2):** Permiten a los atacantes mantener comunicación con los sistemas comprometidos dentro de la red de la víctima. Utilizan técnicas como DNS tunneling para evadir la detección.

**Técnicas de “Application Layer Protocol”:** Involucran el uso de protocolos estándar (como HTTP, HTTPS, DNS) para comunicarse con servidores de C2. Estas técnicas son difíciles de detectar porque el tráfico parece legítimo.

**10. ¿Qué otras herramientas y servicios de AWS podrías utilizar para complementar la investigación de esta alerta de GuardDuty?**

**Herramientas y servicios adicionales de AWS:**

- **AWS CloudTrail:** Para auditar todas las acciones API realizadas en la cuenta de AWS.
- **AWS CloudWatch Logs:** Para monitorear y almacenar los registros de las instancias EC2 y otros recursos de AWS.
- **AWS Config:** Para evaluar y monitorear configuraciones de recursos y cambios.
- **AWS Security Hub:** Para centralizar las alertas de seguridad y realizar un análisis unificado.
- **Amazon Inspector:** Para analizar la seguridad de las instancias EC2 y aplicaciones.

Estos pasos y herramientas permitirán una investigación completa y una respuesta efectiva a la alerta de seguridad detectada por AWS GuardDuty.

## Tarea 7:

Imagina que trabajas como analista de nivel 1 en un SOC. Comienzan a llegar diferentes alertas, con severidades distintas (algunas con severidad “Low”, otras con “Medium”, “High” e incluso algunas con severidad “Critical”). En el siguiente enlace: [https://demo.backstory.chronicle.security/alerts?filtersOperator=AND&filters=%5B%7B%22type%22:%22feedback\\_summary.status%22,%22operator%22:%22!=%3D%22,%22values%22:%5B%22CLOSED%22,%22CLOSED%22%5D%7D%5D&timeRange=%7B%22start%22:%222024-06-23T23:00:00.000Z%22,%22end%22:%222024-06-24T23:00:00.000Z%22%7D](https://demo.backstory.chronicle.security/alerts?filtersOperator=AND&filters=%5B%7B%22type%22:%22feedback_summary.status%22,%22operator%22:%22!=%3D%22,%22values%22:%5B%22CLOSED%22,%22CLOSED%22%5D%7D%5D&timeRange=%7B%22start%22:%222024-06-23T23:00:00.000Z%22,%22end%22:%222024-06-24T23:00:00.000Z%22%7D), aplica el filtro para mostrar únicamente las alertas entre el día 23/06/2024 a las 00:00 hasta el día 24/06/2024 a las 00:00. Dentro de esas alertas:

- ¿Cuáles son las que hay que tratar con más “urgencia”?

Investiga acerca de cómo se suelen tratar las alertas dependiendo del grado de severidad. Por ejemplo:

- ¿Las alertas con severidad “Critical”, suelen analizarlas los analistas de nivel 1 o deben escalarlas directamente a los niveles 2? Comentar varios casos, dependiendo de la severidad. ¿Qué factores influyen a la hora de categorizar una alerta como “Critical” o cualquier otro nivel de severidad?

Google SecOps | Alerts

**ALERTS**

Welcome to Alerts and IoCs. Looking for alerts from other sources? Go to the [Legacy Enterprise Insights page](#)

Status: CLOSED (+1) | Refresh Time: None (default) | Showing: 2024-06-24 04:30:00 ...

**Filters**

STATE	NAME	RULE	PRIORITY	VERDICT	RISK SCORE	SEVERITY	CASE	DETECTION TIME	CREATE
New	rF1kBVVVV.bat	info_bat	Low	[Unspecified]	40	LOW RISK	Low	[n/a]	2024-06-25T00:12...
New	4qlNKe6gr.bat	info_bat	Low	[Unspecified]	40	LOW RISK	Low	[n/a]	2024-06-25T00:12...
New	UZZLnLpk.bat	info_bat	Low	[Unspecified]	40	LOW RISK	Low	[n/a]	2024-06-25T00:12...
New	CtofaTqR.bat	info_bat	Low	[Unspecified]	40	LOW RISK	Low	[n/a]	2024-06-25T00:12...
New	EIWIAJqV.bat	info_bat	Low	[Unspecified]	40	LOW RISK	Low	[n/a]	2024-06-25T00:12...
New	I1g2PtNoMPZB.bat	info_bat	Low	[Unspecified]	40	LOW RISK	Low	[n/a]	2024-06-25T00:12...
New	KnwFAstUnlZ.bat	info_bat	Low	[Unspecified]	40	LOW RISK	Low	[n/a]	2024-06-25T00:12...
New	victim_ip:10.12.13.45	SCC: Malware: Bad ...	[Unspecified]	[Unspecified]	40	LOW RISK	Low	[n/a]	2024-06-24T10:06...
New	victim_ip:10.12.13.44	SCC: Malware: Bad ...	[Unspecified]	[Unspecified]	40	LOW RISK	Low	[n/a]	2024-06-24T10:06...
New	file:3:c1c6d913d2b031d98...	gcti_malicious_file...	High	[Unspecified]	90	MED RISK	High	[n/a]	2024-06-24T10:06...
New	file:3:c1c6d913d2b031d98...	gcti_malicious_file...	High	[Unspecified]	90	MED RISK	High	[n/a]	2024-06-24T10:01...
New	victim_ip:10.12.13.44	SCC: Malware: Bad ...	[Unspecified]	[Unspecified]	40	LOW RISK	Low	[n/a]	2024-06-24T10:06...
New	victim_ip:10.12.13.45	SCC: Malware: Bad ...	[Unspecified]	[Unspecified]	40	LOW RISK	Low	[n/a]	2024-06-24T10:06...
New	hostname:oscar.wild.des...	google_safebrows...	High	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:03...
New	hostname:oscar.wild.des...	google_safebrows...	High	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:03...
New	hostname:oscar.wild.des...	google_safebrows...	High	[Unspecified]	95	HIGH RISK	Critical	[n/b]	2024-06-24T10:03...
New	hostname:DESKTOP1 has...	google_safebrows...	High	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:01...

Google SecOps | Alerts

**ALERTS**

Welcome to Alerts and IoCs. Looking for alerts from other sources? Go to the [Legacy Enterprise Insights page](#)

Status: CLOSED (+1) | Refresh Time: None (default) | Showing: 2024-06-24 04:30:00 ...

**Filters**

STATE	NAME	RULE	PRIORITY	VERDICT	RISK SCORE	SEVERITY	CASE	DETECTION TIME	CREATE
New	attacker_account:prodad...	SCC: Modify VPC S...	[Unspecified]	[Unspecified]	100	HIGH RISK	High	[n/a]	2024-06-24T10:36...
New	attacker_account:prodad...	SCC: Modify VPC S...	[Unspecified]	[Unspecified]	100	HIGH RISK	High	[n/a]	2024-06-24T10:36...
New	hostname:oscar.wild.des...	google_safebrows...	High	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:03...
New	hostname:oscar.wild.des...	google_safebrows...	High	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:03...
New	hostname:DESKTOP1 has...	google_safebrows...	High	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:01...
New	hostname:oscar.wild.des...	google_safebrows...	High	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:03...
New	hostname:esftp.cachemon...	google_safebrows...	High	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:26...
New	hostname:oscar.wild.des...	google_safebrows...	High	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:03...
New	hostname:stevemorris-pc...	google_safebrows...	High	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:02...
New	hostname:mikeross-pc	suspicious_downlo...	Critical	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:04...
New	hostname:steve-watson-pc	suspicious_downlo...	Critical	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:08...
New	hostname:steve-watson-pc	suspicious_downlo...	Critical	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:08...
New	hostname:mikeross-pc	suspicious_downlo...	Critical	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T10:04...
New	hostname:alice-benjamin...	suspicious_downlo...	Critical	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T13:48...
New	hostname:alice-benjamin...	suspicious_downlo...	Critical	[Unspecified]	95	HIGH RISK	Critical	[n/a]	2024-06-24T13:48...
New	ip:185.220.101.42	Successful AWS AP...	[Unspecified]	[Unspecified]	95	HIGH RISK	High	[n/a]	2024-06-24T09:48...

**Filters**

Logical Operator AND

Filter	Show Only	Value
Author		
Case		
Priority		
Reputation		
Rule		
Rule Id		
Severity		
Source		
Status		

Logical Operator AND

Rule Id	Show Only	Value
Case		
Priority		
Reputation		
Rule		
Rule Id		
Severity		
Source		
Status		
Verdict		

**Cancel** **Apply** **Cancel** **Apply**

## **¿Cuáles son las que hay que tratar con más “urgencia”?**

Las alertas están clasificadas con diferentes niveles de severidad: Low, Medium, High y Critical. Las alertas critical y High son las que hay que tratar con más urgencia.

Pasos a Seguir para Priorizar Alertas:

### **1. Identificar Alertas Críticas y de Alta Prioridad:**

- Las alertas con severidad “Critical” y “High” deben ser tratadas con la mayor urgencia.
- Ejemplos de alertas críticas en las capturas incluyen aquellas con un Risk Score de 95 y calificadas como “Critical”.

### **2. Evaluar las Alertas de Severidad Media y Baja:**

- Las alertas con severidad “Medium” y “Low” pueden ser tratadas con menor urgencia, dependiendo de los recursos disponibles y del contexto de la alerta.

**Investiga acerca de cómo se suelen tratar las alertas dependiendo del grado de severidad.**

**Por ejemplo:**

**¿Las alertas con severidad “Critical”, suelen analizarlas los analistas de nivel 1 o deben escalarlas directamente a los niveles 2?**

Las alertas con severidad “Critical” suelen requerir una respuesta rápida y coordinada. Los analistas de nivel 1 son responsables de la monitorización inicial, evaluación rápida para confirmar su veracidad y determinar la naturaleza del incidente. Pueden tomar medidas inmediatas según procedimientos predefinidos, como aislar un sistema afectado, detener procesos maliciosos, y realizar análisis básicos. Si la alerta es confirmada como “Critical” y requiere una investigación más profunda o acciones más complejas, los analistas de nivel 1 escalan la alerta a los analistas de nivel 2.

**Comentar varios casos, dependiendo de la severidad.**

## **Manejo de Alertas según la Severidad**

### **Alertas de Severidad "Critical"**

#### **Caso 1: Ransomware Detectado**

- **Acción Nivel 1:** El analista de nivel 1 detecta el ransomware y aísla inmediatamente los sistemas afectados para evitar la propagación.

- **Escalación:** Escala la alerta al nivel 2 para análisis forense detallado y coordinación con el equipo de TI para restaurar sistemas y datos.
- **Acción Nivel 2:** El analista de nivel 2 realiza un análisis completo del ransomware, identifica la fuente y colabora con otros equipos para la recuperación y medidas preventivas.

### **Caso 2: Acceso No Autorizado a Datos Sensibles**

- **Acción Nivel 1:** Detecta el acceso no autorizado y bloquea las credenciales comprometidas.
- **Escalación:** Escala al nivel 2 para investigar la extensión de la brecha y coordinar con el equipo legal y de cumplimiento.
- **Acción Nivel 2:** Realiza una revisión exhaustiva de los logs, identifica los datos comprometidos, y ayuda en la notificación de la brecha a las autoridades y clientes afectados.

### **Alertas de Severidad "High"**

#### **Caso 1: Malware Detectado en un Sistema Crítico**

- **Acción Nivel 1:** El analista de nivel 1 aísla el sistema afectado y ejecuta un análisis antivirus.
- **Escalación:** Escala al nivel 2 si el malware es sofisticado o requiere análisis avanzado.
- **Acción Nivel 2:** Realiza un análisis detallado del malware, remueve cualquier persistencia y asegura que el sistema está completamente limpio.

#### **Caso 2: Phishing Dirigido a Ejecutivos**

- **Acción Nivel 1:** Detecta el intento de phishing y alerta a los ejecutivos potencialmente afectados.
- **Escalación:** Escala al nivel 2 para una investigación más profunda y la implementación de medidas adicionales de seguridad.
- **Acción Nivel 2:** Investiga el origen del phishing, refuerza las defensas de correo electrónico y educa a los ejecutivos sobre prácticas seguras.

### **Alertas de Severidad "Medium"**

#### **Caso 1: Software No Autorizado Instalado**

- **Acción Nivel 1:** Detecta y desinstala el software no autorizado, documentando el incidente.
- **Escalación:** Puede escalar al nivel 2 si hay indicios de actividad maliciosa relacionada.
- **Acción Nivel 2:** Realiza un análisis más profundo para asegurar que no haya persistencia de malware o acceso no autorizado.

#### **Caso 2: Intentos de Acceso Fallidos Repetidos**

- **Acción Nivel 1:** Monitorea y bloquea la cuenta después de múltiples intentos fallidos.
- **Escalación:** Escala al nivel 2 si los intentos parecen ser parte de un ataque dirigido.
- **Acción Nivel 2:** Investiga la fuente de los intentos de acceso, implementa medidas adicionales de seguridad como la autenticación multifactor.

## **Alertas de Severidad "Low"**

### **Caso 1: Actualización de Software Pendiente**

- **Acción Nivel 1:** Programa la actualización y notifica al equipo de TI.
- **Escalación:** No suele escalarse al nivel 2 a menos que la actualización pendiente tenga implicaciones críticas de seguridad.
- **Acción Nivel 2:** Si es necesario, asegura que la actualización se realice sin interrupciones importantes.

### **Caso 2: Acceso Inusual a Recursos de Red**

- **Acción Nivel 1:** Monitorea y documenta el acceso, revisa los permisos del usuario.
- **Escalación:** Escala al nivel 2 si el acceso inusual sugiere una posible intrusión.
- **Acción Nivel 2:** Investiga el acceso, revisa los logs de seguridad, y ajusta las políticas de acceso si es necesario.

**¿Qué factores influyen a la hora de categorizar una alerta como “Critical” o cualquier otro nivel de severidad?**

## **Factores que Influyen en la Categoría de Severidad de una Alerta**

### **1. Impacto Potencial:**

- **Crítico:** Puede causar un daño significativo a la organización, como la pérdida de datos sensibles, interrupción de operaciones críticas, o comprometer la integridad del sistema.
- **Alto:** Puede tener un impacto considerable pero no catastrófico, como la afectación de servicios importantes o el acceso no autorizado a datos relevantes.
- **Medio:** Puede causar problemas moderados que requieren atención, como la instalación de software no autorizado o intentos de acceso fallidos.
- **Bajo:** Tiene un impacto mínimo o insignificante y puede ser manejado rutinariamente sin mayores consecuencias.

### **2. Alcance del Incidente:**

- **Número de Sistemas Afectados:** Un incidente que afecta a múltiples sistemas o usuarios se categoriza con mayor severidad.
- **Sensibilidad de los Datos Comprometidos:** La exposición de datos altamente sensibles aumenta la severidad de la alerta.

### **3. Probabilidad de Propagación:**

- **Capacidad de Expandirse:** Si el incidente puede propagarse rápidamente a otros sistemas o redes, se categoriza con mayor severidad.
- **Facilidad de Contención:** Incidentes difíciles de contener tienden a ser más graves.

#### 4. Tipo de Amenaza:

- **Malware, Ransomware, Phishing, etc.:** Algunas amenazas son inherentemente más peligrosas que otras, lo que afecta la severidad de la alerta.
- **Sofisticación del Ataque:** Ataques avanzados y persistentes (APT) se consideran más severos.

#### 5. Contexto y Entorno:

- **Contexto Organizacional:** La criticidad puede variar según el entorno específico de la organización y el momento del incidente (por ejemplo, durante una auditoría o un evento crítico de negocio).
- **Criterios Regulatorios y de Cumplimiento:** Incidentes que pueden poner en riesgo el cumplimiento de normativas legales o regulatorias.

#### 6. Alertas Previas y Patrones:

- **Historial de Incidentes:** Incidentes recurrentes o patrones pueden indicar una amenaza subyacente más seria.
- **Frecuencia de Alertas Similares:** Una alta frecuencia de alertas similares puede elevar la severidad.

#### 7. Disponibilidad de Recursos:

- **Capacidad de Respuesta:** La disponibilidad de recursos humanos y técnicos para manejar el incidente puede influir en la categorización.
- **Nivel de Preparación:** La existencia de planes de respuesta y la preparación del equipo para manejar incidentes específicos.

#### 8. Detección y Mitigación:

- **Tiempo de Detección:** Incidentes detectados tarde pueden ser más graves debido a la posible extensión del daño.
- **Efectividad de las Medidas de Mitigación:** La capacidad de mitigar rápidamente el impacto del incidente.

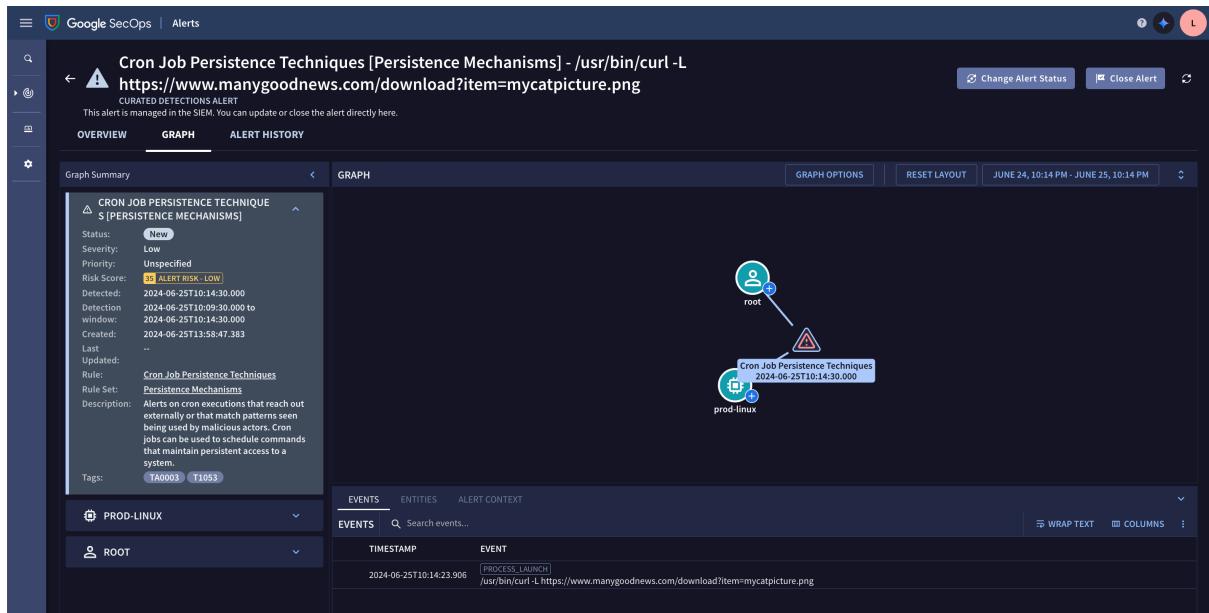
## Tarea 8:

### Utilizando esta información

([https://demo.backstory.chronicle.security/alerts/de\\_196d5688-d49a-4510-3adb-8743f2a7b445/graph](https://demo.backstory.chronicle.security/alerts/de_196d5688-d49a-4510-3adb-8743f2a7b445/graph)), resuelve las siguientes preguntas:

- ¿Cuál es el propósito del comando lanzado por el proceso CRON?
- ¿Qué implicaciones de seguridad podría tener la ejecución del comando mencionado?

- ¿Cómo se relacionan los diferentes campos de metadatos entre sí para proporcionar contexto sobre el evento?
- ¿Por qué es relevante el timestamp de ingesta (Ingested Timestamp) comparado con el timestamp del evento (Event Timestamp)?
- ¿Qué medidas preventivas podrías sugerir para evitar posibles riesgos asociados con este tipo de eventos?



## Análisis del Evento de Alerta CRON Job

### Propósito del Comando Lanzado por el Proceso CRON

El comando ejecutado es:

```
/usr/bin/curl -L https://www.manygoodnews.com/download?item=mycatpicture.png
```

El propósito de este comando es descargar un archivo desde la URL [www.manygoodnews.com](https://www.manygoodnews.com) utilizando curl, una herramienta de línea de comandos para transferir datos con sintaxis URL. En este caso, parece que el comando intenta descargar una imagen llamada "mycatpicture.png".

### Implicaciones de Seguridad de la Ejecución del Comando Mencionado

Las implicaciones de seguridad de este comando son múltiples:

- **Descarga de Archivos Maliciosos:** La URL podría alojar archivos maliciosos, como malware o scripts que comprometan el sistema.
- **Escalada de privilegios.**
- **Persistencia:** Si este comando es parte de un cron job recurrente, puede ser una técnica de persistencia utilizada por un atacante para mantener acceso al sistema.

- **Transferencia de Datos:** El archivo descargado podría contener comandos adicionales que envíen datos sensibles del sistema a actores maliciosos.

## **Relación entre los Diferentes Campos de Metadatos**

Los diferentes campos de metadatos se relacionan entre sí para proporcionar un contexto completo y detallado sobre el evento de seguridad.

### **1. Identificación del Evento**

- **metadata.id**
  - **Descripción:** Un identificador único que permite rastrear y referenciar el evento específico.
  - **Relación:** Este ID se relaciona con todos los demás campos, ya que identifica de manera única este evento específico en el sistema.

### **2. Contexto Temporal**

- **metadata.event\_timestamp**
  - **Descripción:** Marca el momento exacto en el que ocurrió el evento.
  - **Relación:** Proporciona un punto de referencia temporal que se puede correlacionar con otros eventos y actividades en el sistema.
- **metadata.ingested\_timestamp**
  - **Descripción:** Indica cuándo el evento fue registrado en el sistema de monitoreo.
  - **Relación:** Permite comparar el tiempo entre la ocurrencia del evento y su registro, lo cual es útil para detectar retrasos en la detección o el procesamiento.

### **3. Tipo y Origen del Evento**

- **metadata.event\_type**
  - **Descripción:** Especifica el tipo de evento, en este caso, “PROCESS\_LAUNCH”.
  - **Relación:** Ayuda a categorizar el evento y entender qué tipo de actividad se está registrando.
- **metadata.log\_type**
  - **Descripción:** Indica el tipo de sistema de registro, como “NIX\_SYSTEM”.
  - **Relación:** Proporciona contexto sobre el entorno del evento, permitiendo identificar si se trata de un sistema Unix, Windows, etc.

### **4. Información del Sistema y Producto**

- **metadata.product\_name**
  - **Descripción:** Nombre del producto o sistema involucrado, como “Unix System”.
  - **Relación:** Ayuda a identificar el entorno específico en el que ocurrió el evento.

### **5. Información del Activo Principal**

- **principal.asset.hostname**
  - **Descripción:** Nombre del host del activo principal.
  - **Relación:** Identifica el sistema específico donde ocurrió el evento.
- **principal.asset.ip[0]**
  - **Descripción:** Dirección IP del activo principal.
  - **Relación:** Proporciona una dirección de red específica para identificar y rastrear el activo.
- **principal.asset.mac[0]**
  - **Descripción:** Dirección MAC del activo principal.
  - **Relación:** Ofrece una identificación única a nivel de hardware para el dispositivo involucrado.
- **principal.hostname, principal.ip[0], principal.mac[0]**
  - **Descripción:** Información adicional del host principal.
  - **Relación:** Refuerza la identificación del dispositivo, asegurando que se tiene una visión completa de su identidad y conectividad.

## 6. Acciones y Procesos

- **target.application**
  - **Descripción:** La aplicación involucrada en el evento, como “CRON”.
  - **Relación:** Indica el contexto específico del evento, detallando qué aplicación inició la acción.
- **target.process.command\_line**
  - **Descripción:** Comando ejecutado, como “/usr/bin/curl -L <https://www.manygoodnews.com/download?item=mycatpicture.png>”.
  - **Relación:** Proporciona detalles específicos sobre lo que se ejecutó, lo cual es crucial para entender la naturaleza del evento.
- **target.process.pid**
  - **Descripción:** Identificador del proceso.
  - **Relación:** Permite rastrear y gestionar el proceso específico en el sistema.
- **target.user.userid**
  - **Descripción:** ID del usuario que ejecutó el proceso, como “root”.
  - **Relación:** Ofrece información sobre el nivel de acceso y permisos del usuario, ayudando a evaluar el riesgo y la legitimidad del evento.

## 7. Etiquetas y Permisos

- **metadata.base\_labels.allow\_scoped\_access**
  - **Descripción:** Indica si se permite el acceso restringido a los datos base.
  - **Relación:** Define el nivel de acceso y seguridad aplicable a estos datos.
- **metadata.enrichment\_labels.allow\_scoped\_access**
  - **Descripción:** Indica si se permite el acceso restringido a los datos enriquecidos.
  - **Relación:** Similar al anterior, pero aplicado a datos enriquecidos.

## Integración del Contexto Completo

Todos estos campos se integran para proporcionar una visión detallada del evento:

- Identificación:** Se sabe exactamente qué evento está siendo analizado gracias al metadata.id.
- Temporalidad:** Se puede determinar cuándo ocurrió el evento (metadata.event\_timestamp) y cuándo fue registrado (metadata.ingested\_timestamp).
- Tipo y Origen:** Se conoce el tipo de evento (metadata.event\_type) y el entorno en el que ocurrió (metadata.log\_type y metadata.product\_name).
- Activos Involucrados:** Se identifica el dispositivo específico (principal.asset.hostname, principal.asset.ip[0], principal.asset.mac[0]).
- Acciones:** Se detalla la acción específica que tuvo lugar (target.application, target.process.command\_line, target.process.pid, target.user.userid).
- Permisos y Seguridad:** Se sabe si los datos están restringidos y qué nivel de acceso es permitido (metadata.base\_labels.allow\_scoped\_access, metadata.enrichment\_labels.allow\_scoped\_access).

Esta interrelación permite a los analistas de seguridad entender no solo lo que ocurrió, sino también el contexto en el que ocurrió, quién estuvo involucrado, y qué nivel de riesgo representa el evento.

The screenshot displays the 'EVENT VIEWER' interface with two main sections of 'UDM FIELDS':

**Top Section:**

- intermediary[0].hostname: "prod-linux"
- metadata.base\_labels.allow\_scoped\_access: true
- metadata.base\_labels.log\_types[0]: "NIX\_SYSTEM"
- metadata.enrichment\_labels.allow\_scoped\_access: true
- metadata.enrichment\_labels.log\_types[0]: "INFOBLOX\_DHCP"
- metadata.event\_timestamp: "2024-06-25T04:44:23.906624Z"
- metadata.event\_type: "PROCESS\_LAUNCH"
- metadata.id: b"AAAAAN+mRItQ7K9T+0qLo5WNbLIAAAAABgAAAAAAAAA="
- metadata.ingested\_timestamp: "2024-06-25T06:03:29.073148Z"
- metadata.log\_type: "NIX\_SYSTEM"
- metadata.product\_name: "Unix System"
- principal.asset.hostname: "prod-linux"
- principal.asset.ip[0]: "10.220.10.11"
- principal.asset.mac[0]: "0a:6f:30:0a:51:a1"

**Bottom Section:**

- principal.hostname: "prod-linux"
- principal.ip[0]: "10.220.10.11"
- principal.mac[0]: "0a:6f:30:0a:51:a1"
- target.application: "CRON"
- target.process.command\_line: "/usr/bin/curl -L https://www.manygoodnews.com/download?item=mycatpicture.png"
- target.process.pid: "28525"
- target.user.userid: "root"

## Relevancia del Timestamp de Ingesta Comparado con el Timestamp del Evento

- **Timestamp del Evento (Event Timestamp):** Marca el momento exacto en el que ocurrió la actividad sospechosa. “2024-06-25T04:44:23.906624Z”
- **Timestamp de Ingesta (Ingested Timestamp):** Indica cuándo el sistema de monitoreo recogió y registró la actividad. Es importante porque puede haber un retraso entre la ocurrencia del evento y su detección, afectando la rapidez de la respuesta. “2024-06-25T06:03:29.073148Z”

### **Medidas Preventivas para Evitar Riesgos Asociados**

- **Validación de Comandos CRON:** Revisión y validación regular de todos los cron jobs configurados en el sistema.
- **Restricciones de Red:** Implementar controles para restringir las descargas desde URLs desconocidas o no verificadas.
- **Monitoreo de Integridad de Archivos:** Usar herramientas de monitoreo para detectar cambios no autorizados en archivos críticos del sistema.
- **Actualización y Parches:** Mantener el sistema y sus aplicaciones actualizadas con los últimos parches de seguridad.
- **Autenticación y Autorización:** Asegurar que solo usuarios autorizados puedan modificar los cron jobs y ejecutar comandos de descarga.
- **Análisis de Tráfico:** Implementar sistemas de detección de intrusiones (IDS) para monitorear tráfico de red sospechoso.

Estas medidas, combinadas con una revisión constante de las políticas de seguridad y auditorías regulares, pueden ayudar a mitigar riesgos y proteger el sistema contra amenazas similares.

### **Tarea 9:**

A la hora de analizar las alertas, se puede apreciar que existe un apartado denominado “Tags”. En este suelen aparecer una información con la forma “TAXXXX”, TXXXX” y/o “TXXXX.XXX”:

[https://demo.backstory.chronicle.security/alerts?filtersOperator=AND&filters=%5B%7B%22type%22:%22feedback\\_summary.status%22,%22operator%22:%22!%3D%22,%22values%22:%5B%22CLOSED%22,%22CLOSED%22%5D%7D%5D&timeRange=%7B%22start%22:%222024-06-23T23:00:00.000Z%22,%22end%22:%222024-06-24T23:00:00.000Z%22%7D](https://demo.backstory.chronicle.security/alerts?filtersOperator=AND&filters=%5B%7B%22type%22:%22feedback_summary.status%22,%22operator%22:%22!%3D%22,%22values%22:%5B%22CLOSED%22,%22CLOSED%22%5D%7D%5D&timeRange=%7B%22start%22:%222024-06-23T23:00:00.000Z%22,%22end%22:%222024-06-24T23:00:00.000Z%22%7D)

The screenshot shows a table of alerts with the following columns: RISK SCORE, SEVERITY, CASE, DETECTION TIME, CREATED, LAST MODIFIED, SOURCE, and TAGS. The alert details include:

	RISK SCORE	SEVERITY	CASE	DETECTION TIME	CREATED	LAST MODIFIED	SOURCE	TAGS
Case (1)	695	LOW RISK	Low	[n/a]	2024-06-25T00:12...	2024-06-25T00:13...	2024-06-25T00:13...	Custom Rule
Rule (60)	695	LOW RISK	Low	[n/a]	2024-06-25T00:12...	2024-06-25T00:13...	2024-06-25T00:13...	Custom Rule
Priority (5)	695	LOW RISK	Low	[n/a]	2024-06-25T00:12...	2024-06-25T00:13...	2024-06-25T00:13...	Custom Rule
Severity (6)	695	LOW RISK	Low	[n/a]	2024-06-25T00:12...	2024-06-25T00:13...	2024-06-25T00:13...	Custom Rule
Status (1)	695	LOW RISK	Low	[n/a]	2024-06-25T00:12...	2024-06-25T00:13...	2024-06-25T00:13...	Custom Rule
Verdict (1)	695	LOW RISK	Low	[n/a]	2024-06-24T10:06...	2024-06-24T22:10...	2024-06-24T22:10...	Curated Det... TA0011 T1568
Source (2)	695	LOW RISK	Low	[n/a]	2024-06-24T10:06...	2024-06-24T22:10...	2024-06-24T22:10...	Curated Det... TA0011 T1568
		MED RISK	High	[n/a]	2024-06-24T10:01...	2024-06-24T21:39...	2024-06-24T21:39...	Custom Rule
		MED RISK	High	[n/a]	2024-06-24T10:06...	2024-06-24T21:39...	2024-06-24T21:39...	Custom Rule
		LOW RISK	Low	[n/a]	2024-06-24T10:06...	2024-06-24T21:38...	2024-06-24T21:38...	Curated Det... TA0011 T1568
		LOW RISK	Low	[n/a]	2024-06-24T10:06...	2024-06-24T21:38...	2024-06-24T21:38...	Curated Det... TA0011 T1568
		HIGH RISK	Critical	[n/a]	2024-06-24T10:03...	2024-06-24T21:33...	2024-06-24T21:33...	Custom Rule
		HIGH RISK	Critical	[n/a]	2024-06-24T10:03...	2024-06-24T21:33...	2024-06-24T21:33...	Custom Rule
		HIGH RISK	Critical	[n/a]	2024-06-24T10:01...	2024-06-24T21:33...	2024-06-24T21:33...	Custom Rule

- Investiga sobre qué son estas etiquetas y las diferencias entre las tres formas mencionadas.
- ¿Por qué es útil trabajar con estas etiquetas? ¿Cómo pueden ayudar a la hora de realizar un buen análisis de una alerta?
- Por ejemplo, en la siguiente alerta, ¿en qué consisten las etiquetas que aparecen?

[https://demo.backstory.chronicle.security/alerts/de\\_45172954-9550-0f99-67c1-919d4a7fd8aa/overview](https://demo.backstory.chronicle.security/alerts/de_45172954-9550-0f99-67c1-919d4a7fd8aa/overview)

The alert details page shows the following information:

OVERVIEW		GRAPH		ALERT HISTORY													
<b>AWS API Access by root User [AWS - Identity] - arn:aws:iam::987127836822:root - unknown resource</b> <small>CURATED DETECTIONS ALERT</small> This alert is managed in the SIEM. You can update or close the alert directly here.				<a href="#">Change Alert Status</a> <a href="#">Close Alert</a>													
Status	Created	Severity	Priority	Risk score	Last updated												
NEW	2024-06-23T14:29:48.536	High	Unspecified	75 MED RISK	2024-06-23T14:29:48.536												
<b>Tags</b> TA0094 T1078.001																	
<b>DETECTION SUMMARY</b> <table border="1"> <tr> <td>Detection Rule</td> <td>Rule Set:</td> <td>Detection window</td> <td>Detection time</td> <td>Rule Description</td> <td><a href="#">View Other Alerts From This Rule</a></td> </tr> <tr> <td>AWS API Access by root User</td> <td>AWS - Identity</td> <td>2024-06-22T10:30:00.000 to 2024-06-23T10:30:00.000</td> <td>2024-06-23T10:30:00.000</td> <td>Detects root user account API activity.</td> <td></td> </tr> </table>						Detection Rule	Rule Set:	Detection window	Detection time	Rule Description	<a href="#">View Other Alerts From This Rule</a>	AWS API Access by root User	AWS - Identity	2024-06-22T10:30:00.000 to 2024-06-23T10:30:00.000	2024-06-23T10:30:00.000	Detects root user account API activity.	
Detection Rule	Rule Set:	Detection window	Detection time	Rule Description	<a href="#">View Other Alerts From This Rule</a>												
AWS API Access by root User	AWS - Identity	2024-06-22T10:30:00.000 to 2024-06-23T10:30:00.000	2024-06-23T10:30:00.000	Detects root user account API activity.													
<b>EVENTS</b> <table border="1"> <thead> <tr> <th>TIMESTAMP</th> <th>EVENT</th> <th>WRAP TEXT</th> <th>COLUMNS</th> </tr> </thead> <tbody> <tr> <td>2024-06-23T10:13:20.000</td> <td>[RESOURCE_WRITTEN] arn:aws:iam::987127836822:root - unknown resource</td> <td></td> <td></td> </tr> <tr> <td>2024-06-23T10:10:25.000</td> <td>[RESOURCE_CREATION] arn:aws:iam::987127836822:root - unknown resource</td> <td></td> <td></td> </tr> </tbody> </table>						TIMESTAMP	EVENT	WRAP TEXT	COLUMNS	2024-06-23T10:13:20.000	[RESOURCE_WRITTEN] arn:aws:iam::987127836822:root - unknown resource			2024-06-23T10:10:25.000	[RESOURCE_CREATION] arn:aws:iam::987127836822:root - unknown resource		
TIMESTAMP	EVENT	WRAP TEXT	COLUMNS														
2024-06-23T10:13:20.000	[RESOURCE_WRITTEN] arn:aws:iam::987127836822:root - unknown resource																
2024-06-23T10:10:25.000	[RESOURCE_CREATION] arn:aws:iam::987127836822:root - unknown resource																

## Investigación sobre Etiquetas (Tags) en Alertas

- ¿Qué son estas etiquetas y las diferencias entre las tres formas mencionadas?

Las etiquetas (tags) en el contexto de las alertas de seguridad suelen ser identificadores que permiten clasificar y categorizar las alertas para facilitar su análisis y gestión.

### 1. TAXXXX:

- Estas etiquetas suelen ser taxonomías o identificadores que permiten agrupar las alertas bajo una categoría específica. Pueden estar basadas en normas o estándares de la industria para clasificar incidentes de seguridad.
- Ejemplo: TA0011 podría referirse a un tipo específico de ataque o técnica de intrusión.

### 2. TXXXX:

- Similar a la forma anterior, pero más general. Pueden ser etiquetas internas utilizadas para clasificar eventos según criterios definidos por el sistema o la organización.
- Ejemplo: T1058 podría referirse a una técnica específica de ataque o una actividad sospechosa.

### 3. TXXXX.XXX:

- Estas etiquetas suelen ser más detalladas y pueden referirse a subcategorías o variantes específicas dentro de una categoría principal. La parte después del punto podría indicar una subdivisión o un detalle adicional.
- Ejemplo: T1078.001 podría especificar una sub-técnica dentro de una técnica de ataque principal.

## Utilidad de trabajar con estas etiquetas

Trabajar con estas etiquetas es útil por varias razones:

1. **Clasificación y Organización:** Facilita la organización de alertas en categorías, lo que ayuda a priorizar y gestionar grandes volúmenes de datos de seguridad.
2. **Análisis Rápido:** Permite a los analistas de seguridad identificar rápidamente el tipo de amenaza y su gravedad, agilizando la respuesta a incidentes.
3. **Correlación de Datos:** Ayuda a correlacionar eventos similares, identificar patrones de ataque y comprender mejor el contexto de las amenazas.
4. **Automatización:** Las etiquetas pueden ser utilizadas en scripts y herramientas automatizadas para clasificar y responder automáticamente a ciertos tipos de alertas.

## Por ejemplo, en la siguiente alerta, ¿en qué consisten las etiquetas que aparecen?

En la segunda captura se pueden ver las etiquetas del enlace, **TA0004** y **T1078.001**. Según el MITRE podemos detallar lo siguiente.

- **TA0004:** es escala de privilegios para obtener permisos de alto nivel en un sistema o red.

- **T1078.001:** es una subtécnica de T1078 sobre cuentas válidas. Los adversarios pueden abusar y utilizar credenciales de una cuenta predeterminada como medio para obtener acceso inicial, persistencia, escalada de privilegios o evasión de defensas.

Estas etiquetas ayudan a los analistas a comprender rápidamente el contexto y la naturaleza de la alerta, permitiendo una respuesta más efectiva y eficiente.

ATT&CKcon 5.0 returns October 22-23, 2024 in McLean, VA. Stay tuned for registration details!

Home > Tactics > Enterprise > Privilege Escalation

## Privilege Escalation

The adversary is trying to gain higher-level permissions.

Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

Examples of elevated access include:

- SYSTEM/root level
- local administrator
- user account with admin-like access
- user accounts with access to specific system or perform specific function

These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.

**ID:** TA0004  
**Created:** 17 October 2018  
**Last Modified:** 06 January 2021

[Version Permalink](#)

ATT&CKcon 5.0 returns October 22-23, 2024 in McLean, VA. Stay tuned for registration details!

Home > Techniques > Enterprise > Valid Accounts > Default Accounts

## Valid Accounts: Default Accounts

Other sub-techniques of Valid Accounts (4) ▾

Adversaries may obtain and abuse credentials of a default account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Default accounts are those that are built-into an OS, such as the Guest or Administrator accounts on Windows systems. Default accounts also include default factory/provider set accounts on other types of systems, software, or devices, including the root user account in AWS and the default service account in Kubernetes.<sup>[1][2][3]</sup>

Default accounts are not limited to client machines, rather also include accounts that are preset for equipment such as network devices and computer applications whether they are internal, open source, or commercial. Appliances that come preset with a username and password combination pose a serious threat to organizations that do not change it post installation, as they are easy targets for an adversary. Similarly, adversaries may also utilize publicly disclosed or stolen [Private Keys](#) or credential materials to legitimately connect to remote environments via [Remote Services](#).<sup>[4]</sup>

**ID:** T1078.001  
**Sub-technique of:** [T1078](#)

① **Tactics:** [Defense Evasion](#), [Persistence](#), [Privilege Escalation](#), [Initial Access](#)

① **Platforms:** Azure AD, Containers, Google Workspace, IaaS, Linux, Network, Office 365, SaaS, Windows, macOS

① **Permissions Required:** Administrator, User  
**Version:** 1.3  
**Created:** 13 March 2020  
**Last Modified:** 07 March 2024

[Version Permalink](#)

## Tarea 10:

Para finalizar se investigará un incidente crítico en el SIEM relacionado con una descarga sospechosa. En este caso deberás actuar como un analista N1 e informar al cliente lo mejor que puedas acerca de la incidencia ocurrida. Puedes imaginar que la persona involucrada en el incidente es parte de la empresa del cliente al que monitorizas. El link

de la alerta es el siguiente: [https://demo.backstory.chronicle.security/alerts/de\\_f23307f6-462c-3846-dc3e-03ea2ffdd39b/overview](https://demo.backstory.chronicle.security/alerts/de_f23307f6-462c-3846-dc3e-03ea2ffdd39b/overview)

- ¿Por qué crees que esta incidencia puede considerarse crítica?
- Investiga los dos eventos de la alerta (dando click en cada uno de ellos) y asegúrate de recopilar únicamente la información relevante para mandarla al cliente: datos de la persona involucrada, sus acciones y por qué esto puede ser peligroso para la empresa.
- Por último, puedes proponer acciones recomendadas para contener esta acción o asegurarse de que la acción no tendrá mayor incidencia.

The screenshot shows the Google SecOps Alert Overview page for a custom rule alert titled "suspicious\_download\_office - hostname:steve-watson-pc". The alert is managed in the SIEM and is currently in a NEW state. It was created on 2024-06-24T16:33:22.493. The severity is Critical, priority is Critical, and the risk score is HIGH RISK (95). The detection window spans from 2024-06-24T10:03:00.000 to 2024-06-24T10:08:00.000. The rule description indicates an Office Application downloading an executable(.exe) in URL or a suspiciously large file(>100KB). The detection summary table shows two events: a NETWORK.HTTP event at 2024-06-24T10:07:32.000 where steve-watson sent data to manygoodnews.com, and a PROCESS.LAUNCH event at 2024-06-24T10:03:32.426 where EXCEL.exe was launched by 22895. The events section lists these two events with their timestamps and details.

The screenshot shows the Google SecOps Search page. A search query "principal.ip = \"10.205.11.20\" is entered in the search bar. The search results show one event from June 24, 10:05 AM to June 24, 10:10 AM. The event details are displayed in the EVENTS section, showing a timestamp of 2024-06-24T10:07:32.000, an ALERT event type, a NETWORK source, and destination, and a user steve-watson on host steve-watson-pc. The search interface includes a timeline, aggregation fields, and an event viewer pane showing entities like 10.205.11.20, 1a:78:d0:1a:51:32, steve-watson-pc, and manygoodnews.com.

The screenshot shows the Google SecOps interface. In the search bar, the query "principal.ip = \"10.205.11.20\" is entered. The results show 3 filtered events and 4 query events. The timeline highlights specific event times. The event viewer displays details for three events, including timestamp, event type (e.g., PROCESS.L), user, hostname, and process name. The entity list on the right shows various IP addresses and their associated entities.

The screenshot shows detections for rule ru\_4419ba3f-3858-40c1-8d06-e47f61d2cae2. The detections table lists events for users steve-watson, mikeross, and alice across various hostnames and process names. The timeline chart shows the number of detections over time, with a callout highlighting 3 distinct detections on Jun 24, 2024 (UTC).

## ¿Por qué crees que esta incidencia puede considerarse crítica?

Esta es una alerta que indica la descarga de una Aplicación de Office descargando un archivo ejecutable (.exe desde URL) o un archivo sospechosamente grande (más de 100 KB).

La alerta es clasificada como crítica debido a los siguientes motivos:

- Descarga de Ejecutables:** La regla de detección específica que se detectó una aplicación de Office descargando un archivo ejecutable (.exe) de Windows. Este tipo de comportamiento ejecutable puede ser sospechoso porque pueden contener malware.
- Alta Puntuación de Riesgo:** La alerta tiene una puntuación de riesgo de 95, lo que la clasifica como de alto riesgo.

3. **Prioridad y Severidad:** Tanto la prioridad como la severidad de la alerta están marcadas como críticas, indicando que es un incidente que requiere atención inmediata.

**Investiga los dos eventos de la alerta (dando click en cada uno de ellos) y asegúrate de recopilar únicamente la información relevante para mandarla al cliente: datos de la persona involucrada, sus acciones y por qué esto puede ser peligroso para la empresa.**

## Investigación de los Eventos de la Alerta

### Evento 1: NETWORK\_HTTP

- **Timestamp:** 2024-06-24T10:07:32.000
- **Usuario:** steve-watson
- **Hostname:** steve-watson-pc
- **Detalles del Evento:** Steve Watson realizó una conexión HTTP a manygoodnews.com.
- **Riesgo Potencial:** Esta acción sugiere que Steve Watson podría haber descargado un archivo sospechoso desde un sitio web potencialmente malicioso.

### Evento 2: PROCESS\_LAUNCH

- **Timestamp:** 2024-06-24T10:03:32.426
- **Usuario:** steve-watson
- **Hostname:** steve-watson-pc
- **Proceso:** EXCEL.exe fue lanzado por el proceso con ID 22895.
- **Riesgo Potencial:** El lanzamiento de EXCEL.exe puede indicar que el archivo descargado está siendo ejecutado, lo que podría comprometer la seguridad del sistema si el archivo contiene malware.

## Información Relevante para el Cliente

- **Persona Involucrada:** Steve Watson, empleado de la empresa.
- **Acciones Realizadas:**
  - Conexión HTTP a manygoodnews.com, un sitio potencialmente malicioso.
  - Lanzamiento del proceso EXCEL.exe, posiblemente relacionado con el archivo descargado.
- **Riesgo para la Empresa:** La descarga y ejecución de un archivo ejecutable desde una fuente no confiable puede resultar en la instalación de malware, comprometiendo datos sensibles, afectando la operación del sistema y causando posibles filtraciones de información.

**Por último, puedes proponer acciones recomendadas para contener esta acción o asegurarse de que la acción no tendrá mayor incidencia.**

## Acciones Recomendadas

- **Aislamiento del equipo:** Inmediatamente aislar la máquina steve-watson-pc de la red para evitar una posible propagación del malware.
- **Análisis de Malware:** Realizar un análisis exhaustivo del archivo descargado y del sistema para identificar y eliminar cualquier malware presente.
- **Monitoreo de Red:** Revisar los logs de red para identificar cualquier comunicación adicional con manygoodnews.com u otros dominios sospechosos.
- **Actualización de Políticas de Seguridad:** Reforzar las políticas de descarga y ejecución de archivos, asegurando que se bloqueen descargas de ejecutables desde fuentes no confiables.
- **Capacitación al Personal:** Capacitar a los empleados sobre los riesgos asociados con la descarga de archivos desde internet y la importancia de seguir las políticas de seguridad de la empresa.

## Conclusión

La alerta sobre la descarga sospechosa de un archivo ejecutable y la ejecución de EXCEL.exe por parte de Steve Watson representa un riesgo significativo para la seguridad de la empresa. Es crucial tomar medidas inmediatas para contener la posible amenaza y evitar futuros incidentes similares.

## Tarea Opcional:

**Si te ves capacitado/a puedes probar a crear una regla Yara. Para esta regla debes buscar usuarios que hayan iniciado sesión en tu empresa desde dos o más ciudades en menos de 5 minutos. Puedes ayudarte de otras reglas que ya hayan sido creadas.**

**A continuación, se describe el funcionamiento de esta regla:**

- Agrupa los eventos con nombre de usuario (\$user)
- El periodo es de 5 min, lo que significa que solo se correlacionan los eventos con menos de 5 min de diferencia
- Búsqueda de un grupo de eventos (\$udm) cuyo tipo de evento es USER\_LOGIN.
- Para ese grupo de eventos, la regla llama al ID de usuario como \$user y a la ciudad de acceso como \$city.
- Muestra una coincidencia si el numero distinto de valores city (indicados por #city) es mayor que 1 en el grupo de eventos (\$udm) dentro del intervalo de tiempo de 5 minutos.

**Detection -> Rules & Detections -> Rules Editor -> New**

Para crear una regla YARA que detecte si un usuario ha iniciado sesión desde dos o más ciudades diferentes en un período de 5 minutos se ha creado esta regla.

```
rule User_Login_From_Multiple_Cities
{
    meta:
        description = "Detects if a user has logged in from two or more different cities within 5 minutes."
        author = "Sheila"
        date = "2024-07-09"
    events:
        $e.metadata.event_type = "USER_LOGIN"
        $e.principal.user = $user
        $e.source.city_name = $city
    match:
        $user over 5m
    outcome:
        $city_count = count_distinct($city)
    condition:
        $e and $city_count > 1
}
```

## Explicación de la Regla

### Sección Events:

- **\$e.metadata.event\_type == "USER\_LOGIN":** Filtra los eventos para obtener solo los de tipo USER\_LOGIN.
- **\$e.principal.user == \$user:** Define el campo que identifica al usuario y lo asigna a la variable \$user.
- **\$e.source.geo.city\_name == \$city:** Define el campo que identifica la ciudad de acceso y lo asigna a la variable \$city.

### Sección Match:

- **\$user over 5m:** Agrupa los eventos por usuario (\$user) dentro de un período de 5 minutos.

### Sección Outcome:

- **\$city\_count = count\_distinct(\$city):** Cuenta el número de ciudades distintas.

### Sección Condition:

- **\$e and \$city\_count > 1:** Muestra una coincidencia si el número de ciudades distintas es mayor que 1 dentro del grupo de eventos.