Table of Contents

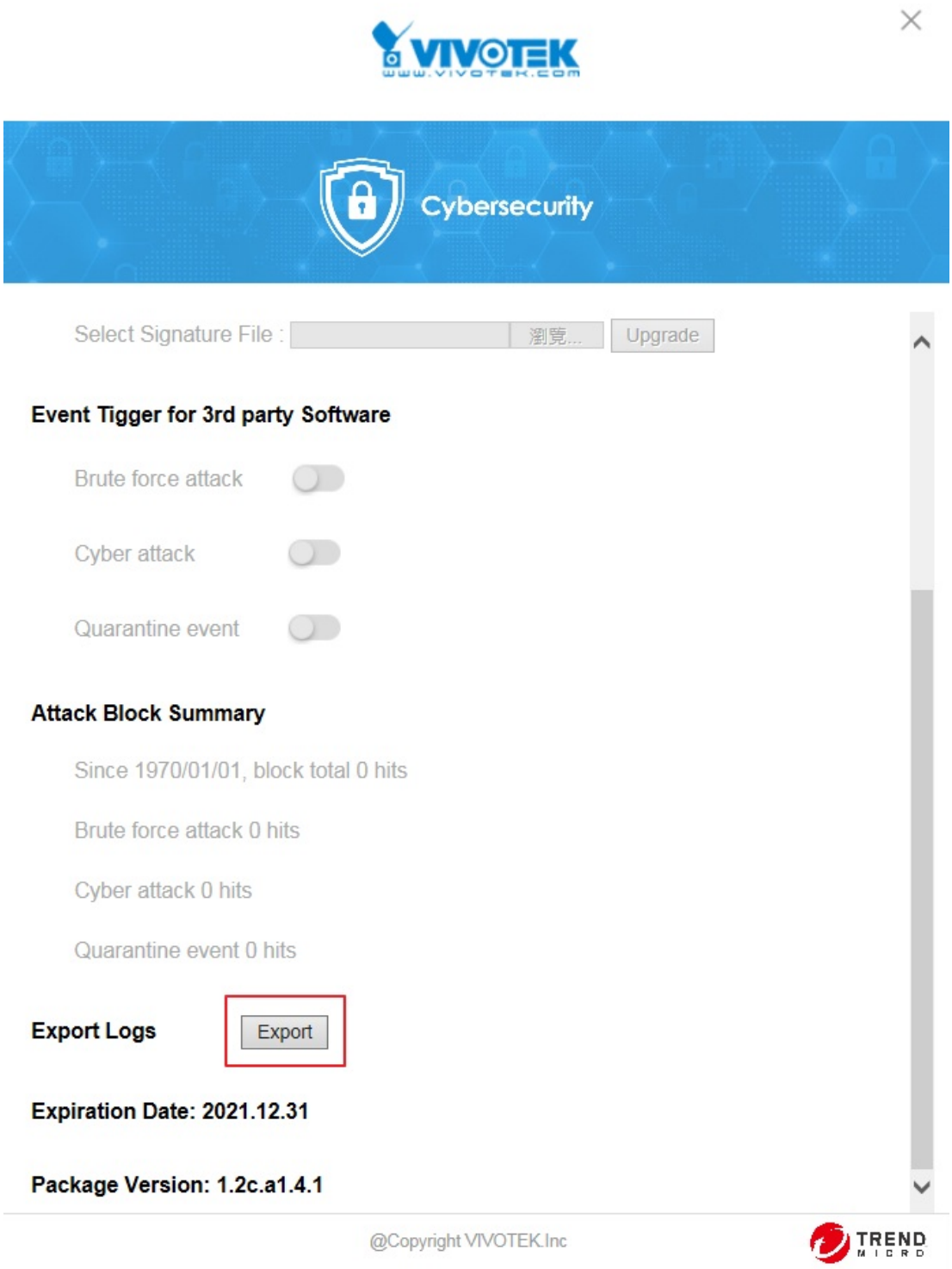
Guías de Configuraciones > VIVOTEK > Cámaras IP

¿Cómo leer el registro de eventos de Trend Micro?

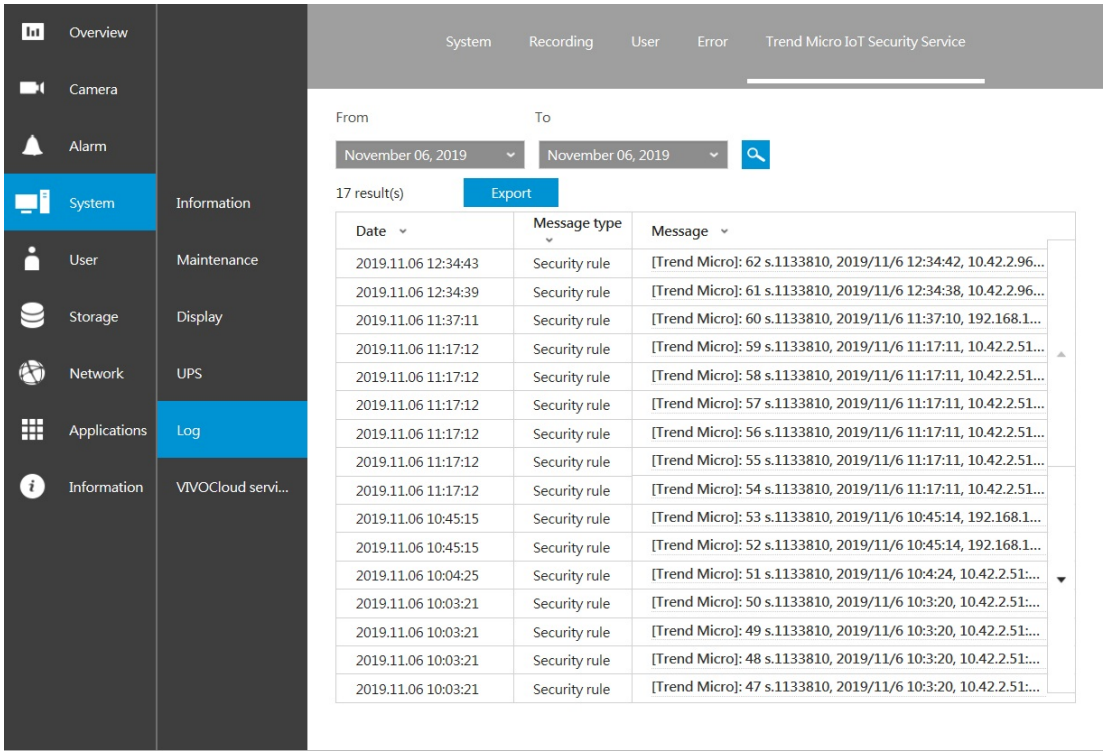
Registros de Eventos de Trend Micro en Productos VIVOTEK

En los productos VIVOTEK, es posible acceder a los registros de eventos generados por Trend Micro. A continuación, se muestran ejemplos de los registros de eventos disponibles en distintas plataformas de VIVOTEK:

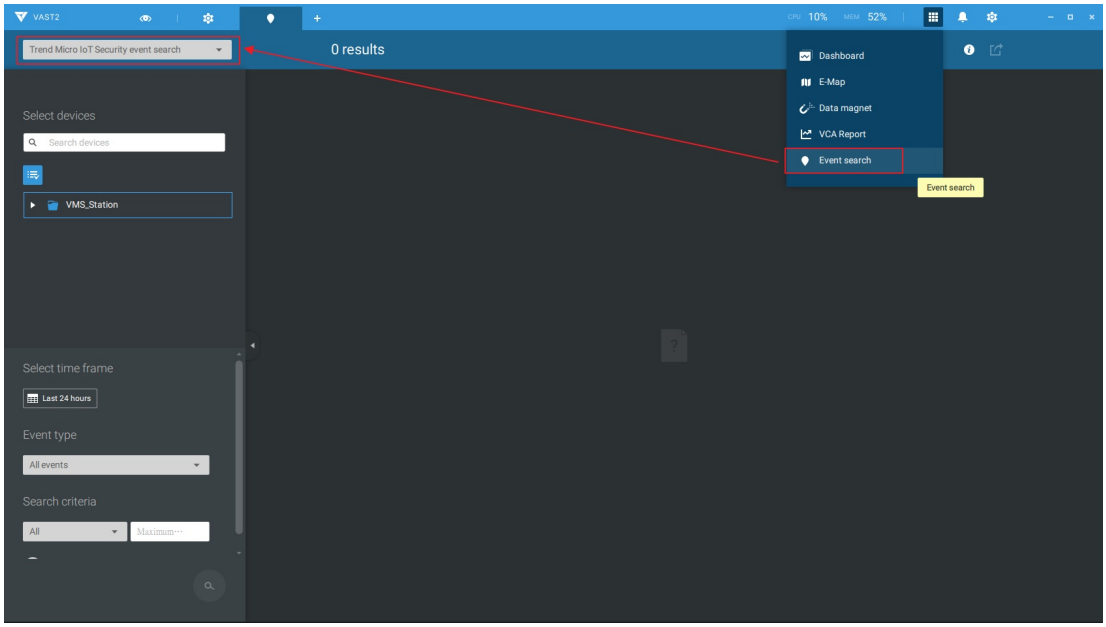
- **Registros de eventos en cámaras VIVOTEK**



- **Registros de eventos en NVRs basados en Linux**



- **Registros de eventos de Trend Micro en VAST2**



Ejemplos de registros de eventos:

En una cámara:

16 de diciembre 00:58:58 [Trend Micro]: 1 s.1133810, 2019/12/16 0:58:58, 10.42.2.33:1775 > 192.168.40.78:80, 10.42.2.33, víctima
16 de diciembre 00 :58:58 [Trend Micro]: 2 s.1133810, 2019/12/16 0:58:58, 10.42.2.33:1829 > 192.168.40.78:80, 10.42.2.33, víctima
16 de diciembre 10:15:22 [Trend Micro]: 3 s.1133810, 2019/12/16 10:15:22, 10.42.2.33:46527 > 192.168.40.78:80, 10.42.2.33, víctima
16 de diciembre 10:15:22 [Trend Micro]: 4 s.1133810, 2019/12/16 10:15:22, 10.42.2.33:46573 > 192.168.40.78:80, 10.42.2.33, Víctima
3 de octubre 19:01:11 [Trend Micro]: WRS, [78, -1, -1, -1], 13/10/2017 13:18:48, '206.130.113.68:80/ eicar.com ' de
octubre 03 19:01:11 60.251.25.44 [Trend Micro]: TRS, [28, -1, -1, -1], 2018/10/4 3:2:47, '201.39.159.204:445/'

En un NVR:

9953 2019-12-12T11:25:24.631862+08:00 Regla de seguridad [Trend Micro]: 3509 s.1133810, 2019/12/12 11:25:23, 192.192.25.221:58483 > 192.192.25.231:809, 2 .25.221, Víctima
9952 2019-12-12T11:25:24.630766+08:00 Regla de seguridad [Trend Micro]: 3508 s.1133810, 2019/12/12 11:25:23, 192.192.25.221:58483 > 192.1292.2 :110, 192.192.25.221, Víctima
9951 2019-12-12T11:25:24.629648+08:00 Regla de seguridad [Trend Micro]: 3507 s.1133810, 2019/12/12 11:25:23, 192.192.25.831:584 > 192.192.25.231:443, 192.192.25.221, Víctima
9950 2019-12-12T11:25:24.628503+08:00 Regla de seguridad [Trend Micro]: 3506 s.1133810, 2019/12/12 11:25:23, 192.192.25.221:58483 > 192.192.25.231:239, 2 .25.221, víctima

VAST2:

Event Type	Time	SeqNum	Message Type	Rule ID	PeerIPAddress	Direction	DeviceIPAddress	OriginatorIPAddress	DeviceRole	Domain Peer:PortPath	PeerIP:ServerPort
Brute force attack	2018/10/9 01:33:52	952	Security Rule	1133810	185.10.68.123:60000	Outside-in	60.251.25.44:23	75.97.250.243	Victim	-	-
Cyber attack	2018/10/9 01:33:52	954	Security Rule	1133835	185.10.68.123:60000	Outside-in	60.251.25.44:23	75.97.250.243	Victim	-	-
Cyber attack	2018/10/9 01:33:52	-	WRS	-	-	-	-	-	-	104.115.235.31:80/eicar.com	-
Cyber attack	2018/10/9 01:33:52	-	TRS	-	-	-	-	-	-	-	104.115.235.31:80
Quarantine event	2018/10/9 01:33:52	953	Security Rule	1133820	185.10.68.123:60000	Inside-out	60.251.25.44:23	60.251.25.44:23	Attacker	-	-

Tipos de eventos

Evento de ataque de fuerza bruta: Este tipo de evento ocurre cuando un atacante intenta obtener acceso a la cámara mediante métodos de prueba y error. Trend Micro bloquea estos intentos y genera un registro de evento.

Evento de cuarentena: Si la cámara ha sido comprometida, podría iniciar ataques contra otras IPs. Trend Micro bloquea estas actividades y notifica el evento. Para proteger el dispositivo, se recomienda restablecer la configuración de fábrica o actualizar el firmware.

Evento de ciberataque: Engloba otros tipos de ciberataques no clasificados como ataques de fuerza bruta o comportamientos anormales de la cámara. Al identificar estos eventos, se debe proporcionar la ID de regla a soporte técnico para asistencia.

Tipos de Mensajes de Seguridad:

- **Regla de seguridad:** Incluye información como el número de secuencia, ID de la regla de Trend Micro, hora del evento, IP de pares, dirección del paquete, IP del dispositivo y del originador.
    - **Atacante:** El dispositivo inicia este evento.
    - **Víctima:** Un intento de ataque hacia el dispositivo.
    - **Bloqueo de IP:** La conexión está bloqueada por el motor DPI de Trend Micro.

Servicios de Reputación Web:

- **WRS (Web Reputation Service):** Protege a la cámara de conexiones con servidores potencialmente maliciosos.
- **TRS (Trend Micro Web Reputation Service):** Similar a WRS, protege la cámara de intentos de conexión desde servidores sospechosos.

ID de Regla:

Para obtener más detalles sobre las IDs de regla de Trend Micro, descargue la información desde el siguiente enlace: VIVOTEK Cybersecurity.

Este formato proporciona una estructura clara sobre cómo VIVOTEK y Trend Micro colaboran para la detección y protección contra amenazas cibernéticas, facilitando al usuario la comprensión de los tipos de eventos y acciones recomendadas.