Table of Contents

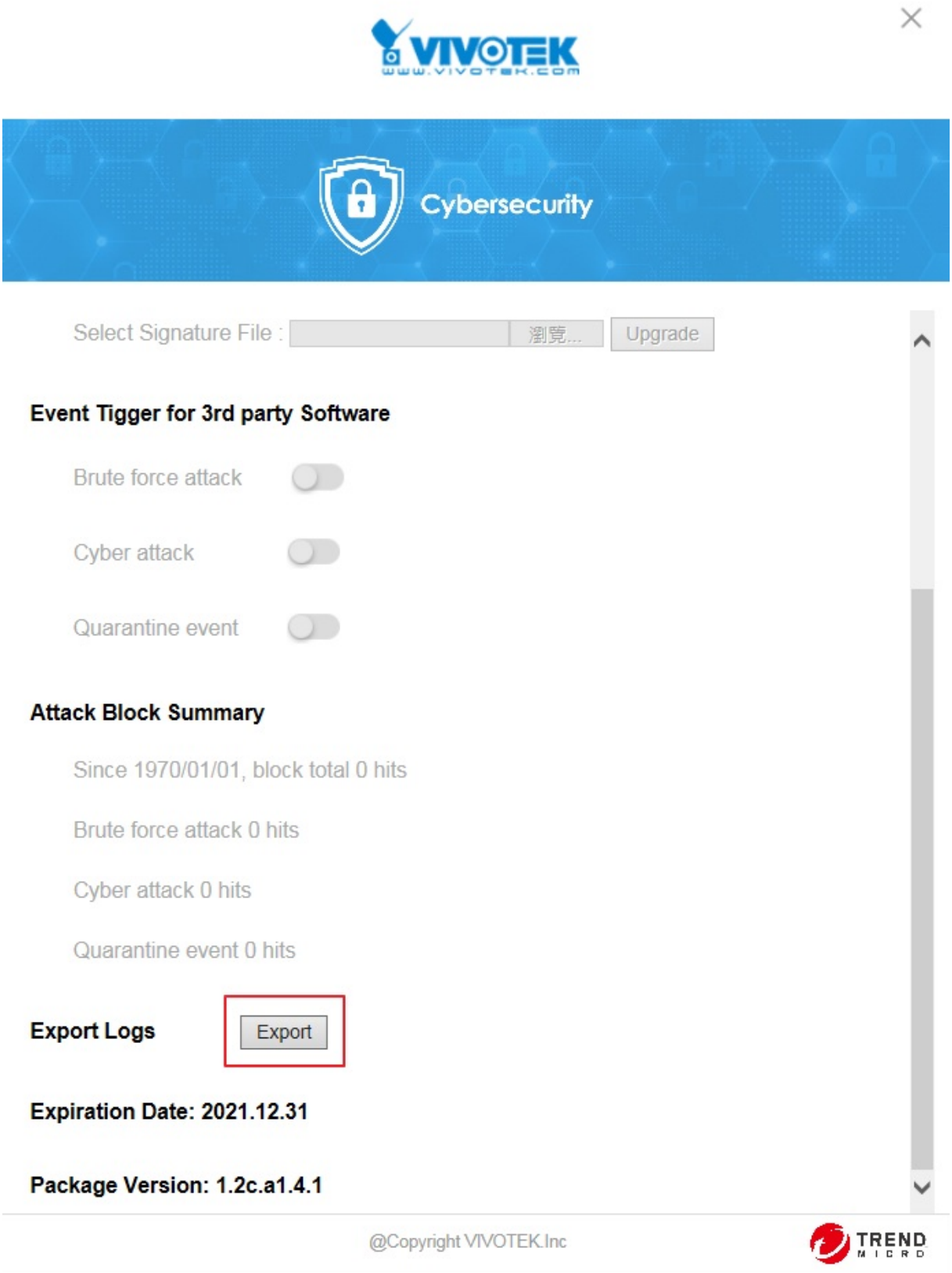
Guías de Configuraciones > VIVOTEK > Cámaras IP

¿Cómo leer el registro de eventos de ciberseguridad de Trend Micro?

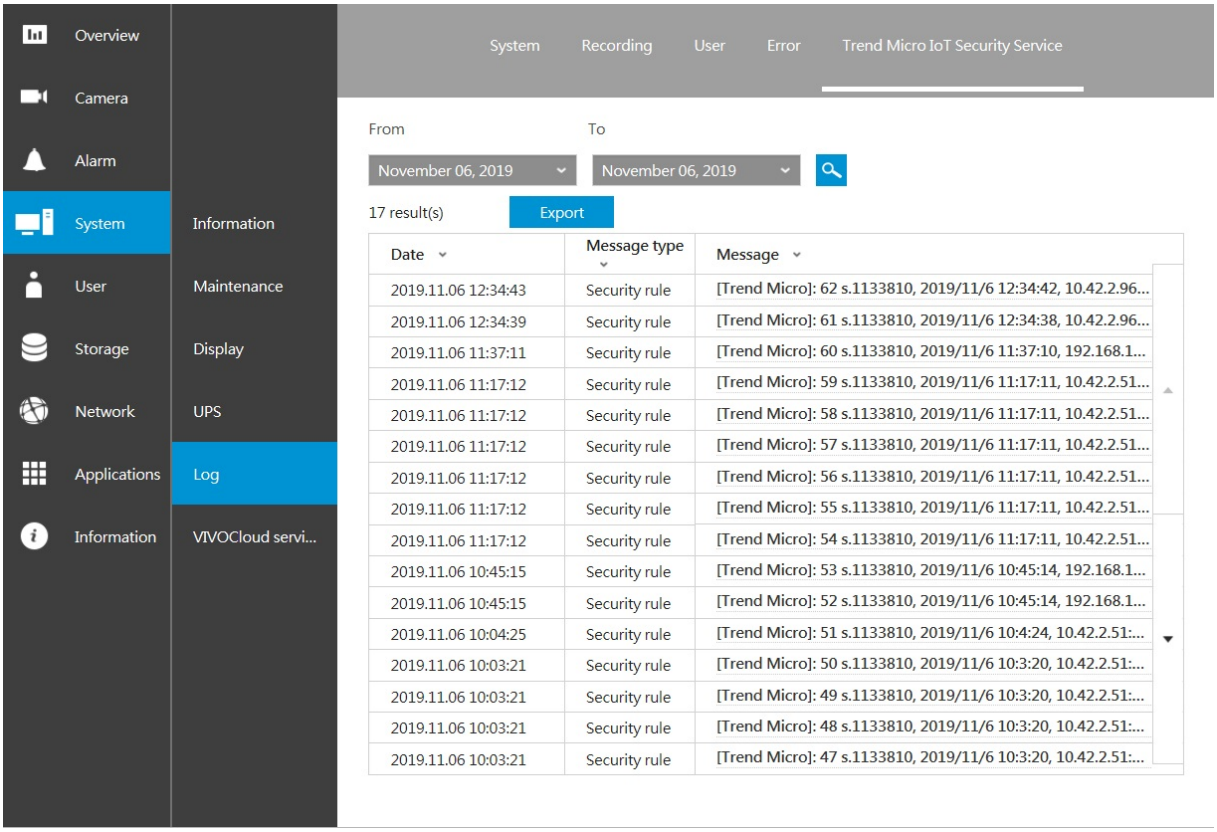
¿Cómo leer el registro de eventos de ciberseguridad de Trend Micro?

Puede encontrar el registro de eventos de Trend Micro de los productos VIVOTEK. El registro de eventos de Trend Micro de cada producto de la serie se muestra a continuación:

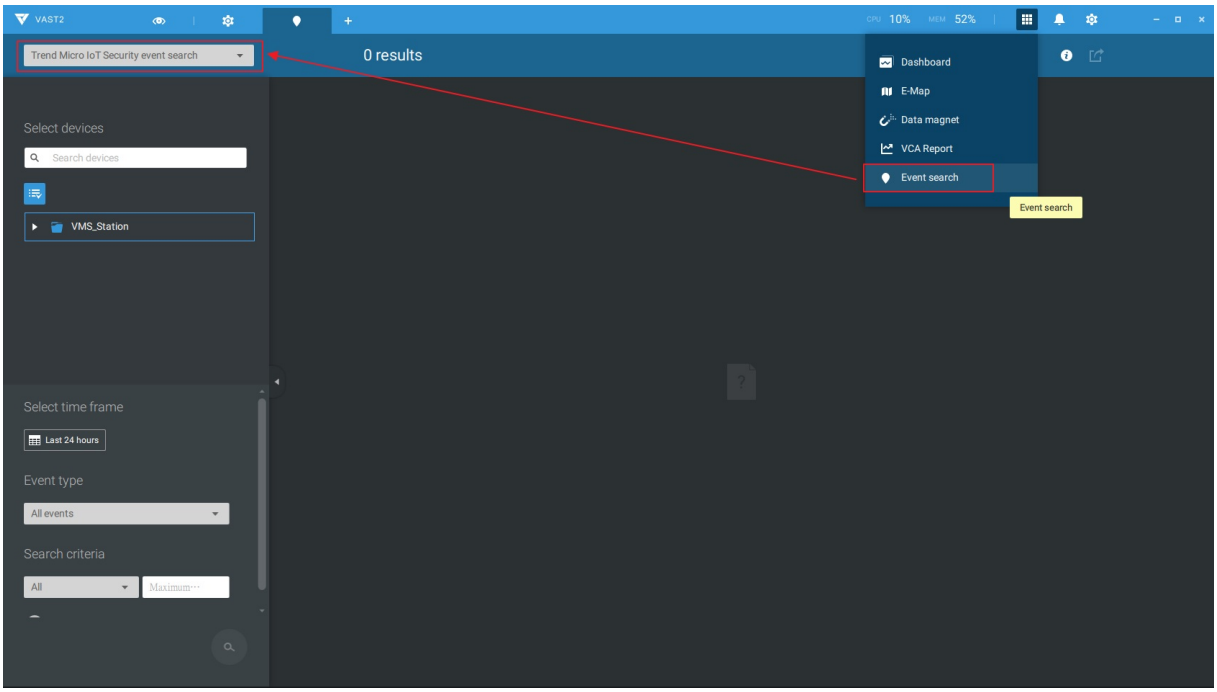
Cámara:



NVR basado en Linux:


Overview
Camera
Alarm
System
User
Storage
Network
Applications
Information
Information
Maintenance
Display
UPS
Log
VIVOCloud servi...
System
Recording
User
Error
Trend Micro IoT Security Service
From
To
November 06, 2019
November 06, 2019
17 result(s)
Export
Date
Message type
Message
2019.11.06 12:34:43 Security rule [Trend Micro]: 62 s.1133810, 2019/11/6 12:34:42, 10.42.2.96...
2019.11.06 12:34:39 Security rule [Trend Micro]: 61 s.1133810, 2019/11/6 12:34:38, 10.42.2.96...
2019.11.06 11:37:11 Security rule [Trend Micro]: 60 s.1133810, 2019/11/6 11:37:10, 192.168.1...
2019.11.06 11:17:12 Security rule [Trend Micro]: 59 s.1133810, 2019/11/6 11:17:11, 10.42.2.51...
2019.11.06 11:17:12 Security rule [Trend Micro]: 58 s.1133810, 2019/11/6 11:17:11, 10.42.2.51...
2019.11.06 11:17:12 Security rule [Trend Micro]: 57 s.1133810, 2019/11/6 11:17:11, 10.42.2.51...
2019.11.06 11:17:12 Security rule [Trend Micro]: 56 s.1133810, 2019/11/6 11:17:11, 10.42.2.51...
2019.11.06 11:17:12 Security rule [Trend Micro]: 55 s.1133810, 2019/11/6 11:17:11, 10.42.2.51...
2019.11.06 11:17:12 Security rule [Trend Micro]: 54 s.1133810, 2019/11/6 11:17:11, 10.42.2.51...
2019.11.06 10:45:15 Security rule [Trend Micro]: 53 s.1133810, 2019/11/6 10:45:14, 192.168.1...
2019.11.06 10:45:15 Security rule [Trend Micro]: 52 s.1133810, 2019/11/6 10:45:14, 192.168.1...
2019.11.06 10:04:25 Security rule [Trend Micro]: 51 s.1133810, 2019/11/6 10:4:24, 10.42.2.51:...
2019.11.06 10:03:21 Security rule [Trend Micro]: 50 s.1133810, 2019/11/6 10:3:20, 10.42.2.51:...
2019.11.06 10:03:21 Security rule [Trend Micro]: 49 s.1133810, 2019/11/6 10:3:20, 10.42.2.51:...
2019.11.06 10:03:21 Security rule [Trend Micro]: 48 s.1133810, 2019/11/6 10:3:20, 10.42.2.51:...
2019.11.06 10:03:21 Security rule [Trend Micro]: 47 s.1133810, 2019/11/6 10:3:20, 10.42.2.51:...

VAST2:


VAST2
Trend Micro IoT Security event search
0 results
CPU 10% MEM 52%
Dashboard
E-Map
Data magnet
VCA Report
Event search
Event search
Select devices
Search devices
VMS_Station
Select time frame
Last 24 hours
Event type
All events
Search criteria
All
Maximum

A continuación, se muestran registros de muestra.

Cámara:
16 de diciembre 00:58:58 [Trend Micro]: 1 s.1133810, 16/12/2019 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, 16/12/2019 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, 16/12/2019 10:15:22, 10.42.2.33:46527 > 192.168.40.78:80, 10.42.2.33, Víctima
16 dic 10:15:22 [Trend Micro]: 4 s.1133810, 16/12/2019 10:15:22, 10.42.2.33:46573 > 192.168.40.78:80, 10.42.2.33, Víctima
03 oct 19:01:11 [Trend Micro]: WRS, [78, -1, -1, -1], 13/10/2017 13:18:48, '206.130.113.68:80/ eicar.com '
03 de octubre 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/'

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 > 192.192.25.231:80, 192.192.25.221, 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 > 192.192.25.231:110, 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, 192.192.25.221:58483 > 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 > 192.192.25.231:23, 192.192.25.221, 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	-	-

Tipo de evento

Evento de ataque de fuerza bruta:
un ataque de fuerza bruta es un método de prueba y error utilizado para iniciar sesión en la cámara u obtener información como la contraseña de un usuario. Cuando la cámara está bajo un ataque de fuerza bruta, Trend Micro bloqueará este tipo de evento y enviará el evento.

Evento de cuarentena:
si la cámara ha sido pirateada, podría convertirse en un atacante y enviar paquetes maliciosos para atacar otras IP. Trend Micro bloqueará este tipo de evento y enviará la notificación del evento. En este momento, el usuario deberá restaurar la cámara a la configuración predeterminada o actualizar el firmware de la cámara para evitar que la cámara sea pirateada nuevamente. La función del dispositivo de este tipo de evento en el registro es Atacante.

Evento de ataque cibernético:
además del ataque de fuerza bruta y el evento de comportamiento anormal de la cámara, todos los demás ataques cibernéticos pertenecen a este tipo. Si encuentra este evento, proporcione la ID de la regla al soporte técnico de VIVOTEK, lo ayudaremos con los problemas.

Tipo de mensaje

Regla de seguridad:

Número de secuencia : el índice de este registro de seguridad.
ID de regla: el motor de TrendMicro ha capturado y comparado la regla de seguridad.
Hora: la hora del evento.
IP del par: la dirección IP del host que está conectado con nuestro dispositivo.
Dirección: identifica la dirección del paquete que cumple con esta política de reglas. NO debemos tomar esto como pistas de infección.
IP del dispositivo : la dirección IP de nuestro dispositivo.
IP del originador: la dirección IP que inicia esta conexión.
Rol del dispositivo:

Atacante: nuestro dispositivo inicia este evento.
Víctima: alguien intenta atacarnos.
Bloqueo de IP: el motor DPI de TrendMicro bloquea esta conexión.

WR

WRS, Trend Micro Web Reputation Service, es un servicio diseñado para proteger la cámara de la conexión a posibles IP o servidores maliciosos.
Hora: hora del evento.
Dominio Peer: PuertoParth: contenido de la consulta

TRS

Por otro lado, TRS, también conocido como Trend Micro Web Reputation Service, es un servicio diseñado para proteger la cámara de la conexión por parte de una posible IP o servidor malicioso.
Hora: hora del evento.
PeerIP:ServerPort: contenido de la consulta

Identificación de la regla

Descargue el ID de la regla de Trend Micro desde aquí para obtener más detalles. Si el enlace no está disponible, consulte la versión más reciente
en: https://www.vivotek.com/cybersecurity