CounterACT® IOC Scanner Plugin
Configuration Guide

Version 2.0.1
Table of Contents

About the CounterACT IOC Scanner Plugin ................................................................. 4
  Use Cases .................................................................................................................... 5
    Broaden the Scope and Capacity of Scanning Activities ...................................... 5
    Use CounterACT Policy Actions to Handle Infected Endpoints ..................... 6
    Perform Enterprise-Wide Forensics .................................................................... 7
  How It Works ............................................................................................................. 7
  IOC Detection .......................................................................................................... 8
  Best Practices ......................................................................................................... 9
  Dependencies ........................................................................................................... 13
    Configuration of Network-based Observables ................................................... 13
    Configuration of Endpoint-based Observables ................................................... 13
  Considerations ......................................................................................................... 13
  What to Do ............................................................................................................... 16

Requirements ............................................................................................................ 16

Upgrade Issues .......................................................................................................... 17

Install the Plugin ......................................................................................................... 18

Configure the Plugin .................................................................................................. 19
  View the IOC Scanner Table .................................................................................... 19
  Remove Threats from the Repository ..................................................................... 21
    Manually Remove Threat Data ............................................................................. 21
    Manage Automatic Removal of Threat Data ...................................................... 21
  Manually Add a Threat ........................................................................................... 22
  View Threat IOCs .................................................................................................... 22
  Manually Add an IOC to a Threat .......................................................................... 24
  Export IOC Scanner Table Information .................................................................. 24
  Manage Threat Exceptions ..................................................................................... 25

Run IOC Scanner Policy Templates ............................................................................. 26
  CounterACT IOC Hunting Policy Template ............................................................ 27
    Run the Template .................................................................................................. 27
  Percentage of Threat Match Policy Template ......................................................... 31
    Run the Template .................................................................................................. 31
  TIP Specific IOCs Detected Policy Template .......................................................... 36
    Run the Template .................................................................................................. 36

Test the IOC Scanner Policy Workflows ..................................................................... 40

Create Custom IOC Scanner Policies ........................................................................... 43
  Detecting IOCs – Policy Properties ....................................................................... 44
IOC Scan Stats ...................................................................................... 44
IOCs Detected by CounterACT ............................................................... 47
Last Reported IOC ............................................................................... 48
Last Scan Status .................................................................................... 49

Scanning Endpoints – Policy Actions ....................................................... 50
Scan and Remediate Known IOCs ............................................................ 50
Add Threat Exception ........................................................................... 53
Remove Threats from the Threat Exception Repository ........................... 53
Manually Remove Threat Exception Data ............................................... 53

Display Inventory Information ............................................................... 55

Appendix 1: The DNS Query Extension ............................................... 56
Configure and Test the Extension ............................................................ 56
Sample Test .......................................................................................... 57
Detecting Endpoints – DNS Query Properties ........................................... 59
Is a DNS Server ................................................................................... 59
DNS Event ............................................................................................. 59

Additional CounterACT Documentation ............................................... 60
Documentation Portal ........................................................................... 60
Customer Support Portal ...................................................................... 61
CounterACT Console Online Help Tools ............................................... 61
About the CounterACT IOC Scanner Plugin

The CounterACT IOC Scanner Plugin leverages threat detection and threat prevention mechanisms of third-party systems with the network visibility and enforcement capabilities of CounterACT.

This alliance ensures that you accelerate response time, automate workflows, achieve major operational efficiency and provide superior security.

CounterACT weighs in with its complete real-time visibility and agentless capabilities to fill the void of third-party threat detection and threat prevention systems which may not have full visibility and consequently may overlook important endpoint activity.

Specifically, the plugin serves as:

- A mechanism for scanning all CounterACT-managed Windows endpoints for Indicators of Compromise (IOC). See Scan and RemEDIATE Known IOCs.
- A centralized repository of all threats and their IOCs reported to CounterACT or added manually. See View the IOC Scanner Table for details.

For each threat in the repository, the IOC Scanner Plugin stores the threat file hash and an unordered list of its IOCs.

When scans indicate a threat, you can complete the security cycle by rolling out CounterACT policy actions to instantly deny or limit network access, mitigate or remediate endpoints, or notify security teams and endpoints users.

Third-party threat detection and prevention systems integrate with CounterACT through ForeScout Modules. In this document, these third-party systems are called Threat Intelligence Providers (TIP) systems.

To use the plugin, you should have a solid understanding of Advanced Persistent Threat (APT) concepts and terminology, and understand how CounterACT policies
and other basic features work. Additionally, you should understand how to leverage threat intelligence distributed by IOCs.

**Use Cases**

This section describes important use cases supported by this plugin.

- **Broaden the Scope and Capacity of Scanning Activities**
- **Use CounterACT Policy Actions to Handle Infected Endpoints**
- **Perform Enterprise-Wide Forensics**

**Broaden the Scope and Capacity of Scanning Activities**

Enhance TIP products by using CounterACT's intelligent scanning capabilities. These capabilities let you achieve sophisticated, actionable high-fidelity scan results.

**Broaden the Scope**

- When a TIP system(s) detects a new threat and reports it to CounterACT, CounterACT can automatically scan the network to see:
  - If other Windows endpoints have been infected, including those not monitored by the TIP system(s).
  - If the malware propagated.
  - If the same threat was propagated or introduced on entry points not monitored by the TIP system(s), such as email or external devices.

See [Scan for New Threats](#).

- Use CounterACT to scan for known threats on Windows endpoints as they attempt to connect to the network. This ensures that infected endpoints are stopped at the threshold of your network. See [Run an Automatic Scan](#).

**Enrich Scanning Intelligence**

- Scan for one or more specific indications. For example, scan to detect endpoints on which all of the following indications were detected:
  - A specific registry value was set.
  - A specific Mutex IOC was detected.
  - A specific DNS Query IOC was detected.
CounterACT IOC Scanner Plugin  Configuration Guide

See TIP Specific IOCs Detected Policy Template.

- Scan endpoints for threats based on specific filters, such as IOC type or severity level. See TIP Specific IOCs Detected Policy Template.

- Evaluate the scan results based on various factors, such as:
  - The severity of the threat detected on the endpoint.
  - The counts and percentages of the IOCs detected on the endpoint of a specific threat. See IOC Scan Stats for details.

Two policy templates are provided to help enrich your scanning intelligence. See CounterACT IOC Hunting Policy Template and TIP Specific IOCs Detected Policy Template for details.

- Continuously monitor all network sessions for all known DNS Query IOCs and for the hostname portion of known CnC Address IOCs, for example for a specific malicious URL.

**Use CounterACT Policy Actions to Handle Infected Endpoints**

Complete the security cycle when scans indicate a threat. Use CounterACT polices to run policy actions that immediately:

- Contain infected endpoints, for example by limiting or blocking network access. This prevents lateral movement of the infection to other endpoints.

- Mitigate infected endpoints, for example by killing suspicious processes.

- Notify stakeholders, for example by sending the security team an email with details about which threats were detected on which endpoints.

- Perform additional actions, for example, running a vulnerability scan via a vulnerability scanner or triggering a patch update via a patch management system.

See Create Custom IOC Scanner Policies for details.

> Use policy actions with caution. It is not uncommon for detected IOCs to be false-positive. See False-Positive Threat Handling.
Perform Enterprise-Wide Forensics

- Use the CounterACT inventory to view scan results from different perspectives. For example, run a CounterACT policy to identify all endpoints impacted by a specific threat, and then use the CounterACT inventory to learn if the threats are location-specific, i.e. if they emanate from a specific subnet or segment. See Display Inventory Information for details.

How It Works

TIP systems use various methods (including but not limited to; sandbox, heuristics, reverse engineering, and human analysis) to gather real-time indication information regarding malware, threats, zero-day attacks, etc.

When a threat is detected by a TIP system, the detection system sends the threat details to CounterACT. The details may include:

- source/destination IP address on which the threat was detected
- timestamp of the event
- threat name, file name, severity and hash
- all the IOC details identified throughout the lifecycle of the threat

The IOC Scanner Plugin adds the data to the IOC repository, and resolves the data as CounterACT properties associated with the endpoint on which the threat was discovered. In addition, the Last Reported IOC property is resolved on all Windows endpoints for the appropriate threat severity. These properties can be used to trigger policy actions, such as triggering a scan or reacting to scan results.

Low severity threats are deleted from the repository after a pre-configured amount of time. See Manage Automatic Removal of Threat Data to configure the severity level and number of days.
IOC Detection

The IOC repository includes all the IOCs identified by TIP system(s) throughout a threat’s lifecycle. The IOC Scanner Plugin uses this information to detect the same threat on other endpoints. For example, plugin-initiated scans of endpoints can detect IOCs used during a threat infection phase and then trigger appropriate restrictive actions.

- For each threat in the repository, the IOC Scanner Plugin stores the threat file hash and an unordered list of its IOCs that were provided by TIP system(s). The plugin does not support YARA rules, STIX, OpenIOC or any other format that identifies and classifies malware families.

- The Scan and RemEDIATE Known IOCs action scans endpoints for many types of known IOCs. The action includes the following remediation option:
  - Kill processes initiated by IOCs.

  Use this option with caution to avoid terminating legitimate processes.

- You can create CounterACT policies that trigger appropriate risk mitigation and restrictive actions.

- The following explains how CounterACT handles CnC Address and DNS Query IOCs differently than other IOCs:
  - CounterACT continuously monitors all network sessions for each known CnC Address and DNS Query IOC from the time the IOC is added to the IOC repository until it is purged from the repository.
  - For other IOC types, CounterACT scans endpoints at a specific point in time.

- For CNC Address IOCs containing a domain name, the IOC Scanner plugin tries to resolve the domain automatically. For each successful resolution, the plugin retries this resolution after one minute. If at any point the resolution fails, the plugin retries to resolve this CNC IOC after one hour. This default behavior can be changed by changing the following plugin properties:
Best Practices

This section describes best practices for scanning Windows endpoints.

- **Initial Scan**
- **Scan for New Threats**
- **Periodic Scan**
- **False-Positive Threat Handling**
- **Risk Mitigation**

**Initial Scan**

To detect IOC types other than *CnC Address* and *DNS Query*, a scan must be run. You can scan:

- All endpoints in a specific subnet whenever a new threat is received from a TIP system.
- Each new endpoint upon admission.

*No scan is required to detect CnC Address and DNS Query IOCs because the plugin continuously monitors all network sessions for these IOCs.*

There are two ways to trigger an endpoint scan:

- **Run a Manual Scan**
- **Run an Automatic Scan**

**Run a Manual Scan**

Run a manual scan on a specific endpoint.

**To run a manual scan:**

1. In the CounterACT Console, NAC tab, right-click the endpoint to be scanned.
2. Select **Remediate > Scan and Remediate Known IOCs**. See **Scan and Remediate Known IOCs**.
Run an Automatic Scan

Use a CounterACT policy to trigger a scan on some or all endpoints in the network. See [Create Custom IOC Scanner Policies](#) for details.

It is recommended to create a policy with the following rules:

- **Main Rule Condition**
  - Network Function: Windows Machine

- **Main Rule Advanced**
  - Recheck unmatch tab: Every 8 hours, Activate on any admission
  - Recheck match tab: Every 8 hours, Recheck on any admission

- **Sub-Rule Condition**
  - Admission: New Host, Occurred within the last 30 minutes
Sub-Rule Action
- Scan and Remediate Known IOCs: All Threats reported in the last 8 hours, All IOC Types

Scan for New Threats
It is recommended to create a policy that scans all endpoints, or endpoints not monitored by a TIP system, for newly reported threats that might pose a significant risk to your network. For example, scan endpoints for new Critical threats no more than one hour after a new Critical severity threats was reported. See Create Custom IOC Scanner Policies for details.

It is recommended to create a policy with the following rules:

Main Rule Condition
- Network Function: Windows Machine

Main Rule Advanced
- Recheck unmatch tab: Every 8 hours, Activate on any admission
- Recheck match tab: Every 8 hours, Recheck on any admission

Sub-Rule Condition
- Last Reported IOC: Critical Severity does not meet the criteria: Older than 1 hour

Sub-Rule Action
- Scan and Remediate Known IOCs: All Critical Severity Threats reported in the last 1 hour, All IOC Types

Depending on your corporate needs, you can create similar policies that scan threats of lower severities less frequently.

Periodic Scan
It is recommended to create a policy that periodically scans all endpoints, or endpoints not monitored by a TIP system, for reported threats that might pose a significant risk to your network. For example, scan endpoints for all Critical threats every 8 hours. See Create Custom IOC Scanner Policies for details.

False-Positive Threat Handling
Different features of the plugin enable you to focus on reported threats that are the most likely to compromise your network security.

- Narrow your selection of threat filters and IOC types in the Scan and Remediate Known IOCs action to scan for threats and indications most likely to compromise your network security.
- If a scan indicates the presence of IOCs on an endpoint, isolate the endpoint and then manually review the scan results to determine if the endpoint requires remediation.
For additional information about the likelihood of a specific threat infection:

- Use the **IOC Scan Stats** property to ascertain how many IOCs the scan detected of a threat of interest, and what percent of its IOCs were detected.
- Modify and run the **CounterACT IOC Hunting Policy Template** to run risk mitigation actions automatically when scan results indicate a likelihood of infection.

Some reported threats do not indicate a security compromise when detected on a specific endpoint. Use the **Add Threat Exception** action to ignore a threat's detection on that endpoint.

**Risk Mitigation**

When an endpoint is suspected of being infected, it is recommended to:

1. Contain the compromised endpoint in a group created for the severity level of the suspected threat.

2. Use CounterACT to automatically isolate endpoints in some or all of the severity groups. For example, isolate all endpoints in the Critical and High Severity group.

3. Manually perform appropriate actions, such as remediation, on each endpoint that was isolated. See **False-Positive Threat Handling**.

4. When it is determined that it is safe to admit the endpoint to the network, use the **Delete Properties** action so that the endpoint is no longer marked for remediation or restriction:

   In the Console, NAC tab, right-click the endpoint, select **Manage > Delete Properties**, select the property to be deleted, and select **OK**.
Dependencies

IOCs are linked to observables and observables are linked to measurable events or stateful properties which can represent anything from the creation of a registry key on a host (measurable event) to the presence of a mutex (stateful property). For the IOC Scanner to function optimally, CounterACT must be able to observe and measure events on the network and endpoint.

To ensure that CounterACT can measure these network and endpoint events, the following configuration is recommended:

- Configuration of Network-based Observables
- Configuration of Endpoint-based Observables

Configuration of Network-based Observables

File Exists, Mutex, Process, Registry Key, Service

CounterACT’s monitor interface must be attached to a Mirror, TAP or SPAN port. This allows the Appliance to monitor and track network traffic. Traffic is mirrored to a port on the switch and monitored by the Appliance. When two switches are connected as a redundant pair, the Appliance must monitor traffic from both switches. No IP address is required on the monitor interface.

For more information, see Setting Up Switch Connections in the CounterACT Installation Guide.

Configuration of Endpoint-based Observables

File Exists, Mutex, Process, Registry Key, Service

CounterACT must be able to manage each endpoint either via Remote Inspection or SecureConnector. For additional information see Accessing and Managing Endpoints in the CounterACT Macintosh/Linux Property Scanner Plugin Guide as well as Accessing and Managing Windows Endpoints in the CounterACT HPS Inspection Engine Plugin Guide.

In addition, endpoint based indicators are scanned on Microsoft supported Windows operating systems. Windows operating systems beyond the “End of Extended Support” published by Microsoft are not supported. See the following link for details:


Considerations

Consider the following limitations when you use this plugin.

Malware Removal Limitation

CounterACT is not designed to remove malware from endpoints. It does allow the user to kill suspicious processes that are detected in real-time, assisting in containing malware propagation and preventing further damage by the malware.
Real-Time Detection Limitation
The plugin supports periodic and on-demand scanning. A scan reflects what is detected on the endpoint at the time of the scan only. It is not persistent on the endpoint.

Process Detection Limitation
Depending on the type of malicious process reported by a TIP system, the plugin may create a related File Exists IOC that can be detected even when the process is not running.

- If the reported malicious process indication is an .exe file, the filename is stored in the IOC repository as two different IOCs:
  - **Process IOC:** The process is detected in real-time if it is running at the time of the scan. Upon detection, it can optionally be killed. However, if a malicious process is short-lived and runs during an interval between scans, the process will not be detected.
  - **File Exists IOC:** Even if the process has stopped running or has not run yet, this IOC is detected during a scan, and appropriate actions can be run.

- If the malicious process indication is a loaded .dll file, the filename is stored as a File Exists IOC only. This version of the IOC Scanner Plugin does not detect a .dll file loaded by a process.

- This version of the IOC Scanner Plugin detects .exe Portable Executable file types only. If a malicious process indication is a different file type, no IOCs are created for the process, and the process will not be detected.

Detection of Changes Limitation
The scan does not track changes made on the endpoint. For example, if malware changes a registry value, a subsequent scan will detect the revised registry value, but it cannot detect that the specific registry key was changed from a different value.

Malware Family Detection Limitation
The IOC Scanner Plugin recognizes each threat file hash and an unordered list of its individual IOCs that were provided by TIP systems. The plugin does not support YARA rules, STIX, OpenIOC or any other format that identifies and classifies malware families.

CnC Detection Limitation
For CnC Address (Command and Control URL) IOC types, CounterACT does not monitor the network for the complete URL value. It monitors only for the hostname portion of the URL provided in the Destination Address field.

The DNS Query Extension enhances detection of CnC Address IOCs.

Suspect DNS Detection
The DNS Query Extension detects DNS interactions that reference specific host names of interest. When the extension is installed, the IOC Scanner Plugin initiates DNS monitoring that detects the suspect host name mentioned in the IOC.

monitoring also enhances detection of CnC Address IOCs. For more information, see Appendix 1: The DNS Query Extension.

**Registry Detection**

**Registry Keys**

The IOC Scanner can scan for the existence of a registry key only, without checking its elements and data. In the example below, you must use the Registry Element `HKEY_LOCAL_MACHINE\SOFTWARE\7-Zip\` (including final backslash) and **not** `HKEY_LOCAL_MACHINE\SOFTWARE\7-Zip\(Default)`. 

**Registry Elements**

To scan for Registry Elements which consist of a Registry Key + Value, use the Registry element: `HKEY_LOCAL_MACHINE\SOFTWARE\7-Zip\Path`. (Without a final backslash)

![Registry Editor](image)

**Data Value**

To scan for an exact data value: `HKEY_LOCAL_MACHINE\SOFTWARE\7-Zip\Path Data: C:\Program Files\7-Zip\` (Without a final backslash)
Detection and CPU Performance

Consider the following CPU performance issues:

- Continuously monitoring all network session for CnC Address and DNS Query IOCs may negatively impact the Appliance's CPU performance.
- Scanning an endpoint for a large number of IOCs may negatively impact the endpoint's CPU performance.

To purge the IOC repository of threats of lower severities, you can automatically delete them a certain number of days after they were reported to CounterACT. See Manage Automatic Removal of Threat Data.

What to Do

You must perform the following to work with this plugin:

1. Verify that you have met system requirements. See Requirements.
2. If you are upgrading from an earlier version of IOC Scanner Plugin, see Upgrade Issues.
3. Install the Plugin.
4. Configure the Plugin. (Optional)
5. Run IOC Scanner Policy Templates or Create Custom IOC Scanner Policies.
6. Display Inventory Information.

Requirements

The plugin requires the following CounterACT releases and other CounterACT components.

- CounterACT version 7.0.0.
Service Pack 2.0.3 or above. It is recommended to install the latest service pack to take advantage of the most current CounterACT updates.

- HPS Inspection Engine Plugin version 10.2.3 or above.
- DNS Query Extension version 1.1.0 or above. See Appendix 1: The DNS Query Extension.

See Dependencies for configurations required to measure network and endpoint events.

Upgrade Issues

Read this section if you are upgrading from an earlier version of IOC Scanner Plugin, even if it is an earlier beta version of IOC Scanner Plugin 2.0.0.

The IOC repository design has been expanded and improved. Your existing IOC repository is not compatible with the upgraded design.

Before upgrading this plugin, it is recommended to do the following:

1. For each Advanced Threat Detection Integration Module plugin installed on your system, ensure that you have access to the plugin .fpi file for version 2.0.0 Beta 2 or above. Refer to the Install the Plugin section in the configuration guide of each installed TIP plugin.

2. Remove all existing policies that use Advanced Threat Detection properties. You can recreate the policies after the plugin installation.

3. Uninstall all Advanced Threat Detection Integration Module plugins lower than version 2.0.0 Beta 2, including the IOC Scanner Plugin (this plugin).

   Advanced Threat Detection Integration Module plugins version 2.0.0 Beta 1 and lower are not compatible with IOC Scanner Plugin 2.0.0 Beta 2 and above.

4. Install the Plugin.

5. For each Advanced Threat Detection Integration Module plugin that you uninstalled in step 3, install version 2.0.0 Beta 2 or above.
Install the Plugin

This section describes how to install the plugin.

To install the plugin:

1. Acquire a copy of the plugin in either one of the following ways:
   - If you are installing a Beta release of this plugin, acquire the plugin .fpi file from your ForeScout representative or contact beta@forescout.com.
   - Otherwise, navigate to the Customer Support Licensed Plugins page and download the plugin .fpi file.

2. Save the file to the machine on which the CounterACT Console is installed.

3. Log in to the CounterACT Console and select Options from the Tools menu.


5. Select Install. The Open dialog box opens.

6. Browse to and select the saved plugin .fpi file.

7. Select Install.

8. Accept the license agreement and select Next.

9. Select OK and Close until the installation is complete. The plugin is listed in the Plugins pane.

10. If the plugin is not automatically started, select the plugin, select Start and start the plugin on all Appliances in the environment.
Configure the Plugin

No plugin configuration is required. Once installed, the plugin will automatically collect and display threats and IOCs detected by installed plugins that report TIP information to the IOC repository.

Verify that the plugin is running on all CounterACT devices in your environment.

You can use the plugin Configure option to:

- View all threats and their IOCs discovered by TIP systems. See View the IOC Scanner Table for details.
- Remove Threats from the Repository.
- Manually Add a Threat to the IOC repository.
- View Threat IOCs.
- Manually Add an IOC to a Threat in the IOC repository.
- Export IOC Scanner Table Information from the repository.
- Manage Threat Exceptions.

View the IOC Scanner Table

The IOC Scanner table displays all the threats and IOCs in the IOC repository.

To view the IOC Scanner table:
1. In the CounterACT Console, select Options from the Tools menu. The Options dialog box opens.
2. Navigate to and select the Plugins folder.
3. In the Plugins pane, select IOC Scanner, and select Configure. The IOC Scanner pane opens.
4. Select the IOC Repository tab.
### IOC Scanner Table Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Reported</td>
<td>The date and time when a threat with this file hash was first reported or manually added to the IOC Scanner Plugin.</td>
</tr>
<tr>
<td>Threat Severity</td>
<td>Low, Medium, High or Critical threat severity level.</td>
</tr>
<tr>
<td>Reported By</td>
<td>The TIP system that reported the threat.</td>
</tr>
<tr>
<td>User-defined</td>
<td>Indicates that the threat was manually added to the IOC repository and was not reported by a TIP system.</td>
</tr>
<tr>
<td>Threat Name</td>
<td>A name used for threat identification purposes only.</td>
</tr>
<tr>
<td>File Name</td>
<td>The file name of the threat.</td>
</tr>
<tr>
<td>File Size (bytes)</td>
<td>The size of the threat file, in bytes. If the file size is not provided, it is indicated as '-' or '0'.</td>
</tr>
<tr>
<td>File Hash</td>
<td>The hash value of the threat file, in hexadecimal format, using lower case characters. This value is used to identify threats in the Scan and Remediate Known IOCs and Add Threat Exception actions. For user-defined threats, this must be a unique identifier. It need not be an actual hash value.</td>
</tr>
<tr>
<td>Hash Type</td>
<td>MD5, SHA-1 or SHA-256 hash algorithm for determining the file hash. If the file hash is not provided, it is indicated as 'None'.</td>
</tr>
<tr>
<td>Operating System</td>
<td>The OS (Operating System) for which the TIP system reported the threat. All indicates that the threat was reported for all operating systems.</td>
</tr>
<tr>
<td>IOCs</td>
<td>Details of the different types of IOCs detected during the lifecycle of the threat.</td>
</tr>
</tbody>
</table>
Remove Threats from the Repository

Threats and their IOCs remain in the IOC repository until:

- They are manually removed.
- They are automatically deleted after 30 days.
- A maximum number of 128 threats is reached.

To prevent a negative impact on your Appliance's CPU performance, it is recommended to routinely purge your IOC repository of threats that no longer pose a risk to your network. There are two ways to remove threats from the repository:

- Manually Remove Threat Data
- Manage Automatic Removal of Threat Data

Manually Remove Threat Data

You can manually remove individual threats from the IOC repository so that all endpoints will no longer be scanned for these threats.

To exempt only specific endpoints from being scanned for a specific threat, see Add Threat Exception.

To manually remove a threat from the IOC repository:

1. In the IOC Scanner, IOC Repository tab, select one or more threats to be removed.
2. Select Remove, and select Apply to apply the changes.

Manage Automatic Removal of Threat Data

A threat whose severity level is not higher than a specific level is maintained in the IOC repository a limited number of days only. Threats higher than this severity level are not automatically deleted. An IOC Scanner Plugin global parameter controls how long threats not higher than a specific severity level remain in the IOC repository.

To set the automatic threat deletion parameter:

1. At the bottom of the IOC Scanner, IOC Repository tab, set the IOC Scanner Plugin global parameters:
   - Select the maximum severity level of threats to be automatically deleted.
   - Set how many days after being added to the repository these threats will be automatically deleted.
2. Select Apply to apply the changes.
Manually Add a Threat
You can manually add threats to the IOC repository.

To manually add a threat to the IOC repository:

1. In the IOC Scanner, IOC Repository tab, select Add.

2. Complete the following fields:
   - **Threat Name**: any value
   - **File Name**: any value
   - **File Hash**: any unique value not already in the IOC repository

3. You can complete other fields if needed. The fields are described in IOC Scanner Table Parameters.

4. Select OK, and then select Apply.

View Threat IOCs
You can view the details of all IOCs detected during the lifecycle of each threat.

**IOC Types**
The following IOC types are stored in the IOC repository.

<table>
<thead>
<tr>
<th>IOC Type</th>
<th>IOC Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>CnC Address (Command and Control URL)</td>
<td>• Destination Address</td>
</tr>
<tr>
<td></td>
<td>See <a href="#">CnC Detection Limitation</a> for more information about CnC Address IOCs.</td>
</tr>
<tr>
<td>DNS (Domain Name System) Query</td>
<td>• DNS Name</td>
</tr>
</tbody>
</table>
### Process
- Process Name
- Process Hash (optional)
- Process Hash Type

See [Process Detection Limitation](#) for more information about Process IOCs.

### File Exists
- File Name
- File Path (optional)
  - If a File Path is not provided, scans detect the file if it is in the local path `%PATH%`.

### Mutex
- Mutex Name

### Registry Key
- Path
- Value (optional)
  - If a Value is not provided, scans detect if the registry path exists.
  - If a Value is provided, scans detect if the value in the registry path matches the value provided.

See [Registry Detection](#) for Registry scan example.

### Service
- Service
  - Any Windows startup or scheduled system service on the computer.

---

**To view the IOCs of a threat:**

1. In the IOC Scanner, IOC Repository tab, select the required threat, and select IOCs. The IOCs in Selected Threat dialog box opens.
IOCs in Selected Threat Parameters

- Threat name of the selected threat
- File name of the selected threat
- Type of each reported IOC
- Details of each reported IOC

Manually Add an IOC to a Threat

You can manually add IOCs to an existing threat in the IOC repository.

💡 When adding user-defined IOCs, first define a threat. See Manually Add a Threat.

To manually add an IOC to a threat:

1. In the IOC Scanner, IOC Repository tab, select the required threat, and select IOCs. The IOCs in Selected Threat dialog box opens.
2. Select Add IOC. The Add IOC dialog box opens.

3. From the dropdown menu, select the required IOC type. See IOC Types.
4. Complete the fields and select OK.
5. To add another IOC to the threat, repeat from step 1.
6. When all the IOCs have been added to the threat, select OK.

Export IOC Scanner Table Information

You can export threat and IOC information to a CSV or PDF file from:

- the IOC Scanner table
- the IOCs in Selected Threat table

To export threat or IOC information:

1. Right-click a cell of the IOC Scanner table or the IOCs in Selected Threat table, and select Export Table.
The Export Table dialog box opens.

2. Enter the file name to which to export the table and select the output file type. For a PDF file, enter a title.

3. Control which information is exported by selecting *Selected rows only* or *Displayed columns only*.

4. Select **OK**. The table creation confirmation dialog box opens with the file location and a prompt to open the table.

5. To open the table, select **Yes**. The table is opened in a Microsoft Office Excel spreadsheet or PDF document.

**Manage Threat Exceptions**

You can trigger the *Add Threat Exception* action on a given endpoint or on all endpoints so that scans ignore results of specific threats. See *Add Threat Exception*.

When you no longer want to ignore a threat in the scanning results, you can remove the threat exception from the action.

**To manage the scan result threat exceptions:**

1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.

2. Navigate to and select the **Plugins** folder.

3. In the **Plugins** pane, select **IOC Scanner**, and select **Configure**. The IOC Scanner pane opens.
4. Select the **Threat Exceptions** tab. A list is displayed of all the threats to be ignored on specific endpoints. Each threat is identified by its **Threat Identifier** value which consists of:

- the threat file hash
- an internal code for the reporting TIP system
- an internal reference to the OS for which the threat was reported

5. To remove one or more threats from the list, select the threat and select **Remove**.
6. Select **Apply** to apply the changes.

### Run IOC Scanner Policy Templates

This plugin provides policy templates that you can use to manage endpoints on which threats and IOCs were detected. To detect IOC types other than **CnC Address** and **DNS Query**, a scan must be run. See CounterACT IOC Hunting Policy Template.

This plugin provides the following policy templates:

- **CounterACT IOC Hunting Policy Template** - this policy triggers an IOC scan on all Windows endpoints based on the severity of a threat if an IOC alert is received by a compatible TIP system.
- **Percentage of Threat Match Policy Template** – this policy generate statistics of potentially compromised endpoints in a CounterACT policy. These statistics show the percentage of IOCs matched to a single threat for detected endpoints thus providing the likelihood of infection.
- **TIP Specific IOCs Detected Policy Template** - this policy identifies endpoints on which specific IOC details were detected.
It is recommended that you have a basic understanding of CounterACT policies before working with the templates. See the CounterACT Templates and Policy Management chapters of the Console User Guide.

**CounterACT IOC Hunting Policy Template**

Use this policy to trigger an IOC scan on all Windows endpoints based on the severity of a threat if an IOC alert is received by a compatible TIP system.

This template is dependent on the successful configuration of ADT and EDR Threat Detections templates not included with this plugin.

* Scanning an endpoint for a large number of IOCs may negatively impact CPU performance.

**Run the Template**

This section describes how to create a policy from the policy template.

**To run the template:**

1. Log in to the CounterACT Console and select the **Policy** tab.
2. Select **Add** from the Policy Manager. The Policy Wizard opens.
3. Expand the **Advanced Threat Detection** folder and select **CounterACT IOC Hunting**. The CounterACT IOC Hunting pane opens.
4. Select **Next**. The **Name** pane opens.

**Name the Policy**

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

1. Define a unique name for the policy you are creating based on this template, and enter a description.

**Naming Tips**

- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as `My_Compliance_Policy`.
- Use a descriptive name that indicates what your policy is verifying and which actions will be run.
- Ensure that the name indicates whether the policy criteria must be met or not met.
- Avoid having another policy with a similar name.

2. Select **Next**. The Scope pane and IP Address Range dialog box opens.

**Define Which Hosts Will Be Inspected - Policy Scope**

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.

3. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

- **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close the IP Address Range dialog box, and select **Segments** from the Scope pane.
- **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address. Not applicable for this policy template.

   - Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.

4. Select **OK**. The added range appears in the Scope pane.

5. Select **Next**. The Main Rule pane opens.
Main Rule

The main rule of this policy detects endpoints on which any IOC was detected on a Windows machine.


Sub-Rules

Hosts that match the Main Rule are included in the policy inspection. *Hosts that do not match this rule are not inspected for this policy.*

Sub-rules allow you to automatically follow up with hosts after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the policy starts to scan all endpoints with no recently identified IOCs. If the endpoint does not match the requirements of the sub-rule, the next rule is examined.

The sub-rules of this policy identify all endpoints with IOCs detected within the last hour. If a new threat is detected, all endpoints are scanned for IOCs contained in the threat:

- IOC Alert – Within the Last Hour
- IOC Detected by CounterACT – Severity Critical
- IOC Detected by CounterACT – Severity High
- IOC Detected by CounterACT – Severity Medium
- IOC Detected by CounterACT - Severity Low
- No Recent IOC Alerts

7. Select Finish to create the policy.

8. On the CounterACT Console, select Apply to save the policy.

Percentage of Threat Match Policy Template

Use this policy to generate statistics of potentially compromised endpoints in a CounterACT policy. These statistics show the percentage of IOCs matched to a single threat for detected endpoints thus providing the likelihood of infection. The higher the percentage, the greater the threat.

- Scanning an endpoint for a large number of IOCs may negatively impact CPU performance.

Run the Template

This section describes how to create a policy from the policy template.

To run the template:

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the Advanced Threat Detection folder and select CounterACT IOC Hunting. The CounterACT IOC Hunting pane opens.
4. Select **Next**. The **Name** pane opens.

**Name the Policy**

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

5. Define a unique name for the policy you are creating based on this template, and enter a description.
Naming Tips

- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
- Use a descriptive name that indicates what your policy is verifying and which actions will be run.
- Ensure that the name indicates whether the policy criteria must be met or not met.
- Avoid having another policy with a similar name.


Define Which Hosts Will Be Inspected - Policy Scope

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.

7. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

- **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK to close the IP Address Range dialog box, and select Segments from the Scope pane.
CounterACT IOC Scanner Plugin Configuration Guide

- **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address. Not applicable for this policy template.

Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.

8. Select **OK**. The added range appears in the Scope pane.
9. Select **Next**. The Main Rule pane opens.

**Main Rule**
The main rule of this policy detects endpoints on which any IOC was detected on a Windows machine.

10. Select **Next**. The Sub-Rules pane opens.

**Sub-Rules**
Hosts that match the Main Rule are included in the policy inspection. Hosts that do not match this rule are not inspected for this policy.
Sub-rules allow you to automatically follow up with hosts after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the policy sends a notification to the administrator. In addition, an action can be used to log the event to syslog, add endpoints with multiple IOCs detected to a group, and quarantine an endpoint. This action is disabled by default. If the endpoint does not match the requirements of the sub-rule, the next rule is examined.

The sub-rules of this policy sort endpoints by the percent of IOCs matched in a threat:

- 100% Match
- 75% Match
- 50% Match
- 25% Match
- <25% Match
- 1 Match

11. Select Finish to create the policy.

12. On the CounterACT Console, select Apply to save the policy.
TIP Specific IOCs Detected Policy Template

Modify this policy template to identify endpoints within the policy scope on which specific IOC details were detected.

You can add actions to sub-rules. For example, notify the user by email if a specific threat name is detected, or assign the endpoint to a VLAN if a Process IOC is detected.

Run the Template

This section describes how to create a policy from the policy template.

To run the template:

1. Log in to the CounterACT Console and select the Policy tab.
2. Select Add from the Policy Manager. The Policy Wizard opens.
3. Expand the Advanced Threat Detection folder and select TIP Specific IOCs Detected. The TIP Specific IOCs Detected pane opens.
4. Select Next. The Name pane opens.

Name the Policy

The Name pane lets you define a unique policy name and useful policy description. Policy names appear in the Policy Manager, the Views pane, NAC Reports and in other features. Precise names make working with policies and reports more efficient.

1. Define a unique name for the policy you are creating based on this template, and enter a description.
Naming Tips

- Make sure names are accurate and clearly reflect what the policy does. For example, do not use a generic name such as My_Compliance_Policy.
- Use a descriptive name that indicates what your policy is verifying and which actions will be run.
- Ensure that the name indicates whether the policy criteria must be met or not met.
- Avoid having another policy with a similar name.

2. Select Next. The Scope pane and IP Address Range dialog box opens.

Define Which Hosts Will Be Inspected - Policy Scope

The Scope pane and IP Address Range dialog box let you define a range of endpoints to be inspected for this policy.
3. Use the IP Address Range dialog box to define which endpoints are inspected. The following options are available for defining a scope:

- **All IPs**: Include all addresses in the Internal Network. The Internal Network was defined when CounterACT was set up.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select **OK** to close the IP Address Range dialog box, and select **Segments** from the Scope pane.
- **IP Range**: Define a range of IP addresses. These addresses must be within the Internal Network.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address. Not applicable for this policy template.

Filter the range by including only certain CounterACT groups and/or by excluding certain endpoints or users or groups when using this policy.

4. Select **OK**. The added range appears in the Scope pane.
5. Select **Next**. The Main Rule pane opens.

**Main Rule**

The main rule of this policy detects endpoints on which any threat was detected.
6. Select **Next**. The Sub-Rules pane opens.

**Sub-Rules**

Hosts that match the Main Rule are included in the policy inspection. *Hosts that do not match this rule are not inspected for this policy.*

Sub-rules allow you to automatically follow up with hosts after initial detection and handling. Creating sub-rules lets you streamline separate detection and actions into one automated sequence.

Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the endpoint. If the endpoint does not match the requirements of the sub-rule, the next rule is examined.

The sub-rules in this policy template contain sample data. Edit or remove each sub-rule to comply with your corporate requirements.

7. For each sub-rule required:
a. Select the sub-rule and select **Edit**.
b. In the Condition area, select each criterion and select **Edit**.
c. Change the string containing the brackets `<>` and optionally change other settings to comply with your corporate requirements.

8. Remove sub-rules not required.
9. Select **Finish** to create the policy.
10. On the CounterACT Console, select **Apply** to save the policy.

**Test the IOC Scanner Policy Workflows**

To create a host with IOCs to detect:

1. Create a dummy observable on a 'managed' Windows host in the path `c:\IOCs\` and name it `bad.txt`.

2. Create a fake registry entry in the path `HKEY_CURRENT_USER\IOCs` and name the key string: `bad-reg`.

3. Create a fake Threat in the IOC Scanner:
   a. Go to **Options** and select **IOC Scanner**.
   b. Select **Add**.
4. Create a Fake Threat with the following details:
   - Name: **Test.Backdoor**
   - File Name: **bad.txt**
   - File Size: **1**
   - File Hash: **abc** *(optionally add real MD5 or SHA hash)*
   - Hash Type: **-None-**
   - Threat Severity: **Critical**

5. Create fake IOCs:
   a. Highlight the **Test.Backdoor** Threat.
   b. Select **IOCs**.
   c. Select **Add**.
6. Create the following IOCs:
   - File: **bad.txt**
   - Registry Key: **bad-reg**
   - CnC Address: **google.com**
   - DNS Query: **google.com**

7. Select **OK**.

8. On the endpoint where the IOCs were created, open an internet browser and navigate to google.com.

9. From the CounterACT console, locate the test host, right-click **Remediate** then select **Scan and Remediate Known IOCs**. This will launch the Stage 2 of the workflow and proceed through Stage 3.
Create Custom IOC Scanner Policies

Custom CounterACT policy tools provide you with an extensive range of options for detecting and handling endpoints. Specifically, you can use the policy to instruct CounterACT to apply a policy action to endpoints that do or do not match property values defined in policy conditions.

Properties

CounterACT policy properties let you instruct CounterACT to detect hosts with specific attributes. For example, create a policy that instructs CounterACT to detect hosts running a certain Operating System or having a certain application installed.

Actions

CounterACT policy actions let you instruct CounterACT how to control detected devices. For example, assign a detected device to an isolated VLAN or send the device user or IT team an email.

You may need to create a custom policy to deal with issues not covered in the IOC Scanner policy templates.

In addition to the bundled CounterACT properties and actions available for detecting and handling endpoints, you can work with IOC Scanner related properties and actions to create the custom policies. These items are available when you install the plugin.
For more information about working with policies, select Help from the policy wizard.

**To create a custom policy:**

1. Log in to the CounterACT Console.
2. On the Console toolbar, select the **Policy** tab. The Policy Manager opens.
3. Select **Add** to create a policy.

## Detecting IOCs – Policy Properties

Policy properties are available when you install the CounterACT IOC Scanner Plugin.

![Property Tree](image)

**To access properties:**

1. Navigate to the Properties tree from the Policy Condition dialog box.
2. Expand the **Advanced Threat Detection** folder in the Properties tree. The following properties are available:
   - **IOC Scan Stats**
   - **IOCs Detected by CounterACT**
   - **Last Reported IOC**
   - **Last Scan Status**

### IOC Scan Stats

IOC Scan Stats is a composite property that detects the count and percentage statistics of IOCs found during endpoint scans for a selected threat. You can use these statistics to determine the likelihood of the endpoint being compromised by a threat of interest.

When an endpoint is scanned for a threat, the IOC Scanner Plugin calculates:

- how many IOCs of each IOC type were detected on the endpoint
- the relationship of the number of detected IOCs to the number of IOCs that were reported for the threat

See [Sample Statistics Scenario](#) for details.

Only the following IOC types are included in the statistics:

- CnC Address
- DNS Query
- IOCs selected in the **Scan and Remediate Known IOCs** action

In addition to working with the property in policies, you can use the Inventory view to see the scan result statistics for each threat. See [Display Inventory Information](#) for more information.

**IOC Scan Stats Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Severity</td>
<td>The severity (Low, Medium, High or Critical) of the threat whose IOCs are required.</td>
</tr>
<tr>
<td>IOC Type</td>
<td>Each IOC type to be considered for these statistics. Total of All Types includes all IOCs of all types.</td>
</tr>
<tr>
<td># IOCs Detected of Threat</td>
<td>The number of IOCs of the selected IOC type detected on this endpoint for the selected threat.</td>
</tr>
<tr>
<td># IOCs Reported in Threat</td>
<td>The number of IOCs of the selected IOC type defined in the IOC repository for the selected threat.</td>
</tr>
<tr>
<td>% IOCs Detected of Same Type in Threat</td>
<td>Percent of detected IOCs of the selected type out of all IOCs of the same type defined for the selected threat.</td>
</tr>
<tr>
<td>% IOCs Detected of All Types in Threat</td>
<td>Percent of detected IOCs of the selected type out of all IOCs of all types defined for the selected threat.</td>
</tr>
</tbody>
</table>
### Threat Name
Name of the threat whose IOC counts and statistics are required.

### Threat Reported By
The TIP system that reported the threat containing the detected IOC.

## Sample Statistics Scenario
In this example, endpoint 1.2.3.4 is scanned for all IOC types in the threat named XYZ.

<table>
<thead>
<tr>
<th>IOC Type</th>
<th># IOCs Reported in Threat</th>
<th># IOCs Detected of Threat</th>
<th>% IOCs Detected of Same Type in Threat</th>
<th>% IOCs Detected of All Types in Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>CnC Address</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DNS Query</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>File Exists</td>
<td>4</td>
<td>3</td>
<td>75 (%)</td>
<td>15 (%)</td>
</tr>
<tr>
<td>Mutex</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Process</td>
<td>4</td>
<td>1</td>
<td>25 (%)</td>
<td>5 (%)</td>
</tr>
<tr>
<td>Registry Key</td>
<td>4</td>
<td>4</td>
<td>100 (%)</td>
<td>20 (%)</td>
</tr>
<tr>
<td>Service</td>
<td>4</td>
<td>2</td>
<td>50 (%)</td>
<td>10 (%)</td>
</tr>
<tr>
<td><strong>Total IOCs</strong></td>
<td><strong>20</strong></td>
<td><strong>10</strong></td>
<td><strong>50 (%)</strong></td>
<td><strong>50 (%)</strong></td>
</tr>
</tbody>
</table>

Four scan result statistics values are calculated for each IOC type.

- **# IOCs Reported in Threat**: The TIP system reported that Threat XYZ has 4 IOCs of each of the following types: Process, Service, File Exists, Registry Key and CnC Address. The total number of IOCs reported is 20.
- **# IOCs Detected of Threat**: Of the IOCs defined in Threat XYZ, the scan detected 1 Process IOC, 2 Service IOCs, 3 File Exists IOCs, and 4 Registry Key IOCs. The total number of IOCs detected is 10.
- **% IOCs Detected of Same Type in Threat**: For each IOC type, the percent is calculated of # IOCs Detected of Threat / # IOCs Reported in Threat.
- **% IOCs Detected of All Types in Threat**: For each IOC type, the percent is calculated of # IOCs Detected of Threat / # Total IOCs Reported in Threat.

## Sample Property Values
If IOC type Service and Threat Name XYZ are selected in the IOC Scan Stats property, the values to match for the Service IOC types are shown on the second row of the Sample Statistics Scenario table.

- **# IOCs Reported in Threat**: 4
- **# IOCs Detected of Threat**: 2
- **% IOCs Detected of Same Type in Threat**: 50
- **% IOCs Detected of All Types in Threat**: 10
IOCs Detected by CounterACT

This composite property lists all network-based IOCs and all IOCs discovered by the Scan and Remediate Known IOCs action for a particular endpoint.

### IOCs Detected by CounterACT Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOC Type</td>
<td>Type of IOC detected.</td>
</tr>
<tr>
<td>Raw IOC Data</td>
<td>IOC details reported by the TIP system.</td>
</tr>
<tr>
<td>Threat Severity</td>
<td>Low, Medium, High or Critical severity level.</td>
</tr>
<tr>
<td>Threat Name</td>
<td>The name of the threat containing the detected IOC.</td>
</tr>
<tr>
<td>Threat File Name</td>
<td>The file name of the detected threat.</td>
</tr>
<tr>
<td>Threat File Hash</td>
<td>The file hash of the detected threat.</td>
</tr>
<tr>
<td>Threat Hash Type</td>
<td>MD5, SHA-1 or SHA-256 hash algorithm of the threat file hash.</td>
</tr>
<tr>
<td>Threat Reported By</td>
<td>The TIP system that reported the threat.</td>
</tr>
<tr>
<td>Operating System</td>
<td>The OS (Operating System) for which the TIP system reported the threat.</td>
</tr>
<tr>
<td>Detection Time</td>
<td>The time period in which the IOC was detected.</td>
</tr>
</tbody>
</table>
Last Reported IOC

Use the date of the newest threat received by the IOC Scanner Plugin as a policy property to trigger endpoint scans. This property indicates when a threat having the selected severity (Low, Medium, High or Critical) was last reported to the IOC Scanner Plugin from any TIP system on any endpoint in the CounterACT network.

Any threat received by the plugin, regardless of the source, causes this property to be updated on all endpoints. Unlike most CounterACT properties, the value of this property is the same for all CounterACT endpoints.

You can use this property in policies to trigger the Scan and Remediate Known IOCs action on endpoints when new threats are reported by a TIP system. However, if several threats are reported within a short time, it may be inefficient to scan all endpoints each time a new threat is received.

It is recommended to create policies that trigger endpoint scans if the following two conditions are met:

- A threat was reported after the last scan was run.
- A certain period of time has passed since the last scan was run.
All threats reported after last scan was run will be detected in the next scan.

**Last Scan Status**

This property displays the status of the last [Scan and Remediate Known IOCs](#) action performed on the endpoint.

As soon as a [Scan and Remediate Known IOCs](#) action begins to run, this property’s **Scan Start Date** and **Scan Status** fields are populated. The remaining property values are populated upon scan completion.

**Last Scan Status Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Start Date</strong></td>
<td>The time that the scan started.</td>
</tr>
<tr>
<td><strong>Scan Duration (seconds)</strong></td>
<td>The length of time the scan ran, in seconds.</td>
</tr>
</tbody>
</table>
Scan Status | The current status of the scan:
---|---
- Failed to run
- Finished
- Finished with errors
- Never scanned
- No threat exists for selected filters
- Running

Scan Errors | Errors reported if the scan failed.

### Scanning Endpoints – Policy Actions

CounterACT policy actions let you instruct CounterACT how to control detected devices. For example, assign potentially compromised endpoints to an isolated VLAN, or notify the endpoint user or IT team.

In addition to the bundled CounterACT actions available for handling endpoints, you can work with the plugin related actions to create custom policies. These actions are available when you install the plugin.

The following actions are available:
- [Scan and Remediate Known IOCs](#)
- [Add Threat Exception](#)

### Scan and Remediate Known IOCs

Network-based TIP systems might not have full visibility of the network, and agent-based systems might not be installed on all endpoints. The IOC Scanner Plugin fills in these gaps by using the data obtained from various TIP systems to scan Windows endpoints discovered and managed by CounterACT.

Use the **Scan and Remediate Known IOCs** action to scan Windows endpoints for IOCs reported by TIP systems to your IOC repository. Determining which endpoints to scan may depend on the type of installed TIP system, the severity of the threat or other business considerations.

You may want to scan specifically:
- Endpoints on which a TIP agent is not installed.
- Endpoints on which a TIP agent cannot be installed.
- Endpoints that are not otherwise covered by a TIP system.

If a TIP system reports a malicious file on an endpoint, you may want to immediately initiate a scan on other endpoints (either a group, or all endpoints) for the reported IOC. Use Advanced Threat Detection properties as policy conditions to trigger the **Scan and Remediate Known IOCs** action on a given endpoint or on all endpoints when new IOCs are reported.

You can perform scans of varying intensities depending on the severity of the threat. For example, you can perform a scan for all IOCs of a threat with a severity level of High or Critical only.
Scanning involves finding the relevant files and checking their details, such as file hash values, against all IOC details currently listed for the selected threats in the IOC repository. For example, scanning for a threat’s Service IOCs means checking:

- the hash of the executable behind each of the endpoint's system services
- the hash of each executable set to run on the endpoint at start-up by any user

To enable the list of IOC details used during the scan, ensure that the endpoints scanned by this action can connect back to their managed CounterACT Appliance using HTTP (port 80/TCP).

The *Scan and Remediate Known IOCs* action does the following:

- Scans endpoints within the selected scope only.
- Scans only for threats that were reported for all Operating Systems or for the specific OS running on the endpoint.
- Scans for IOCs of selected types defined in threats that:
  - Match the selected filters.
  - Are not in the Threat Exceptions list for that endpoint. See Add Threat Exception.

*CnC Address and DNS Query IOCs of threats not in the Threat Exceptions list are always detected.*

The action also offers the following immediate remediation:

- Kill processes initiated by IOCs detected during the scan.

*Use this option with caution to avoid terminating legitimate processes.*

**To access this action:**

1. Navigate to the Actions tree from the Policy Action dialog box.
2. Expand the **Remediate** folder in the Actions tree, and select **Scan and Remediate Known IOCs**.
### Scan and RemEDIATE Known IOCs Properties

<table>
<thead>
<tr>
<th>Threat Selection Filters</th>
<th>Scan for IOCs defined in threats within the selected filters only. The subset of threats that match the filters is dynamically determined each time the action is run.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Name</td>
<td>Scan for IOCs defined in the selected threat or threats that meet the Threat Selection Filters. Each threat name is followed by the threat file hash.</td>
</tr>
<tr>
<td>IOC Types</td>
<td>Scan for the selected IOC types only. See <a href="#">IOC Types</a>. Note: The action always scans the network session for CnC Address and DNS Query IOCs.</td>
</tr>
<tr>
<td>Remediation: Kill initiated processes</td>
<td>If an IOC process was initiated on the endpoint, kill the process. <em>Use this option with caution to avoid terminating legitimate processes.</em></td>
</tr>
</tbody>
</table>
Add Threat Exception

In a typical deployment, some endpoints have legitimate characteristics that match IOCs defined in your IOC repository. These legitimate indications are detected on the endpoints whenever a scan is run. If the threats and the endpoints that produce false-positive scan results are known, the operator can run an action that:

- Deletes the properties on the endpoint of previous scan results of the specified threat.
- Excludes the specified threat in future scans of the endpoint.

To delete a threat permanently so that no endpoint will be scanned for it, see Remove Threats from the Repository.

Remove Threats from the Threat Exception Repository

Threats and their IOCs remain in the IOC repository until:

- They are manually removed.
- A maximum number of 128 threats is reached.

Manually Remove Threat Exception Data

You can manually remove individual threats from the Threat Exceptions repository so that endpoints will no longer be scanned for specific threats.

To manually remove a threat from the Threat Exception repository:

1. In the IOC Scanner, Threat Exception tab, select one or more threats to be removed.
2. Select Remove, and select Apply to apply the changes.

Use Advanced Threat Detection properties as policy conditions to trigger the Add Threat Exception action on a given endpoint or on all endpoints.

To access this action:

1. Navigate to the Actions tree from the Policy Action dialog box.
2. Expand the Manage folder in the Actions tree, and select Add Threat Exception.
Add Threat Exception Properties

**Threat Name**
Select a threat to be ignored in future scans and whose current scan results will be deleted from the endpoint properties. In the dropdown menu, you can hover over each threat name to see the following information:

- Threat Name
- Threat Severity
- Threat Identifier that consists of:
  - the threat file hash
  - an internal code for the reporting TIP system
  - an internal reference to the OS for which the threat was reported

Note: To remove the threat exception, you must select the same **Threat Identifier** value in the IOC Scanner, Threat Exceptions tab.

**Description**
Enter a textual description of the exception or a relevant comment. (Optional)

**Tags**
To insert endpoint property values in a field, place the cursor in the appropriate field, select **Tags** and select the appropriate tags.

You can use the **IOC Scanner, Threat Exceptions** tab to remove this action for a threat. See [Manage Threat Exceptions](#).
Display Inventory Information

Use the CounterACT Inventory to view a real-time display of IOC Scanner threat network activity at multiple levels, such as threat names, file names and severity levels.

The Inventory lets you:

- Broaden your view of the organizational network from device-specific to activity-specific
- View threats and IOCs that have been detected with specific attributes
- Easily track threat activity
- Incorporate inventory detections into policies

The following information, based on plugin related host properties, is available:

- IOC Scan Stats

- IOCs Detected by CounterACT
To access the inventory:
1. Select the **Inventory** icon from the Console toolbar.
2. Navigate to the **Advanced Threat Detection** entries.

Refer to *Working at the Console* > *Working with Inventory Detections* in the *CounterACT Console User Manual* or the Console Online Help for information about how to work with the CounterACT Inventory.

**Appendix 1: The DNS Query Extension**

The DNS Query Extension detects and parses DNS messages in the network that reference specific host names. The extension does not report other DNS interactions.

The extension provides the **DNS Event** host property that reports details of intercepted DNS messages that reference specific host names of interest. See [DNS Event](#).

**Configure and Test the Extension**

No configuration is required to work with the extension. Only the test parameters need to be defined.

Run a test to:
- Verify that the appliance can see DNS traffic.
- See the DNS traffic witnessed in the test time-frame (or within a packet count limit).
- Develop and verify regular expressions to use as policy conditions for the DNS Event Property.

Running a test does not let you:
- See values in the properties (DNS Event, Is DNS Server).

Follow this procedure to test the extension’s ability to intercept DNS messaging:
To configure and test the extension:

1. In the CounterACT Console, select **Options** from the **Tools** menu. The Options dialog box opens.

2. Navigate to and select the **Plugins** folder.

3. In the **Plugins** pane, select **DNS Query Extension**, and select **Configure**. The Select Appliances dialog box opens.

4. Select the Appliance or Enterprise Manager to which these configuration settings apply. Then select **OK**. The DNS Query Extension Configuration dialog box opens.

5. Configure the following fields that are used to test the CounterACT device’s connection to DNS servers it detects.

<table>
<thead>
<tr>
<th>Test domain name</th>
<th>Indicates a domain name used in test queries sent to DNS servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test regexp</td>
<td>Indicates whether the text in the <strong>Test domain name</strong> field should be evaluated as a regular expression.</td>
</tr>
<tr>
<td>Test period</td>
<td>Indicates the maximum time period of the test, in seconds.</td>
</tr>
<tr>
<td>Test max packets</td>
<td>Indicates the maximum number of packets that are processed during the test.</td>
</tr>
</tbody>
</table>

6. Select **OK** to configure the CounterACT device with the specified values.

7. Repeat this procedure to configure other CounterACT devices.

8. Select **Test** to test the extension.

**Sample Test**

- Test domain name: `•*google.*
- Test regexp: *(Checked)*
- Test period: 40
- Test max packets: 800

This runs a traffic sniffer (pcap) for a maximum of 40 seconds or until the packet count is reached.
While capturing, it displays the packets that matched the exact name unless "regexp" was selected, in which case it prints all those that constitute a regular expression.

As an example and in order to generate traffic, open an internet browser and navigate to drive.google.com or mail.google.com on a computer connected to a CounterACT monitored network.

The output appears as follows:

Processing up to 800 DNS packets during 40 seconds...

Listening for DNS traffic on [eth0 eth1]

Name=drive.google.com Type=A Client= endpoint-ip Server= dns-server-ip Response=0 Answers=

<...etc...>

Name=drive.google.com Type=A Client=10.41.1.136 Server=10.44.1.1 Response=1
Answers=drive.google.com. 8 IN A 216.58.210.14

Name=goolgemail.l.google.com Type=A Client=10.41.1.1 Server=10.0.0.4
Response=1 Answers=goolgeemail.l.google.com. 117 IN A 216.58.208.37

Name=goolgeemail.l.google.com Type=A Client=10.41.1.1 Server=10.0.0.4
Response=1 Answers=goolgeemail.l.google.com. 117 IN A 216.58.208.37

Name=drive.google.com Type=A Client=10.41.1.136 Server=10.44.1.1 Response=0
Answers=

Name=drive.google.com Type=A Client=10.41.1.136 Server=10.44.1.1 Response=0
Answers=
Detecting Endpoints – DNS Query Properties

This extension provides the following host properties in the Device Information folder:

- **Is a DNS Server**
- **DNS Event**

You can use these properties in custom policies. See [Create Custom IOC Scanner Policies](#).

**Is a DNS Server**

This Boolean property indicates if the DNS Query Extension has observed the endpoint accepting and responding to DNS queries.

**DNS Event**

This composite property indicates details of DNS messages to and from the endpoint that were intercepted by the DNS Query Extension.

Only messages that reference specific host names of interest are reported. DNS monitoring of a host name is invoked in one of two ways:

- When a **DNS Query IOC** is reported to CounterACT, the IOC Scanner Plugin initiates DNS monitoring that detects all DNS interactions that reference the suspect host name mentioned in the IOC.
- When you create a policy condition using the **DNS Event** property provided by the extension, CounterACT monitors DNS traffic that matches the host name you specify.

The following information is reported for each DNS message.

<table>
<thead>
<tr>
<th><strong>DNS Name</strong></th>
<th>Indicts the hostname that the DNS server is asked to resolve.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DNS Query Type</strong></td>
<td>Indicates the Query Type of the DNS message. This is also known as the Request Type, Record Type, or Lookup Type.</td>
</tr>
<tr>
<td><strong>DNS Query/Response</strong></td>
<td>Indicates whether this message is the initial query or the response of the DNS Server. Valid string values are &quot;query&quot; and &quot;response&quot;.</td>
</tr>
</tbody>
</table>
### DNS Zone
In DNS response messages, contains the response message in zone file format.

### DNS Address(es)
In DNS response messages, indicates the IP address(es) returned by the DNS server.

### DNS Server Address
Indicates the IP address of the DNS server to which the query is addressed.

### DNS Monitoring Tag
Indicates the reason that CounterACT monitors messaging for the specified hostname. Valid values are:
- Policy – this hostname is specified in a policy condition using this host property.
- TIP – Advanced Threat Detection mechanisms have identified this hostname for monitoring.
Both values can be valid simultaneously for a single DNS name.

## Additional CounterACT Documentation
For more detailed information about the CounterACT features described here or additional CounterACT features and modules, refer to the following resources:

- [Documentation Portal](#)
- [Customer Support Portal](#)
- [CounterACT Console Online Help Tools](#)

## Documentation Portal
The ForeScout Documentation Portal is a Web-based library containing information about CounterACT tools, features, functionality and integrations.

**To access the Documentation Portal:**
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.
Customer Support Portal

The Customer Support Portal provides links to CounterACT version releases, service packs, plugins and modules as well as related documentation. The portal also provides a variety of How-to Guides, Installation Guides and more.

To access the Customer Support Portal:
2. Select the CounterACT version you want to discover.

CounterACT Console Online Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons
Use context sensitive Help buttons to quickly access information about the tasks and topics you are working with.

Console User Manual
Select CounterACT Help from the Help menu.

Plugin Help Files
1. After the plugin is installed, select Options from the Tools menu and then select Plugins.
2. Select the plugin and then select Help.

Documentation Portal
Select Documentation Portal from the Help menu.
Legal Notice

Copyright © ForeScout Technologies, Inc. 2000-2017. All rights reserved. The copyright and proprietary rights in this document belong to ForeScout Technologies, Inc. ("ForeScout"). It is strictly forbidden to copy, duplicate, sell, lend or otherwise use this document in any way, shape or form without the prior written consent of ForeScout. All other trademarks used in this document are the property of their respective owners.

These products are based on software developed by ForeScout. The products described in this document may be protected by one or more of the following U.S. patents: #6,363,489, #8,254,286, #8,590,004, #8,639,800 and #9,027,079 and may be protected by other U.S. patents and foreign patents.

Redistribution and use in source and binary forms are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials and other materials related to such distribution and use acknowledge that the software was developed by ForeScout.

Unless there is a valid written agreement signed by you and ForeScout that governs the below ForeScout products and services:

- If you have purchased any ForeScout products, your use of such products is subject to your acceptance of the terms set forth at http://www.forescout.com/eula/;
- If you have purchased any ForeScout support service ("ActiveCare"), your use of ActiveCare is subject to your acceptance of the terms set forth at http://www.forescout.com/activecare-maintenance-and-support-policy/;
- If you have purchased any ForeScout Professional Services, the provision of such services is subject to your acceptance of the terms set forth at http://www.forescout.com/professional-services-agreement/;
- If you are evaluating ForeScout’s products, your evaluation is subject to your acceptance of the applicable terms set forth below:
  - If you have requested a General Availability Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/evaluation-license/.
  - If you have requested a Beta Product, the terms applicable to your use of such product are set forth at: http://www.forescout.com/beta-test-agreement/.
  - If you have purchased any ForeScout Not For Resale licenses, such license is subject to your acceptance of the terms set forth at http://www.forescout.com/nfr-license/.

Send comments and questions about this document to: documentation@forescout.com

2017-05-26 15:14