Event Investigation Using Web-Based Resources

Event Investigation Using Web-Based Resources

Use the contextual cross-launch feature to quickly find more information about potential threats in web-based resources outside of the Secure Firewall Management Center. For example, you might:

- Look up a suspicious source IP address in a Cisco or third-party cloud-hosted service that publishes information about known and suspected threats, or
- Look for past instances of a particular threat in your organization's historical logs, if your organization stores that data in a Security Information and Event Management (SIEM) application.
- Look for information about a particular file, including file trajectory information, if your organization has deployed Cisco Secure Endpoint.

When investigating an event, you can click directly from an event in the event viewer or dashboard in the Secure Firewall Management Center to the relevant information in the external resource. This lets you quickly gather context around a specific event based on its IP addresses, ports, protocol, domain, and/or SHA 256 hash.

For example, suppose you are looking at the Top Attackers dashboard widget and you want to find out more information about one of the source IP addresses listed. You want to see what information Talos publishes about this IP address, so you choose the "Talos IP" resource. The Talos web site opens to a page with information about this specific IP address.

You can choose from a set of pre-defined links to commonly used Cisco and third-party threat intelligence services, and add custom links to other web-based services, and to SIEMs or other products that have a web interface. Note that some resources may require an account or a product purchase.

About Managing Contextual Cross-Launch Resources

Manage external web-based resources using the **Analysis** > **Advanced** > **Contextual Cross-Launch** page.

Pre-defined resources offered by Cisco are marked with the Cisco logo. The remaining links are third-party resources.

You can disable or delete any resources that you do not need, or you can rename them, for example by prefixing a name with a lower-case "z" so the resource sorts to the bottom of the list. Disabling a cross-launch resource disables it for all users. You cannot reinstate deleted resources, but you can re-create them.

To add a resource, see Add Contextual Cross-Launch Resources, on page 2.

Requirements for Custom Contextual Cross-Launch Resources

When adding custom contextual cross-launch resources:

- Resources must be accessible via web browser.
- Only http and https protocols are supported.
- Only GET requests are supported; POST requests are not.
- Encoding of variables in URLs is not supported. While IPv6 addresses may require colon separators to be encoded, most services do not require this encoding.
- Up to 100 resources can be configured, including pre-defined resources.

Add Contextual Cross-Launch Resources

You can add contextual cross-launch resources such as threat intelligence services and Security Information and Event Management (SIEM) tools.

In multidomain deployments, you can see and use resources in parent domains, but you can only create and edit resources in the current domain. The total number of resources across all domains is limited to 100.

Before you begin

- If you are adding links to a Secure Network Analytics appliance, check to see if the links you want already exist; most links are automatically created for you when you configure Security Analytics and Logging (On Premises).
- See Requirements for Custom Contextual Cross-Launch Resources, on page 2.
- If needed for the resource you will link to, create or obtain an account and the credentials needed for access. Optionally, assign and distribute credentials for each user who needs access.
- Determine the syntax of the query link for the resource that you will link to:

  Access the resource via browser and, using the documentation for that resource as needed, formulate the query link needed to search for a specific sample of the type of information you want your query link to find, such as an IP address.

  Run the query, then copy the resulting URL from the browser's location bar.

  For example, you might have the query URL `https://www.talosintelligence.com/reputation_center/lookup?search=10.10.10.10`.

Procedure

Step 1 Choose **Analysis** > **Advanced** > **Contextual Cross-Launch**.

Step 2 Click **New Cross-launch**.

In the form that appears, all fields marked with an asterisk require a value.

Step 3 Enter a unique resource name.

Step 4 Paste the working URL string from your resource into the **URL Template** field.

Step 5 Replace the specific data (such as an IP address) in the query string with an appropriate variable: Position your cursor, then click a variable (for example, **ip**) once to insert the variable.

In the example from the "Before You Begin" section above, the resulting URL might be **`https://www.talosintelligence.com/reputation_center/lookup?search={ip}`**. When the contextual cross-launch link is used, the {ip} variable in the URL will be replaced by the IP address that the user right-clicks on in the event viewer or dashboard.

For a description of each variable, hover over the variable.

You can create multiple contextual cross-launch links for a single tool or service, using different variables for each.

Step 6 Click **Test with example data** (↗) to test your link with example data.

Step 7 Fix any problems.

Step 8 Click **Save**.

Investigate Events Using Contextual Cross-Launch

Before you begin

If the resource you will access requires credentials, make sure you have those credentials.

Procedure

Step 1 In the Secure Firewall Management Center, click **Analysis** > **Unified Events**.

Step 2 Right-click the event of interest and choose the contextual cross-launch resource to use.

If necessary, scroll down in the context menu to see all available options.

The data type you right-click on determines the options you see; for example, if you right-click an IP address, you will only see contextual cross-launch options that are relevant to IP addresses.

For example, to get threat intelligence from Cisco Talos about a source IP address in the intrusion event, choose **Talos SrcIP** or **Talos IP**.

If a resource includes multiple variables, the option to choose that resource is available only for events that have a single possible value for each included variable.

The contextual cross-launch resource opens in a separate browser window.

It may take some time for the query to be processed, depending on the amount of data to be queried, speed of and demand on the resource, and so on.

Step 3 Sign in to the resource if necessary.