DARKTRACE/ZERO TRUST JUMPCLOUD MODULE

Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate with enterprise software and cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module brings the insight of the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection to enterprise software and cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

How it works

The Darktrace/Zero Trust Jumpcloud module provides coverage over administration of the JumpCloud platform and enables JumpCloud logins to be tracked against devices in the Darktrace Threat Visualizer. User activity is retrieved directly from the JumpCloud Directory Insights API, returned information is therefore limited to the events that JumpCloud makes available and the data recorded as part of each log event. Typically, the following events will be surfaced in the Threat Visualizer:

- Login Success
- Login Failure
- Group Modified
- New System Added
- Command Run
- App Added

In addition to events surfaced in the Threat Visualizer for users of the JumpCloud Platform, the module provides tracking information to Darktrace DETECT/Network for devices accessed via JumpCloud agents and for logins to those JumpCloud agents. If this functionality is desired, please ensure the IPs of devices accessed via JumpCloud are explicitly included in the **Deployment Scope** on the System Config page.

JumpCloud events makes events available to the Darktrace module within minutes of the event occurring. In order to achieve more accurate, real-time monitoring, high frequency polling is recommended. Returned events are organized by Darktrace into categories which appear as metrics in the Darktrace Threat Visualizer. This allows events to be easily identified and for models to be written which can identify similar unusual activity across a range of different modules.

Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud or Darktrace/Zero Trust modules will provide access to the SaaS Console, a specialized interface for investigating SaaS and Cloud activity. The console is powered by the Cyber AI Analyst and Darktrace's unique 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments whilst also maintaining existing workflows for operators already familiar with the Darktrace Threat Visualizer. The SaaS console provides access to global maps of activity, detailed logs of user activity and visualization of anomalous chains of behavior.

Considerations

Delays may be incurred where the external platform does not make events available to the Darktrace module for processing and analysis within the expected timeframe. Delays of this nature are the responsibility of the third-party platform. Latency between event occurrence and when it was made available to the module are indicated in the event metadata within the Threat Visualizer.

By default, the module polls every 60 seconds and makes at least one API call per loop. The module may make additional calls to determine the names of users, groups and apps associated with events. This polling interval can be altered by a member of Darktrace support if desired. If throttling problems are encountered, there are several contingency plans we can enact such as introducing a wait time between querying each different subscription to spread the requests out over a longer time period.

License Requirements: The JumpCloud module requires a JumpCloud license with the "Directory Insights" add-on.

Deployment Process

1. Open the Darktrace Threat Visualizer and navigate to the **System Config** page. Select **Modules** from the left-hand menu.

2. Select **Jumpcloud** from the available **Cloud/SaaS Security** modules. A new dialog will appear. Ensure the module is **enabled**.

3. Click the "**New Account**" button to create an account - if an account is already configured, the button is located underneath the existing entry. Add an **Account Name** - this field will be displayed in the Threat Visualizer alongside events from Jumpcloud. Save your changes.

4. Log in to the JumpCloud console as an administrator.

   Open the drop down menu in the top right corner by clicking on the email address of the administrator. Select the '**API Settings...**' option.

5. **Copy the API Key shown**.

   Please note, if the API Key associated with this administrator is regenerated at any point, the Darktrace JumpCloud module will need to be re-authorized.

6. Return to the **System Config** page on the Darktrace Threat Visualizer and paste the API Key into the **Administrator API Key** field.

7. Click the "**Authorize**" button to begin monitoring your Jumpcloud environment.

   After attempting to retrieve data for the first time, the module will report whether the poll cycle was successful. If any errors occur, these will be reported in the **Status** section

Your JumpCloud module is now authorized. Events should appear in the Threat Visualizer after a short delay. This is a one-time process and no maintenance should be required unless the administrator API Key is regenerated.