DARKTRACE/APPS DROPBOX 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/Apps Dropbox Module provides visibility and analysis over file activity and administrative activity within Dropbox. Data is retrieved directly from the Dropbox API, returned information is therefore limited to the events that Dropbox makes available and the data recorded as part of those entries. Typically, the following events will be surfaced in the Threat Visualizer:

- Login activity and access changes
- File modifications and deletions
- File uploads and downloads
- File and folder access permissions changes
- Changes to group membership and user roles
- File sharing changes

Please note, customers with the Dropbox Standard Business plan will have visibility over login events only.

Monitoring is achieved by utilizing the Business API and relevant Dropbox SDK - by default, the module for Dropbox polls every 60 seconds. In order to achieve more accurate, real-time monitoring, high frequency polling is recommended. Dropbox event logs are updated in real time, allowing for real-time monitoring processes.

The data retrieved from Dropbox is organized by Darktrace into categories which appear as metrics in the Threat Visualizer and are available for custom model creation. Additionally, Darktrace provides a selection of models to identify potential Data Loss incidents and anonymous file access events.

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

Dropbox imposes a limit on the number of HTTPS requests allowed in a given time period; this limit is not made publicly available. Dropbox limits HTTPS requests on a per-app basis. This means that the number of requests utilized by the module for Dropbox will not impact other applications installed by the customer, and vice-versa.

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.

License Requirements: It is highly recommended for customers with the Standard Business plan to upgrade to the Advanced Business plan, as this allows the Darktrace/Apps Dropbox Module to monitor all events related to files. For customers with the Dropbox Standard Business plan, the module for Dropbox can only detect login events.

Permissions

Darktrace/Apps Dropbox Module requires access to the company's team information, as well as the team's detailed activity log. Although these permissions must be granted by an Admin user, the module for Dropbox does not acquire any Admin permissions and appears as a separate entity to the Dropbox system.

Deployment Process

1. Open the Darktrace Threat Visualizer and navigate to the **System Config** page. Select **Modules** from the left-hand menu.
2. Select **Dropbox** 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 Dropbox.
4. Under **Information**, click the authorization link.
5. Login in with an account with administrative permissions over the domain you wish Darktrace to monitor and grant the requested permissions.
6. Generate the authorization code. Return to the Darktrace Threat Visualizer **System Config** page and enter the authorization code into the appropriate field. For security reasons, the code will expire after a short period so this step must be performed immediately after generation.
7. Click the "**Authorize**" button to begin monitoring your Dropbox 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

The module is now authorized and monitoring your domains. Please note, if changes are made to your Dropbox domains or the administrator credentials change, this authorization may have to be repeated; your Darktrace representative can advise on whether this is necessary.