Darktrace Security Module for Box

Introduction

Darktrace Security Modules integrate with enterprise SaaS software and Cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Enterprise Immune System defense 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 SaaS 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 Security Module for Box utilizes the Box SDK to provide visibility over content management and user activity within the Box platform. Data is retrieved directly from the Admin logs generated by Box, returned information is therefore limited to the events that Box chooses to audit and the data recorded as part of those log entries. Typically, the following events will be surfaced in the Threat Visualizer:

- Login activity
- User management (creation, deletion)
- Collaboration actions
- Content uploads and downloads
- Content modification

Box makes events available to the Darktrace Security Module within minutes of the event occurring. Monitoring is achieved via sets of HTTPS requests made with an authenticated token to the Box API - by default, one set of requests is made every minute.

The data retrieved from Box 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 Security 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

Box makes at least one HTTPS request per loop. The number of HTTPS requests made increases linearly with the number of events being created (which depends on the number of users and how frequently they do things). Box imposes a limit on the number of HTTPS requests allowed in a given time period. This limit is 25,000 API calls per month for a Starter account, 50,000 for Business-tier accounts and 100,000 for an Enterprise account.

Due to this limit, please consider the following factors when selecting an appropriate polling policy or modifying the default configuration for your environment:

- Time lapse between the occurrence of an event and its detection
- Cost of upgrading the account to increase the number of HTTPS requests that can be made per day

Delays may be incurred where the SaaS or Cloud platform does not make events available to the Darktrace Security 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.

Permissions

Darktrace Security Module for Box requires the following permissions in order to fetch events:

- Read and write all files and folders stored in Box
- Manage enterprise
- Manage users
- Manage groups
- Manage enterprise properties
- Manage retention policies
- Manage webhooks v2

Although these permissions must be granted by an Admin user, the module for Box module does not acquire any Admin permissions, and appears as a separate entity to the Box 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 **Box** 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 Box.

4. Under **Information**, click the authorization link.

5. Login in with an account with administrative permissions over the domains you wish Darktrace to monitor and grant the requested permissions.

6. 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 Box 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 Box domains or the user who performed the authorization is modified or deleted, this authorization may have to be repeated; your Darktrace representative can advise on whether this is necessary.