DARKTRACE/ZERO TRUST EGNYTE 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 Egnyte module provides visibility over login activity, file system modification and changes to file and folder access. Egnyte produces three audit reports on demand - Login Audit, File Audit and Permissions Audit - which are requested and processed by the module to achieve monitoring. Data is retrieved directly from each audit report, returned information is therefore limited to the events that Egnyte chooses to audit and the data recorded as part of each entry. Processing all reports provides coverage over the following events:

- Login activity
- File modifications
- File uploads and downloads
- File and folder access permissions changes

Login activity is available almost immediately, but file activity is only collated by Egnyte periodically. The module will retrieve and surface events in the Threat Visualizer as soon as they are made available to it. Monitoring is achieved via sets of HTTPS requests made with an authenticated token to the Egnyte API - by default, one set of audit report requests is made every 10 minutes.

The data retrieved from Egnyte 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

Egnyte restricts the maximum number of requests available to Darktrace module to 5,000 per day. Under default configuration options, the Egnyte module makes approximately 15 requests per cycle so should not reach this limit. If the polling frequency is altered manually and the cap is reached, the module will automatically double the time between poll cycles and wait until the request limit has reset. All events will still be retrieved, but there will be significant delay between the activity and their appearance in the Threat Visualizer.

The module regularly generates and deletes audit reports which may result in some notifications appearing on your Egnyte Dashboard. It is currently not possible to turn these notifications off in Egnyte. The reports referenced are deleted shortly after creation to avoid filling up cloud storage space.

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.

The Darktrace/Zero Trust Egnyte module requires the domain selected for monitoring to have an Egnyte license that includes the 'Advanced Security Package'. This package is included by default in Business and Enterprise editions.

Permissions

The Darktrace module for Egnyte requires the `Egnyte.audit` permission scope in order to generate and read audit reports. The permissions required also allow us to delete audit reports

Deployment Process

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

2. Select **Egnyte** 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 Egnyte.

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

5. Enter your Egnyte domain name in the following page, it will redirect to an Egnyte login page. Log in to Egnyte, generating a unique authorization code.

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 Egnyte 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 Egnyte domains or the administrator credentials change, this authorization may have to be repeated; your Darktrace representative can advise on whether this is necessary.