DARKTRACE/APPS GOOGLE WORKSPACE MODULE

Introduction

Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules integrate Darktrace DETECT and RESPOND capabilities with enterprise SaaS software and Cloud platform solutions, bringing visibility and threat analysis to critical systems. Extending Darktrace's Self-Learning AI beyond the physical enterprise network, each module introduces 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 Google Workspace module provides visibility over user activity, user management, file creation and sharing, and administrative events. Data is retrieved directly from the Google Workspace audit log, returned information is therefore limited to the events that Google Workspace chooses to audit and the data recorded as part of those audit log entries. Typically, the following events will be recorded and fed through to the Threat Visualizer:

- Login events (including failed)
- Access method changes (multi-factor authentication usage)
- User and Role creation/modification
- Group membership changes
- Calendar event creation and invites
- File and folder modification events including creation and deletion
- File visibility changes or sharing events
- General administrative activity such as organizational unit changes, licensing and app approval

Monitoring is achieved via sets of HTTPS requests made with API access to the Google Workspace (formerly G Suite) audit log - by default, one set of requests is made every minute. In order to achieve highly accurate, real-time monitoring, high frequency polling is recommended. This polling interval can be altered by a member of Darktrace support if desired. The Google Workspace module makes at least two HTTPS requests per loop, and this increases linearly with the number of events being created (which depends on the number of users and how frequently they do things).

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 and Darktrace/Zero Trust modules will provide access to the SaaS Console (Customer Portal), a specialized interface for investigating SaaS and Cloud activity. The SaaS console is powered by the Cyber AI Analyst and Darktrace's 'pattern of life' anomaly detection; each element is purpose built for monitoring and analysis in these environments, while maintaining existing workflows for operators that are already familiar with the Darktrace Threat Visualizer. The SaaS console contextualizes activity on a world map, visualizes anomalous behavior and presents detailed logs of user activity.

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.

Google Workspace imposes a complex and regularly updated limit policy on how many HTTPS requests can be made in a given time period. 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 increasing the number of HTTPS requests that can be made per day

License Requirements: Business Standard or higher is required for the Darktrace/Apps Google Workspace module to function.

Autonomous Response

The Darktrace/Apps Google Workspace module supports Darktrace RESPOND autonomous response. The module can perform two actions in response to highly anomalous and potentially malicious activity - force a user to logout and disable a user. The available inhibitors and platforms will be expanded in future releases.

SaaS platforms are at the center of many businesses; granular controls are therefore provided to slowly build up confidence in autonomous actions before enabling them across the business environment. Users can be added to a global or per-inhibitor 'immune list', preventing Darktrace RESPOND from taking one or more actions against their account. Darktrace RESPOND can also operate in confirmation mode, where a human is required to approve autonomous actions before they are taken.

Please note, modules authorized solely for monitoring must be reauthorized to add additional Darktrace RESPOND API scopes. Please refer to the configuration guide (Customer Portal)**.**

Google Drive

To prevent desktop-based Google Drive sync applications syncing user changes to/from the cloud, the "Disable User" action should be applied. Whilst the "Disable User" action is active, syncing will be prevented.

Users will be required to sign in again to any desktop-based Google Drive sync applications after the "Disable User" action has cleared or expired. After the action is cleared or expired, syncing will resume and any changes made locally by the user will be synced to Google Drive. Therefore, it is recommended that a longer action period is used when performing this action manually so that all investigations can take place before the user is able to resume sync.

Darktrace RESPOND/Apps for Google Workspace Considerations

- The Google Workspace super administrator user who performs the configuration/authorization process cannot be actioned using "Disable User".

- Users will be required to sign in again to any desktop-based Google Drive sync applications after the "Disable User" action has cleared or expired.

Permissions

Darktrace/Apps Google Workspace module requires access to the Google Workspace Admin Log to fetch events. A service account with the minimal, read-only Project > Viewer role is created during configuration to facilitate this.

Deployment Process

The deployment process for Darktrace/Apps Google Workspace module is relatively straightforward and is described in more detail in the setup guide. Essentially the process comes down to:

1. Create a new development project and enable Admin SDK.
2. Create a new Service Account for the newly created project to be utilized by Darktrace and provide the Service Account with Domain-Wide authority.
3. Input details, such as an Account Name, your Admin Email and a JSON file created during the process into the Darktrace Threat Visualizer configuration page.