DARKTRACE/CLOUD GOOGLE CLOUD PLATFORM 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/Cloud Google Cloud Platform module (GCP) provides visibility over administration and user activity within your Google Cloud environment. The module utilizes the Google Cloud logging API to retrieve GCP-audited events - information available to the module is therefore limited to the events that GCP chooses to audit, and the data recorded as part of those audit-log entries. Administration and system events logs are produced by default by GCP and provide the Darktrace module visibility over the creation of cloud resources, API activity and changes to cloud resource configurations. This includes events generated by users and system actions at both the organizational and project-level.

Typically, the following events will be recorded and passed to the Threat Visualizer:

- Resource creation through administrative actions or API calls, such as VM creation
- Resource modification through administrative actions or API calls, such as permission changes
- Resource configuration changes performed by system events
- User-driven API calls and changes to user-provided resource data (*derived from Data Access logs, please see below*)

A comprehensive list of GCP services which support Cloud Audit Log monitoring and the type of events that are audited can be found in the relevant Google documentation.

Data Access logs can also be produced within GCP and processed by the module to gain additional insight into specific components. Data Access logs are not produced by default and must be enabled on a per-component basis to gain greater insight. Please note, Data Access audit logs do not record data-access operations on resources that are publicly shared (available to *All Users* or *All Authenticated Users*), or that can be accessed without logging into Google Cloud.

Firebase

Some monitoring is also available over Google Firebase events. Firebase management activity is recorded in the Cloud Admin Activity log and the Cloud Data Access log. Full details of audited events can be found in the Firebase documentation. As the production of Data Access logs is optional, additional configuration is required to produce these logs and make them available to the module. This additional configuration is covered in the setup guide.

Visualization

Deploying one or more Darktrace/Apps, Darktrace/Cloud and Darktrace/Zero Trust modules will provide access to the Platform Accounts Console (Customer Portal), a specialized interface for investigating SaaS and Cloud activity.

The Platform Accounts 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 Platform Accounts Console contextualizes activity on a world map, visualizes anomalous behavior and presents detailed logs of user activity.

Considerations

User access to GCP is authenticated and managed via the Google Workspace platform; this activity is not visible to the GCP module. To monitor logins, user activity, and resource creation/modification across the entire platform, it is recommended to deploy both modules (Darktrace/Apps Google Workspace and Darktrace/Cloud GCP). The deployment guide provides alternative deployment methods, including a dual deployment for fresh installations and an extension process for organizations that already use the Darktrace Google Workspace module.

Data Access logs are an optional part of the Google Cloud Logging service. This logging is largely free, but costs may be incurred above a certain volume of log creation/ingestion. For most organizations, this limit will not be reached (see the relevant Log Pricing resources from Google), but your Darktrace representative can limit the rate of data access events if such costs are a concern.

GCP Cloud Logs are restricted to 60 API requests per minute. By default, the module monitors all projects in the organization for which it is authenticated. If the module regularly makes more than 60 requests per minute, or specific projects like testing environments do not need to be monitored, this scope can be reduced by entering only the project IDs of interest.

Delays may be incurred if the external platform does not make events available to the Darktrace module for processing and analysis within the expected period. Such delays are the responsibility of the third-party platform. Latency between the time an event occurred and the time it was made available to the module are shown in the event metadata within the Threat Visualizer.

License Requirements: The GCP module requires that Google Cloud Operations Cloud Logging be enabled. This should be enabled on all license types by default. If you are not sure whether this available with your GCP license, please see the Google Cloud Operations documentation for more information.

Permissions

Darktrace/Cloud GCP module requires the roles **Logging** -> **Private Logs Viewer** and **Resource Manager** -> **Organization Viewer** to be granted to a Service Account at the Organizational level.

Deployment Process

The deployment process for Darktrace/Cloud GCP module is covered in more detail in the configuration guide. Three deployment processes are offered for organizations who wish to just deploy GCP, to deploy both GCP and G Suite modules together or for those with an existing G Suite module who wish to extend its coverage.

Essentially the process comes down to:

1. Create a new development project and enable Cloud Logging APIs.
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. Add the Service Account at the organizational level and grant it the required roles.
4. Input details such as an Account Name and a JSON file created during the process into the Darktrace Threat Visualizer configuration page.