PRODUCT GUIDE

DARKTRACE/APPS SALESFORCE 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 Salesforce module provides coverage over administrative, resource modification and file events. By default, it monitors a subset of sObjects - resources in the Salesforce environment - but this is easily expandable on the System Config page to ensure coverage over your desired resources. The module queries the Salesforce API for creation, modification and deletion of sObjects that it is actively monitoring. By default, the following classes are monitored:

- Account
- Contact
- Dashboard
- Content Document
- Document
- Event
- Task
- User

Login activity and modifications to the Setup area are also retrieved from auditing endpoints, separate from sObject monitoring.

In addition, the module retrieves and processes Salesforce Event Logs which cover the following events:

- Report creation
- Report exports/downloads
- File uploads
- File downloads
- Content document distribution (sharing)

Salesforce attempts to create a new Event Log every hour but will default to 24 hours if an error occurs - the module will request the Event Log hourly if available.

By default, the module for Salesforce polls every 60 seconds. In order to achieve more accurate, real-time monitoring, high frequency polling is recommended.

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

Salesforce imposes a limit on the number of HTTPS requests executed by a company over a rolling 24 hour period, calculated by Salesforce license type. This limit is between 15,000 and 1,000,000 requests per day and is applied across all services querying the API of a specific Salesforce instance. In default configuration, the module makes 8 queries for sObjects, 2 queries for audit information (Login History and Setup modifications) and 1 query for Event Logs at a polling rate of every 5 minutes. Over 24 hours, this produces a minimum of 3,168 requests. Adding additional sObjects, or high volumes of user activity, will greatly increase the number of requests required.

Your Darktrace representative can alter the polling frequency if rate-limiting is occurring. Please consider the following factors when selecting an appropriate polling policy or modifying the default monitoring configuration for your environment:

- Number of sObject classes monitored
- Time lapse between the occurrence of an event and its detection
- Differentiation of separate events occurring within a short time frame on the same sObject, as queries only register the most recent modification
- Demand for API requests across all services querying Salesforce
- Cost of increasing the HTTPS request limit

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: Lightning Enterprise License or higher is required for the Darktrace/Apps Salesforce module to function.

The module is currently limited to Salesforce Sales Cloud. Salesforce Commerce Cloud (Demandware) and Marketing Cloud are not supported.

Permissions

Darktrace/Apps Salesforce module requires permission to:

- Access your basic information
- Access and manage your data
- Provide access to your data via the web
- Access and manage your Chatter data
- Provide access to custom applications
- Allow access to your unique identifier
- Access custom permissions
- Access and manage your Wave data
- Access and manage your Eclair data
- Perform requests on your behalf at any time

These permissions are required in order to monitor for events, and so that Darktrace for Salesforce can continue monitoring with no further user interaction required.

Deployment Process

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

2. Select **Salesforce** 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 Salesforce.

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. Generate the authorization code and URL.

6. Return to the Darktrace Threat Visualizer **System Config** page and enter the authorization code and URL into the appropriate fields. 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 Salesforce 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 Salesforce 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.