DARKTRACE/APPS MICROSOFT 365 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 Microsoft 365 module provides visibility over a number of sub-products including Sharepoint/ OneDrive for Business, Dynamics, Teams, and other Microsoft 365 services. Depending on the service, this user activity can include user management, file creation and sharing, and administrative events. Data is retrieved directly from the Microsoft unified audit log, returned information is therefore limited to the events that Microsoft chooses to audit and the data recorded as part of those audit log entries. Returned events will also be restricted to products that your organization has licensed with Microsoft 365.

Monitoring is achieved via sets of HTTPS requests made with an authenticated token to the Microsoft unified audit log - by default, one set of requests is made every minute. The unified audit log is populated by Microsoft 365 with aggregated "content blobs" for each service; when an auditable event is created, it can take up to 3 hours for the "blob" it is contained within to be made available in the log. The data retrieved from Microsoft 365 is organized by Darktrace into categories which appear as metrics in the Threat Visualizer and are available for custom model creation.

Please note, Audit Log Search must be enabled for comprehensive monitoring.

Sharepoint (OneDrive for Business)

Darktrace retrieves user activity for Sharepoint (OneDrive for Business) and activity produced by Microsoft 365 services which interact with Sharepoint. This activity includes file and folder creation, deletion and modification. Visibility changes and sharing events are also retrieved. Additionally, Darktrace provides a selection of models to identify potential Data Loss incidents and anonymous file access events.

Dynamics 365

The module can surface Dynamics 365 user activity in the Threat Visualizer where compatible auditing has been configured in the Dynamics instance. Please see the relevant Microsoft documentation on configuring Dynamics 365 auditing. The events returned by the module will depend on the configuration settings of each Dynamics environment; entities with auditing enabled will produce create, read and modify events in the Darktrace Threat Visualizer.

Please note, Microsoft does not produce audit logs for sandbox environments.

Teams

The Darktrace/Apps Microsoft 365 module can retrieve a subset of Microsoft Teams activity including logins and changes to team membership. Also retrieved are administrative actions such as Team and Channel creation and the addition or removal of Apps, Connectors and bots from Channels.

Administration and Access

Microsoft 365 login activity is managed by Azure AD. Organizations with the Darktrace/Apps Microsoft 365 module will see a limited number of login and management events handled by Azure but will not have full visibility over all administrative activity. Events that will be retrieved include login and access activity, changes to recovery information and changes to multi-factor authentication use. User administration changes including role assignment and removal, group membership, user creation and user deletion will also be retrieved.

In addition to Microsoft 365 events handled by Azure, the module also processes administrative events from a number of services. This includes Microsoft 365 mailbox administration as well as general administrative activity like quarantine management, licensing and app approval.

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

Microsoft 365 imposes a complex and regularly updated limit policy on HTTPS requests. If this limit is regularly reached, it may be necessary to make the intervals between polls longer - doing so will increase the time lapse between the occurrence of an event and its detection. Please discuss implementing a larger interval with your Darktrace representative or a member of Darktrace support.

The module will only make requests at the defined interval - default 1 minute - if the previous request cycle has completed within the interval. Therefore in high traffic environments, or where a large amount of activity has occurred, it may take longer than the defined interval for the next poll to occur.

The module requires access to specific endpoints in the third-party environment to retrieve event data. The required endpoints are listed on the System Configuration page. Please ensure these endpoints are allowed by any intermediary firewalls.

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.

Please note that it can take up to 12 hours for Microsoft 365 to produce the first event logs after enabling the unified audit log.

License Requirements: monitoring is compatible with any license that includes access to the Security and Compliance Centre and Unified Audit Logging. These features are included in the Microsoft 365 Business Basic, Business Premium and Enterprise Licenses by default.

Please see the Microsoft documentation for further information on whether your license is compatible.

Autonomous Response

The Darktrace/Apps Microsoft 365 module supports Darktrace RESPOND autonomous response. The module can perform three actions in response to highly anomalous and potentially malicious activity - force a user to logout, disable a user and block an IP (or IP range). 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 before v5, or authorized solely for monitoring, must be reauthorized to add additional Darktrace RESPOND Permissions to the Graph API authorization. Please refer to the configuration guide for your chosen deployment method for more information.

Darktrace RESPOND Considerations

- An Azure P1 license is required for access to the Graph API.
- Due to restrictions on application-level permissions, admin users cannot be disabled or forced to logout using the default authentication method. Block IP actions can still be performed.

  Authentication with Device Code flow is required to perform these actions on administrative users.
- Where an on-premises Azure AD is synced via Azure AD Connect, actions taken against users in the cloud-based environment (***force logout***, ***disable user***) will be overwritten.

  To prevent this, turn on "Repeat All Actions" within Darktrace RESPOND settings for the module. This setting will continuously apply the action, so any overwritten changes by Azure AD Connect are reinstated.

Permissions

In the default deployment mode, the Microsoft 365 module requires the following permissions to be granted by a Global Administrator user.

Monitoring Permissions

- Read DLP policy events including detected sensitive data
- Read activity data for your organization
- Read service health information for your organization
- Read all users' full profiles
- Read all audit log data
- Read and write all applications
- Read directory data
- Sign in and read user profile

Darktrace RESPOND Only Permissions

- Read and write all users' full profiles
- Read your organization's policies
- Read your organization's security actions
- Read your organization's security events
- Read and write your organization's conditional access policies

The exact permissions requested differs slightly between the two deployment methods offered - full details are provided in the deployment guide.

Deployment Process

Two deployment modes are offered for the Darktrace/Apps Microsoft 365 module - the appropriate method will depend on your organizational policies. Selecting a method is described in more detail in Selecting a Deployment Mode for the Microsoft 365 Module.

The default method, for example, can be simplified to:

1. Access the 'Modules' section of the Darktrace System Config page and select Office 365.
2. Provide the domain of the authorizing user and then in the authorization prompt, click the link.
3. Login in with a Global Admin account and grant the requested permissions. Successful authorization will redirect to darktrace.com
4. Return to the System Config page to confirm the setup was successful.