DARKTRACE/CLOUD AZURE 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/Cloud Azure Module provides visibility over Microsoft 365 administration and adds additional coverage over IaaS administration in Microsoft Azure.

Access Management

The Darktrace/Cloud Azure Module provides visibility over management activity and user access handled by Azure AD; Azure Active Directory tracks user activity and sign-in metrics and creates audit log reports that can be retrieved via the Graph API. Data is retrieved directly from the Microsoft Azure audit log endpoint, 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. Typically, the Azure module will provide coverage over:

- Group administration activity including creation, membership and deletion.
- Access control including management of Service Principals, app authorizations and licensing.
- Login activity such as failed logins, successful logins and changes to passwords.

Monitoring is achieved via sets of HTTPS requests made with an authenticated token to the Microsoft Graph API - by default, one set of requests is made every minute. The data retrieved from Azure is organized by Darktrace into categories which appear as metrics in the Threat Visualizer and are available for custom model creation.

Cloud Environment

The Darktrace/Cloud Azure Module also retrieves cloud infrastructure resource creation and management events from Microsoft Azure via reader access to the Azure Activity Log. Returned data and events are limited to those that Azure chooses to record and the data recorded as part of those log entries. There may also be a short delay between the event occurring and the Azure Activity Log entry creation. Typically, the following events will be recorded and fed through to the Threat Visualizer:

- Creation of virtual resources including virtual machines, data factories, virtual networks and Azure websites.
- Modification of resource visibility such as network security group changes, Public IP modification, API account creation and changes to the Front Door service.
- Subscription to and validation of cloud services including containerized services, Blockchain providers, Visual Studio and hosting plan changes.

This information is surfaced in the Darktrace Threat Visualizer as management events only - devices and subnets will not be created for virtual machines or other infrastructure which is seen in the activity log. For visibility over virtual resources at the network level, please discuss deploying Darktrace virtual sensors with your Darktrace representative.

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 Azure 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.

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, 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.

License Requirements

- The module is only available for customers with a "Premium P1" license or above, which grants access to Advanced Security/ Usage Reports.
- Azure only produces user activity audit logs for Microsoft 365 services and features that your organization has licensed.

The module is currently limited to standard Microsoft Azure environments. National Clouds including Azure Government and Azure Germany are not supported.

Permissions

In the default deployment mode, the Azure module requires the following permissions to be granted by a Global Administrator user:

- Read all audit log data
- Read all usage reports
- Read and write all applications
- Read directory data
- Sign in and read user profile

Deployment Process

Two deployment modes are offered for the Darktrace/Cloud Azure Module - the appropriate method will depend on your organizational policies. For most organizations, the default method will be suitable and can be simplified to:

1. Access the 'Modules' section of the Darktrace System Config page and select Azure.
2. 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. Optionally grant the module reader access in the Azure Portal to monitor virtual resources.
5. Return to the System Config page to confirm the setup was successful.

Selecting a method is described in more detail in Selecting a Deployment Mode for the Azure Module.