Darktrace Security Module for AWS

Introduction

Darktrace Security Modules integrate with enterprise SaaS software and Cloud platform solutions to bring visibility and threat analysis to critical systems. Extending Darktrace's Enterprise Immune System defense 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 SaaS and Cloud-based environments, ensuring that user activity is monitored whether it originates inside the network or from remote locations.

aws partner network

Advanced
Technology Partner

How It Works

The Darktrace Security Module for AWS monitors management and administration activity via interaction with AWS CloudTrail. AWS CloudTrail audits Data Events and Management Events which are compiled into logfiles and stored in the AWS S3 bucket created during the configuration process. Data is processed directly from the CloudTrail logfiles, returned information is therefore limited to the events that AWS chooses to audit for each service via CloudTrail and the data recorded as part of each entry. The Darktrace Security Module can monitor AWS services including:

- EC2
- IAM
- S3
- VPC
- Lambda

Full information about AWS services which support CloudTrail monitoring can be found in the relevant AWS documentation. The Security Module does not currently support the monitoring of CloudTrails created via AWS ControlTower.

AWS CloudTrail events are produced up to 15 minutes after activity occurs. In high-traffic environments, the volume of events that must be retrieved in each polling cycle may result in latency between CloudTrail log production and appearance in the Threat Visualizer.

The diverse event types produced by AWS are organized by Darktrace into categories based on the action type and the AWS service that generates it. These categories then appear as metrics in the Darktrace Threat Visualizer which can be used for modeling.

Visualization

Deploying one or more Darktrace Security 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

AWS works on a 'pay-as-you-go' policy for event logging and API calls. Hence there are small charges involved in CloudTrail detecting events, the API request performed by the Darktrace appliance to get these events and storage costs for the event logs. Costs are dependent upon the amount of activity within AWS, the interval between Darktrace polls and any additional configuration settings applied.

Darktrace Security Module for AWS also automatically removes associated log files from S3 a day after they are generated, thereby preventing significant data build up. This setting can be disabled via the System Config page and is not available in *Restricted Mode*.

Delays may be incurred where the SaaS or Cloud platform does not make events available to the Darktrace Security 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.

Write-Only Mode

Write-Only Mode filters CloudTrail to only record AWS "Write" management events, significantly decreasing processing time in busy environments and reducing costs for log storage, API requests made, and number of events recorded. The filter utilizes the "read-only" and "write-only" settings available in AWS CloudTrail - more information can be found in the AWS documentation.

To use this mode, "Automatically Configure CloudTrail" and "CloudTrail Write Event Filter" must be enabled on the Darktrace System Config page.

Permissions

Darktrace Security Module for AWS requires the linked IAM user to have permission to see and modify AWS CloudTrails and have full access to the S3 bucket associated with monitoring. These permissions allow Darktrace Security Module for AWS to access AWS CloudTrail logfiles, reconfigure the CloudTrail if a misconfiguration is detected, and modify the bucket containing logfiles to ensure there is not an increasing buildup of old logs.

The Security Module provides an automatic configuration option - "Automatically Configure CloudTrail" - which allows the module to propagate changes made on the System Config page back to AWS, as well as detect and fix misconfigurations of the associated CloudTrail.

Restricted Mode

The module can be deployed in a restricted mode where the linked IAM user is granted "read" and "list" permissions to the S3 bucket containing the monitoring logs, but is not granted access to CloudTrail.

Please note, this mode prevents the module from detecting misconfigurations, automatically retrieving log location information or managing (deleting) log files.

Deployment Process

The deployment process for Darktrace Security Module for AWS is relatively straightforward and is described in more detail in Deploying Darktrace AWS Security Module. For deployments in *Restricted Mode* or with alternative configuration settings, these steps may differ.

For default configuration, the process outline is:

1. Create a new Trail (in AWS CloudTrail); by default the Trail applies to all regions and outputs all logfiles into an S3 bucket.

2. Create an IAM user that has permission to access and modify the CloudTrail and associated S3 bucket.

3. Input configuration details, such as the new IAM user access keys, into the Darktrace Threat Visualizer configuration page.

After performing these steps, your Darktrace Security Module for AWS will be authorized and begin monitoring events immediately.