Microsoft Defender for Cloud Apps Operational Guide

Abstract

The Operational Guide to help SOC and security teams with planning and performing security activities. Particularly useful for new MDA users.

Microsoft Defender for Cloud Apps
Customer Experience Engineering Team

Table of Contents

Document purpose

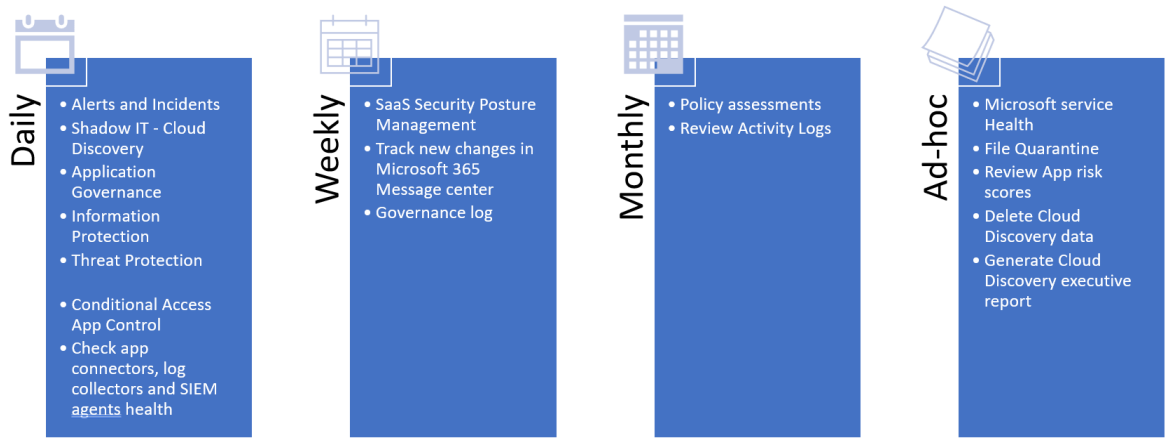
The purpose of the this guide is to help SOC teams and security administrators with planning and performing security activities. This should be particularly useful for new MDA users.

The document assumes that MDA is deployed, if you need help with deployment please review Microsoft Defender for Cloud Apps setup guide and also review MDA Ninja Training.

Microsoft Defender for Cloud Apps (previously known as Microsoft Cloud App Security) is now part of Microsoft 365 Defender. The Microsoft 365 Defender portal allows security admins to perform their security tasks in one location. This will simplify workflows, and add the functionality of the other Microsoft 365 Defender services. Microsoft 365 Defender will be the home for monitoring and managing security across your Microsoft identities, data, devices, apps, and infrastructure. For more information about these changes, see Microsoft Defender for Cloud Apps in Microsoft 365 Defender.

Quick Look:

Activities to protect your cloud environment



Daily Activities to protect your cloud environment

Incidents and Alerts

Why Important: Alerts and Incidents are one of the top items in MDA to be reviewed by Security Operations Team on daily basis. It's important to triage them regularly from the Incidents Queue , prioritising High and Medium severity alerts.

Persona: SOC Analyst

Where: M365 Defender portal > Incidents & Alerts

List of alert types and recommended solutions

Activities to be performed when triaging incidents:

1. View the incident dashboard, filter on:
    - Status: New, In progress
    - Severity: High, Medium, Low
    - Service source: Keep all service sources checked which should be the most fidelity alerts with correlation across different XDR workloads. Select MDA, App Governance to see explicitly what comes from MDA.
2. Select each incident:
    - Review all tabs
    - Use Activity log and Advanced Hunting > In Evidence and Response tab select each evidence, in the burger menu (three dots) select Investigate in Activity log / Go hunt
3. Select **Manage incident**
    1. under **Classification** select "True positive", "False positive" or "Informational, expected activity". For true alerts, specify the threat type. Note: This classification helps your security team see threat patterns and defend your organization from them.
    2. When actively investigated Assign Incident to a person and change status to In Progress.
4. Set an Incident / Alert to In Progress

5. Once the remediated, **resolve the incident**. Resolving the incident resolves all linked and related active alerts.

Incidents: For more information about the Incidents queue, see Prioritize incidents in Microsoft 365 Defender and how to response to the Incidents see Incident response playbooks

***MDI:** If MDI integration is enabled, MDI alerts still need to be triaged in the MDA Portal, please access here for more information.

SIEM: If SIEM integration is enabled, the SIEM solution is normally used first for triaging.

Why Important: It's adding more context via additional logs and offering additional SOAR functionality. Then Microsoft 365 Defender is used if deep understanding of alerts and incident timeline is required.

Persona: Security Administrator

Prerequisites: Microsoft Sentinel integration , Generic SIEM integration, Enabling the Microsoft 365 Defender connector

For bi-directional incidents sync it's recommended enable Microsoft 365 Defender and select Microsoft Defender for Cloud Apps option. Microsoft Sentinel's Microsoft 365 Defender incident integration allows you to stream all Microsoft 365 Defender incidents into Microsoft Sentinel and keep them synchronized between both portals. Incidents from Microsoft 365 Defender include all associated alerts, entities, and relevant information, providing you with enough context to perform triage and preliminary investigation in Microsoft Sentinel. Once in Sentinel, incidents will remain bi-directionally synced with Microsoft 365 Defender, allowing you to take advantage of the benefits of both portals in your incident investigation.

Consider using streaming API - It can be used to send data to an EventHub and then can be consumed through a vendor SIEM connector for instance has an EventHub connector (or placed in Azure Storage).

Additional information: Working with Microsoft 365 Defender incidents in Microsoft Sentinel and bi-directional sync, Streaming API

Persona: SOC Analyst

More information:

Navigate and triage incidents in Microsoft Sentinel

Create custom analytics rules to detect threats

Threat Detection

Why Important: Cloud apps threat detection is one of the main MDA pillars, it's where SOC analysts focus their daily activities, identifying high-risk users showing abnormal behavior. MDA Threat Detection benefits from Microsoft threat intelligence and security research data. The alerts are available in M365D and should be triaged as part of the established process based on recommendations in "Incidents and Alerts" chapter above.

Persona: Security administrators and SOC analysts

Where: M365 Defender portal > Incidents & Alerts

M365 Defender portal > Cloud apps > Policies > Policy management > Threat Detection

M365 Defender portal > Cloud apps > Oauth apps

There are three main types of Threat Detection policies in MDA Security admins and SOC analysts when dealing with alerts will deal with:

- Activity policies
- Anomaly detection policies
- OAuth Policies and App governance policies (depicted in the next chapter)

Persona: Security administrator

Creation and prerequisites of *Threat protection policies*

Application Governance

Where: M365 Defender portal > Incidents & Alerts

M365 Defender portal > Incidents & Alerts / App governance

Why important: App governance offers in-depth visibility and control over OAuth apps registered on Azure Active Directory and helps to combat increasingly sophisticated campaigns that exploit the apps deployed on-premises and cloud infrastructures, establishing a starting point for privilege escalation, lateral movement, and exfiltration of data.

App governance is part of MDA and alerts are also part of M365D Incidents and alerts and should be reviewed as described in the Alerts section. It uses machine learning-based detection algorithms to detect anomalous app behaviour in your Microsoft 365 tenant and generates alerts that you can see, investigate, and resolve. Beyond this built-in detection capability, you can use a set of default policy templates or create your own app policies that generate other alerts.

Persona: SOC analyst

Investigate threat detection alerts and corresponding MITRE ATT&CK tactics

How to Investigate pre-defined app policy alerts

Investigate and remediate risky OAuth apps

Check the Overview page

Where: M365 Defender portal > Incidents & Alerts

M365 Defender portal > Cloud apps > App governance > Overview tab

Why important: Quick assess the compliance posture of the apps and incidents in the tenant.

Persona: SOC analyst and Security administrator

List of checks:

- number of overprivileged, highly privileged apps
- apps with unverified publisher
- data usage for various services and resources that were accessed using Graph API
- number of apps that accessed data with the most common sensitivity labels
- number of apps that accessed data with and without sensitivity labels across Microsoft 365 services
- overview of app governance related incidents

Based on reviewed data create new or adjust app governance policies if required.

View and get detailed information on your Oauth apps

Where: M365 Defender portal > Incidents & Alerts

M365 Defender portal > Cloud apps > App governance > Apps

Why important: Quickly gain deep insights into the Microsoft 365 OAuth apps in your tenant.

Examples:

- A list of OAuth-enabled apps in the tenant, together with relevant app metadata and usage data.
- App details with deeper insights and information by selecting an app in the list.

For more information please go to:

View your apps

Obtain detailed information on an app

Create and manage app policies

Where: M365 Defender portal > Cloud apps > App governance > Policies

Why important: Get in-depth visibility and control over OAuth apps registered on Azure Active Directory. Generate alerts based on machine learning algorithms

Persona: Security administrator

Create app policies in app governance

Manage app policies

Conditional Access App Control

Where: M365 Defender portal > Incidents & Alerts

M365 Defender portal > Cloud apps > Policies > Policy Management > Conditional access

Config: M365 Defender portal> Settings > Cloud apps > Conditional Access App Control

Why important: Conditional Access App Control (CAAP) enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Generated alerts are available in M365D portal and should be triaged as described in the alerts section.

Persona: Security administrator

Out of the box there is no CAAP access nor session policies deployed therefore no related alerts available. Any web app can be onboarded to work with access and session controls, there are number of popular apps that are pre-onboarded, once onboarding completed and first traffic generate, you should be able to create first session and access policies suitable for your environment.

- Access policies
- Session policies

Best practices:

- Block and protect download of sensitive data to unmanaged or risky devices
- Secure collaboration with external users by enforcing real-time session controls

Persona: SOC administrator

- Review alerts in M365D
- Review Activity log – filter out by source, Access control and Session control

Shadow IT- Cloud Discovery

Where: M365 Defender portal > Incidents & Alerts

M365 Defender portal > Cloud apps > Cloud discovery / Cloud app catalog

M365 Defender portal > Cloud apps > Policies > Policy Management > Shadow IT

Why Important: Cloud Discovery analyses your traffic logs against the Microsoft Defender for Cloud Apps catalog of over 31,000 cloud apps. The apps are ranked and scored based on more than 90 risk factors to provide you with ongoing visibility into cloud use, Shadow IT, and the risk Shadow IT poses into your organization.

Alerts related to Cloud Discovery are available in M365D and should be triaged as part of the process described above.

Persona: Security Administrator

Default Cloud Discovery anomaly detection policies have been depreciated. Security administrators need to create app discovery policies to start alerting / tagging newly discovered apps based on certain conditions, risk score, category etc and also app behaviour like daily traffic, downloaded data etc.

Full list of conditions and criteria and details how to create cloud discovery policies can be found here: Create Cloud Discovery policies

Examples of detection Cloud Discovery policies and prerequisites can be found here:
Cloud Discovery policies

Prerequisites: Set up Cloud Discovery

MDE Integration: We are recommending enabling Microsoft Defender for Endpoint integration to allow you to use Cloud Discovery beyond your corporate network or secure gateways and ability to apply governance actions seamlessly on the endpoints (see govern discovered apps chapter).

Best practices: MDE Integration and MDA Shadow IT Discovery

Persona: Security & Compliance Administrator, SOC Analyst

Examples: How to use discovered App Filters and App Queries

Discovered app filters and queries in Microsoft Defender for Cloud Apps - useful when there are large numbers of discovered apps.

Check the dashboard

Where: M365 Defender portal > Cloud apps > Cloud discovery > Dashboard

Why Important: In addition to alerts Cloud discovery dashboard should be reviewed on daily basis. It is designed to give you more insight into how cloud apps are being used in your organization. It provides an at-a-glance overview of what kinds of apps are being used, your open alerts, the risk levels of apps in your organization.

Persona: Security & Compliance Administrator, SOC Analyst

1. First look at the overall cloud app use in your organization in the High-level usage overview.
2. Use filtering to generate specific views depending on your interest
3. Then, dive one level deeper to see which are the top categories used in your org for each of the different use parameters. You can see how much of this usage is by Sanction apps.
4. Go even deeper and see all the apps in a specific category in the Discovered apps tab.
5. You can see the top users and source IP addresses to identify which users are the most dominant users of cloud apps in your organization.
6. Check how the discovered apps spread according to geographic location (according to their HQ) in the App Headquarters map.
7. Review the risk score of the discovered app in the App risk overview.
8. Check the discovery alerts status to see how many open alerts should you investigate.

Full information: Working with discovery data

Working with discovered apps

Govern discovered apps

Where: M365 Defender portal > Cloud apps > Cloud discovery > Dashboard

Why Important: After you've reviewed the list of discovered apps in your environment, you should secure your environment by approving safe apps (Sanctioned) or prohibiting unwanted apps (Unsanctioned) or apply custom tags.

Persona: Security & Compliance Administrator

You can also proactively review and apply tags to the apps available in Cloud app catalog before they are discovered in your environment. To help you with governing those applications, relevant cloud discovery policies can be created triggered by specific tags. This activity can be performed on ad hoc or regularly

Please note that depending on cloud Discovery integration implemented in your environment, you may benefit from seamless and automated blocking or even “warn and educate” capabilities provided by Microsoft Defender for Endpoint.

Best practices:

Govern discovered apps using Microsoft Defender for Endpoint

Apply cloud governance policies

Information Protection

Where: M365 Defender portal > Incidents & Alerts

M365 Defender portal > Cloud apps > Files

M365 Defender portal > Cloud apps > Policies > Policy Management > Information Protection

Why Important: Defender for Cloud Apps file policies and alerts allow you to enforce a wide range of automated processes. Policies can be set to provide information protection, including continuous compliance scans, legal eDiscovery tasks, and DLP for sensitive content shared publicly. Alerts should be triaged as per process described earlier in the Alerts section.

Persona: Security & Compliance Administrator, SOC Analyst

In addition to acting on existing File Policies alerts, SOC teams can perform additional pro active actions and run queries in the Files section to check the following:

- How many files are shared publicly so that anyone can access them without a link?
- With which partners are you sharing files (outbound sharing)?
- Do any files have a sensitive name?
- Are any of the files being shared with someone's personal account?

Based on the results existing file policies can be adjusted or new policies deployed.

Examples of Detections with Information Protection policies: Information protection policies

Weekly Activities to protect your cloud environment

SaaS Security Posture Management

Where: M365 Defender portal > Secure Score

Why Important: SaaS Security Posture Management capabilities in Microsoft Defender for Cloud Apps enable you to get deeper visibility and automatically identify SaaS apps misconfigurations, and help you remediate them to improve your organizational security. This experience is integrated into the Microsoft 365 Defender dashboard to enable security teams to see their holistic security posture across the enterprise with Microsoft Secure Score.

Persona: Security & Compliance Administrator, SOC Analyst

Tip: For best high level overview of list of actions per product, go to Secure Score and select Recommended actions and select group by in the right corner and select Product

Check app connectors, log collectors and SIEM agents health

Where: M365 Defender portal > Settings > Cloud apps

Persona: Security & Compliance Administrator, SOC Analyst

Why Important: System alerts are special type of alerts raised when connector, agent or log collector fails, it's not possible to send a notification to an administrator in MDA portal. It's important to check health of your app connectors, log collectors and SIEM agents

If SIEM agent is used, System alerts can be injected go to M365D settings > System >SIEM Agents and Configure SIEM agent. In Data Types section select Alerts, make sure Alert type filter contain system alerts.

It's recommended to review status of:

- App connectors
    - Settings > Cloud apps > Connected apps > App Connectors
- Conditional Access App control Apps
    - Settings > Cloud apps > Connected apps > CAAP
- Automatic log upload
    - Settings > Cloud apps > Cloud Discovery > Automatic log upload
- API tokens
    - Settings > Cloud apps > System > API tokens

Track new changes in Microsoft 365 Message center

Where: M365 admin center > Health > Message center

Why Important: Message center helps you to keep track of upcoming changes, including new features, planned maintenance, or other important announcements that may affect your MDA environment.

Persona: Security administrator

More information: Track new and changed features in the Microsoft 365 Message center.

Governance log

Why Important: The Governance log provides a status record of each task that you set Defender for Cloud Apps to run, including both manual and automatic tasks. These tasks include those you set in policies, governance actions that you set on files and users, and any other action you set Defender for Cloud Apps to take.

Where: M365 Defender portal > Cloud apps > Governance log

Persona: Security and Compliance administrator

More information: Full list of Governance log

Monthly Activities to protect your cloud environment

Monthly activities can be performed more frequently or as needed, depending on your environment and needs.

Policy assessments

Why Important: Review the policies and make any necessary updates to ensure they are still appropriate for your organization.

Where: M365 Defender portal > Cloud apps > Policy management

Persona: Security and Compliance administrator

- Check for and false positive / benign true positive rates: adjust policies where rates is too high:
    - Example: ensure that any new corp IP is properly filled up in MDA settings to avoid Impossible travel False Positive.
- Review business needs and assess requirement for custom policies
    - Example: is the threat detected by this policy still relevant? Or is there a new built in solution to detect that threat?
- Clear old alerts
    - Example: select alerts time 6 months, filter out alerts with resolved status, group similar alerts and verify why they were not attended, if they are benign and can be dismissed and policies adjusted

Review Activity Logs

Why Important: Activity logs are frequently reviewed in relation to alerts and are part of threat investigation. Additionally it's beneficial to re-visit the Activity log after certain period of time and look from the time perspective for repeated activities by an entity like multiple searches or log on by a user. Pivot results by activity type for example failed log on, deletion or privilege assignment. Then narrow down activity to an app or a user. Based on the results you may create a new policy which will help with closer monitor and respond to potential threat.

Where: M365 Defender portal > Cloud apps > Activity log

Persona: Security and Compliance administrator

Ad-hoc Activities

Microsoft Service Health

Why Important: If you are experiencing problems with a cloud service, please check the service health to determine whether this is a known issue with a resolution in progress before you call support or spend time troubleshooting.

Where: M365 admin center > Health > Service health

Microsoft 365 Service health status (office365.com)

Twitter: @MSFT365status

Advanced Hunting

Why Important: Similar to reviewing activity logs, Advanced Hunting can be used as a scheduled activity, ability to create custom detections or ad-hoc to proactively hunt for threats. Advanced Hunting is a unified tool that allows you to hunt for threats across M365D. It's a good practice to save frequently used queries for faster manual threat hunting and remediation. Heare are a couple of examples of AH queries for MDA:

Persona: SOC analyst

Where: M365 Defender portal > Hunting > Advanced hunting

Office - FileDownloaded Events

```
CloudAppEvents
| where ActionType == "FileDownloaded"
| extend FileName = RawEventData.SourceFileName, Site = RawEventData.SiteUrl,
FileLabel = RawEventData.SensitivityLabelId, SiteLabel =
RawEventData.SiteSensitivityLabelId
| project
Timestamp,AccountObjectId,ActionType,Application,FileName,Site,FileLabel,SiteL
abel
```

Office - MailItemsAccessed Details

```
CloudAppEvents
| where ActionType == "MailItemsAccessed" //Defines the action type we want to
filter on
```

```
| extend Folders = RawEventData.Folders[0] //Set variable and then use the
index to trim the [] to data can be accessed
| extend MailboxPath = Folders.Path //set a variable for the path
| mv-expand Folders.FolderItems //expand the list of items because some
entries might contain multiple items which were accessed
| extend MessageIDs = tostring(Folders_FolderItems.InternetMessageId) //extend
and then convert to string so table can be joined
| join EmailEvents on $left.MessageIDs == $right.InternetMessageId //join the
email events table to access subject and mailbox information
| project
Timestamp,AccountType,AccountDisplayName,AccountObjectId,UserAgent,IPAddress,C
ountryCode,City,ISP,NetworkMessageId,MailboxPath,Subject,SenderFromAddress,Rec
ipientEmailAddress
| sort by Timestamp desc
```

Extract activity objects

```
CloudAppEvents
| take 100
| mv-expand(ActivityObjects)
| evaluate bag_unpack(ActivityObjects)
```

AAD - Add to Role

```
CloudAppEvents
| where ActionType in ("Add member to role.")
| extend FirstElement = ActivityObjects[0], SecondElement =
ActivityObjects[1], ThirdElement = ActivityObjects[2]
| extend Type = FirstElement.ServiceObjectType,
    RoleName = FirstElement.Name,
    UserAddedName = SecondElement.Name,
    UserAddedId = SecondElement.Id
| project
Timestamp,Type,ActionType,RoleName,UserAddedName,UserAddedId,AccountId,Account
DisplayName
```

AAD - Group Adds

```
CloudAppEvents
| where ActionType in ("Add member to group.") and AccountType == "Regular"
| extend SecondElement = RawEventData.ModifiedProperties[1]
| extend UserAddedId = RawEventData.ObjectId, GroupName =
SecondElement.NewValue
| project Timestamp, ActionType,UserAddedId,PerformedBy =
AccountDisplayName,GroupName
```

File Quarantine

Why Important: Microsoft Defender for Cloud Apps can be used to detect unwanted files stored in your cloud that leave you vulnerable, and take immediate action to stop them in their tracks and lock down the files that pose a threat by using Admin quarantine to protect your files in the cloud, remediate problems, and prevent future leaks from occurring. Files in Admin quarantine can be reviewed as part of alert investigation. For governance and compliance reasons you may be required to manage quarantined files.

Where: M365 Defender portal > Cloud apps > Files

Query: *Quarantined is True*

Persona: Compliance administrator

More information: Understand how quarantine works

Review App risk scores

Why Important: The Cloud app catalog rates risk for your cloud apps based on regulatory certification, industry standards, and best practices. It's recommended to review the score for each of the application in your environment to make sure it's aligned with your company regulations. You may submit a request to change an app risk score. You can also customize the risk score in Cloud Discovery > Score metrics.

Persona: Compliance administrator

Where: M365 Defender portal > Cloud apps > Cloud app catalog

More information: Working with the risk score

Delete Cloud Discovery data

Why Important: There are a number of reasons why you may want to delete your Cloud Discovery data. We recommend deleting it in the following cases:

- If you manually uploaded log files and a long time passed before you updated the system with new log files and you don't want old data affecting your results.
- When you set a new custom data view, it will apply only to new data from that point forward. So, you may want to erase old data and then upload your log files again to enable the custom data view to pick up events in the log file data.
- If many users or IP addresses recently started working again after being offline for some time, their activity will be identified as anomalous and may give you false positive violations.

Persona: Compliance administrator

Where: M365 Defender portal > Settings > Cloud apps > Cloud Discovery > Delete Data

More information: Deleting Cloud Discovery data

Generate Cloud Discovery executive report

Why Important: The best way to get an overview of Shadow IT use across your organization is by generating a Cloud Discovery executive report. This report identifies the top potential risks and helps you plan a workflow to mitigate and manage risks until they're resolved.

Where: M365 Defender portal > Cloud apps > Cloud discovery > Dashboard > Actions

Persona: Compliance administrator

More information: Generate Cloud Discovery executive report

Create Cloud Discovery snapshot report

Why Important: If you don't have a log yet and you want to see an example of what your log should look like, download a sample log file.

Where: M365 Defender portal > Cloud apps > Cloud discovery > Dashboard > Actions

Persona: Security and Compliance administrator

More information: Create snapshot Cloud Discovery reports