News Incident response Microsoft Entra

5 min read

# New Microsoft Incident Response guides help security teams analyze suspicious activity

By Microsoft Incident Response

January 17, 2024

Microsoft Entra ID

Microsoft Incident Response

Microsoft Security Experts

Microsoft 365

Today Microsoft Incident Response are proud to introduce two one-page guides to help security teams investigate suspicious activity in Microsoft 365 and Microsoft Entra. These guides contain the artifacts that Microsoft Incident Response hunts for and uses daily to provide our customers with evidence of Threat Actor activity in their tenant.

With more than 3,000 different activities (also known as operations) logged into the Microsoft 365 suite, knowing which are useful for your investigation can be daunting. With these guides, our goal is to make triaging and analyzing data in Microsoft 365 simpler. Many of these operations are data-based storytelling vehicles, helping Microsoft Incident Response to piece together an attack chain from beginning to end. We have worked on hundreds of cloud-centric cases with our customers, and while tactics, techniques, and procedures (TTPs) change with the times, analysis methodology and data triage techniques remain consistently successful. To enable Microsoft Incident Response to find ground truth quickly and effectively in an investigation, data mining based on known factors is essential. The known factors could be investigation specific, such as an IP address, known compromised username, or suspicious user agent string. It is also just as important to filter based on how actors move through a cloud environment and gather data. This is where these guides come into their own, and our hope is that sharing these guides can help you in the same way they help us every day.

## Microsoft Incident Response guides

These new one-page guides from Microsoft Incident Response helps security teams analyze cyberthreat data in Microsoft 365 and Microsoft Entra.

Download the guides

## Analyze the Unified Audit Log in Microsoft 365

First up is our general Microsoft 365 guide, centered around key activities in Exchange Online and SharePoint—Microsoft 365 products commonly targeted in cybersecurity attacks. Keep in mind that the motives of a Threat Actor, the tools available to them, and the level of access they have achieved will determine the actions they take. No two incidents are ever the same.

Actions carried out in a tenant are recorded in the Unified Audit Log, which can be accessed from the Security Portal or through PowerShell. You can filter the audit log by date, user, activity, IP address, or file name. You can also export the audit log to a CSV file for further analysis.

Most of the operations in these sheets are self-explanatory in nature, but a few deserve further context:

**SearchQueryPerformed**—A user or an administrator has performed a search query in SharePoint Online or OneDrive for Business. This operation returns information about a search query performed in SharePoint Online, including the query text used. Keep in mind that interacting with certain components of SharePoint will trigger background 'searches.'

**SearchQueryInitiatedSharePoint and SearchQueryInitiatedExchange**—These operations are only logged if you have enabled them using the Set-Mailbox PowerShell cmdlet. This operation is much like SearchQueryPerformed, but applies to mailbox-level searches.

**SearchExportDownloaded**—A report was downloaded of the results from a content search in Microsoft 365. This operation returns information about the content search, such as the name, status, start time, and end time.

**Update**—A message item was updated, including metadata. One example of this is when an email attachment is opened, which updates the metadata of the message item and generates this event. An update operation is not always indicative of an email message being purposefully modified by a Threat Actor.

**FileSyncDownloadedFull**—User establishes a sync relationship and successfully downloads files for the first time to their computer from a SharePoint or OneDrive for Business document library.

## Detailed identity and access data with Microsoft Entra

Our Microsoft Entra guide covers actions which allow organizations to manage and protect their identities, data, and devices in the cloud. As an industry-leading identity platform, Microsoft Entra ID offers advanced security features, such as multifactor authentication, Conditional Access policies, identity protection, privileged access management, and identity governance.

To view the activities performed by users and administrators in Microsoft Entra ID, you can use the Microsoft Entra ID audit log, which stores events related to role management, device registration, and directory synchronization to name a few. To view detailed sign-in information, you can use the Sign-In Logs. The events located in these two data sources can help you detect and investigate security incidents, such as unauthorized access or configuration changes to the identity plane.

You can use the following methods to access Microsoft Entra ID audit log data:

**Microsoft Entra Admin Portal**—Go to the portal and sign in as an administrator. Navigate to Audit and/or Sign-ins under Monitoring. Filter, sort, and export the data as needed.

**Graph PowerShell**—Install the Graph PowerShell module and connect to Microsoft Entra ID. Use Get-MgAuditLogDirectoryAudit and/or Get-MgAuditLogSignIn to get the data you need.

**Microsoft Graph API**—Register an application in Microsoft Entra ID and give it the permissions to read audit log data (AuditLog.Read.All and Directory.Read.All). Use /auditLogs/directoryAudits and /auditLogs/signIns API endpoints to query the data, along with query parameters such as $filter to refine the results.

Most of the operations in these sheets are self-explanatory in nature, but as with our Microsoft 365 operations, a few deserve further context:

**Suspicious activity reported**—This log event indicates that a user or an administrator has reported a sign-in attempt as suspicious. The log event contains information about the reported sign-in—such as the user, the IP address, the device, the browser, the location, and the risk level. It also shows the status of the report—whether it was confirmed, dismissed, or ignored by the user or the administrator. This log event can help identify potential security incidents, including phishing, credential compromise, or malicious insiders.

**Update application: Certificates and secrets management**—This log event indicates that an administrator has updated the certificates or secrets associated with an application registered in Microsoft Entra ID—such as creation, deletion, expiration, or renewal. Applications are frequently misused by Threat Actors to gain access to data, making this a critical administrative event if found during an investigation.

**Any operation ending in '(bulk)'**—These are interesting as they demonstrate a bulk activity being performed—such as 'Download users' or 'Delete users.' Keep in mind, however, that these are only logged if the bulk activity is performed using the graphical user interface. If PowerShell is used, you will not see these entries in your log.

**Elevate Access**—Assigns the currently logged-in identity the User Access Administrator role in Azure Role-Based Access Control at root scope (/). This grants permissions to assign roles in all Azure subscriptions and management groups associated with the Microsoft Entra directory. This toggle is only available to users who are assigned the Global Administrator role in Microsoft Entra ID. It can be used by Threat Actors to gain complete control of Azure resources, often for the purposes of crypto mining or lateral movement from cloud to on-premises.

## Improve security analysis with the Microsoft Incident Response guides

We hope that these one-page guides will be a valuable resource for you when you need to quickly identify and analyze suspicious or malicious activity in Microsoft 365 and Microsoft Entra ID. Print them out, save them as your desktop background, or put them on a mouse pad. Whatever you do, let us know what you find useful and remember that the audit logs in Microsoft 365 and Microsoft Entra ID are not the only source of evidence in a cloud-based case, and you should always correlate and validate your findings with other data sources where possible.

To access further information on what data lies in these logs and how you can access them, reference the following blog posts from the Microsoft Incident Response team:

- Forensic artifacts in Office 365 and where to find them—Microsoft Community Hub.
- Good UAL Hunting—Microsoft Community Hub.

## Learn more

Learn more about Microsoft Incident Response.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and Twitter (@MSFTSecurity) for the latest news and updates on cybersecurity.

## Related Posts

A security practitioner works at a computer.

News

Endpoint security

Microsoft Intune

**Feb 1**
**8 min read**

### 3 new ways the Microsoft Intune Suite offers security, simplification, and savings

The main components of the Microsoft Intune Suite are now generally available. Read about how consolidated endpoint management adds value and functionality for security teams.

Engaged developer in focused work in the context of automation in manufacturing to build intelligent apps powered by Azure.

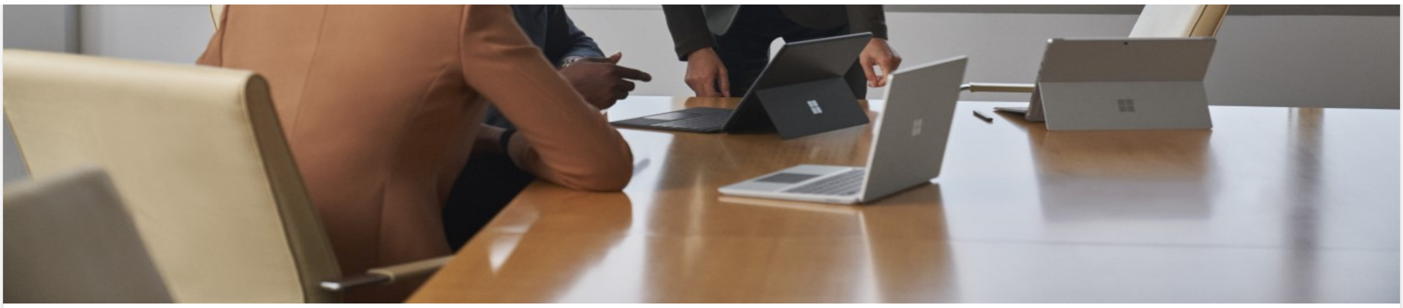
Industry trends

Microsoft Intune

**Jan 29**
**<1 minute read**

### Best practices in moving to cloud native endpoint management

This blog is the second of three that details our recommendation to adopt cloud native device management. Understand the lessons from various Intune customers in their journeys and how they achieved greater security, cost savings, and readiness for the future through their cloud transformations.

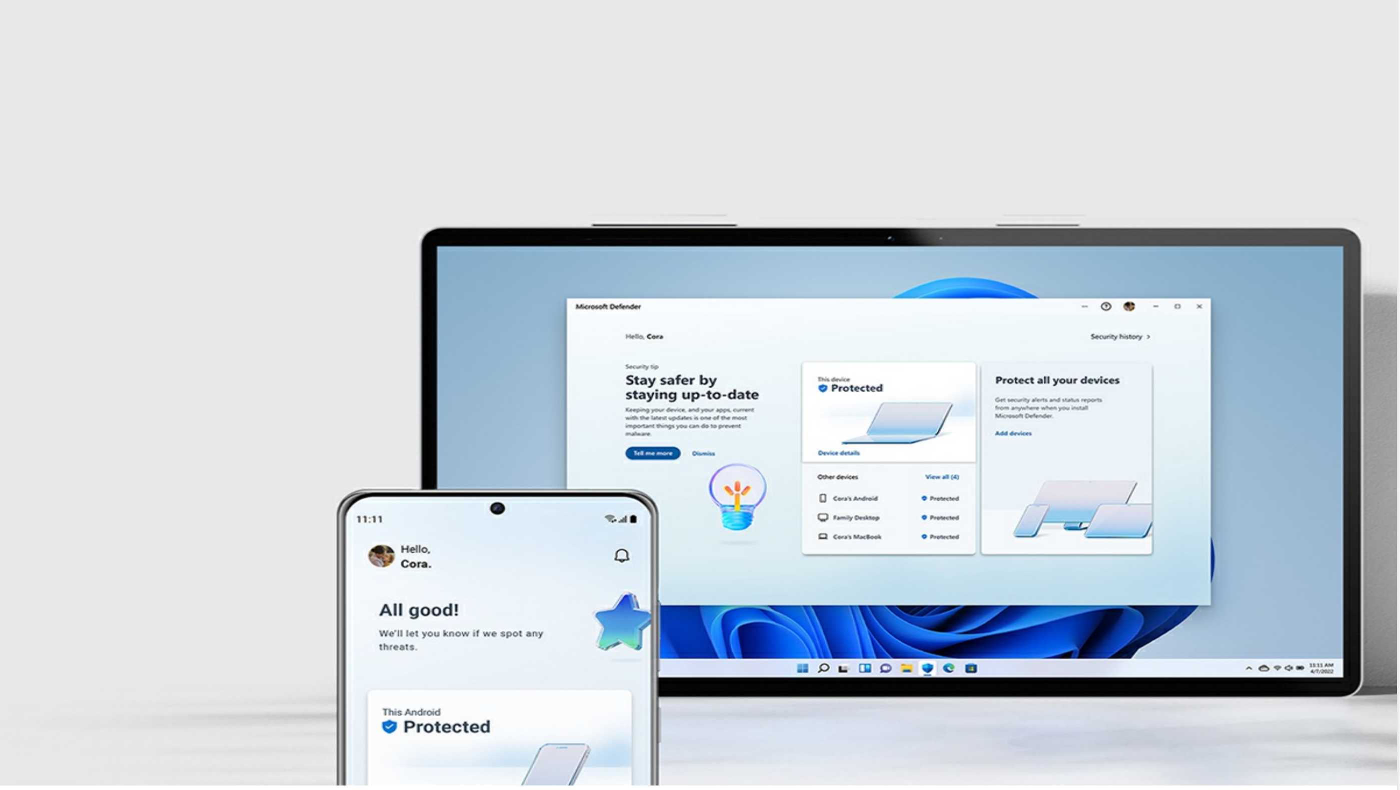


[News](#)
[Analyst reports](#)
[Microsoft Defender](#)

**Jun 22**
**2 min read**

## Microsoft Defender for Office 365 receives highest award in SE Labs Enterprise Email Security Services test

Microsoft received an AAA Protection Award for Microsoft Defender for Office 365, the highest possible award that vendors can achieve in this test.



[News](#)
[Cloud security](#)
[Microsoft Defender](#)

**Jun 16**
**3 min read**

## Making the world a safer place with Microsoft Defender for individuals

Microsoft Defender for individuals helps people keep their families safer online with simplified cybersecurity and cross-platform online protection.

## Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

### What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

### Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

### Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

## Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

## Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

## Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads