

# Next generation Microsoft 365 Logging: Exploring new features

SANS Webcast

KORSTIAAN STAM

## About me

---



- SANS Instructor FOR509: Enterprise Cloud Forensics and Incident Response
- Founder & CEO Invictus Incident Response B.V.
- Previous IR positions at PwC and Northwave Cybersecurity
- Open-source developer
  - Microsoft-Extractor-Suite
- Parttime teacher at Amsterdam University of Applied science
- Most importantly cloud incident response enthusiast!

# Topics

## 1 Background

Let's talk about how we got to this point and the necessity of improvements

## 2 Recent changes

A lot has happened recently, this is the TLDR

## 3 The Present

What is the status of auditing in Microsoft 365 and Entra ID for investigations

## 4 The Future

What do we have to look forward to and how long do we have to wait

## 5 Takeaways

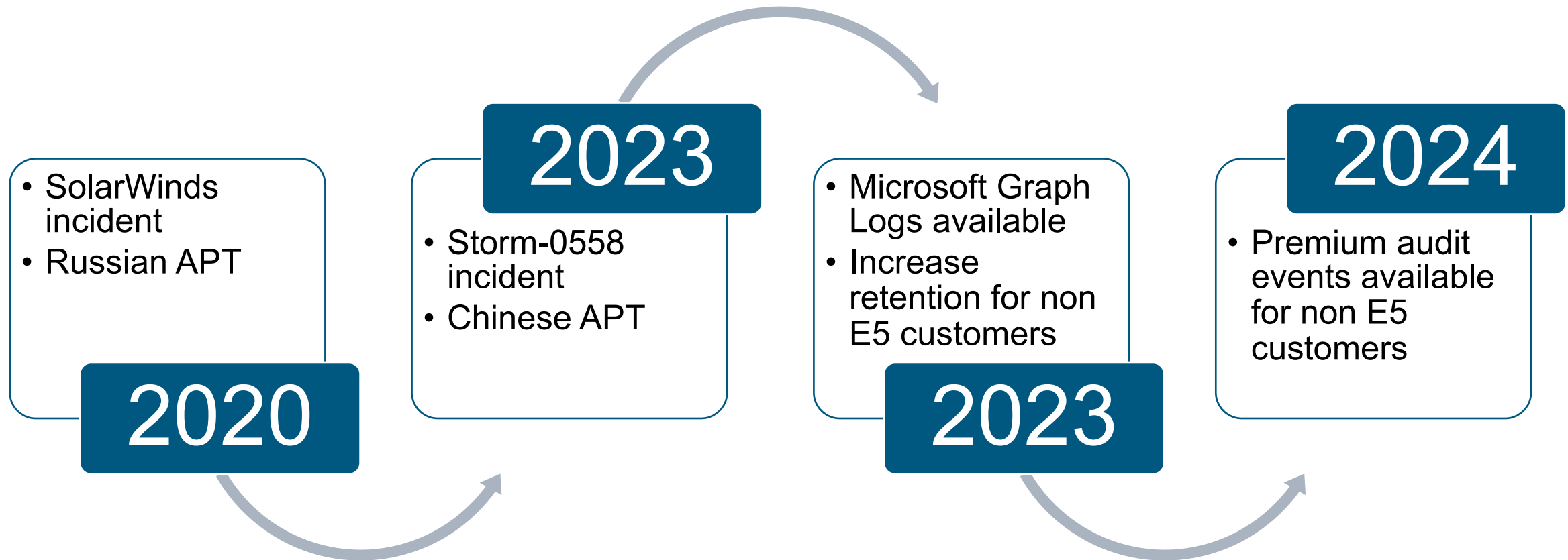
## 6 Q&A

# Background

Some context on the why of this talk



## Background





# Background

---

## PUBLICATION

# Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023

## 2.1.3 AUDIT LOGGING NORMS

Logging is essential to detection, investigation, and remediation of potential intrusions. In this case, the logs State Department used to detect this incident (MailItemsAccessed) are of critical value and have enabled detection of other nation-state compromises involving Exchange Online. Despite this obvious utility, these logs, and similar logs at other CSPs, are not available for all types of critical business data stored by CSPs. The Board recommends the following.

- **RECOMMENDATION 10:** CSPs, as part of a CISA-led task force, should define and adopt a minimum standard for default audit logging in cloud services. This standard should, at a minimum, ensure that all access (including access by the CSP itself) to customer business data in the cloud produces logs that are available to the customer without additional charges, with a minimum default retention of six months by the CSP.
-

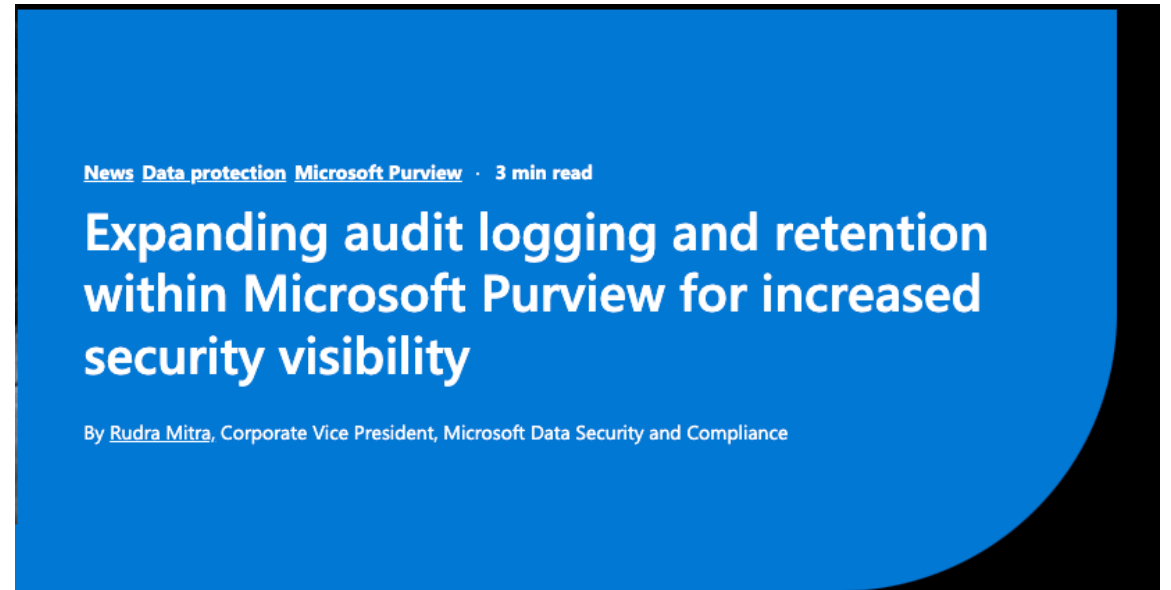
# Recent changes

What has changed?



## Recent changes

- **Microsoft made a commitment to:**
  - Increase retention
  - Additional logs for non-premium users
  - Programmatic access via Graph API
  - Improve searching for audit logs in Purview (GUI)
  - Customized retention policies
- **Other (not transparent):**
  - Higher bandwidth API access
  - Enriched logs by Microsoft AI



Source: <https://www.microsoft.com/en-us/security/blog/2023/10/18/expanding-audit-logging-and-retention-within-microsoft-purview-for-increased-security-visibility/>



## Status

---

### Increased retention

Implemented  
October 2023

### Graph API access

Currently in preview  
May 2024

### Premium events

In development  
June 2024

## Recent changes - Increased retention



### Get-AdminAuditLog

```
PS /Users/korstiaan> Get-AdminAuditLogConfig

AdminAuditLogEnabled      : True
LogLevel                  : None
TestCmdletLoggingEnabled  : False
AdminAuditLogCmdlets      : {*}
AdminAuditLogParameters   : {*}
AdminAuditLogExcludedCmdlets : {}
AdminAuditLogAgeLimit     : 90.00:00:00
LoadBalancerCount         : 3
RefreshInterval           : 10
PartitionInfo             : {}
AdminAuditLogMailbox      :
UnifiedAuditLogIngestionEnabled : True
UnifiedAuditLogFirstOptInDate : 05/06/2023 17:09:58
AdminDisplayName          :
ExchangeVersion           : 0.10 (14.0.100.0)
Name                      : Admin Audit Log Settings
DistinguishedName         : CN=Admin Audit Log Settings,CN=Global Settings,
Identity                  : Admin Audit Log Settings
ObjectCategory            : EURPR05A013.PROD.OUTLOOK.COM/Configuration/Sche
ObjectClass               : {top, msExchAdminAuditLogConfig}
WhenChanged               : 05/06/2023 19:10:12
WhenCreated               : 03/02/2023 16:23:39
WhenChangedUTC            : 05/06/2023 17:10:12
WhenCreatedUTC            : 03/02/2023 15:23:39
ExchangeObjectId          : c40bb749-7a73-4eb7-a41b-115fadd0c4c1
OrganizationalUnitRoot    : invictusir.onmicrosoft.com
OrganizationId            : EURPR05A013.PROD.OUTLOOK.COM/Microsoft Exchange
Id                        : Admin Audit Log Settings
Guid                     : c40bb749-7a73-4eb7-a41b-115fadd0c4c1
OriginatingServer         : PA6PR05A13DC004.EURPR05A013.PROD.OUTLOOK.COM
IsValid                   : True
ObjectState               : Changed
```

## Recent changes – Increased retention

---

```
PS /Users/korstiaan> (Get-Date).AddDays(-90)
```

```
Monday, 5 February 2024 13:29:51
```

```
PS /Users/korstiaan> (Get-Date).AddDays(-180)
```

```
Tuesday, 7 November 2023 13:29:54
```

```
PS /Users/korstiaan> Search-UnifiedAuditLog -StartDate 07-11-2023 -EndDate 01-12-2023 |Select-Object ResultCount -First 1
```

```
ResultCount
```

```
-----
```

```
20802
```

# Recent changes - Premium events

## Premium events



What are premium events?



Why do we care about them?

## Overview

### Exchange

Send, MailItemsAccessed, SearchQueryInitiatedExchange

### SharePoint Online

SearchQueryInitiatedSharePoint

### Stream

StreamInvokeGetTranscript, streamInvokeChannelView, StreamInvokeGetTextTrack, StreamInvokeGetVideo, StreamInvokeGroupView

### Microsoft Teams

MeetingParticipantDetail, MessageSent, MessagesListed, MeetingDetail, MessageUpdated, ChatRetrieved, MessageRead, MessageHostedContentRead, SubscribedToMessages, MessageHostedContentsListed, ChatCreated, ChatUpdated, MessageCreatedNotification, MessageDeletedNotification, MessageUpdatedNotification

### Microsoft Viva Engage

ThreadViewed, ThredAccessFailure, MessageUpdated, FileAccessFailure, MessageCreation, GroupAccessFailure

# My top 4

Ranking of the most useful premium events from an IR perspective

## Table of Contents

PAGE

Operation	Reason
MailItemsAccessed	Who or what accessed an email or folder
SearchQueryInitiatedSharePoint	Find insiders and threat actors searching through your SharePoint/OneDrive
SearchQueryInitiatedExchange	What search queries were ran against a mailbox works for all clients
ChatCreated	Who is creating a chat, especially interesting with external participants (e.g. Teams phishing)



## Recent changes – Graph API

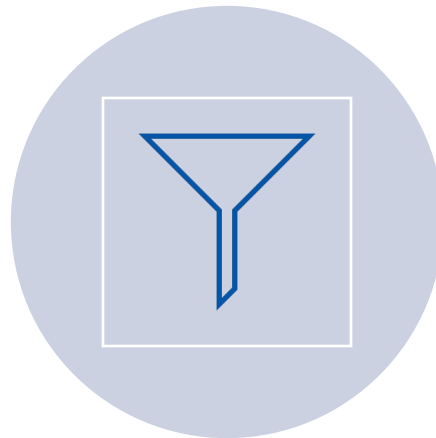
---

### Topics

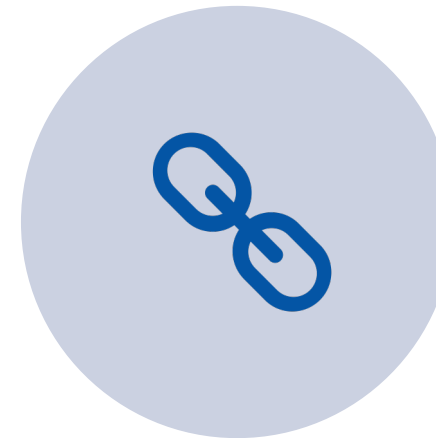
---



WHAT IS THE GRAPH  
API



CURRENT EXPORT  
OPTIONS



HOW TO CONNECT?

# What is the Graph API

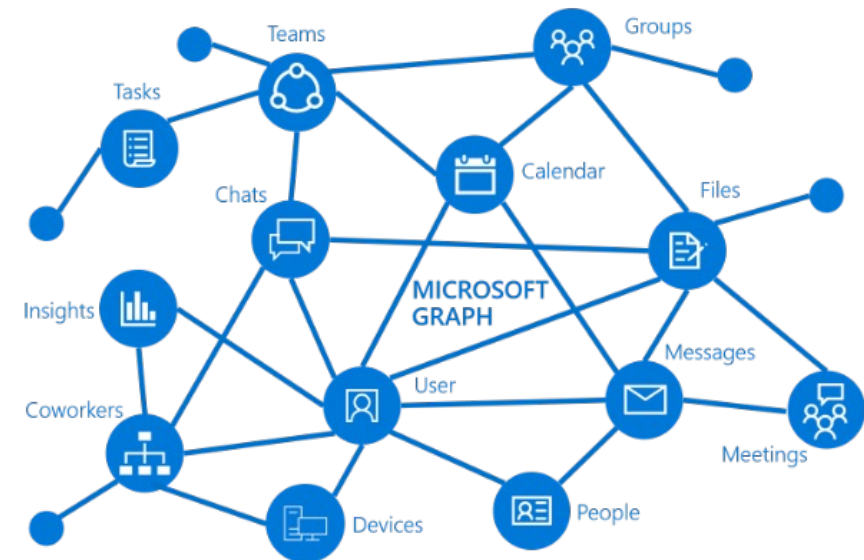
*“Microsoft Graph is the gateway to data and intelligence in Microsoft 365. It provides a unified programmability model that you can use to access the tremendous amount of data in Microsoft 365, Windows, and Enterprise Mobility + Security. Use the wealth of data accessible through Microsoft Graph to build apps for organizations and consumers that interact with millions of users.”*

My interpretation:

The location where **all\*** relevant data for a Microsoft 365 tenant can be accessed, very powerful for us as investigators.

\* Not everything is there yet

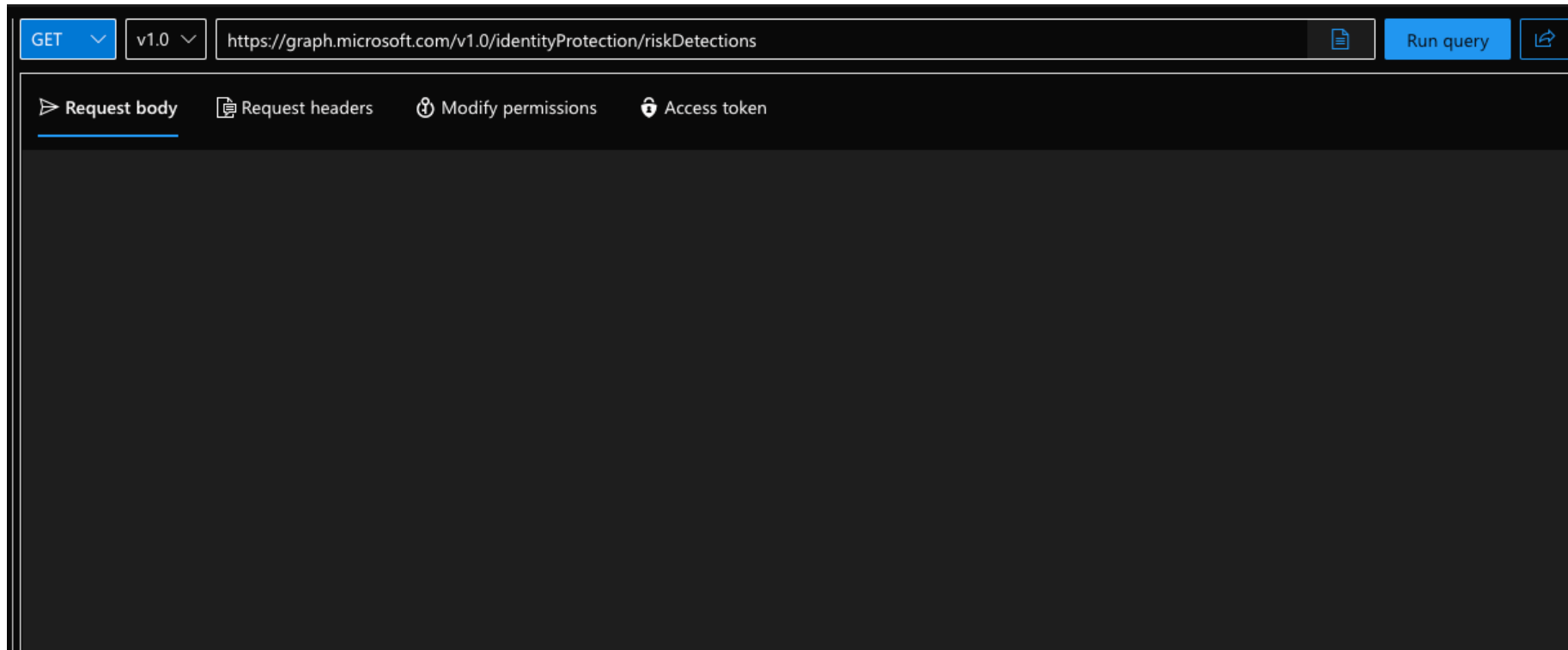
\*\* Also there's other API's that attackers use



Source: <https://learn.microsoft.com/en-us/graph/overview>

# Graph Explorer

Never used the Graph API before or intimidated by all information that is out there? Try the Microsoft Graph Explorer: <https://developer.microsoft.com/en-us/graph/graph-explorer>



Live demo

## Unified Audit Log – Current export options

---

### Compliance (GUI)

---

- Useful for quick checks and IOC searches
- Slow to search large datasets
- Export limitations

### PowerShell

---

- Useful to grab all data
- Slow because of 5k records per call
- Limited filtering options
- Not very analysis friendly

### Management API

---

- Setup can be challenging
- Limited history (7 days)
- Blazing fast

## Graph API – The solution to all problems?

Enter the auditLogQuery API

- Currently in beta
- Offers 4 methods to interact with the auditlogs (UAL)
- It's integrated with Purview (e.g. launching a query via API will show the search in Purview and vice-versa)

Method	Description
<a href="#">List auditLogQueries</a>	Get a list of the <a href="#">auditLogQuery</a> objects and their properties.
<a href="#">Create auditLogQuery</a>	Create a new <a href="#">auditLogQuery</a> object.
<a href="#">Get auditLogQuery</a>	Read the properties and relationships of a <a href="#">auditLogQuery</a> object.
<a href="#">List records</a>	Get the auditLogRecord resources from the records navigation property.



## Graph API – How to connect

---

1

Create an app  
with the right  
permissions

2

Create a  
secret/certificate

3

Connect to the  
Graph

4

Call the  
auditLogQuery  
API directly or;




5



Use the  
Microsoft-  
Extractor-Suite


# Graph API – Permissions


Permission	Admin consent required
▼ AuditLogsQuery-CRM	
<input type="checkbox"/> AuditLogsQuery-CRM.Read.All ⓘ Read audit logs data from Dynamics CRM workload	Yes
▼ AuditLogsQuery-Endpoint	
<input type="checkbox"/> AuditLogsQuery-Endpoint.Read.All ⓘ Read audit logs data from Endpoint Data Loss Prevention workload	Yes
▼ AuditLogsQuery-Entra	
<input type="checkbox"/> AuditLogsQuery-Entra.Read.All ⓘ Read audit logs data from Entra (Azure AD) workload	Yes
▼ AuditLogsQuery-Exchange	
<input type="checkbox"/> AuditLogsQuery-Exchange.Read.All ⓘ Read audit logs data from Exchange workload	Yes
▼ AuditLogsQuery-OneDrive	
<input type="checkbox"/> AuditLogsQuery-OneDrive.Read.All ⓘ Read audit logs data from OneDrive workload	Yes
▼ AuditLogsQuery-SharePoint	
<input type="checkbox"/> AuditLogsQuery-SharePoint.Read.All ⓘ Read audit logs data from SharePoint workload	Yes
▼ AuditLogsQuery	
<input type="checkbox"/> AuditLogsQuery.Read.All ⓘ Read audit logs data from all services	Yes


# This is what it should look like

 **Graph-APP-for-log-acquisition | API permissions**  


<<  Refresh |  Got feedback?


 Overview


 Quickstart


 Integration assistant


**Manage**


 Branding & properties


 Authentication


 Certificates & secrets


 Token configuration


 **API permissions**


 Expose an API


 App roles

 Owners

 Roles and administrators



 Manifest






 Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. [Learn more](#)

 The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

### Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

 Add a permission  Grant admin consent for invictus-ir.com

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (2) 				
<a href="#">AuditLogsQuery.Read.All</a>	Application	Read audit logs data from all services	Yes	 Granted for invictus-ir.c... 
<a href="#">User.Read</a>	Delegated	Sign in and read user profile	No	 Granted for invictus-ir.c... 

## Graph API – Secret/Certificate

- When using a secret make sure you store the Value

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

Description	Expires	Value ⓘ	Secret ID
secret-for-demo	8/6/2024	muZ*****	0de13326-9155-4417-a3e6-f568c9a62b52  

## Graph API – Time to connect

---

### Configure the following variables in PowerShell

```
$ClientId = "ID-of-your-app"
```

```
$TenantId = "ID-of-your-tenant"
```

```
$ClientSecret = "Secret-of-your-app"
```

### Convert the client secret to a secure string

```
$ClientSecretPass = ConvertTo-SecureString -String $ClientSecret -AsPlainText -Force
```

### Create a credential object using the client ID and secure string

```
$ClientSecretCredential = New-Object -TypeName System.Management.Automation.PSCredential -  
ArgumentList $ClientId, $ClientSecretPass
```

Gist: <https://gist.github.com/invictus-korstiaan/74101206ddcb98dc6f95cc7952c3a0bc>



## Graph API – Time to connect


### Connect

```
Connect-MgGraph -TenantId $tenantId  
-ClientSecretCredential  
$ClientSecretCredential
```

### Check your permissions

Get-MgContext

```
PS /Users/korstiaan> get-mgcontext  
  
ClientId           : 992272bc-8182-497f-a9f7-047933c349ab  
TenantId           : 88de8f9f-41b9-4b9d-8751-f11a580f3543  
Scopes              : {AuditLogsQuery.Read.All}  
AuthType           : AppOnly  
TokenCredentialType : ClientSecret  
CertificateThumbprint :  
CertificateSubjectName :  
Account            :  
AppName            : Graph-APP-for-log-acquisition  
ContextScope       : Process  
Certificate         :  
PSHostVersion       : 7.4.1  
ManagedIdentityId  :  
ClientSecret        : System.Security.SecureString  
Environment         : Global  
  
PS /Users/korstiaan> get-mgcontext |select -ExpandProperty Scopes  
AuditLogsQuery.Read.All
```



## Graph API – Call the AuditLogQuery API directly

### # Get current queries

```
$results = Invoke-MGGraphRequest -Method  
get -Uri  
'https://graph.microsoft.com/beta/security/  
auditLog/queries' -OutputType PSObject -  
Headers @{'ConsistencyLevel' = 'eventual' }
```

### # Get result details

```
$results.value
```

```
PS /Users/korstiaan> $results.value  
  
id : 48174294-4c34-4e41-993e-7169841ea625  
displayName : demo-search  
filterStartDateTime : 07/05/2024 00:00:00  
filterEndDateTime : 08/05/2024 00:00:00  
recordTypeFilters : {}  
keywordFilter :  
serviceFilters : {Exchange}  
operationFilters : {}  
userPrincipalNameFilters : {}  
ipAddressFilters : {}  
objectIdFilters : {}  
administrativeUnitIdFilters : {}  
status : succeeded
```

## Graph API – The easy way

### # Just use the Extractor

Get-UALGraph -searchName "SANS test" -startDate "01-05-2024" -endDate "07-05-2024"

```
PS /Users/korstiaan> Get-UALGraph -searchName "SANS test" -startDate "01-05-2024" -endDate "07-05-2024"
[INFO] Running Get-UALGraph
[INFO] New Unified Audit Log Search started with the name: SANS test and Id: 72db0ba8-3e46-4f1d-84d1-08bfcfc06f2e
[INFO] Unified Audit Log search is stil running. Waiting...
```

### # Check on the progress in the GUI if you want

Search name ▾	Job status ▾	Progr... ▾	Searc... ▾	Total results ▾	Creation tim... ↓ ▾	Search performed by ▾
<input type="checkbox"/> SANS test	In progress	0%	1m, 36s	0	8 May 2024 10:25	korstiaan@invictus-ir.com



## Graph API - Tips

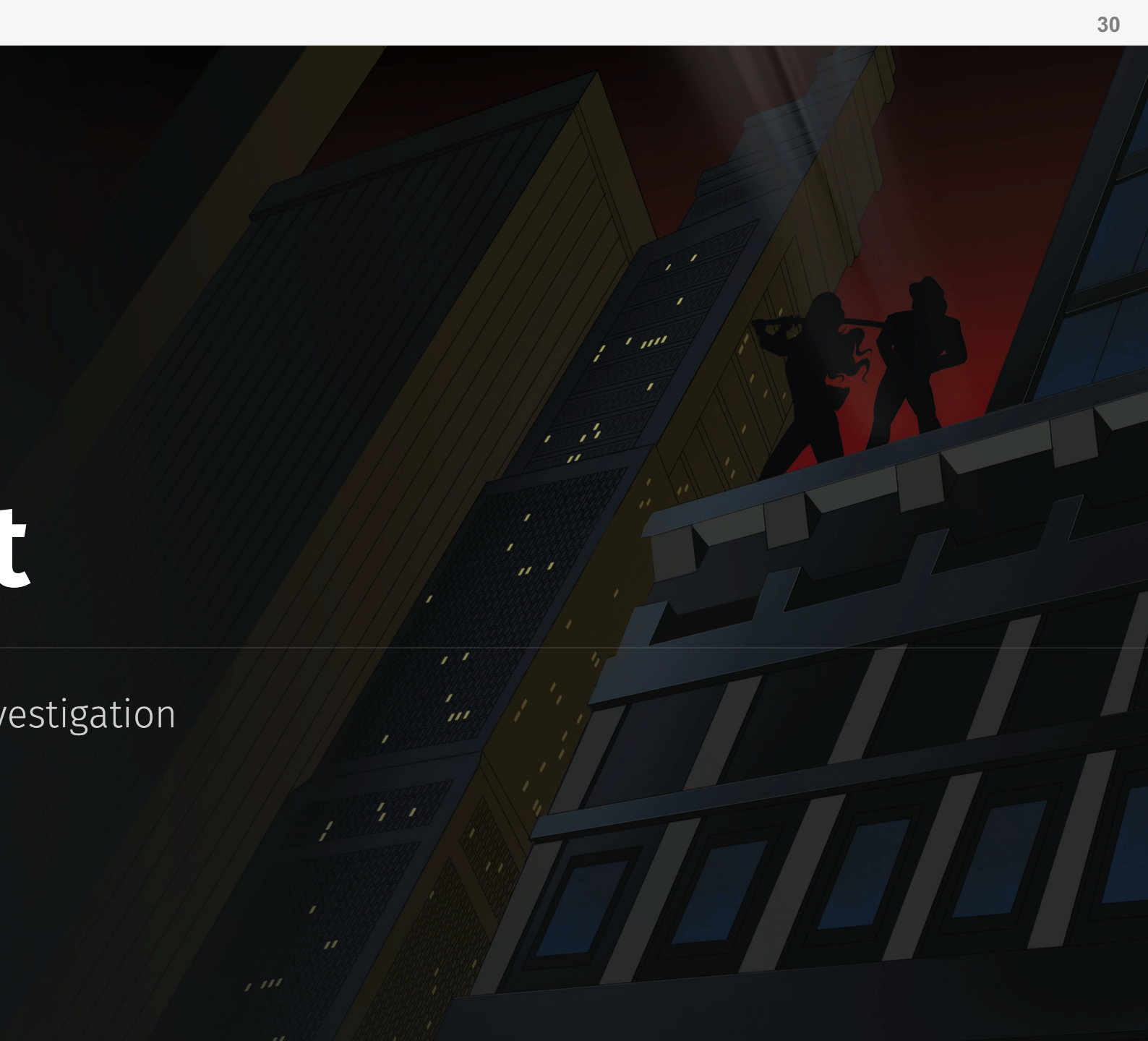
---

- Use at your own risk, sometimes you will receive internal server errors (5xx) we believe that's because it's still in beta
- The output is consistent which is a big plus compared to the Search-UnifiedAuditLog module and the GUI
- Setup an application beforehand that has the permissions to read the Audit Logs
- If you like the GUI, you can always check the progress of your export in the GUI too
- You can load in the output in SOF-ELK or Splunk or whatever you like it's .json

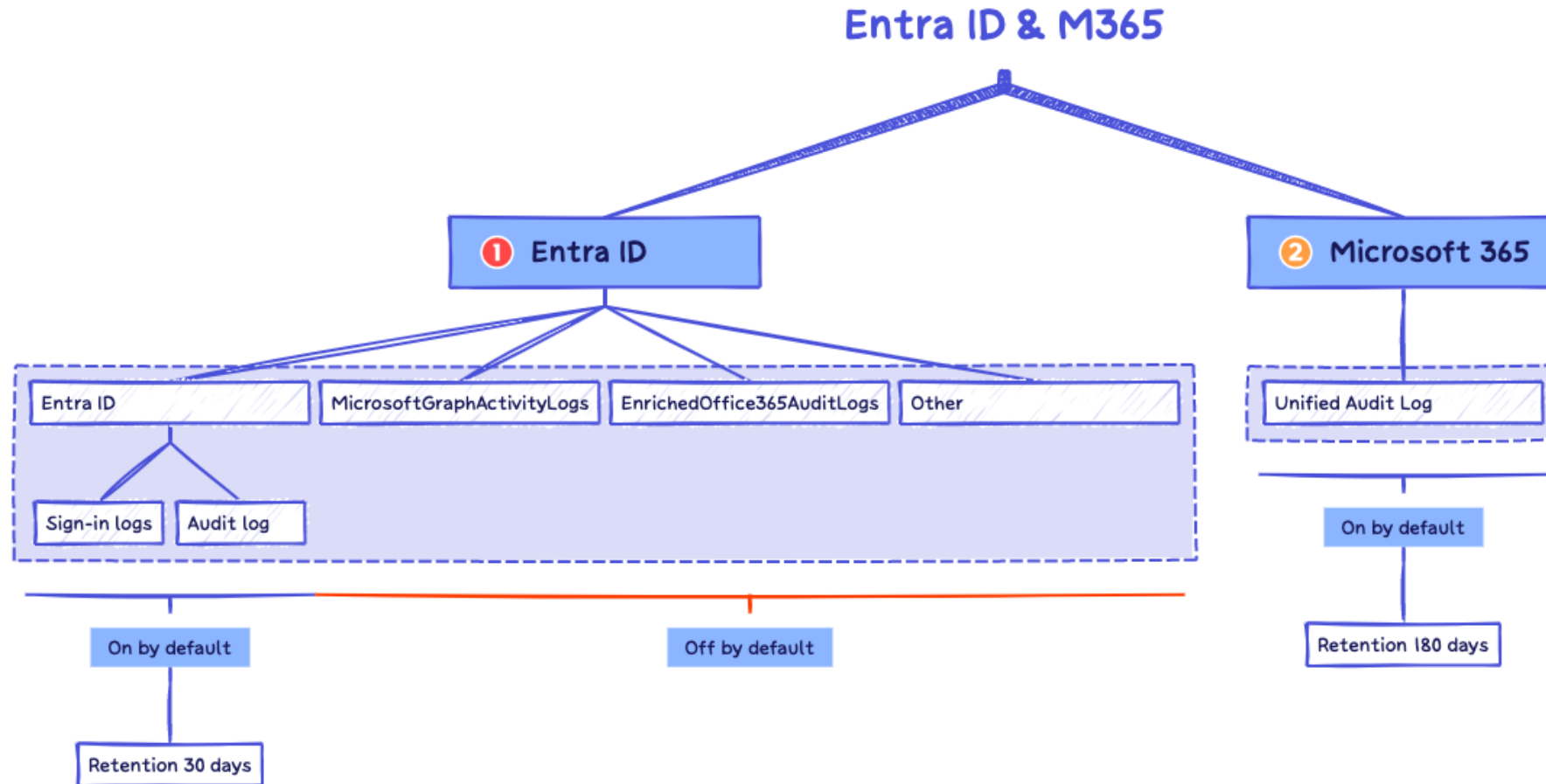


# The present

What audit logs are available for investigation



# Log overview for Entra ID & M365



## Recent changes

---

### Entra ID

---

Available since October 2023

Available since March 2024

### Logs

---

# GraphActivityLogs

---

# EnhancedO365AuditLogs

## GraphActivityLogs - Overview

---

### What is it?

Queries made using the Graph API will be logged in this log source.

### Relevance?

- **Storm-0558**, was a high-impact incident against US government and several undisclosed entities. A notable aspect of this attack was the attackers making API calls to read emails. However, if these actions had been carried out through Entra ID apps and Graph API calls, proper logging might have provided an opportunity to detect this earlier.
- The **Solarwinds** attack, allegedly carried out by a nation-state actor, where Entra ID applications were leveraged to access and acquire sensitive data.

## GraphActivityLogs - Content


Fieldname	Note
RequestMethod	Use this field to quickly filter by type of requests such as GET or POST request.
ResponseStatusCode	All events are HTTP request this field helps identify successful or failed requests.
IpAddress	For requests made with Service Principals the IP-address will be a Microsoft IP-address. For requests made via a UserId you can get the real IP-address of the request.
RequestUri	This is a very important field as it reveals the endpoint of the request in other words what was requested.
ResponseSizeBytes	Using this field you can identify the amount of data returned by the request.
ApplId	This field helps you identify the application that is initiating the request.
ServicePrincipalId	When a service principal object is used this field is filled with its identifier.
UserId	When a user object is used, this field is populated allowing you to identify the specific user responsible for making the request.
UserAgent	Can be useful to identify (un)common applications making requests.
Scopes	The permissions assigned to the application making the request.
Roles	also known as application permissions this can help you identify what possible access an app has.

## User making a request


Request...	Respon...	IPAddress	RequestUri	AppId	UserId ↑↓	UserAgent	Scopes
> GET	404	83.87	https://graph.microsoft.com/...	d3590ed6-52b3-4102-aeff-...	8eed292e-e42f-48b4-a2d4-...	Microsoft Office PowerPoint/...	AuditLog.Read.All Calendar.
> GET	200	83.87	https://graph.microsoft.com/...	d3590ed6-52b3-4102-aeff-...	8eed292e-e42f-48b4-a2d4-...	PowerPoint/16.84.24042223 ...	AuditLog.Read.All Calendar.
> GET	404	83.87	https://graph.microsoft.com/...	d3590ed6-52b3-4102-aeff-...	8eed292e-e42f-48b4-a2d4-...	PowerPoint/16.84.24042223 ...	AuditLog.Read.All Calendar.

## Application making a request

Application  
(e.g. Splunk)



Associated SP  
(allowed to make the call)



Results		Chart				
Request...	Res...	IPAddress	RequestUri	ApplId	ServicePrincipalId	
> GET	200	20.221.88.168	https://graph.microsoft.com/...	d29a4c00-4966-492a-84dd-47e779578fb7	eaabce31-ae07-4fd7-9506-f730be98b755	
> GET	200	68.219.174.77	https://graph.microsoft.com/...	98785600-1bb7-4fb9-b9fa-19afe2c8a360	2acd561f-87c1-44e3-8ed2-f63e1a289812	
> GET	200	20.93.99.220	https://graph.microsoft.com/...	60ca1954-583c-4d1f-86de-39d835f3e452	21d1b38f-f260-4d50-8502-4886769a58ee	

## GraphActivityLogs - Tips

---

- Think before you turn it on, it's a lot of data (\$\$\$)
- Filter on POST calls to find write events
- The IP-address field contains a Microsoft IP addresses for calls made through a Service Principal when a User performs the call it's the 'Real' IP-address
- Use cases:
  - Failed calls by applications (e.g. unauthorized)
  - Data exfiltration through the Graph API
  - C2 via the Graph API
  - Audit your enterprise applications



## GraphActivityLogs - Further reading

---

**Bert-Jan Pals** (KQL master and part of Team Invictus) has created a nice blog on using the Graph Activity Log to investigate threats:

<https://kqlquery.com/posts/graphactivitylogs/>

**Fabian Bader** has created a blog series on detecting threats using this log:

<https://cloudbrothers.info/en/detect-threats-microsoft-graph-logs-part-1/>

We have a blog series on GraphRunner detection that heavily relies on this log:

<https://www.invictus-ir.com/news/a-defenders-guide-to-graphrunner-part-i>

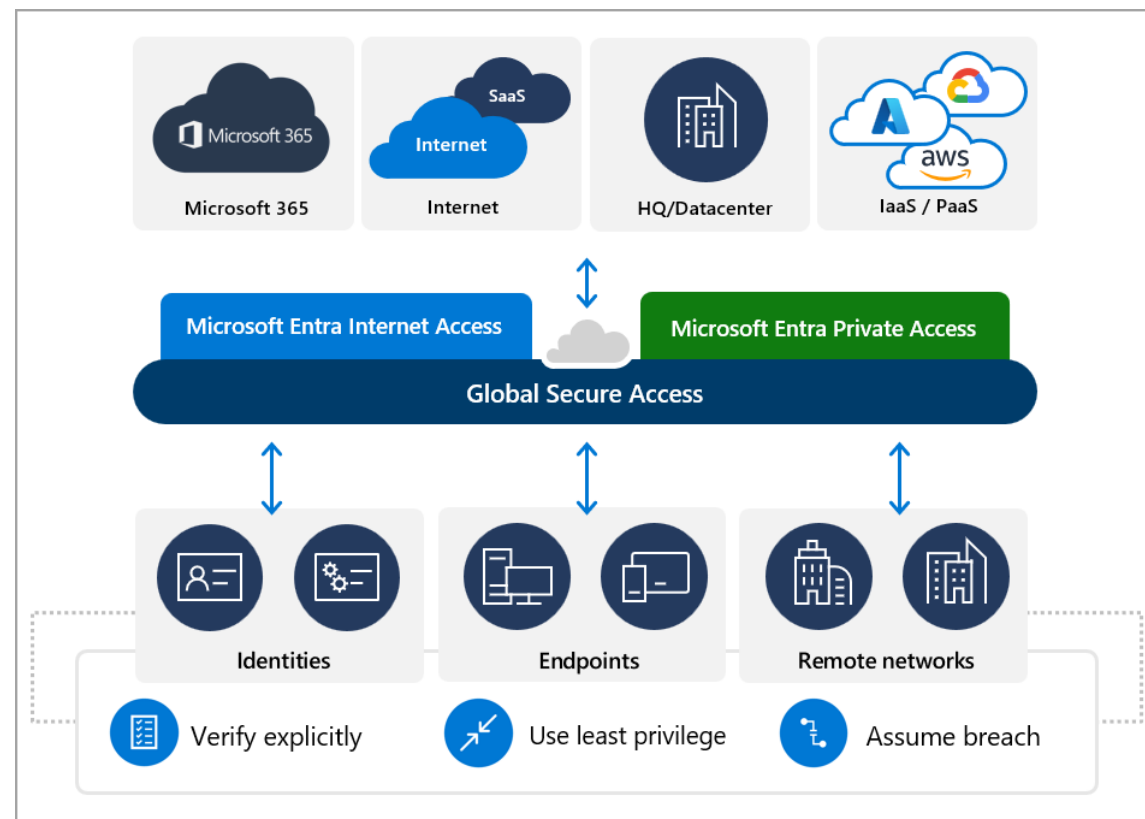
<https://www.invictus-ir.com/news/a-defenders-guide-to-graphrunner-part-ii>

## EnrichedO365AuditLogs - Overview

### What is it?

A new log source that can be enabled on the tenant level.

The EnrichedOffice365AuditLogs are part of a new Microsoft service called Global Secure Access (GSA). In short GSA is a new Microsoft service that goes all in on the zero-trust principle.



## EnrichedO365AuditLogs - Relevance

---

- Only relevant if you use Global Secure Access which is in preview
- Limited to SharePoint/OneDrive
- Exchange & Teams are coming
- The only 'real' change is actual IP information

## EnrichedO365AuditLogs - Content

...				
Results		Chart		
TimeGenerated [UTC] ↑↓		Operation	SourceIp	ClientIp
>	3/5/2024, 12:17:04.000 PM	FileAccessed	4.234.11.243	128.94.17.78
>	3/5/2024, 12:16:57.000 PM	ListCreated	4.234.11.243	128.94.17.78
>	3/5/2024, 12:16:49.000 PM	PageViewed	4.234.11.243	128.94.17.78
>	3/5/2024, 12:16:26.000 PM	FileAccessed	4.234.11.243	128.94.17.78
>	3/5/2024, 12:05:38.000 PM	FileDownloaded	4.234.11.243	128.94.18.48
>	3/5/2024, 12:05:38.000 PM	FileDownloaded	4.234.11.243	128.94.18.48
>	3/5/2024, 12:05:15.000 PM	FileAccessed	4.234.11.243	128.94.18.48
>	3/5/2024, 12:05:11.000 PM	PageViewed	4.234.11.243	128.94.18.48
>	3/5/2024, 12:05:09.000 PM	FileAccessed	4.234.11.243	128.94.18.48
>	3/5/2024, 12:05:06.000 PM	FileAccessed	4.234.11.243	128.94.18.48

## EnrichedO365AuditLogs – Further reading

---

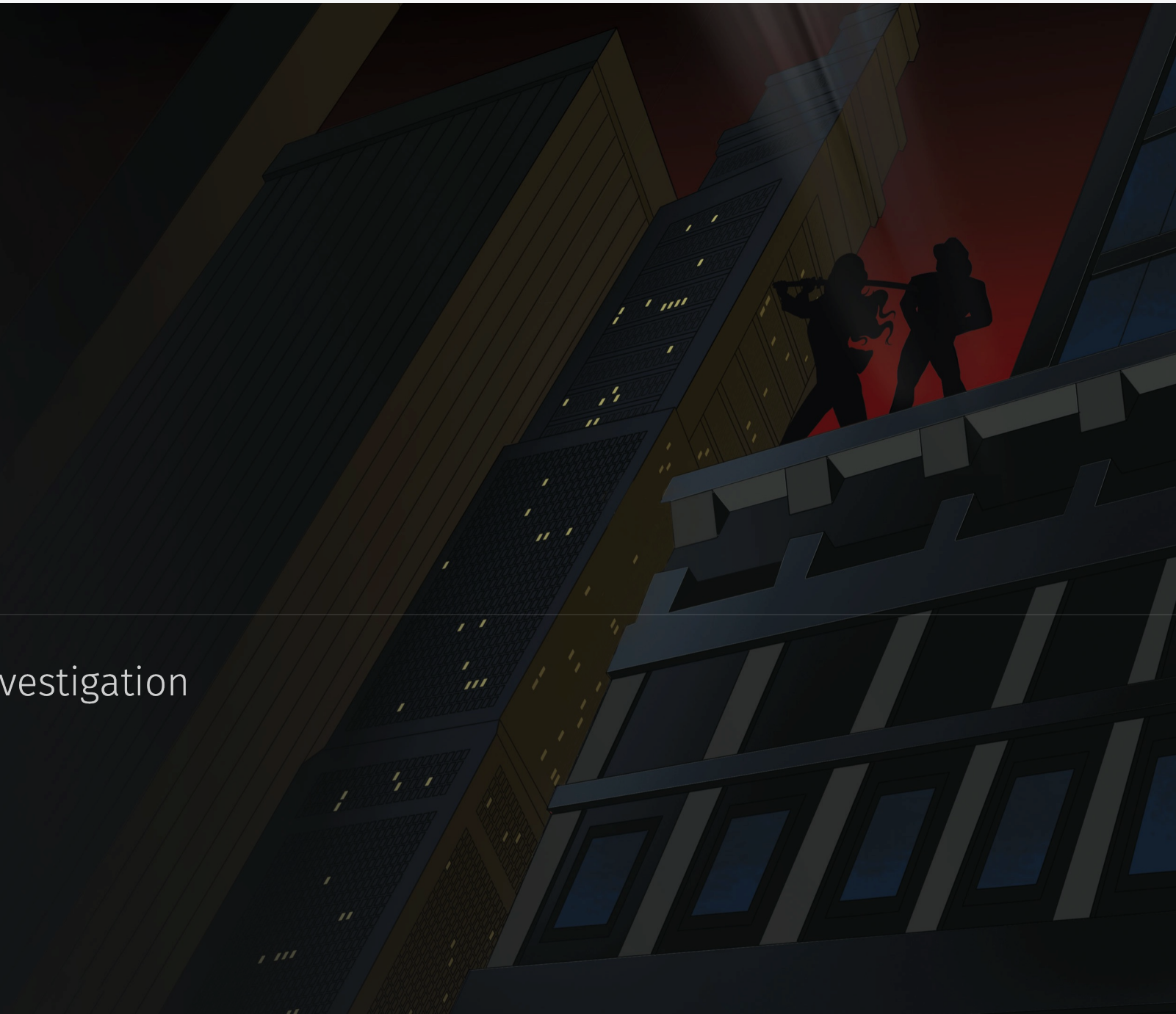
We wrote a blog on how to configure this log if you want to play with it yourselves:

<https://www.invictus-ir.com/news/the-mystery-of-the-enrichedoffice365auditlogs-solved>

It seems no-one else wants to write about it 😞

# The future

What audit logs are available for investigation



## What's coming?

This is more a wishlist to be honest:

- Improved Graph API performance for the Unified Audit Log to be able to do faster acquisitions
- Search-UnifiedAuditLog will be fixed or killed
- One API to rule them all (GraphAPI)
  - Good for monitoring
  - Bad you don't know whether all the old stuff will still work and/or available





# Takeaways

This is what matters





# Takeaways

---

## What you should remember

---

- Microsoft is making lots of changes and improvements to auditing, which is good for us
- Include the UAL for your investigations, don't rely on Entra ID logging only you will miss information
- Make sure you have a logging strategy, whether that is saving it to a storage account for a rainy day or continuous monitoring
- If you don't use GraphActivityLogs you will be blind to lots of activity
- The EnrichedO365AuditLogs are only available when using GSA

## Do you want know more?

---

- **More information on FOR509**
  - <https://www.sans.org/for509/>
- **Training opportunities FOR509**
  - Munich - June 2024
  - Amsterdam – July 2024
  - London – August 2024
- **Don't be a stranger**
  - <https://www.linkedin.com/in/korstiaanstam/>

Q&A



?

?

?