



Stay One Step Ahead

Threat Detection with Microsoft Graph Activity Logs





```
print
```

```
name = "Fabian Bader",  
title = "Cyber Security Architect",  
company = "glueck□kanja",  
awards = "Microsoft MVP"
```

Microsoft Graph Activity Logs?

- Microsoft Graph is THE Microsoft 365 Cloud API
- Changes to e.g. users are tracked in audit logs (PATCH)
- Information gathering is not (GET)
- All REST calls can be logged



How to configure?

- Entra Portal
- Sentinel

Targets

- Log Analytics
- Storage Account
- Event Hub

The screenshot shows the configuration interface for a Log Analytics workspace in Microsoft Sentinel. It is divided into two main sections: 'Logs' and 'Destination details'.

Logs

Categories

- ☒ AuditLogs
- ☒ ServicePrincipalSignInLogs
- ☒ ManagedIdentitySignInLogs
- ☒ ProvisioningLogs
- ☒ ADFSSignInLogs
- ☒ RiskyUsers
- ☒ UserRiskEvents
- ☒ NetworkAccessTrafficLogs
- ☒ RiskyServicePrincipals
- ☒ ServicePrincipalRiskEvents
- ☒ EnrichedOffice365AuditLogs
- ☒ MicrosoftGraphActivityLogs

Destination details

- ☒ Send to Log Analytics workspace

Subscription

MVP c4a8korriban Tier 0

Log Analytics workspace

log-c4a8korriban-sentinel-prd-weu (westeurope)

- ☐ Archive to a storage account
- ☐ Stream to an event hub
- ☐ Send to partner solution

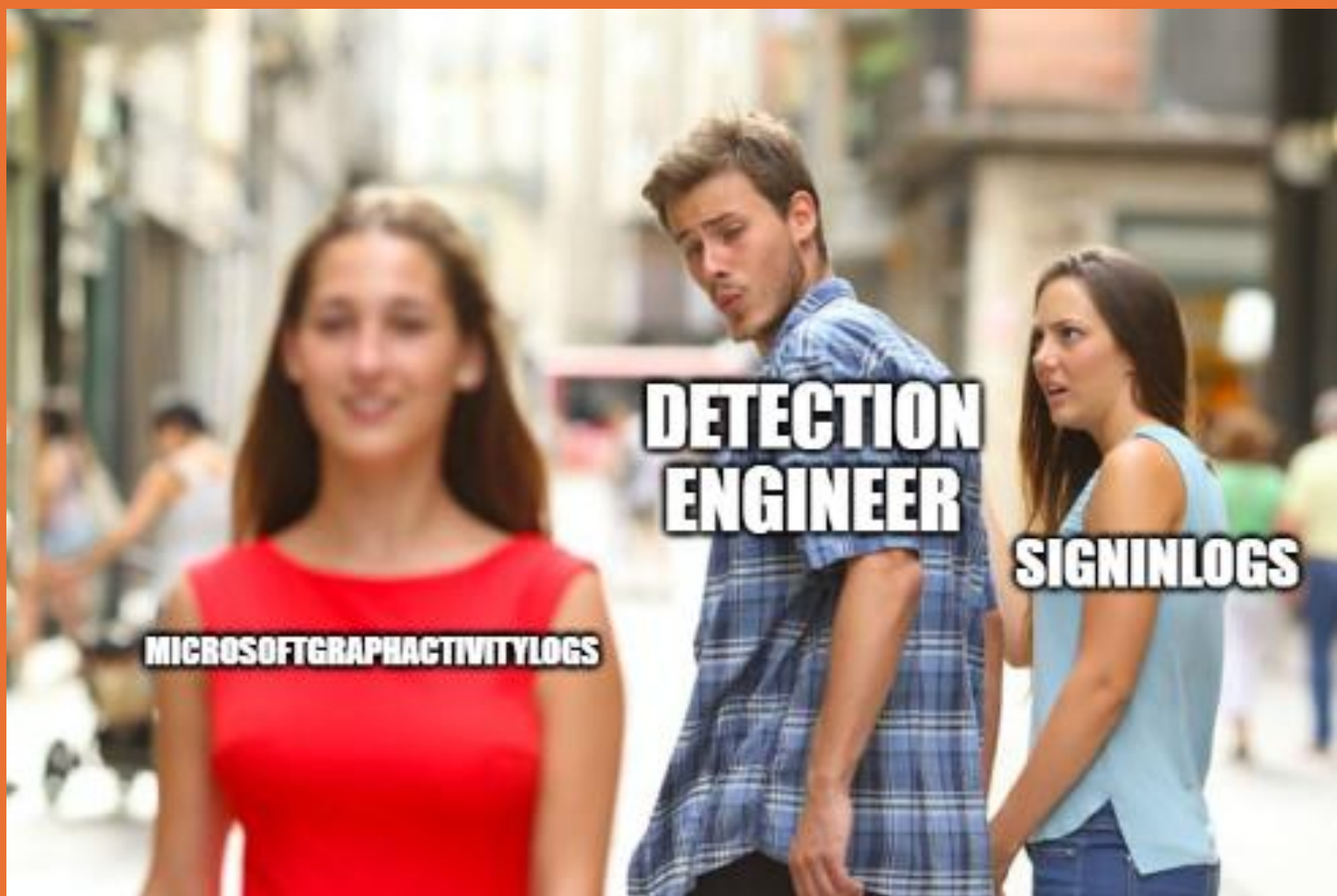
How does this help me?

- Early detection of an attacker in the discovery phase (TA0007)
- Detect anomalies in usage pattern 🚗
- Analyze application behavior
- Correlate data in incident response

https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf

Interesting fields

Fieldname	Purpose
RequestMethod	GET, UPDATE, PATCH, DELETE
OperationId	Match multiple operations to one request
IPAddress	The IP address of the caller
UserAgent	User agent of the caller (easy to change)
ResponseSizeBytes	Size of the Graph response message in bytes
ServicePrincipalId/UserId	Object Id of the initiating identity
SignInActivityId	Correlate with sign-in activity
Scopes	Active scopes of the Graph request



```
PS C:\Research\azurehound-windows-amd64> .\azurehound.exe list -t e3686c4f-af27-4f22-b9de-062f05b93aac -j $JWT -o tenant2.json
```

AzureHound v2.1.0

Created by the BloodHound Enterprise team - <https://bloodhoundenterprise.io>

No configuration file located at C:\Users\fabian\.config\azurehound\config.json

No configuration file located at C:\Users\fabian\.config\azurehound\config.json

2025-07-01T09:47:18Z INF collecting azure objects...

2025-07-01T09:47:18Z ERR unable to continue processing tenants error="invalid audience"

2025-07-01T09:47:18Z INF warning: unable to process azure management groups; either the organization has no management groups or azurehound does not have the reader role on the root management group.

2025-07-01T09:47:18Z ERR unable to continue processing subscriptions error="invalid audience"

2025-07-01T09:47:18Z INF finished listing all resource groups

2025-07-01T09:47:18Z INF finished listing all key vaults

2025-07-01T09:47:18Z INF finished listing all automation accounts

2025-07-01T09:47:18Z INF finished listing all web apps

2025-07-01T09:47:18Z INF finished listing all function apps

2025-07-01T09:47:18Z INF finished listing all managed clusters

2025-07-01T09:47:18Z INF finished listing all virtual machines

2025-07-01T09:47:18Z INF finished listing all container registries

2025-07-01T09:47:18Z INF finished listing all web app role assignments

2025-07-01T09:47:18Z INF finished listing all virtual machine scale sets

2025-07-01T09:47:18Z INF finished listing all logic app role assignments

2025-07-01T09:47:18Z INF finished listing all management group role assignments

2025-07-01T09:47:18Z INF finished listing all subscription role assignments

2025-07-01T09:47:18Z INF finished listing all subscription user access admins

2025-07-01T09:47:18Z INF finished listing all resource group role assignments

2025-07-01T09:47:18Z INF finished listing all key vault role assignments

2025-07-01T09:47:18Z INF finished listing all virtual machine role assignments

2025-07-01T09:47:18Z INF finished listing all function app role assignments

2025-07-01T09:47:18Z INF finished listing all management group descendants

2025-07-01T09:47:18Z INF finished listing all automation account role assignments

2025-07-01T09:47:18Z INF finished listing all container registry role assignments

2025-07-01T09:47:18Z INF finished listing all logic apps

2025-07-01T09:47:18Z INF finished listing all managed cluster role assignments

2025-07-01T09:47:18Z INF finished listing all vm scale set role assignments

2025-07-01T09:47:18Z INF finished listing all users count=86

2025-07-01T09:47:18Z INF finished listing all apps count=45

2025-07-01T09:47:18Z INF finished listing all devices count=43

2025-07-01T09:47:19Z INF finished listing all app owners

2025-07-01T09:47:19Z INF finished listing all device owners

2025-07-01T09:47:19Z INF finished listing all roles count=122

2025-07-01T09:47:19Z INF finished listing all role assignments

2025-07-01T09:47:19Z INF finished listing all groups count=180

2025-07-01T09:47:19Z INF finished listing all group owners

2025-07-01T09:47:19Z INF finished listing members for all groups

2025-07-01T09:47:23Z INF finished listing all service principals count=849

2025-07-01T09:47:24Z INF finished listing all app role assignments

2025-07-01T09:47:24Z INF finished listing all service principal owners

2025-07-01T09:47:24Z INF collection completed duration=5.6683098s

shutting down gracefully, press ctrl+c again to force

PS C:\Research\azurehound-windows-amd64> _



Demo

Dive into the data...



What about the money?



What about the money?

# User	Log Size (30day)
1000	15 GB

100.000 1200 GB

<https://learn.microsoft.com/en-us/graph/microsoft-graph-activity-logs-overview#cost-planning-estimates>

# User	Log Size (30day)
50	3 GB

150 6 GB

300 5 GB

400 7 GB

8.000 74 GB

19.000 71 GB

What about the money?

☐	DataType	TotalUsers	TotalEvents	DataGB
☐	> MicrosoftGraphActivityLogs	111	869111	1.3318702720000002

☐	DataType	TotalUsers	TotalEvents	DataGB
☐	> MicrosoftGraphActivityLogs	107218	1726724348	1446.074216499

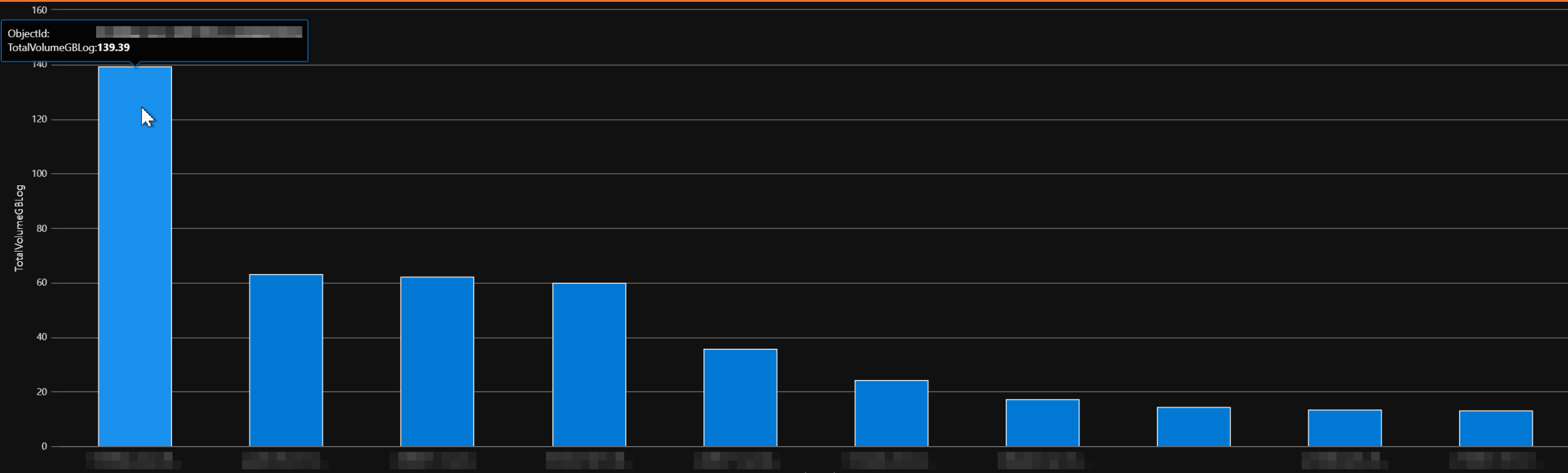
What about the money?

- Use workspace data collection transformations to reduce size or sent to different log tier (basic / auxiliary)
- Use summary rules to leverage data for detections

<https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-transformations>

What about the money?

- Identify outliers
 - Exclude from Analytics data (easy)
 - Optimize underlying usage (very hard)



What about the money?

```
// Identify the top 10 identities contributing to your graph usage
MicrosoftGraphActivityLogs
| where TimeGenerated > ago(90d)
| extend ObjectID = coalesce(UserId, ServicePrincipalId)
| extend ObjectType = iff(isempty(UserId), "ServicePrincipalId", "UserId")
| summarize
    TotalVolumeGBLog = round(sum(_BilledSize / 1024 / 1024 / 1024), 2),
    arg_max(TimeGenerated, ObjectID)
    by ObjectID
| project-away TimeGenerated, ObjectID1
| sort by TotalVolumeGBLog desc
| limit 10
| render columnchart
```



Demo

Money, money, ingestion size...



Known blindspots

- No insights into (PATCH) payload
- Azure AD Graph
 - AADInternals
 - ROADr ☒ AzureADGraphActivityLogs
 - PingCache

Follow along until it's shutdown for good
<https://aka.ms/aadgraphupdate>

Map Audit Logs to Graph Calls

Identify which Graph API Call triggers which Entra ID audit event

Community sourced dataset available on GitHub

Contribute your anonymised data to

<https://github.com/f-bader/EntraIDAuditLogToMicrosoftGraph>

Queries and detections

All queries and detections can be found in my blog posts or in my personal GitHub

<https://github.com/f-bader/AzSentinelQueries>

<https://cloudbrothers.info/>



Thank you

0xF4B1A₀