

From Entra ID Logs to Valuable Insights

Bert-Jan Pals

Dutch Microsoft Entra Meetup 13/11/2025

Bert-Jan Pals



Defensive Security Expert



<https://x.com/BertJanCyber>



<https://www.linkedin.com/in/bert-janpals/>



<https://github.com/bert-janp>



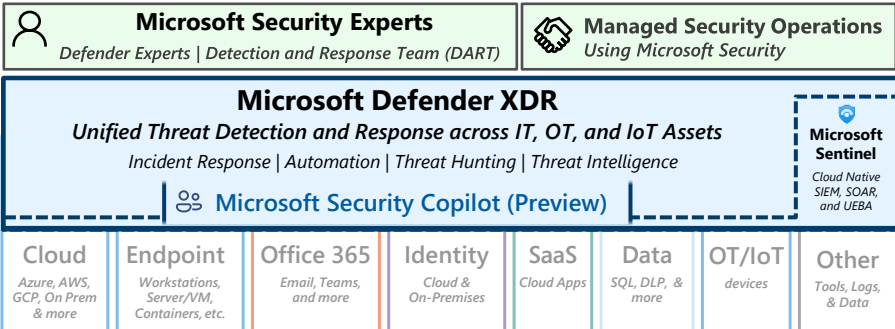
<https://kqlquery.com/>

Agenda

- What data is available?
- 🗄️ 🗄️ 🗄️
- Inside the logs
- Automate log discovery
- Use cases: Query Logs
- Use cases: Workbooks
- Use cases: Reporting

What data is available?

Security Operations / SOC



Cybersecurity Reference Architecture

Security modernization with Zero Trust Principles

December 2023 – aka.ms/MCRA

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Security Guidance

1. [Security Adoption Framework](#)
2. [Security Documentation](#)
3. Cloud Security [Benchmarks](#)

Software as a Service (SaaS)

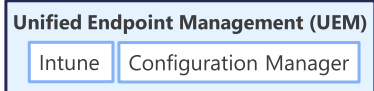


Microsoft Entra Internet Access

Identity & Access

Conditional Access – Zero Trust Access Control decisions based on explicit validation of user trust and endpoint integrity

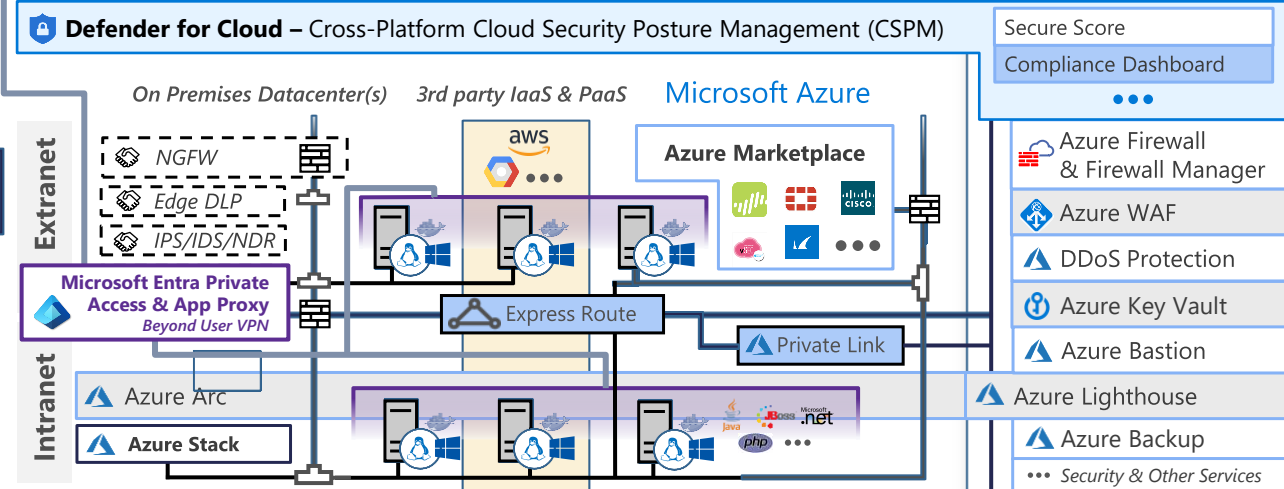
Endpoints & Devices



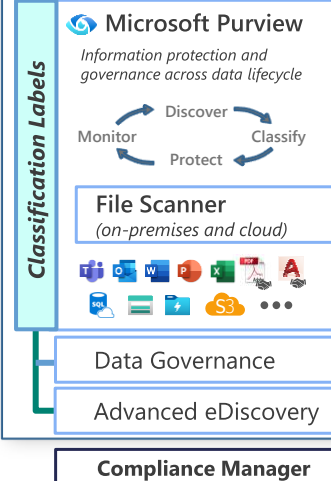
Microsoft Defender for Endpoint
Unified Endpoint Security

- Endpoint Detection & Response (EDR)
- Web Content Filtering
- Threat & Vuln Management
- Endpoint Data Loss Protection (DLP)

Hybrid Infrastructure – IaaS, PaaS, On-Premises



Information Protection



Microsoft Entra

- Passwordless & MFA
 - Hello for Business
 - Authenticator App
 - FIDO2 Keys
- Entra ID Protection
 - Leaked cred protection
 - Behavioral Analytics
- ID Governance
- Microsoft Entra PIM
- External Identities

Defender for Identity

Active Directory

Securing Privileged Access – aka.ms/SPA

Entra Permission Management – Discover and Mitigate Cloud Infrastructure Permission Creep

Privileged Access Workstations (PAWs) – Secure workstations for administrators, developers, and other sensitive users

Security Posture Management – Monitor and mitigate technical security risks using [Secure Score](#), [Compliance Score](#), [CSPM: Defender for Cloud](#), [Microsoft Defender External Attack Surface Management \(EASM\)](#) and [Vulnerability Management](#)

Windows 11 & 10 Security

- Network protection
- Credential protection
- Full Disk Encryption
- Attack surface reduction
- App control
- Exploit protection
- Behavior monitoring
- Next-generation protection

IoT and Operational Technology (OT)



- Microsoft Defender for IoT (and OT)**
- ICS, SCADA, OT
 - Internet of Things (IoT)
 - Industrial IoT (IIoT)
 - Asset & Vulnerability management
 - Threat Detection & Response

Defender for Cloud – Cross-Platform, Multi-Cloud XDR
Detection and response capabilities for infrastructure and development across IaaS, PaaS, and on-premises



Defender for APIs (preview)

People Security

- Attack Simulator
- Insider Risk Management
- Communication Compliance

GitHub Advanced Security & Azure DevOps Security
Secure development and software supply chain

Threat Intelligence – 65+ Trillion signals per day of security context

Service Trust Portal – How Microsoft secures cloud services

Security Development Lifecycle (SDL)

Entra ID Logs

- Configuration needed to store logs
- Diagnostics settings

Capability	Microsoft Entra ID Free	Microsoft Entra ID P1 or P2 / Microsoft Entra Suite
Audit logs	Yes	Yes
Sign-in logs	Yes	Yes
Provisioning logs	No	Yes
Custom security attributes	Yes	Yes
Health	No	Yes
Microsoft Graph activity logs	No	Yes
Usage and insights	No	Yes

Custom security attributes

Certificate authorities

External Identities ★

Cross-tenant synchronization

Entra Connect

Domain names

Custom branding

Mobility

Monitoring & health ^

Sign-in logs

Audit logs

Provisioning logs

Health

Log Analytics

Diagnostic settings

Workbooks

Usage & insights

Bulk operations

ID Protection ∨

[Home](#) > [Microsoft Entra](#) > [Sign-ins](#) > [Gallery](#) > [Diagnostic settings | General](#) > [Gallery](#) >

Diagnostic settings | General

KQLQuery.com

« Refresh Feedback

Diagnostic settings

General

Custom security attributes

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings independent destinations. [Learn more about diagnostic settings](#)

Diagnostic settings

Name	Storage account	Event hub	Log Analytics workspace	Partner solution
EntraID-Sentinel	-	-	sentinel	-

[+ Add diagnostic setting](#)

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- AuditLogs
- SignInLogs
- NonInteractiveUserSignInLogs
- ServicePrincipalSignInLogs
- ManagedIdentitySignInLogs
- ProvisioningLogs
- ADFSSignInLogs
- RiskyUsers
- UserRiskEvents
- NetworkAccessTrafficLogs
- RiskyServicePrincipals
- ServicePrincipalRiskEvents
- EnrichedOffice365AuditLogs
- MicrosoftGraphActivityLogs
- RemoteNetworkHealthLogs
- NetworkAccessAlerts
- NetworkAccessConnectionEvents
- MicrosoftServicePrincipalSignInLogs
- AzureADGraphActivityLogs
- NetworkAccessGenerativeAllInsights



Entra ID Logs

Table	Description
AuditLogs	Audit log for Azure Active Directory. Includes system activity information about user and group management managed applications and directory activities.
SignInLogs	Interactive Azure Active Directory sign-in logs from user.
NonInteractiveUserSignInLogs	Non-interactive Azure Active Directory sign-in logs from user.
ServicePrincipalSignInLogs	Service principal Azure Active Directory sign-in logs.
ManagedIdentitySignInLogs	Managed identity Azure Active Directory sign-in logs.
ProvisioningLogs	
ADFSSignInLogs	Logs generated by Active Directory Federation Service.
RiskyUsers	Logs generated by identity protection for Azure AD risky users.
UserRiskEvents	Logs generated by identity protection for Azure AD user risk events.

Entra ID Logs

Table	Description
NetworkAccessTrafficLogs	This table is part of Identity and Network Access, which contains Network Traffic Access logs. These logs can be leveraged for policy, risk, and traffic management, as well as to monitor users experience.
RiskyServicePrincipals	Logs generated by identity protection for Azure AD risky service principals.
ServicePrincipalRiskEvents	Logs generated by identity protection for Azure AD service principal risk events.
EnrichedOffice365AuditLogs	This table is part of Identity and Network Access, which contains Enriched Microsoft 365 Audit logs. These logs can be leveraged for policy, risk, and traffic management, as well as to monitor users experience.
MicrosoftGraphActivityLogs	Microsoft Graph Activity Logs provide details of API requests made to Microsoft Graph for resources in the tenant.
RemoteNetworkHealthLogs	This table is part of Identity and Network Access, which contains Remote Network Health logs. These logs can be leveraged for knowing the state of your remote networks health state.

Entra ID Logs

Table	Description
NetworkAccessAlerts	This table is part of Identity and Network Access, which contains Network Access Alerts. These Alerts can be leveraged for knowing the state of your network access.
NetworkAccessConnectionEvents	This table is part of Identity and Network Access, which contains Network Traffic Connection Events. These logs can be leveraged for security, and traffic management, as well as to monitor users experience.
MicrosoftServicePrincipalSignInLogs	Microsoft applications' service principal sign-in logs.
AzureADGraphActivityLogs	AAD Graph Activity Logs provide details of legacy API requests made to Azure Active Directory Graph for resources in the tenant.
MicrosoftGraphActivityLogs	Microsoft Graph activity logs provide an audit trail of all HTTP requests that the Microsoft Graph service receives and processes for a tenant. Tenant admins can turn on log collection and set up downstream destinations by using diagnostic settings in Azure Monitor.



Your security tools also audit Entra ID activities.

If you are an Entra ID P2 customer:

AADSignInEventsBeta & AADSpnSignInEventsBeta are available in security.microsoft.com

Table	Description
AADSignInEventsBeta	The AADSignInEventsBeta table in the advanced hunting schema contains information about Microsoft Entra interactive and non-interactive sign-ins.
AADSpnSignInEventsBeta	The AADSpnSignInEventsBeta table in the advanced hunting schema contains information about Microsoft Entra service principal and managed identity sign-ins.
EntralDSignInEvents	
EntralDSpnSignInEvents	

Defender For Cloud Apps

Once the Microsoft 365 connector is configured the CloudAppEvents will list Entra ID Audit logs.

The logs flow from Entra ID -> Unified Audit Log -> Defender For Cloud Apps

Table	Description
CloudAppEvents	The CloudAppEvents table in the advanced hunting schema contains information about events involving accounts and objects in Office 365 and other cloud apps and services.
OAuthAppInfo	The OAuthAppInfo table in the advanced hunting schema contains information about Microsoft 365-connected OAuth applications in the organization that are registered with Microsoft Entra ID and available in the Microsoft Defender for Cloud Apps app governance capability.

Defender For Identity

Table	Description
IdentityLogonEvents	The IdentityLogonEvents table in the advanced hunting schema contains information about authentication activities made through your on-premises Active Directory captured by Microsoft Defender for Identity and authentication activities related to Microsoft online services captured by Microsoft Defender for Cloud Apps.

GraphAPIAuditEvents

Table	Description
GraphAPIAuditEvents	The GraphApiAuditEvents table in the advanced hunting schema contains information about Microsoft Entra ID API requests made to Microsoft Graph API for resources in the tenant.

Why do I need to keep this data?

- Security Operations
- Regulatory requirements
- Troubleshooting operational issues
- Exposure management
- Proactive goldmine to secure tenants

Coverage comparison

		Entra ID	Defender XDR
Sign-In	User	✓	✓
	ServicePrincipal	✓	✓
	MangedIdentity	✓	✓
	ADFS	✓	✗
AuditLogs		✓	⚠
RiskEvents		✓	✗
Global Secure Access		✓	✗
Graph API		✓	✓

Log Access

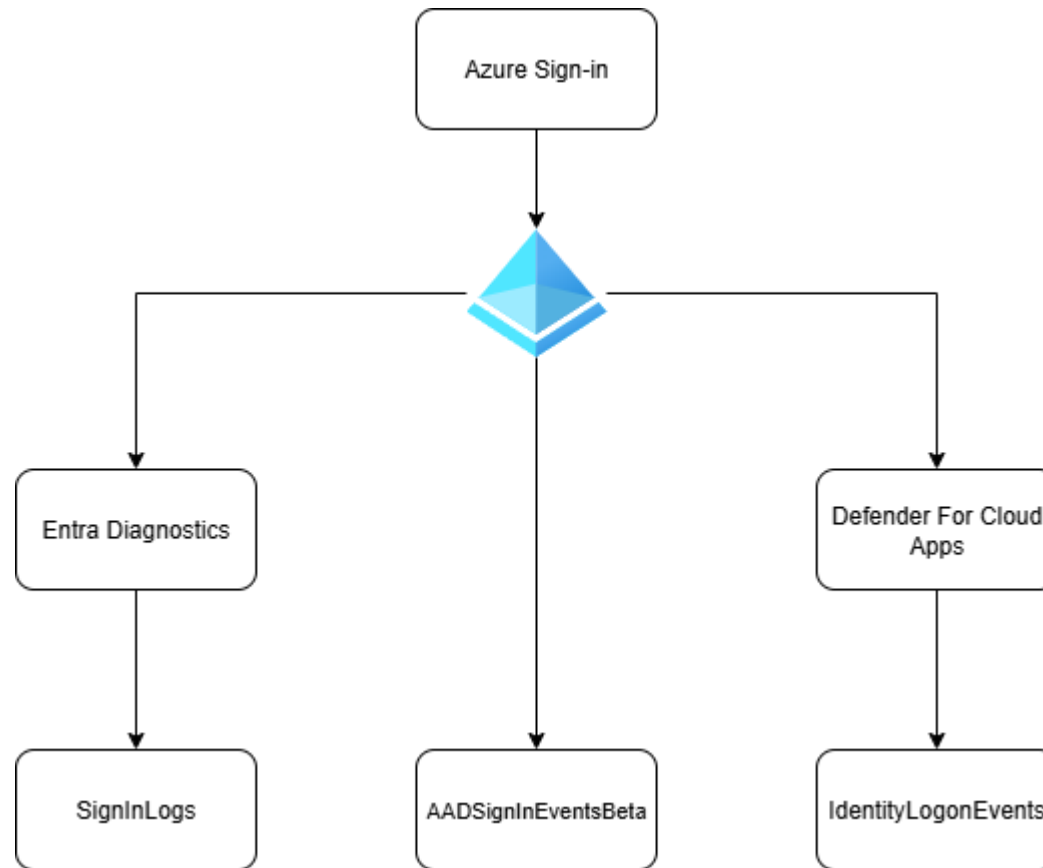
- Log Analytics Workspace, table based
- Defender XDR portal, no table based access yet

I'm Bert and I sign-in to Azure

How often is my sign-in logged?



3 events for the same sign-in



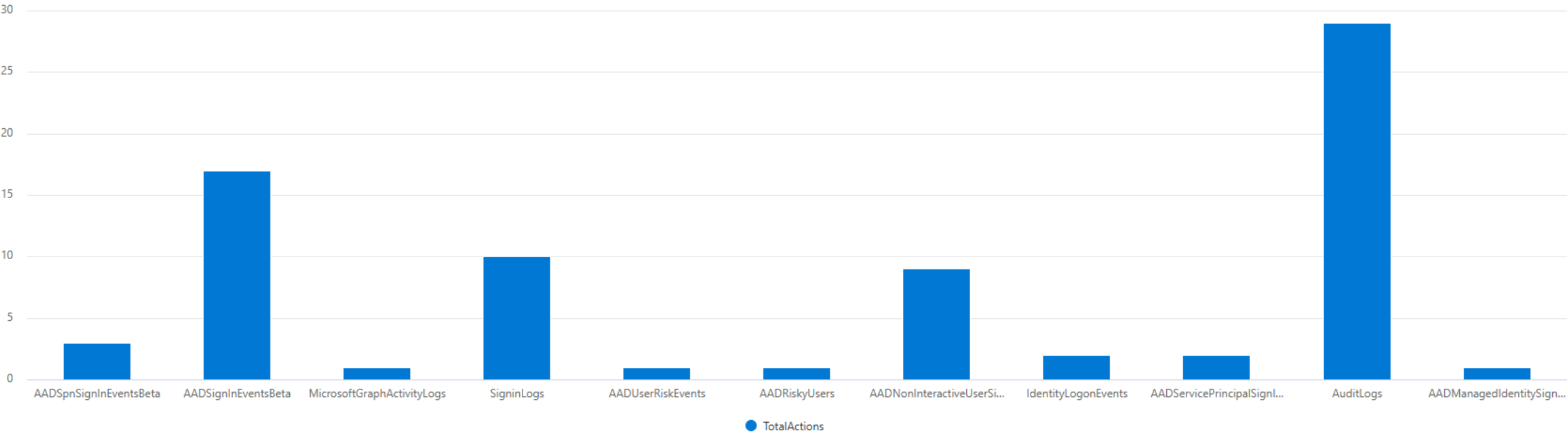
So 3^* times the same log :)

* 4 EntralSignInEvents



Inside the logs

```
1 union withsource=TableName AuditLogs, SigninLogs, AADNonInteractiveUserSignInLogs, AADServicePrincipalSignInLogs, AADManagedIdentitySignInLogs, AADRiskyUsers, AADUserRiskEvents, AADServicePrincipalSignInLogs,
2 | extend Action = coalesce(ResultType, OperationName, tostring(ErrorCode), ActionType, RiskDetail)
3 | summarize TotalActions = dcount(Action) by Type
```



Query

```
1 union withsource=TableName AuditLogs, SigninLogs, AADNonInteractiveUserSignInLogs, AADServicePrincipalSignInLogs, AADManagedIdentitySignInLogs, AADRiskUsers, AADUserRiskEvents, AADServicePrincipalSignInLogs, MicrosoftGraphActivityLogs,
2 | extend Action = coalesce(ResultType, OperationName, tostring(ErrorCode), ActionType, RiskDetail)
3 | summarize TotalActions = count() by Type, Action
```

Getting started Results Query history

Export Show empty columns

92 items Search 00:05.993 Low Chart type Full screen

<input type="checkbox"/>	Type ↑	Action	TotalActions
<input type="checkbox"/>	> AADSignInEventsBeta	50125	5
<input type="checkbox"/>	> AADSignInEventsBeta	50207	5
<input type="checkbox"/>	> AADSignInEventsBeta	50158	8
<input type="checkbox"/>	> AADSignInEventsBeta	50011	9
<input type="checkbox"/>	> AADSignInEventsBeta	50078	2
<input type="checkbox"/>	> AADSignInEventsBeta	50199	4
<input type="checkbox"/>	> AADSignInEventsBeta	50132	1
<input type="checkbox"/>	> AADSignInEventsBeta	50126	3
<input type="checkbox"/>	> AADSignInEventsBeta	53003	9
<input type="checkbox"/>	> AADSignInEventsBeta	500121	5
<input type="checkbox"/>	> AADSignInEventsBeta	90094	1
<input type="checkbox"/>	> AADSpnSignInEventsBeta	0	150942
<input type="checkbox"/>	> AADSpnSignInEventsBeta	7000222	91
<input type="checkbox"/>	> AADSpnSignInEventsBeta	7000113	28
<input type="checkbox"/>	> AADUserRiskEvents	User Risk Detection	25
<input type="checkbox"/>	> AuditLogs	Update user	75

Query


```
union withsource=TableName AuditLogs, SigninLogs, AADNonInteractiveUserSignInLogs, AADServicePrincipalSignInLogs,  
AADManagedIdentitySignInLogs, AADRiskyUsers, AADUserRiskEvents, AADServicePrincipalSignInLogs,  
MicrosoftGraphActivityLogs, IdentityLogonEvents, AADSignInEventsBeta, AADSpnSignInEventsBeta  
| extend Action = coalesce(ResultType, OperationName, tostring(ErrorCode), ActionType, RiskDetail)  
| summarize TotalActions = count() by Type
```

```
1 search "rick.astley@kqlquery.com"
2 | summarize Rows = count() by Type
```

Getting started

Results

Query history

↓ Export ▾  Show empty columns

Filters:  Add filter

<input type="checkbox"/>	Type ↑	Rows
<input type="checkbox"/>	> AADNonInteractiveUserSignInLogs	1237
<input type="checkbox"/>	> AADRiskyUsers	6
<input type="checkbox"/>	> AADSignInEventsBeta	1323
<input type="checkbox"/>	> AADUserRiskEvents	9
<input type="checkbox"/>	> AlertEvidence	383
<input type="checkbox"/>	> AuditLogs	24
<input type="checkbox"/>	> BehaviorAnalytics	77
<input type="checkbox"/>	> CloudAppEvents	1498

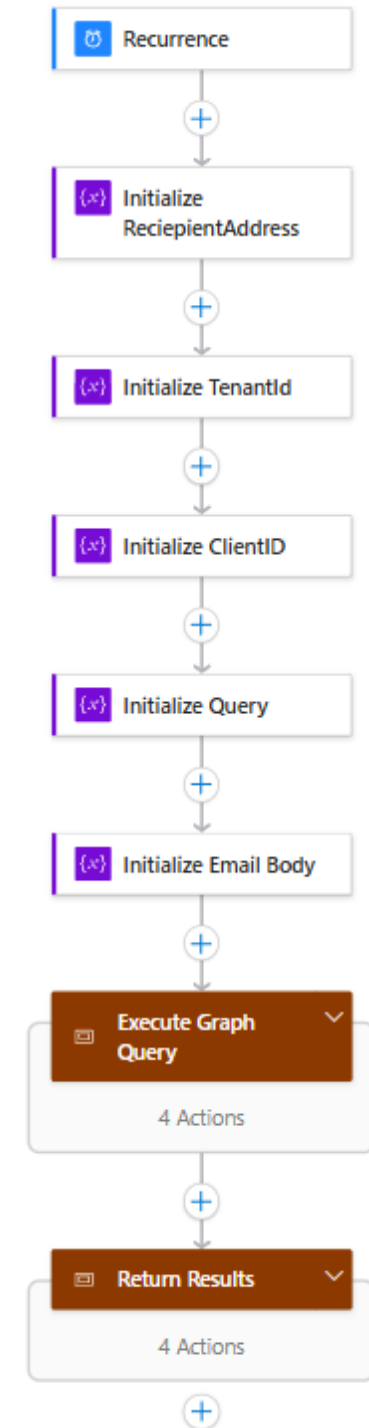
Knowing your data is key to success

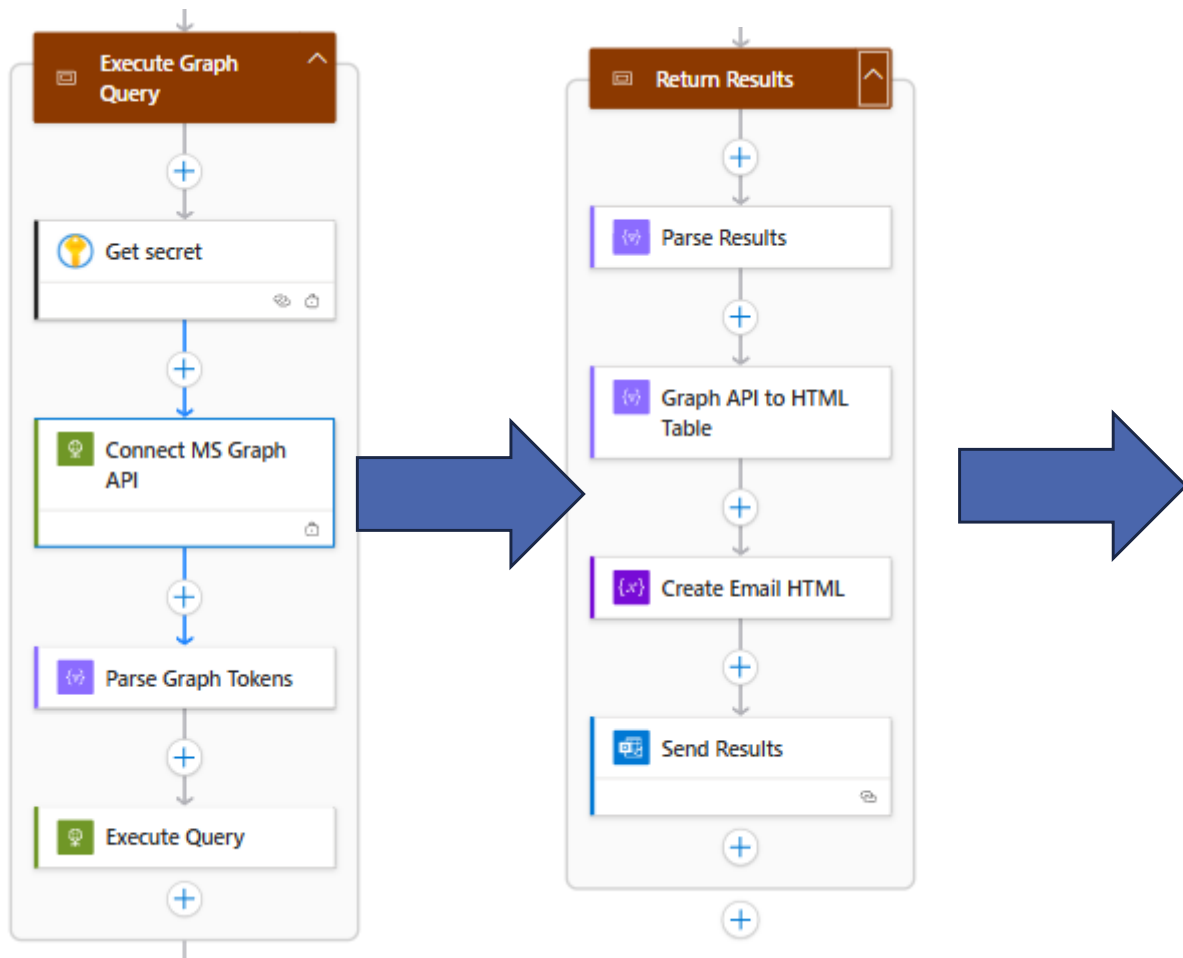
- Knowing which table to use
- Improved efficiency
- Cost optimization
- Discover new reporting potential

Automate the discovery of new logs

Keeping up with all release notes is impossible.

Logic App that runs every week and sends a mail listing all new actions found.





Weekly New Action Types

Bert-Jan Pals
To: Bert-Jan Pals

Mon 9/15/2025 9:45 AM

New Action Types This Week

Here's a summary of new action types added to Unified XDR (Defender XDR and Sentinel) this week.

Table	Action	TotalEntries
AuditLogs	GroupsODatav4_Get	4
AuditLogs	Group_GetDynamicMembershipUserBaseAttributes	1
AuditLogs	Add owner to group	1
AzureActivity	MICROSOFT.POLICYINSIGHTS/REGISTER/ACTION	2
AzureActivity	MICROSOFT.AUTHORIZATION/POLICYASSIGNMENTS/WRITE	2
BehaviorAnalytics	Add owner to group	1
CloudAppEvents	Write ScheduledActions	2
CloudAppEvents	Write PolicyAssignments	4
CloudAppEvents	Write Budgets	2
CloudAppEvents	Rename Microsoft.Subscription	4
CloudAppEvents	RemovableMediaMount	3
CloudAppEvents	Register Microsoft.PolicyInsights	4
CloudAppEvents	CheckNameAvailability Microsoft.CostManagement	2
CloudAppEvents	Add owner to group.	1

Powered by Logic Apps, KQL and Graph API.
© Bert-Jan Pals.

Details:
<https://github.com/Bert-JanP/Sentinel-Automation>
<https://kqlquery.com/posts/monitor-new-actions/>

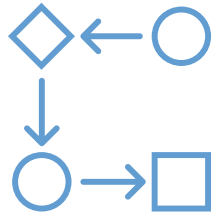
Demo

Now we know what is inside the logs, we can get value from them.

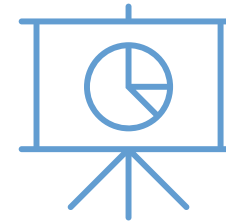
Reporting 101



Collect data



Prepare data

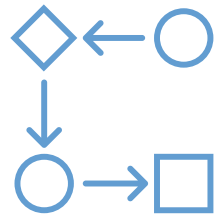


Present data

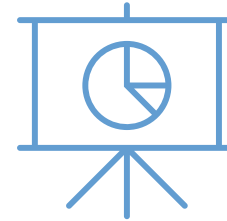
Reporting 101



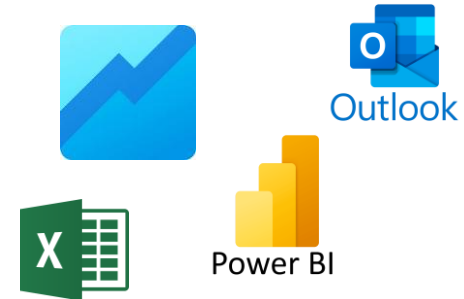
Collect data



Prepare data



Present data



Kusto API Support

Table Category	Azure Monitor API	Graph API	Graph API (Without Unified XDR)	Defender ATP API
Alerts & behaviors	✗	✓	✓	✗
Apps & identities	✗	✓	✓	✗
Email & collaboration	✗	✓	✓	✗
Devices	✗	✓	✓	✓
Defender Vulnerability Management	✗	✓	✓	✓
Email & collaboration	✗	✓	✓	✗
Cloud Infrastructure	✗	✓	✓	✗
Sentinel - Connector Data	✓	✓	✗	✗
Sentinel - Custom Logs	✓	✓	✗	✗

API Permissions

API	Application	Permission	Admin Consent
Azure Monitor API	Log Analytics API	Data.Read	Required
Graph API	Graph	ThreatHunting.Read.AI	Required
Defender ATP API	WindowsDefenderATP	AdvancedQuery.Read.All	Required

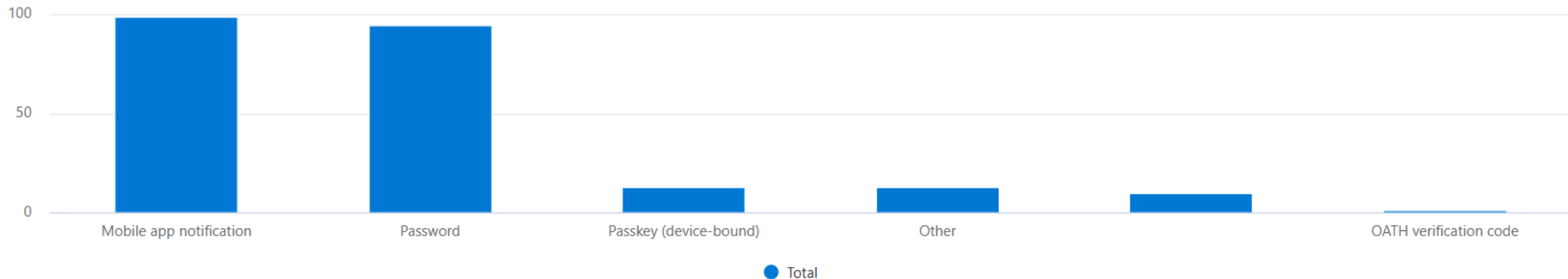
Use cases: Query Logs

Authentication Methods Used

```
1 SigninLogs
2 | where UserType == "Member"
3 | mv-expand todynamic(AuthenticationDetails)
4 | extend AuthenticationMethod = tostring(AuthenticationDetails.authenticationMethod)
5 | where AuthenticationMethod != "Previously satisfied"
6 | summarize Total = count() by AuthenticationMethod
7 | sort by Total
```

Getting started **Results** Query history

🕒 00:01:59 📊 Low ⓘ [Chart type](#) [Full screen](#)



Authentication methods

```
SigninLogs  
| where UserType == "Member"  
| mv-expand todynamic(AuthenticationDetails)  
| extend AuthenticationMethod = tostring(AuthenticationDetails.authenticationMethod)  
| where AuthenticationMethod != "Previously satisfied"  
| summarize Total = count() by AuthenticationMethod  
| sort by Total
```

CA Policy changes

```
1 AuditLogs
2 | where TimeGenerated > ago(90d)
3 | where OperationName has 'conditional access policy'
4 | extend ImpactedPolicy = TargetResources.[0].displayName, Actor = InitiatedBy.user.userPrincipalName
5 | project TimeGenerated, Actor, OperationName, ImpactedPolicy, TargetResources
```

Getting started **Results** Query history

Export Show empty columns

5 items Search

00:01.178 Low Chart type Full screen

Filters: Add filter

<input type="checkbox"/>	TimeGenerated	Actor	OperationName	ImpactedPolicy	TargetResources
<input type="checkbox"/>	> Sep 21, 2025 1:34:...	[REDACTED]@kqlquery.com	Add conditional access policy	Require phishing-resistant multifactor authentication for admins	["id": "c299f89c-0b9c-47...
<input type="checkbox"/>	> Sep 21, 2025 1:35:...	[REDACTED]@kqlquery.com	Add conditional access policy	Block access for unknown or unsupported device platform	["id": "3ba7cdf8-5a6d-4...
<input type="checkbox"/>	> Sep 23, 2025 7:35:...	[REDACTED]@kqlquery.com	Update conditional access policy	Require phishing-resistant multifactor authentication for admins	["id": "c299f89c-0b9c-47...
<input type="checkbox"/>	> Sep 23, 2025 7:35:...	[REDACTED]@kqlquery.com	Delete conditional access policy	Require phishing-resistant multifactor authentication for admins	["id": "c299f89c-0b9c-47...
<input type="checkbox"/>	> Sep 23, 2025 7:35:...	[REDACTED]@kqlquery.com	Add conditional access policy	Securing security info registration	["id": "a3e3dfec-7416-4...

CA Policy changes

AuditLogs

| where TimeGenerated > ago(90d)

| where OperationName has 'conditional access policy'

| extend ImpactedPolicy = TargetResources.[0].displayName, Actor = InitiatedBy.user.userPrincipalName

| project TimeGenerated, Actor, OperationName, ImpactedPolicy, TargetResources

Use cases: Workbooks

Azure Workbooks

The screenshot displays the Azure Workbooks gallery. On the left is a navigation pane with categories like 'Monitoring & health' and 'ID Protection'. The main area shows a 'Gallery' for Microsoft Entra ID with tabs for 'All', 'Workbooks', 'Public Templates', and 'My Templates'. It includes filters for 'Subscription' and 'Resource Group', both set to 'All'. The content is organized into sections: 'Quick start' with 'Empty' and 'Dashboard (Preview)' options; 'Recently modified workbooks (0)' with a 'No items found' message; 'Usage (11)' with 11 workbook tiles; 'Conditional access (5)' with 5 tiles; 'ID Protection (2)' with 2 tiles; and 'Troubleshoot (4)' with 4 tiles. Each tile features a globe icon and a title.

Home >

Gallery

Microsoft Entra ID

+ New Refresh Feedback ? Help Community Git repo Browse across galleries Open recycle bin

All Workbooks Public Templates My Templates

Filter by name or category Subscription : All Resource Group : All Reset filters

Quick start

- Empty: A completely empty workbook.
- Dashboard (Preview): An empty dashboard (preview).

Recently modified workbooks (0)

No items found.

Usage (11)

- Sign-ins using Legacy Aut...
- Sign-ins
- Access Package Activity
- Application Role Assignme...
- App Consent Audit
- Sign-In Analysis (Preview: ...)
- Authentication Prompts A...
Monitor authentication prompts to d...
- Tenant restriction insights
- Cross-tenant access activity
- Phishing-Resistant Passwo...

Conditional access (5)

- Conditional Access Insight...
Monitor the impact of your Condition...
- Continuous access evaluat...
- Sign-ins by Conditional Ac...
- Sign-ins by Grant Controls...
- Conditional Access Gap A...

ID Protection (2)

- ID Protection Risk Analysis
- Impact analysis of risk-bas...

Troubleshoot (4)

- Sensitive Operations Report
- Sign-ins Failure Analysis
- Provisioning Analysis
- Archived Log Date Range

Entra ID Workbooks

Prerequisites

To use Azure Workbooks for Microsoft Entra ID, you need:

A Microsoft Entra tenant with a [Premium P1 license](#)

A Log Analytics workspace *and* access to that workspace

The appropriate roles for Azure Monitor *and* Microsoft Entra ID

Log Analytics workspace

You must create a [Log Analytics workspace](#) *before* you can use Microsoft Entra Workbooks. several factors determine access to Log Analytics workspaces. You need the right roles for the workspace *and* the resources sending the data.

For more information, see [Manage access to Log Analytics workspaces](#).

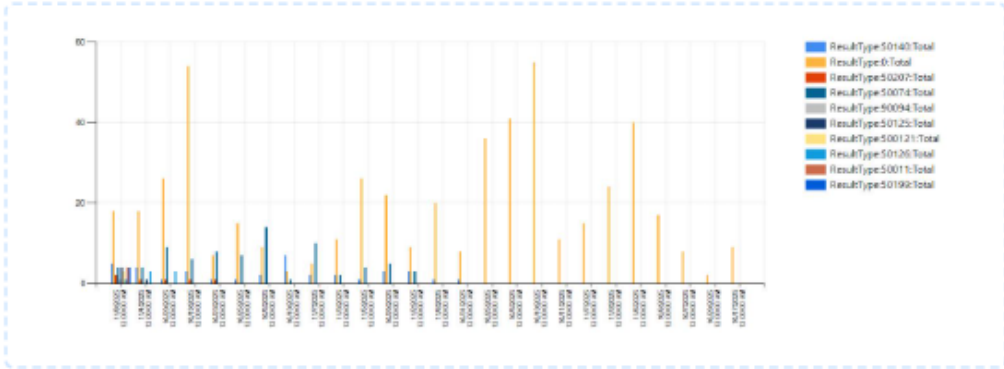
Demo

- **Conditional Access Insights and Reporting**
- **Phishing-Resistant Passwordless Deployment (Preview)**

Use cases: Reports

1. Sign-in activity (bar chart)

This section contains a visual overview of sign-in trends over the reporting period. It highlights successful and failed sign-ins, sign-ins from risky locations, and interactive vs non-interactive sign-ins.



2. Service Principals with Graph ReadWrite permissions added

This section lists service principals that were granted Graph API delegated or application permissions with ReadWrite scope during the reporting period.

TimeGenerated	InitiatedByUserPrincipalName	ActivityDisplayName	AddedPermission	IP	ServicePrincipalAppId
2025-11-08T10:06:52.4546245Z		Add app role assignment to service principal	Application.ReadWrite.All	91.214.67.196	0cad27dc-ec0f-47c7-9a6b-a8a4757687e5
2025-11-08T10:06:52.5256309Z		Add app role assignment to service principal	RoleManagement.ReadWrite.Directory	91.214.67.196	0cad27dc-ec0f-47c7-9a6b-a8a4757687e5
2025-11-08T10:06:52.5946245Z		Add app role assignment to service principal	UserAuthenticationMethod.ReadWrite.All	91.214.67.196	0cad27dc-ec0f-47c7-9a6b-a8a4757687e5

Entra Admin Report

Demo

Conclusion

- There are lots of different logs available
- Almost every action in Entra is logged
- Log data is spread across different tools
- A proactive approach is recommended
- Automate where possible
- Get access to the data relevant to your job

Questions?

Entra ID Queries: <https://github.com/Bert-JanP/Hunting-Queries-Detection-Rules/tree/main/Azure%20Active%20Directory>

OAuthAppInfo Queries: <https://github.com/Bert-JanP/Hunting-Queries-Detection-Rules/tree/main/Defender%20For%20Cloud%20Apps/OAuthAppInfo>

Graph API Endpoints

GraphAPIAuditEvents

| extend ParsedUri = toString(parse_url(RequestUri).Path)

// Normalize Data

| extend GraphAPIPath = tolower(replace_string(ParsedUri, "///", "/"))

// Extract

| extend GraphAPIResource = toString(split(GraphAPIPath, "/")[2])

| project RequestUri, GraphAPIPath, GraphAPIResource

| summarize TotalRequest = count() by GraphAPIResource

| sort by TotalRequest