

KustoCon

Learn | Share | Practice



The Kusto Approach to Unified Audit Log

Bert-Jan Pals

Thanks to our Sponsors

baseVISION

glueck■kanja

water

IT Security & Defense

prospex

KustoWorks

KustoCon
Learn | Share | Practice

Bert-Jan Pals



Background:

5+ years security experience in financial sector

- SOC Lead
- Threat Hunting
- Detection Engineering
- Incident Response
- SOAR/Automation

Defensive Security Expert

Blogs: <https://kqlquery.com>

Tools & Queries: <https://github.com/bert-JanP>



<https://x.com/BertJanCyber>



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

Agenda

- Unified Audit Log 101
- How to get the logs
- UAL Comparison
- UAL Enrichment
- Big Yellow Taxi



Unified Audit Log 101

Unified Audit Log 101

- Centralized repository for M365 user and admin activities
- Exchange, Teams, SharePoint, Azure, OneDrive, Defender XDR

Workloads

Exchange	Microsoft365Defender
OneDrive	SharePoint
MicrosoftTeams	SecurityComplianceCenter
MicrosoftDefenderForIdentity	Copilot
AzureActiveDirectory	CompliancePostureManagement
MicrosoftForms	URBAC
MicrosoftDefenderForEndpoint	Yammer
Planner	Mip
Viva	PublicEndpoint

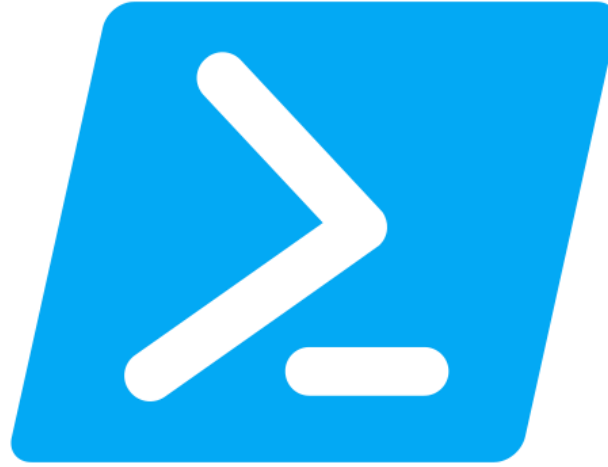
Example Entries

Operation	Workload
MailItemsAccessed	Exchange
New-InboxRule	Exchange
HardDelete	Exchange
Add member to role	Azure
FileAccessed	OneDrive
Search	SharePoint
DownloadOffboardingPkg	Defender XDR

Use Cases

- Incident Response
- Compliance
- Threat Hunting/Detection Engineering
- Reporting

UAL Availability



Purview

1. CloudAppEvents – Defender XDR (Sentinel)

The CloudAppEvents table contains enriched logs from all SaaS applications connected to Microsoft Defender for Cloud Apps

Microsoft 365 Connector required to receive UAL Logs

App Connectors

Microsoft recommends using short-lived access tokens for connecting apps. Atlassian, Egnyte, and Zendesk don't support short-lived tokens today. We recommend renewing the app access token every 6 months and revoking the old access token as a security best practice. Please look at the respective app connection guide for more details.





App connectors provide you with greater visibility and control over your cloud apps.

Filters: Advanced filters

App: **Select apps** App category: **Select category** Connected by: **Select users**

+ Connect an app

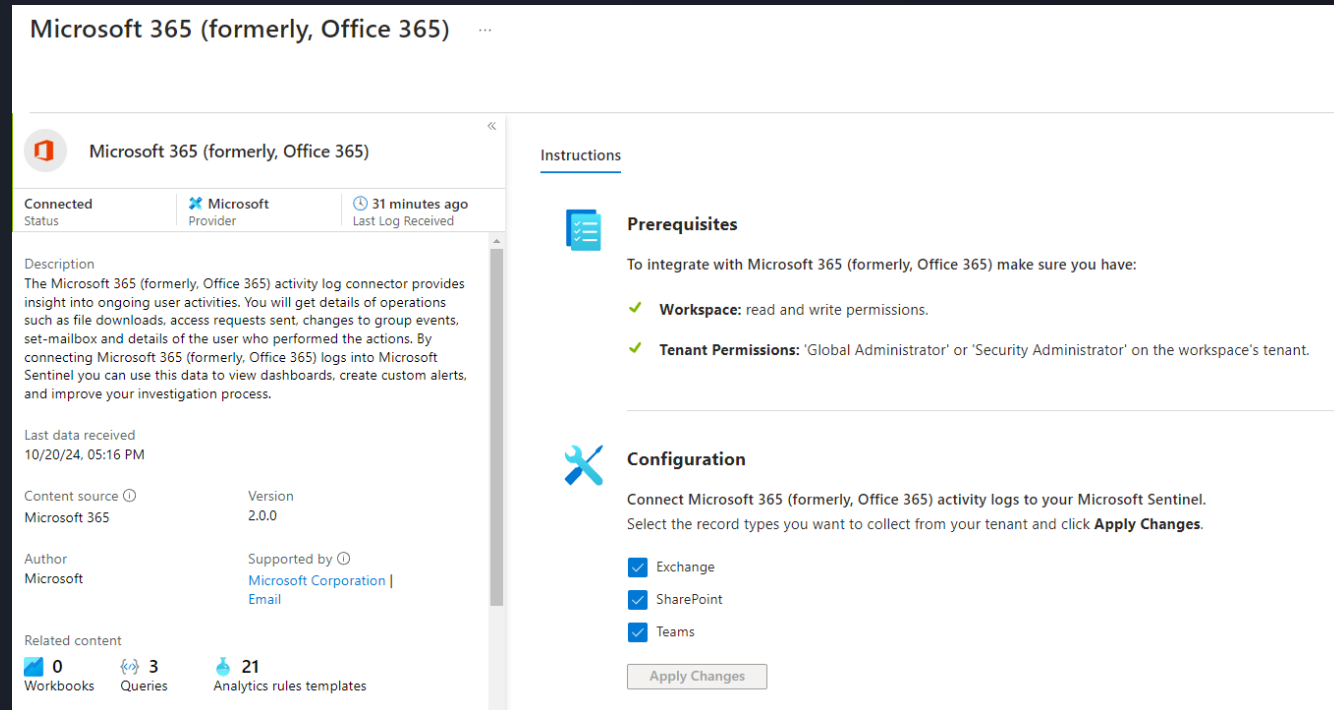
1 - 2 of 2 connected apps [Show details](#) [Hide filters](#) [Table settings](#)

App	Status	Was connected on	Last activity	Accounts
 Microsoft 365 Collaboration	 Connected	May 23, 2024 6:12 PM	Oct 20, 2024 4:37 PM	336
 Microsoft Azure Cloud computing platform	 Connected	May 23, 2024 6:12 PM	Oct 20, 2024 3:55 PM	12

2. OfficeActivity - Sentinel

Audit logs for Office 365 tenants collected by Azure Sentinel. Including Exchange, SharePoint and Teams logs.

Data ingested with Sentinel
Microsoft 365 connector.



The screenshot displays the configuration interface for the Microsoft 365 (formerly, Office 365) connector in Azure Sentinel. The page is divided into two main sections: a left-hand details pane and a right-hand configuration pane.

Left-hand details pane:

- Header:** Microsoft 365 (formerly, Office 365)
- Connected Status:** Microsoft Provider, 31 minutes ago, Last Log Received
- Description:** The Microsoft 365 (formerly, Office 365) activity log connector provides insight into ongoing user activities. You will get details of operations such as file downloads, access requests sent, changes to group events, set-mailbox and details of the user who performed the actions. By connecting Microsoft 365 (formerly, Office 365) logs into Microsoft Sentinel you can use this data to view dashboards, create custom alerts, and improve your investigation process.
- Last data received:** 10/20/24, 05:16 PM
- Content source:** Microsoft 365
- Version:** 2.0.0
- Author:** Microsoft
- Supported by:** Microsoft Corporation | Email
- Related content:** 0 Workbooks, 3 Queries, 21 Analytics rules templates

Right-hand configuration pane:

- Instructions:**
- Prerequisites:** To integrate with Microsoft 365 (formerly, Office 365) make sure you have:
 - ✓ **Workspace:** read and write permissions.
 - ✓ **Tenant Permissions:** 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
- Configuration:** Connect Microsoft 365 (formerly, Office 365) activity logs to your Microsoft Sentinel. Select the record types you want to collect from your tenant and click **Apply Changes**.
 - ☒ Exchange
 - ☒ SharePoint
 - ☒ Teams
- Apply Changes** button

3. Microsoft Extractor Suite



PowerShell module for acquisition of data from Microsoft 365 and Azure for Incident Response and Cyber Security purposes.

```
Microsoft-Extractor-Suite 2.1.0
PS C:\Users\bert-jan> Get-UALAll -StartDate 10/1/2024 -EndDate 10/20/2024
[INFO] Running Get-UALAll
[INFO] Creating the following directory: Output\UnifiedAuditLog\20241020131753
[INFO] Extracting all available audit logs between 2024-10-01T00:00:00Z and 2024-10-20T00:00:00Z
[INFO] Found 891 audit logs between 2024-10-01T00:00:00Z and 2024-10-01T12:00:00Z
[INFO] Successfully retrieved 891 records out of total 891 for the current time range. Moving on!
[INFO] Found 12 audit logs between 2024-10-01T12:00:00Z and 2024-10-02T00:00:00Z
[INFO] Successfully retrieved 12 records out of total 12 for the current time range. Moving on!
[INFO] Found 889 audit logs between 2024-10-02T00:00:00Z and 2024-10-02T12:00:00Z
[INFO] Successfully retrieved 889 records out of total 889 for the current time range. Moving on!
[INFO] Found 114 audit logs between 2024-10-02T12:00:00Z and 2024-10-03T00:00:00Z
[INFO] Successfully retrieved 114 records out of total 114 for the current time range. Moving on!
[INFO] Found 948 audit logs between 2024-10-03T00:00:00Z and 2024-10-03T12:00:00Z
[INFO] Successfully retrieved 948 records out of total 948 for the current time range. Moving on!
[INFO] Found 43 audit logs between 2024-10-03T12:00:00Z and 2024-10-04T00:00:00Z
[INFO] Successfully retrieved 43 records out of total 43 for the current time range. Moving on!
[INFO] Found 892 audit logs between 2024-10-04T00:00:00Z and 2024-10-04T12:00:00Z
[INFO] Successfully retrieved 892 records out of total 892 for the current time range. Moving on!
[INFO] Found 21 audit logs between 2024-10-04T12:00:00Z and 2024-10-05T00:00:00Z
[INFO] Successfully retrieved 21 records out of total 21 for the current time range. Moving on!
[INFO] Found 889 audit logs between 2024-10-05T00:00:00Z and 2024-10-05T12:00:00Z
[INFO] Successfully retrieved 889 records out of total 889 for the current time range. Moving on!
[INFO] Found 10 audit logs between 2024-10-05T12:00:00Z and 2024-10-06T00:00:00Z
[INFO] Successfully retrieved 10 records out of total 10 for the current time range. Moving on!
[INFO] Found 895 audit logs between 2024-10-06T00:00:00Z and 2024-10-06T12:00:00Z
[INFO] Successfully retrieved 895 records out of total 895 for the current time range. Moving on!
[INFO] Found 11 audit logs between 2024-10-06T12:00:00Z and 2024-10-07T00:00:00Z
[INFO] Successfully retrieved 11 records out of total 11 for the current time range. Moving on!
[INFO] Found 895 audit logs between 2024-10-07T00:00:00Z and 2024-10-07T12:00:00Z
[INFO] Successfully retrieved 895 records out of total 895 for the current time range. Moving on!
```

Microsoft Extractor Suite Download: <https://github.com/invictus-ir/Microsoft-Extractor-Suite>
Invictus IR: <https://www.invictus-ir.com/>

Microsoft Extractor Suite



bert-jan > Output > UnifiedAuditLog > 20241020131753				
<input type="checkbox"/> Name	Date modified	Type	Size	
UAL-20241001000000.csv	10/20/2024 1:18 PM	CSV File	1,112 KB	
UAL-20241001120000.csv	10/20/2024 1:18 PM	CSV File	14 KB	
UAL-20241002000000.csv	10/20/2024 1:18 PM	CSV File	1,108 KB	
UAL-20241002120000.csv	10/20/2024 1:18 PM	CSV File	111 KB	
UAL-20241003000000.csv	10/20/2024 1:18 PM	CSV File	1,183 KB	
UAL-20241003120000.csv	10/20/2024 1:19 PM	CSV File	75 KB	
UAL-20241004000000.csv	10/20/2024 1:19 PM	CSV File	1,100 KB	
UAL-20241004120000.csv	10/20/2024 1:19 PM	CSV File	32 KB	
UAL-20241005000000.csv	10/20/2024 1:19 PM	CSV File	1,089 KB	
UAL-20241005120000.csv	10/20/2024 1:19 PM	CSV File	13 KB	
UAL-20241006000000.csv	10/20/2024 1:19 PM	CSV File	1,099 KB	
UAL-20241006120000.csv	10/20/2024 1:19 PM	CSV File	16 KB	
UAL-20241007000000.csv	10/20/2024 1:19 PM	CSV File	1,106 KB	
UAL-20241007120000.csv	10/20/2024 1:19 PM	CSV File	83 KB	
UAL-20241008000000.csv	10/20/2024 1:20 PM	CSV File	1,203 KB	
UAL-20241008120000.csv	10/20/2024 1:20 PM	CSV File	1,421 KB	
UAL-20241009000000.csv	10/20/2024 1:20 PM	CSV File	118 KB	
UAL-20241009120000.csv	10/20/2024 1:20 PM	CSV File	934 KB	
UAL-20241010000000.csv	10/20/2024 1:20 PM	CSV File	10 KB	
UAL-20241010120000.csv	10/20/2024 1:20 PM	CSV File	957 KB	
UAL-20241011000000.csv	10/20/2024 1:21 PM	CSV File	12 KB	
UAL-20241011120000.csv	10/20/2024 1:21 PM	CSV File	937 KB	
UAL-20241012000000.csv	10/20/2024 1:21 PM	CSV File	15 KB	

I want to query the CSVs with KQL

Connections

+ Add

★ Favorites

FreeCluster

Demo

UAL_ExtractorSuite_Invictus

1 UAL_ExtractorSuite_Invictus

2 summarize Total = count() by Operations

Table 1

+ Add visual

Stats

Operations	Total
MDCRegulatoryComplianceAssessments	15,060
MDCAssessments	1,681
Search	842
MailItemsAccessed	460
UserLoggedIn	331
Validate	191
FileSyncUploadedFull	164
Set-MailboxPlan	135
GATFRTOKENIssue	121
Set-Mailbox	117
FileModifiedExtended	108
FileAccessed	56
Get-AutoSensitivityLabelPolicy	54
Get-LabelPolicy	52

> help



Azure Data Explorer

Not good enough (yet)!



Query
the UAL
from ADX



Query
ADX data
from Sentinel

Query ADX Data From Sentinel

Microsoft Sentinel | Logs

Selected workspace: 'sentinel'

Search

Log Analytics Try the new Log Analytics Feedback Queries

Log Analytics Run Time range : Last 24 hours Save Share New alert rule Export Pin to Format query

Log Analytics Schema and Filter

```
1 let StartTime = datetime(10/1/2024);
2 let EndTime = datetime(10/20/2024);
3 let UAL_ExtractorSuite_Invictus_Events = adx("https://kvc-8mgx1d5be7e559uecb.northeurope.kusto.windows.net/Demo").UAL_ExtractorSuite_Invictus
4 | where CreationDate between(StartTime .. EndTime)
5 | distinct Operation = Operations
6 | extend DataSource = "ExtractorSuite_InvictusIR";
7 UAL_ExtractorSuite_Invictus_Events
```

Results Chart Add bookmark

<input type="checkbox"/> DataSource	Operation
<input type="checkbox"/> > ExtractorSuite_InvictusIR	MDCRegulatoryComplianceAssessments
<input type="checkbox"/> > ExtractorSuite_InvictusIR	MDCAssessments
<input type="checkbox"/> > ExtractorSuite_InvictusIR	Search
<input type="checkbox"/> > ExtractorSuite_InvictusIR	MailItemsAccessed
<input type="checkbox"/> > ExtractorSuite_InvictusIR	UserLoggedIn
<input type="checkbox"/> > ExtractorSuite_InvictusIR	Validate
<input type="checkbox"/> > ExtractorSuite_InvictusIR	FileSyncUploadedFull
<input type="checkbox"/> > ExtractorSuite_InvictusIR	Set-MailboxPlan
<input type="checkbox"/> > ExtractorSuite_InvictusIR	GATFRTOKENIssue
<input type="checkbox"/> > ExtractorSuite_InvictusIR	Set-Mailbox
<input type="checkbox"/> > ExtractorSuite_InvictusIR	FileModifiedExtended
<input type="checkbox"/> > ExtractorSuite_InvictusIR	FileAccessed

4. Purview Audit Search

Audit

[New Search](#) [Audit retention policies](#)

Searches completed: 2 | Active searches: 0 | Active unfiltered searches: 0

Date and time range (UTC) *

Start: Oct 30 2024 00:00

End: Oct 31 2024 00:00

Keyword Search

Enter the keyword to search for

Admin Units

Choose which Admin Units to search for

Activities - friendly names

Choose which activities to search for

Activities - operation names

Enter operation values, separated by commas

Record Types

Select the record types to search for

Search name

Give the search a name

Users

Add the users whose audit logs you want to search

File, folder, or site

Enter all or a part of the name of a file, website, or folder

Workloads

Enter the workloads to search for

Search **Clear all**

Copy this search Delete Refresh

6 items

Search name	Job status	Progress (%)	Search time	Total results	Creation time	Search performed by
<input type="checkbox"/> KustoCon - UAL	Completed	100%	4m, 38s	29066	Oct 31, 2024 7:31 P...	bert-jan@kqlquery.com
<input type="checkbox"/> Oct 1 - Oct 31	Cancelled	0%	1m, 52s	0	Oct 31, 2024 7:20 P...	bert-jan@kqlquery.com

<https://learn.microsoft.com/en-us/purview/audit-search?tabs=microsoft-purview-portal>

<https://github.com/PuravsPoint/DecipheringUAL/tree/main>

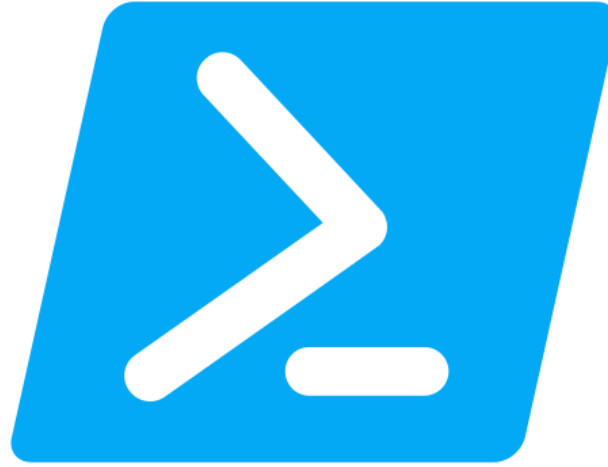
Demo time: UAL Comparison



Differences

<input type="checkbox"/> Workload ↑↓	Defender For Cloud Apps	ExtractorSuite_InvictusIR	Sentinel OfficeActivity	UAL_Audit_Search
<input type="checkbox"/> > AzureActiveDirectory	35	37	0	37
<input type="checkbox"/> > CompliancePostureManagement	2	2	0	2
<input type="checkbox"/> > Copilot	1	1	0	1
<input type="checkbox"/> > Exchange	19	33	33	33
<input type="checkbox"/> > Microsoft365Defender	10	10	0	10
<input type="checkbox"/> > MicrosoftDefenderForEndpoint	8	8	0	8
<input type="checkbox"/> > MicrosoftDefenderForIdentity	12	12	0	12
<input type="checkbox"/> > MicrosoftForms	7	7	0	7
<input type="checkbox"/> > MicrosoftTeams	12	13	11	13
<input type="checkbox"/> > Mip	1	1	0	1
<input type="checkbox"/> > OneDrive	25	25	25	25
<input type="checkbox"/> > Planner	1	1	0	1
<input type="checkbox"/> > PublicEndpoint	2	2	0	2
<input type="checkbox"/> > SecurityComplianceCenter	24	24	0	24
<input type="checkbox"/> > SharePoint	13	16	16	16
<input type="checkbox"/> > URBAC	5	5	0	5
<input type="checkbox"/> > Yammer	2	2	0	2

**UAL =
Unaligned
Activity
Logs**



Purview

Differences

Different schema used for the logs.

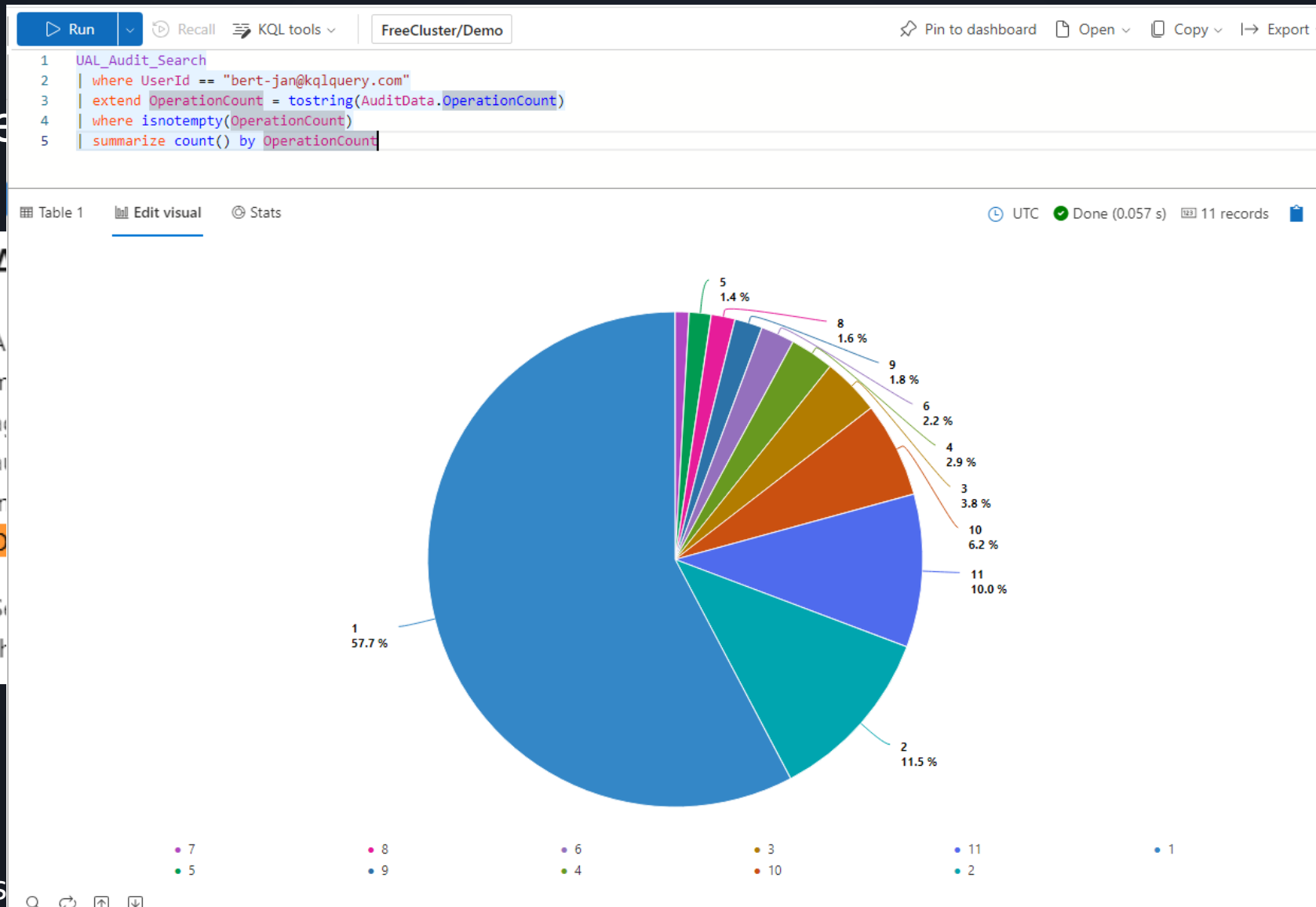
Example: OperationCount

Included	Excluded
ExtractorSuite_Invictus_UAL	OfficeActivity
UAL_Audit_Search	
CloudAppEvents	

Details matter

For Three

nse



Details matter

OfficeActivity

| where Operation == "MailItemsAccessed"

| extend MailAccessType =
parse_json(OperationProperties[o]).Value, IsThrottled
= parse_json(OperationProperties[1]).Value

<input type="checkbox"/>	TimeGenerated [UTC]	MailAccessType ↑↓	IsThrottled	RecordType	Operation
<input type="checkbox"/>	> 11/5/2024, 7:01:02.000 PM	Sync	False	ExchangeItem	MailItemsAccessed
<input type="checkbox"/>	> 11/5/2024, 7:01:02.000 PM	Sync	False	ExchangeItem	MailItemsAccessed
<input type="checkbox"/>	> 11/5/2024, 7:01:02.000 PM	Sync	False	ExchangeItem	MailItemsAccessed
<input type="checkbox"/>	> 11/5/2024, 7:00:55.000 PM	Sync	False	ExchangeItem	MailItemsAccessed
<input type="checkbox"/>	> 11/7/2024, 5:07:11.000 AM	Bind	False	50	MailItemsAccessed
<input type="checkbox"/>	> 11/7/2024, 5:07:11.000 AM	Bind	False	50	MailItemsAccessed
<input type="checkbox"/>	> 11/7/2024, 5:07:10.000 AM	Bind	False	50	MailItemsAccessed

Bind & Sync access details: <https://learn.microsoft.com/en-us/purview/audit-log-investigate-accounts?view=o365-worldwide#auditing-sync-access>



Differences Data Availability

Active querying:

- OfficeActivity
- CloudAppEvents

Data acquisition needed:

- Purview Search
- Microsoft Extractor Suite

Enrichment

Enrich email information



EmailEvents



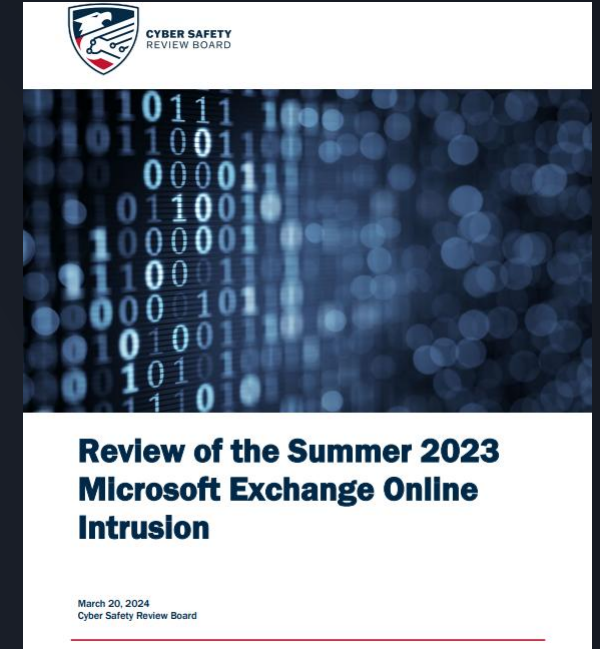
MailItemsAccessed

Big Yellow Taxi



Big Yellow Taxi

State Department was the first victim to discover the intrusion when, on June 15, 2023, State's security operations center (SOC) detected anomalies in access to its mail systems. **The next day, State observed multiple security alerts from a custom rule it had created, known internally as "Big Yellow Taxi," that analyzes data from a log known as MailItemsAccessed, which tracks access to Microsoft Exchange Online mailboxes.**



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

```

let DefaultInboxFolders = pack_array("Inbox", "Drafts", "Sent Items", "Archive", "rss", "Inbox", "Deleted Items", "Junk Email");
let BinSize = 30m;
let TimeFrame = 14d;

OfficeActivity

// List all MailItemsAccessed that are created because of a sync audit activity.

// The audit volume for sync operations is huge. So, instead of generating an audit record for each mail item that's synched, we generate an audit event for the mail
folder containing items that were synched and assume that all mail items in the synched folder have been compromised.

// Info: https://learn.microsoft.com/en-us/purview/audit-log-investigate-accounts?view=0365-worldwide#auditing-sync-access

| where Operation == "MailItemsAccessed"
| extend MailAccessType = tostring(parse_json(OperationProperties[0]).Value), IsThrottled = tostring(parse_json(OperationProperties[1]).Value)
| where MailAccessType == "Sync"

// Parse synchronised folders. All FolderNames should be considered compromised.
| extend ParentFolder = parse_json(Item).ParentFolder
| extend SyncedFolder = tostring(ParentFolder.Name), Path = tostring(ParentFolder.Path)
| summarize TotalFolders = dcount(SyncedFolder), Folders = make_set(SyncedFolder) by bin(TimeGenerated, BinSize), UserId, Client_IPAddress, MailboxGuid

// Filter & enrich results
| where TotalFolders >= array_length(DefaultInboxFolders)
| extend GeoIPInfo = geo_info_from_ip_address(Client_IPAddress)
| extend country = tostring(parse_json(GeoIPInfo).country)

| join kind=leftouter (SigninLogs | where TimeGenerated > startofday(ago(TimeFrame)) | project ResultType, UserPrincipalName, IPAddress | summarize TotalSuccess
= countif(ResultType == 0), TotalFailed = countif(ResultType != 0) by UserPrincipalName, IPAddress) on $left.Client_IPAddress == $right.IPAddress, $left.UserId ==
$right.UserPrincipalName

```

UAL & Defender XDR

The screenshot displays the Microsoft Sentinel 'Endpoints' configuration page. The left sidebar contains navigation links: Microsoft Sentinel, Identities, Endpoints, Email & collaboration, Cloud apps, SOC optimization, Reports, Learning hub, Trials, More resources, System, Audit, Permissions, Health, Settings, and Customize navigation. The main content area is titled 'Endpoints' and features a left-hand menu with sections: General (Advanced features, Licenses, Email notifications, Auto remediation), Permissions (Roles, Device groups), APIs (SIEM), and Rules (Alert suppression, Deception rules, Indicators). The 'Advanced features' section is active, showing four settings: 'Unified audit log' (On), 'Device discovery' (On), 'Download quarantined files' (On), and 'Default to streamlined connectivity when onboarding devices in Defender portal' (Off). Each setting includes a descriptive paragraph and a 'Save preferences' button at the bottom.

Microsoft Sentinel

- Identities
- Endpoints
- Email & collaboration
- Cloud apps
- SOC optimization
- Reports
- Learning hub
- Trials
- More resources
- System
- Audit
- Permissions
- Health
- Settings
- Customize navigation

Endpoints

- General**
 - Advanced features**
 - Licenses
 - Email notifications
 - Auto remediation
- Permissions**
 - Roles
 - Device groups
- APIs**
 - SIEM
- Rules**
 - Alert suppression
 - Deception rules
 - Indicators

Unified audit log (On)

Block access to websites containing unwanted content and track web activity across all domains. To specify the web content categories you want to block, create a [web content filtering policy](#). Ensure you have network protection in block mode when deploying the [Microsoft Defender for Endpoint security baseline](#).

Device discovery (On)

Allows onboarded devices to discover unmanaged devices in your network and assess vulnerabilities and risks. For more information, see [Device discovery settings](#) to configure discovery settings.

Download quarantined files (On)

Backup quarantined files in a secure and compliant location so they can be downloaded directly from quarantine.

Default to streamlined connectivity when onboarding devices in Defender portal (Off)

With streamlined connectivity, devices connect to fewer URLs and static IPs. You'll still be able to select standard connectivity. [Learn about streamlined connectivity](#)

ⓘ To avoid service connectivity issues, update devices and ensure they can connect to *.endpoint.security.microsoft.com before onboarding. [View requirements](#)

Save preferences

CloudAppEvents

```
| extend WorkLoad =  
tostring(parse_json(RawEventData).Workload)  
| where WorkLoad contains "Defender"  
| distinct ActionType
```


Conclusion

- UAL logs are powerful
- Use this data source proactive
- Be aware of the differences in logged UAL activities
- Data acquisition is worth it, especially if you can narrow the search

Thanks to our Sponsors

baseVISION

glueck■kanja

water

IT Security & Defense

prospex

KustoWorks

KustoCon
Learn | Share | Practice

Q&A

Thank you!



<https://x.com/BertJanCyber>



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

Blogs: <https://kqlquery.com>

Tools & Queries: <https://github.com/bert-JanP>

KustoCon
Learn | Share | Practice