Session 8 | Session Title

KQL|Cafe

Session 8 | Session Title

Your | hosts

Alex Verboon

https://twitter.com/alexverboon

https://www.linkedin.com/in/verboonalex/

https://github.com/alexverboon

https://www.verboon.info/

MVP Microsoft® Most Valuable Professional

Gianni Castaldi

https://twitter.com/castello_johnny

https://www.linkedin.com/in/giannicastaldi/

https://github.com/KustoKing

https://www.kustoking.com/

Today’s | Guest

Mattias Borg

NinjaCat | Trusted Cyber Security Advisor | Onevinn

My blog: https://blog.sec-labs.com/
LinkedIn Profile: https://www.linkedin.com/in/matteborg82
Twitter: https://twitter.com/MattiasBorg82

Show | Agenda

Welcome

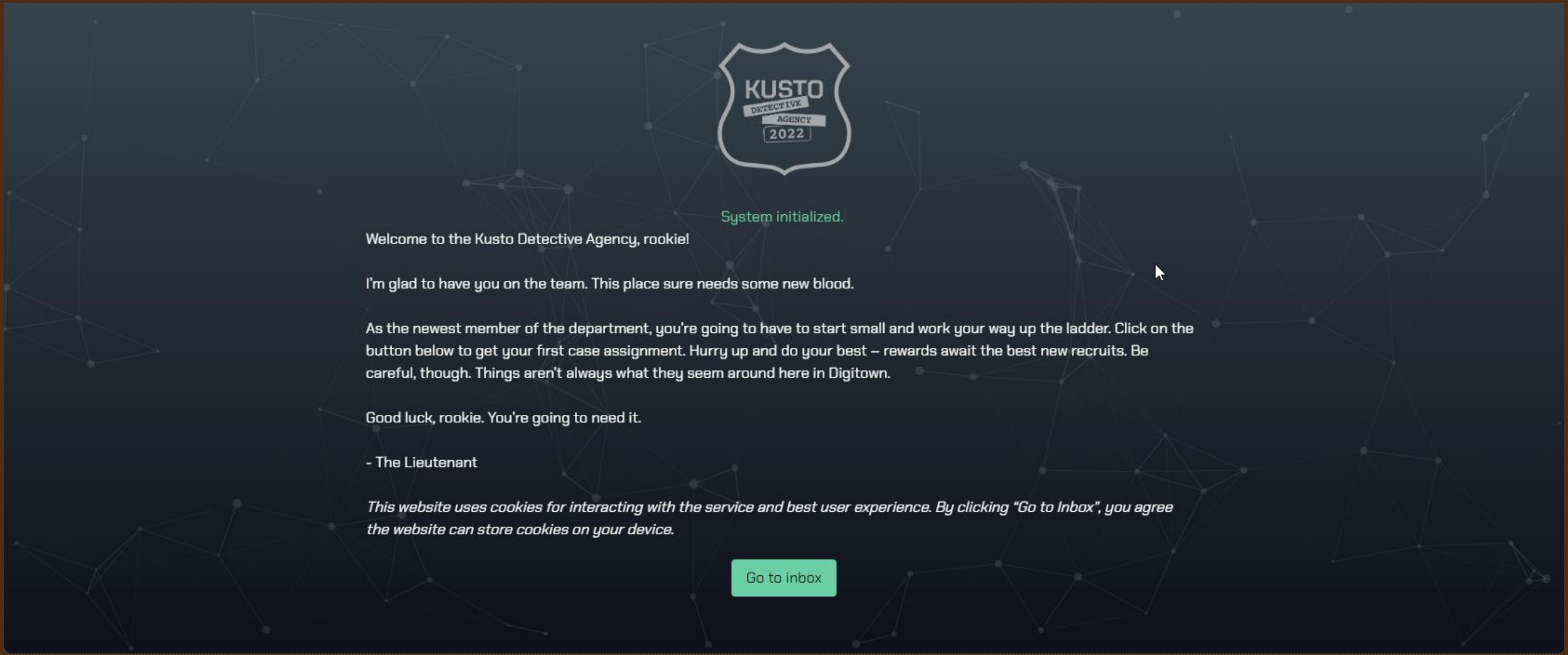
What's new in KQL

Learning KQL

Our KQL Guest

What did you do with KQL this month?

Kusto Detective - https://detective.kusto.io/



System initialized.

Welcome to the Kusto Detective Agency, rookie!

I'm glad to have you on the team. This place sure needs some new blood.

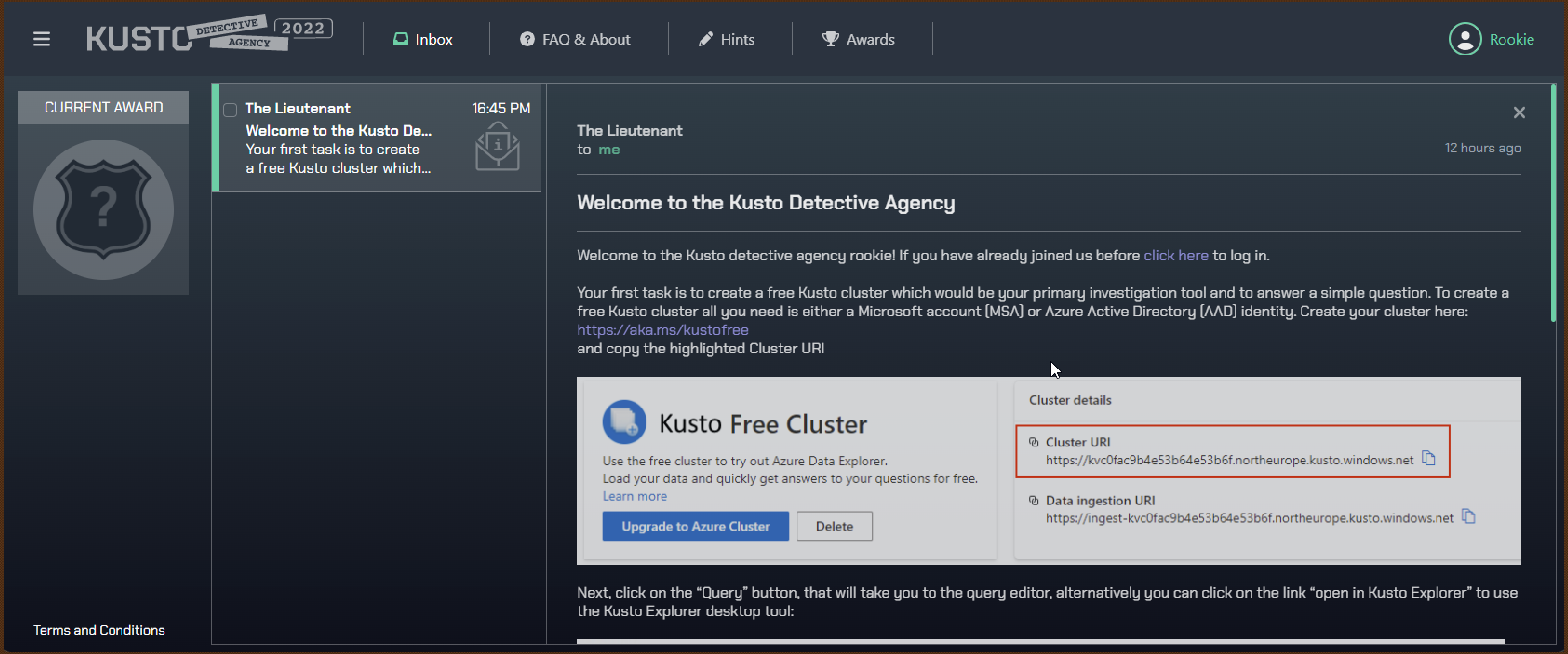
As the newest member of the department, you're going to have to start small and work your way up the ladder. Click on the button below to get your first case assignment. Hurry up and do your best – rewards await the best new recruits. Be careful, though. Things aren't always what they seem around here in Digitown.

Good luck, rookie. You're going to need it.

- The Lieutenant

This website uses cookies for interacting with the service and best user experience. By clicking “Go to Inbox”, you agree the website can store cookies on your device.

What’s new in KQL



□ **The Lieutenant** 16:45 PM
Welcome to the Kusto De...
Your first task is to create
a free Kusto cluster which...

The Lieutenant
to me
12 hours ago

Welcome to the Kusto Detective Agency

Welcome to the Kusto detective agency rookie! If you have already joined us before click here to log in.

Your first task is to create a free Kusto cluster which would be your primary investigation tool and to answer a simple question. To create a free Kusto cluster all you need is either a Microsoft account (MSA) or Azure Active Directory (AAD) identity. Create your cluster here:
https://aka.ms/kustofree
and copy the highlighted Cluster URI

Kusto Free Cluster

Use the free cluster to try out Azure Data Explorer.
Load your data and quickly get answers to your questions for free.
Learn more

Upgrade to Azure Cluster | Delete

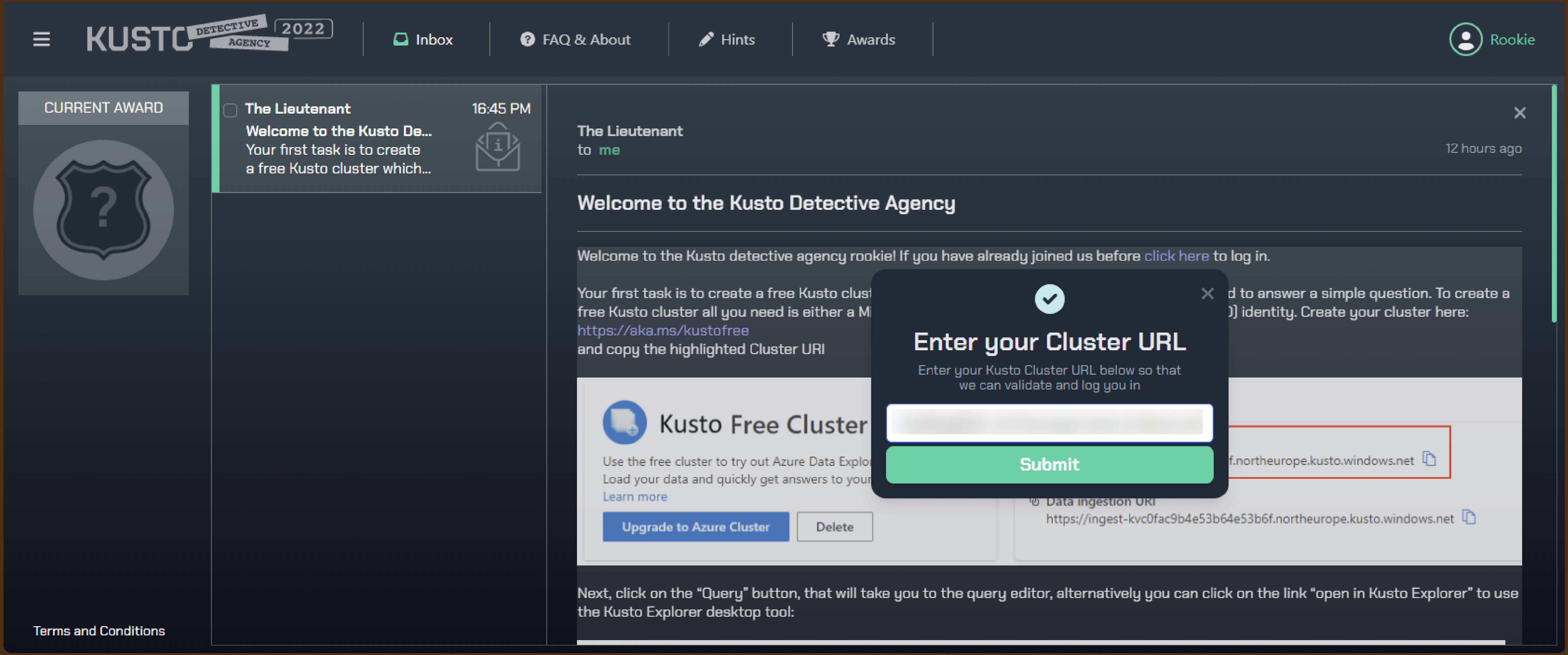
Cluster details

Cluster URI
https://kvc0fac9b4e53b64e53b6f.northeurope.kusto.windows.net

Data ingestion URI
https://ingest-kvc0fac9b4e53b64e53b6f.northeurope.kusto.windows.net

Next, click on the “Query” button, that will take you to the query editor, alternatively you can click on the link “open in Kusto Explorer” to use the Kusto Explorer desktop tool:

What’s new in KQL



The Lieutenant 16:45 PM
Welcome to the Kusto De...
Your first task is to create a free Kusto cluster which...

The Lieutenant
to me

12 hours ago

Welcome to the Kusto Detective Agency

Welcome to the Kusto detective agency rookie! If you have already joined us before click here to log in.

Your first task is to create a free Kusto clust d to answer a simple question. To create a free Kusto cluster all you need is either a Mi)] identity. Create your cluster here:
https://aka.ms/kustofree
and copy the highlighted Cluster URI

Use the free cluster to try out Azure Data Explor
Load your data and quickly get answers to your
Learn more

f.northeurope.kusto.windows.net

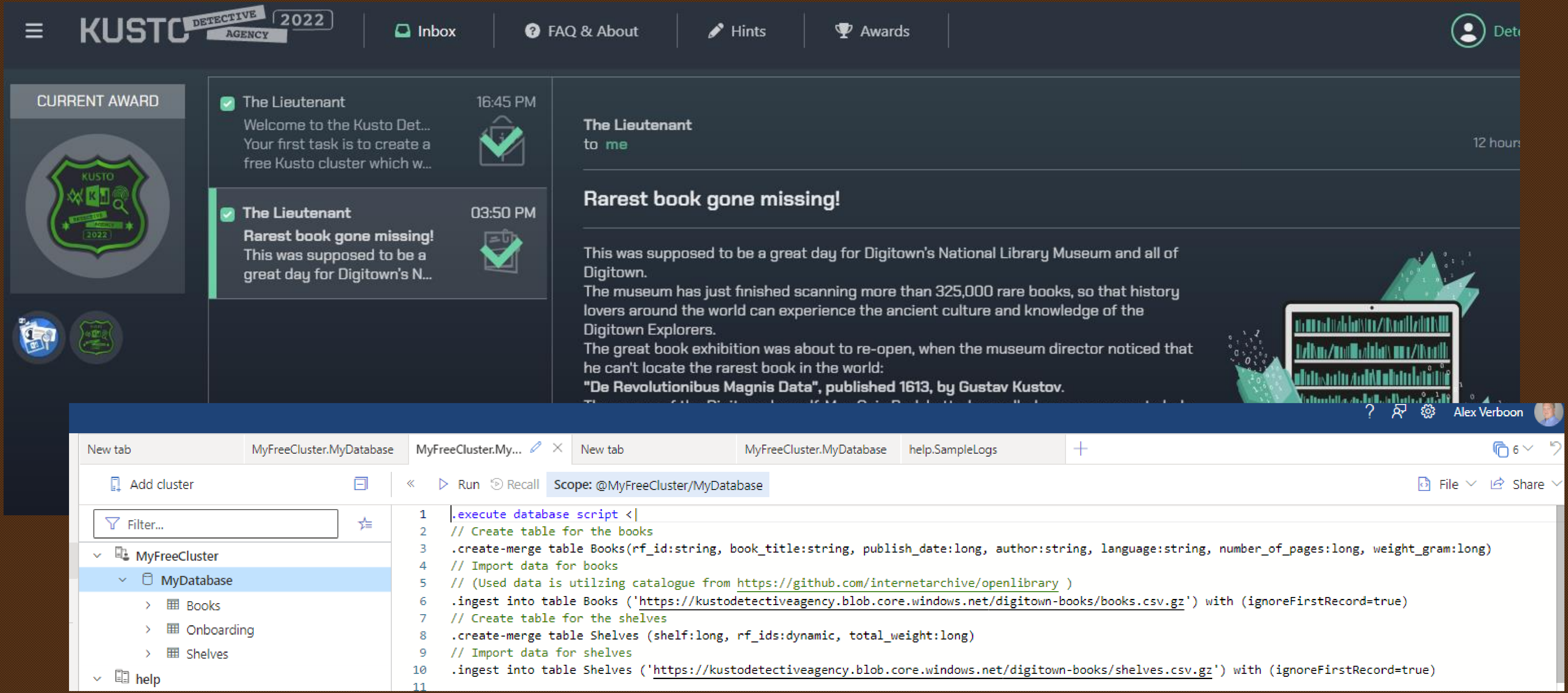
Data ingestion URI
https://ingest-kvc0fac9b4e53b64e53b6f.northeurope.kusto.windows.net

Next, click on the “Query” button, that will take you to the query editor, alternatively you can click on the link “open in Kusto Explorer” to use the Kusto Explorer desktop tool:

Enter your Cluster URL

Enter your Kusto Cluster URL below so that we can validate and log you in

What’s new in KQL



The Lieutenant 16:45 PM
Welcome to the Kusto Det...
Your first task is to create a free Kusto cluster which w...

The Lieutenant 03:50 PM
Rarest book gone missing!
This was supposed to be a great day for Digitown's N...

The Lieutenant
to me
12 hours

Rarest book gone missing!

This was supposed to be a great day for Digitown's National Library Museum and all of Digitown.
The museum has just finished scanning more than 325,000 rare books, so that history lovers around the world can experience the ancient culture and knowledge of the Digitown Explorers.
The great book exhibition was about to re-open, when the museum director noticed that he can't locate the rarest book in the world:
"De Revolutionibus Magnis Data", published 1613, by Gustav Kustov.

```
.execute database script <|
// Create table for the books
.create-merge table Books(rf_id:string, book_title:string, publish_date:long, author:string, language:string, number_of_pages:long, weight_gram:long)
// Import data for books
// (Used data is utilzing catalogue from https://github.com/internetarchive/openlibrary )
.ingest into table Books ('https://kustodetectiveagency.blob.core.windows.net/digitown-books/books.csv.gz') with (ignoreFirstRecord=true)
// Create table for the shelves
.create-merge table Shelves (shelf:long, rf_ids:dynamic, total_weight:long)
// Import data for shelves
.ingest into table Shelves ('https://kustodetectiveagency.blob.core.windows.net/digitown-books/shelves.csv.gz') with (ignoreFirstRecord=true)
```

What’s new in KQL

Kusto Detective

Scan operator Revisited

Suspicious executables

Get one execution

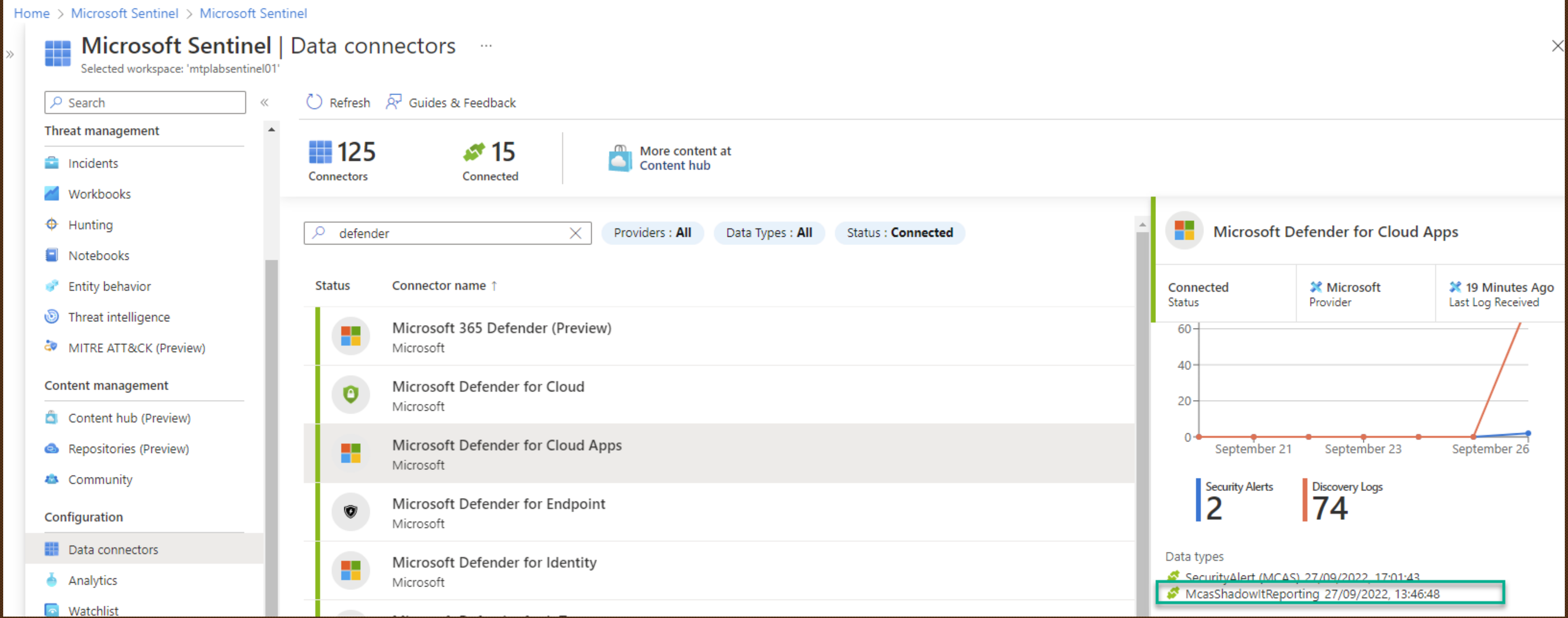
Show all

Getting starting with hunting

| Mattias Borg

How do we start?

Microsoft Defender for Cloud Apps - McasShadowItReporting



Microsoft Sentinel | Data connectors ···

Selected workspace: 'mtplabsentinel01'

125 Connectors

15 Connected

defender

Providers : **All**   Data Types : **All**   Status : **Connected**

Status	Connector name ↑
	Microsoft 365 Defender (Preview) Microsoft
	Microsoft Defender for Cloud Microsoft
	Microsoft Defender for Cloud Apps Microsoft
	Microsoft Defender for Endpoint Microsoft
	Microsoft Defender for Identity Microsoft

Microsoft Defender for Cloud Apps

Connected	Microsoft	19 Minutes Ago
Status	Provider	Last Log Received

Security Alerts 2

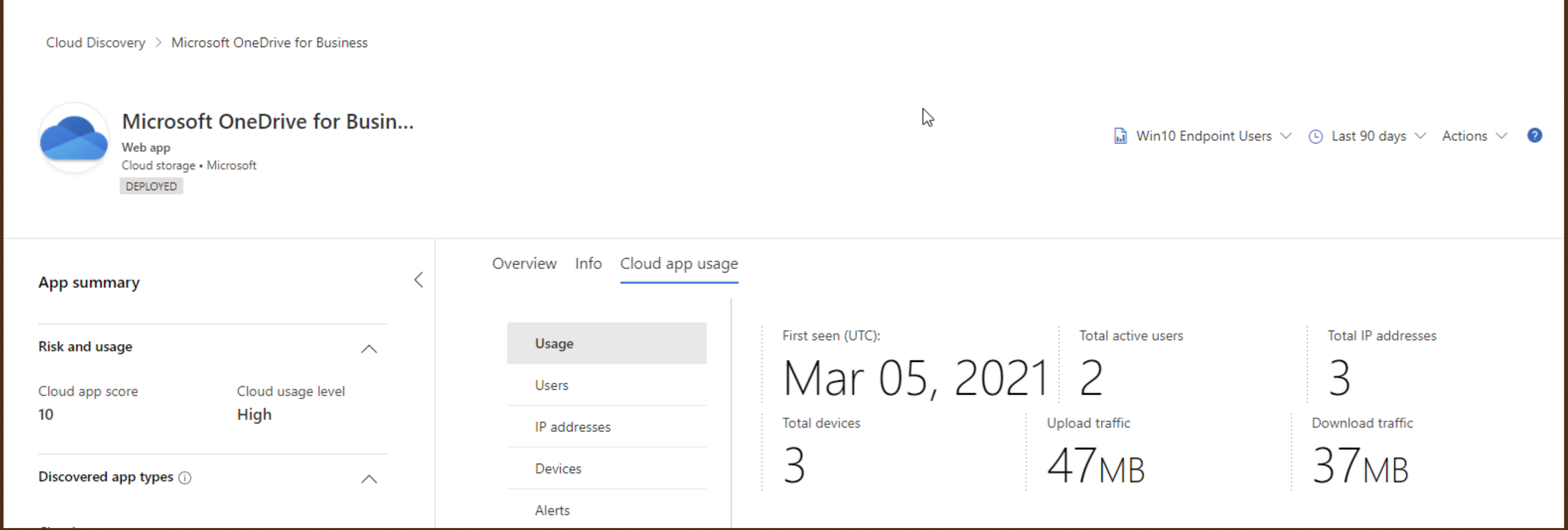
Discovery Logs 74

Data types

SecurityAlert (MCAS) 27/09/2022, 17:01:43

McasShadowItReporting 27/09/2022, 13:46:48

Microsoft Defender for Cloud Apps - McasShadowItReporting



Cloud Discovery > Microsoft OneDrive for Business

Microsoft OneDrive for Busin...

Web app

Cloud storage • Microsoft

DEPLOYED

Win10 Endpoint Users | Last 90 days | Actions

App summary

Risk and usage

Cloud app score: 10

Cloud usage level: High

Discovered app types

First seen (UTC): Mar 05, 2021

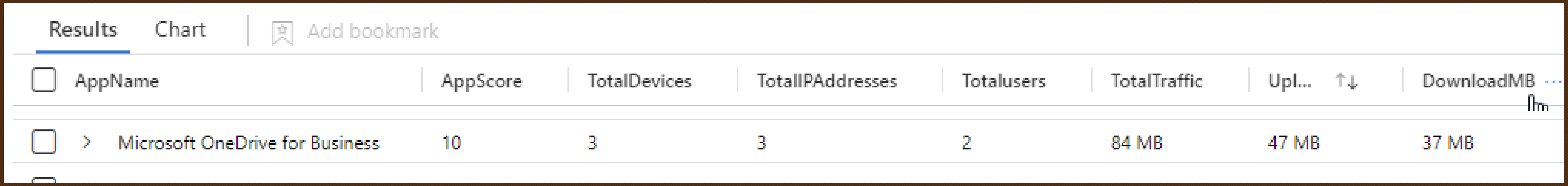
Total active users: 2

Total IP addresses: 3

Total devices: 3

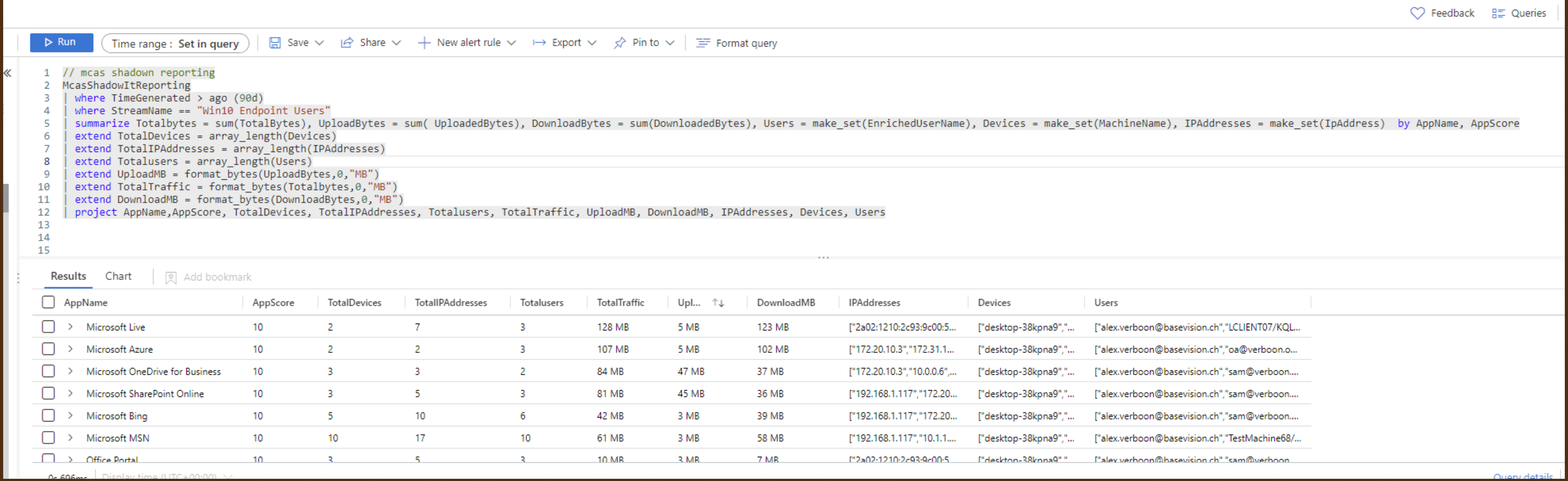
Upload traffic: 47MB

Download traffic: 37MB



AppName	AppScore	TotalDevices	TotalIPAddresses	Totalusers	TotalTraffic	Upl...	DownloadMB
Microsoft OneDrive for Business	10	3	3	2	84 MB	47 MB	37 MB

Microsoft Defender for Cloud Apps - McasShadowItReporting

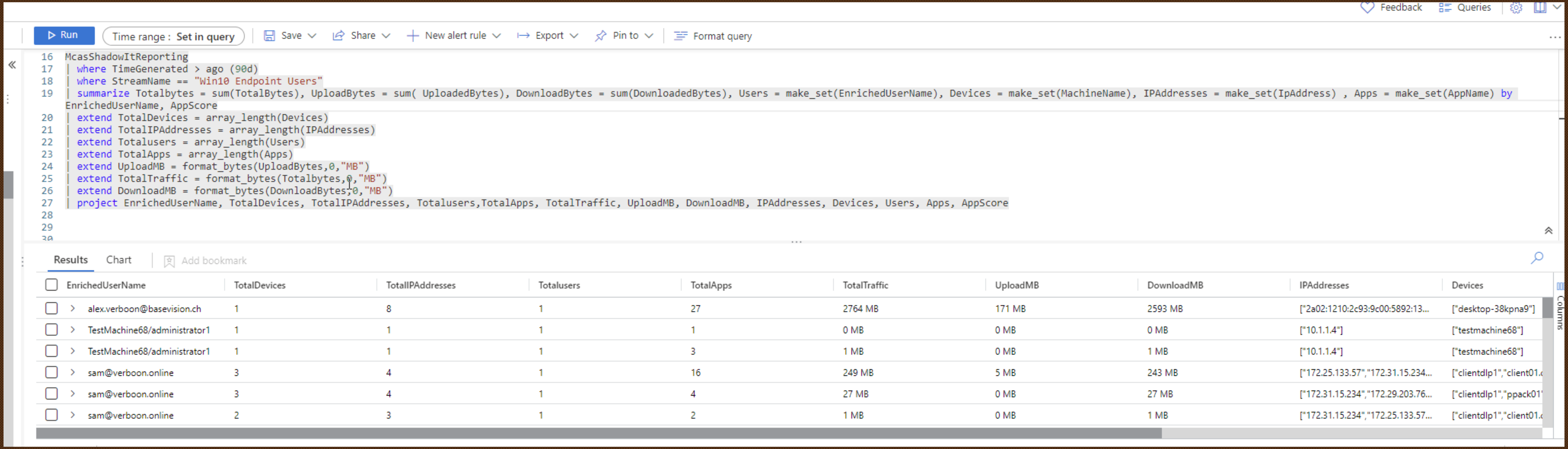


```
// mcas shadown reporting
McasShadowItReporting
| where TimeGenerated > ago (90d)
| where StreamName == "Win10 Endpoint Users"
| summarize Totalbytes = sum(TotalBytes), UploadBytes = sum( UploadedBytes), DownloadBytes = sum(DownloadedBytes), Users = make_set(EnrichedUserName), Devices = make_set(MachineName), IPAddresses = make_set(IpAddress)  by AppName, AppScore
| extend TotalDevices = array_length(Devices)
| extend TotalIPAddresses = array_length(IPAddresses)
| extend Totalusers = array_length(Users)
| extend UploadMB = format_bytes(UploadBytes,0,"MB")
| extend TotalTraffic = format_bytes(Totalbytes,0,"MB")
| extend DownloadMB = format_bytes(DownloadBytes,0,"MB")
| project AppName,AppScore, TotalDevices, TotalIPAddresses, Totalusers, TotalTraffic, UploadMB, DownloadMB, IPAddresses, Devices, Users
```

AppName	AppScore	TotalDevices	TotalIPAddresses	Totalusers	TotalTraffic	Upl... ↑↓	DownloadMB	IPAddresses	Devices	Users
Microsoft Live	10	2	7	3	128 MB	5 MB	123 MB	["2a02:1210:2c93:9c00:5...	["desktop-38kpna9","...	["alex.verboon@basevision.ch","LCLIENT07/KQL...
Microsoft Azure	10	2	2	3	107 MB	5 MB	102 MB	["172.20.10.3","172.31.1...	["desktop-38kpna9","...	["alex.verboon@basevision.ch","oa@verboon.o...
Microsoft OneDrive for Business	10	3	3	2	84 MB	47 MB	37 MB	["172.20.10.3","10.0.0.6",...	["desktop-38kpna9","...	["alex.verboon@basevision.ch","sam@verboon....
Microsoft SharePoint Online	10	3	5	3	81 MB	45 MB	36 MB	["192.168.1.117","172.20...	["desktop-38kpna9","...	["alex.verboon@basevision.ch","sam@verboon....
Microsoft Bing	10	5	10	6	42 MB	3 MB	39 MB	["192.168.1.117","172.20...	["desktop-38kpna9","...	["alex.verboon@basevision.ch","sam@verboon....
Microsoft MSN	10	10	17	10	61 MB	3 MB	58 MB	["192.168.1.117","10.1.1....	["desktop-38kpna9","...	["alex.verboon@basevision.ch","TestMachine68/...
Office Portal	10	3	5	3	10 MB	3 MB	7 MB	["2a02:1210:2c93:9c00:5...	["desktop-38kpna9","	["alex.verboon@basevision.ch","sam@verboon...

Microsoft Defender for Cloud Apps - McasShadowItReporting

Let’s flip things, so we get traffic by user



```
McasShadowItReporting
| where TimeGenerated > ago (90d)
| where StreamName == "Win10 Endpoint Users"
| summarize Totalbytes = sum(TotalBytes), UploadBytes = sum( UploadedBytes), DownloadBytes = sum(DownloadedBytes), Users = make_set(EnrichedUserName), Devices = make_set(MachineName), IPAddresses = make_set(IpAddress) , Apps = make_set(AppName) by EnrichedUserName, AppScore
| extend TotalDevices = array_length(Devices)
| extend TotalIPAddresses = array_length(IPAddresses)
| extend Totalusers = array_length(Users)
| extend TotalApps = array_length(Apps)
| extend UploadMB = format_bytes(UploadBytes,0,"MB")
| extend TotalTraffic = format_bytes(Totalbytes,0,"MB")
| extend DownloadMB = format_bytes(DownloadBytes,0,"MB")
| project EnrichedUserName, TotalDevices, TotalIPAddresses, Totalusers,TotalApps, TotalTraffic, UploadMB, DownloadMB, IPAddresses, Devices, Users, Apps, AppScore
```

□	EnrichedUserName	TotalDevices	TotalIPAddresses	Totalusers	TotalApps	TotalTraffic	UploadMB	DownloadMB	IPAddresses	Devices
□	alex.verboon@basevision.ch	1	8	1	27	2764 MB	171 MB	2593 MB	["2a02:1210:2c93:9c00:5892:13...	["desktop-38kpna9"]
□	TestMachine68/administrator1	1	1	1	1	0 MB	0 MB	0 MB	["10.1.1.4"]	["testmachine68"]
□	TestMachine68/administrator1	1	1	1	3	1 MB	0 MB	1 MB	["10.1.1.4"]	["testmachine68"]
□	sam@verboon.online	3	4	1	16	249 MB	5 MB	243 MB	["172.25.133.57","172.31.15.234...	["clientdlp1","client01.
□	sam@verboon.online	3	4	1	4	27 MB	0 MB	27 MB	["172.31.15.234","172.29.203.76...	["clientdlp1","ppack01
□	sam@verboon.online	2	3	1	2	1 MB	0 MB	1 MB	["172.31.15.234","172.25.133.57...	["clientdlp1","client01.

Security Events usage

How much do we use?

Questions?

Thanks for attending

KQL|Cafe