



INVICTUS
INCIDENT RESPONSE



Accelerate cloud incident response Microsoft & Security NL meetup

Korstiaan Stam, Invictus Incident Response

**Who has done
investigations in
O365/M365?**



INVICTUS
INCIDENT RESPONSE

Who knows what the Unified Audit Log is?



INVICTUS
INCIDENT RESPONSE

Who knows the export limits for the UAL?



INVICTUS
INCIDENT RESPONSE

Who are we?



- Invictus Incident Response is specialized in responding to cloud incidents across all major clouds AWS, Azure, GC as well as SaaS platforms such as M365 and Google Workspace and many more
- Based in the Netherlands, but active everywhere
- Background in IT forensics and Incident Response
- Previously PwC, Northwave & Tesorion
- SANS Instructor



What we do

Cloud IR Overview



Proactive		Reactive
IR Readiness	Knowledge & Training	Cloud Breach (Incident Response)
<ul style="list-style-type: none">• Customized Cloud Readiness Assessment (AWS, Azure, GC)• Customized SaaS Readiness Assessment, (M365, GWS)	<ul style="list-style-type: none">• Microsoft Cloud IR (Azure, M365)• AWS Cloud IR• Google Cloud IR• Custom Cloud IR Table Top Exercises	<ul style="list-style-type: none">• Cloud Incident Response (Emergency 24 x 7)• Compromise Assessment• Post-incident forensics and custom IR improvement program.
Retainer Services (Premium, Advanced and Ultimate)		

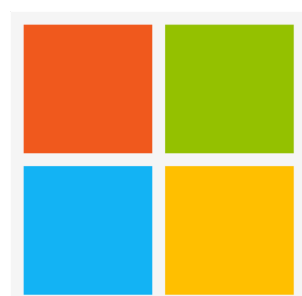
Why this talk

Open-Source



- We strongly believe in developing open-source tools for the community
- The tools we build are meant to help security analysts and DFIR people to make their lives easier and/or do their job better
- Helps build our brand and trust
- We have been developing open-source tools for a long time

“Continuously innovate and develop open-source incident response tools and solutions tailored specifically for cloud environments.”



Microsoft Extractor Suite

<https://github.com/invictus-ir/Microsoft-Extractor-Suite>

Google Workspace



ALFA

<https://github.com/invictus-ir/ALFA>



Invictus-AWS

<https://github.com/invictus-ir/Invictus-AWS>

Datasets

Microsoft 365:

https://github.com/invictus-ir/o365_dataset

Google Workspace:

https://github.com/invictus-ir/gws_dataset

AWS CloudTrail:

https://github.com/invictus-ir/aws_dataset

Microsoft- Extractor-Suite



INVICTUS
INCIDENT RESPONSE

Want to dive right in?
This is your chance



<https://github.com/invictus-ir/Microsoft-Extractor-Suite>



<https://microsoft-365-extractor-suite.readthedocs.io/>

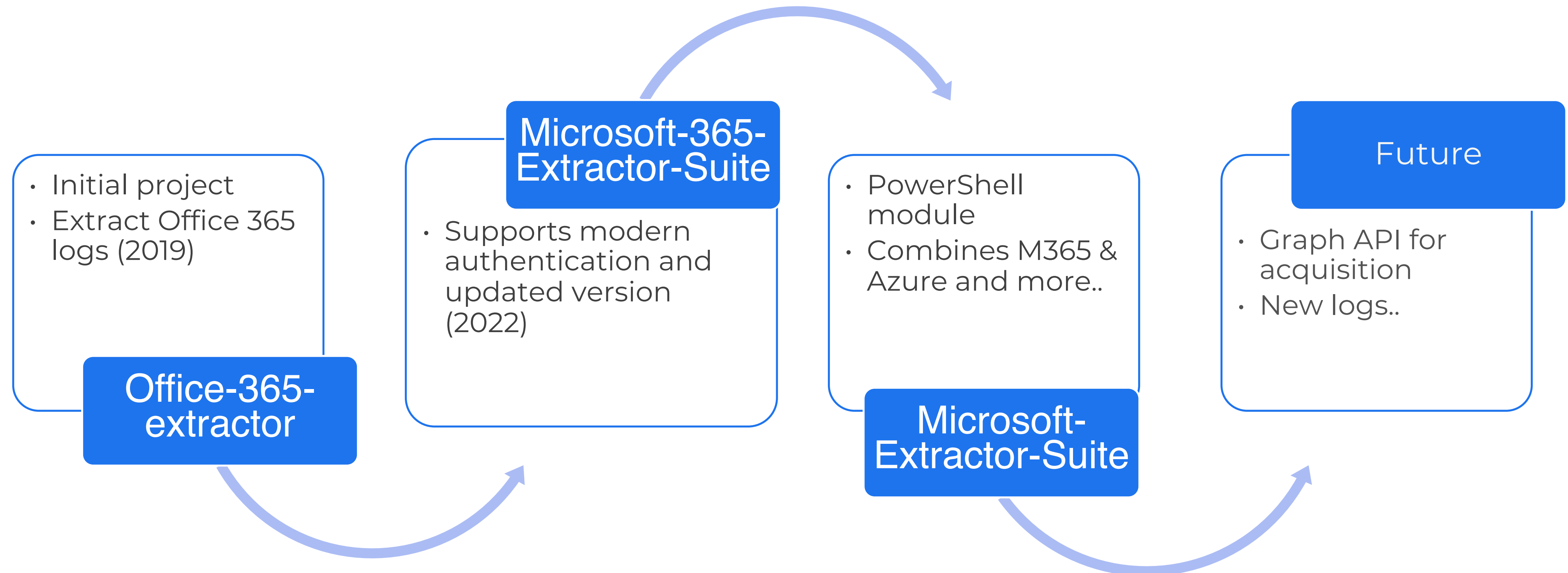


Install-Module -Name **Microsoft-Extractor-Suite**

Background

History

- Started from a BEC project into a full fledged acquisition solution for Microsoft 365 and Entra ID logging



What is it?



- A complete stand-alone PowerShell module
- Can be used to acquire data from Microsoft 365 (formerly known as Office 365) and Microsoft Entra ID (formerly known as Azure Active Directory) environments
- Especially useful for incident responders and security people doing investigations in Microsoft cloud environments
- It solves several challenges around acquisition such as maximum export and export formats
- Can easily be extended to add more log sources in the Microsoft cloud
- Fully open-source and standard license (GNU) which allows you to do everything, but we're not responsibly if you mess it up 😊
- It is **not** an analysis tool, it will acquire all data you need, but you'll need to perform the analysis which can be done in Splunk, Data Explorer or SOF-ELK or whatever you prefer!

Microsoft-Extractor-Suite

Capabilities



Data sources



- Unified Audit Log
- Admin Audit Log
- Mailbox Audit Log
- Email rules (Mailbox and Transport)
- Message Trace Logs



- Azure AD/Entra ID Sign-In Log
- Azure AD/Entra ID Audit Logs
- Azure Activity Logs for each subscription
- Registered Oauth applications in Azure AD

More to come....

Microsoft-Extractor-Suite

Functions

The tool has 22 standalone functions:

CommandType	Name
-----	----
Function	Connect-Azure
Function	Connect-AzureAZ
Function	Connect-GraphAPI
Function	Connect-M365
Function	Get-ActivityLogs
Function	Get-ADAuditLogs
Function	Get-ADAuditLogsGraph
Function	Get-AdminAuditLog
Function	Get-ADSignInLogs
Function	Get-ADSignInLogsGraph
Function	Get-MailboxAuditLog
Function	Get-MailboxRules
Function	Get-MessageTraceLog
Function	Get-OAuthPermissions
Function	Get-TransportRules
Function	Get-UALAll
Function	Get-UALGroup
Function	Get-UALSpecific
Function	Get-UALSpecificActivity
Function	Get-UALStatistics
Function	Show-MailboxRules
Function	Show-TransportRules

Overview of all available functions

\$ Get-Command -Module Microsoft-Extractor-Suite

- 4 Connect-* functions for connecting to M365 and Azure Active Directory
- 2 Show-* functions for live triage
- 16 Get-* functions for acquiring data from M365, Azure & Entra ID

Want to know what a function does and how it works?

\$ Get-Help -Command <insert-command>

Microsoft-Extractor-Suite

Challenges

Export limits Unified Audit Log (UAL)

- Script does a check
 - if number of events > 5k
 - Shorten time period and redo check
 - If number of events < 5k
- Acquire logs

```
PS /Users/korstiaan/Downloads> get-ualAll -startDate 2023-09-18 -endDate 2023-09-20
[INFO] Running Get-UALAll
[INFO] Setting the Interval to the default value of 720
[INFO] Output set to CSV
[INFO] MergeCSVOutput set to n
[INFO] Creating the following directory: Output\UnifiedAuditLog\20231101141856
[INFO] Extracting all available audit logs between 2023-09-17T22:00:00Z and 2023-09-19T22:00:00Z
[INFO] Found 933 audit logs between 2023-09-17T22:00:00Z and 2023-09-18T10:00:00Z
[INFO] Successfully retrieved 933 records out of total 933 for the current time range. Moving on!
[INFO] Found 192 audit logs between 2023-09-18T10:00:00Z and 2023-09-18T22:00:00Z
[INFO] Successfully retrieved 192 records out of total 192 for the current time range. Moving on!
[INFO] Found 1014 audit logs between 2023-09-18T22:00:00Z and 2023-09-19T10:00:00Z
[INFO] Successfully retrieved 1014 records out of total 1014 for the current time range. Moving on!
[INFO] Found 98 audit logs between 2023-09-19T10:00:00Z and 2023-09-19T22:00:00Z
[INFO] Successfully retrieved 98 records out of total 98 for the current time range. Moving on!
[INFO] Acquisition complete, check the Output directory for your files..
```

Prerequisites & Setup

Acquisition

Microsoft 365 account with sufficient permissions

- View-Only Audit log permission

Entra ID account with sufficient permissions

- Reports Reader
- Security Reader
- Security Administrator
- Global Reader
- Global Administrator

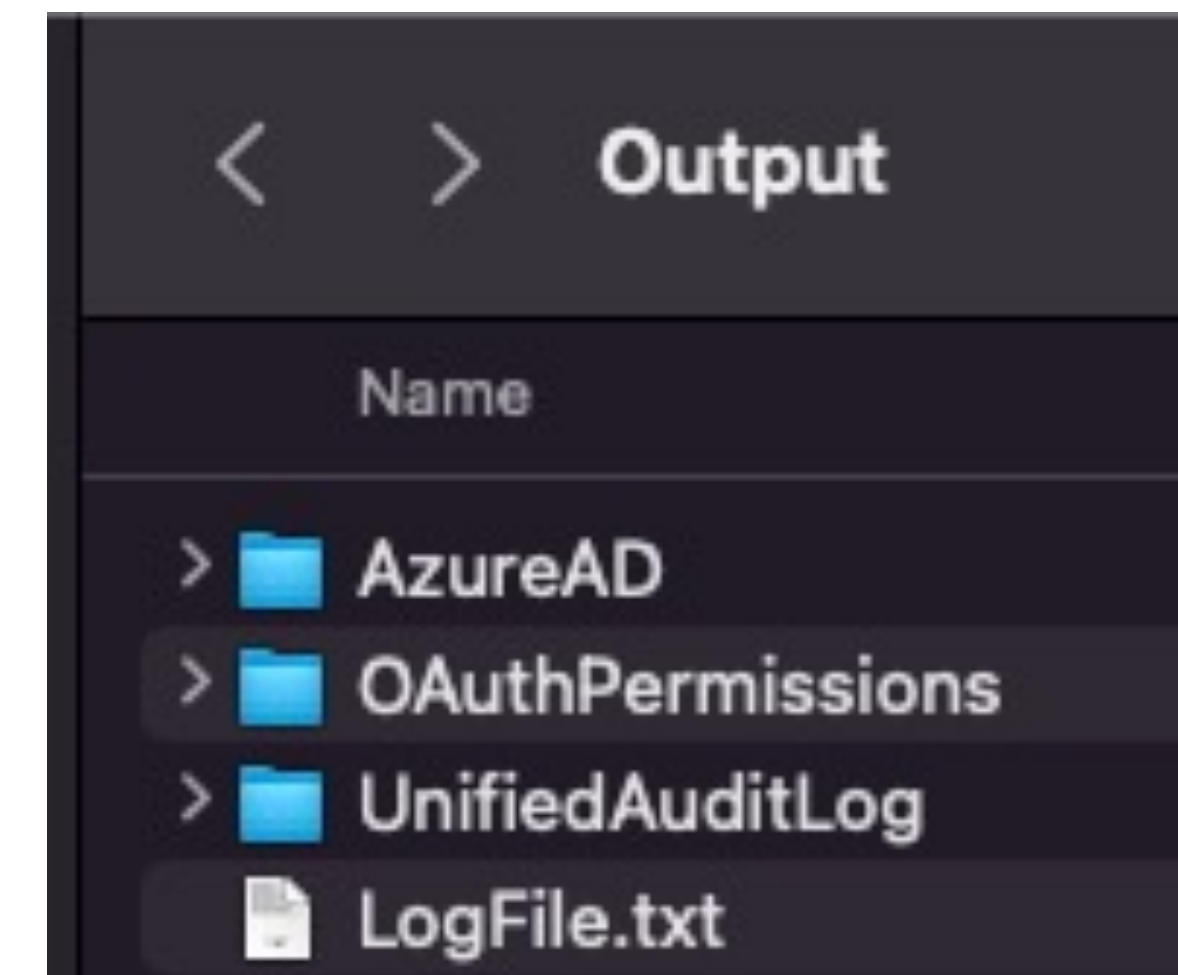
PowerShell

- Install-Module -Name Microsoft-Extractor-Suite
- Connect-M365 or Connect-Azure*
- Run function (e.g. Get-ADAuditLogs)

Output

- Output will be stored in separate folder with an audit LogFile

* Requires Connect-ExchangeOnline and Connect-AzureADPreview modules to be installed



Microsoft cloud incidents



INVICTUS
INCIDENT RESPONSE

Microsoft-Extractor-Suite

Use cases



Attack 1 - BEC

Business email compromise which leads to data exfiltration and/or follow up attacks.

Run:

- Show-MailboxRules
- Show-TransportRules
- Get-UALAll



Attack 2– Malicious app

Malicious OAuth app registration which leads to unauthorized access of user data by an application in the background.

Run:

- Get-OAuthPermissions
- Get-ADSignInLogs

Microsoft-Extractor-Suite

Notable incidents

SolarWinds

Large supply-chain attack of IT provider which led to infection of their software product Orion, which was installed on approx. 18k systems. Supposedly carried out by the SVR.

Cloud IR component, Azure AD applications compromised; certificates/secrets added which led to unauthorized access of emails.

Storm-0558

Targeted compromise of US organizations by supposedly the Chinese government.

Cloud IR component, attacker used access to access M365/Exchange information.

What do these two have in common?

Unified Audit Log

MailItemsAccessed



The US Cybersecurity and Infrastructure Security Agency (CISA) said in a [security advisory](#) last week that a federal executive branch agency discovered a breach of Exchange Online data "by leveraging enhanced logging—specifically of MailItemsAccessed events—and an established baseline of normal Outlook activity (e.g., expected AppID)." This "enables detection of otherwise difficult to detect adversarial activity," CISA said.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Search

Topics ▾ Spotlight Resources & Tools ▾ News & Events ▾ Careers ▾ About ▾

[Home](#) / [News & Events](#) / [News](#)

BLOG

When Tech Vendors Make Important Logging Info Available for Free, Everyone Wins

Released: July 19, 2023

A group of people in a meeting room, with one person standing and pointing at a screen displaying data charts.

News Data protection Microsoft Purview Audit · 3 min read

Expanding cloud logging to give customers deeper security visibility

By [Vasu Jakka](#), Corporate Vice President, Security, Compliance, Identity, and Management

July 19, 2023

In response to the increasing frequency and evolution of nation-state

Timeline

Now we wait



■ ■ ■ Microsoft Purview compliance portal: **Rollout**
☑ Audit - New default retention for Audit (Standard) **Start:**
October 2023

The default retention period for Microsoft Purview Audit (Standard) will change from 90 days to 180 days. The default retention period for Audit (Premium) remains at 1 year.

Feature ID: 171160
Added to roadmap: 9/13/2023
Last modified: 10/18/2023
Product(s): Microsoft Purview compliance portal
Cloud instance(s): Worldwide (Standard Multi-Tenant)
Platform(s): Web
Release phase(s): General Availability

☑ ■ ■ ■ Microsoft Purview compliance portal: Audit - New Exchange and SharePoint Logs for Microsoft Purview Audit Standard Users **Preview Available:**
June 2024
Rollout Start:
September 2024

Microsoft Purview is expanding access to wider cloud security activity events for Microsoft Exchange and SharePoint. As part of the changes, standard users of Purview Audit will begin to generate 4 new Microsoft Exchange and SharePoint events that were previously generated only for Audit Premium licensed users. The following events will now be provided for all Audit Standard users: 1. MailItemsAccessed; 2. Send; 3. SearchQueryInitiatedExchange; 4. SearchQueryInitiatedSharepoint; The following logs will differ based upon the user's license. This following additional metadata is added to Exchange logs when the user is assigned an Audit Premium license: Premium Insight 1: SensitivityLabel for MailItemsAccessed

Feature ID: 182259
Added to roadmap: 10/18/2023
Last modified: 10/19/2023
Product(s): Microsoft Purview compliance portal
Cloud instance(s): Worldwide (Standard Multi-Tenant), GCC, GCC High, DoD
Platform(s): Web
Release phase(s): General Availability, Preview

📧 📡

Demo



INVICTUS
INCIDENT RESPONSE

Demo

Commands



Scenario 1 – Acquire within a certain timeperiod and save it as a json file

- Connect-M365
- Get-UALAll –StartDate 10-04-2023 –EndDate 20-04-2023 –Output json

Scenario 2 – Acquire for a specific user with a custom interval

- Connect-M365
- Get-UALAll -UserIds korstiaan@invictus-ir.com -Interval 10000

Scenario 3 – Show all mailbox rules in your environment

- Connect-M365
- Show-MailboxRules

Analysis



INVICTUS
INCIDENT RESPONSE

What's next?

Option 1 – Azure Data Explorer

Once you've acquired the logs, what can you do next:

- Open up Azure Data Explorer (free cluster)
- Create Database
- Load in logs
- Start querying

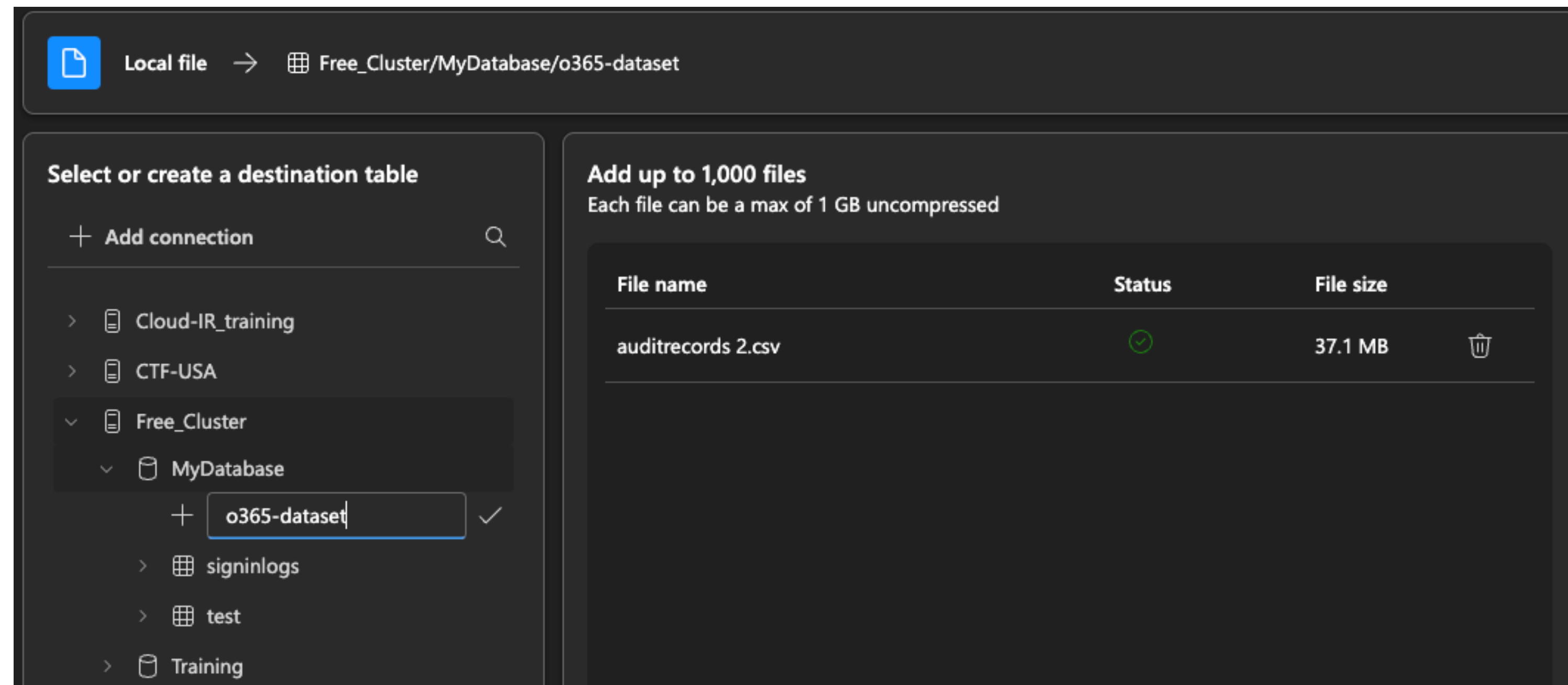
Also referenced in blog (<https://kqlquery.com/posts/kql-incident-response-everything-else/>)

What's next?

Option 1 – Azure Data Explorer

Once you've acquired the logs, what can you do next:

- Open Azure Data Explorer (free cluster)
- Create Database
- Load in logs
- Start querying



Write-up (<https://kqlquery.com/posts/kql-incident-response-everything-else/>)

Option 1 – Azure Data Explorer

Forwarding rules



```
"Parameters": [  
  {  
    "Name": "Name",  
    "Value": "."  
  },  
  {  
    "Name": "SetAuditSeverity",  
    "Value": "DoNotAudit"  
  },  
  {  
    "Name": "Mode",  
    "Value": "Enforce"  
  },  
  {  
    "Name": "Comments",  
    "Value": ""  
  },  
  {  
    "Name": "StopRuleProcessing",  
    "Value": "False"  
  },  
  {  
    "Name": "BlindCopyTo",  
    "Value": "ITCornpany@gmail.com"  
  },  
  {  
    "Name": "SubjectOrBodyContainsWords",  
    "Value": "password;payment;invoice;project"  
  },  
]
```

What's next?

Option 2 – Splunk

- Long time ago built a Splunk App called Blue team app for O365 & Azure
<https://splunkbase.splunk.com/app/4667>
- Idea behind the app is, load in the UAL and automatically the dashboards will light up
- Tell you where to focus your attention to
- Forwarding Rules, Permission Changes, Weird logins, eDiscovery abuse
- Some examples in the next slides

This dashboards contains all kind of interesting login acitivity searches, helping you to identify suspicious behavior.

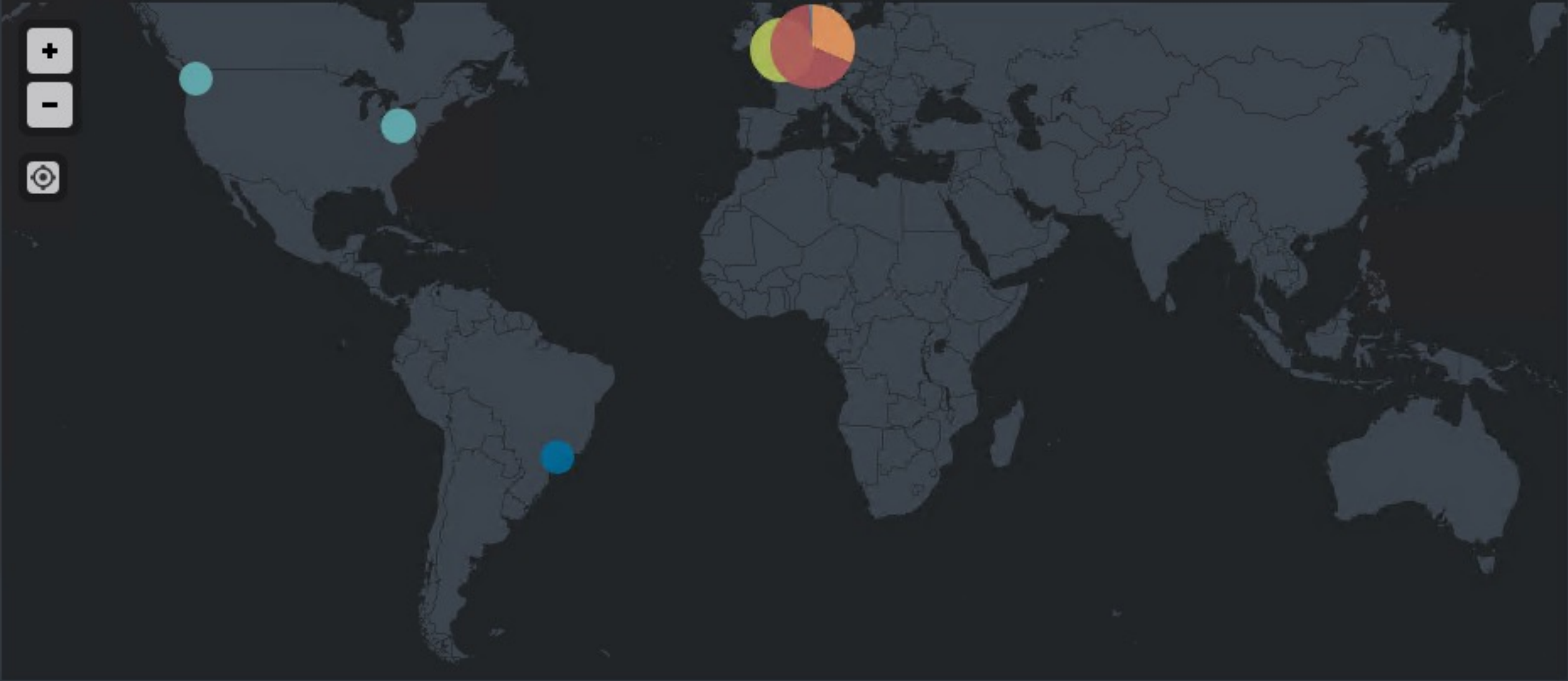
Successfull logins - Unique Users

14

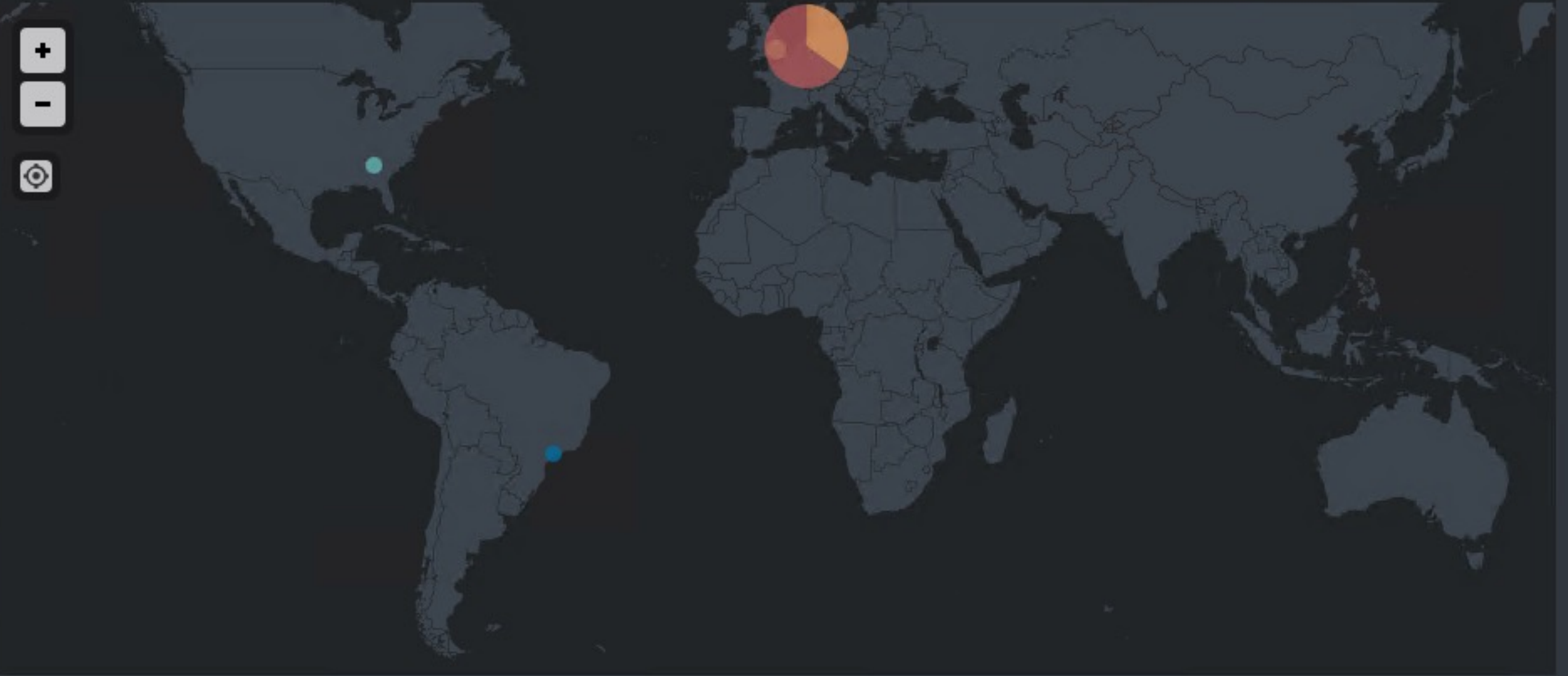
Successfull logins - Unique Source IP addresses

21

Successful logins per country



Bruteforce attempts by Country of origin



Failed logins because of MFA errors

UserId	ClientIP	LogonError	count
r.perez@gehim.onmicrosoft.com	164.143.240.34	UserStrongAuthClientAuthNRequired	5
r.perez@gehim.onmicrosoft.com	164.143.240.34	UserStrongAuthClientAuthNRequiredInterrupt	4

Multi Factor Disabled

CreationTime	Operations	SourceAccount	TargetAccount
2019-05-06T14:00:04	Disable Strong Authentication.	bobbyir@gehim.onmicrosoft.com	bobbyir@gehim.onmicrosoft.com

- Some things to note:
- Logins per country, spot logins from ‘interesting’ countries
 - Users that are locked out
 - Login failures due to Multi-Factor Authentication

Mail Forwarding Rules

Edit

Export

Regular users can setup or modify email forwarding rules in different ways detection can be done using the following operations:

- New-InboxRule
- Set-InboxRule

Administrative users or users with certain privileges can create or modify mail flow rules, these rules can be set for more than one mailbox and are harder to detect, however it is possible with the Unified Audit Log (UAL). Look for the following operations:

- New-TransportRule
- Set-TransportRule

For more information on New-TransportRule see: <https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance/new-transportrule?view=exchange-ps>

For more information on Set-TransportRule see:<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance/set-transportrule?view=exchange-ps>

For more information on New-InboxRule see: <https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/new-inboxrule?view=exchange-ps>

For more information on Set-InboxRule see: <https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-inboxrule?view=exchange-ps>

Number of forwarding rules in this dataset

21

Overview of Forwarding rules

CreationTime	Operations	MailRuleId	RuleName	SourceAccount	SourceIP
2019-07-18T08:02:47	Set-TransportRule	44014dbf-48ef-4acf-6b10-08d70b565283	Forward_All_Mail	bobbyir@gehim.onmicrosoft.com	164.143.240.34
2019-07-18T08:14:08	Set-TransportRule	19371680-9e79-458b-ee3c-08d70b57e87a	... 2	bobbyir@gehim.onmicrosoft.com	164.143.240.34
2019-07-18T07:54:34	New-TransportRule	a7b1e3de-3d8f-49b4-a015-08d70b552cdb	-	bobbyir@gehim.onmicrosoft.com	164.143.240.34
2019-07-01T10:49:27	Set-TransportRule	65f20e71-d592-4037-94c6-08d6fe11c9cb	...	bobbyir@gehim.onmicrosoft.com	46.144.22.5
2019-07-01T10:49:27	Set-TransportRule	65f20e71-d592-4037-94c6-08d6fe11c9cb	...	bobbyir@gehim.onmicrosoft.com	46.144.22.5
2019-07-01T10:51:03	New-TransportRule	53674c30-40f7-457d-b785-08d6fe1202e8	...	bobbyir@gehim.onmicrosoft.com	46.144.22.5
2019-07-01T10:51:53	New-TransportRule	541bad3b-7a3d-4d59-aeae-08d6fe1220e4	-----	bobbyir@gehim.onmicrosoft.com	46.144.22.5
2019-05-02T12:00:15	New-InboxRule	492cd11f-ea88-47a7-9093-08d6cef5bd11	ForwardingEmailsRebecca	r.perez@gehim.onmicrosoft.com	91.151.26.1
2019-05-02T12:05:30	Set-InboxRule	33b1ba98-b99b-4647-d6ab-08d6cef678c2	33d63ef1-6676-4fa5-8edd-ac85af56d17b\7639512342903914497	r.perez@gehim.onmicrosoft.com	91.151.26.1
2019-05-02T12:06:14	Set-TransportRule	b8e42d6c-6d68-40e0-937f-08d6cef69335	Forward_Mail_For_Approval	bobbyir@gehim.onmicrosoft.com	91.151.26.1
2019-05-02T07:57:52	New-TransportRule	cae97c41-06a5-47fd-e579-08d6ced3e11c	DeleteMessages	bobbyir@gehim.onmicrosoft.com	46.144.22.5
2019-05-02T08:04:45	New-TransportRule	84e67562-0119-4ecc-9c1b-08d6ced4d6b4	FowrardMail	bobbyir@gehim.onmicrosoft.com	46.144.22.5
2019-05-02T08:05:37	Set-TransportRule	22774654-9523-40d4-0e38-08d6ced4f5b8	FowrardMail	bobbyir@gehim.onmicrosoft.com	46.144.22.5

How can you help?

We need you

- Please use this in your tests or IR cases and when you do it would be great if you could share any feedback through Email/LinkedIn/Twitter
- If you have an active IR engagement and you want to use this product..
 - Ask for help we are happy to run the engagement with you or for you..
 - We can support you in the backend with any questions
- If you have cool (new) things you want added either try to build it yourself and if it works we will add or request it on GitHub

Training Invictus Academy



- Microsoft Cloud Incident Response
- Azure Incident Response
- Microsoft 365
- OnDemand
- **Live training Utrecht 30-11 en 01-12**



academy.invictus-ir.com

Questions?

Let's connect

LinkedIn: To stay in touch and our latest offerings:

<https://www.linkedin.com/company/invictus-incident-response>

Medium: We publish our research here: <https://invictus-ir.medium.com/>

Twitter: Updates on our latest tools and research: <https://twitter.com/InvictusIR>

GitHub: This is where the magic happens: <https://github.com/invictus-ir>