INVICTUS
INCIDENT RESPONSE

Accelerate cloud incident response: Introducing our new acquisition tool

Korstiaan Stam, Founder
korstiaan@invictus-ir.com

Who are we?

- We are an incident response company and we love doing cloud incident response and specialise in supporting organisations facing a cyber attack.
- Based in the Netherlands, but active everywhere

Microsoft-Extractor-Suite

INVICTUS
INCIDENT RESPONSE

Want to dive right in?

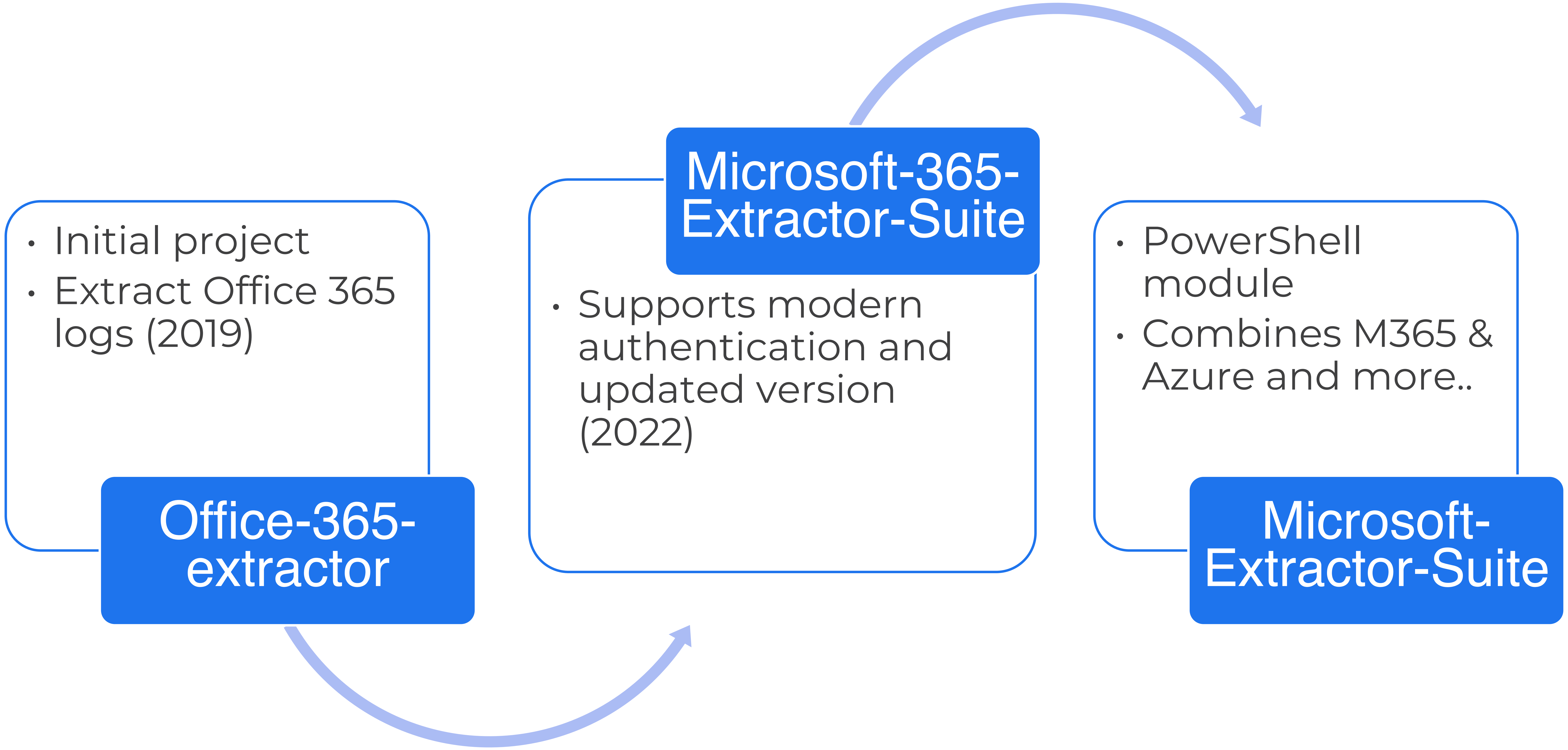
This is your chance

GitHub	https://github.com/invictus-ir/Microsoft-Extractor-Suite
Read the Docs	https://microsoft-365-extractor-suite.readthedocs.io/

Background

History

- Started from a BEC project into a full fledged acuiqistion solution for Microsoft 365 and Azure AD logging



Office-365-extractor

- Initial project
- Extract Office 365 logs (2019)

Microsoft-365-Extractor-Suite

- Supports modern authentication and updated version (2022)

Microsoft-Extractor-Suite

- PowerShell module
- Combines M365 & Azure and more..

What is it?

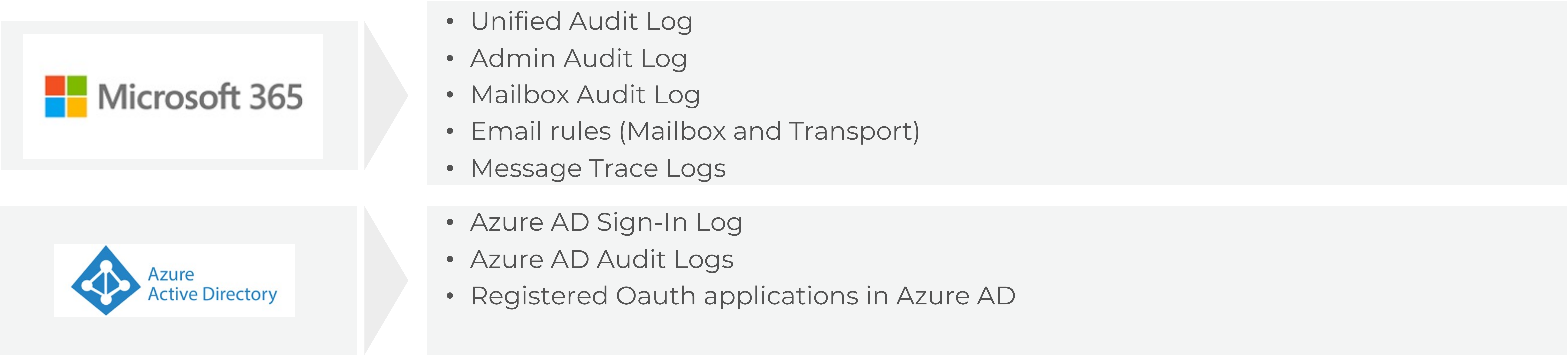
- A complete stand-alone PowerShell module
- Can be used to acquire data from Microsoft 365 (formerly known as Office 365) and Microsoft Azure Active Directory environments
- Especially useful for incident responders and security people doing investigations in Microsoft cloud environments
- It solves 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 or SOF-ELK or whatever you prefer!

Microsoft-Extractor-Suite

Capabilities

Data sources



Microsoft 365

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

Azure Active Directory

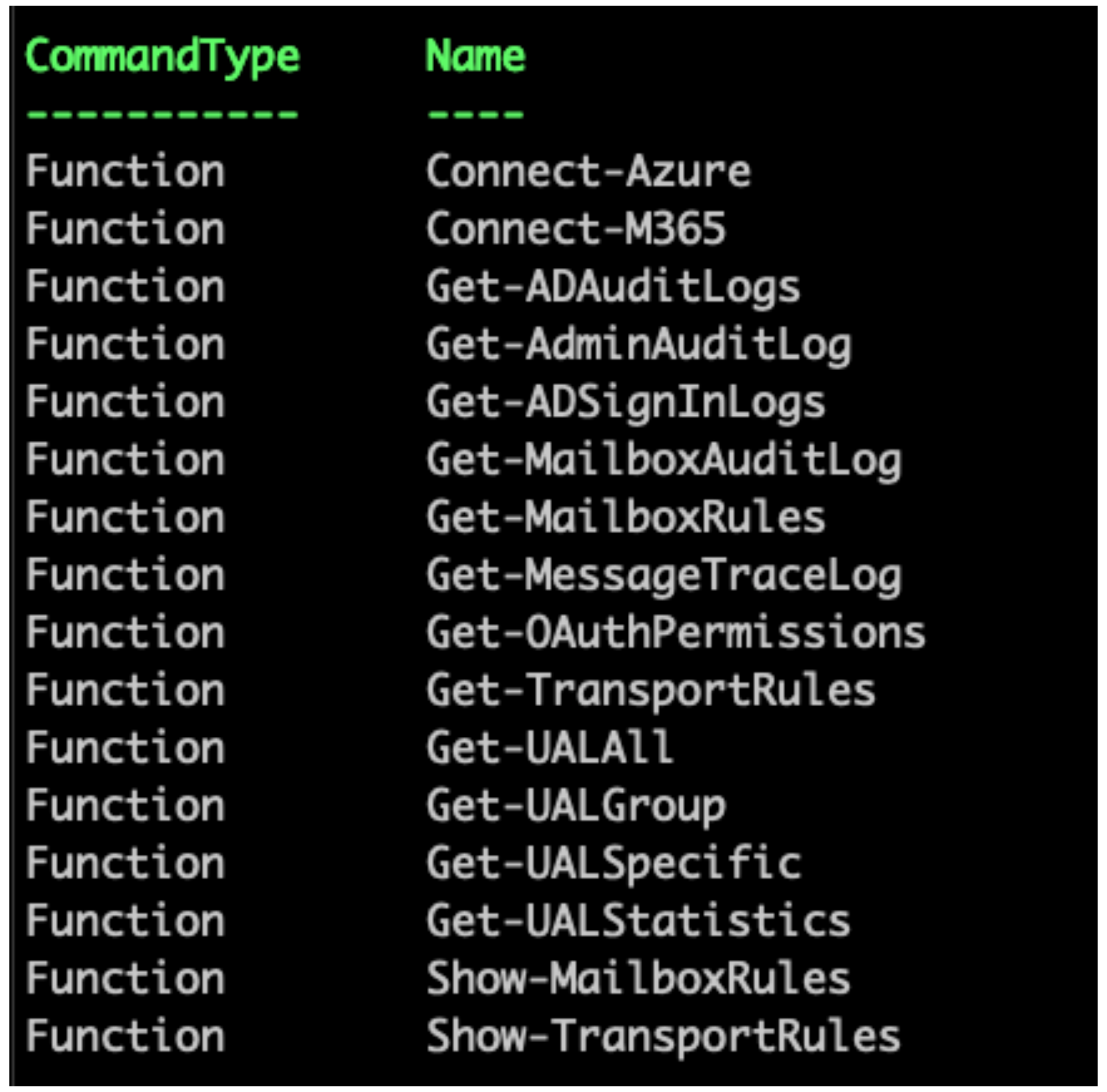
- Azure AD Sign-In Log
- Azure AD Audit Logs
- Registered Oauth applications in Azure AD

More to come....

Microsoft-Extractor-Suite

Functions

The tool has 16 standalone functions



```
CommandType     Name
-----------     ----
Function        Connect-Azure
Function        Connect-M365
Function        Get-ADAuditLogs
Function        Get-AdminAuditLog
Function        Get-ADSignInLogs
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-UALStatistics
Function        Show-MailboxRules
Function        Show-TransportRules
```

Overview of all available functions

$ Get-Command –Module Microsoft-Extractor-Suite

- 2 Connect-* functions for connecting to M365 and Azure Active Directory
- 2 Show-* functions for live triage
- 12 Get-* functions for acquiring data from M365 & Azure Active Directory

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

$ Get-Help –Command <insert-command>

Prerequisites & Setup

Acquisition

Microsoft 365 account with sufficient permissions

- View-Only Audit log permission

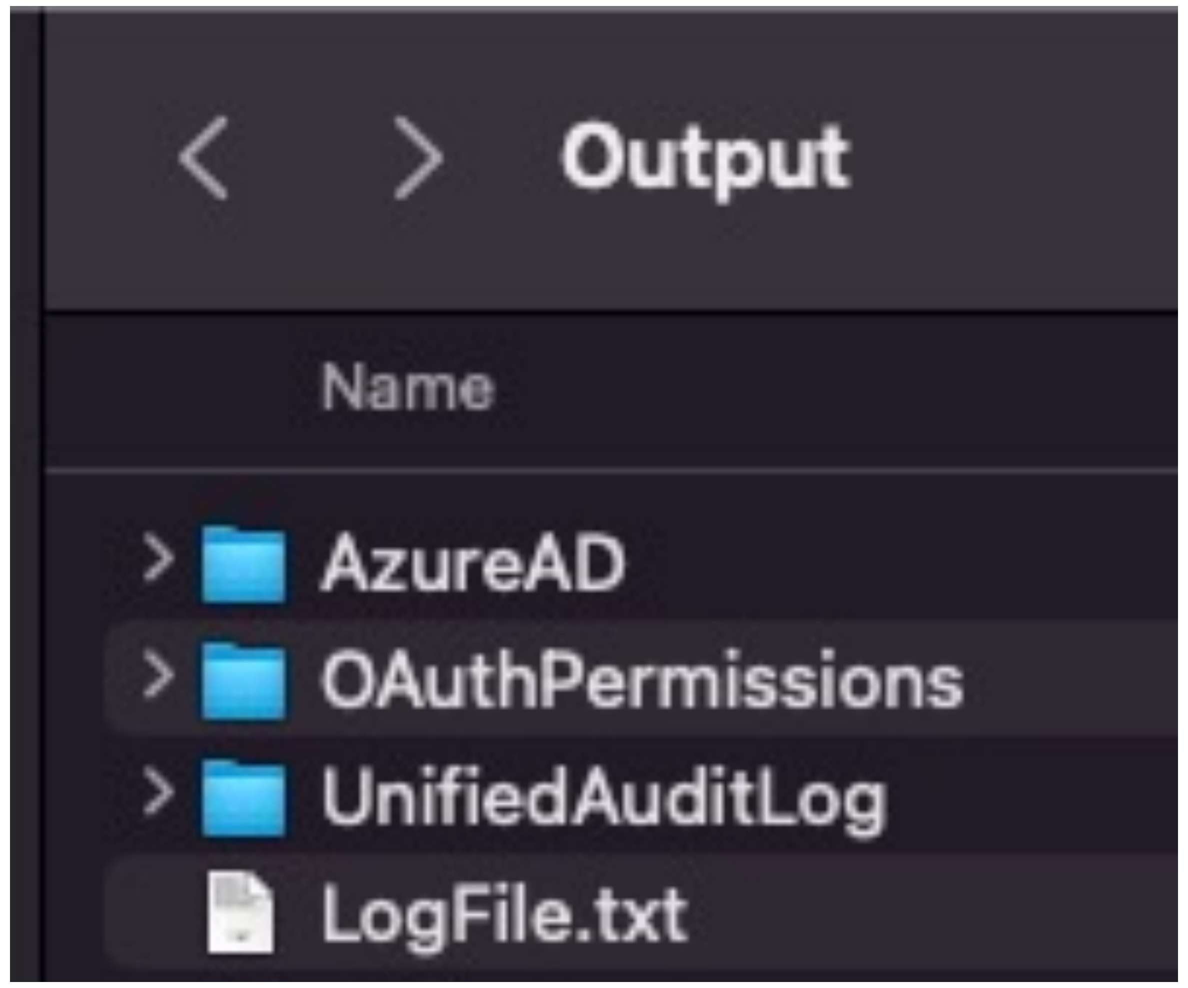
Azure AD account with sufficient permissions

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

PowerShell

- Import-Module .\Microsoft-Extractor-Suite.psd1
- Connect-M365 **or** Connect-Azure*
- Run function (e.g. Get-ADAuditLogs)

Output will be stored in separate folder with an audit LogFile



```
AzureAD
OAuthPermissions
UnifiedAuditLog
LogFile.txt
```

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

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

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

Demo

Commands

Scenario 4 – Acquire AD logging

- Connect-Azure
- Get-ADAuditLogs
- Get-ADSignInLogs

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 either run the engagement for you or..
  - 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
- Join one of our trainings on Microsoft Cloud Incident Response, more details coming soon…

Questions?

INVICTUS
INCIDENT RESPONSE

Korstiaan Stam
Founder, Invictus Incident Response
@InvictusIR
E: korstiaan@invictus-ir.com
W: invictus-ir.com