SSTIC 2021 – DFIR-O365RC

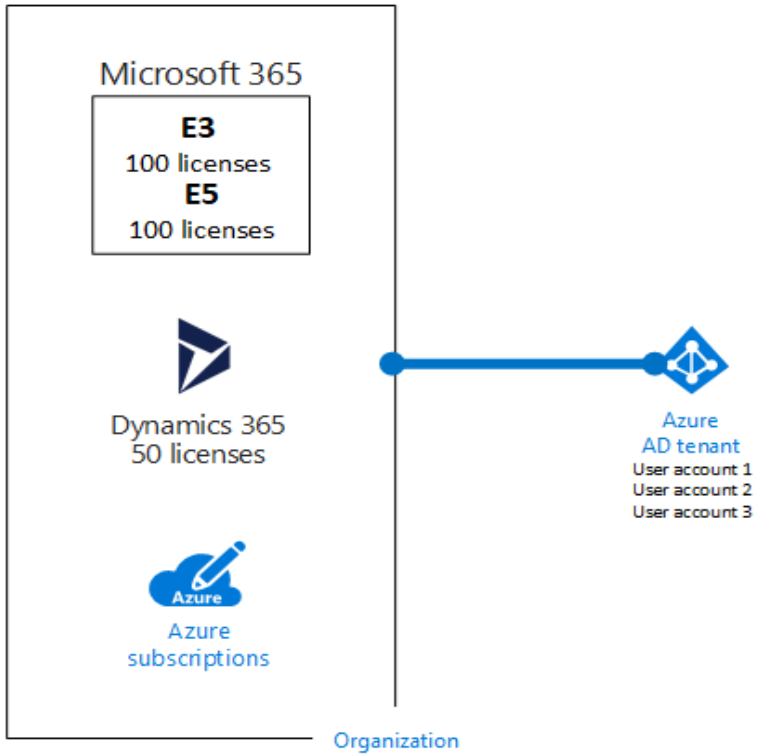
Léonard SAVINA

ANSSI – Sous-direction Opérations - Division Réponse

https://github.com/ANSSI-FR/DFIR-O365RC

Office 365 - présentation

- Office 365 est une solution SaaS de travail collaboratif.
- C'est une souscription au sein d'une organisation Azure dont les comptes sont stockés au sein d'un tenant Azure AD.
- Une boîte mail est un compte Azure AD avec une licence O365 activée.
- Un compte peut être « *cloud only* » ou synchronisé depuis l'AD « *on-prem* », on parle alors d'authentification hybride.



https://docs.microsoft.com/en-us/microsoft-365/enterprise/subscriptions-licenses-accounts-and-tenants-for-microsoft-cloud-offerings?view=o365-worldwide

Office 365 – les défis

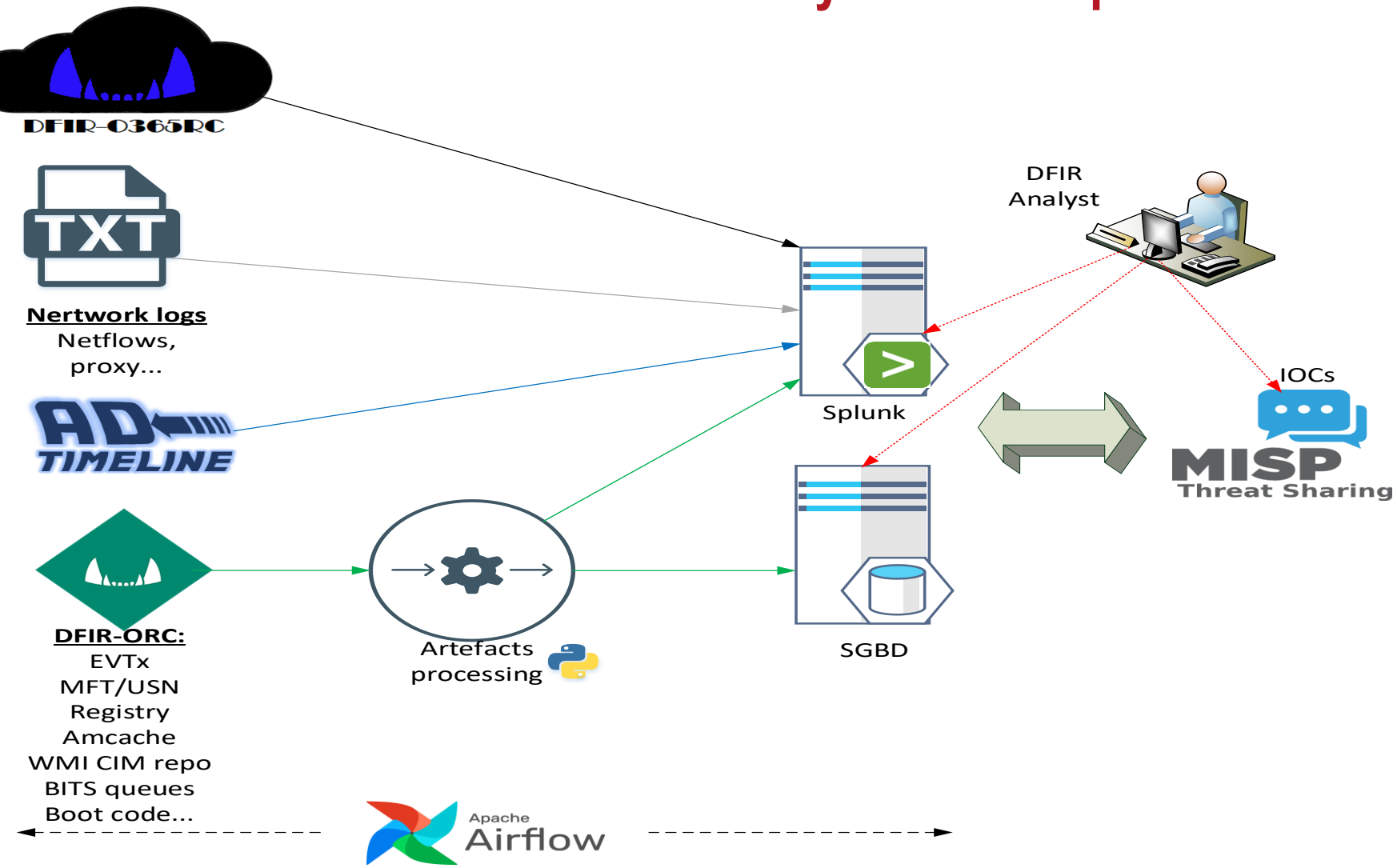
- La compromission sur Office 365 (Azure AD) peut entraîner une compromission "*on-prem*" (AD).

Et vice et versa…

- Une compromission "*on-prem*" (AD) peut entraîner une compromission sur Office 365 (Azure AD).

Il est donc indispensable lors d'une réponse à incidents d'analyser et faire des recoupements entre les éléments collectés "*on-prem*" et ceux collectés sur Office 365.

Chaîne de traitement d'analyse forensique



DFIR-O365RC – le besoin

Le but de DFIR-O365RC a été de réaliser un outil de collecte pour les investigations Office 365:

- Qui soit modulaire et permettant de s'adapter aux contraintes de l'investigation (niveau de licences, taille du tenant Azure AD).
- Collectant les journaux Office 365 et Azure AD avec le meilleur compromis performance/exhaustivité.
- Ayant un format de sortie adapté (JSON) et s'intégrant facilement dans la chaîne de traitement d'analyse forensique du CERT-FR.
- Compatible PowerShell Core.

Office 365 – les autres outils DFIR

DFIR-O365RC se concentre sur la collecte de journaux, il ne réalise pas de relevé de configuration, contrairement à:

- Hawk: https://github.com/T0pCyber/hawk
- Sparrow: https://github.com/cisagov/Sparrow
- CRT: https://github.com/CrowdStrike/CRT

DFIR-O365RC s'est inspiré de *Office 365 Extractor* pour la partie collecte des journaux unifiés d'audit:

https://github.com/PwC-IR/Office-365-Extractor

Office 365 – les sources de journaux

Source/Moyen	Historique/ Perf	Prérequis	Scope	DFIR-O365RC
Unified Audit Logs/O365 Management API	7J/Bonne	Via création App Azure	Office 365 + Azure AD	
Unified Audit Logs/Exchange Online Psh	90J/Mauvaise	Module Psh MSAL.PS	Office 365 + Azure AD	X
Azure AD Logs/Azure AD Psh Preview	30j/Bonne	Module Psh Windows	Azure AD audit et signins	
Azure AD Logs/MS Graph API	30j/Bonne	Module Psh MSAL.PS	Azure AD audit et signins	X
Azure Activity Logs/ Azure CLI ou Az Psh	90j/Bonne	Module Az Psh/CLI	Souscription Azure	
Azure Activity Logs/ Azure Monitor REST API	90j/Bonne	Module Psh MSAL.PS	Souscription Azure	X

DFIR-O365RC – Les fonctions

Nom	Source	Exhaustif	Perf	Détail
Get-O365Full	UAL	Complet	Mauvaise	Sur petite période ou petit tenant uniquement.
Get-O365Light	UAL	Partiel	Bonne	Opérations « d'intérêt » uniquement.
Get-DefenderforO365	UAL	Partiel	Bonne	Soumis à licence E5. Logs M365 Defender.
Search-O365	UAL	Complet	Dépend	Fonction de recherche IP/Utilisateur/FreeText.
Get-AADLogs	Az AD	Complet	Bonne	Az AD Audit + signins (licence Az AD P1)
Get-AADApps	Az AD	Partiel	Bonne	Az AD Audit enrichis et liés aux applications.
Get-AADDevices	Az AD	Partiel	Bonne	Az AD Audit enrichis et liés aux appareils.
Get-AzRMActivityLogs	Az Activity	Complet	Bonne	Logs souscriptions Azure (IaaS, PaaS…)

Get-O365Light - Exemples

> Mise en place de règle de redirection de courriels:

```
index="*" sourcetype="o365UAL_json" Workload="Exchange"
(Operation="New-InboxRule" OR Operation="Set-InboxRule")
Parameters{}.Name = "ForwardTo"
```

> Exposition de données via lien en accès anonyme:

```
index="*" sourcetype="o365UAL_json" (Workload="SharePoint" OR
Workload="OneDrive") Operation="AnonymousLinkCreated" | stats
values(SourceRelativeUrl), distinct_count(SourceRelativeUrl)
as nbUrls, values(ClientIP) by UserId | sort -nbUrls
```

Get-AADLogs - Exemple

Journaux d'authentification Azure AD, les protocoles « *legacy* »:

```
index="*" sourcetype="AADsignin_json" status.errorCode=0 | stats
count by clientAppUsed | sort count
```

Ils sont utilisés par les attaquants pour contourner l'authentification multi-facteurs. A bloquer via les stratégies d'accès conditionnelles.

> ...The numbers on legacy authentication from an analysis of Azure Active Directory (Azure AD) traffic are stark:
>
> - More than 99 percent of password spray attacks use legacy authentication protocols
> - More than 97 percent of credential stuffing attacks use legacy authentication
> - Azure AD accounts in organizations that have disabled legacy authentication experience 67 percent fewer compromises than those where legacy authentication is enabled

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

Get-AADDevices - Exemple

Journaux d'audit enrichis liés aux opérations sur les appareils enregistrés ou joints à Azure AD.

Le statut de conformité d'un appareil peut influencer les politiques appliquées à celui-ci. Ce statut peut être édité avec, par exemple, le module PowerShell *AADInternals*. Il est normalement édité par l'application Intune.

```
index="*" sourcetype="ADDDevices_json" activityDisplayName="Update
device" targetResources{}.modifiedProperties{}.displayName="IsCompliant"
isCompliant="true"
| fillnull value=null initiatedBy.user.userPrincipalName
| stats values(initiatedBy.app.displayName), distinct_count(displayName),
values(isManaged) by initiatedBy.user.userPrincipalName
```

https://o365blog.com/post/mdm/
https://github.com/Gerenios/AADInternals

Journaux DFIR-O365RC, recoupements journaux « on-prem » - Exemple

Scénario: Identifiants obtenus via attaque par brute force IMAP sur Office 365 et rejoués pour accéder au système d'information « *on-prem* » via la passerelle Netscaler.

On recherche dans le journaux Syslog du Netscaler si une IP ayant réalisé de l'IMAP se connecte aussi à la passerelle:

```
index = "*" sourcetype="citrix:netscaler:syslog"
    [ search index="*" sourcetype="AADsignin_json" clientAppUsed="IMAP4"
status.errorCode=0
    | rename ipAddress as ClientIP
    | fields ClientIP ]
```

Merci!

On recrute à la division réponse:

https://talents.ssi.gouv.fr/offresdemploi

https://github.com/ANSSI-FR/DFIR-O365RC