DUTCH
MICROSOFT SECURITY
MEETUP

Incident response_

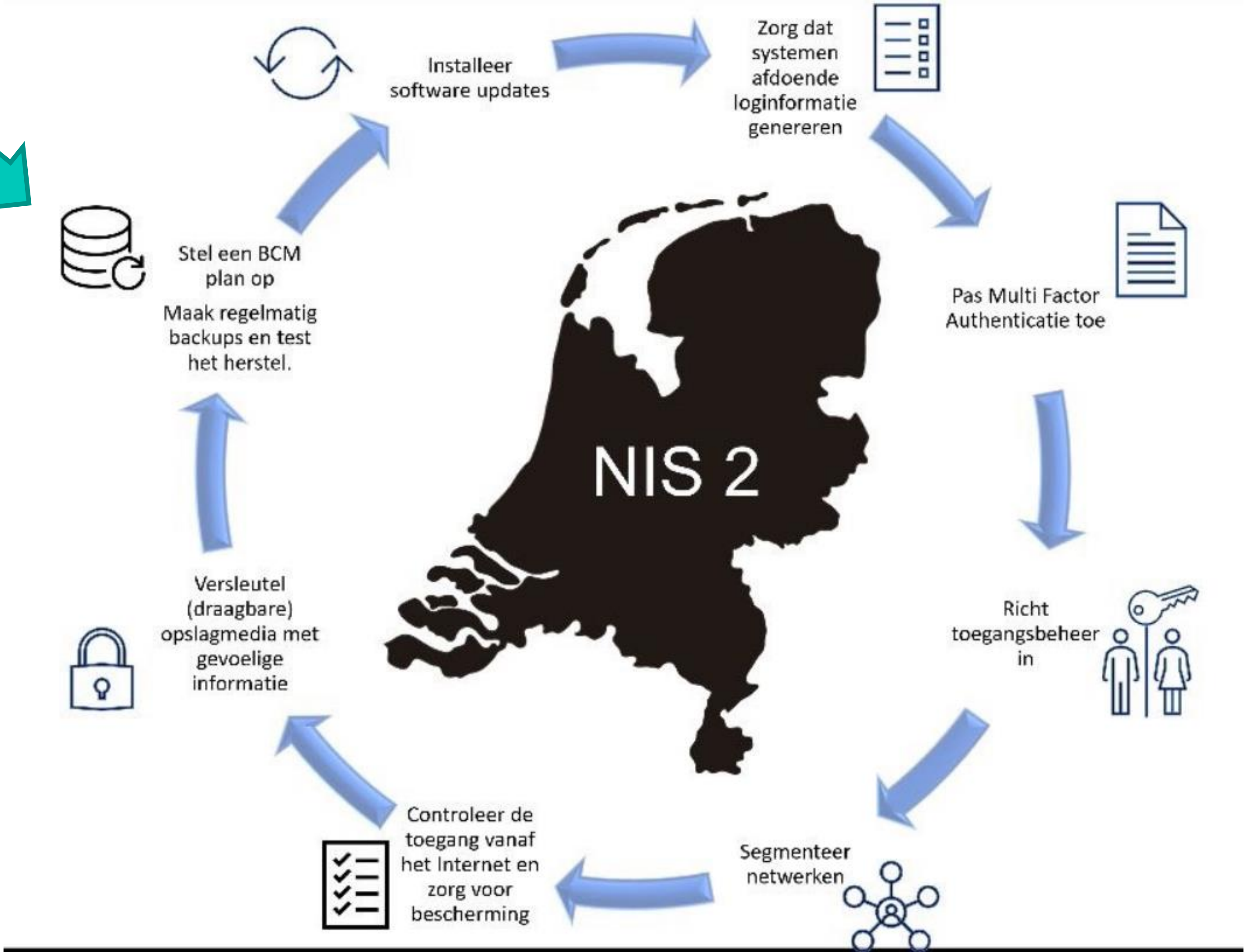
100%
フリッパー
FLIPPER

RV39
vanaf nu alleen te openen
met de nieuwe milieupas
FLIPPER

PROXSYS*

Incident response_

P.Wettstein



NIS 2

Installeer software updates

Zorg dat systemen afdoende loginformatie genereren

Pas Multi Factor Authenticatie toe

Richt toegangsbeheer in

Segmenteer netwerken

Controleer de toegang vanaf het Internet en zorg voor bescherming

Versleutel (draagbare) opslagmedia met gevoelige informatie

Stel een BCM plan op

Maak regelmatig backups en test het herstel.

*

Incident Response Plan

“The purpose of an Incident Response Plan is to act fast and effective in case of an incident, but save the correct data for further investigation”

Where to start

PROXSYS*

Prepare_

Prepare: Read Guidelines

SIDN (link)

NCSC (IR ransomware)

www.google.com

podcast cyberhelden #45

Episode 45: Diemer Kransen – Cyberhelden.nl

Microsoft

Microsoft Digital Defense Report 2022

Executive Summary

Illuminating the threat landscape
and empowering a digital defense.

Prepare: Read public cases

Gemeente Buren (Hunt & Hackett)

Senzer Logistics (Northwave)

Universiteit Maastricht (FoxIT)

Hof van Twente (NFIR)

aka TestAdmin - Welkom2020

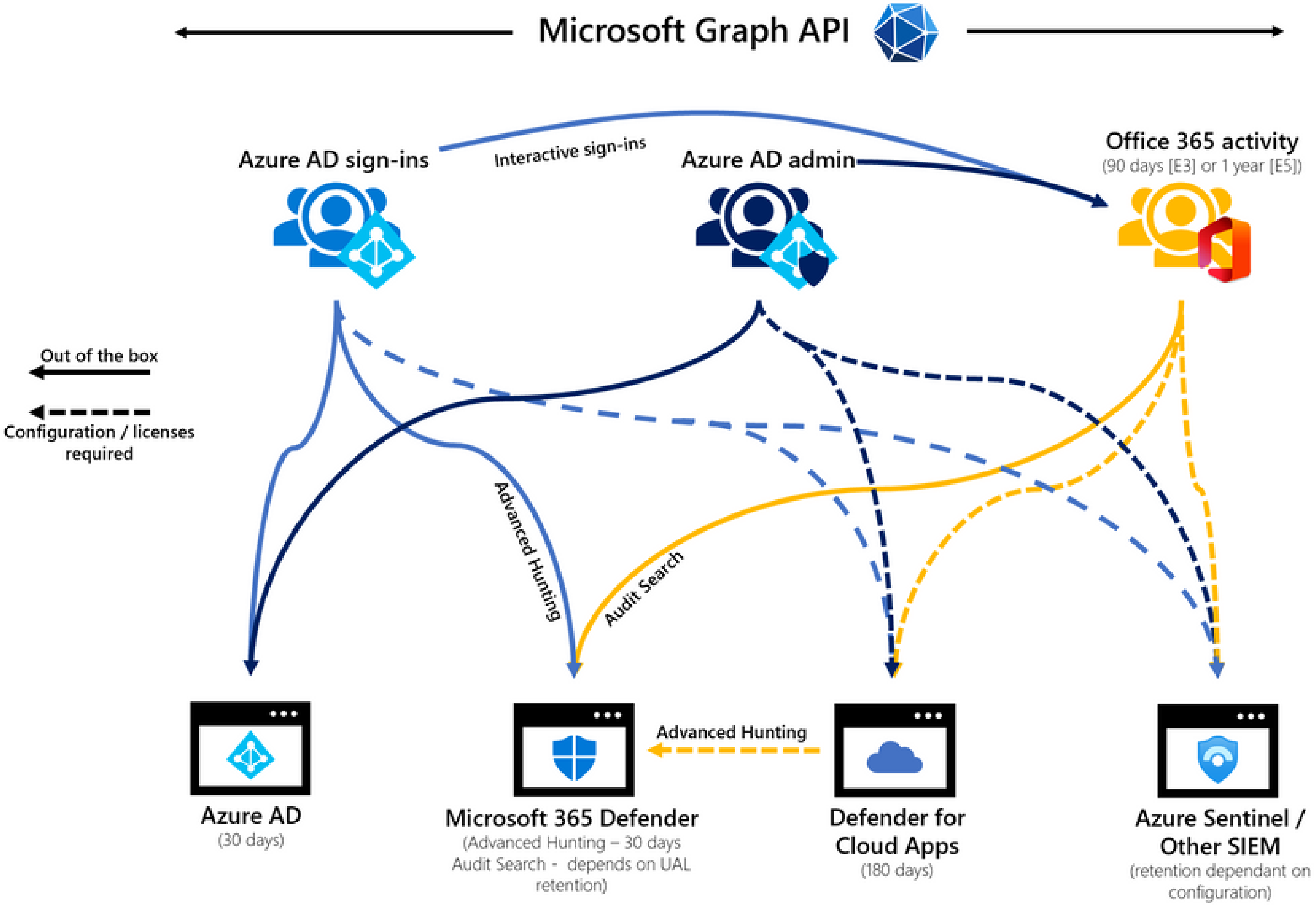
Prepare : Define the team

Communication
CISO
Backup & DR Operator
Security Research
Identity
Network

Prepare: Enable logging

Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration

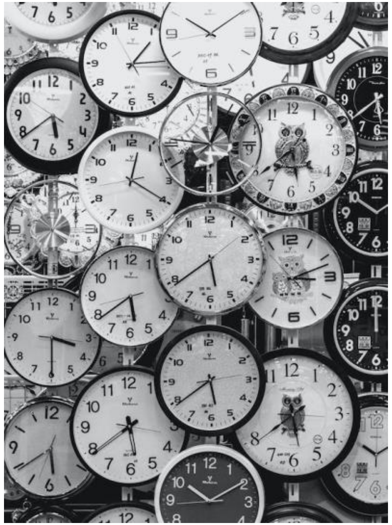
Computer Configuration -> Administrative Templates -> System -> Audit Process Creation (Include command line in process creation event)


Microsoft Graph API
Azure AD sign-ins
Interactive sign-ins
Azure AD admin
Office 365 activity
(90 days [E3] or 1 year [E5])
Out of the box
Configuration / licenses required
Advanced Hunting
Audit Search
Advanced Hunting
Azure AD
(30 days)
Microsoft 365 Defender
(Advanced Hunting – 30 days
Audit Search - depends on UAL retention)
Defender for Cloud Apps
(180 days)
Azure Sentinel / Other SIEM
(retention dependant on configuration)

PROXSYS*

Incident_

siterep



3. Start investigation

Draaiboek

Tijdstip	Wie	Activiteit	Plaats	Opmerking
9:00	Anne	Sprekers kleedkamer wijzen	Grote hal	Voldoende drinken beschikbaar in kleedkamer
		Goodiebags klaarzetten	Garderobe	Deze zijn 18 januari geleverd, gemaakt en staan klaar in ruimte 2a
9:10	Els	Garderobe bemannen	Garderobe	
			Grote hal	
9:00	Chris	Start		
10:00	Allen			

Communication
CISO
Backup & DR Operator
Security Research
Identity
Network

Practice, practice, practice

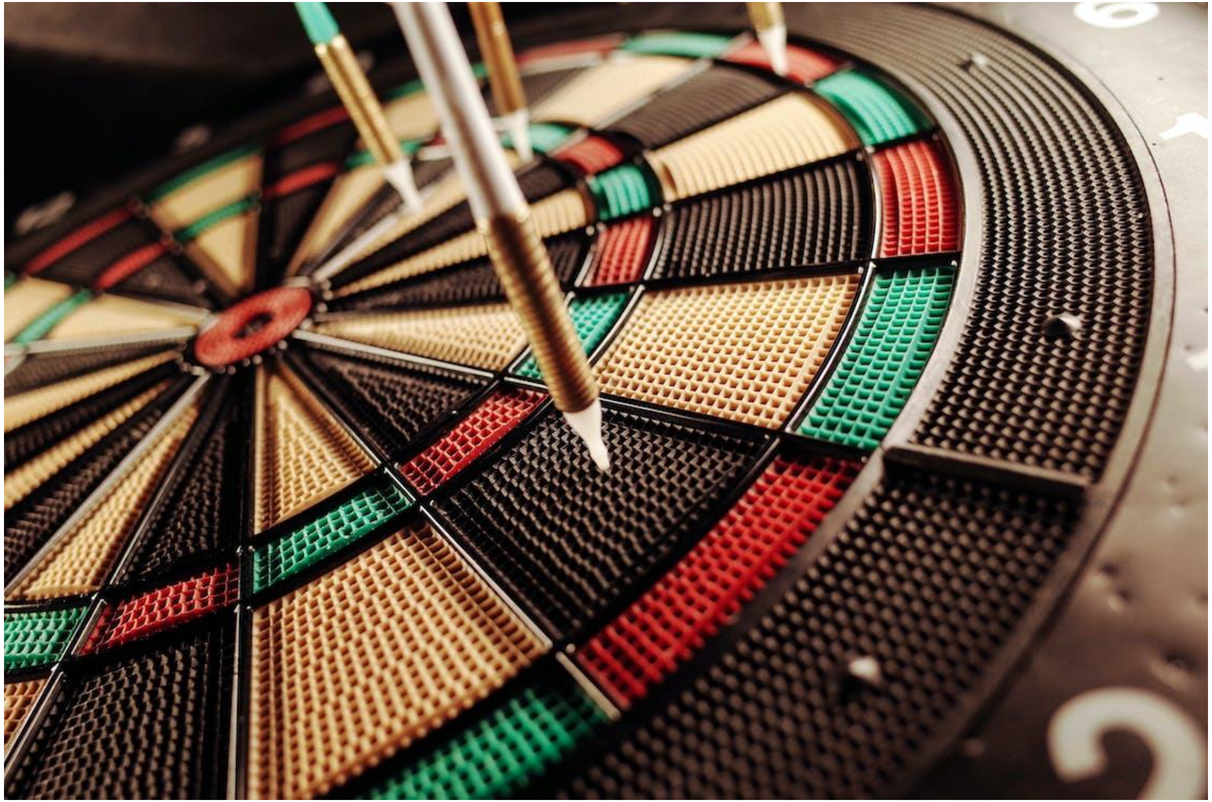
Leerpunten cyberoefening ISIDOOR 2021 | Rapport | Rijksoverheid.nl

Evaluate_

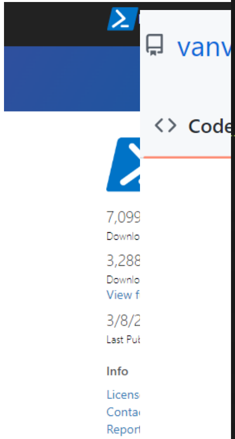
2 weeks later

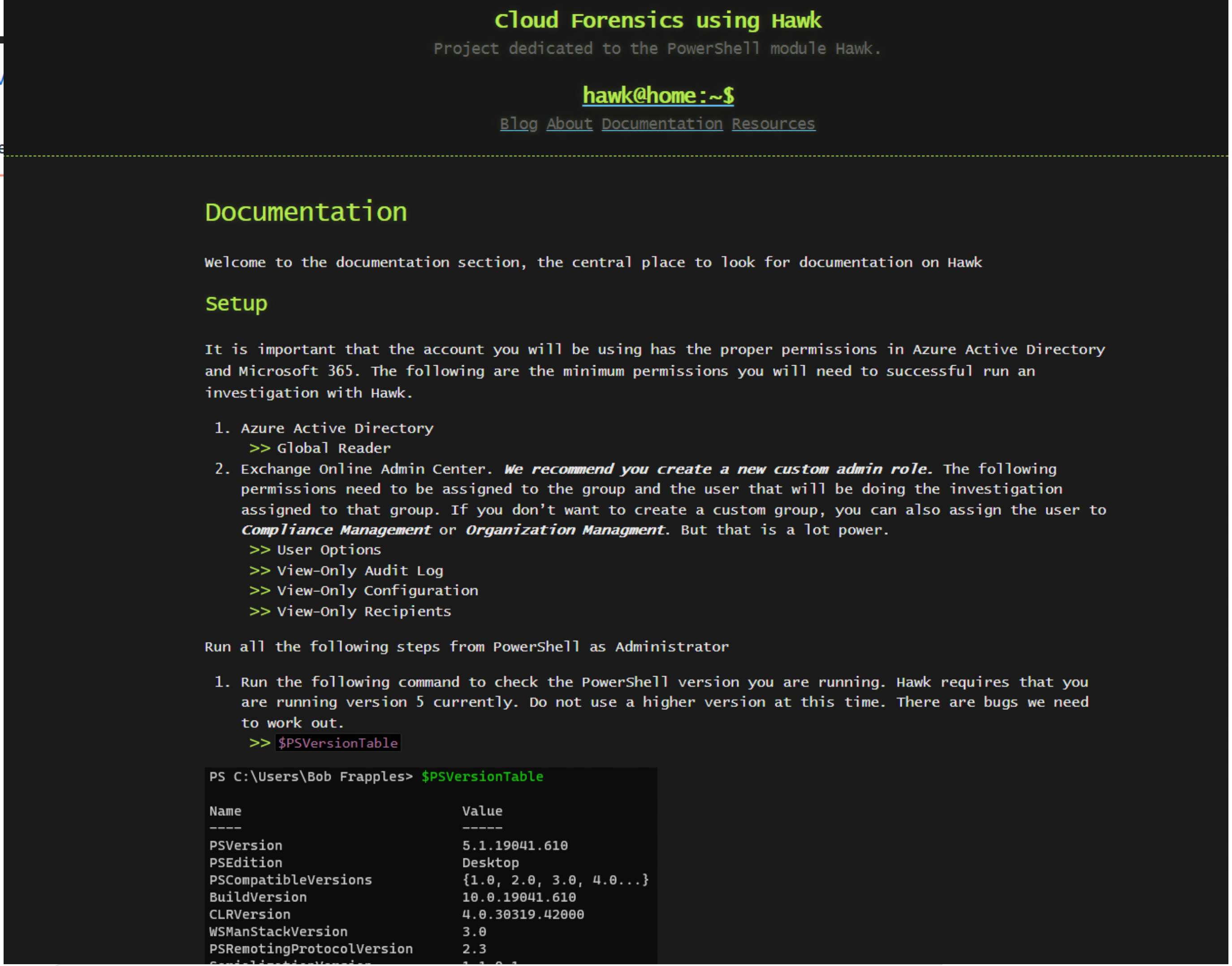
PROXSYS*

Tips for IR in 365_



Incident response playbooks | Microsoft Learn





Cloud Forensics using Hawk

Project dedicated to the PowerShell module Hawk.

hawk@home:~$

Blog About Documentation Resources

Documentation

Welcome to the documentation section, the central place to look for documentation on Hawk

Setup

It is important that the account you will be using has the proper permissions in Azure Active Directory and Microsoft 365. The following are the minimum permissions you will need to successful run an investigation with Hawk.

1. Azure Active Directory
   >> Global Reader
2. Exchange Online Admin Center. ***We recommend you create a new custom admin role.*** The following permissions need to be assigned to the group and the user that will be doing the investigation assigned to that group. If you don’t want to create a custom group, you can also assign the user to ***Compliance Management*** or ***Organization Managment***. But that is a lot power.
   >> User Options
   >> View-Only Audit Log
   >> View-Only Configuration
   >> View-Only Recipients

Run all the following steps from PowerShell as Administrator

1. Run the following command to check the PowerShell version you are running. Hawk requires that you are running version 5 currently. Do not use a higher version at this time. There are bugs we need to work out.
   >> `$PSVersionTable`

```
PS C:\Users\Bob Frapples> $PSVersionTable

Name                           Value
----                           -----
PSVersion                      5.1.19041.610
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.19041.610
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
```

PROXSYS*

Demo_

PROXSYS*

How did we do ?_

Wrapup

- Prepare
- Script
- Exercise
- Evaluate

QUIZ!

DUTCH

MICROSOFT SECURITY

MEETUP

PROXSYS*

Thank You!