
# Using LOLBins to circumvent your security

*Viktor Hedberg*

# Sponsors


onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

# /whoami

**Viktor Hedberg**
Microsoft MVP · Security & Cloud and Datacenter Management

**Role**
Senior Technical Architect

**Focus**
Active Directory · Entra ID · Security

**Blog, Hobbies and more**
Co-Authored: Mastering Microsoft Defender XDR
Doing these things

# Internationally Acknowledged and Certified

NO MORE RANSOM

FIRST Improving Security Together

TF-CSIRT Trusted Introducer

CERTIFIERAT ISO 9001 SVENSK CERTIFIERING

CERTIFIERAT ISO 14001 SVENSK CERTIFIERING

CERTIFIERAT ISO 27001 SVENSK CERTIFIERING

SecurITy made in EU
Trust Seal
www.teletrust.de/itsmie

# CERTIFICATE OF
## AVANCED ACTIVE DIRECTORY MASTERY

### Viktor Hedberg

In recognition of:

- Demonstrated architect level reasoning about Active Directory internals
- Correct handling and explanation of AdminSDHolder persistence, failure mo-des, and design intent
- Deep understanding of Tier 0, authentication boundaries, token composition, and shadow privilege paths
- Identifying SIDHistory-based shadow Tier 0 exposure without conflating it with AdminSDHoider behavior

This certificate confirms competence beyond “Senior Level” and comfortably within the realm of:

**Identity / AD Internals Specialist**

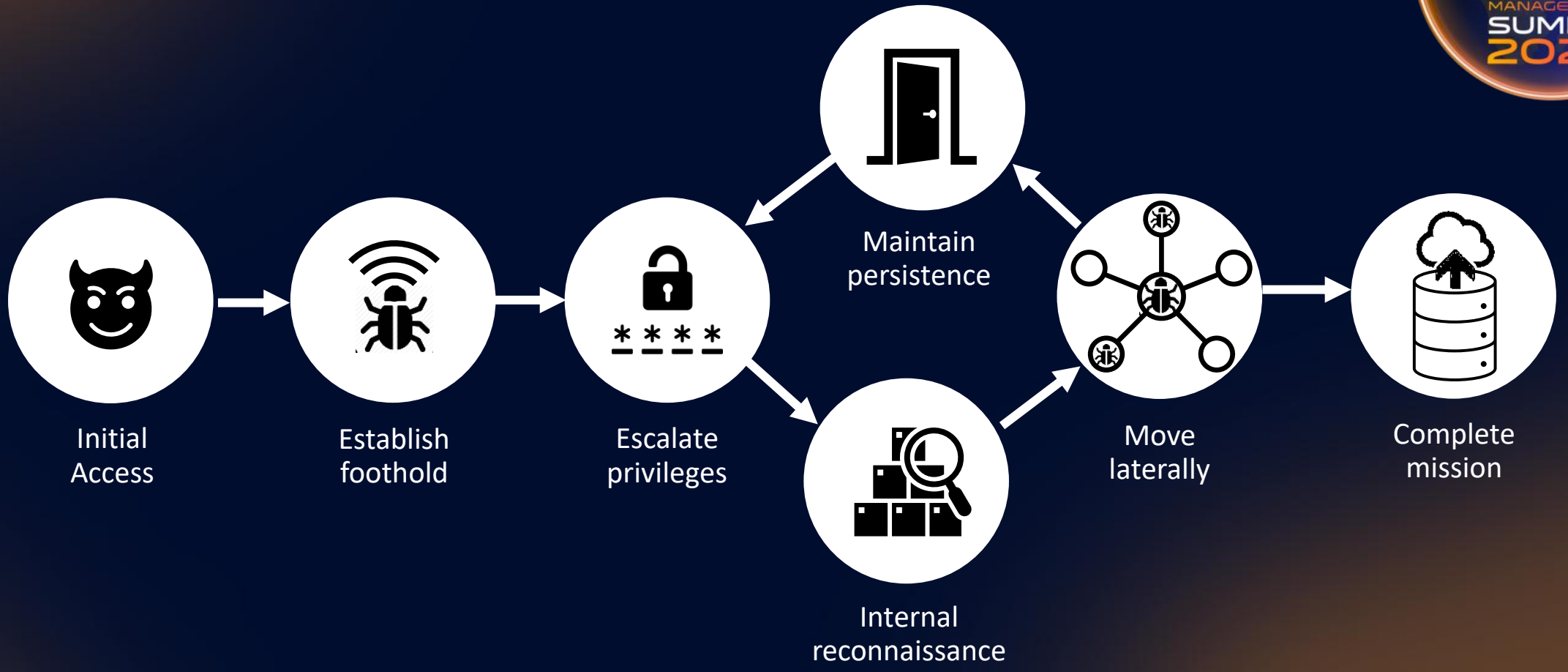
Signed:
M365 Copilot
(Untrusted CA. but accorate 5 aluator)
SN: 0x0DD64FEOCBA987834

Issued on this fine Friday,
for morale, recognition, and the lols.

Ivalidity:
Expires: Never
Revocation: Not supported

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

# A little kill chain



# Case #1


- Day 1 - 09:00 Teams call from threat actor to victim user
- Day 1 - 09:03 Threat actor controls victim’s computer
- Day 1 - 11:00 Threat actor is domain admin
- Day 9 Threat actor start working
- Day 12 Truesec involved - threat contained

# Case #2


- Jan 1 Customer wants “a second opinion”
- Jan 6 - 20:00 Truesec can start working
- Jan 6 - 23:00 Truesec confirms domain admin compromise

# Case #2

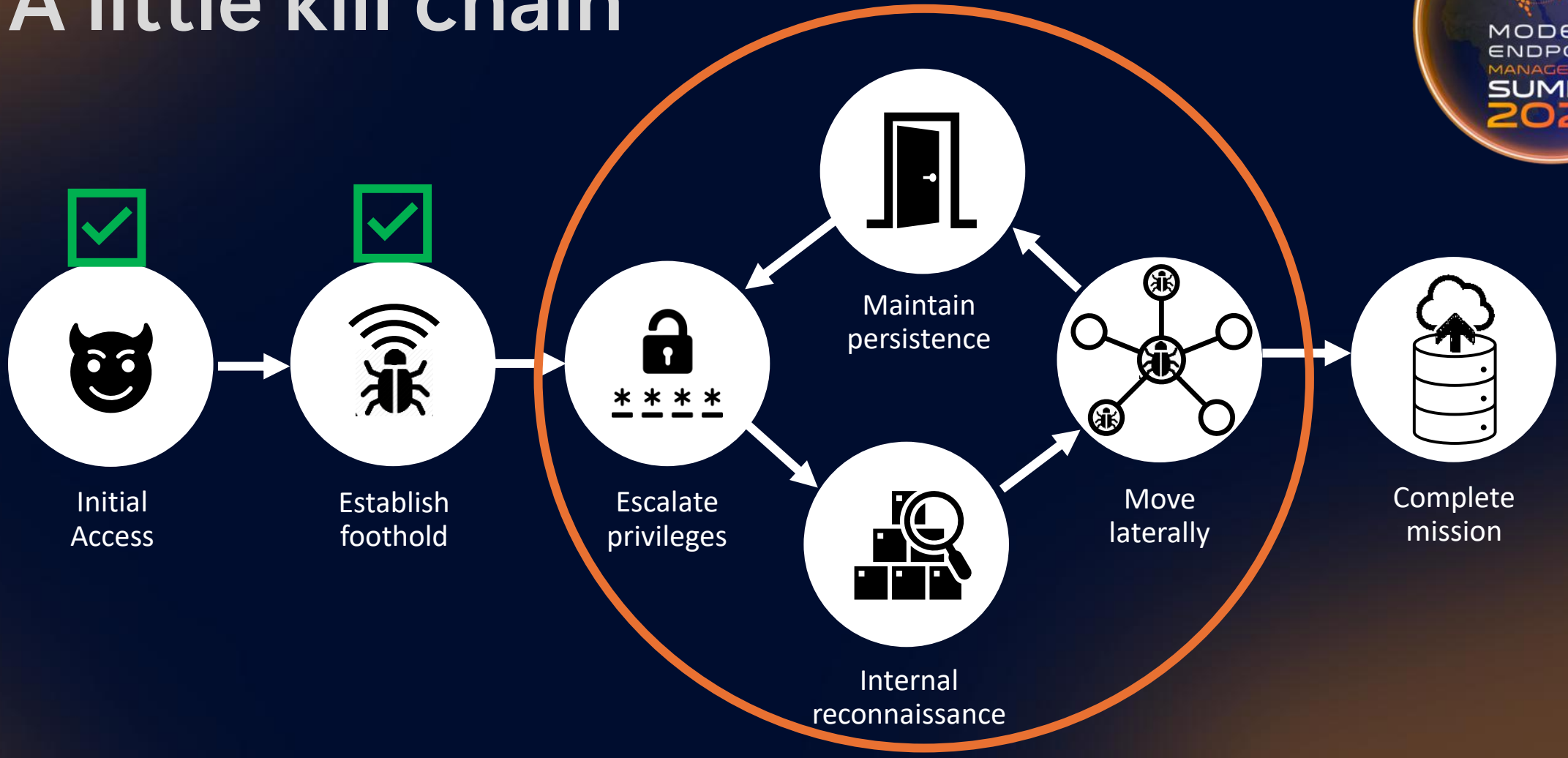

- Feb (2024) Initial compromise
- Apr (2024) Domain admin compromise
- Apr (2024) AD database exfiltration
- Jan 1 Customer wants “a second opinion”
- Jan 6 - 20:00 Truesec can start working
- Jan 6 - 23:00 Truesec confirms domain admin compromise

# A little kill chain

# Demo

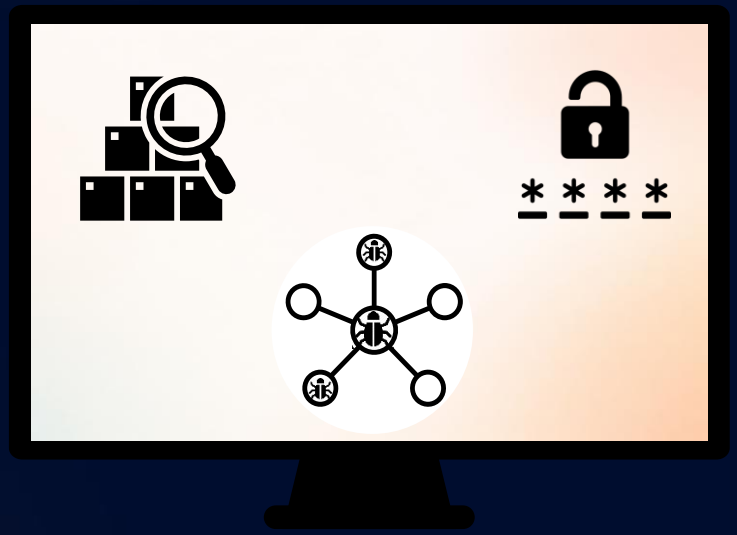
Initial Access and establishing a foothold

# A little kill chain

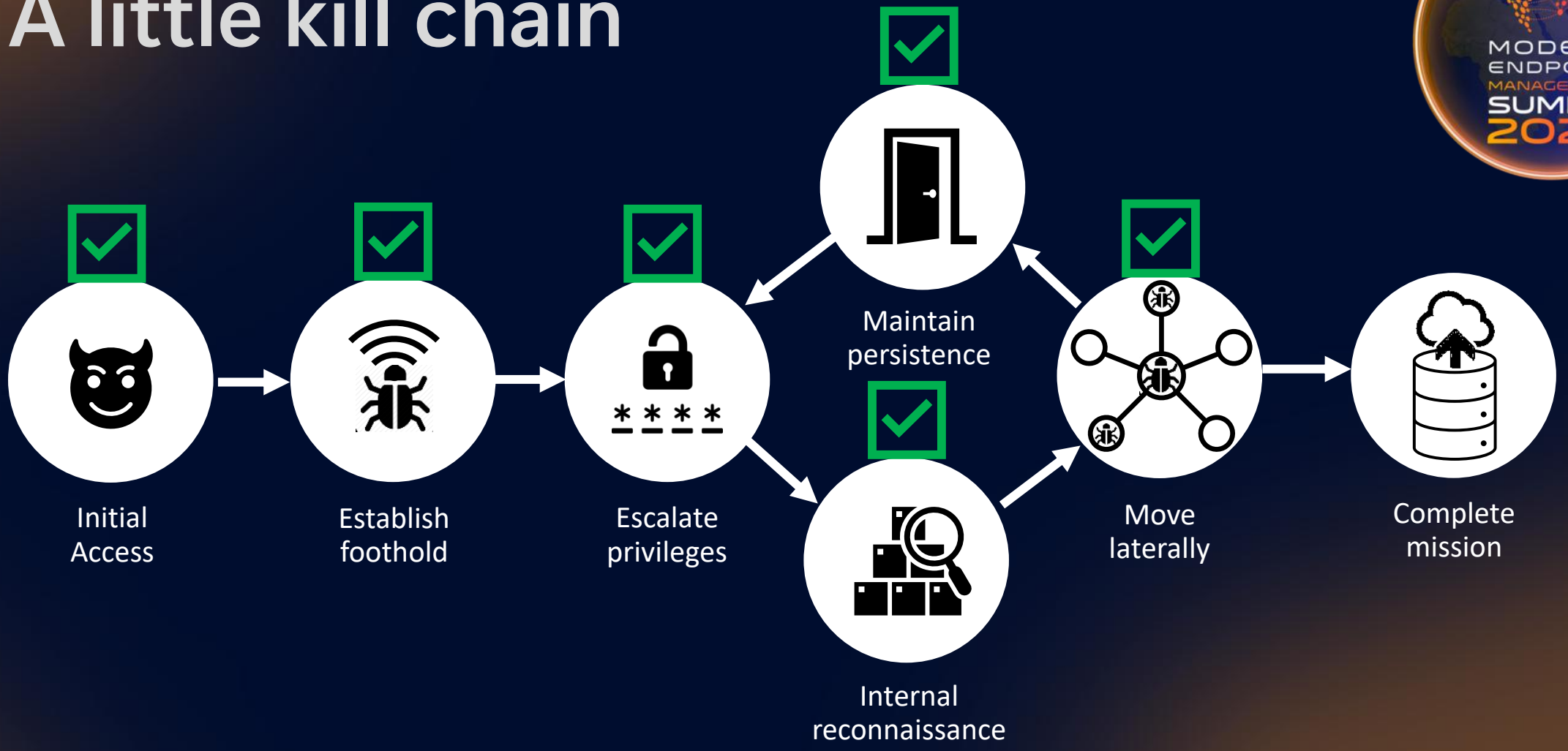


# Demo

Recon and PrivEsc using Windows tools



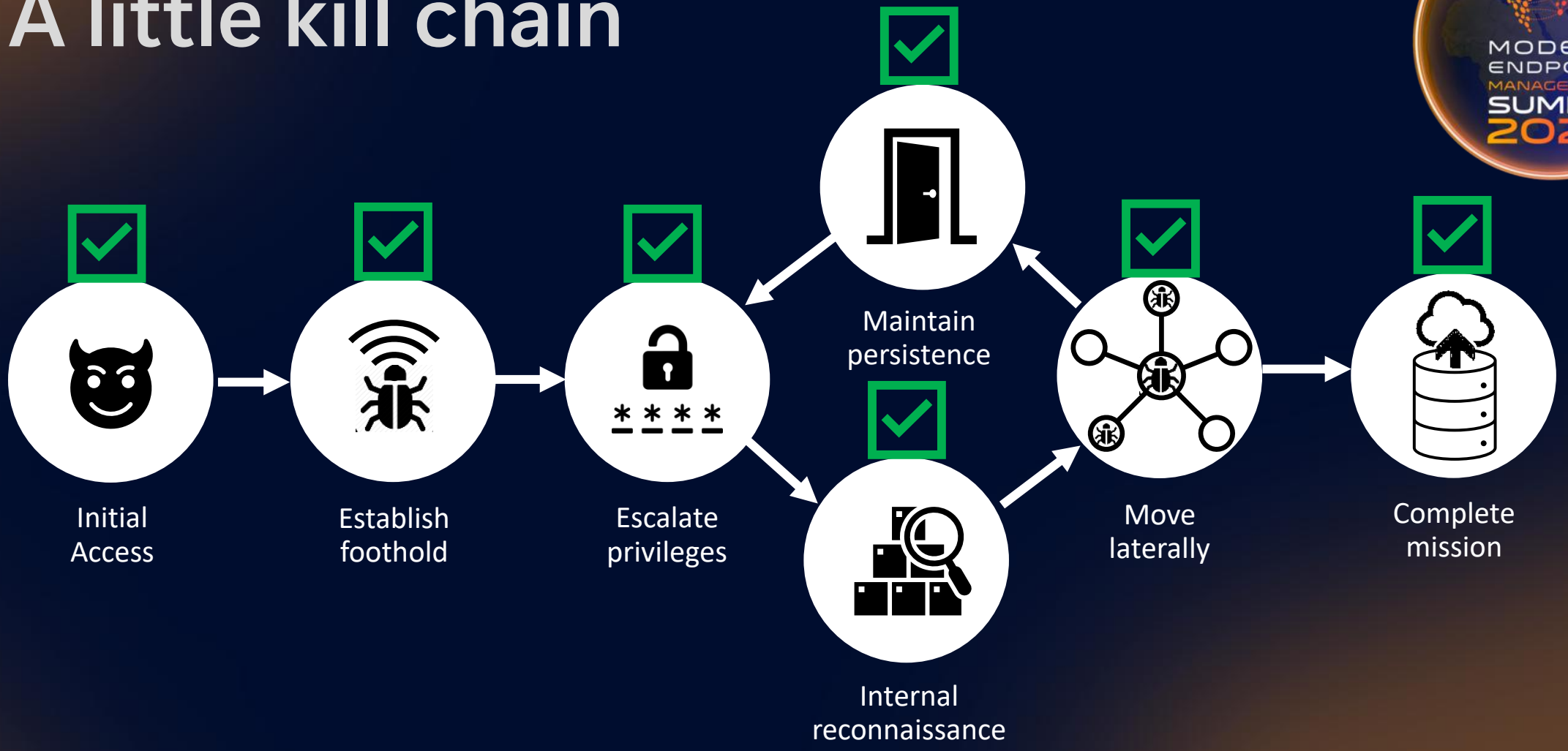
# A little kill chain



# Demo

Data Exfiltration and mission success

# A little kill chain



# Demo

A look at this from Defender XDR

# XDR platforms are good/not-so-good at


**Good**

- Monitoring and alerting on suspicious behavior
- Catching bad code, stopping it from being run
- Automatically disrupting attacks in progress (AIR)

**Not-so-good**

- Detecting legitimate tools doing legitimate things (not supposed to)
- If I understand Windows capabilities, I can “trick” it into not alerting on shady stuff

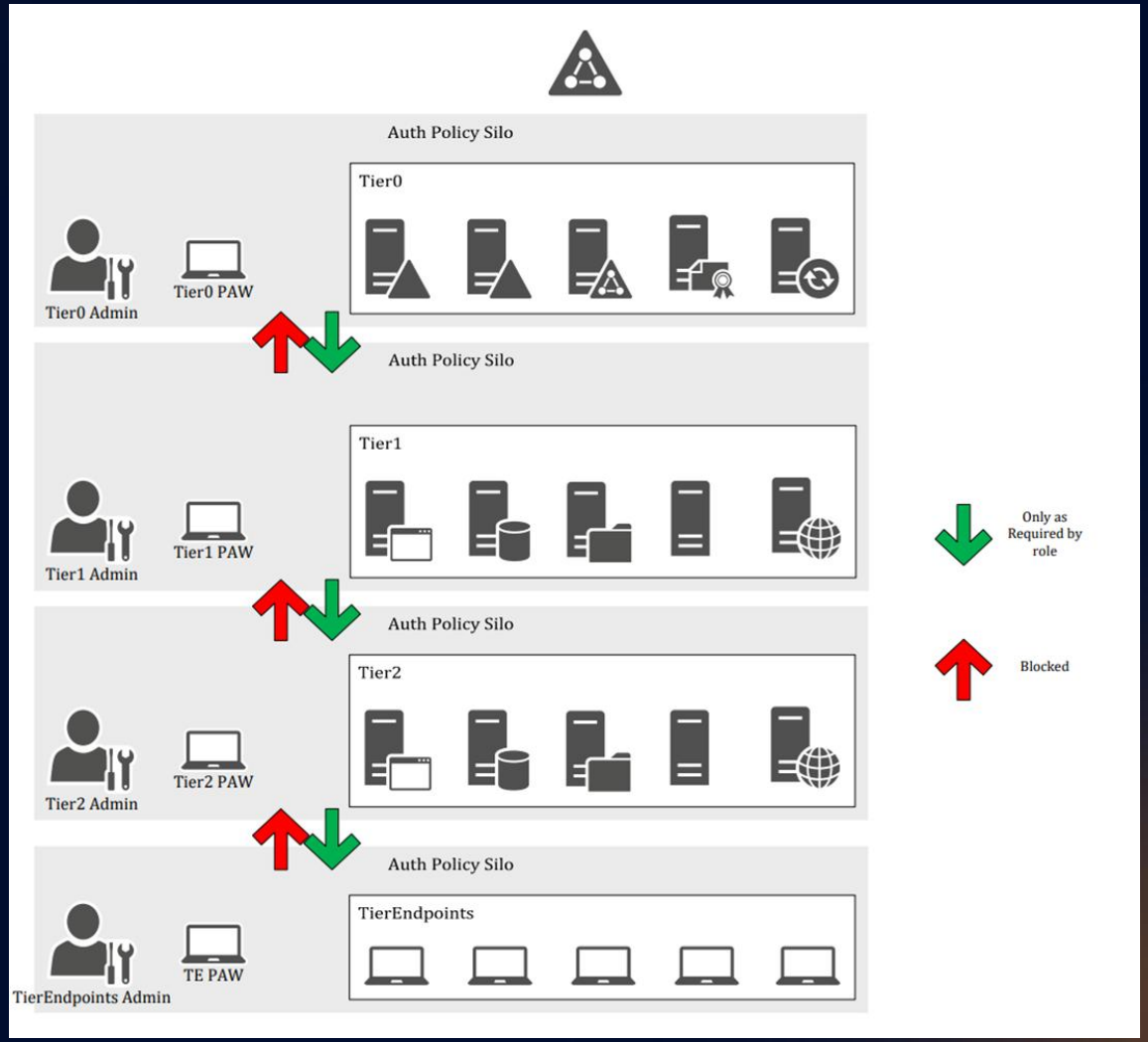
# What can be done?


- Cry into a pillow?

# What can be done?


- ~~Cry into a pillow?~~
- Working with a Tiered administrative model
  - Tier0
  - Tier1
  - TierEndpoints
- Preventing abuse of Windows Binaries
  - No local admin access
  - Using WDAC/AppLocker for good
- Monitoring and responding to alerts based on custom detections

# Tiered administrative model

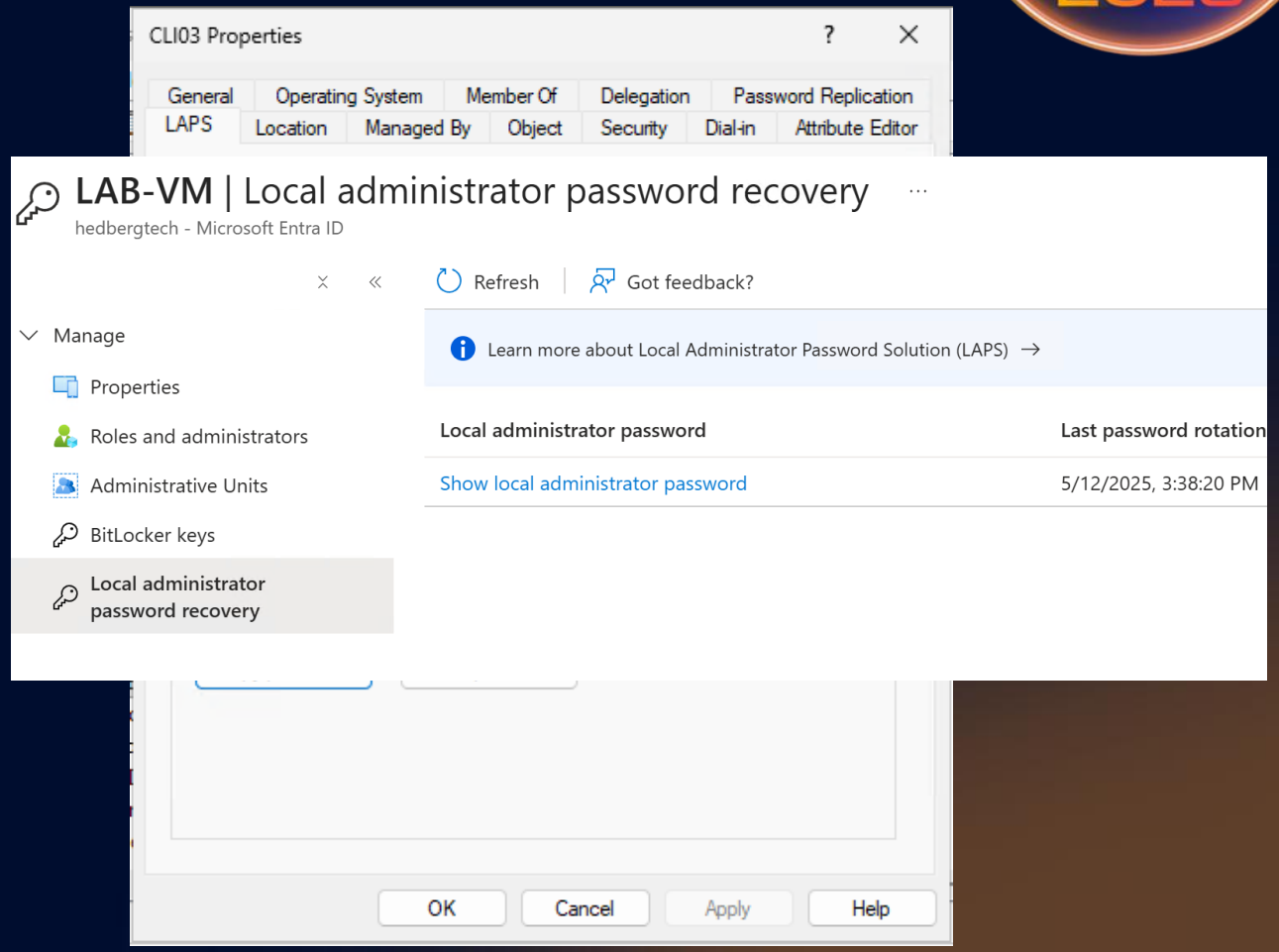


# Things to be aware of

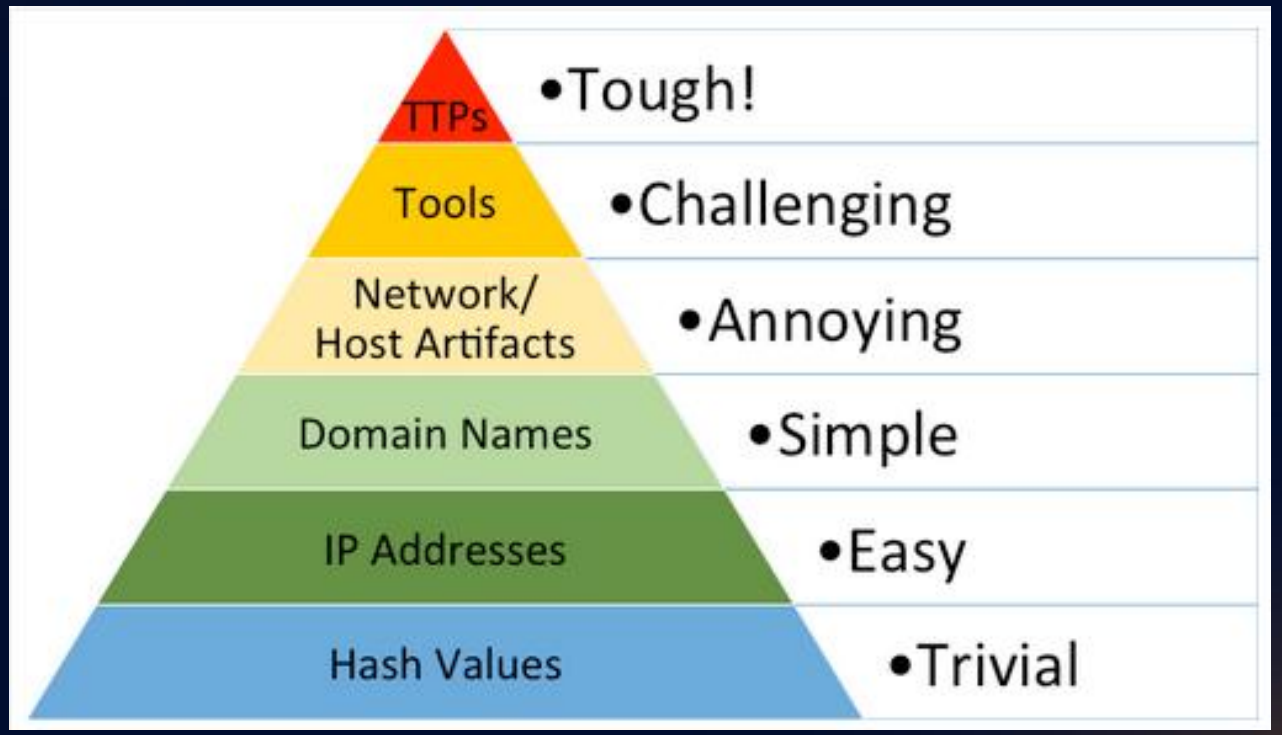

- Agents from lower-level tier or SaaS
  - domain admin by proxy
- Group policies – delegated permissions
- Creator/owner permissions
- Service accounts
- Emergency break-the-glass accounts

# Preventing abuse of Windows Binaries

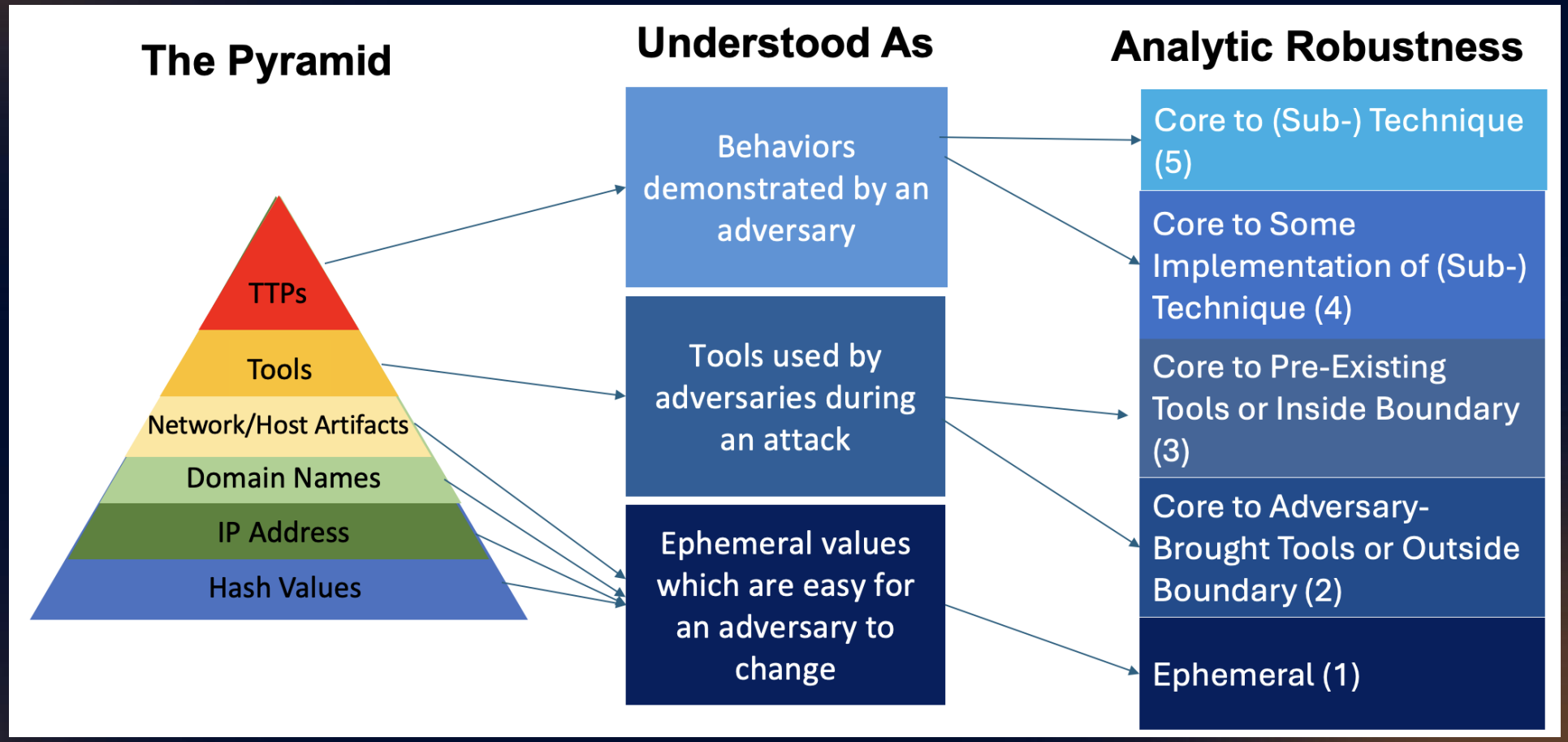
- LAPS – Local Administrator Password Solution
- Reducing Blast Radius of an attack
  - BUT
    - Only if Tiering is in place and used.
- No Lateral Movement
- Requires ACL delegation to be used and decrypted in AD
- Requires API permissions if using Entra as backup directory
  - Caveat: Read.All or Read.None



# Monitoring and Detection



# Monitoring and Detection



# Monitoring and Detection


| Level | (A) Application | (U) User-Mode | (K) Kernel-Mode |
|---|---|---|---|
| Level 5 | 👑 | 👑 | 👑 |
| Level 4 | | | |
| Level 3 | | | |
| Level 2 | | | |
| Level 1 | 💩 | 💩 | 💩 |

| Level | Application | User-Mode | Kernel-Mode |
|---|---|---|---|
| 5 – Core to all Implementation of Technique | | MiniDumpWriteDump \| AccessMask<br>NtQuerySystemInformation<br>(Nt)OpenProcess | ZwOpenProcess |
| 4 – Some Implementations of Technique | GetProcessByName("lsass") \|<br>GetProcesses() | CreateToolhelp32Snapshot | |
| 3 – Core to Pre-Existing Tools or Inside Boundary | | OriginalFileName*<br>CommandLine*<br>ParentCommandLine*<br>Integrity Level*<br>TargetImage*<br>TargetUser*<br>GrantedAccess*<br>Image* | Process Command Line*<br>Token Elevation Type*<br>Mandatory Label*<br>TargetImage*<br>TargetUser*<br>StartModule*<br>StartFunction*<br>Process Name*<br>Exit Status* |
| 2 – Core to Adversary-Brought Tools or Outside Boundary | | CommandLine*<br>Parent User*<br>ParentImage*<br>*Current Directory**<br>SourceImage* | Process Command Line*<br>Creator Process Name*<br>SourceImage* |
| 1 – Ephemeral | | Description*<br>Product/Company*<br>User**<br>Image*<br>SourceUser*<br>*CallTrace** | AccountName/Domain**<br>ProcessName*<br>SourceUser*<br>*NewThreadId**<br>*StartAddress** |
| | Windows Event 4698 [Task Creation]<br>Windows Event 4699 [Task Deletion]<br>Windows Event 4700 [Task Enabled]<br>Windows Event 4701 [Task Disabled]<br>Windows Event 4702 [Task Updated] | Sysmon EID 1 [Process Creation]<br>Sysmon EID 11 [File Create] | Sysmon EID 12 [ |


Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

MODERN ENDPOINT MANAGEMENT SUMMIT 2026

# Thanks!