

Today

Azure AD Connect Fileless Malware

by

TEMS SECURITY SERVICES





PHILIP BERGER

MICHAEL MEIXNER

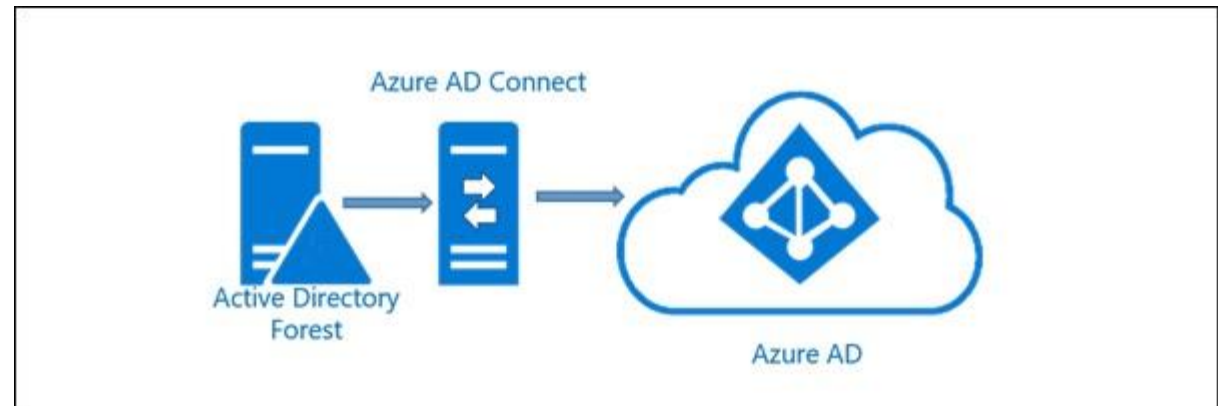
Agenda

- Azure AD Connect
- Fileless Malware (PoC)

Azure AD Connect

Azure AD Connector

- NTLM Passwords are stored in MD4 Format
- Passwords are encoded with UTF-16 binary format
- Password length limited to 16-bytes
- No MD4 Password hash will be sent through the Azure AD Connector to Microsoft



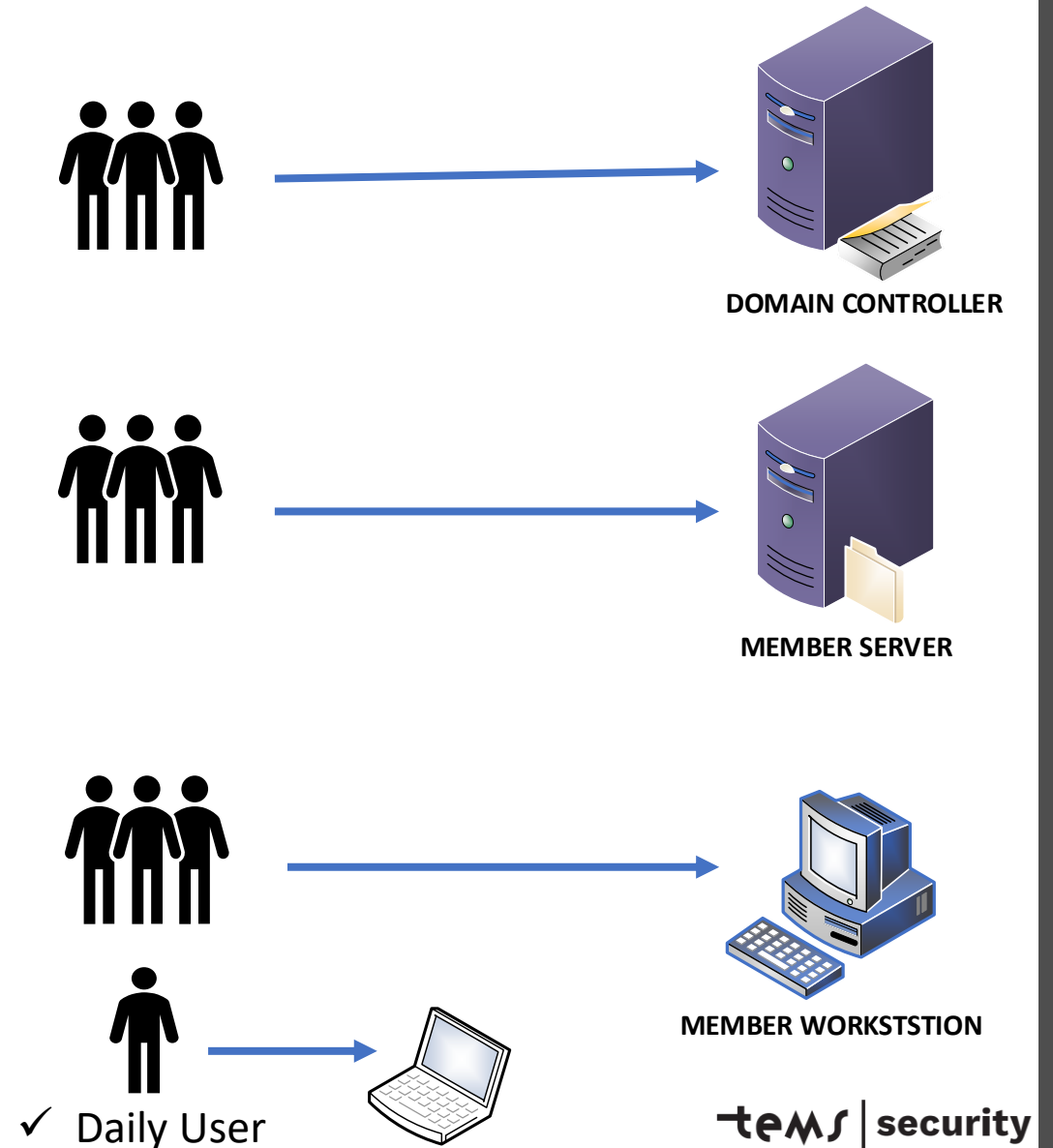
Poll 1:
In which Tier Level Model should
an Azure AD Sync Server run



1. Tier 0
2. Tier 1
3. Tier 2
4. Any Tier Level will be fine
5. I don't know

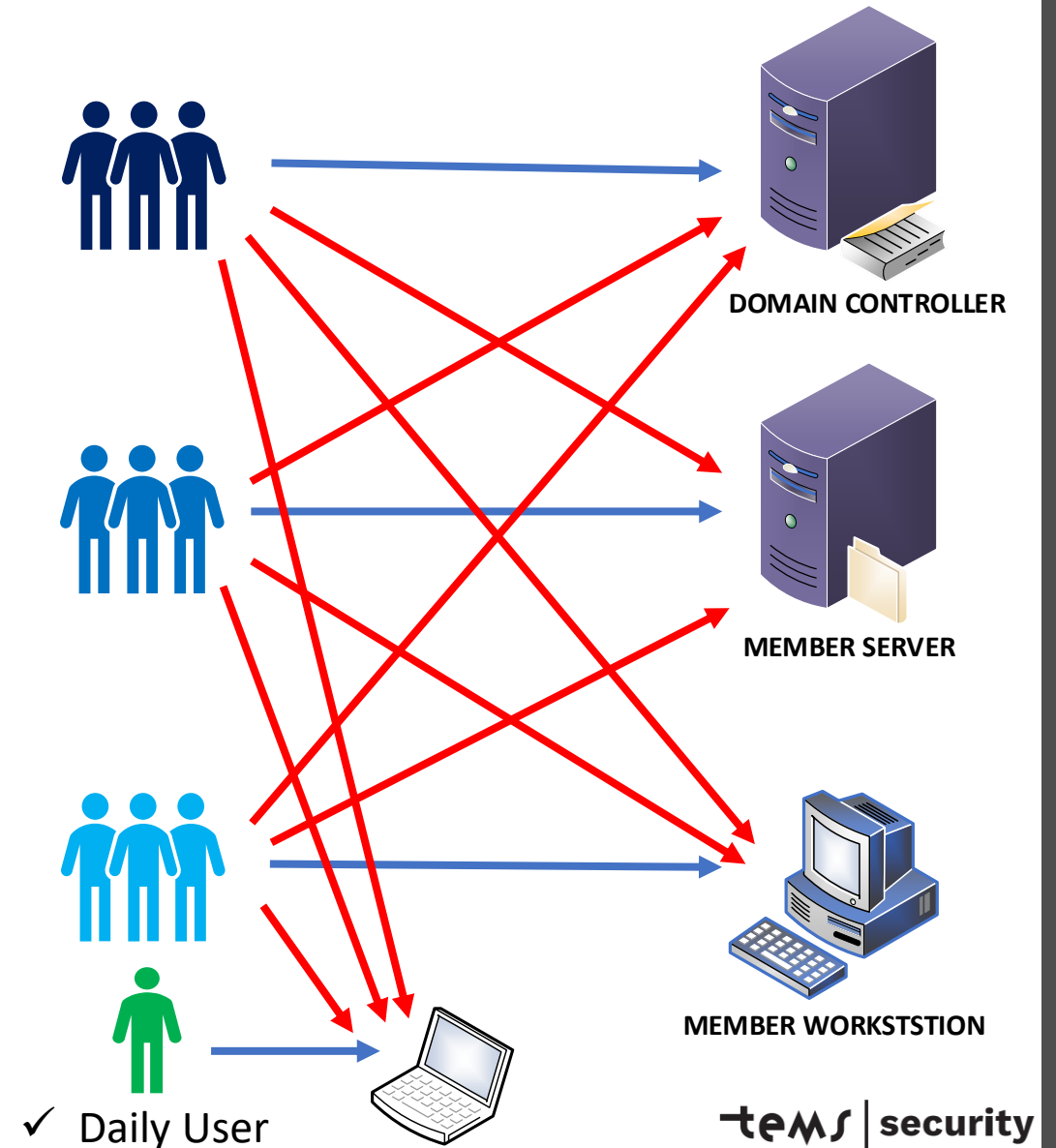
Tier Level Model (Basic implementation)

- ❑ Four user accounts for Domain Admins
- ❑ Three user accounts for Server Admins
- ❑ Two user accounts for Desktop Admins
- ❑ Easy to implement with IT-Security focus
- ❑ Challenge for hacker to gain access to Servers or Domain Controllers



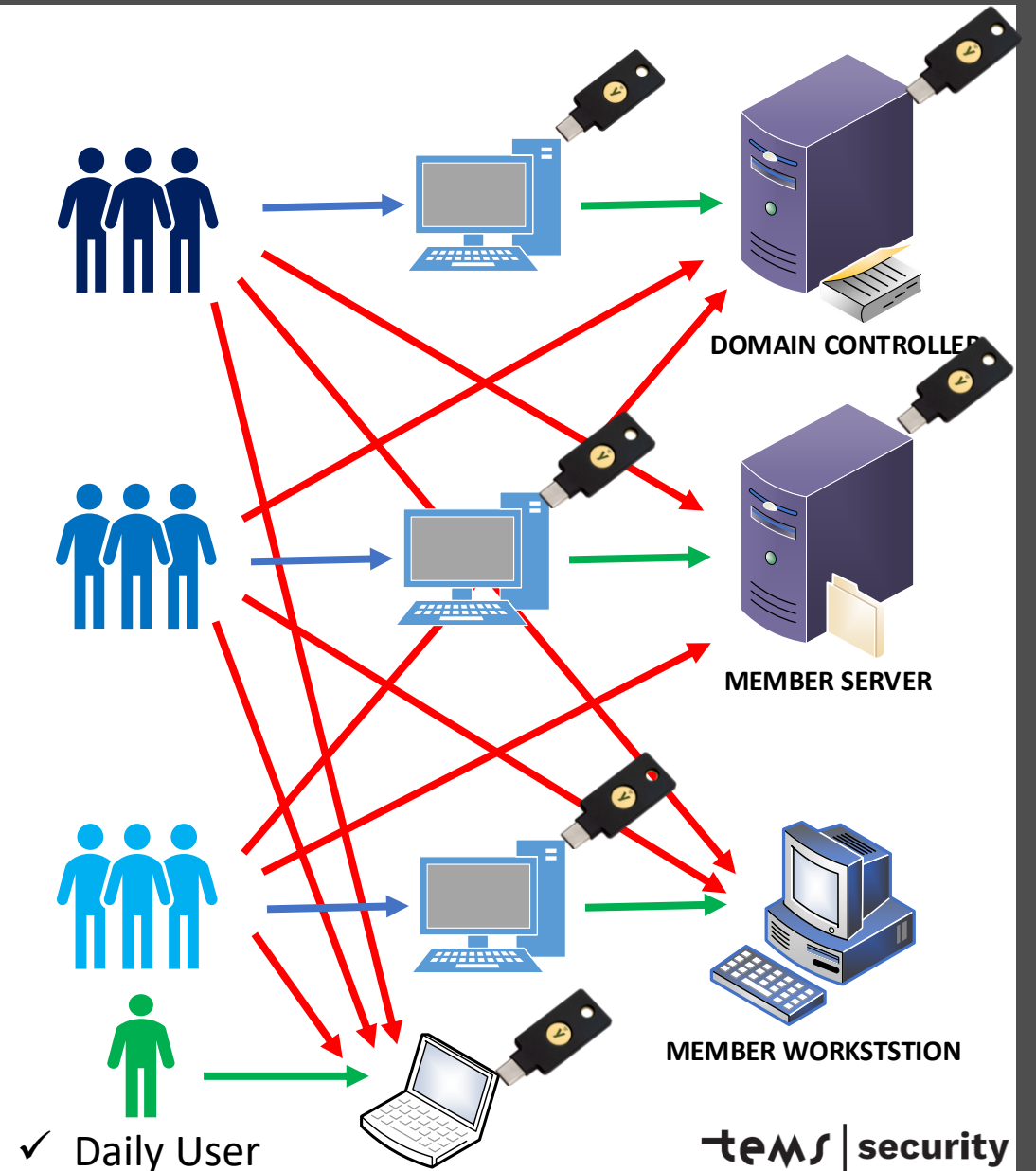
Tier Level Model (with enforcement)

- ❑ Four user accounts for Domain Admins
- ❑ Three user accounts for Server Admins
- ❑ Two user accounts for Desktop Admins
- ❑ Easy to implement with IT-Security focus
- ❑ Difficult for hacker to gain access to Servers or Domain Controllers



Tier Level Model (state of the Art)

- ❑ Administration only with "Privileged Access Workstation" (aka PAW)
- ❑ Four user accounts for Domain Admins
- ❑ Three user accounts for Server Admins
- ❑ Two user accounts for Desktop Admins
- ❑ Easy to implement with IT-Security focus
- ❑ Very difficult for hacker to move laterally within the network

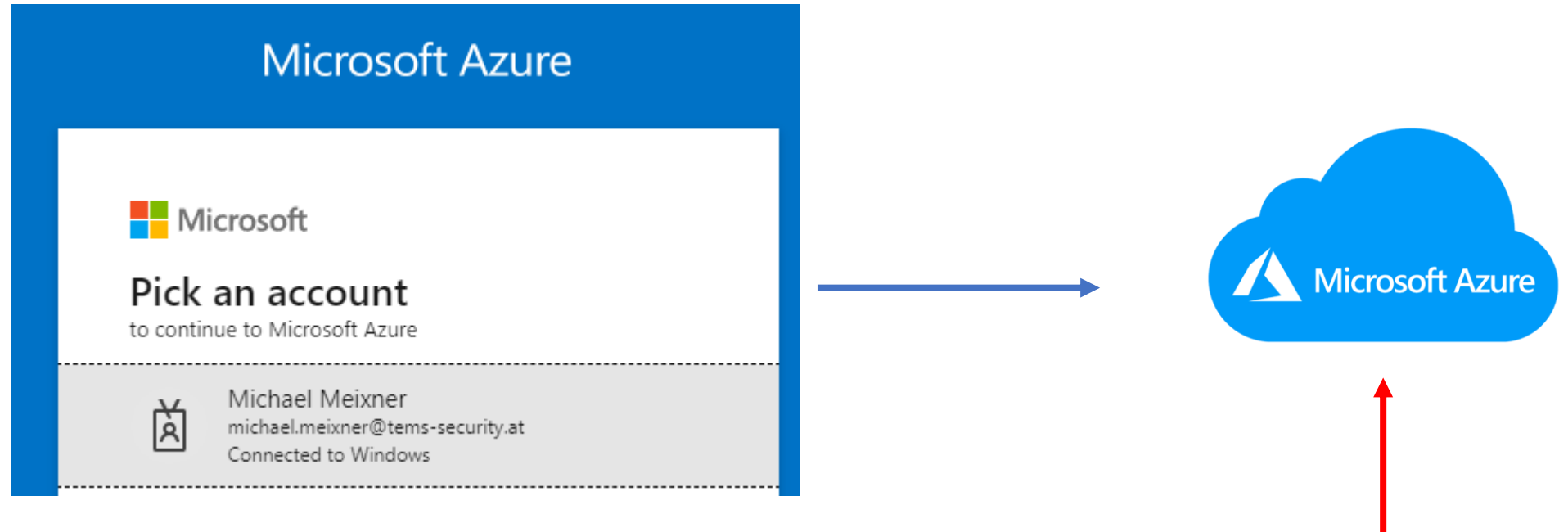


Poll 2:
What is the maximal password
length (character) in Active Directory



1. 32
2. 64
3. 96
4. 128
5. 1000

Azure AD Logon with OnPrem Password



MD4+salt+PBKDF2+HMAC-SHA256 (1000 iterations) = 32-byte hash

Password-Based Cryptography
Specification Version 2.0 (RFC2898)

Computes a Hash-based
Message Authentication Code

Active Directory Password

- The field length is 16 bytes
- 1 byte = 8 bits
- $16 * 8 = 128$ characters

MD4+salt+PBKDF2+HMAC-SHA256

What can we sync with Azure AD Connector



Password Sync from OnPrem to Azure AD
(default every 2 min.) -
User based.



User attribute
(enabled, Name, cn, co,
company, country
Code, Force Password
Change on Next Logon,
....)



Mailbox attribute
(Mailbox and Public
Folders)



Computer objects



AD Groups



Azure AD app
Office 365, Exchange
Online, Share, Azure
RMS, Intune, CRM
and 3rd party

Hybrid Authentication
 - Password Hash Sync (PHS) + SSO
 - Pass-Through Authentication (PTA) + SSO
 - Federated Authentication (ADFS)

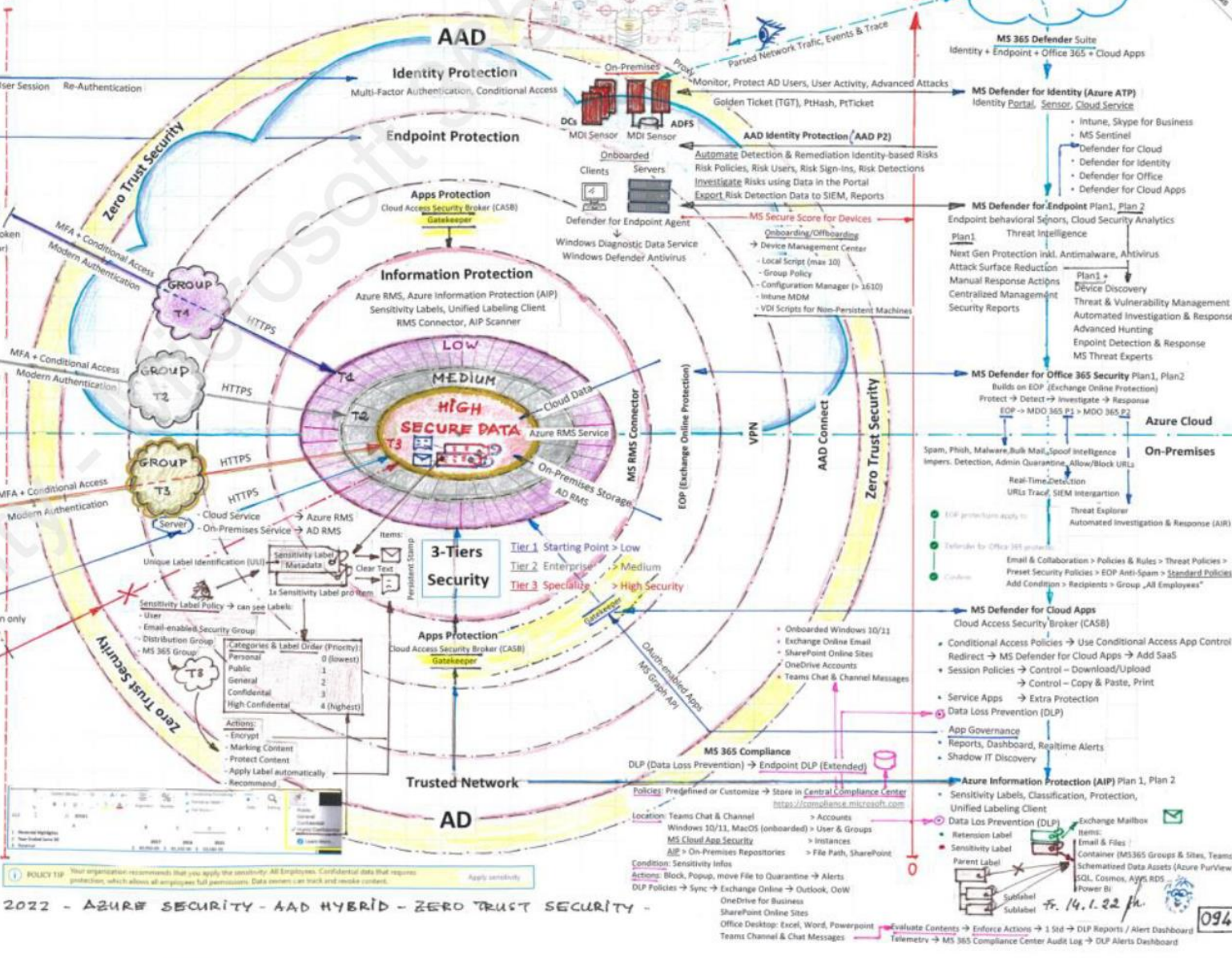
Conditional Access Evaluation (CAE)
 CAE enabled Client → CAE enabled Services
 Outlook, Office, Teams, Exchange, SharePoint, Teams, OneDrive

Trusted Network
 - TPM 2.0
 - Credential Guard
 - BitLocker
 - Modern Authentication
 - Windows Hello For Business
 - VPN-Split Client

AIP Clients
 - Office Built-in Labeling Solution
 - AIP Classic Client (Legacy) + 3.2021
 - AIP Unified-Labeling Client
 - File Explorer Support
 - PowerShell Support
 - Viewer protected PDF + Image
 - Scanner for On-Premises Data Store

Conditional Access
 Groups: T3
 Client Apps: Modern Authentication
 Access Control: Device Compliance
 Devices: Domain Joined
 Platform Type: Windows
 Application: App approved
 Location: IP-Range Trusted Network
 Sensitivity Label Policy: AIP enabled

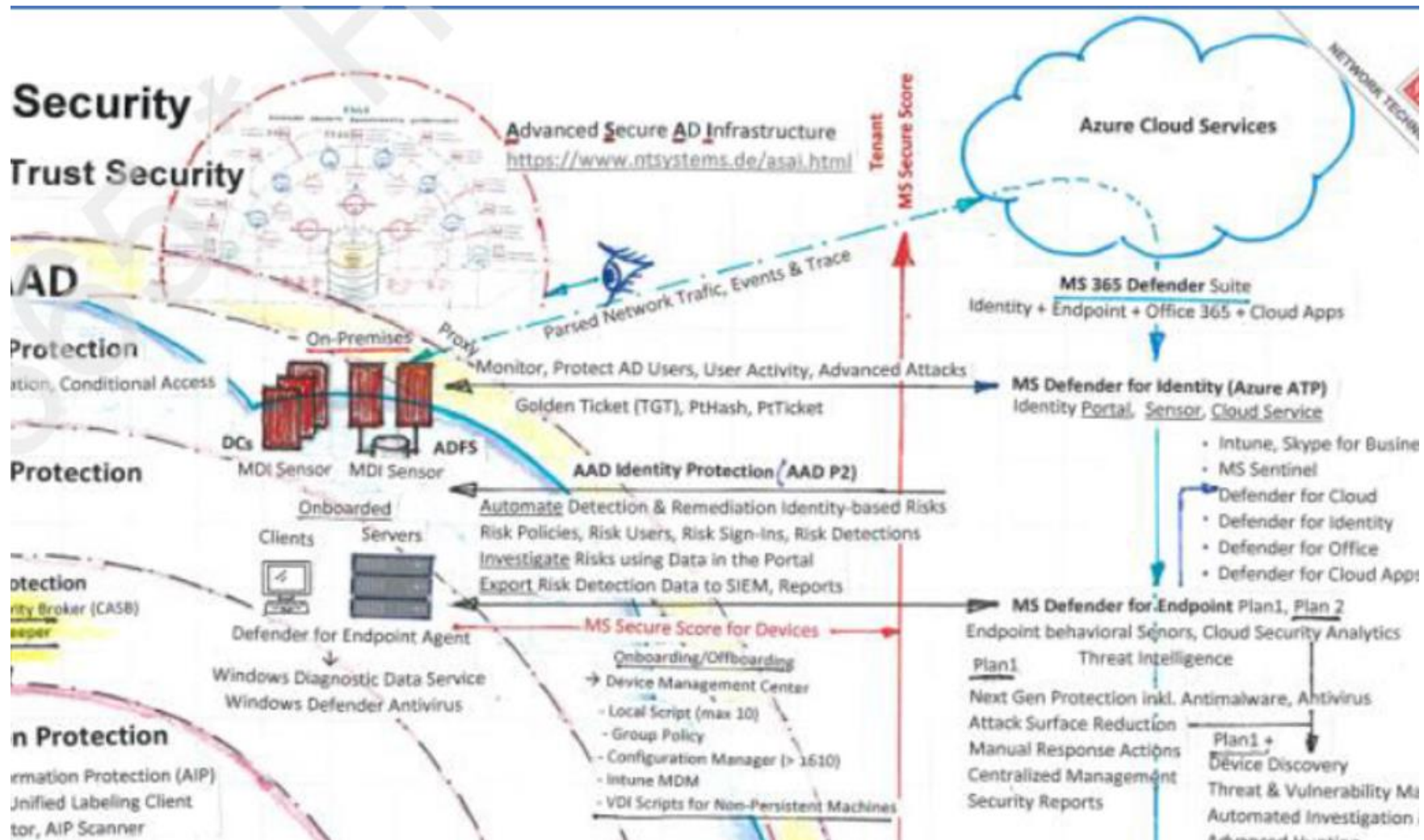
Azure Security
MS 365 Zero Trust Security



3-Tiers Security
 Tier 1 Starting Point > Low
 Tier 2 Enterprise > Medium
 Tier 3 Specialize > High Security

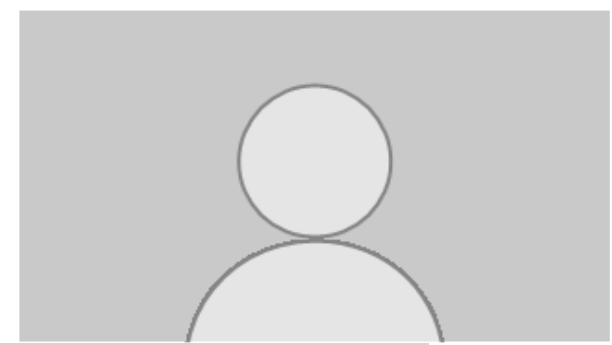
MS 365 Compliance
 DLP (Data Loss Prevention) → Endpoint DLP (Extended)
 Policies: Prerequisite or Customize → Store in Central Compliance Center
 Location: Teams Chat & Channel, Windows 10/11, MacOS (onboarded) → User & Groups, MS Cloud App Security, AIP → On-Premises Repositories → File Path, SharePoint
 Condition: Sensitivity Infos
 Actions: Block, Popup, move File to Quarantine → Alerts
 DLP Policies → Sync → Exchange Online → Outlook, OneDrive for Business, SharePoint Online Sites
 Office Desktop: Excel, Word, Powerpoint
 Evaluate Contents → Enforce Actions → 1. Sid → DLP Reports / Alert Dashboard
 Telemetry → MS 365 Compliance Center Audit Log → DLP Alerts Dashboard

Communication flow Azure AD Connect



Azure AD Connect

Azure AD Connect – OnPrem setup

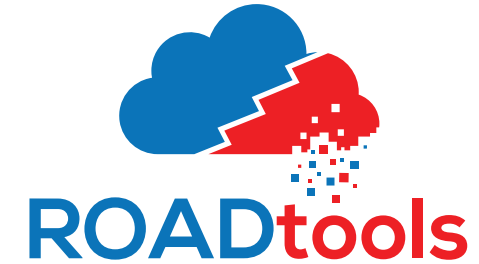


- ✓ 2 Server (1x active, 1x staging)
- ✓ Member Server only
- ✓ No Sync of Admin accounts
- ✓ No Sync of Admin workstations
- ✓ Lockdown Server with YubiKeys (restrict shares and remote PowerShell)
per Firewall rule on Windows Server
- ✓ Strict separation between OnPrem and Azure Admin accounts
- ✓ Configure PIM for all high-privileged tasks
- ✓ Tier Level Model for OnPrem
- ✓ Disable Legacy Authentication
- ✓ Active Monitoring of OnPrem Server

Pass-the-PRT Attacks

Primary Refresh Token

Pass-the-cookie attacks



- A PRT is issued to users only on registered devices. A registered device can either be an Azure AD joined, Hybrid AD joined or AD registered.

1. Dump of an office app
2. Parse with strings for `eyJ0eX`
3. Use the cookie

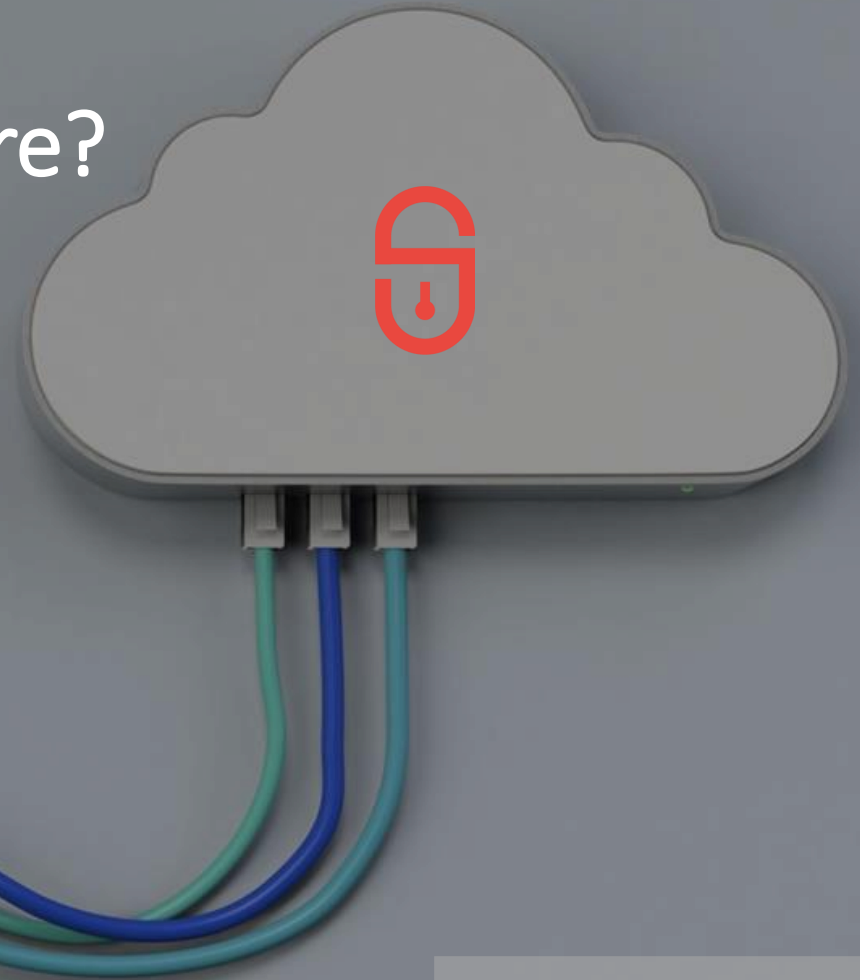
```
roadrecon auth --prt-init  
Requested nonce from server to use with ROADtoken: AQABAAAAAB2UyzwtQEKR7-rWbgdcBZIJ3LUNT8vP0ZW8dI8AB3zTVy1r1rTFR35qK3
```

Fileless Malware

Poll 3:

Do you know about Fileless Malware?

1. Yes, of course
2. Sorry I don't

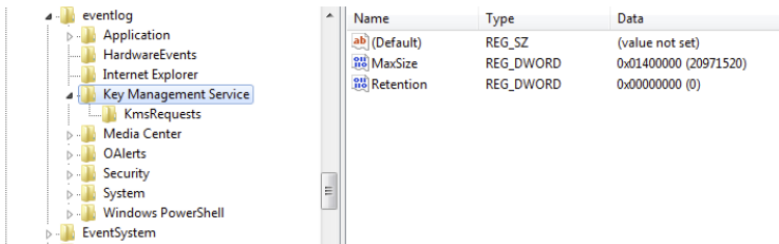


One Example of Fileless Malware

Dropper in DLL, search order hijacking

We start custom module analysis from the wrapper-dropper dynamic library. This code is injected into Windows processes such as explorer.exe. At its single entry point after being loaded into the virtual address space of the launcher process, the dropper removes files created by previous stages or executions.

Firstly, the module copies the original legitimate OS error handler WerFault.exe to C:\Windows\Tasks. Then it drops one of the encrypted binary resources to the wer.dll file in the same directory for typical DLL search order hijacking. For the sake of persistence, the module sets the newly created WerFault.exe to autorun, creating a Windows Problem Reporting value in the Software\Microsoft\Windows\CurrentVersion\Run Windows system registry branch.



The dropper not only puts the launcher on disk for side-loading, but also writes information messages with shellcode into existing Windows KMS event log

The dropped wer.dll is a loader and wouldn't do any harm without the shellcode hidden in Windows event logs. The dropper searches the event logs for records with category 0x4142 ("AB" in ASCII) and having the Key Management Service as a source. If none is found, the 8KB chunks of shellcode are written into the information logging messages via the ReportEvent() Windows API function (lpRawData parameter). Created event IDs are automatically incremented, starting from 1423.

Launcher in wer.dll

This launcher, dropped into the Tasks directory by the first stager, proxies all calls to wer.dll and its exports to the original legitimate library. At the entry point, a separate thread combines all the aforementioned 8KB pieces into a complete shellcode and runs it. The same virtual address space, created by a copy of the legitimate WerFault.exe, is used for all this code.

persistence,

8KB chunks of shellcode

Key Management Service as a source

shellcode hidden in Windows event logs.

Event log with chunk of Binary data

The screenshot shows the Windows Event Viewer interface. The left pane displays the navigation tree, with 'Applications and Services Logs' expanded and 'Key Management Service' selected. The main pane shows a list of 34 events from the 'Key Management Service'. The selected event, ID 1337, is expanded to show its details. The 'Details' tab is active, displaying a large block of binary data represented in hexadecimal characters.

Level	Date and Time	Source	Event ID
Information	21/05/2022 12.46.54	Cobalt	1337
Information	21/05/2022 12.46.54	Cobalt	1337
Information	21/05/2022 12.46.54	Cobalt	1337
Information	21/05/2022 12.46.54	Cobalt	1337
Information	21/05/2022 12.46.54	Cobalt	1337
Information	21/05/2022 12.46.54	Cobalt	1337

Event 1337, Cobalt

General Details

```
4D5A4152554889E54881EC20000000488D1DEAFFFFFFF4889DF4881C39C640100FFD341B8F0B5A25  
668040000005A4889F9FFD0000000000000000000000000F80000000E1FBA0E00B409CD21B8014CCD21546  
869732070726F6772616D2063616E6E6F742062652072756E20696E20444F53206D6F64652E0D0D0A  
24000000000000EFDABAE0ABBBD4B3ABBBD4B3ABBBD4B3CD551AB3AABBD4B3885406B333B  
BD4B3351B13B3AABBD4B35A7D1BB382BBD4B35A7D1AB322BBD4B35A7D19B3A1BBD4B3A2C34  
7B3A0BBD4B3ABBBD5B379BBD4B388541AB39FBBD4B3CD551EB3AABBD4B3CD5518B3AABBD4B
```

<https://github.com/improsec/SharpEventPersist>

Event log Detail Information

Event Properties - Event 8224, VSS

General **Details**

Friendly View XML View

+ System
- **EventData**

2D20436F64653A2020434F5253564343303030303037

Binary data:

In Words

```
0000: 6F43202D 203A6564 524F4320 43435653
0010: 30303030 32373730 6143202D 203A6C6C
0020: 524F4320 43435653 30303030 34353730
0030: 4950202D 20203A44 30303030 38323638
0040: 4954202D 20203A44 30303030 34363636
0050: 4D43202D 20203A44 575C3A43 4F444F49
```

Event Properties - Event 8224, VSS

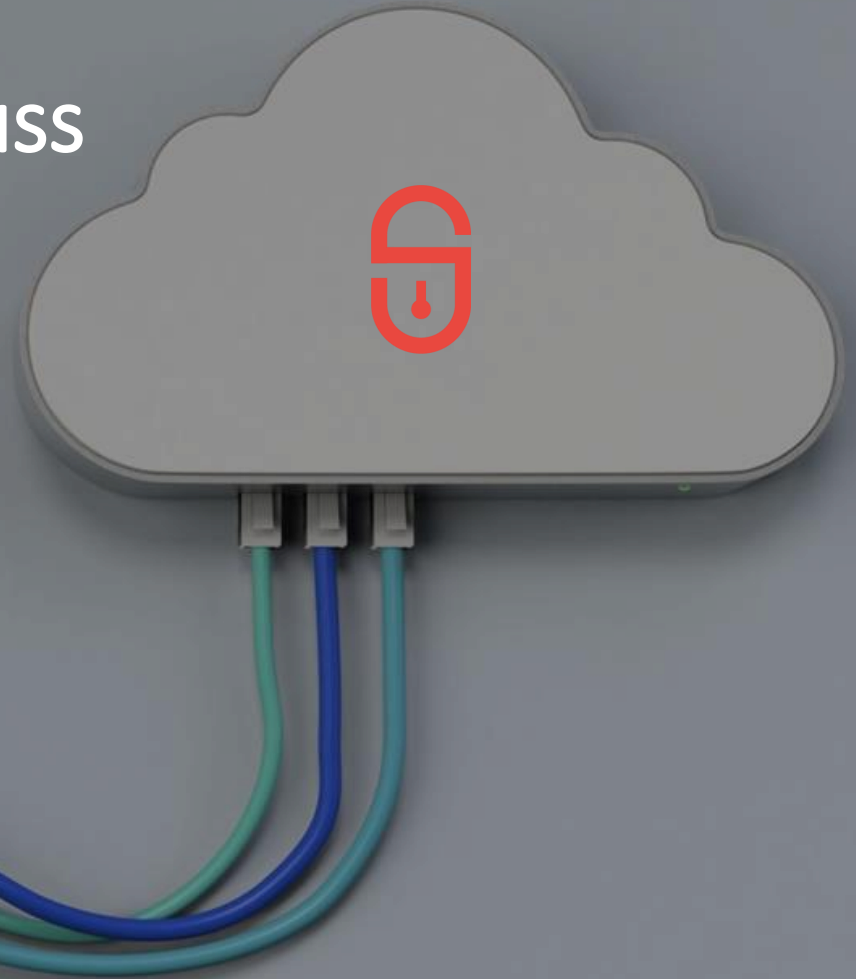
General **Details**

Friendly View XML View

In Bytes

```
0000: 2D 20 43 6F 64 65 3A 20 - Code:
0008: 20 43 4F 52 53 56 43 43   CORSVCC
0010: 30 30 30 30 30 37 37 32   00000772
0018: 2D 20 43 61 6C 6C 3A 20 - Call:
0020: 20 43 4F 52 53 56 43 43   CORSVCC
0028: 30 30 30 30 30 37 35 34   00000754
0030: 2D 20 50 49 44 3A 20 20 - PID:
0038: 30 30 30 30 38 36 32 38   00008628
0040: 2D 20 54 49 44 3A 20 20 - TID:
0048: 30 30 30 30 36 36 36 34   00006664
0050: 2D 20 43 4D 44 3A 20 20 - CMD:
0058: 43 3A 5C 57 49 4E 44 4F   C:\WINDO
0060: 57 53 5C 73 79 73 74 65   WS\sysse
0068: 6D 33 32 5C 76 73 73 76   m32\vssv
0070: 63 2E 65 78 65 20 20 20   c.exe
```


Poll 4:
When did IT-Sec pro`s start to discuss
Fileless Malware in Event logs?



1. 2023
2. 2022
3. 2021
4. 2020



Next Webinar



July 12th 2023
09:00am



Azure
Cross-tenant setup


Q&A

tems
security




Contact information

Philip Berger
Managing Director

 +43(664) 343 8644

 Philip.berger@tems-security.at

Michael Meixner, CISSP
Managing Director

 +43(664) 1453328

 Michael.meixner@tems-security.at