Experts Live Netherlands

Welcome to the Dutch Microsoft Security Meetup Capture the Flag

Microsoft · SOFTWARE CENTRAL · Capgemini · inforcer · DELL Technologies · nerdio · SUPER VISION · INTERSTELLAR · kpn Partner Network · INSPARK

Experts Live Netherlands

DUTCH MICROSOFT SECURITY MEETUP

Microsoft · SOFTWARE CENTRAL · Capgemini · inforcer · DELL Technologies · nerdio · SUPER VISION · INTERSTELLAR · kpn Partner Network · INSPARK

Experts Live Netherlands

Fabian

Detection
KQL, hunting, analytics rules

Response
IR, forensics, triage

Hardening
CA, ASR, baselines, Tamper Protection

Offensive
Red teaming

Automation
PowerShell, playbooks, Graph API, custom log ingestion

Architecture
SOC design, multi-tenant, log routing

Microsoft · SOFTWARE CENTRAL · Capgemini · inforcer · DELL Technologies · nerdio · SUPER VISION · INTERSTELLAR · kpn Partner Network · INSPARK

Experts Live Netherlands

Tom

Detection
KQL, hunting, analytics rules

Response
IR, forensics, triage

Hardening
CA, ASR, baselines, Tamper Protection

Offensive
Red teaming

Automation
PowerShell, playbooks, Graph API, custom log ingestion

Architecture
SOC design, multi-tenant, log routing

Microsoft · SOFTWARE CENTRAL · Capgemini · inforcer · DELL Technologies · nerdio · SUPER VISION · INTERSTELLAR · kpn Partner Network · INSPARK

Experts Live Netherlands

Myron

Compliance
Risk management, laws & regulations

Data Security
Information Protection, DLP, Insider Risk Management, MAM

Defender for
Endpoint, Cloud Apps, Office 365, Cloud, Identity

Identity
Conditional Access, Entra ID Protection, PIM

Automation
PowerShell, playbooks, Graph API, custom log ingestion

Infrastructure
Hardware, networking, servers, storage, on-premises

Microsoft · SOFTWARE CENTRAL · Capgemini · inforcer · DELL Technologies · nerdio · SUPER VISION · INTERSTELLAR · kpn Partner Network · INSPARK

Experts Live Netherlands

Koos

Detection
KQL, hunting, analytics rules

Response
IR, forensics, triage

Hardening
CA, ASR, baselines, Tamper Protection

Custom Log Ingestion
Application Security

Automation
Logic Apps, playbooks, Graph API, custom log ingestion

Architecture
SOC design, multi-tenant, log routing

Microsoft · SOFTWARE CENTRAL · Capgemini · inforcer · DELL Technologies · nerdio · SUPER VISION · INTERSTELLAR · kpn Partner Network · INSPARK

Experts Live Netherlands

Ronny

Detection
KQL, hunting, analytics rules

Response
IR, forensics, triage

Hardening
CA, ASR, baselines, Tamper Protection

Offensive
Red teaming

Automation
Logic Apps, playbooks, Graph API, custom log ingestion

Architecture
SOC design, multi-tenant, log routing

Microsoft · SOFTWARE CENTRAL · Capgemini · inforcer · DELL Technologies · nerdio · SUPER VISION · INTERSTELLAR · kpn Partner Network · INSPARK

Experts Live Netherlands

Chandni

Detection
KQL, hunting, analytics rules

Response
IR, forensics, triage

Hardening
Endpoint, Cloud Apps, Office 365, Cloud, Identity

Offensive
Red teaming

Automation
Logic Apps, playbooks, Graph API, custom log ingestion

Architecture
SOC design, multi-tenant, log routing

Microsoft · Software Central · Capgemini · inforcer · Dell Technologies · nerdio · Super Vision · Interstellar · kpn Partner Network · Inspark

Experts Live Netherlands

Agenda

- 08:30 – 09:15 Opening & CTF Setup
- 09:15 – 10:00 CTF - 20 + 50
- 10:00 – 10:15 Break
- 10:15 – 11:00 CTF - 25 + 50 + 100
- 11.00 – 11:45 Theory
- 11.45 – 12:45 Lunch
- 12:45 – 13:30 CTF - 200 + 500
- 13.30 – 14:15 Theory
- 14:15 – 14:30 Break
- 14:30 – 15:00 Theory
- 15.00 – 16:00 Pubquiz
- 16:00 – 17:00 Drinks & Bites

DUTCH MICROSOFT SECURITY MEETUP

Microsoft · SOFTWARE CENTRAL · Capgemini · inforcer · DELL Technologies · nerdio · SUPER VISION · INTERSTELLAR · kpn Partner Network · INSPARK

Experts Live Netherlands

The meetup numbers

- 2150+ members
- Rating: 4.6 (700+ reviews) 
- 6x times a year meetup
- 450+ visitors in 2025

DUTCH MICROSOFT SECURITY MEETUP

Microsoft · Software Central · Capgemini · inforcer · Dell Technologies · nerdio · Super Vision · Interstellar · kpn Partner Network · Inspark

Experts Live Netherlands

Mission

- Knowledge sharing about Microsoft Security
- Connecting professionals with each other in the Netherlands
- By organizing in-person events in the Netherlands
- Free access made possible by sponsors

Microsoft SOFTWARE CENTRAL Capgemini inforcer DELL Technologies nerdio SUPER VISION INTERSTELLAR kpn Partner Network INSPARK

Koos Goossens
@KoosGoossens

Attending a jam-packed #DutchSecMeetup with a very entertaining session from @sannemaasakkers and some insightful backdoors by @_dirkjan

7:42 PM · Dec 15, 2022 · **886** Views

Andre van den Berg - #WIMVP @aavdb... · Sep 6, 2022

Today attending #dutchsecmeetup at @microsoftnl with sessions about "Let's go hunting: looking outside of the EDR" by @_ChezDaniela, and "Microsoft Intune als backdoor en ransomware distributie" by @rikvduijn look who I found @JamesvandenBerg and @MyStickerbox came with me.

1 5

Maarten Eekels @maarteneekels · Jul 14, 2022

Super interesting vulnerability playground for #Kubernetes: Kubernetes Goat github.com/madhuakula/kub... - Explained by the creator himself, @madhuakula at #DutchSecMeetup

5 15

Gianni @castello_johnny · Dec 15, 2022

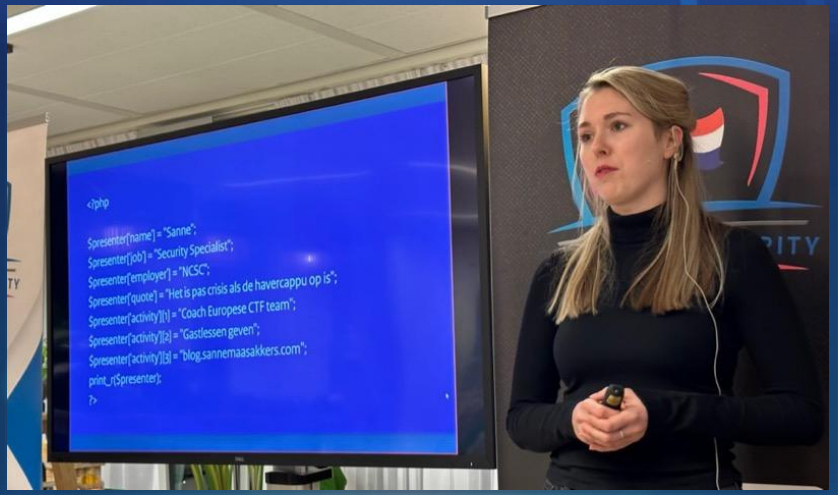
Session 1 @ #DutchSecMeetup @sannemaasakkers You hacked the Dutch government and all I got is this ___ report

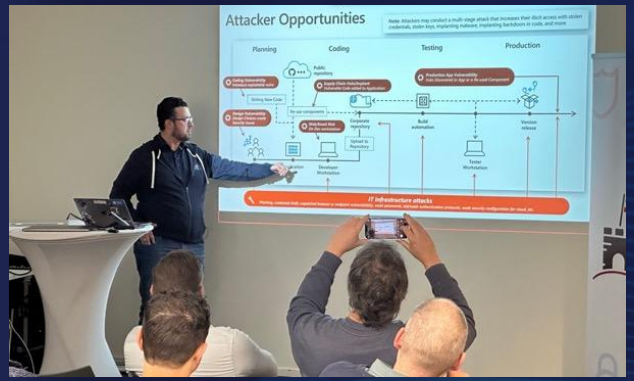
Maarten Goet @maarten_goet · Jul 7, 2022

🚨1K🚨 De security community is alive-and-kicking in nederland 💙 Dank aan alle leden, sprekers en sponsors! meetup.com/microsoft-secu... #DutchSecMeetup

Pouyan Khabazi | MVP @PKhabazi · Jun 16, 2022

Finally some community time after a long time #dutchsecmeetup where @castello_johnny kicks off with everything you want to know about #KQL (not the new #PowerShell 😂)





Microsoft · SOFTWARE CENTRAL · Capgemini · inforcer · DELL Technologies · nerdio · SUPER VISION · INTERSTELLAR · kpn Partner Network · INSPARK

Microsoft MVP Program Blog

Search this community

MICROSOFT MVP PROGRAM BLOG 3 MIN READ

YellowHat 2025: A Global Stage for Deep Microsoft Security Insights

Microsoft SOFTWARE CENTRAL Capgemini inforcer DELL Technologies nerdio SUPER VISION INTERSTELLAR Partner Network INSPARK

Experts Live Netherlands

Questions

- Hands up if you're a security analyst
- Hands up if you're a security administrator
- Hands up if you're a security consultant
- Hands up if you're not in security at all

Experts Live Netherlands

Questions

- Who's here for their first CTF?
- What are your expectations for today?

Experts Live Netherlands

Capture the Flag setup

- Use the credentials on the table to sign in
- Change your password, register MFA
- Reconnect credential to PowerApps (if required)
- Open the portal, you'll see a PowerApp
- Ask us if you get stuck

Experts Live Netherlands

Capture the Flag setup

- From: **Sunday 31 May 2026 to Sunday 07 June 2026**
- Accounts names format: 0426-Dominance_4367_[0-19]@ctf.alpineskihouse.co
- Password format: **CatchTheNinja!_[0-19]**
- Scenario: **0426 - Dominance**
- Access: https://aka.ms/ninjactf

Experts Live Netherlands

CREDENTIAL ACCESS | MITRE T1003.001

Mimikatz

RISK LEVEL **CRITICAL**

DETECTION Event 4656 · MDE alert: Credential dumping · LSASS access

FOCUSED ON CREDENTIAL ACCESS

HOW DOES IT WORK?

Reads credentials directly from LSASS memory via `SeDebugPrivilege`. The most widely used tool for credential dumping after initial access.

INDICATORS OF COMPROMISE

01 Memory dumps of `lsass.exe` (via ProcDump or Task Manager)

02 Access to LSASS with `GrantedAccess 0x1010` or `0x1410`

03 Process opens handle to `lsass.exe` with debug rights

04 Known strings in memory: `sekurlsa`, `mimikatz`

Experts Live Netherlands

LATERAL MOVEMENT | MITRE T1021.002

PsExec

Sysinternals

USED FOR LATERAL MOVEMENT

HOW DOES IT WORK?

Legitimate Sysinternals tool that executes processes remotely via SMB and the `ADMIN$` share. Attackers use it for lateral movement after credential theft.

RISK LEVEL **HIGH**

DETECTION Event 7045 · Event 4624 type 3 · SMB to ADMIN$

INDICATORS OF COMPROMISE

01 Service `PSEXESVC` created on target system (`Event 7045`)

02 Connection via SMB to the `ADMIN$` share

03 Process execution as `SYSTEM` via remote service

04 Combined with stolen credentials (`Event 4624` type 3)

Experts Live Netherlands

PARTS 1 & 2

Initial Access, Defense Evasion & Credential Theft

CTF CONTEXT

Malicious PowerShell script executed by user `rayt`

Drops Mimikatz, PsExec and Rubeus on the endpoint

Runs `Set-MpPreference` to disable real-time monitoring

Discovery performed via `net.exe`

01 · DEFENDER

Tamper Protection

Ignores local admin or CLI attempts to disable Defender including `Set-MpPreference -DisableRealtimeMonitoring`.

02 · WINDOWS

Credential Guard

Isolates NTLM hashes and Kerberos tickets via VBS, rendering Mimikatz virtually useless against LSASS.

03 · INTUNE

ASR Rules

Block credential stealing from `lsass.exe`, obfuscated scripts, and untrusted executables via Intune Endpoint Security.

04 · WDAC

PowerShell CLM

Constrained Language Mode via WDAC prevents malicious scripts from calling arbitrary Windows APIs.

Experts Live Netherlands

PARTS 1 & 2

Tamper Protection

Protected Components

Core AV Engine Features

Locks critical services including Real-time protection, Cloud-delivered protection, Behavior monitoring, IOfficeAntivirus (IOAV), and Security intelligence updates.

Local Override Prevention

Centralized Control

Stops changes made via local Registry, PowerShell, or Group Policy. Only central management tools like Intune or the Microsoft Defender Portal can push authorized updates.

Troubleshooting Mode

Secure Maintenance

Stops changes made via local Registry, PowerShell, or Group Policy. Only central management tools like Intune or the Microsoft Defender Portal can push authorized updates.

Enabled by Default

Out-of-the-Box Security

Stops changes made via local Registry, PowerShell, or Group Policy. Only central management tools like Intune or the Microsoft Defender Portal can push authorized updates.

Experts Live Netherlands

PARTS 1 & 2

Credential Guard

Virtualization-Based Security

Core AV Engine Features

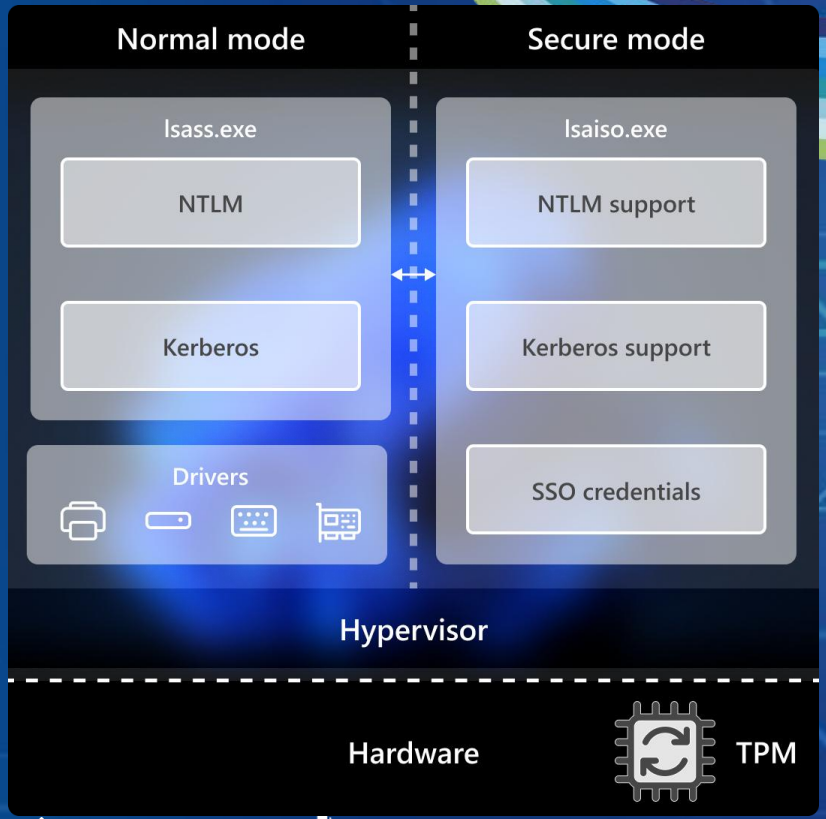
Isolates the Local Security Authority (LSA) inside a hardware-backed, virtualized container, separated from the main OS.

Even if malware gains full Administrator privileges, it cannot access the virtualized credential vault.

Protects NTLM password hashes and Kerberos Ticket Granting Tickets

Enabled by default on Windows 11, 22H2 and Windows Server 2025

Requires Windows Enterprise



Experts Live Netherlands

PARTS 1 & 2

Attack Surface Reduction (ASR) Rules

Defense in Depth

- **Behavioral Tripwires:** Automatically targets and blocks risky software actions, such as Office apps launching malicious child processes or scripts downloading payloads.
- **Behavior vs. Signature:** Operates at the behavior layer. This stops zero-day threats and human-operated ransomware that traditional signature-based antivirus misses.
- **Phased Deployment:** Best practice dictates starting in Audit Mode to identify and exclude legitimate workflows before moving to Warn or Block Mode.
- **Targeted Defenses:** Rules are pre-configured to lock down common attack vectors, including credential theft from LSASS and WMI persistence abuse.

Experts Live Netherlands

PARTS 1 & 2

Attack Surface Reduction (ASR) Rules

Defense in Depth

- **Block credential stealing from the Windows local security authority subsystem (lsass.exe)**
  Noisy in audit mode, but block mode can be safely activated in 99% of cases

- **Standard rules safely activated in most environments**
  Block abuse of exploited vulnerable signed drivers
  Block persistence through WMI event subscription

- **Block process creations originating from PSExec and WMI commands**
  Do not enable in environments that still use Microsoft Configuration Manager

- **Block use of copied or impersonated system tools**
  Can be pretty false positive prone, as many vendor software (e.g. Adobe) use the same “technique”

Experts Live Netherlands

LIVING-OFF-THE-LAND | MITRE T1059.001

PowerShell

Scripts

LIVING-OFF-THE-LAND ATTACKS

HOW DOES IT WORK?

PowerShell is a legitimate management tool, but attackers abuse it for downloaders, reconnaissance and payload execution, without dropping external tools.

RISK LEVEL **MEDIUM**

DETECTION Event 4104 (ScriptBlock) · AMSI alerts · MDE: Suspicious PowerShell

INDICATORS OF COMPROMISE

01 Disabled or bypassed script execution policy

02 PowerShell spawned from Office, browser or service

03

Experts Live Netherlands

PARTS 1 & 2

PowerShell: Constrained Language Mode (CLM)

The default mode

Full Language Mode

- **Total System Access:** Grants access to all language elements, APIs, and .NET frameworks.
- **Post-Exploitation Dream:** Attackers use it to reflectively load malware into memory (fileless), dump credentials, and move laterally.
- **The Default State:** Historically, if an attacker gets a foothold, they can launch an unrestricted PowerShell process to execute advanced payloads (like Mimikatz).

The secure mode

Constrained Language Mode

- **Drastic Reduction of Attack Surface:** Limits the capability of PowerShell to only basic, safe commands required for standard administration.
- **Blocks Memory Injection:** Prevents the execution of inline C# and loading of unmanaged DLLs, stopping most modern fileless malware frameworks.
- **WDAC required:** Simply running $ExecutionContext.SessionState.LanguageMode = "ConstrainedLanguage" is easily bypassed. To be effective, CLM must be enforced by Windows Defender Application Control (WDAC)

Experts Live Netherlands

KERBEROS ABUSE | MITRE T1558 / T1550.003

Rubeus

RISK LEVEL **HIGH**

DETECTION Event 4769 (RC4, Legacy encryption)
Event 4768 0x17 · MDE: Kerberoasting

KERBEROS-RELATED ABUSE

HOW DOES IT WORK?

Pure C# toolset for Kerberos attacks. Used for ticket dumping, Pass-the-Ticket, Kerberoasting and AS-REP Roasting against service accounts.

INDICATORS OF COMPROMISE

01 Abnormally high number of TGS requests (`Event 4769`)

02 RC4(Legacy) encryption in TGS for accounts that normally use AES

03 AS-REQ without pre-authentication (`Event 4768` `Pre-Auth type 0`)

04 .NET assembly loaded in memory (PowerShell / MSBuild Compile)

Experts Live Netherlands

PART 3

Lateral Movement & Pass-the-Ticket

CTF CONTEXT

Attacker pivots to `aaronb-pc` using `Get-KRBTicket.ps1` and PsExec

`Xcopy` used to drop `Rubeus.exe` on the target machine

Defender disabled again on the new host

Kerberos tickets extracted - Pass-the-Ticket executed

01 · ASR

Block PsExec & WMI

Directly breaks the lateral movement chain by blocking process creations originating from PsExec and WMI commands.

02 · FIREWALL

Network Isolation

Block inbound SMB / RPC between workstations via Intune firewall policy, prevents horizontal movement.

03 · MDI

Defender for Identity

MDI monitors domain controllers for anomalous Kerberos requests from Rubeus and triggers high-severity PtT and PtH alerts.

04 · PASSWORDS

Windows LAPS

Native in Intune and Entra ID , gives every endpoint a unique local admin password, blocking credential reuse via PsExec.

Microsoft SOFTWARE CENTRAL Capgemini inforcer DELL Technologies nerdio SUPER VISION INTERSTELLAR kpn Partner Network INSPARK

Experts Live Netherlands

PART 3

Network Isolation

Like implementing fire doors in your environment

- **Stopping Lateral Movement**
  If a single Windows workstation is compromised, isolation prevents the attacker from "hopping" to other devices, databases, or Domain Controllers on the network. Management ports must not be available to every John Doe in marketing.

- **Built-in Windows Firewall**
  Windows natively supports robust inbound/outbound traffic filtering. Blocking unnecessary ports severely limits what an attacker can see and touch.

- **Instant Threat Containment**
  During an active breach, Microsoft Defender for Endpoint allows security teams to instantly "Isolate Device." This cuts almost all network access except a secure lifeline for remote investigation. Since May 2025 automatically as part of Automatic Attack Disruption

Experts Live Netherlands

PART 3

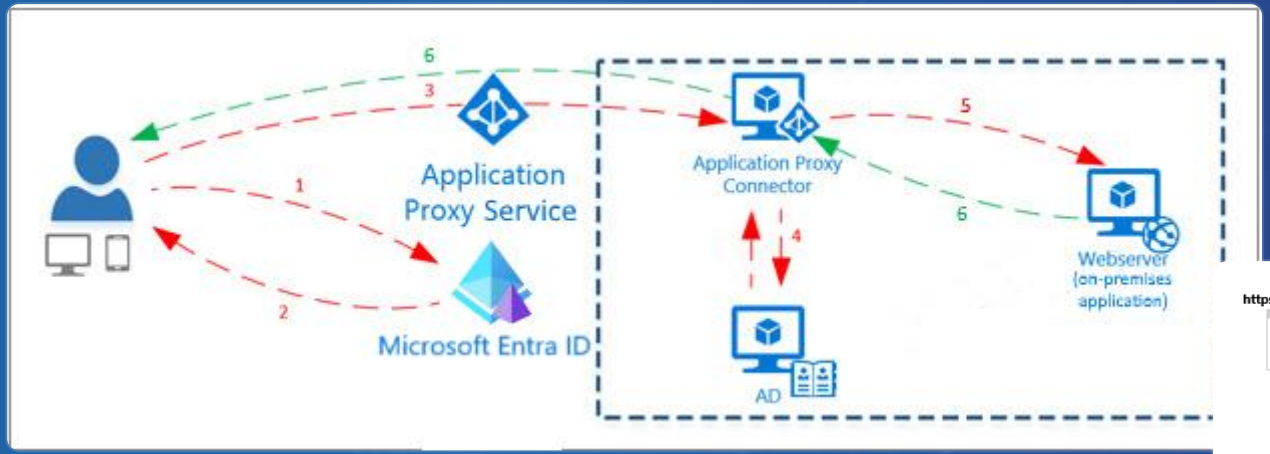
Micro Segmentation

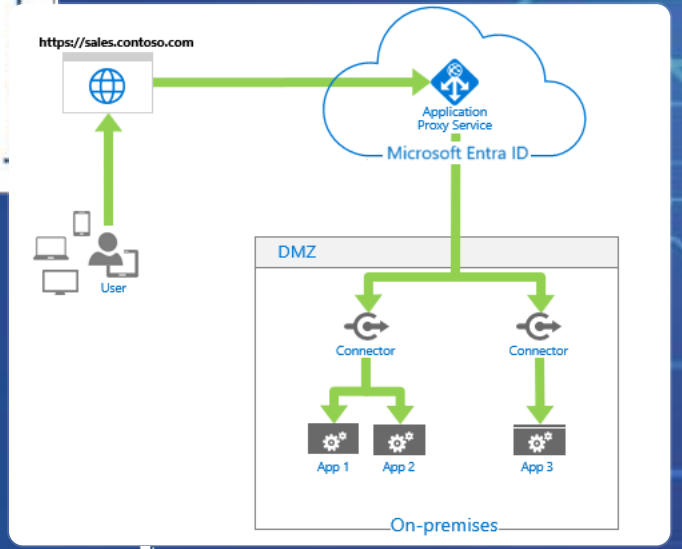
Throw workstations out of your datacenter

- **Microsoft Entra application proxy**
  Publish on-premises web applications in a secure manner without expanding your public footprint. Limited to outbound connections from the connector, attackers can't reach those apps directly. Included in Entra ID P1 and P2.

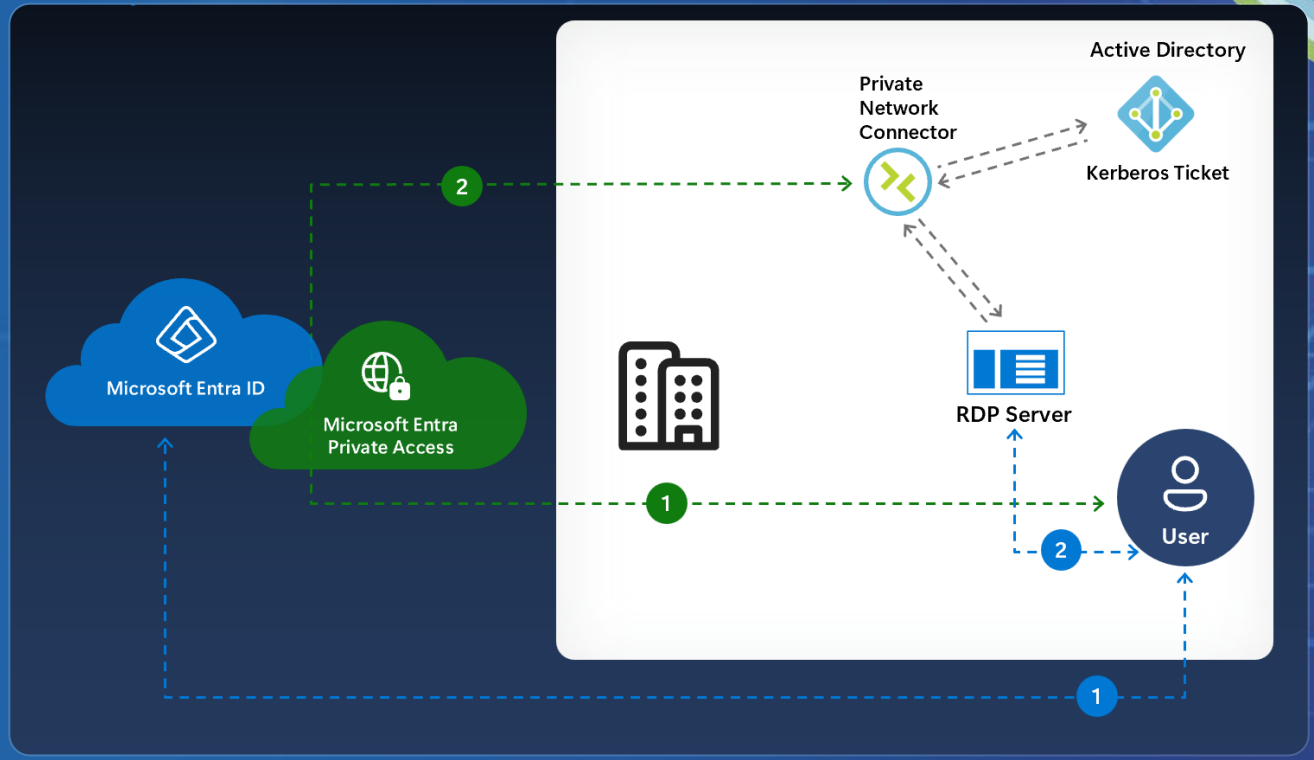
- **Grant network access based on authentication**
  Microsoft Entra Private Access limits data traffic to those servers (applications) user really need for their daily work.
  And Entra Conditional Access is utilized for Pre-Authentication.

- **Restrict Machine to Machine communication**
  Servers need to talk to each other, but not without limits. Group them by application and only expose required ports to other app groups. More restrictive implementation using Kerberos based IPsec tunnels are hard to implement and maintain.


6
3
1
2
Application
Proxy Service
Microsoft Entra ID
Application Proxy
Connector
4
AD
5
6
Webserver
(on-premises
application)


https://sales.contoso.com
Application
Proxy Service
Microsoft Entra ID
User
DMZ
Connector
Connector
App 1
App 2
App 3
On-premises

Experts Live Netherlands



Microsoft SOFTWARE CENTRAL Capgemini inforcer DELL Technologies nerdio SUPER VISION INTERSTELLAR kpn Partner Network INSPARK

Experts Live Netherlands

PART 3

Microsoft Defender for Identity

Securing identities everywhere...

- **Detects Advanced Threats**
  Identifies malicious activities like Pass-the-Ticket, Pass-the-Hash, and Golden Ticket attacks using deep packet inspection, before they fully compromise the domain.

- **ADFS and Entra Connect**
  Besides on domain controllers MDI can also protect Active Directory Federation Service (AD FS) and Entra Connect servers and therefor covers the most critical identity assets in your environment.

- **Protection beyond on-premises**
  While MDI is still often only associated with on-premises identity protection it has expanded to first and third-party Cloud IdPs like Entra ID and Okta. CyberArk, SailPoint are two other third-part integrations currently in public preview.

Experts Live Netherlands

PART 3

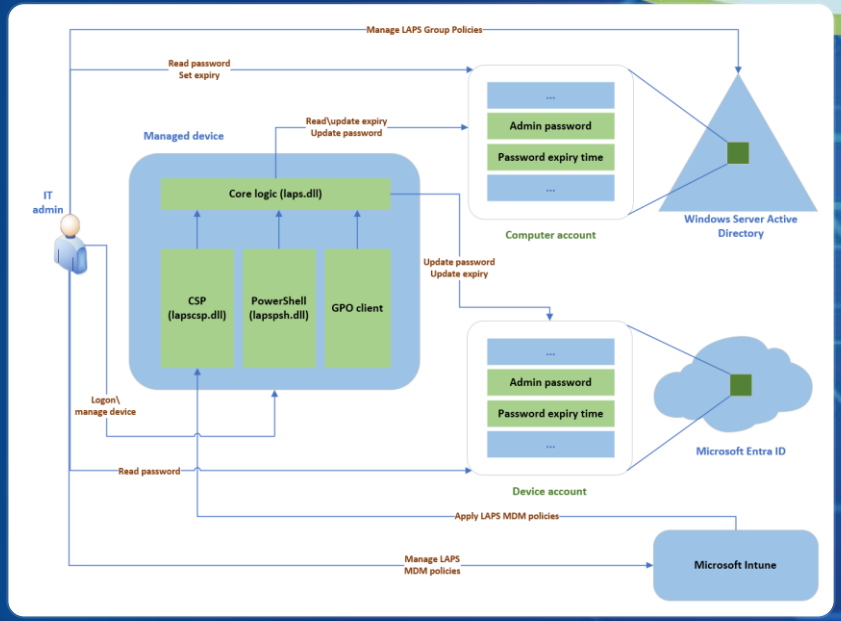
LAPS

Local Administrator Password Solution

- **Unique Credentials**
  Automatically generates and enforces a unique, randomized, and complex password for the built-in local administrator account on every single endpoint.

- **Limits Lateral Movement**
  Because no two machines share the same local admin password, an attacker compromising one endpoint cannot use those credentials to access others.

- **Automated Rotation**
  Passwords can be automatically rotated upon expiration or immediately after they are used by IT, ensuring stolen credentials quickly become useless.



Microsoft · Software Central · Capgemini · inforcer · Dell Technologies · nerdio · Supervision · Interstellar · kpn Partner Network · Inspark

Experts Live Netherlands

CTF - Question Remakrs

PAY ATTENTION!

- **50.5** Only provide the executable without parameters
- **50.6** Type only the username OR the complete UserPrincipalName
- **100.4** Make sure to ALSO include parameters, not only the PowerShell Cmdlet.
- **200.3** SAMaccountname = without “domain\”
- **500.1** Do not apply “quotes” to the NTLM hash

Experts Live Netherlands

CTF - Question Remakrs

BONUS ROUND! 🎉

- **100.11 Use Security Copilot to lookup the technique profile and select common Kerberos attack techniques**
    A. Kerberos brute-force
    B. ASREQRoast
    C. Kerberoasting
    D. Pass-the-Beer

Experts Live Netherlands

CTF – Question Remakrs

BONUS ROUND! 🎉

- **100.12 Which of these recommended actions protects against this kind of attack?**
  - A. Block credential stealing from Windows LSASS
  - B. Resolve unsecure domain configurations
  - C. Set restrictive ACL on krbtgt
  - D. Remove dormant accounts from sensitive groups

Experts Live Netherlands

CTF - Question Remakrs

BONUS ROUND! 🎉

- **100.13 What are the key features of Mimikatz?**

  Select <u>two</u>

  A. Forging Kerberos Golden

  B. Signing Primary Refresh Token

  C. Decrypting DPAPI data

  D. Simulating domain replication with TimeSync

Time for some lunch!

We will continue at 13:45

Experts Live Netherlands

AUTHENTICATION ABUSE

MITRE T1550.003 / T1558

Kerberos

Tickets

TICKETS ARE LEGITIMATE – THE ABUSE IS NOT

HOW DOES IT WORK?

Kerberos tickets themselves are legitimate. But stolen or forged tickets (Golden / Silver Ticket, Pass-the-Ticket) give an attacker persistent access without a password.

RISK LEVEL **HIGH**

DETECTION Event 4769 · Event 4771 · Unusual TGT lifetime

INDICATORS OF COMPROMISE

01 Tickets from outside normal working hours or unknown IPs

02 Unusual TGT lifetime (Golden Ticket)

03

Experts Live Netherlands

PARTS 1 & 2

Privilege Escalation, AD Attacks, & Containment

CTF CONTEXT

The attacker targets `celesteb` (a Domain Admin) whose credentials were left exposed on a compromised machine. They attempt to create a new DA (`BDAdmin`) and perform a DCSync attack against the `krbtgt` account. Automatic Attack Disruption contained one user but missed the initial victim due to an exclusion.

01 · Design

Enterprise access model

Highly privileged accounts like Domain Administrators must not sign in on office workstations. Separation of administrative accounts is a must

02 · SOAR

Automatic Attack Disruption

Do not exclude accounts from protective features like Attack Disruption without countermeasures.
Those automations will help to protect you in case of an incident in seconds.

03 · CHPWD

Rotate krbtgt password

Credentials of system credentials that are the source for Kerberos trust must be rotated

04 · OUTLOOK

Secure Defender Configuration

XXXX

Experts Live Netherlands

PART 4 & 5

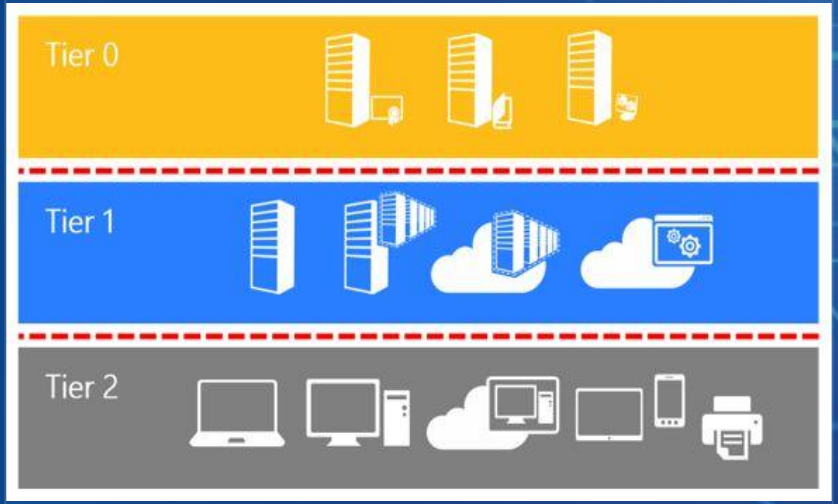
Tiered Administration Model

No, not (air)planes!

- **Tier 0 (Control Plane)**
  The keys to the kingdom. Domain Controllers, Identity Providers (Entra ID), and the accounts that manage them. Complete isolation is required.

- **Tier 1 (Management Plane)**
  Enterprise application servers, database servers, and cloud resources. These house the business data but do not control the core identities.

- **Tier 2 (User/Data Plane)**
  The high-risk zone. Standard user workstations, mobile devices, and email clients exposed directly to internet threats and phishing.



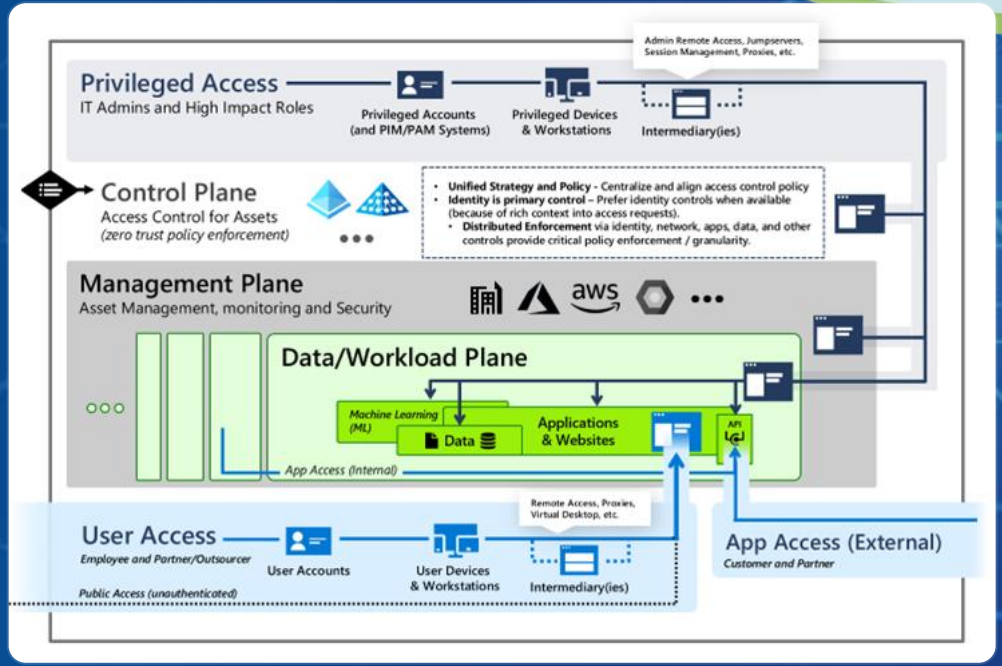
Experts Live Netherlands

PART 4 & 5

Enterprise access model

High-tier administrative accounts must never log into lower-tier systems.

This completely severs lateral movement paths for attackers.



Microsoft · Software Central · Capgemini · inforcer · DELL Technologies · nerdio · Supervision · Interstellar · kpn Partner Network · INSPARK

Experts Live Netherlands

PART 4 & 5

XDR Automatic Attack Disruption

Halting lateral movement and ransomware at machine speed.

- **Signal Correlation**
  Defender XDR correlates telemetry across endpoints, identities, cloud apps, and email to detect high-confidence, in-progress attacks.

- **Instant Containment**
  When a severe threat (like human-operated ransomware) is identified, XDR acts autonomously - isolating compromised devices and disabling compromised identities.

- **Stopping the Spread**
  This immediately severs the attacker's foothold and blocks lateral movement before data exfiltration or mass encryption can occur.

- **Buying Time**
  Gives you, the SOC team, critical time to investigate, remediate, and evict the adversary without the business grinding to a halt.

Experts Live Netherlands

PART 4 & 5

Defending the krbtgt Account

The master key to the domain and the necessity of strategic password rotation.

- **The Master Key**
  The `krbtgt` account is the Kerberos authentication service. Its password hash is used to encrypt and sign every Ticket Granting Ticket (TGT) in the domain

- **The Golden Ticket Threat**
  If an attacker extracts this hash (DCSync), they can forge "Golden Tickets" - granting themselves invisible, unrestricted Domain Admin access that bypasses normal login checks.

- **Why Rotation is Critical**
  Regular password rotation is the only way to invalidate compromised Kerberos tickets and evict an attacker relying on a forged Golden Ticket.

- **Rule #2 "Double Tap"**
  Active Directory validates tickets against the current and previous krbtgt passwords. To truly lock out an attacker, the password must be reset twice (allowing hours/days in between for ticket expiration).

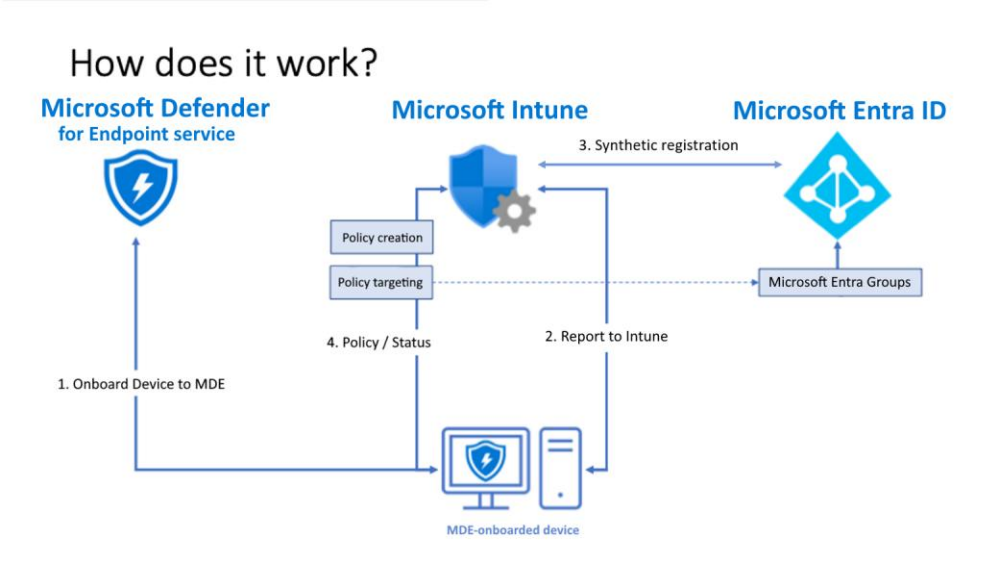
Experts Live Netherlands

PART 4 & 5

Security settings management

- **AV/EDR configuration**
  Ensuring your endpoints are configured to prevent attacks, with features like real-time protection, behavior monitoring, network protection, credential guard, attack surface reduction rules, tamper protection, sample submission, and more.

- **Security setting management**
  Allows Intune to apply its security policies through Microsoft Defender for Endpoint. This lets us use Intune to manage and push configurations for every type of device, including servers and unmanaged devices that would normally rely on GPO or Config Manager instead of Intune.



Microsoft · SOFTWARE CENTRAL · Capgemini · inforcer · DELL Technologies · nerdio · SUPER VISION · INTERSTELLAR · kpn Partner Network · INSPARK

Controlled configuration

- **Conflicts, overlap, and missing features**
  When you manage configurations from multiple places for different device types, conflicting or overlapping policies can happen quickly. It also increases the chance of missing certain features because each platform handles settings differently.

- **Controlled configuration for Defender antivirus (NEW)**
  Controlled configuration is a new feature that enforces Intune as the single source of truth for Defender Antivirus settings. It makes sure that other sources like GPO or Config Manager cannot change those configurations, which reduces conflicts, prevents overlap, and keeps your Defender settings consistent across all devices.

Experts Live Netherlands

WINDOWS SECURITY DEEP-DIVE CTF · PART- X

Attack Tools

& Techniques

Credential Access | Lateral Movement | Kerberos | Living-off-the-Land

MIMIKATZ · RUBEUS · PSEXEC · POWERSHELL · KERBEROS TICKETS

EXPERTS LIVE NL · 2026

Overview matrix

Tool · Category · MITRE · Risk · Detection signal

TOOL	CATEGORY	MITRE	RISK	DETECTION SIGNAL
Mimikatz	Credential Access	T1003.001	CRITICAL	MDE Credential dumping · LSASS access
Rubeus	Kerberos Abuse	T1558	HIGH	Event 4769 RC4 · Event 4768 error 0x17
PsExec	Lateral Movement	T1021.002	HIGH	Event 7045 · SMB ADMIN$ share
PowerShell	Living-off-the-Land	T1059.001	MEDIUM	Event 4104 · Encoded commands · AMSI
Kerberos Tickets	Authentication Abuse	T1550.003	HIGH	Event 4769 · Unusual TGT lifetime

It’s time for the Kahoot quiz!

Download the Kahoot app, or use the browser

https://kahoot.it/

Experts Live Netherlands

DUTCH MICROSOFT SECURITY MEETUP

Microsoft · SOFTWARE CENTRAL · Capgemini · inforcer · DELL Technologies · nerdio · SUPER VISION · INTERSTELLAR · kpn Partner Network · INSPARK

Experts Live Netherlands

Download the slides!

Safe to click. Rick Astley stayed home, we promise!

DUTCH MICROSOFT SECURITY MEETUP

Microsoft · SOFTWARE CENTRAL · Capgemini · inforcer · DELL Technologies · nerdio · SUPER VISION · INTERSTELLAR · kpn Partner Network · INSPARK