ERNW
providing security.

Active Directory and Azure – Core Security Principles

Friedwart Kuhn, Heinrich Wiederkehr

TROOPERS
MAKE THE WORLD A SAFER PLACE

Who We Are

- Friedwart Kuhn
  - Head of Microsoft Security Team @ERNW
  - 15+ years experience in security assessments, administration, publications and trainings
  - IT security professional with a focus on Windows Security and Active Directory Security

- Heinrich Wiederkehr
  - Member of Microsoft Security Team @ERNW
  - 5+ years in security assessments and trainings
  - IT security professional with a focus on Windows Security and Active Directory Security

Agenda

- Who We Are
- Intro & Current Active Directory Threat Landscape
- Common Core Security Controls for Active Directory
- Limits of Common Controls: Cross Forest Security Dependencies
- New Core Security Controls for Active Directory and Azure

ERNW
providing security.

Why should you care about on-premise and cloud AD security?

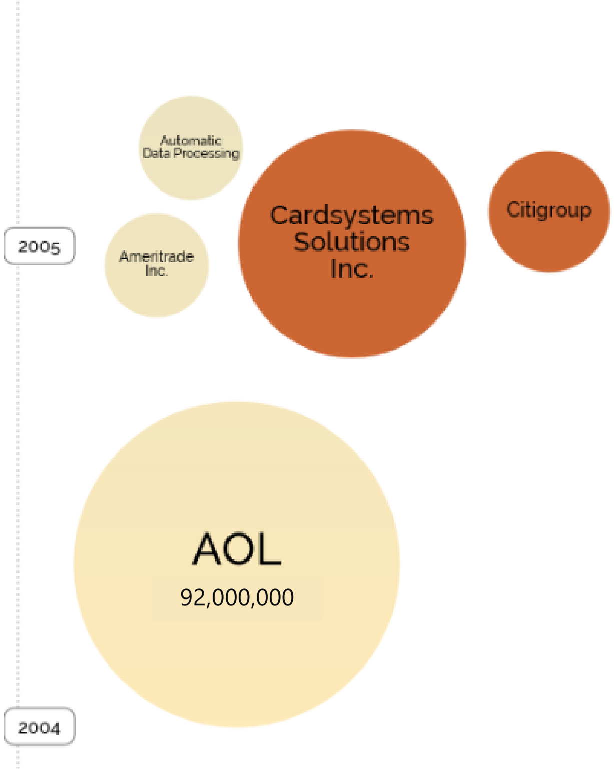
- Active Directory (AD) is the main authentication backend in nearly every organization
  - Holds the keys to the crown jewels!

- AD is heavily targeted by attackers that are using powerful, publicly available tool sets

- AD cannot be seen as a standalone entity
  - Connections to other ADs (e.g. via trust relationships) or the Cloud (e.g. via Azure AD Connect) open up new threat scenarios
  - This creates far- reaching “security dependencies”

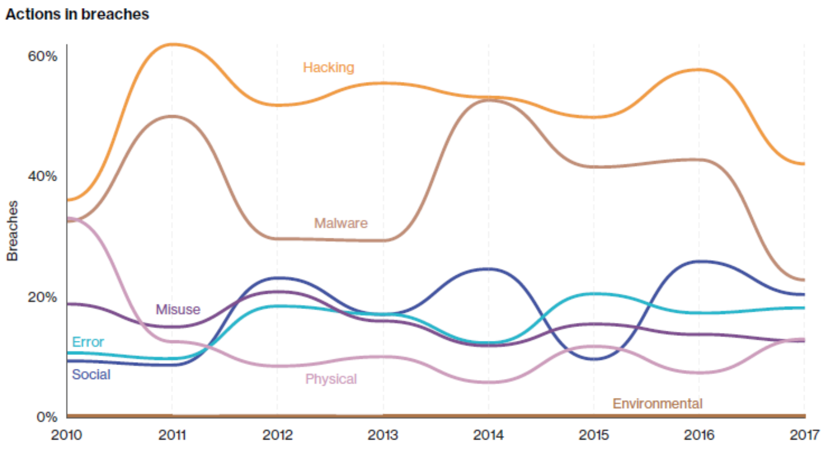
Current Active Directory Threat Landscape

Credential Theft Is Today’s Crisis

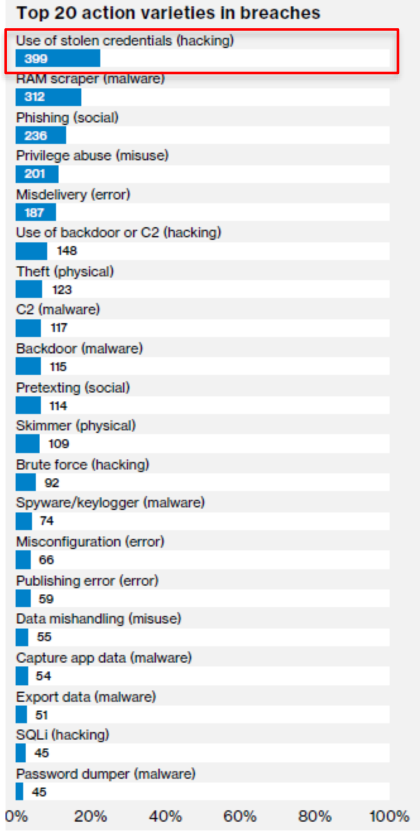


See: https://myignite.techcommunity.microsoft.com/sessions/65954?source=sessions

Relevance of Credential Theft Attacks


Actions in breaches

Data from DBIR 2018, cf. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf


Top 20 action varieties in breaches

ERNW
providing security.

Paradigm Shift in Security Realities

- **Active Directory attacks are in many cases:**
  - easy to perform (PtH in 48 hours)
  - not detected
  - difficult to recover

- **“Assume Breach”** is the (new) mindset

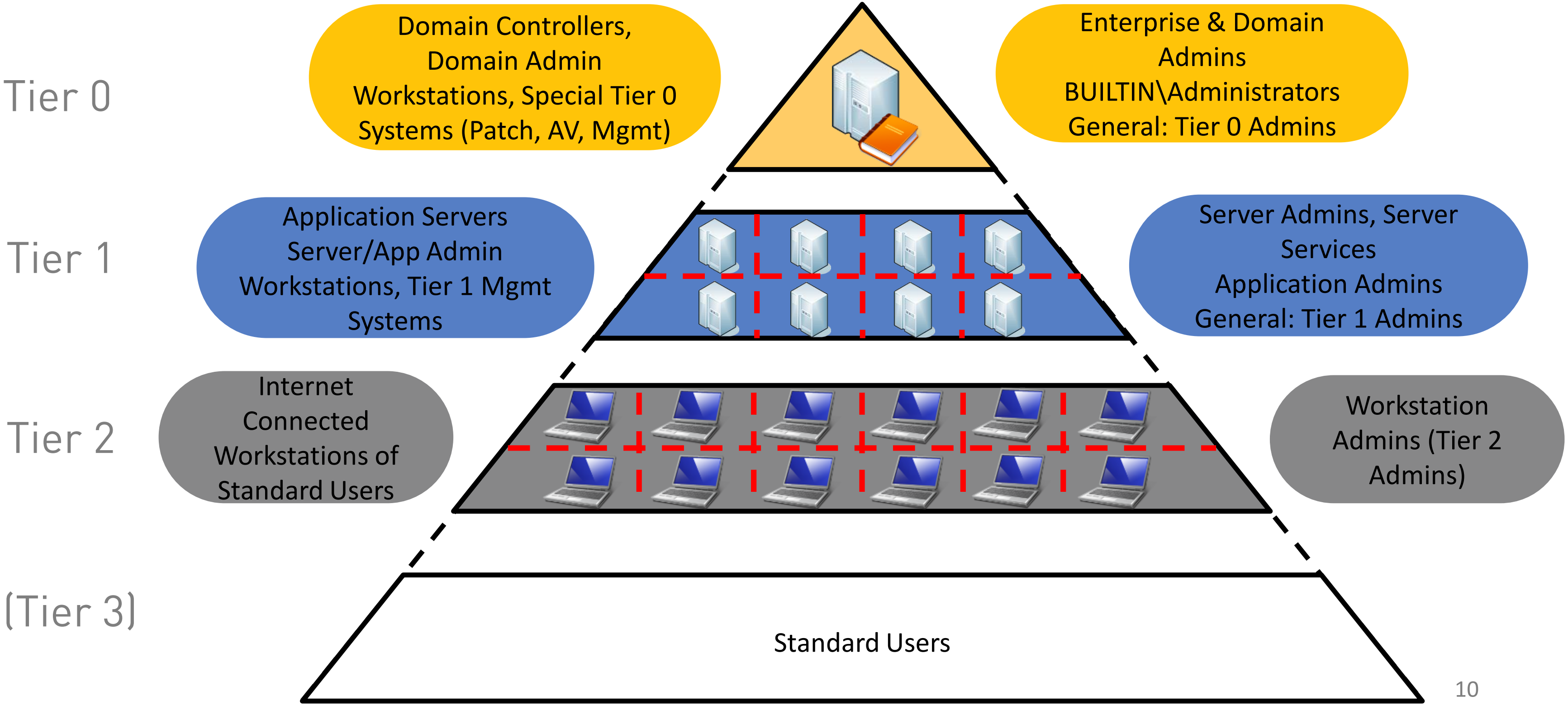
- **Identities** become the new **“perimeter”** in the corporate network and the cloud

- The overall strategy is **containment**, not prevention

Common Core Security Controls for Active Directory

- Admin Tiering
- Clean Source Principle
- Management of Security Dependencies

Control 1: Implement Administrative Tiers



Tier 0

Domain Controllers, Domain Admin Workstations, Special Tier 0 Systems (Patch, AV, Mgmt)

Enterprise & Domain Admins
BUILTIN\Administrators
General: Tier 0 Admins

Tier 1

Application Servers
Server/App Admin Workstations, Tier 1 Mgmt Systems

Server Admins, Server Services
Application Admins
General: Tier 1 Admins

Tier 2

Internet Connected Workstations of Standard Users

Workstation Admins (Tier 2 Admins)

(Tier 3)

Standard Users

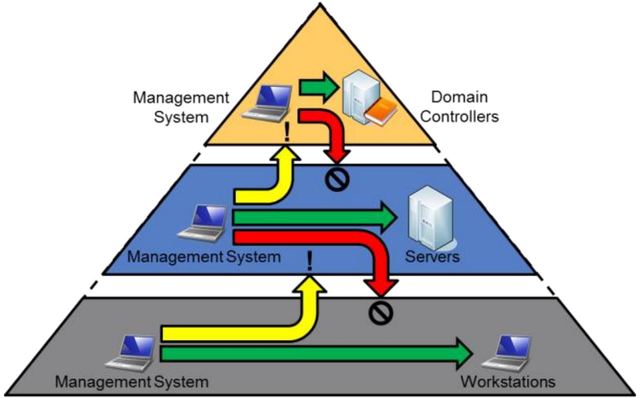
Tier Model Principles / Implementation Steps

Control 1a: Classify: *Every single* security principal, system, or application **has to be classified as belonging *only* to one tier**

Control 1b: Restrict Logons: Security principals of a higher tier ***must never log on to*** **a resource on a lower tier** (→ Implement logon restrictions)

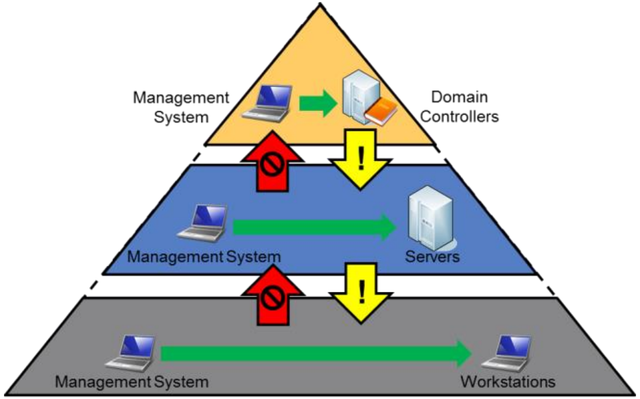
Control 1c: Restrict Control: Security principals of a lower tier ***must never control*** **resources of a higher tier** (→ Implement control restrictions)

Control 1b: Implement Logon Restrictions



- The **objective of logon restrictions is to limit credential exposure** (especially of privileged accounts) to the minimum necessary
  - Administrators (and other accounts) of a higher-privileged tier should not be able to logon to systems and applications of a lower tier
    - Sample: If a Domain Admin logs on to a workstation, the whole domain is at risk, if the workstation is compromised. (This should not be the case.)
  - **Accounts of a lower tier should be allowed to logon to a system of a higher tier *only as required by their role***
    - Sample: a standard user that works on a file server
  - **Implement logon restrictions**
    - **Via Authentication Policies & Authentication Silos** (white listing approach for T0)
    - **Via logon deny GPOs** that restrict allowed logons **for security principals of T0 on asset of T1 and T2** (respectively for security principals of T1 on asset of T2)

Control 1c: Implement Control Restrictions



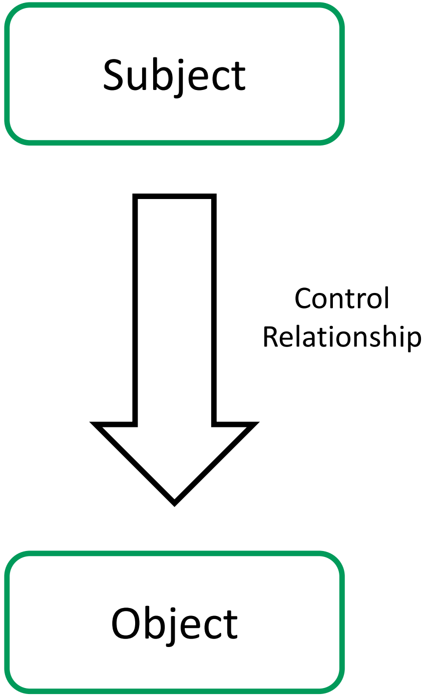
- The **objective of control restrictions is to prevent privilege escalation** in Active Directory
  - Administrators (and other accounts) of a lower tier should not be able to control systems, applications and accounts of a higher tier
    - Sample: If a server operator on a member server is member of the Enterprise Administrators group, he controls DCs. (This should not be the case.)

- **Implement control restrictions through supervision/ hardening** of:
  - Privileged group membership in Active Directory
  - Rights on sensitive Active Directory objects
    - (AdminSDHolder, Domain object, Domain Controller object, sensitive OUs, GPOs => all critical objects in T0 & T1)
    - Extended rights (e.g. replicating directory changes all…)
  - Delegation of sensitive user accounts & computer accounts trusted for delegation
  - Privileged local group membership
  - System privileges
  - NTFS rights
  - Registry rights

Control 2: Implement Clean Source Principle

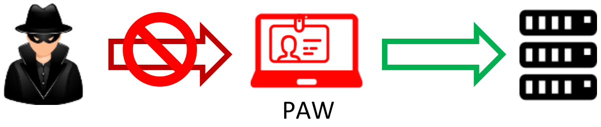
- Any subject in control of an object is a security dependency of that object
  - The assurances for all security dependencies **must be at or above** the **desired security level of the object** itself
  - ⚠ **Control is transitive!** (For example if A controls B and B controls C, then A also indirectly controls C.)

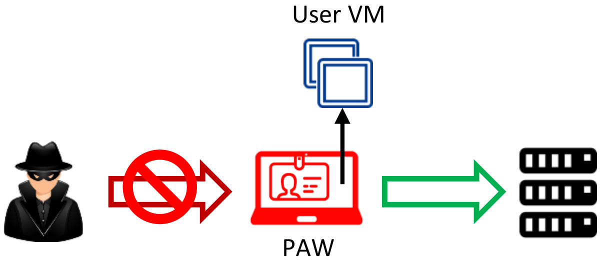
- Most common areas of control are:
  - the hardware where systems are installed,
  - the installation media for the systems,
  - the architecture and configuration of the system,
  - and daily operations.



Clean Source Principle: Privileged Access Workstations

- PAW hardware profiles can be:
  - **Dedicated hardware**
    - Separate dedicated devices for user tasks vs. administrative tasks
  - **Simultaneous use**
    - Single device that can run user tasks and administrative tasks concurrently by taking advantage of OS or presentation virtualization. For example:
      - Adding a local user VM
      - Adding RemoteApp, RDP, or a VDI



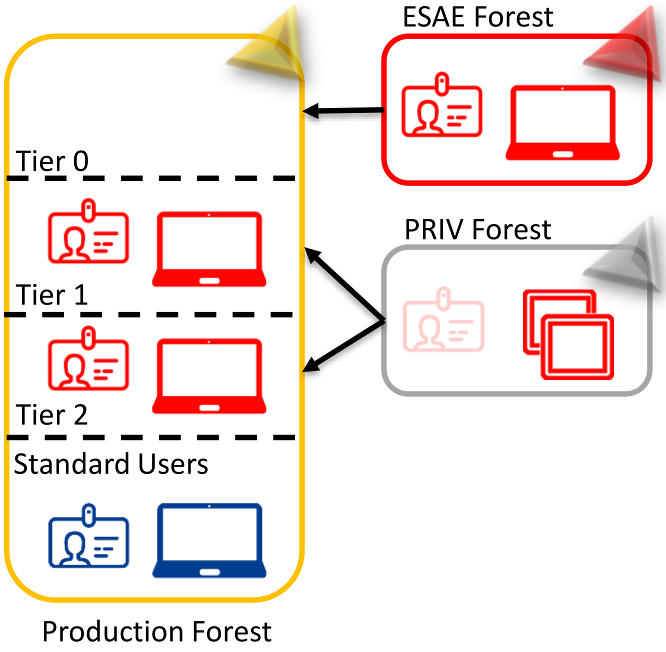


Clean Source Principle: ESAE/PRIV Forest

- Dedicated administrative forest
  - Hosts administrative accounts, workstations, groups
  - Environment has stronger security controls than the production environment

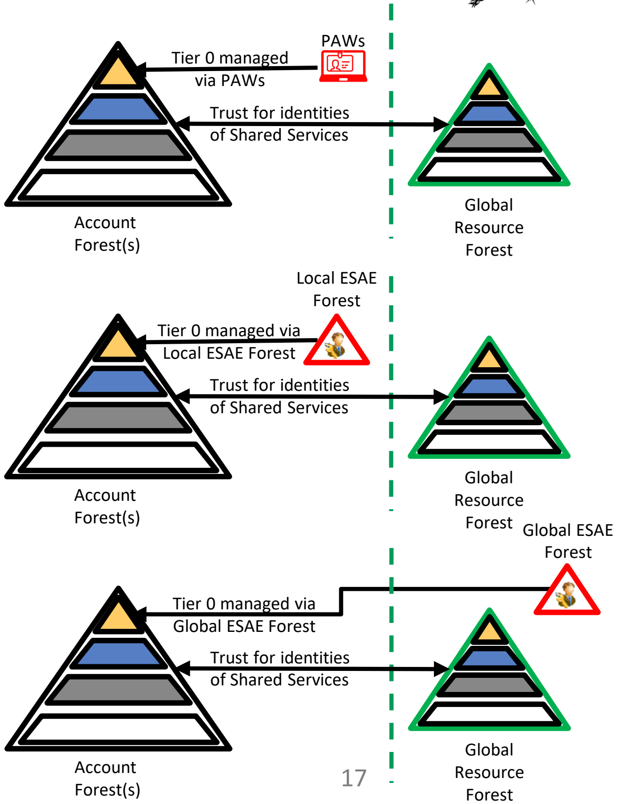
- **ESAE forest** moves all sensitive objects for Tier 0 administration to a separate forest
  - Except the krbtgt account and most likely service accounts
  - Balance between security benefit and operational effort unfavourable in a 1:1 relationship
    - Much better if one ESAE forest is used for multiple productive forests

- **PRIV forest** moves administrative identities for Tier 1 & 2 administration to a separate forest and combines this with a PAM solution (e.g. MIM 2016)



Exemplary Secure Administration Environment Models

- **Prerequisite:** Admin Tiering must be implemented
- **Option 1:**
  - Tier 0 managed exclusively via PAWs
- **Option 2:**
  - Tier 0 managed by a Local ESAE Forest (utilizing PAWs)
- **Option 3:**
  - Tier 0 managed by a Global ESAE Forest (utilizing PAWs; used for management of multiple forests)
- **Optional:** Combining the administration model with a PRIV Forest



PAWs

Tier 0 managed via PAWs

Trust for identities of Shared Services

Account Forest(s)

Global Resource Forest

Local ESAE Forest

Tier 0 managed via Local ESAE Forest

Trust for identities of Shared Services

Account Forest(s)

Global Resource Forest

Global ESAE Forest

Tier 0 managed via Global ESAE Forest

Trust for identities of Shared Services

Account Forest(s)

Global Resource Forest

Control 3: Understand and Manage Security Dependencies in Active Directory

- **Clean source principle** covers the **hardening of security dependencies** which could potentially open up new **attack paths**

- **Challenge** lies in the **identification** of these attack paths based on:
  - Group nesting
  - Local admin rights
  - Active user sessions
  - ACLs/ACEs on sensitive AD objects
  - GPOs and GPO links

- **Focus** on the **defender side** must shift from the hardening of single assets to a more **holistic view**

> *"Defenders think in lists.*
> *Attackers think in graphs.*
> *As long as this is true,*
> *attackers win."*

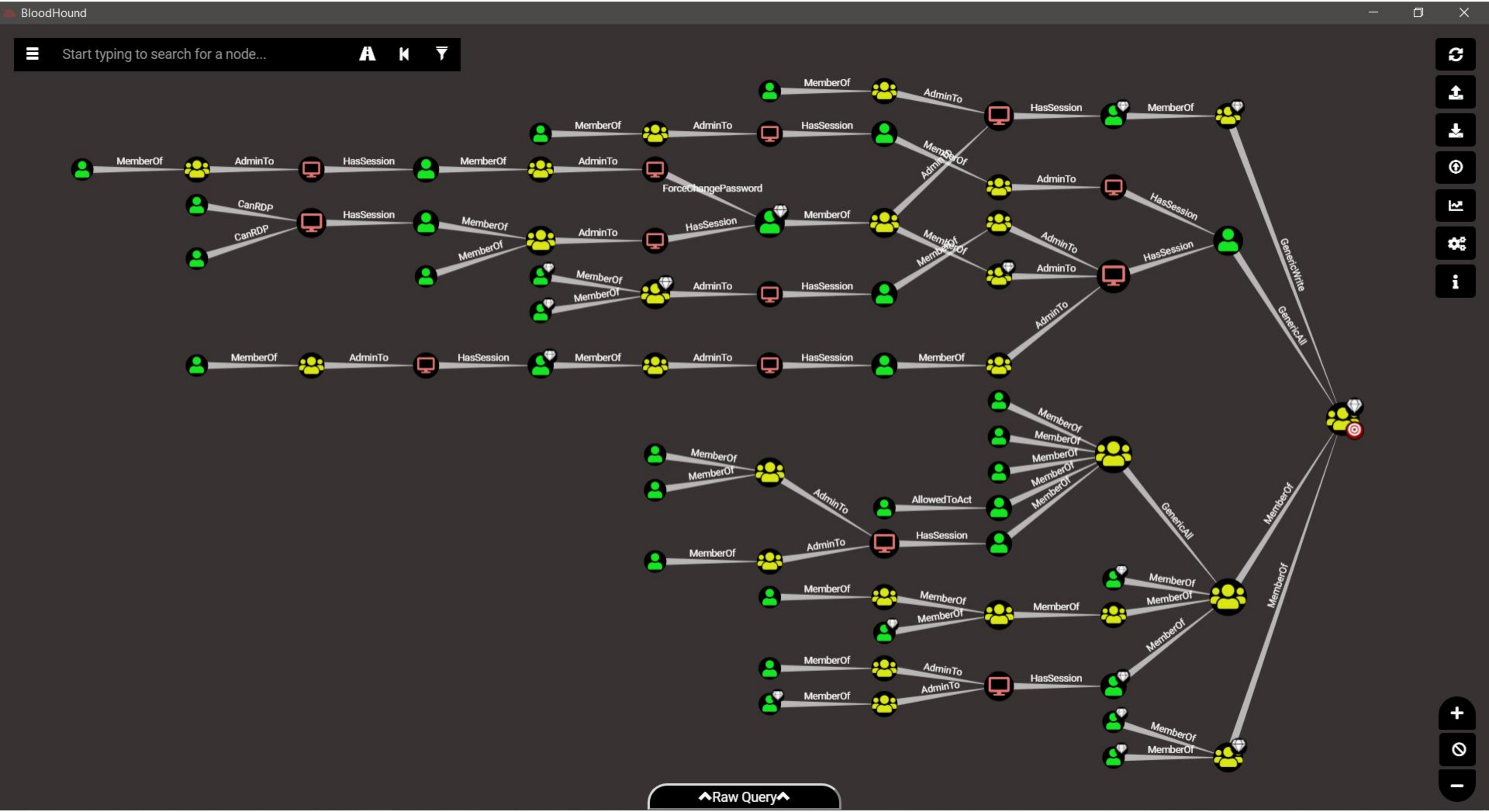
John Lambert,
Microsoft Threat
Intelligence Center

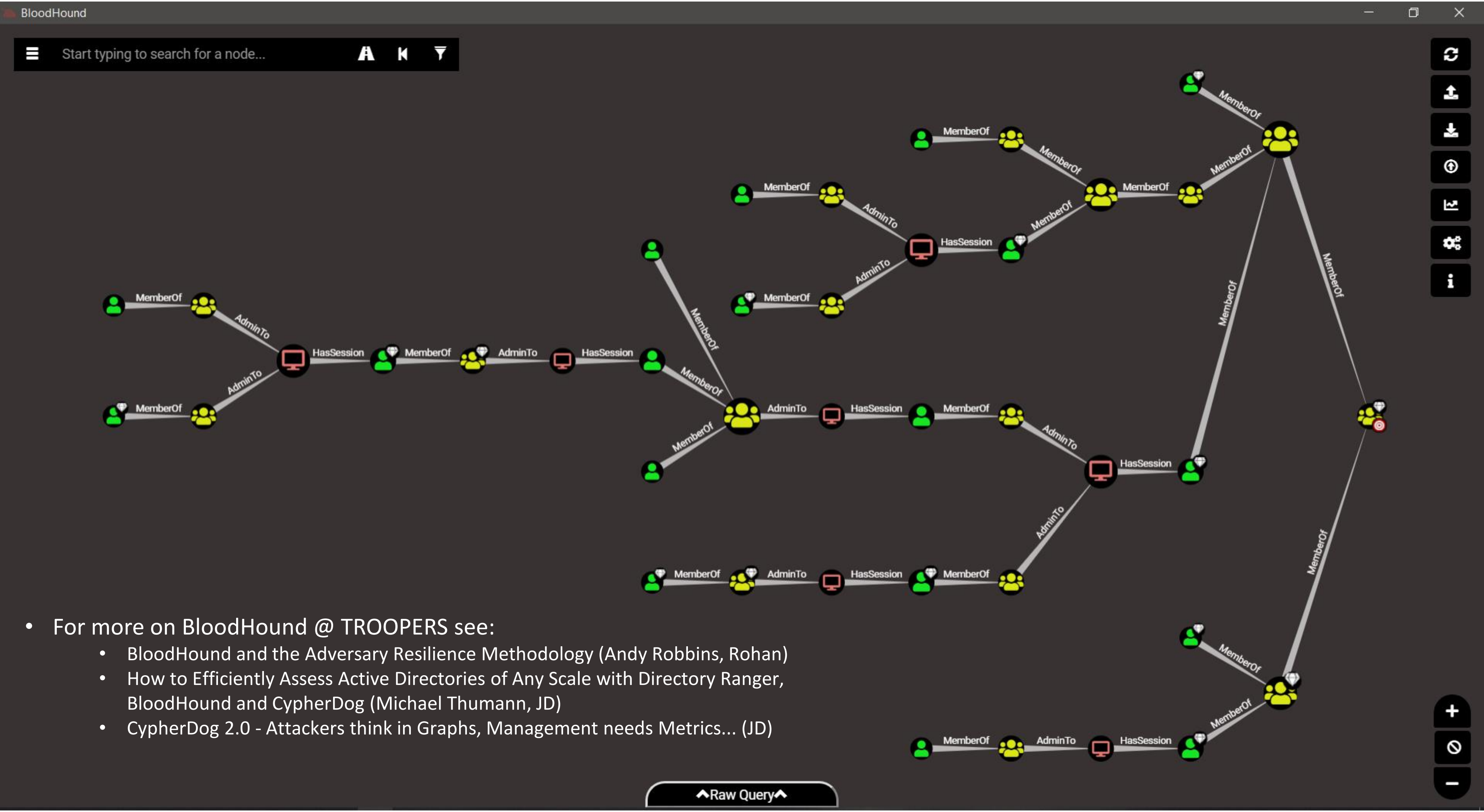
Management of Security Dependencies in Active Directory

- **Constructing** the **attack paths** can be done **manually** by reviewing permissions, group memberships etc.
- Or by using a tool such as **BloodHound**

- **BloodHound** uses **graph theory** to **reveal relationships** between users, computers, groups, and containers
  - Reveals additional security principals which are highly privileged and represent "**shadow admins**"

- Should be defined as a **process** for a **regular procedure** to
  - Get a better understanding of the impact of your configurations
  - Track changes over time in your AD environments

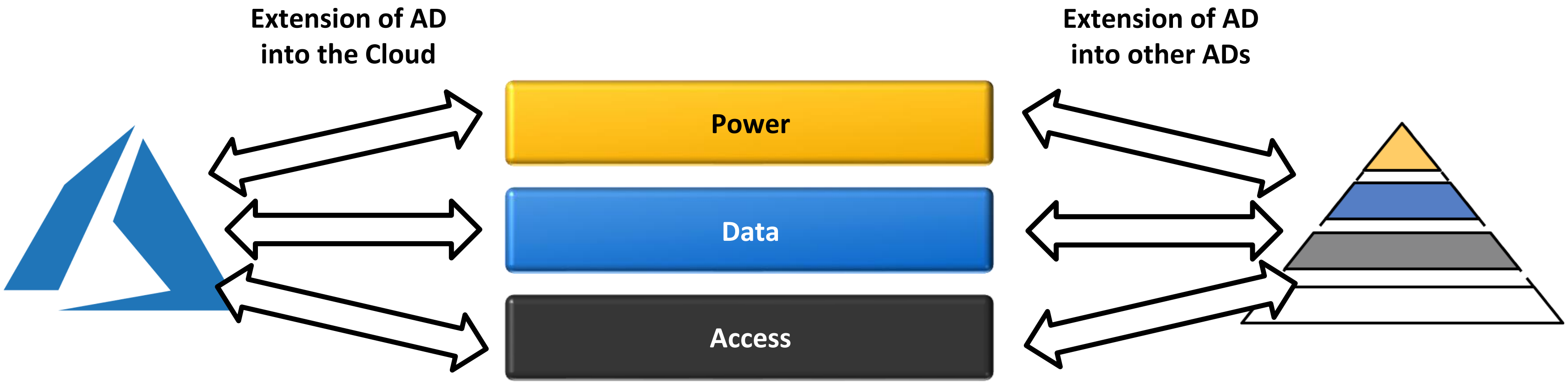

BloodHound
Start typing to search for a node...
MemberOf
AdminTo
HasSession
CanRDP
ForceChangePassword
AllowedToAct
GenericWrite
GenericAll
Raw Query



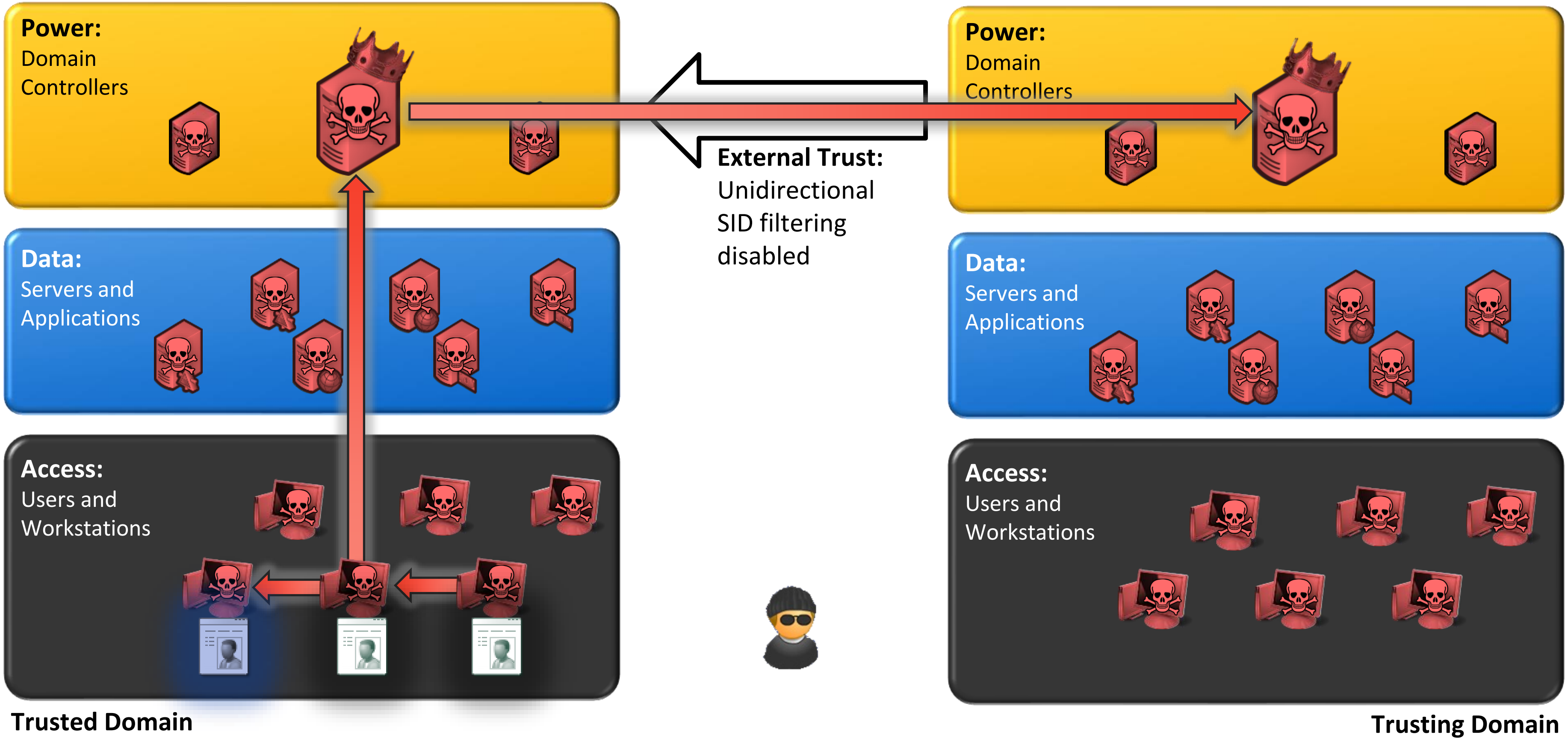
- For more on BloodHound @ TROOPERS see:
    - BloodHound and the Adversary Resilience Methodology (Andy Robbins, Rohan)
    - How to Efficiently Assess Active Directories of Any Scale with Directory Ranger, BloodHound and CypherDog (Michael Thumann, JD)
    - CypherDog 2.0 - Attackers think in Graphs, Management needs Metrics... (JD)

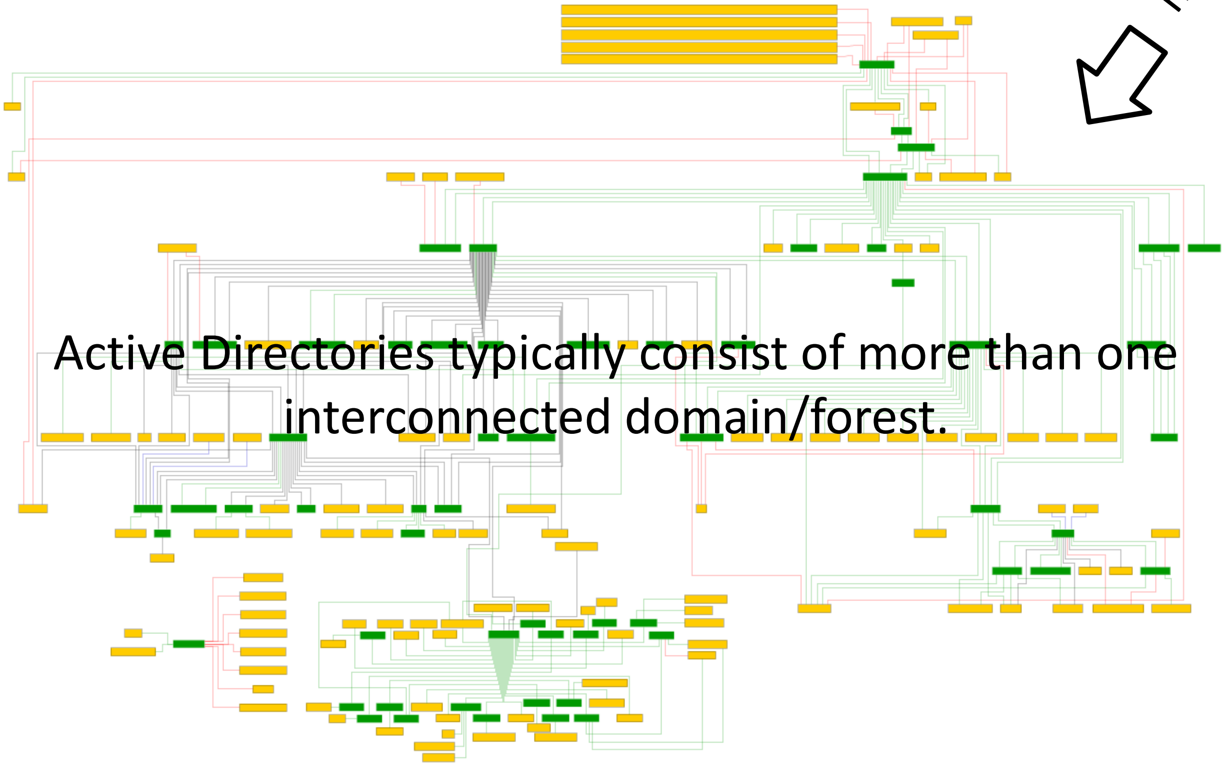
Limits of Common Controls: Cross Forest Security Dependencies

Security Dependencies May Extend Credential Theft & Reuse


Extension of AD into the Cloud
Extension of AD into other ADs
Power
Data
Access

Example: Pass-the-Credential via AD Trust Relationship

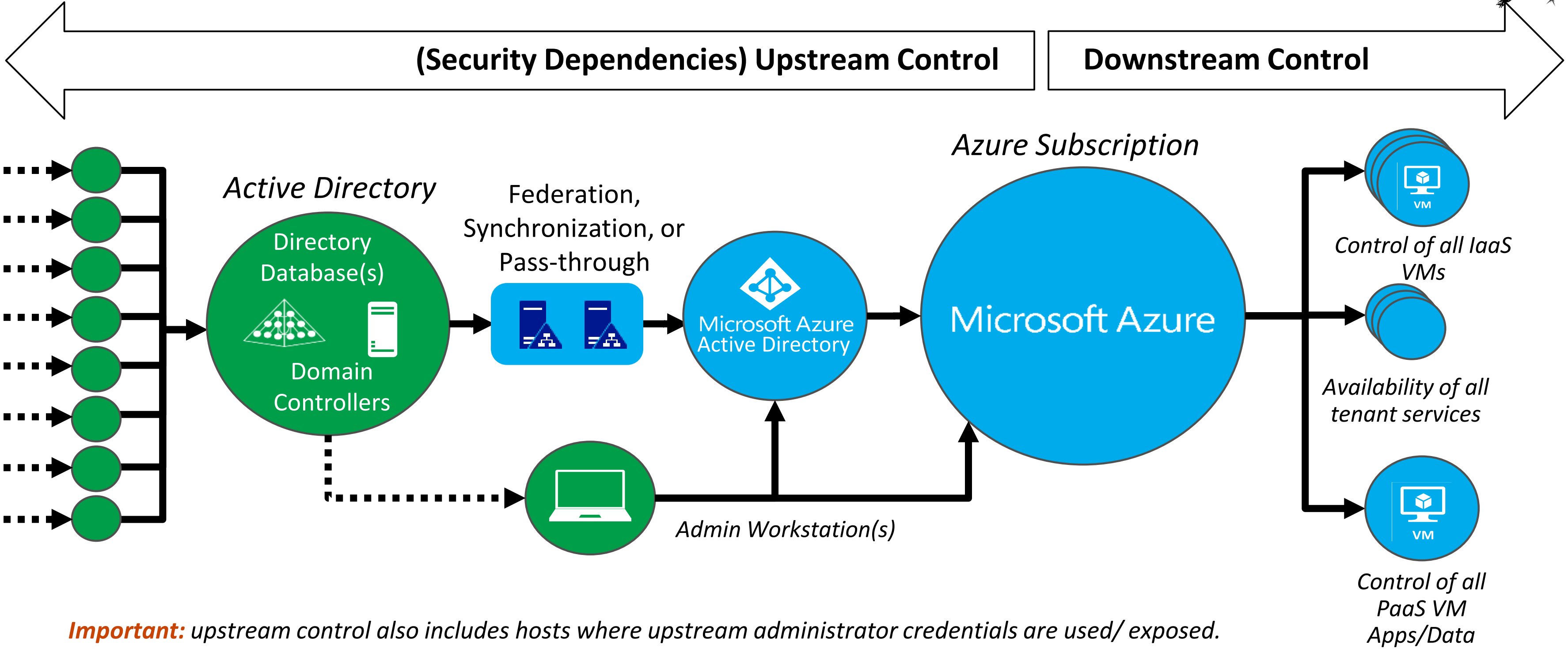




Active Directories typically consist of more than one interconnected domain/forest.

not a joke!

Means of Control in Azure



(Security Dependencies) Upstream Control
Downstream Control
Active Directory
Directory Database(s)
Domain Controllers
Federation, Synchronization, or Pass-through
Microsoft Azure Active Directory
Azure Subscription
Microsoft Azure
Admin Workstation(s)
VM
Control of all IaaS VMs
Availability of all tenant services
VM
Control of all PaaS VM Apps/Data

Important: *upstream control also includes hosts where upstream administrator credentials are used/ exposed.*

Source: Based on N. Raja: Architecting Azure For an Enterprise (https://channel9.msdn.com/Events/Ignite/Australia-2015/ARC341)

Example: Golden SAML

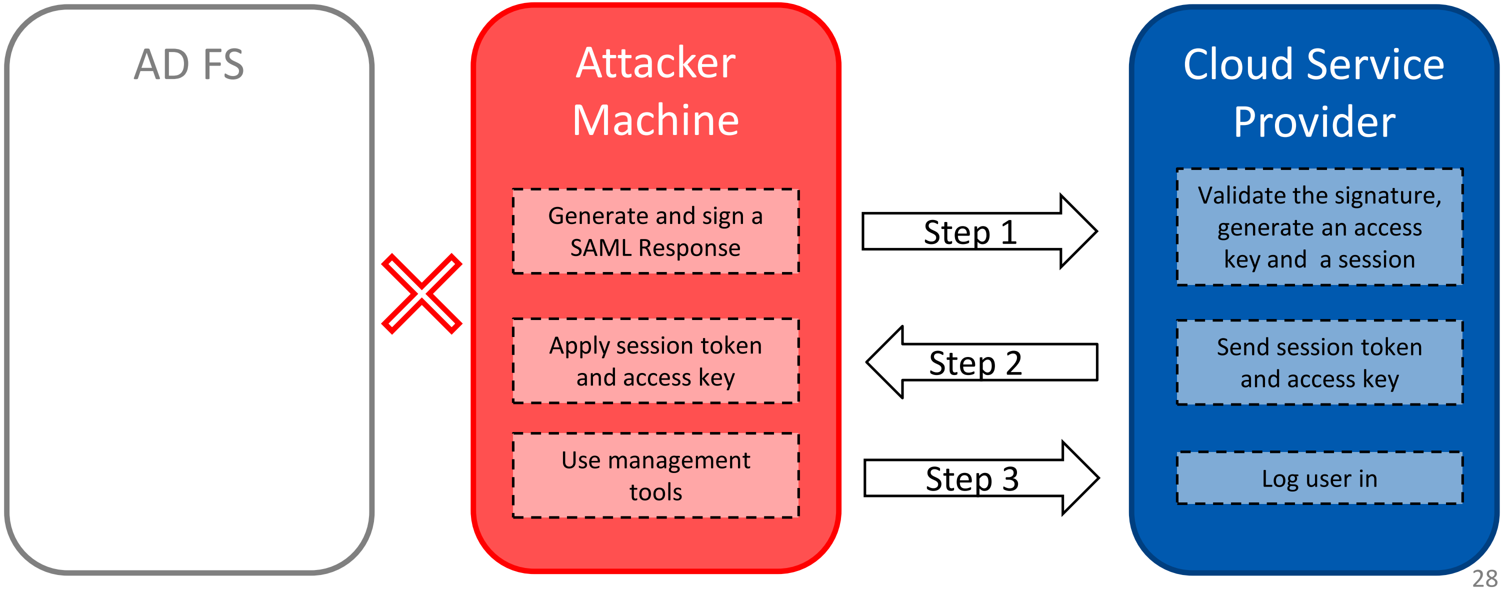
- **AD FS** can utilize the **SAML protocol** to:
  - Exchange authentication and authorization data between an identity provider (e.g. on-premise AD) and a service provider (e.g. Azure)
  - Provide SSO for web applications
  - Based on public-key cryptography to sign (and encrypt) SAML responses

- **Compromise the token-signing private key** of the Identity Provider means **unauthorized access to any service** in a federation with any privileges
  - Similar to a Golden Ticket
  - Does not require the compromise of a Domain Controller, only an AD FS server

- CyberArk has published a blog post and a tool that implements this attack
  - https://www.cyberark.com/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-cloud-apps/

- For more on AD FS @ TROOPERS see:
  - I am AD FS and so can you: Attacking Active Directory Federated Services (Doug Bienstock, Austin Baker)

Example: Golden SAML



AD FS
Attacker Machine
Generate and sign a SAML Response
Apply session token and access key
Use management tools
Step 1
Step 2
Step 3
Cloud Service Provider
Validate the signature, generate an access key and a session
Send session token and access key
Log user in

New Core Security Controls for Active Directory and Azure

- Hardening of Cross Forest Security Dependency Paths
- Admin Tiering in Azure
- Clean Source Principle in Azure

Hardening of Cross Forest Security Dependency Paths

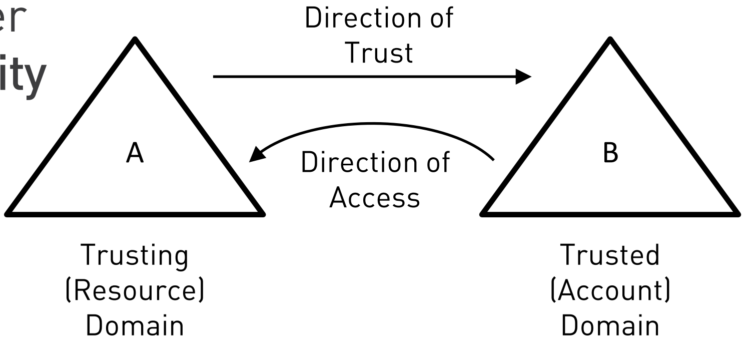
- Security of AD Trust Relationships
- Security of Azure AD Connections

Security of AD Trust Relationships

Security of AD Trust Relationships

- **Every trust relationship** to other ADs (other stage, DMZ, foreign) will **impact the security** of the own AD
  - Regardless of the trust direction!

- The **trust direction** influences whether **identities or resources** are exposed to the trusted/trusting AD



- For more on AD trusts @ TROOPERS see:
  - Not A Security Boundary: Breaking Forest Trusts (Will Schroeder, Lee Christensen)

ERNW
providing security.

Implement Hardening of AD Trust Relationships

- **Prerequisite:** All ADs that have connections via trusts should ideally also implement administrative tiers
  - Guarantees an comparable level of security
  - If necessary, the tiers of the source AD can be extended into the connected AD

Control 4: Implement Hardening of AD Trust Relationships

- When the need for a trust has been established, the following questions should be asked:
  - **Which direction of the trust is technically required?**
    - Unidirectional trusts should always be preferred

  - **Is the trust required for a migration project? Must SID filtering be disabled?**
    - SID filtering on external trusts should always be enabled
    - Forest trusts should not be treated as external trusts with regards to SID history and SID filtering

Control 4: Implement Hardening of AD Trust Relationships

- When the need for a trust has been established, the following questions should be asked:
  - **Should all users of the trusted domain/forest be able to access all resources of the trusting domain/forest?**
    - Selective Authentication should be enabled if technically and operationally feasible
  - **Will the trust be used for administrative purposes?**
    - Personnel with highly sensitive privileges should use a separate account for administrating the trusting forest/domain

ERNW
providing security.

Control 4: Implement Hardening of AD Trust Relationships

- After the aforementioned questions have been clarified:
  - **Results** should be **documented**
  - **Trusts** should be **configured accordingly**
  - **Trust configurations** should be regularly **reviewed** based on the documentation to catch drift (**every 6 – 12 months**)

- This **process** and **general guidelines** should be defined in a **"AD Trust Policy"**

Security of Azure AD Connections

- Hardening Azure AD Connect Accounts and Systems
- Hardening of AD FS Authentication
- Hardening of Pass-through Authentication

Control 5: Implement Hardening of Azure AD Connect Accounts and Systems

- System(s) running **Azure AD Connect sync engine** and **corresponding SQL database** should be treated and hardened as **Tier 0 system(s)**
  - Don't forget the basics, e.g. patching of Azure AD Connect

- The **ADSync service account** should run as a **Virtual Service Account** or at least a **Group Managed Service Account**, but not a normal user account

- The **AD DS Connector Account** should be hardened in accordance with **Microsoft Security Advisory 4056318**

Azure Active Directory Connect

AD DS Connector Account Overview

- With express settings created with **prefix MSOL_**
- Has a long complex **password** that **does not expire**
- Used to read/write information to Active Directory
- **Not protected** by **the AdminSDHolder object**
- Created directly under the on-premises AD **User container**
  - Members of the Account Operators group can escalate privileges

Permission through Express Installation	Used for
Replicate Directory Changes **Replicate Directory Changes All**	Password hash sync
Read/Write all properties User	Import and Exchange hybrid
Read/Write all properties iNetOrgPerson	Import and Exchange hybrid
Read/Write all properties Group	Import and Exchange hybrid
Read/Write all properties Contact	Import and Exchange hybrid
Reset password	Preparation for enabling password writeback

Implement Hardening of Azure AD Connect Accounts and Systems

- **Avoid** using the **Express Installation**
- **Avoid** use of **Account Operators** group
- **Move the AD DS Connector account** into an OU that is **only accessible by Tier 0 admins**
- Delegate the **Reset-Password permission** only to **Tier 0 admins**

- **Lock down** of **access to the AD DS connector account** by implementing **permission changes**
  - Azure AD Connect version **1.1.654.0** (and later) implements these changes
  - Upgrade will **not retroactively** apply these changes

Control 5: Implement Hardening of AD FS Authentication

- **Strict OS Hardening as a basis**
  - AD FS servers are as important as DCs!
  - Treat the AD FS servers as **Tier 0 systems** (no server administrators should have access)
  - **Protect the private key** used to sign/encrypt the tokens (e.g. with a HSM)
- **Use a Web Application Proxy (WAP)**
  - Only open necessary ports on the firewall
  - Limit number of endpoints enabled on the proxy
- Best Practices for AD FS Authentication:
  - Use the "Extended Protection for Authentication" feature
  - Use Extranet lockout protection

Active Directory Federation Services

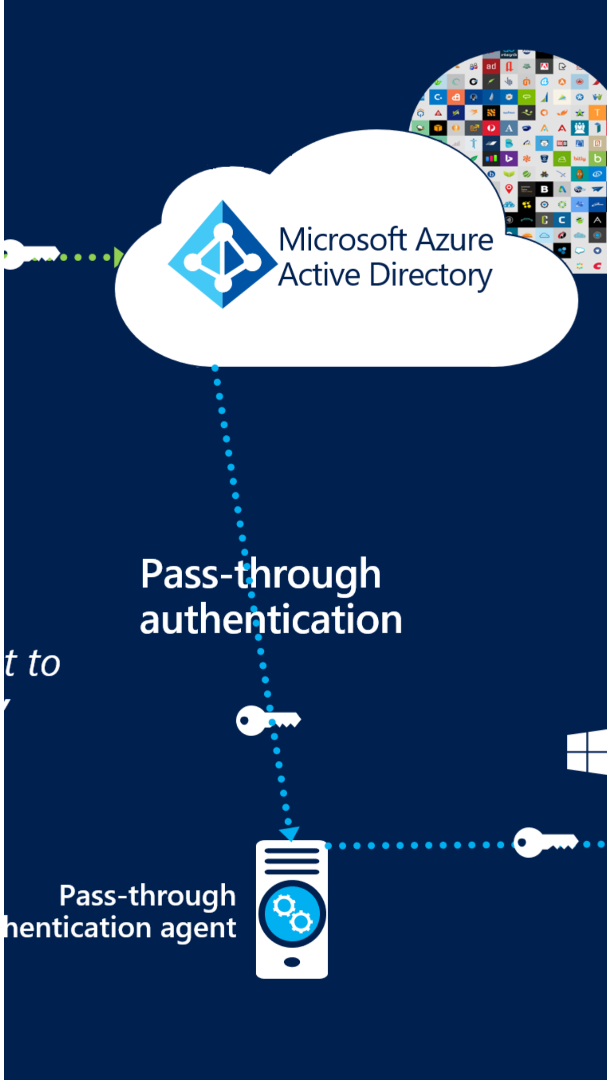
Microsoft Azure

Control 5: Implement Hardening of Azure AD Pass-through Authentication

- Compromise of servers running the authentication agent would **expose Azure resources**
  - Systems should be treated as **Tier 0 systems**

- **Open ports** on the firewall for **inbound** communication **not required**
  - If outbound filtering is enabled:
    - Open the necessary ports for outbound communication of the agent

- **Patching** and **certificate renewal** is **handled** by **Microsoft**



Admin Tiering in Azure

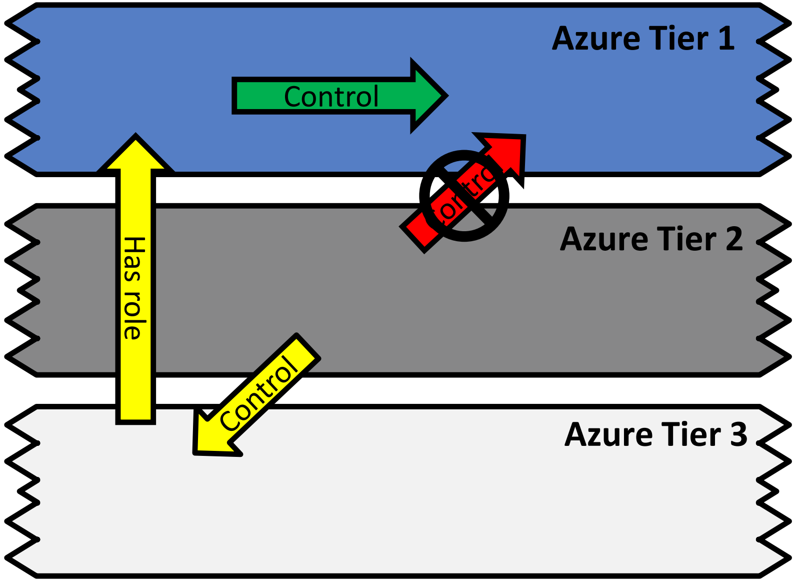
Administrative Tier Model in Azure (?)!

- Credential theft and privilege escalation are relevant for Azure too… So are Administrative Tiers ;-)

- **Administrative Tiers in Azure are in *any case* relevant security controls**
  - In case of an extension of your on-prem AD to Azure
  - In case of a potential future connection between your on-prem AD and Azure
  - Even in case of a complete separation of your on-prem AD and Azure

Example: User Account Administrators and Enterprise Application Owners (Issue)

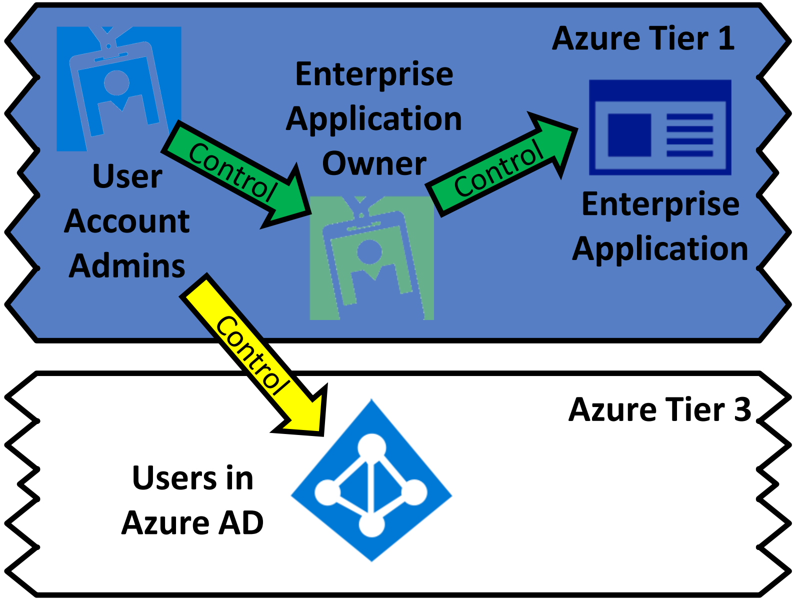
Enterprise Application Owner



User Account Administrator

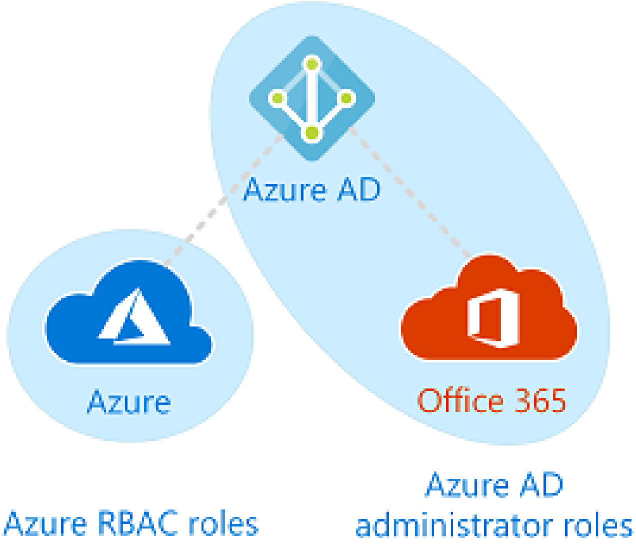
Users in Azure AD

Example: User Account Administrators and Enterprise Application Owners (Possible Solution)



Administrative Role Types in Azure You Have to Keep in Mind…

- **Azure AD roles (tenant-wide)**
  - Over 30 roles for administration of Identities, Applications, Devices and SaaS (such as Office 365)
- **Azure "classic" administration model roles**
  - Account Administrator (tenant-wide), Service Administrators and Co-Administrators (subscription-wide)
- **Azure Resource Manager model (Azure RBAC) roles**
  - Over 70 fine-grained administrative roles for administration of Azure resources



ERNW
providing security.

TROOPERS
MAKE THE WORLD A SAFER PLACE

Tier 0 Equivalency in Azure

- **Identities that grant the possibility to take control over an Azure tenant, have to be considered Tier 0**

- Tier 0 equivalency in Azure corresponds to the following accounts
  - Global Administrator (AAD role)
  - Privileged Role Administrator (AAD role)
  - Billing Administrator (Update organization.trustedCAsForPasswordlessAuth property in Azure Active Directory) (AAD role)

Tier 1 Equivalency in Azure

- **Most Azure and Office 365 resources can be seen** as equivalent to on-premise assets like
  - Enterprise servers (file servers, database servers, virtualization components etc.)
  - Services (patch management, AV, backups etc., Exchange Online)
  - Applications (SAP etc.)

- … and therefore **as belonging to Tier 1**
  - The administrators controlling the subscriptions and resources as well as most administrative roles in Azure AD that are not considered Tier 0 have to be placed in Tier 1
  - User Account Administrators may belong to Azure T 1, depending on the accounts they manage.

Tier 2 Equivalency in Azure

- Azure Tier 2 contains:
  - Systems /applications
    - Windows 10 machines joined to Azure AD
    - (If existent): VMs and applications (in Azure AD or Azure ADDS) that are classified as belonging to Azure T2
  - Administrative identities (such as):
    - Cloud Device Administrator
    - Device Administrators
    - Intune Administrator
    - Additionally local administrator of the devices
- But be careful as standard users in Azure AD can be authorized to have administrative privileges in Azure or Office 365 subscriptions

Implementation Steps of Admin Tiers in Azure

- Basically, the same as in on-prem Active Directory

- Every single security principal, system, or application has to be **classified** as belonging only to one tier

- Implement **control restrictions**
  - Via AAD administrative roles and RBAC model roles

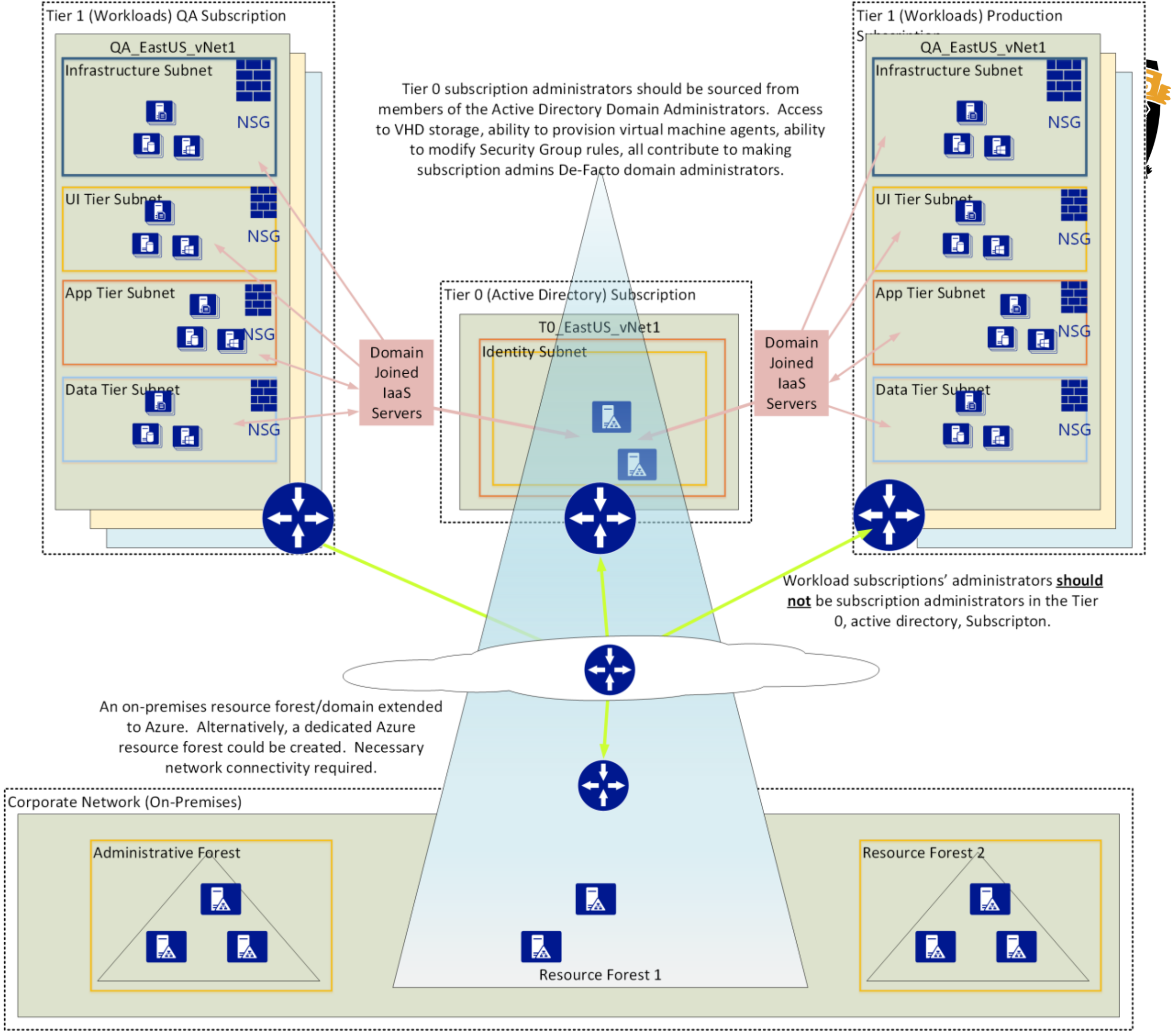
- Implement **logon restrictions** to prevent
  - Azure T 0 accounts from logging on to non-Tier 0 asset such as:
    - Azure T1 enterprise applications /services
    - AAD-joined (physical) Win10 devices (T2)
    - (If existent): VMs in Azure or in Azure ADDS that are defined as belonging to T2

  - Azure T 1 accounts from logging on to T2 asset such as:
    - AAD-joined (physical) Win10 devices
    - (If existent): VMs in Azure or in Azure ADDS that are defined as belonging to T2

ERNW
providing security.

Example: Admin Tiering for Tier 0 Assets Extended to Azure

See:
https://mva.microsoft.com/en-us/training-courses/security-in-a-cloudenabled-world-12725?l=ciV5MdAcB_5904300474



Tier 0 subscription administrators should be sourced from members of the Active Directory Domain Administrators. Access to VHD storage, ability to provision virtual machine agents, ability to modify Security Group rules, all contribute to making subscription admins De-Facto domain administrators.

Workload subscriptions' administrators **should not** be subscription administrators in the Tier 0, active directory, Subscripton.

An on-premises resource forest/domain extended to Azure. Alternatively, a dedicated Azure resource forest could be created. Necessary network connectivity required.

Controls for Admin Tiering in Hybrid ADs

- **Control 6:** Implement Administrative Tiers in Azure (in an equivalent manner to on-prem AD)
- Separate on-prem AD-Administration from Azure Administration
  - Separate on-prem Admin Tiers from Admin Tiers in Azure
  - Use on-prem AD identities for on-prem AD administration
  - Use Azure identities for Azure Administration
    - ⇒ *Don´t sync* on-prem admins of T0/T1/T2 to Azure
    - ⇒ *Don´t extend* on-prem T0/T1/T2 into Azure (use instead Azure AD Domain Services)
    - ⇒ *Use separate T1 admins* for on-prem domain-joined servers in Azure in case you already extended your T1 into Azure

Azure AD Privileged Identity Management

- Use Azure AD PIM if possible (requires E5 licence)

- PIM can be used to support the Least Privilege Principle and Admin Tiering by providing:
  - Just-in-time privileged access to Azure AD and Azure resources
  - Time-bound access to resources
  - Approval process to activate privileged roles (including a requirement for justification and sending of notifications)
  - Auditing capabilities (access logs, download functionality)

- Note: The following roles cannot be managed in PIM
  - Classic subscription administrator roles (Account Administrator, Service Administrator, Co-Administrator)
  - Roles within Exchange Online or SharePoint Online, except for Exchange Administrator and SharePoint Administrator

Clean Source Principle in Azure

ERNW
providing security.

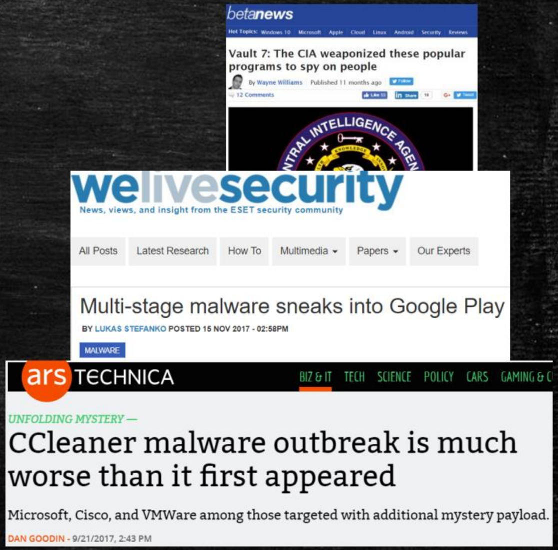
Control 7: Clean Source Principle in Azure (Software Installation)

- Installation of software or usage of downloaded data should follow the same principles as in the on-premise AD
  - New sources of software are available in the form of the Azure Marketplace
  - The market place provides various forms of "product types":
    - SaaS
    - Solution Templates
    - VM Images

- Pay special attention to VM images for IaaS from the Azure Marketplace as they are often outdated!

Cloud marketplaces are supply chains

- Supply chain attacks are increasingly common
- Cloud marketplaces could be next
- Lots of resources; high value targets
- Minimal validation of 3rd party IaaS VM images
- 3rd party IaaS images are ***OLD***
  - Average Azure Age: **123 days**
  - Average AWS Age: **717 days**
- Updating IaaS VM images is not retroactive



betanews
Hot Topics: Windows 10 Microsoft Apple Cloud Linux Android Security Reviews

Vault 7: The CIA weaponized these popular programs to spy on people

By Wayne Williams Published 11 months ago

12 Comments

welivesecurity
News, views, and insight from the ESET security community
All Posts
Latest Research
How To
Multimedia
Papers
Our Experts

Multi-stage malware sneaks into Google Play

BY LUKAS STEFANKO POSTED 15 NOV 2017 - 02:58PM

MALWARE

ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & C

UNFOLDING MYSTERY —

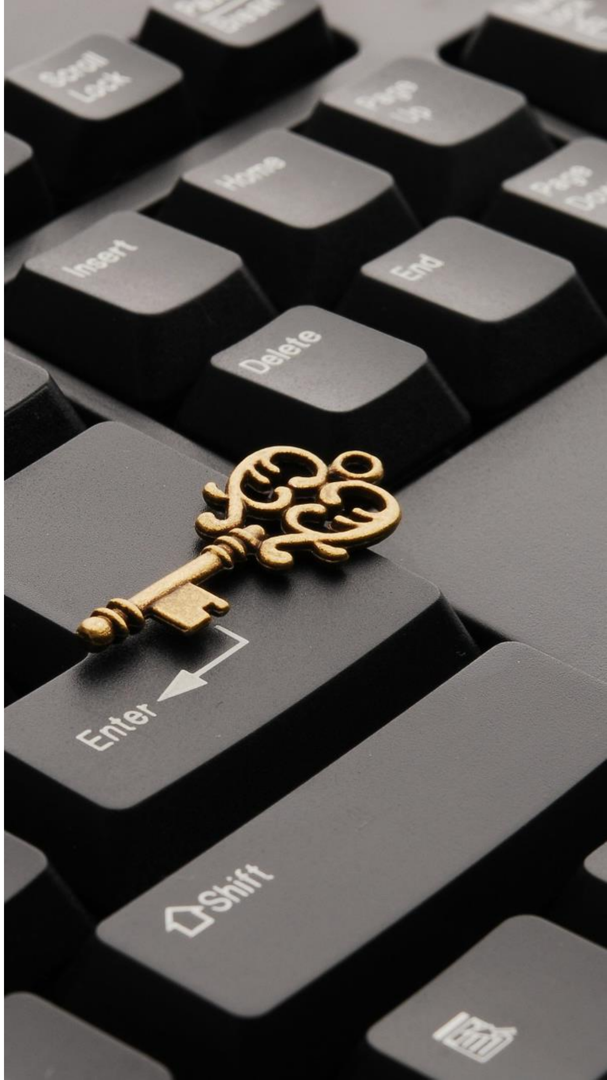
CCleaner malware outbreak is much worse than it first appeared

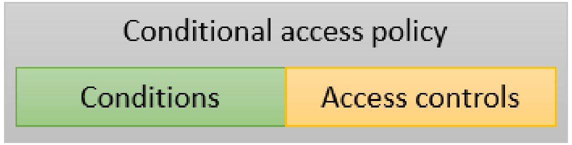
Microsoft, Cisco, and VMWare among those targeted with additional mystery payload.

DAN GOODIN - 9/21/2017, 2:43 PM

Control 7: Clean Source Principle in Azure (Administration)

- **Administration** of high-value Azure assets also **requires** the use of **PAWs**
  - Alternatives do not exist
  - Microsoft also does this for all on-premise and Azure resources!
- **Hardening** the **access path** becomes more important
  - Management of resources does not only take place inside your own network, but also over the Internet
  - Securing the “edge” becomes a priority by utilizing traditional network-based isolation/segmentation using IP-based firewall and route ACLs
- Network-based controls should be supplemented with user and machine identity checks





Azure AD Conditional Access

- **Conditions** ("when this happens“):
  - **Users and groups**
    - All or specific users/groups?
  - **Cloud apps**
    - All or specific apps?)
  - **Sign-in risk**
    - Via Azure AD Identity Protection
  - **Device platforms**
    - All or specific OSs?
  - **Device state**
    - All or only unmanaged devices?
  - **Locations**
    - Any or specific locations?

- **Access controls** (“then do this“):
- Grant or block access based on:
  - Multi-factor authentication
  - Compliant device (MDM)
  - Hybrid Azure AD joined device
  - Approved client app

- **Example:** Block access for global administrators on unmanaged devices.

Special Clean Source Principle Measures for Azure Administrators

- Use Azure Multi-Factor Authentication (MFA)
  - Should be required **at least** for all individual users who are permanently assigned to one or more of the Azure AD admin roles: Global administrator, Privileged Role administrator, Exchange Online administrator, and SharePoint Online administrator
  - Ideally, enabled for **all** Azure AD admin roles
  - ⚠ Keep in mind: MFA should not be the sole protection mechanism for admin accounts!

- Use **work accounts** instead of Microsoft accounts
  - Microsoft accounts should be replaced by **individual cloud-based** or **synchronized accounts**

- Global administrator accounts should not have personal email addresses

> “Only 0.73% of tenant admins have Multi-factor Authentication enabled.”

Microsoft Ignite 2017 BRK3016

Core Security Controls Overview

Core Security Controls Overview

- Common Core Security Controls for Active Directory
  - Control 1: Implement Administrative Tiers
    - Control 1a: Classify every security principal, system, or application as belonging only to one tier
    - Control 1b: Implement logon restrictions
    - Control 1c: Implement control restrictions
  - Control 2: Implement Clean Source Principle
    - Control 2a: Implement PAWs
    - Control 2b: Implement ESAE
  - Control 3: Understand and Manage Security Dependencies in Active Directory
    - Control 3a: Identify security dependencies in Active Directory
    - Control 3b: Supervise & harden security dependencies in Active Directory
    - Control 3c: Apply change management to security dependencies in Active Directory

Core Security Controls Overview

- New Core Security Controls for Active Directory and Azure
  - Control 4: Implement Hardening of AD Trust Relationships
    - Control 4a: Implement unidirectional trusts
    - Control 4b: Disable SID filtering only within a well-defined time frame
    - Control 4c: Use selective authentication whenever possible
    - Control 4d: Use dedicated accounts for cross-forest administration
  - Control 5: Implement Hardening of Azure AD Connections
    - Control 5a: Harden Azure AD Connect Accounts and Systems
    - Control 5b: Harden of AD FS Authentication
    - Control 5c: Harden of Pass-through Authentication

Core Security Controls Overview

- New Core Security Controls for Active Directory and Azure
  - Control 6: Implement Administrative Tiers in Azure including Logon Restrictions and Control Restrictions (in an equivalent manner to on-prem AD)
    - Control 6a: Separate on-prem Admin Tiers from Azure Admin Tiers
    - Control 6b: Separate on-prem administration from Azure administration (use on-prem AD identities for on-prem AD administration and Azure identities for Azure Administration)
    - Control 6c: Don’t sync on-prem admins of T0/T1/T2 to Azure
    - Control 6d: Don’t extend on-prem T0/T1/T2 into Azure (use instead Azure AD Domain Services)
    - Control 6e: Use Azure AD PIM if possible
  - Control 7: Implement Clean Source Principle in Azure
    - Control 7a: Clean Source Principle for Software Installation
    - Control 7b: Clean Source Principle for Administration

@DirectoryRanger

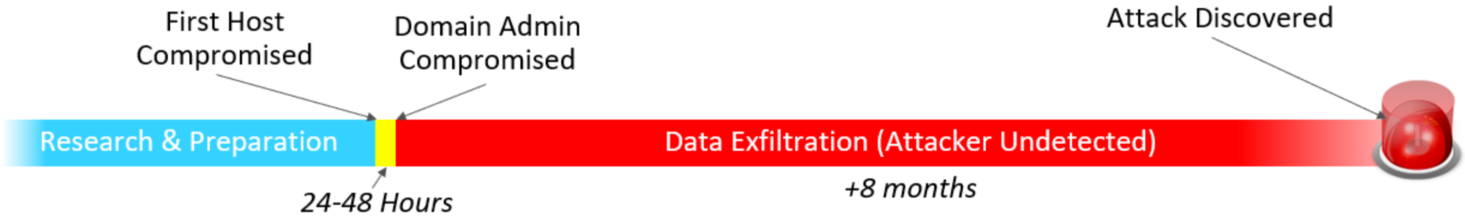
Thank you for your attention!

fkuhn@ernw.de
hwiederkehr@ernw.de

www.ernw.de

www.insinuator.net

Backup /Additional Information



Attack Sophistication
Attack operators will exploit any weakness
Target information on any device or service

Exploiting Credentials
On-premises Active Directory controls access to business assets
Attackers commonly target AD DS and IT Admins

Attacks not detected
Current detection tools miss most attacks
You may be under attack (or compromised)

Response and Recovery
Response requires advanced expertise and tools.
Expensive and challenging to successfully recover from.

See: https://msdnshared.blob.core.windows.net/media/2018/02/SLAM-and-ATA-CIP-Presentation_Updated_2_21_2018.pptx

Sources

- Icons
  - https://icons8.com/