RSA®Conference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: STR-R02

Future Forests: Realistic Strategies for AD Security & "Red Forest" Architecture

Katie Knowles

Security Consultant
MWR InfoSecurity
@_sigil

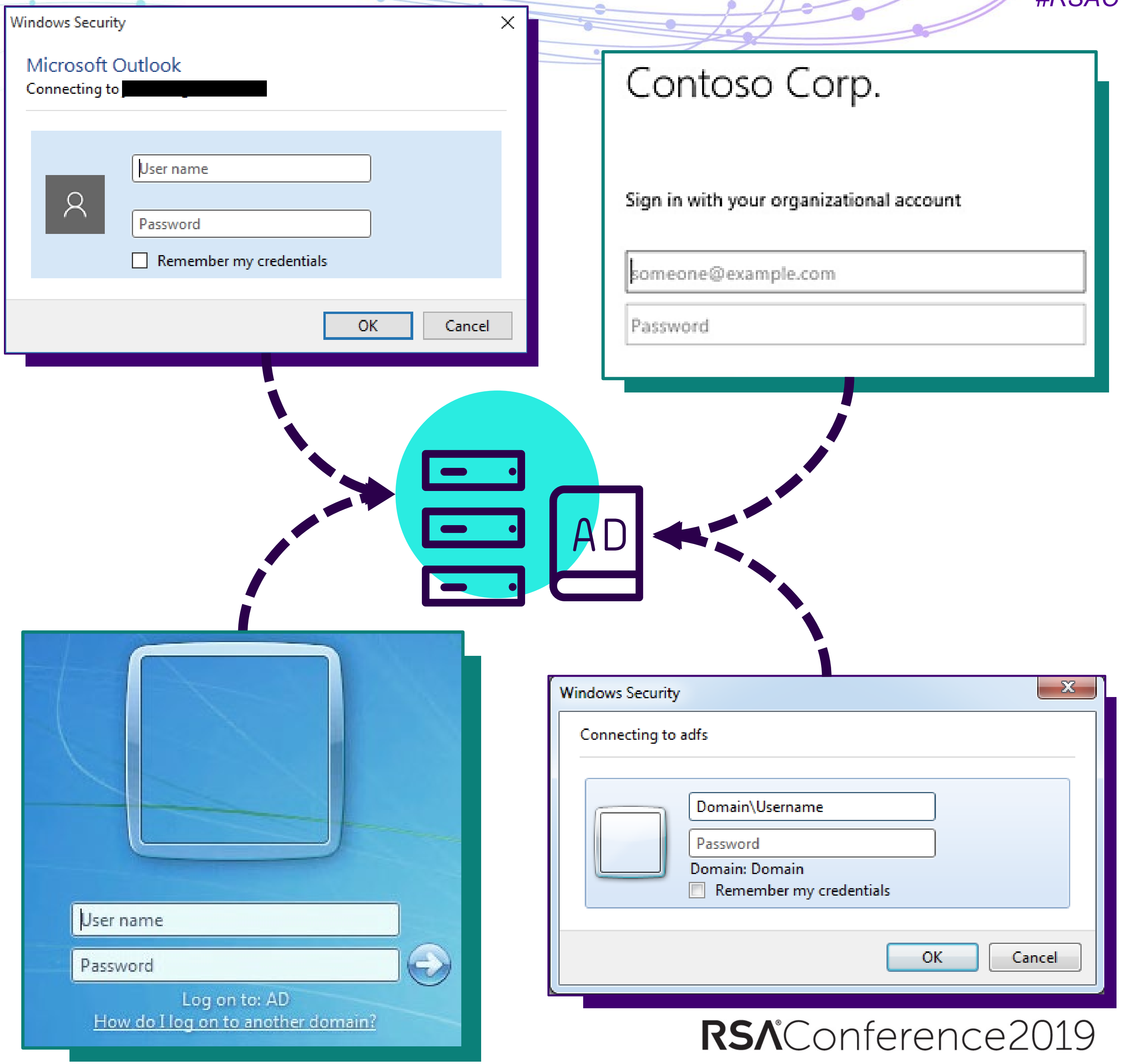
- Introduction:
  - Why AD Matters
  - How AD is Targeted
- Preventing Compromise:
  1. Local Credentials
  2. Administrative Systems
- Reducing Impact:
  - *What’s a “Red Forest”?*
  3. Administrative Forest
  4. Administrative Permissions
  5. Tiered Architecture
- Takeaways & Applications

Why AD Matters

- Used by 90% of organizations
- Tools allow quick mapping to high-value targets
- Compromise of domain = Compromise of forest

"Game Over":

Domain Administrator (DA) access to Domain Controller (DC)



Windows Security

Microsoft Outlook

Connecting to [redacted]

User name

Password

□ Remember my credentials

Contoso Corp.

Sign in with your organizational account

someone@example.com

Password

User name

Password

Log on to: AD

How do I log on to another domain?

Windows Security

Connecting to adfs

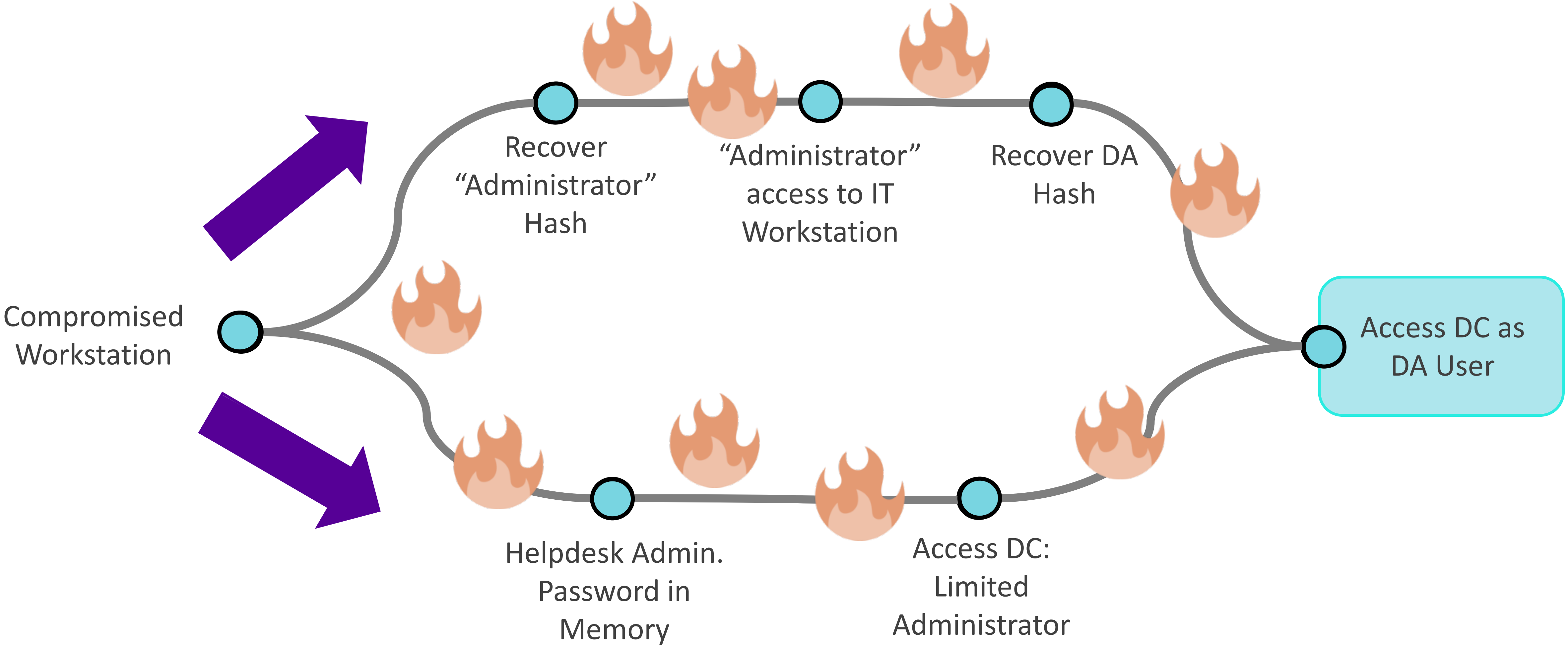
Domain\Username

Password

Domain: Domain

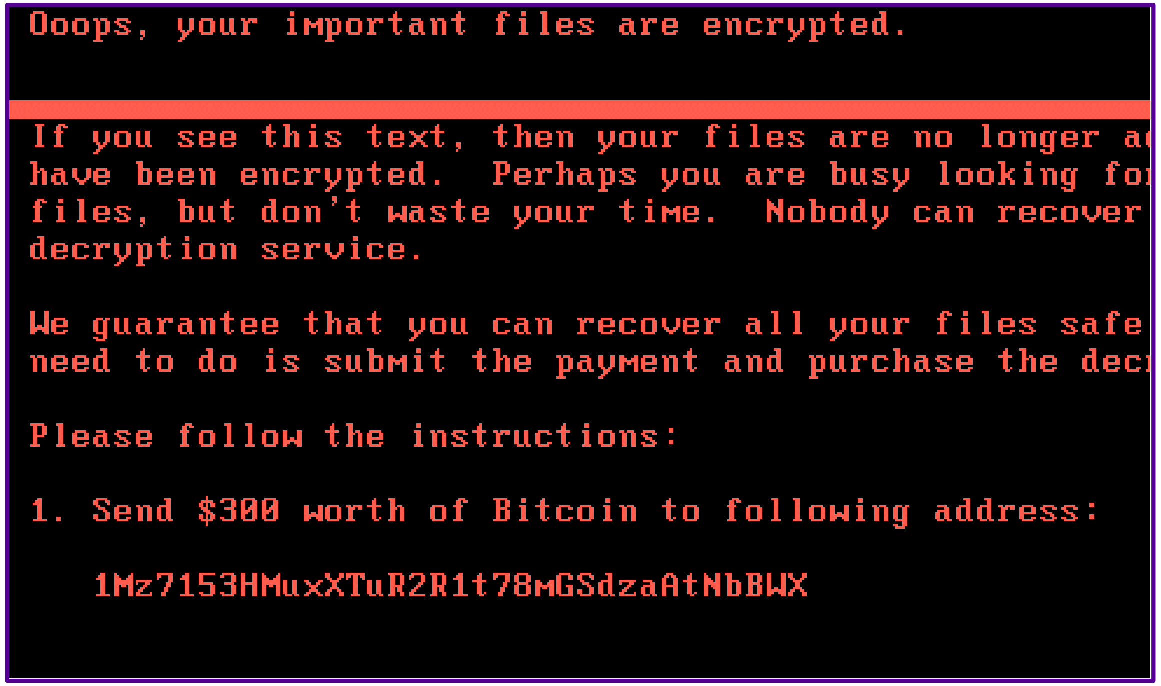
□ Remember my credentials

How AD is Compromised


Compromised Workstation
Recover "Administrator" Hash
"Administrator" access to IT Workstation
Recover DA Hash
Helpdesk Admin. Password in Memory
Access DC: Limited Administrator
Access DC as DA User

NotPetya

- Backdoor in tax software allows attackers to deploy “wiper” disguised as ransomware
- NotPetya spreads…
  - EternalBlue (MS17-010)
  - Dumping credentials
- Maersk Estimated Impact:
  - $250-300 million in earnings
  - 45k+ PCs + 4k servers rebuilt over 10 days



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer ac
have been encrypted.  Perhaps you are busy looking for
files, but don't waste your time.  Nobody can recover
decryption service.

We guarantee that you can recover all your files safe
need to do is submit the payment and purchase the dec

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
```

WIRED, “The Untold Story of NotPetya”: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Detection vs. Prevention

Fire Tower:

- Identify fires
- Monitor spread of fires
- Alert base to dispatch firefighters

Incident Detection

Fire Break:

- Separate risky environments
- Prevent spread of fire
- Increase difficulty to burn

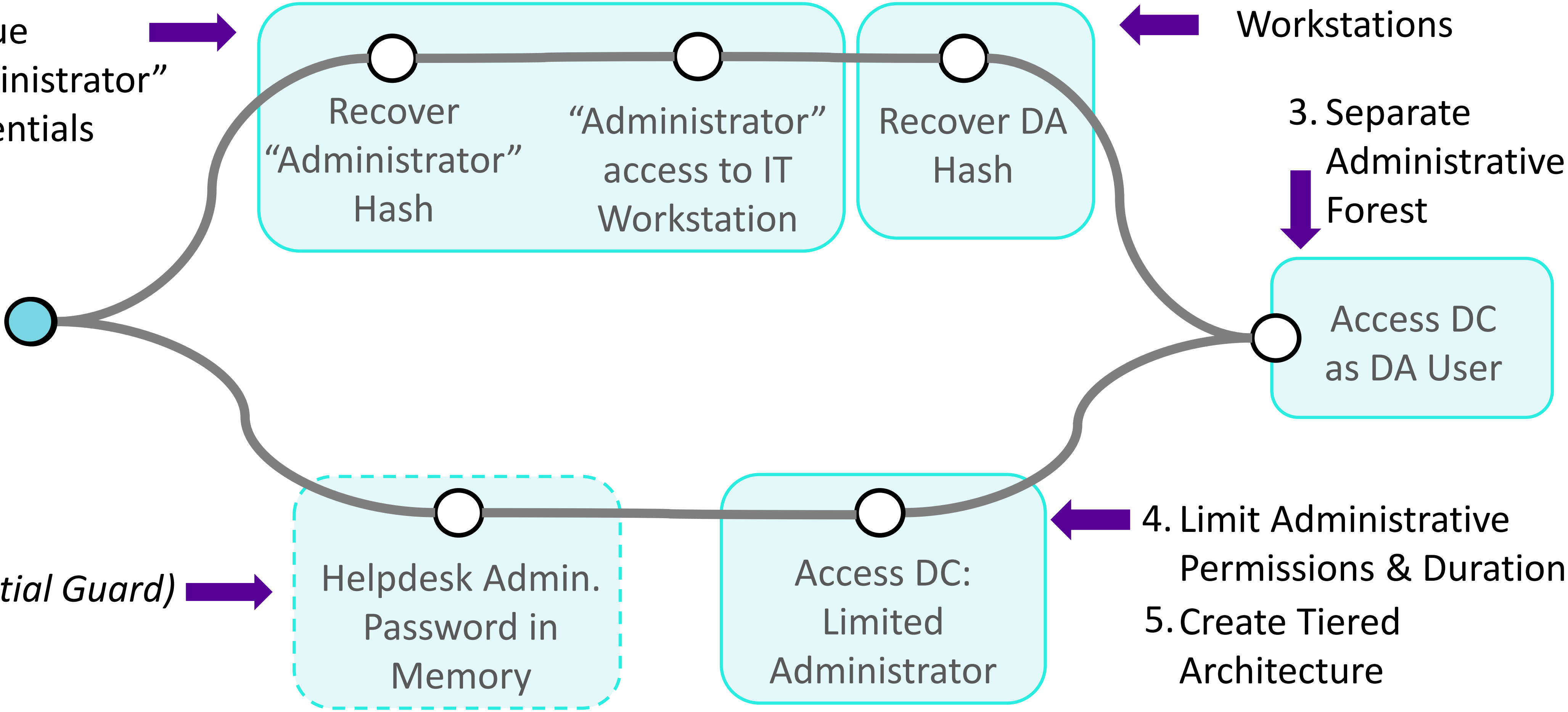
Incident Prevention

Resilient AD Architecture

1. Secure Local Credentials
2. Isolate Administrative Systems
3. Create Administrative Forest *
4. Limit Administrative Permissions & Duration *
5. Adopt Tiered Architecture *

***** *Red Forest/ESAE Core Concepts*

Piecing it All Together

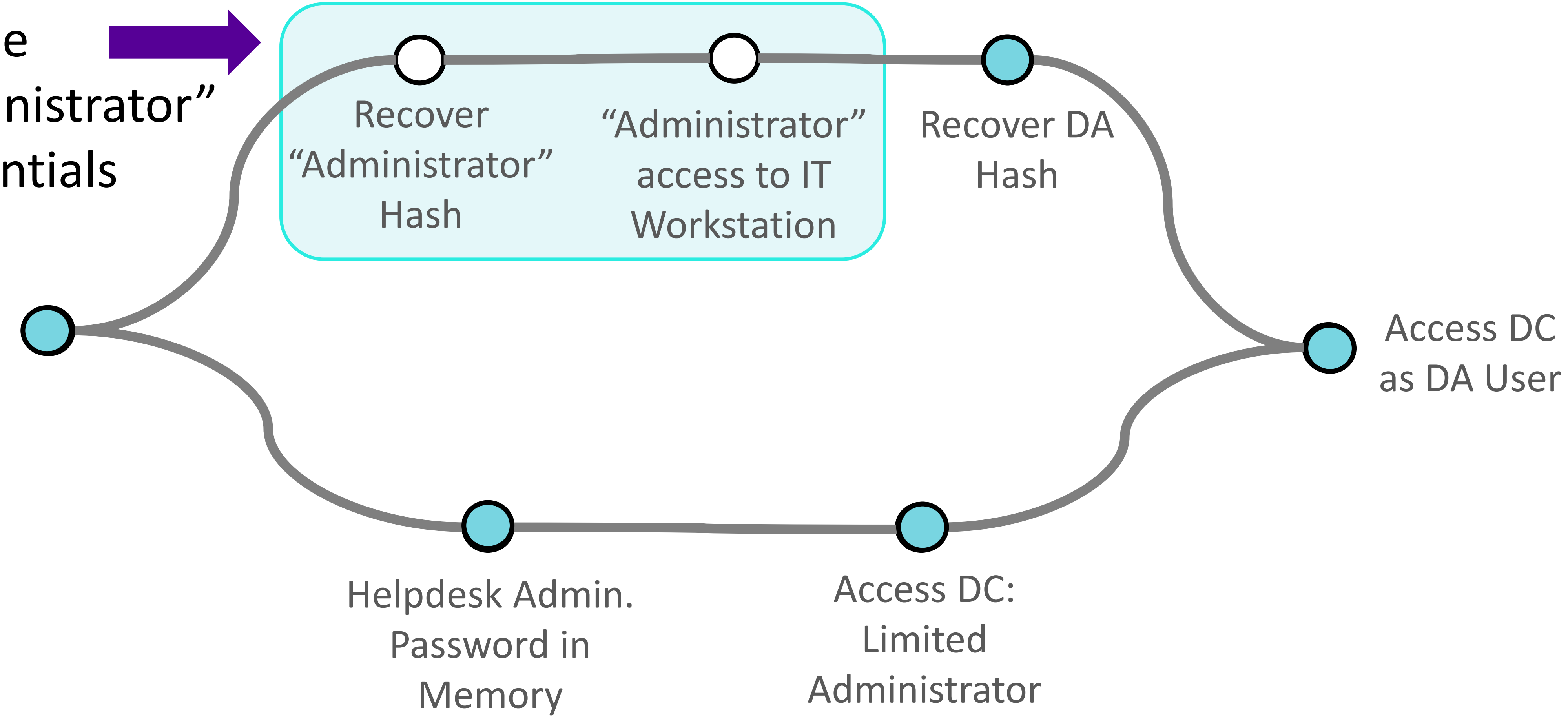

Compromised Workstation
Recover "Administrator" Hash
"Administrator" access to IT Workstation
Recover DA Hash
Access DC as DA User
Helpdesk Admin. Password in Memory
Access DC: Limited Administrator

1. Unique "Administrator" Credentials
2. Separate Administrative Workstations
3. Separate Administrative Forest
4. Limit Administrative Permissions & Duration
5. Create Tiered Architecture

(Credential Guard)

Secure Local Credentials

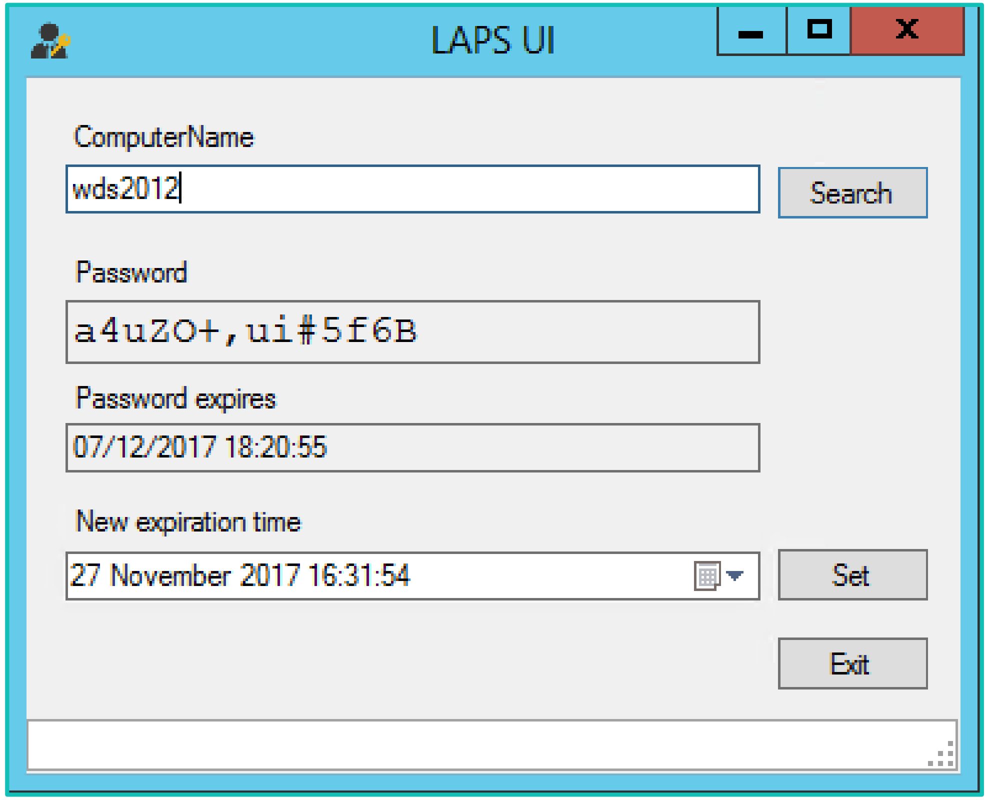
1. Unique "Administrator" Credentials


Recover "Administrator" Hash
"Administrator" access to IT Workstation
Recover DA Hash
Compromised Workstation
Access DC as DA User
Helpdesk Admin. Password in Memory
Access DC: Limited Administrator

Secure Local Credentials

- Each local system contains a built-in “Administrator” account
- Credential reuse allows attackers to pivot & Pass the Hash

- Generate unique passwords for the “Administrator” account



ComputerName: wds2012

Password: a4uZO+,ui#5f6B

Password expires: 07/12/2017 18:20:55

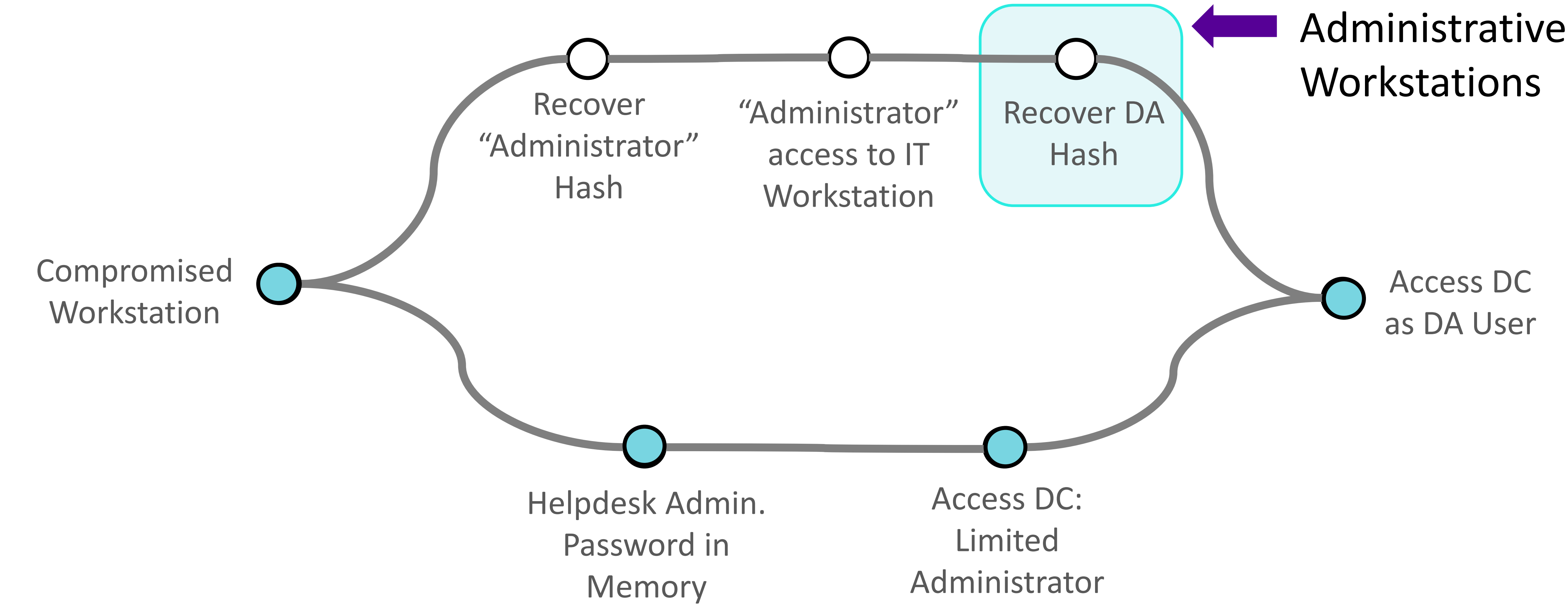
New expiration time: 27 November 2017 16:31:54

Microsoft’s Local Administrative Password Solution (LAPS) randomizes “Administrator” passwords

Suggestions

- Credentials (passwords, hashes) can still be recovered from memory without Credential Guard
  - Implement for Win10/Server 2016
- Disable or remove remote access from the “Administrator” account

Isolate Administrative Systems



Compromised Workstation

Recover "Administrator" Hash

"Administrator" access to IT Workstation

Recover DA Hash

Access DC as DA User

Helpdesk Admin. Password in Memory

Access DC: Limited Administrator

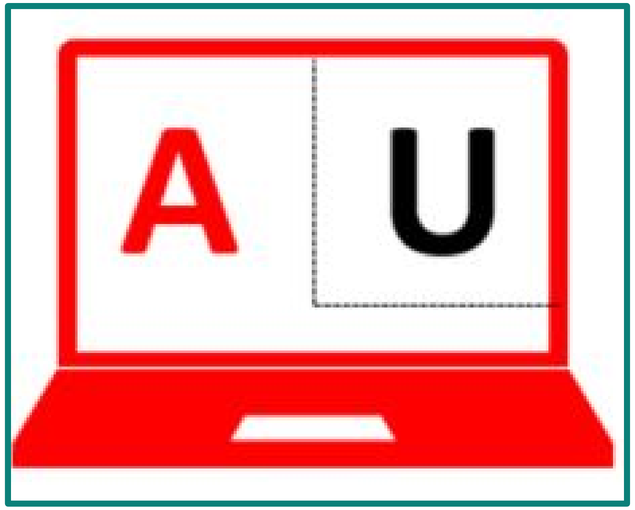
2. Separate Administrative Workstations

Isolate Administrative Systems

- Same workstation for user and admin functions
- User workstation compromise leads to administrative session compromise

↓

- Separate user and administrator tasks to separate systems

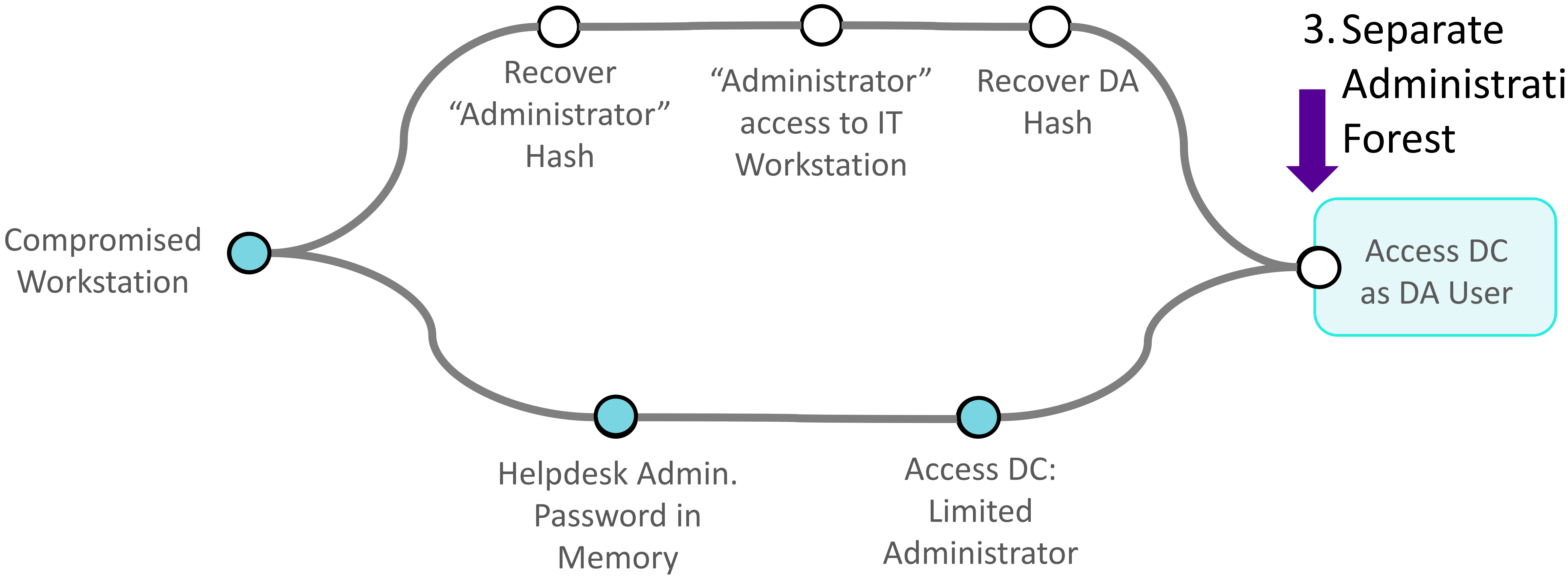


Microsoft's Privileged Access Workstation (PAW) architecture separates Admin & User functions

Suggestions

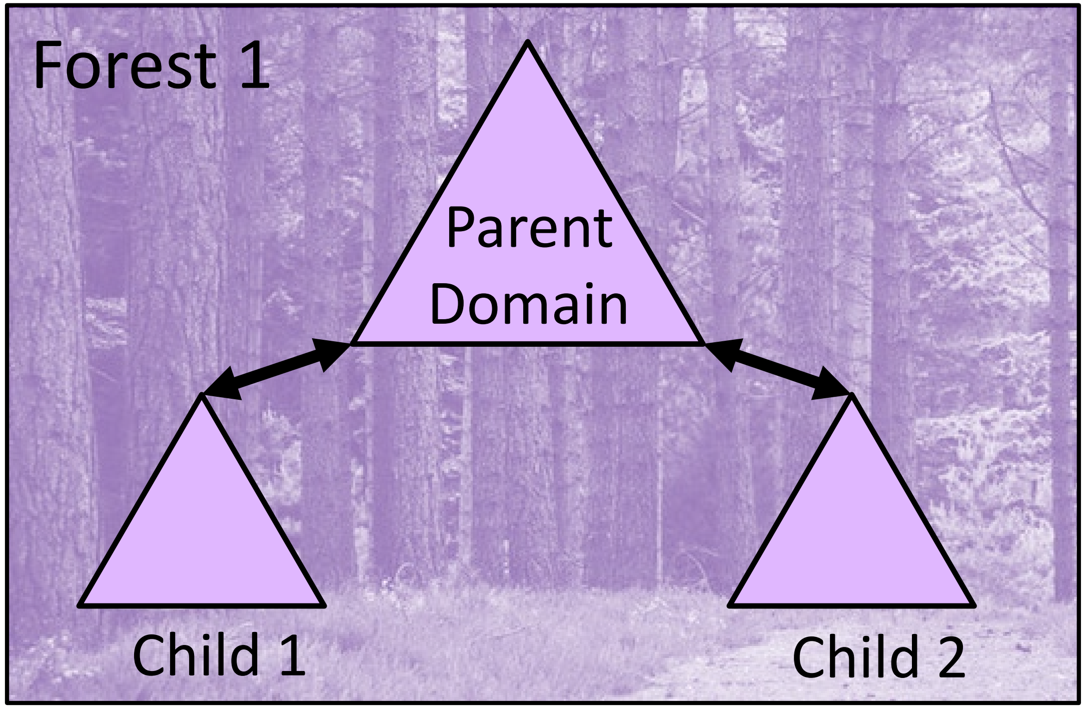
- Environments relying on cloud solutions may require administrative access to external URLs
- Consider a hardened administrative system with access to only specific domains

Create Administrative Forest

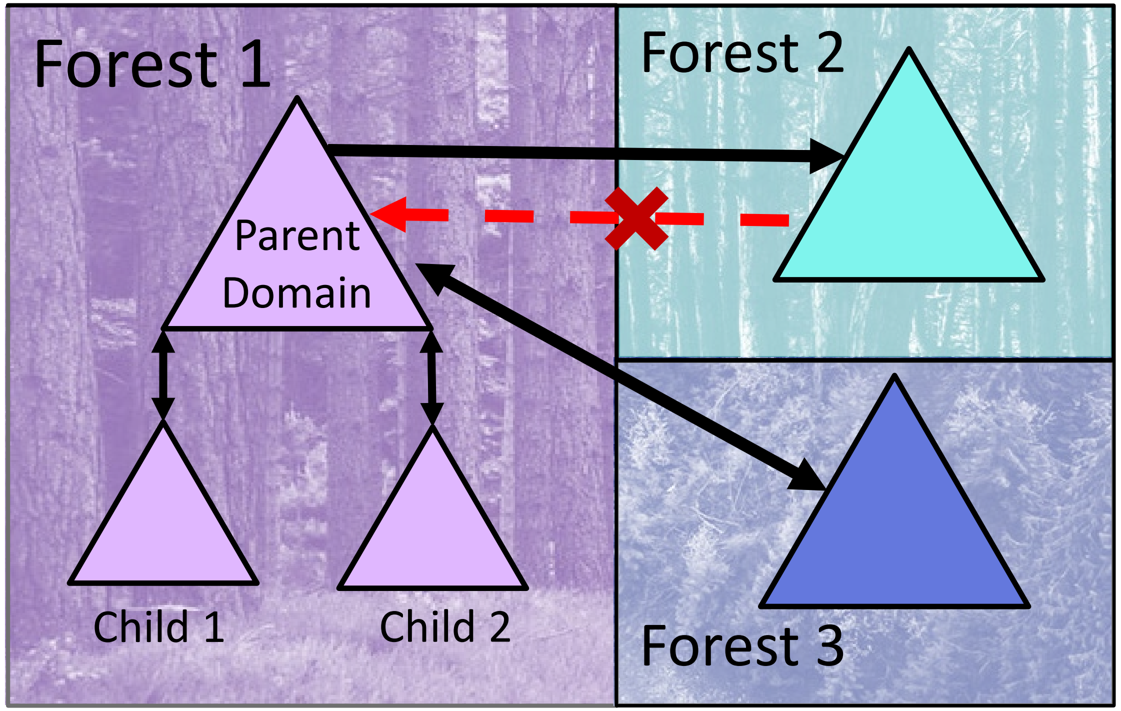

Compromised Workstation
Recover "Administrator" Hash
"Administrator" access to IT Workstation
Recover DA Hash
Helpdesk Admin. Password in Memory
Access DC: Limited Administrator
Access DC as DA User

3. Separate Administrative Forest

Why a Separate Forest?

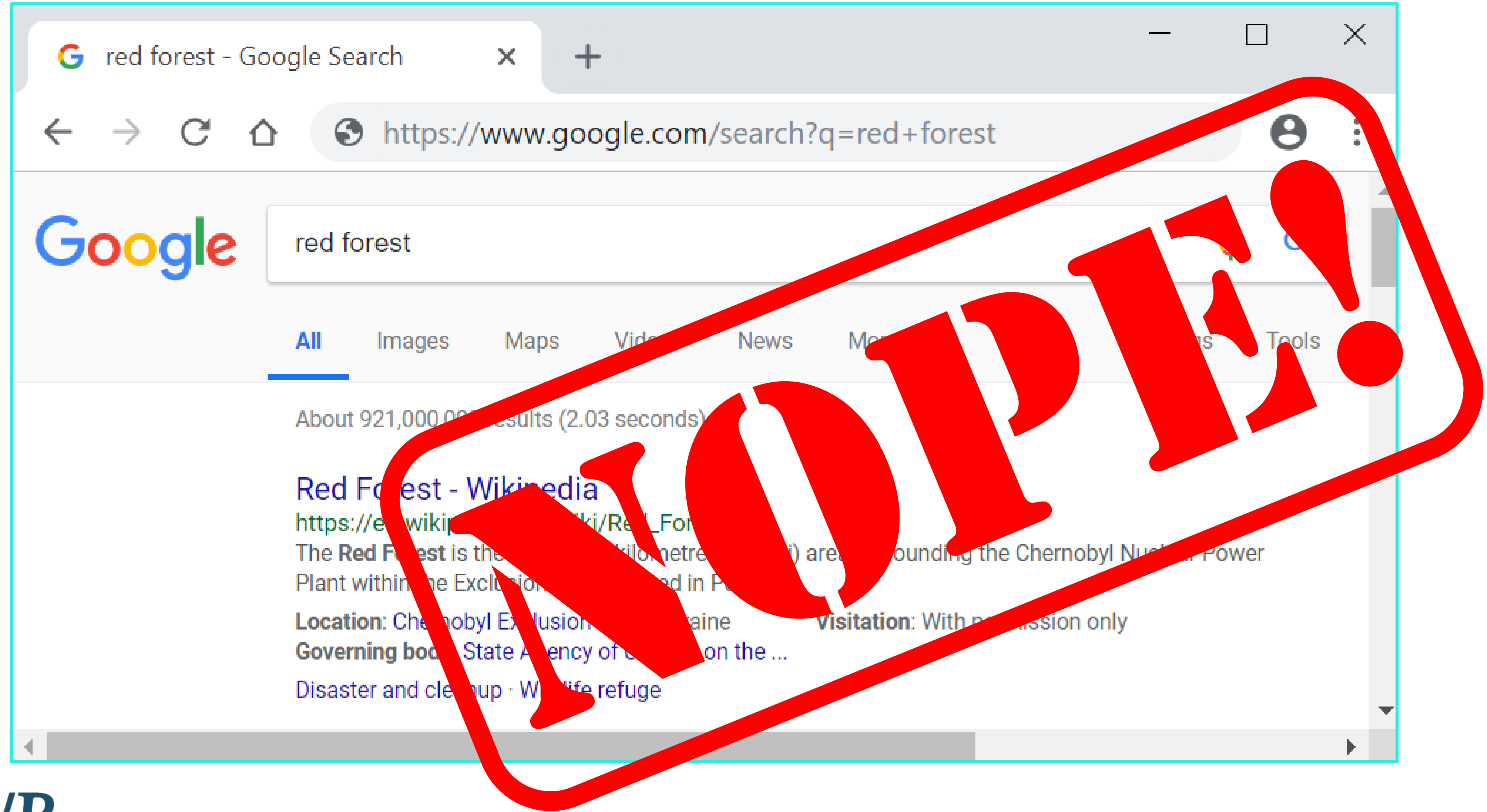


- Transitive trust exists between all domains in a forest
- All trust relationships are two-way
- Compromise of **Child 1** =
  Compromise of **Child 2** & **Parent**



- Nontransitive trust between forests allows creation of external trusts
- Two-way or one-way trust possible
- Compromise of **Forest 1** =/=
  Compromise of **Forest 2**

What’s a “Red Forest”?



red forest - Google Search
https://www.google.com/search?q=red+forest
Google
red forest
All
Images
Maps
Vid
News
Mo
Tools

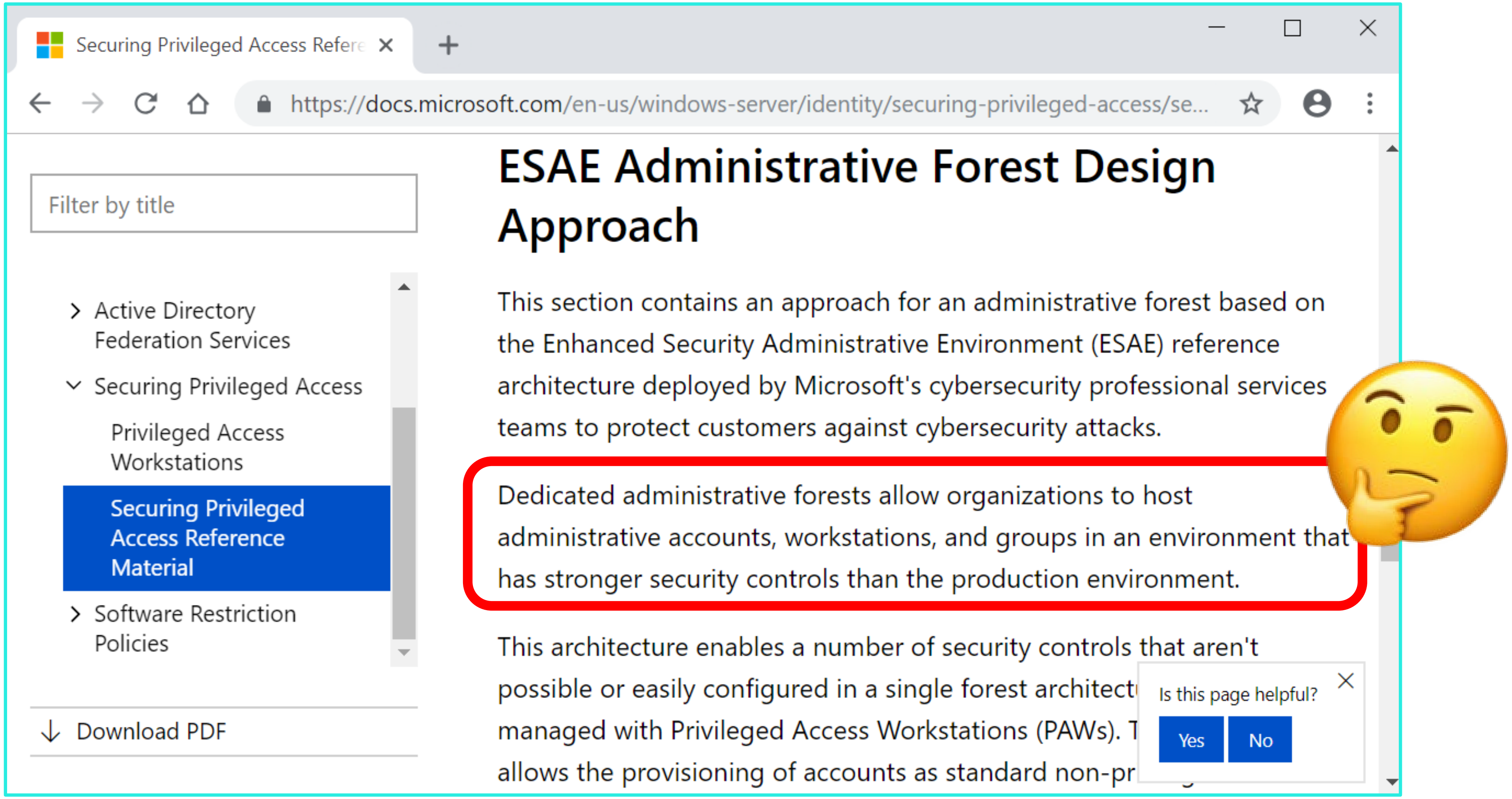
About 921,000,00 esults (2.03 seconds)

Red Fo est - Wiki edia
https://e wiki ki/Re _For
The **Red F est** is the kilometre) are ounding the Chernobyl Nu Power Plant withi he Exclusio ed in P

Location: Che obyl E lusio aine **Visitation:** With ssion only
Governing bod State A ency of on the ...
Disaster and cle up · W life refuge

NOPE!

What’s a “Red Forest”?



Securing Privileged Access Refere ×
+
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/se...
Filter by title
Active Directory Federation Services
Securing Privileged Access
Privileged Access Workstations
Securing Privileged Access Reference Material
Software Restriction Policies
Download PDF
Is this page helpful?
Yes
No

ESAE Administrative Forest Design Approach

This section contains an approach for an administrative forest based on the Enhanced Security Administrative Environment (ESAE) reference architecture deployed by Microsoft's cybersecurity professional services teams to protect customers against cybersecurity attacks.

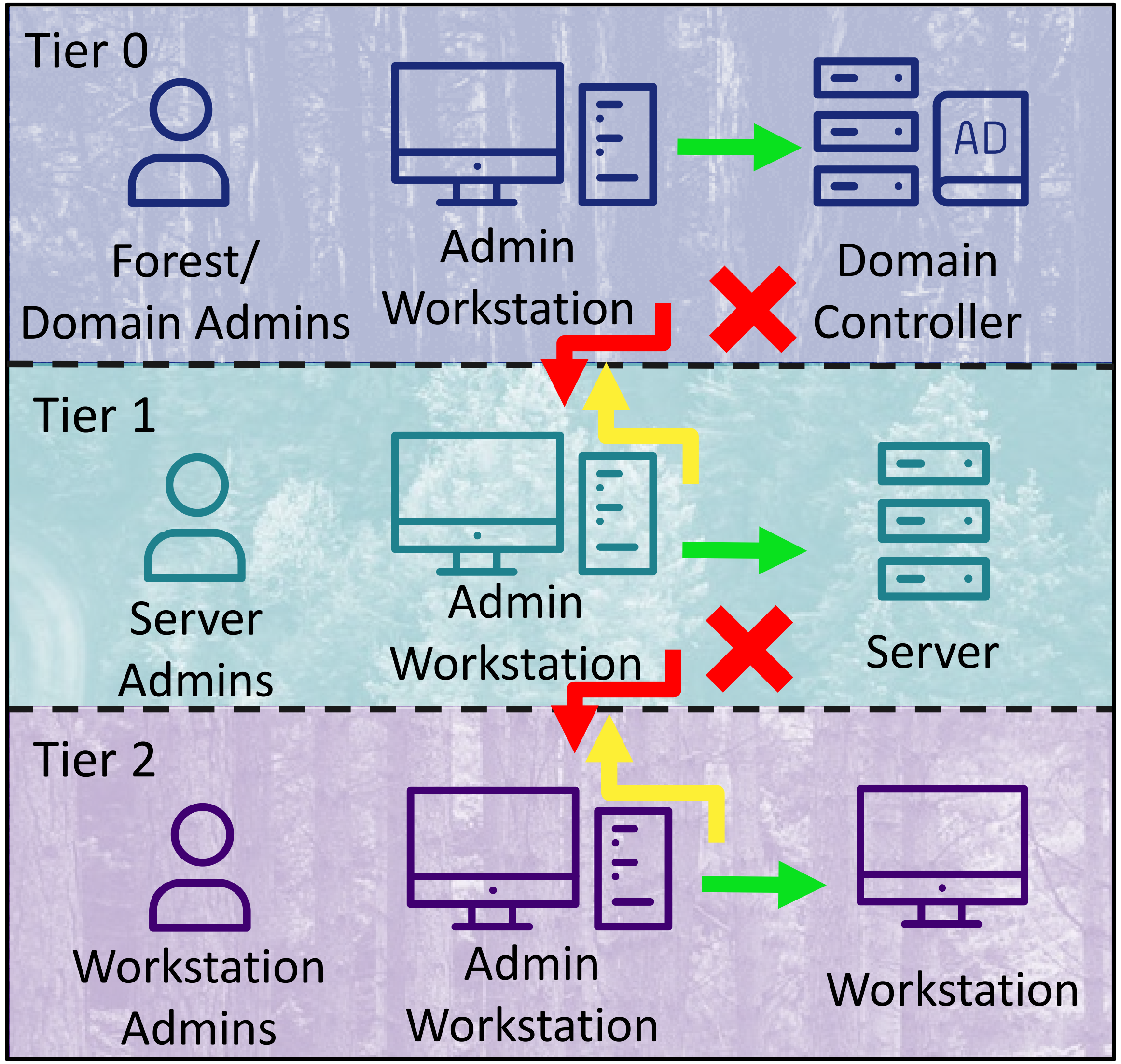
Dedicated administrative forests allow organizations to host administrative accounts, workstations, and groups in an environment that has stronger security controls than the production environment.

This architecture enables a number of security controls that aren't possible or easily configured in a single forest architect managed with Privileged Access Workstations (PAWs). T allows the provisioning of accounts as standard non-pr

What’s a “Red Forest”?

- Enhanced Security Administrative Environment (ESAE, aka “Red Forest”)
- AD architecture by Microsoft to maximize resiliency
- Architecture based on:
  1. Separation of systems by risk
  2. Restriction of highest risk accounts to highest risk systems

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material



Resilient AD Architecture

1. Secure Local Credentials
2. Isolate Administrative Systems
3. Create Administrative Forest *
4. Limit Administrative Permissions & Duration *
5. Adopt Tiered Architecture *

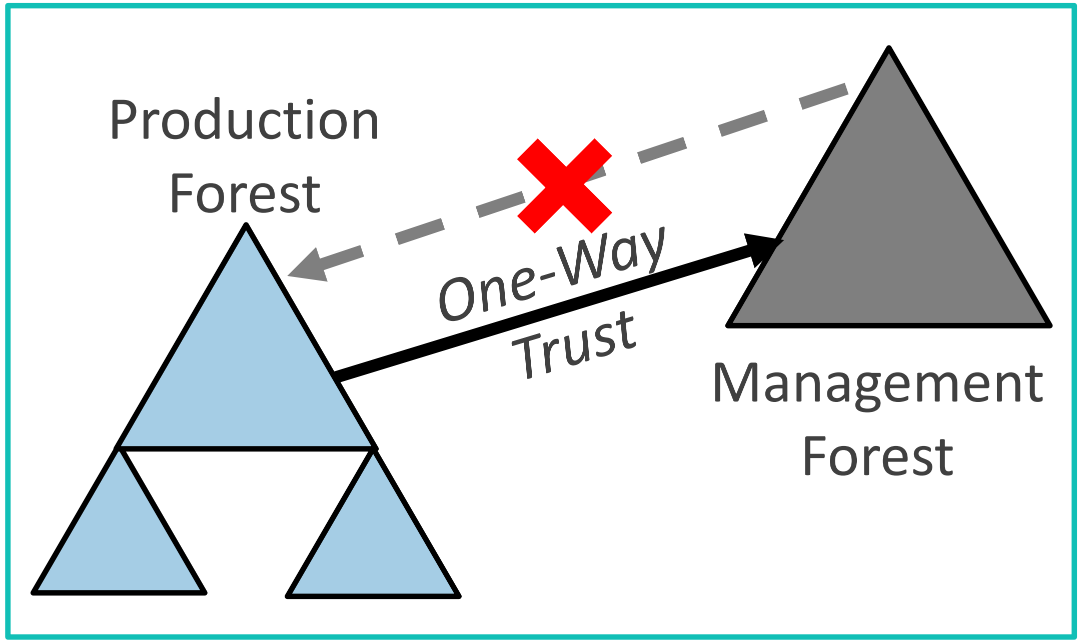
**Red Forest/ESAE Core Concepts*

Separate Administrative Forest

- Compromising users can lead to compromising DAs
- Compromise of domain = Compromise of forest

⬇

- Isolate administrative accounts in a separate forest

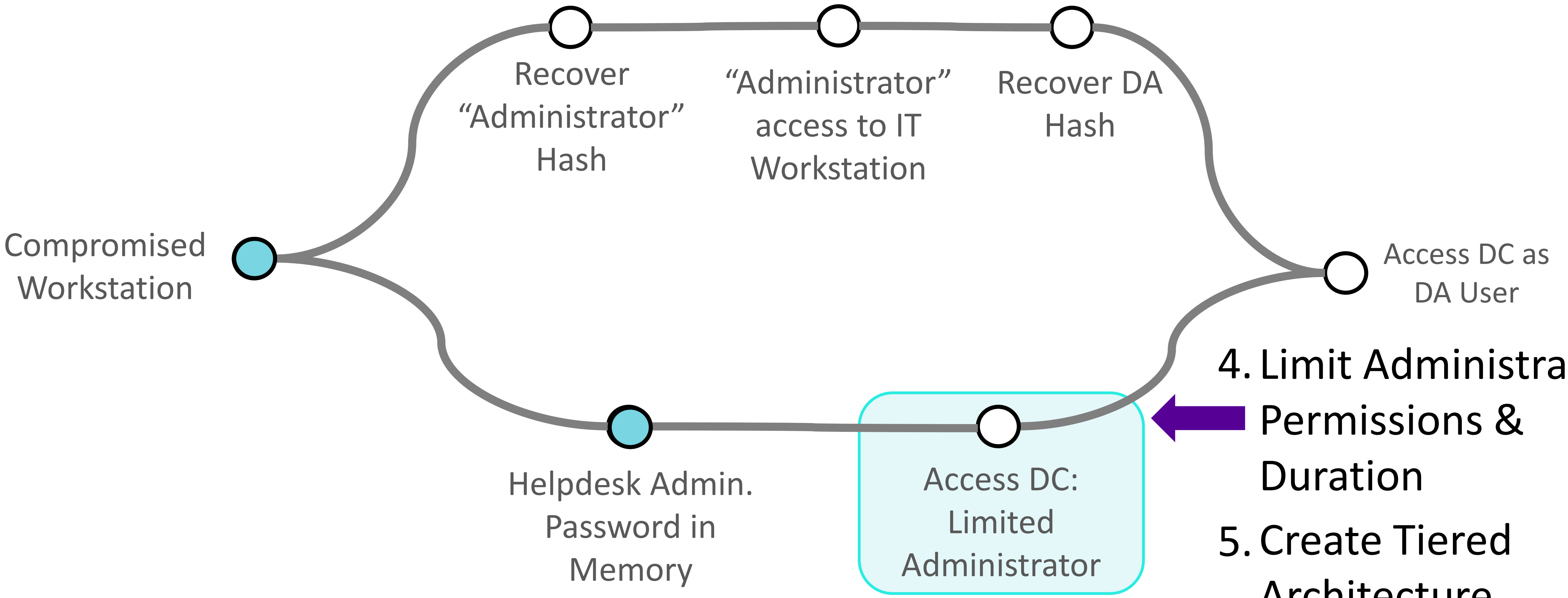


Microsoft's Privileged Access Management (PAM) tools isolate administrators in a separate forest

Suggestions

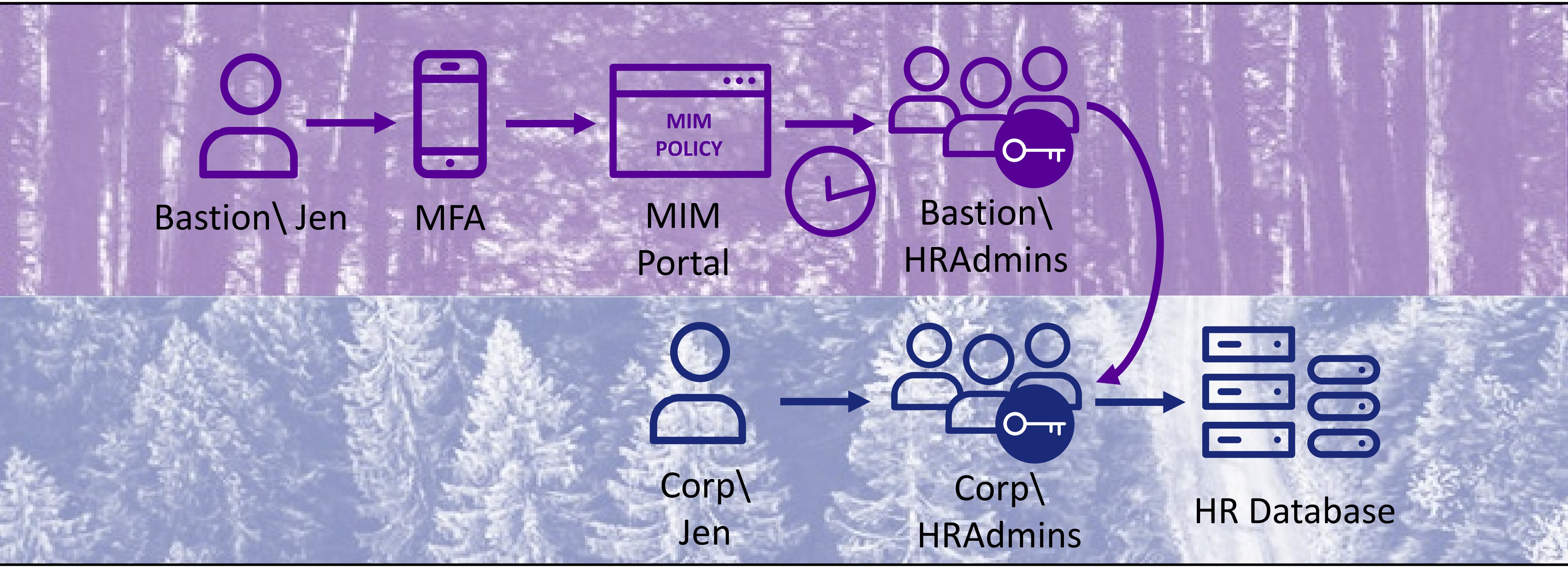
- Changes can be “reversed” by breaking production & management forest trust
- Make notes on tier separation as changes progress
- There will likely be a balance between cost, risk, and overhead:
  - e.g. Logging in multiple tiers

Permissions & Tiers


Compromised Workstation
Recover "Administrator" Hash
"Administrator" access to IT Workstation
Recover DA Hash
Access DC as DA User
Helpdesk Admin. Password in Memory
Access DC: Limited Administrator

4. Limit Administrative Permissions & Duration
5. Create Tiered Architecture

The Implementation:

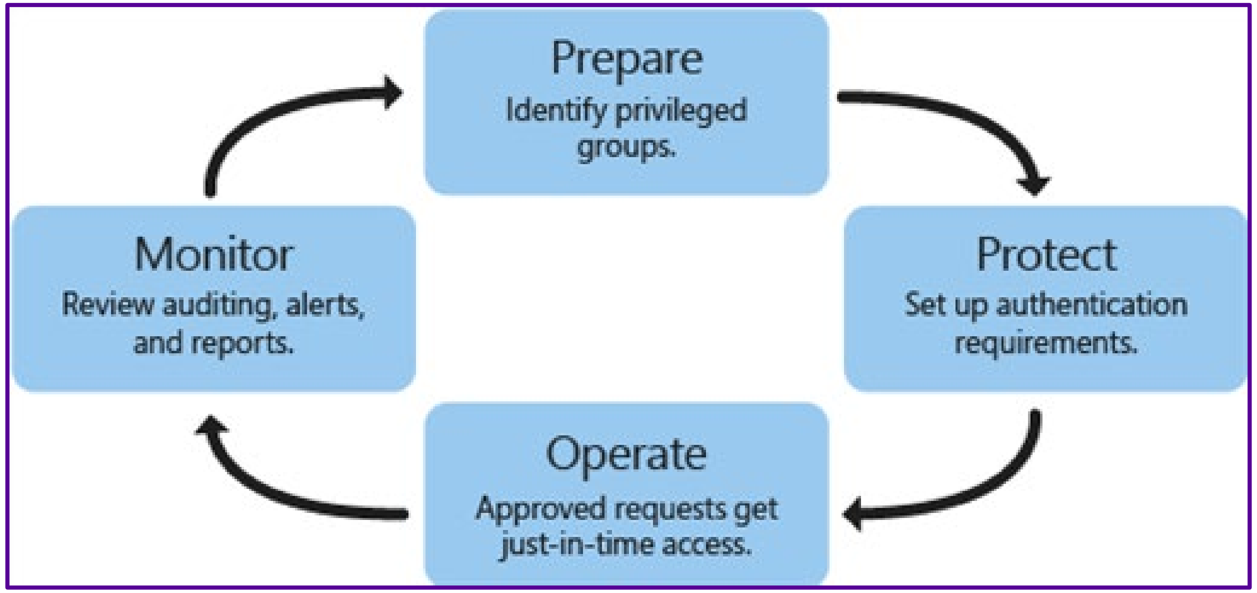


https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

Limit Administrative Availability

- Administrators frequently require (or request) Domain Admin for one-time tasks
- More Domain Admins create more paths to compromise

- Limit permissions, and only grant them for the time required



Prepare
Identify privileged groups.

Protect
Set up authentication requirements.

Operate
Approved requests get just-in-time access.

Monitor
Review auditing, alerts, and reports.

Microsoft's Just Enough Administration (JEA) & Just in Time (JIT) tools limit permissions and availability

Suggestions

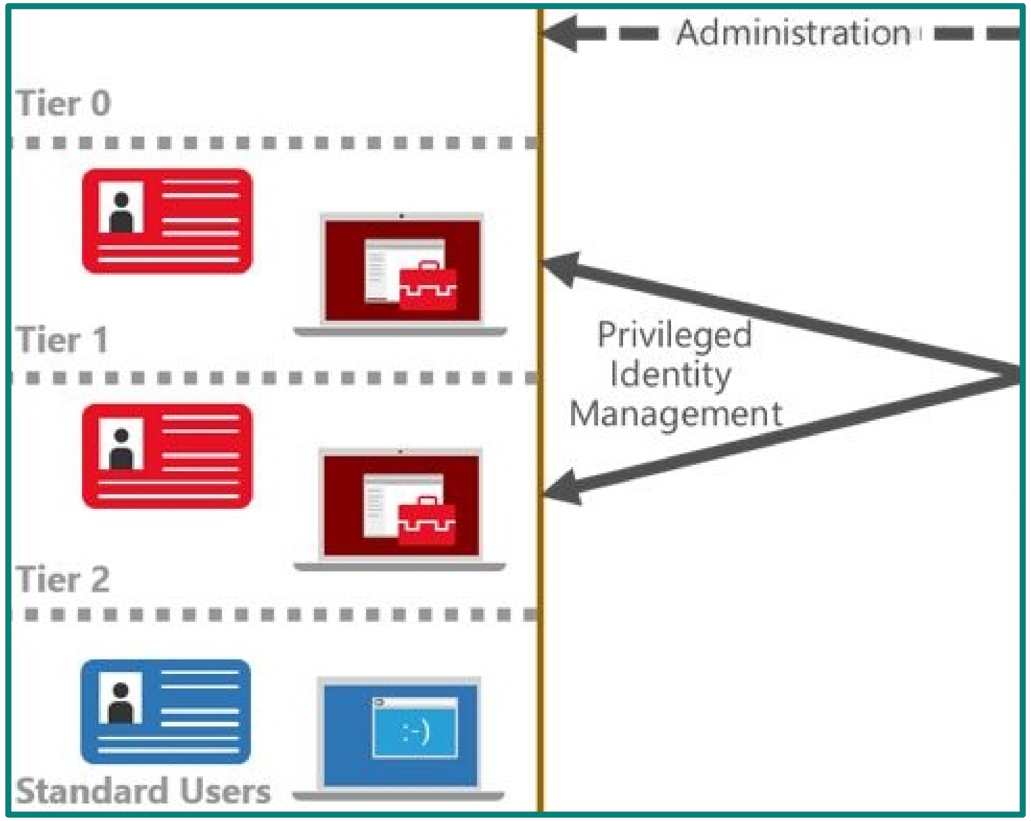
- Once authenticated, a session will maintain its privileges
  - Set session timeout on critical systems
- JEA does not require MIM
  - Consider testing JEA before administrative tiers if MIM is not on the roadmap

Reduce Breach Impact

- Different devices have different risk levels & needs, e.g.:
  - User workstation needs external web access
  - Domain Controller does not

↓

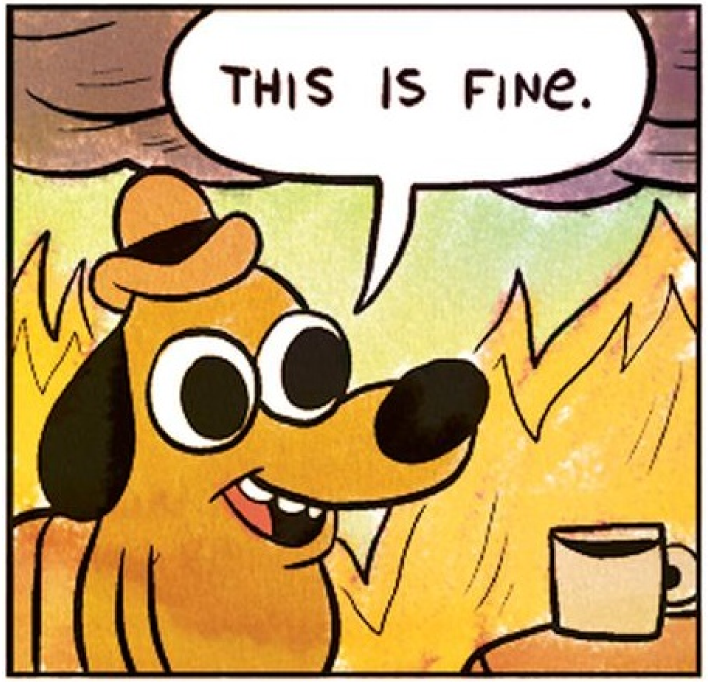
- Separate devices into "Tiers" based on risk & needs



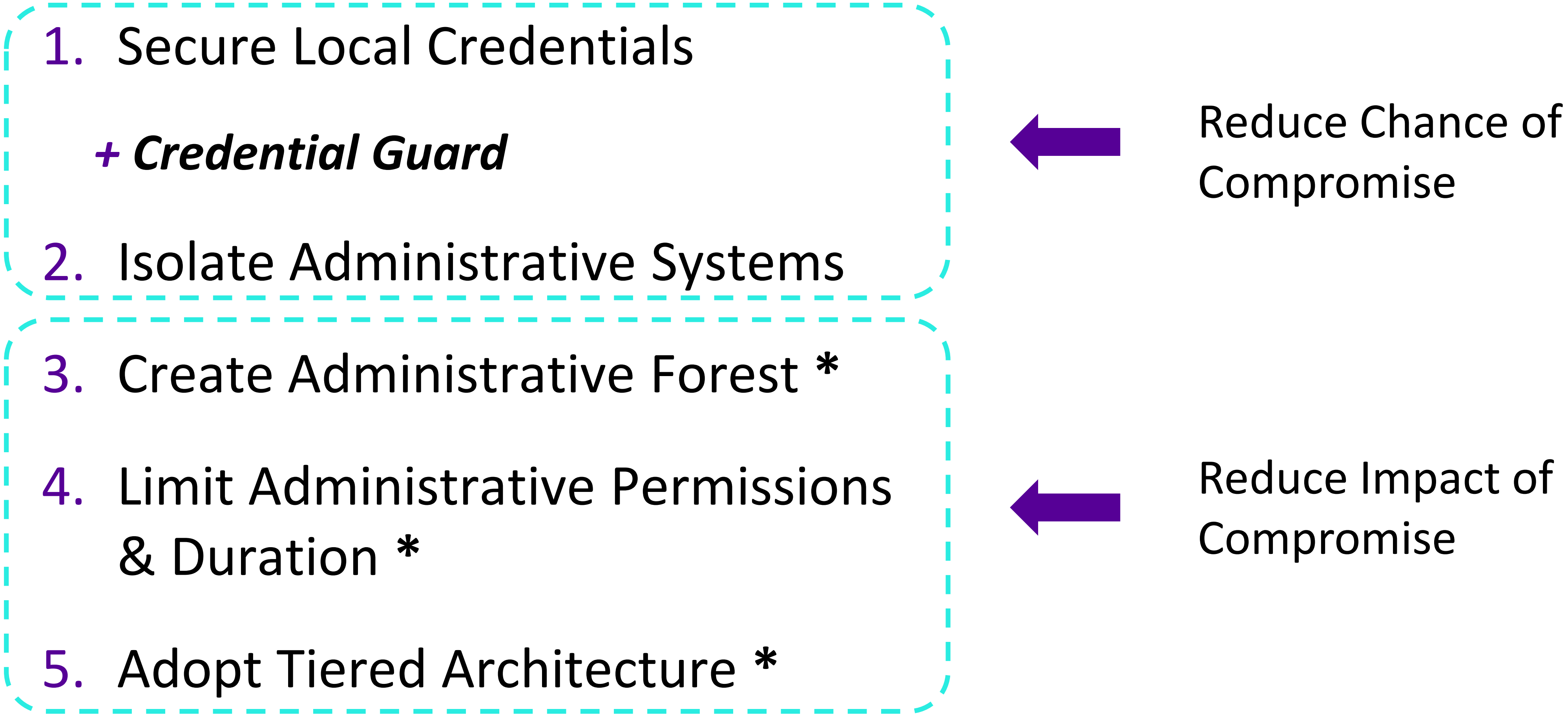
Microsoft's "Red Forest" separates devices by tier, with suggested devices and hardening requirements for Tier 0 systems

Suggestions

- Microsoft recommends 3 tiers:
  - Tier 0: Domain Controllers
  - Tier 1: Servers & sensitive applications
  - Tier 2: User systems, workstations, etc.
- Consider whether this works for the environment that will be changed
- Be realistic about what can and cannot be duplicated within tiers



As A Process:



1. Secure Local Credentials

   + *Credential Guard*

2. Isolate Administrative Systems

Reduce Chance of Compromise

3. Create Administrative Forest *

4. Limit Administrative Permissions & Duration *

5. Adopt Tiered Architecture *

Reduce Impact of Compromise

******Red Forest/ESAE Core Concepts*

Software Compatibility

Feature	Description	Domain Level	OS
Credential Guard	Protect credentials in memory from attackers with administrative access.	N/A	Server 2016 / Windows 10
LAPS	Configure unique passwords for local “Administrator” account on each system.	2003 SP1	Server 2003 SP2 / Vista
JEA	Powershell tools to limit permissions a user can request, and for how long requested permissions are granted.	N/A	Server 2012 / Windows 8
MIM	Allows simple creation of a separate management forest.	2003*	N/A
PAM	Contains JIT functionality. Implemented using MIM.	N/A	Server 2012 R2 / Windows 8
ESAE	Separation of devices into tiers. Management via MIM, PAM, JEA, & JIT.	See above.	See above.

** Forest created for management must be 2012+*

Takeaways

- Securing Active Directory is critical to avoiding large-scale incidents
- Microsoft's "Red Forest" prevents the major methods attackers use against AD
- Each step towards Red Forest significantly improves AD security *

** Even if full Red Forest is not currently feasible*

SUPPORTED BY THE DEPARTMENT OF WATER AFFAIRS & FORESTRY. FOR MORE INFORMATION CALL 0800 200 200
DON'T START FIRES YOU CAN'T STOP.
BE FIREWISE.
FIREWISE
WILDFIRE
MOVES
QUICKER
THAN YOU
THI

Get Started:

- Quick Wins *(1-3 months)*
  - Implement Local Administrative Password Solution (LAPS)
  - Configure Credential Guard on applicable systems
- Feasibility Assessment *(2-5 months, "Proof of Concept")*
  - Test hardened administrative workstations (PAWs)
  - Create an isolated administrative forest to test common tasks
- Decisions *(3-6 months)*
  - Determine if "Red Forest" implementation makes sense based on:
    - Proof of Concept findings
    - Business priorities

RSAConference2019

Questions?

Or reach out any time:

✉ katie.knowles@mwrinfosecurity.com

@_sigil

Article:
www.mwrinfosecurity.com/our-thinking/planting-the-red-forest-improving-ad-on-the-road-to-esae/