



Gold partner:



Generální partner:



Pass-the-Hash Attacks

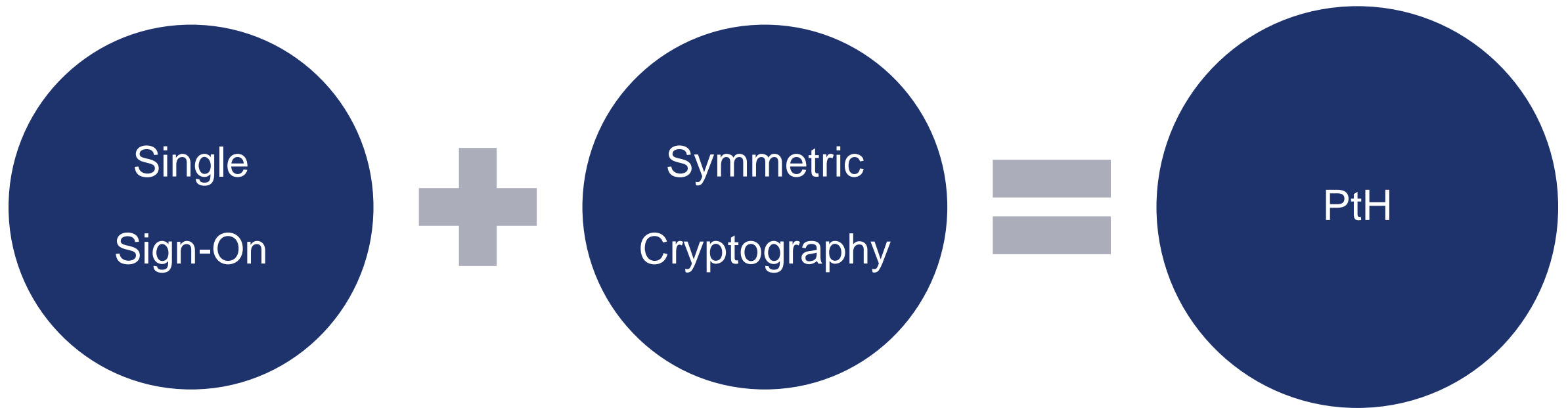
Michael Grafnetter
www.dsinternals.com

18. – 21. května 2015
Tech·Ed
DevCon 

Agenda

- PtH Attack Anatomy
- Mitigation
 - Proactive
 - Reactive
- Windows 10

PtH Attack Premises



PtH Attack Anatomy



Theft

Use

Compromise



GOPAS

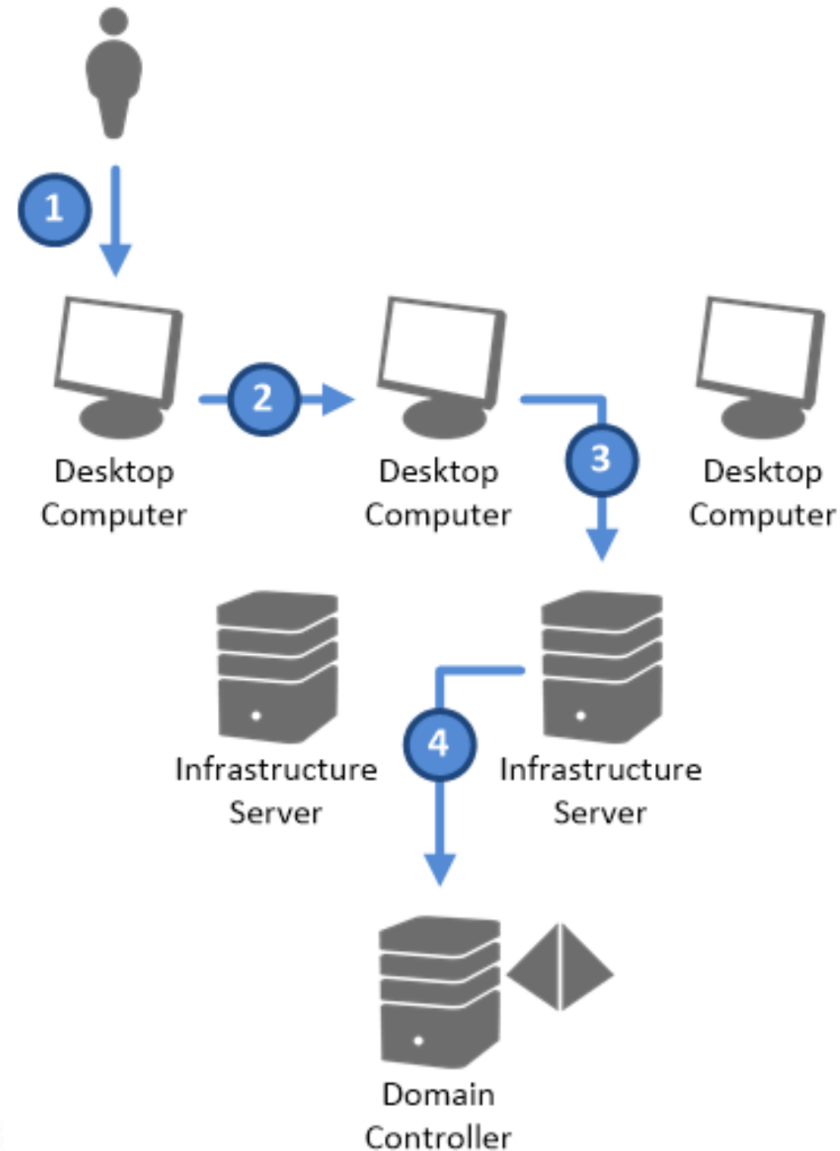


DAQUAS



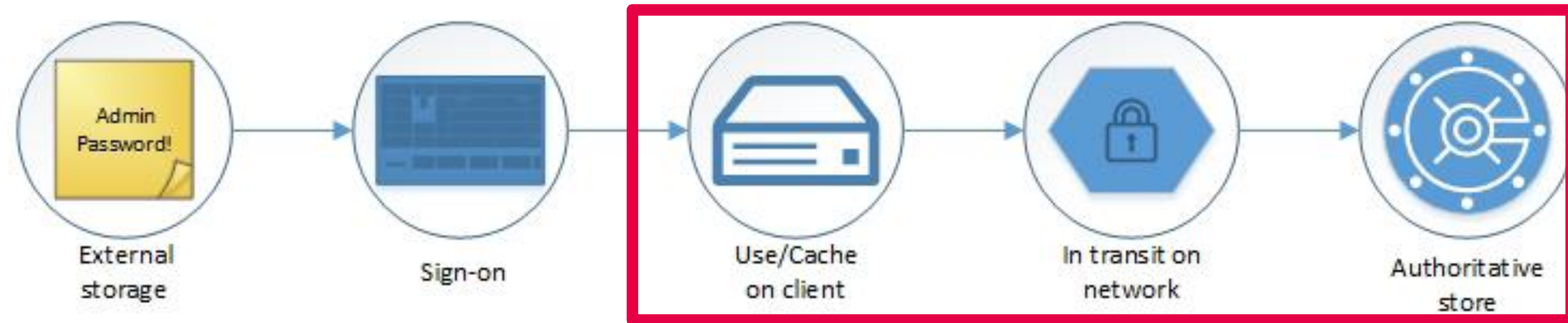
Microsoft

PtH Attack Anatomy



Stealing the Hash

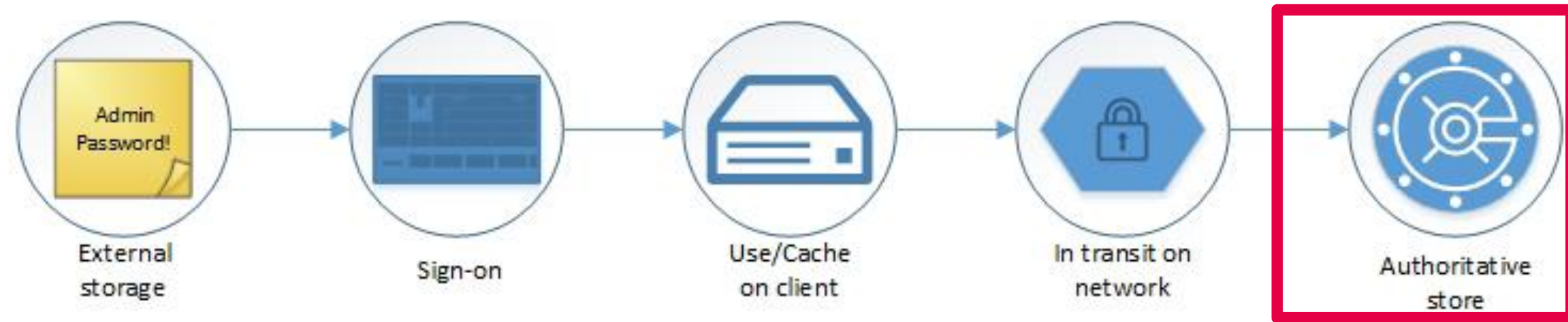
Credentials Lifecycle / Attack Vectors



Hashes in Windows

Authentication Method	Hash Function	Salted
LM	DES	NO
NTLM, NTLMv2	MD4	NO
Kerberos (RC4)	MD4	NO
Kerberos (AES)	PBKDF2	YES
Digest	MD5	YES

Credentials Lifecycle / Attack Vectors



Active Directory Database - Offline

- Files

- C:\Windows\NTDS\ntds.dit
- C:\Windows\System32\config\SYSTEM

- Acquire

- Locally – ntdsutil IFM
- Remotely – WMI (Win32_Process), psexec
- VHDs, VMDKs, Backups

- Extract

- libesedb+ntdsxtract
- Windows Password Recovery

NTDSXtract

```
esedbexport ntds.dit
```

```
python dsusers.py ntds.dit.export/datatable.4  
--name Administrator --syshive SYSTEM  
-- supplcreds --passwordhashes
```

Password hashes:

Administrator:\$NT\$cc36cf7a8514893efccd332446158b1a:::

Supplemental credentials:

Kerberos newer keys

salt: ADATUM.COMAdministrator

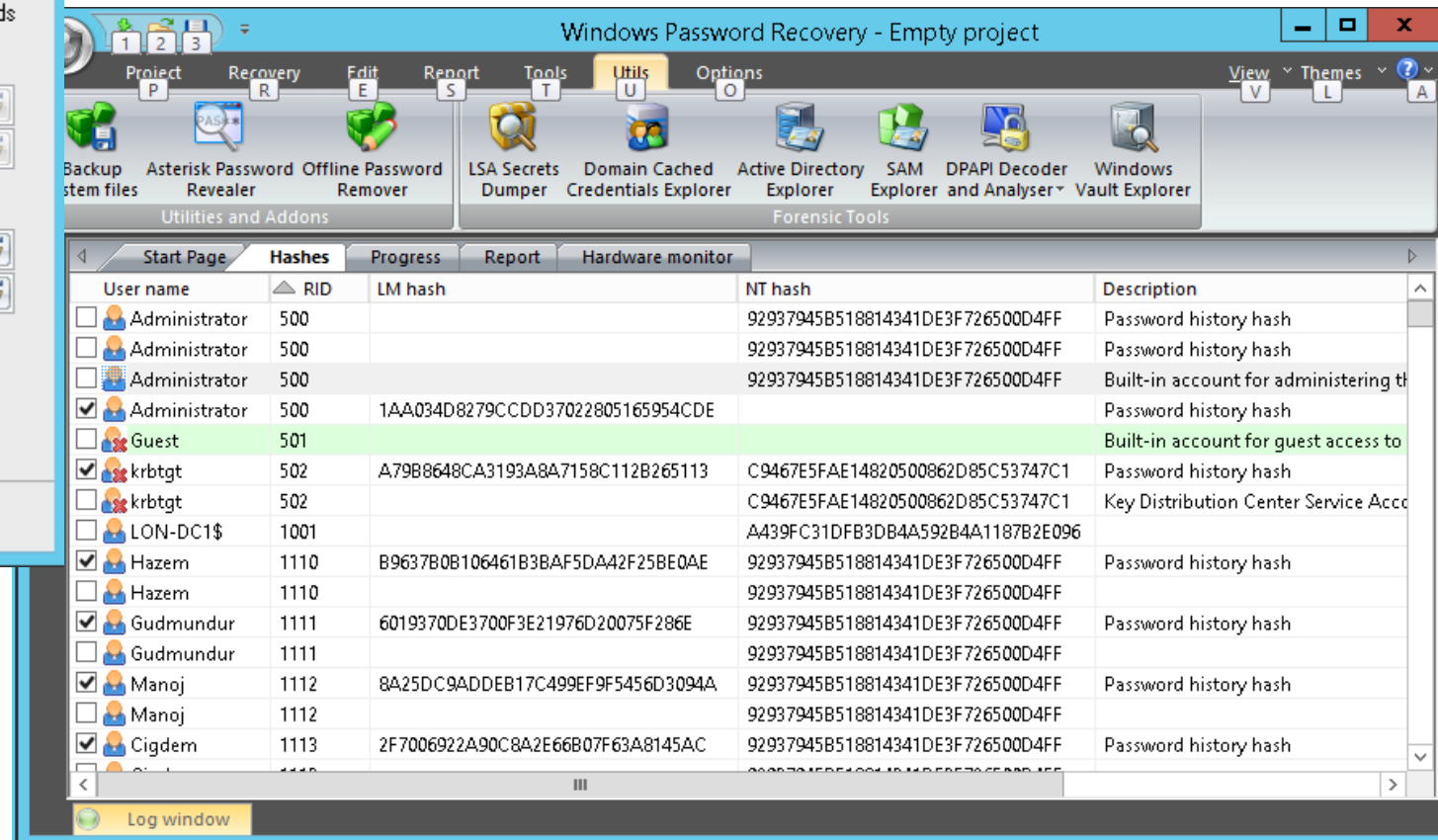
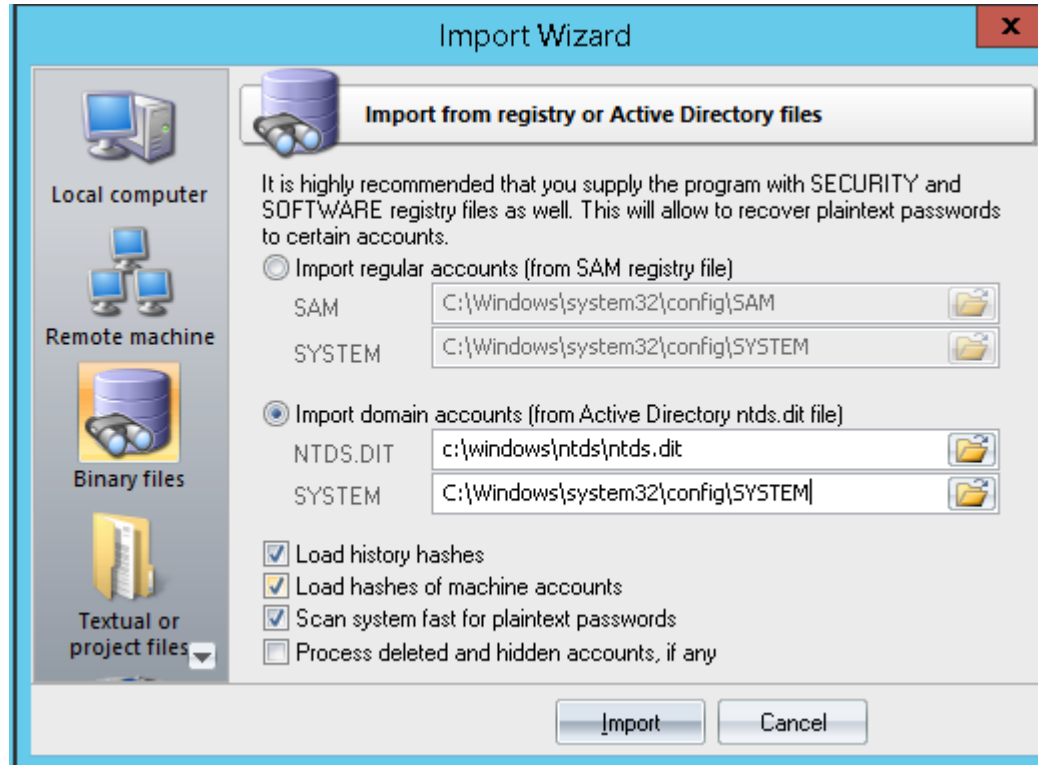
Credentials

18 b7268361386090314acce8d9367e55f55865e7ef8e670fbe4262d6c94098a9e9

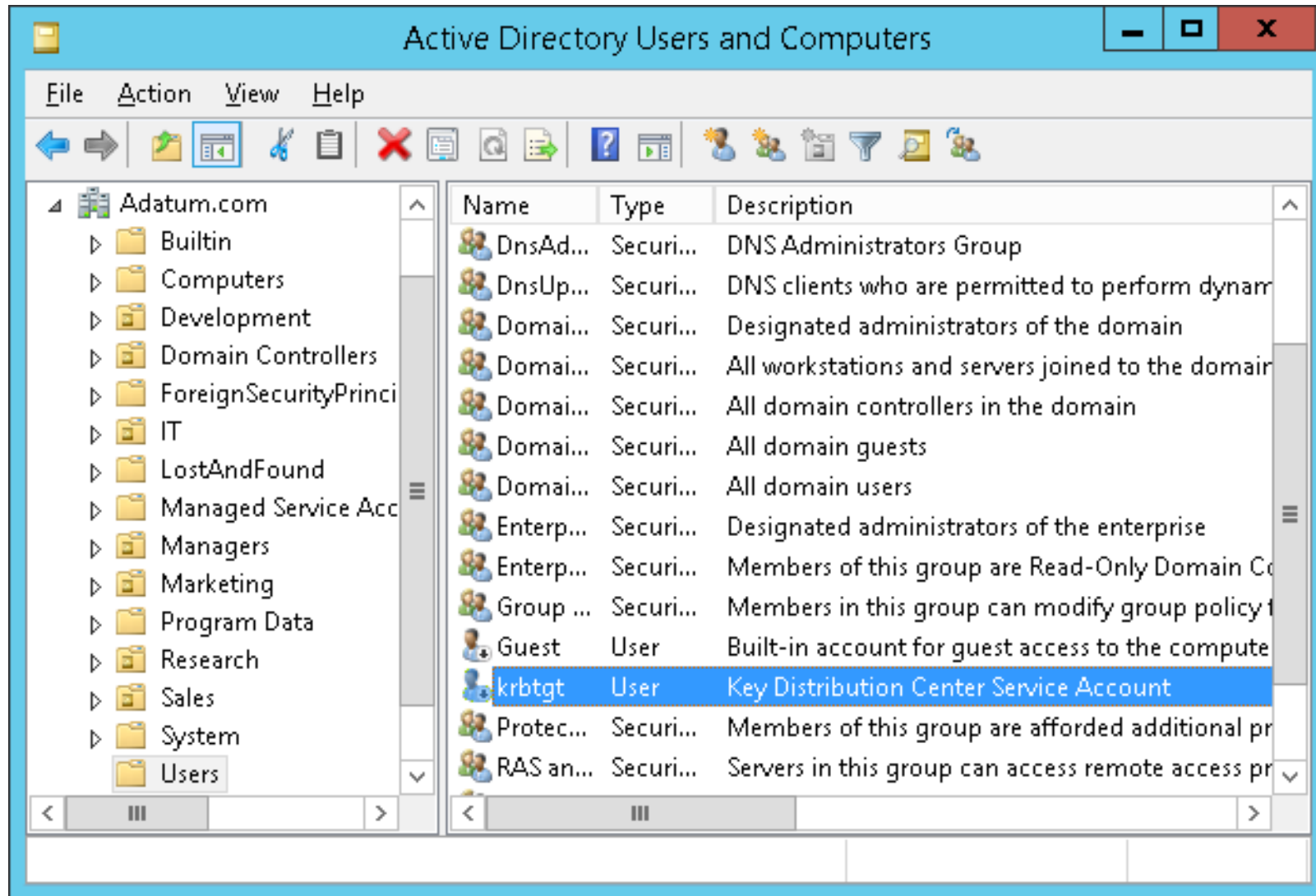
17 8451bb37aa6d7ce3d2a5c2d24d317af3

3 f8fd987fa7153185

Windows Password Recovery - AD



KRBTGT Account



DEMO

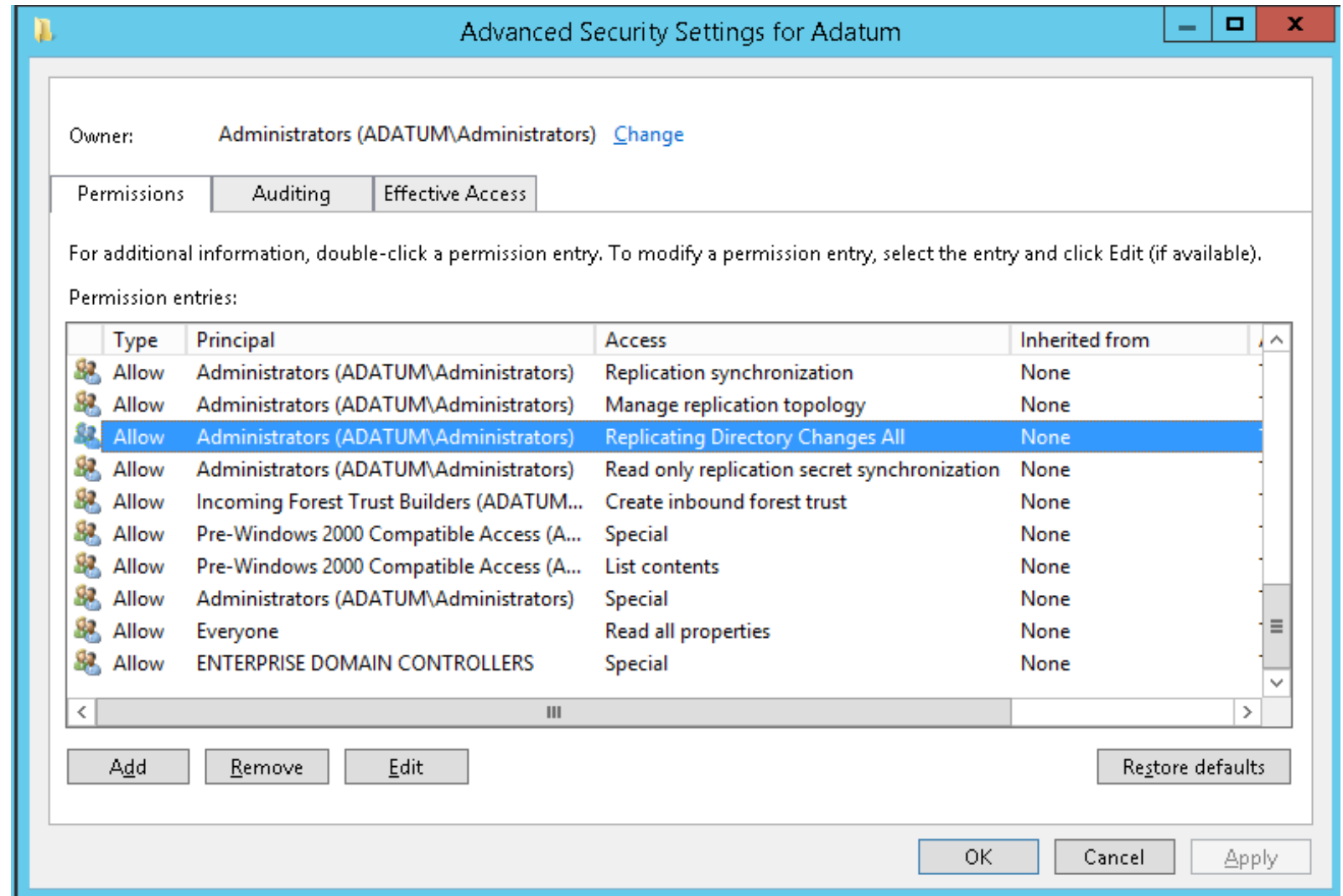
IFM + Windows Password Recovery

Proactive Measures

- Encryption
- RODC
- Backup protection
- Regular password changes

Active Directory Database - Online

- MS-DRSR/RPC



Proactive Measures

- Avoid using administrative accounts
- Do not run untrusted SW

SAM Database

- Offline
 - Files
 - C:\Windows\System32\config\SAM
 - C:\Windows\System32\config\SYSTEM
 - Tools
 - Windows Password Recovery
- Online
 - Mimikatz

DEMO

SAM dump using Mimikatz

Proactive Measures

- Restrict administrative access
- Bitlocker
- Randomize local Administrator passwords

GP Local Admin Pwd Management Solution

The screenshot shows the 'Password Settings' window. At the top, there are 'Previous Setting' and 'Next Setting' buttons. Below these, there are three radio buttons: 'Not Configured', 'Enabled' (which is selected), and 'Disabled'. To the right of these is a 'Comment:' text box. Below the radio buttons is a 'Supported on:' section with the text 'At least Microsoft Windows XP Professional or Windows Server 2003 family'. Under the 'Options:' heading, there are three settings: 'Password Complexity' (a dropdown menu set to 'Large letters + small letters + numbers + specials'), 'Password Length' (a numeric spinner set to 12), and 'Password Age (Days)' (a numeric spinner set to 30). To the right of these settings is a 'Help:' section containing three paragraphs of explanatory text.

Password Settings

Previous Setting Next Setting

☐ Not Configured ☒ Enabled ☐ Disabled

Comment:

Supported on: At least Microsoft Windows XP Professional or Windows Server 2003 family

Options:

Help:

Password Complexity

Large letters + small letters + numbers + specials

Password Length 12

Password Age (Days) 30

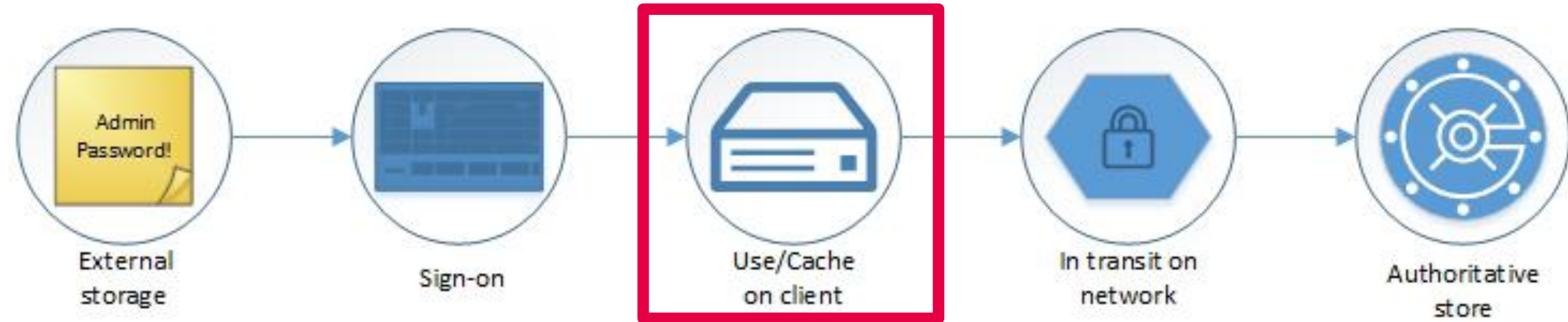
Configures AdmPwd password parameters

Password complexity: which characters are used when generating a new password
Default: Large letters + small letters + numbers + special characters

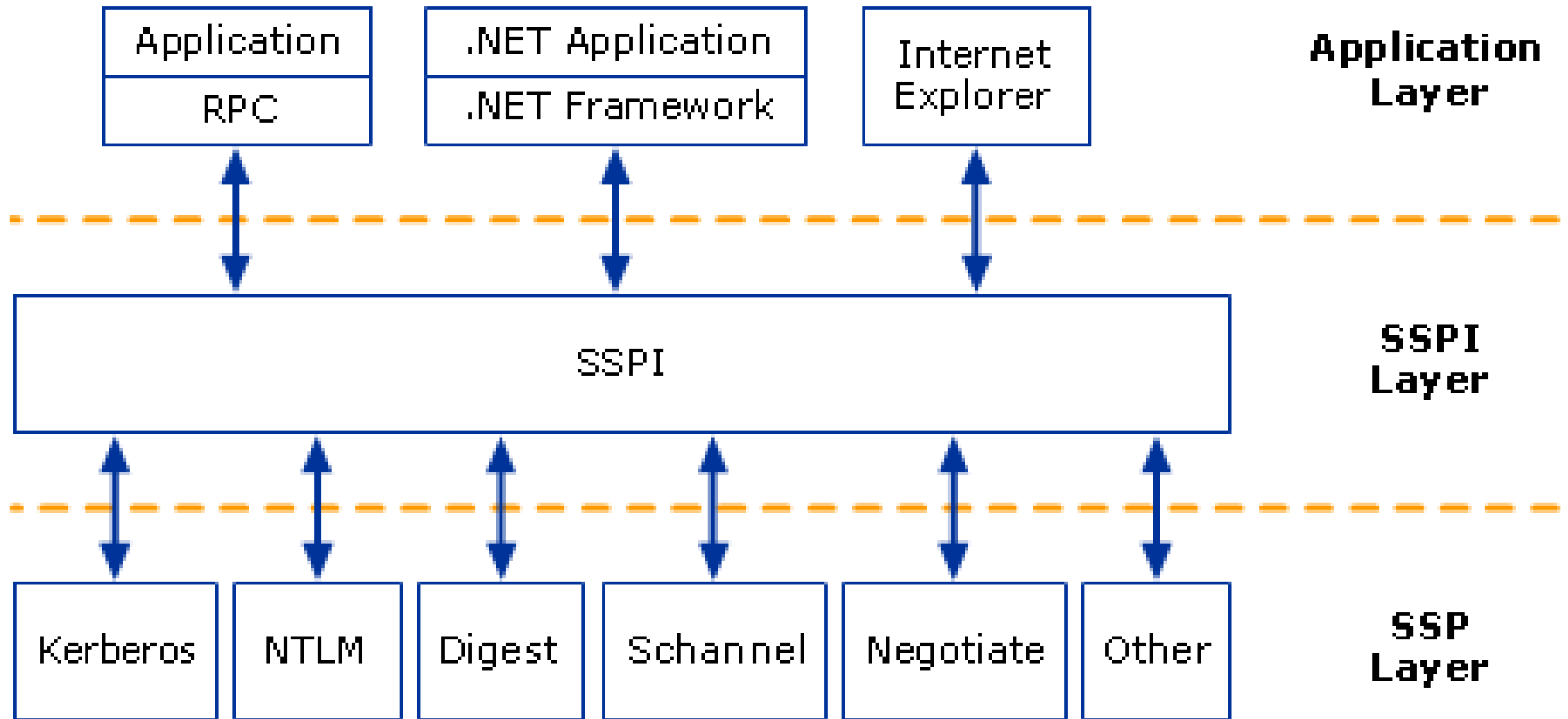
Password length
Minimum: 12 characters
Maximum: 64 characters
Default: 12 characters

Password age in days
Minimum: 1 day
Maximum: 365 days
Default: 30 days

Credentials Lifecycle / Attack Vectors



Windows Integrated Authentication





SSP Cached Creds (SSO)

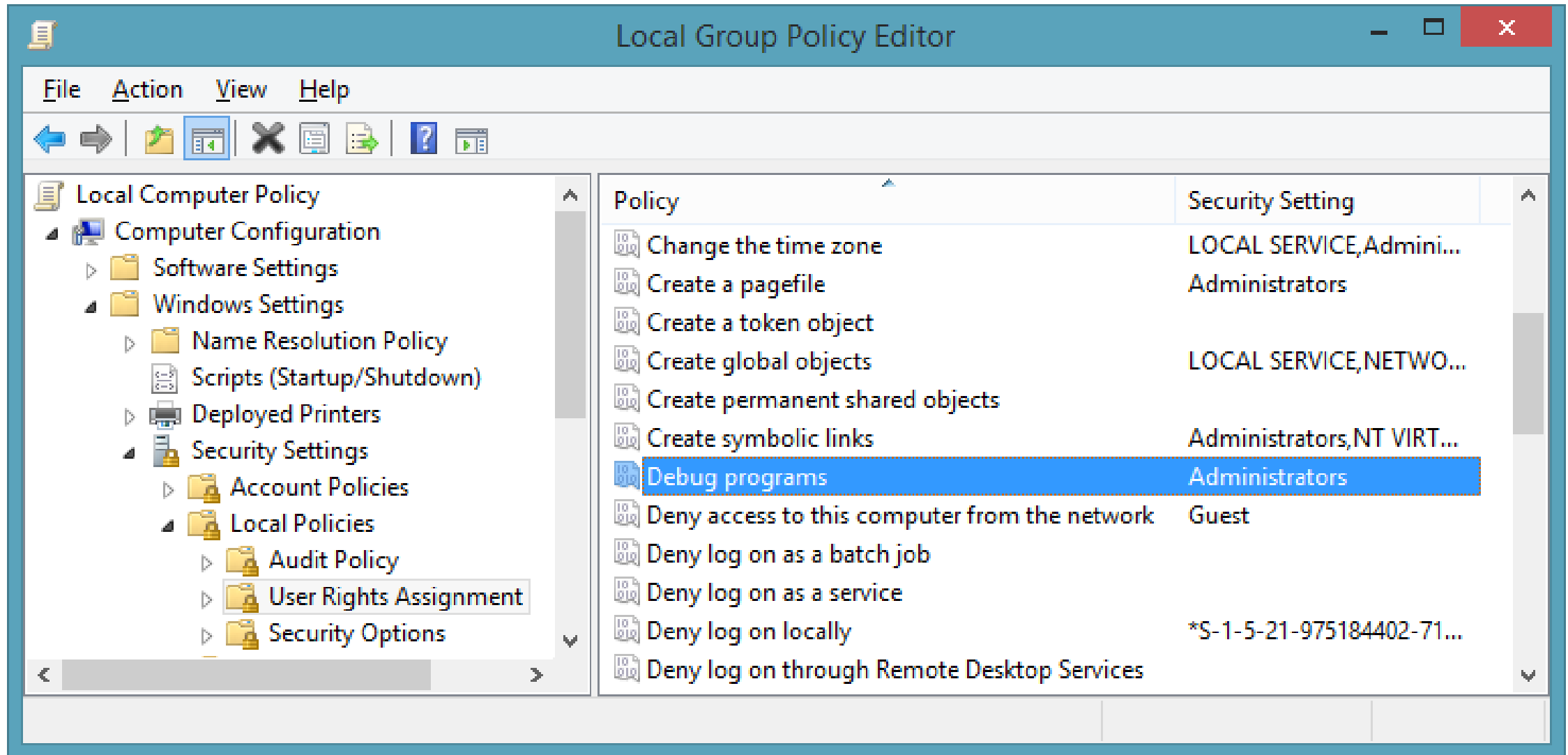
		Kerb	Hashes		Plaintext-Equivalent Passwords				
		TGT	LM	NT	Tspkg	Wdigest	Kerb	LiveSSP	3rd Party SSP
Windows 8.0 and previous	Microsoft Account								
	Local Account								
	Domain Account								
					*	*			
Windows 8.1 Defaults	Microsoft Account				*	*			
	Local Account				*	*			
	Domain Account								
Windows 8.1 Features	Protected Users								
	Restricted Admin RDP								

* Off by Default

Based on a table by Benjamin Delpy
twitter.com/gentilkiwi/status/352557093640892416/photo/1

 No Password Data in Memory
 Password Data in Memory

Debug Privilege



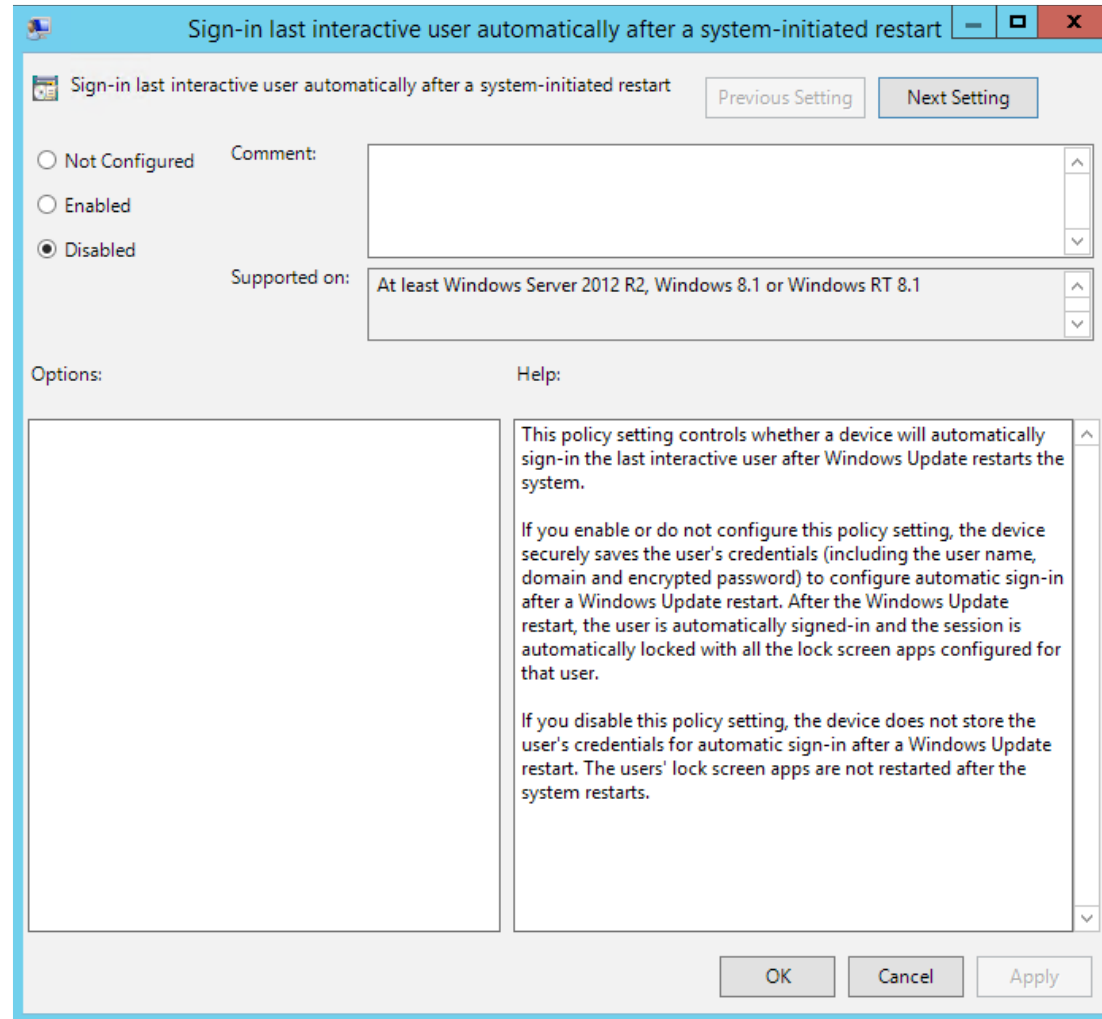
DEMO

LSA dump using Mimikatz

Proactive Measures

- Restrict administrative access
- Applocker/SRP whitelisting
- Enable Additional LSA Protection
- Protected Users group
- Restricted Admin RDP
- Authentication Policies and Silos
- Shorten Kerberos ticket lifetime
- Disable Automatic Restart Sign-On

Automatic Restart Sign-On



The screenshot shows a Windows Group Policy Editor window titled "Sign-in last interactive user automatically after a system-initiated restart". The window has a blue title bar with standard Windows window controls. Below the title bar, there's a header area with the policy name and two buttons: "Previous Setting" and "Next Setting".

The main content area is divided into two columns. The left column contains three radio buttons: "Not Configured", "Enabled", and "Disabled". The "Disabled" option is selected. To the right of these radio buttons is a "Comment:" text box. Below the radio buttons is a "Supported on:" section with a text box containing "At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1".

The right column is titled "Options:" and "Help:". The "Options:" section is currently empty. The "Help:" section contains a text box with the following text:

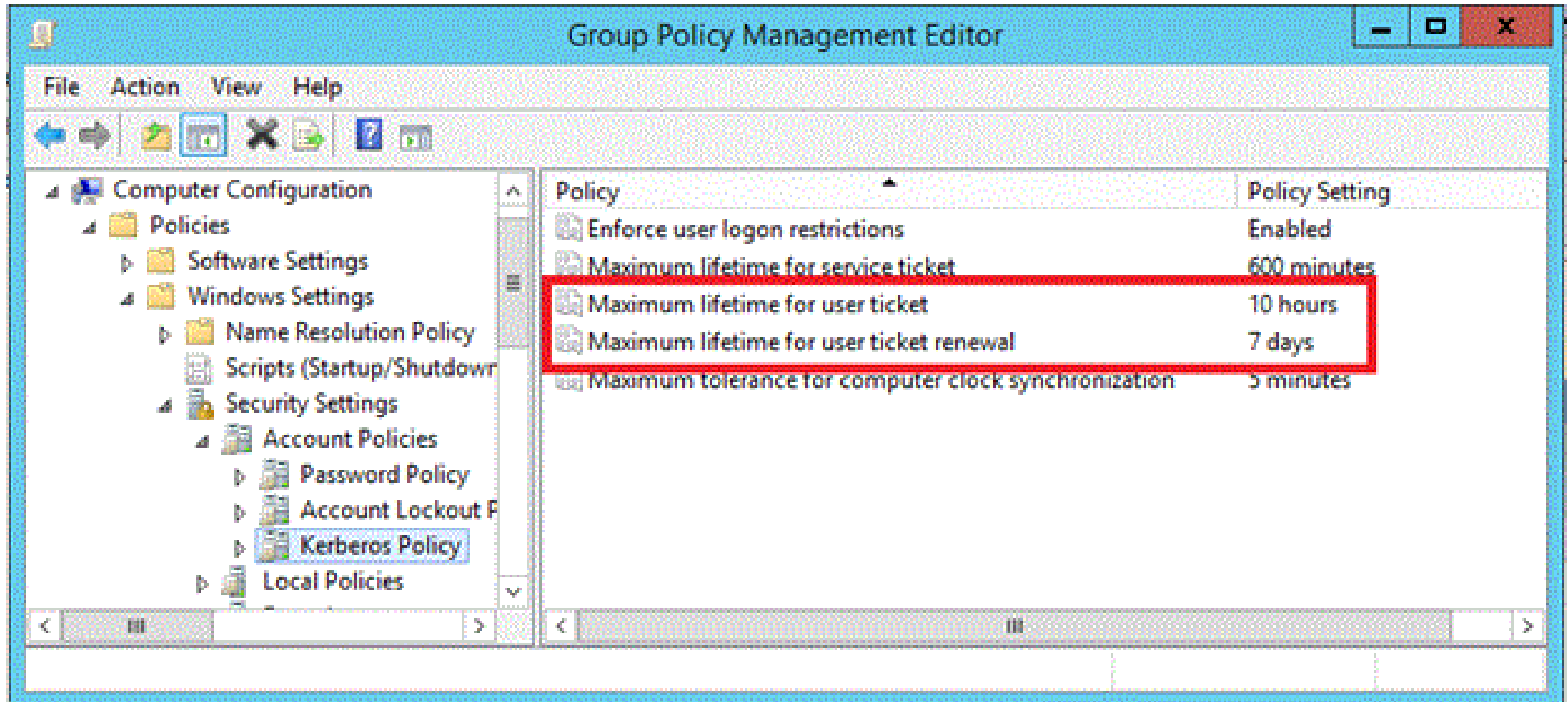
This policy setting controls whether a device will automatically sign-in the last interactive user after Windows Update restarts the system.

If you enable or do not configure this policy setting, the device securely saves the user's credentials (including the user name, domain and encrypted password) to configure automatic sign-in after a Windows Update restart. After the Windows Update restart, the user is automatically signed-in and the session is automatically locked with all the lock screen apps configured for that user.

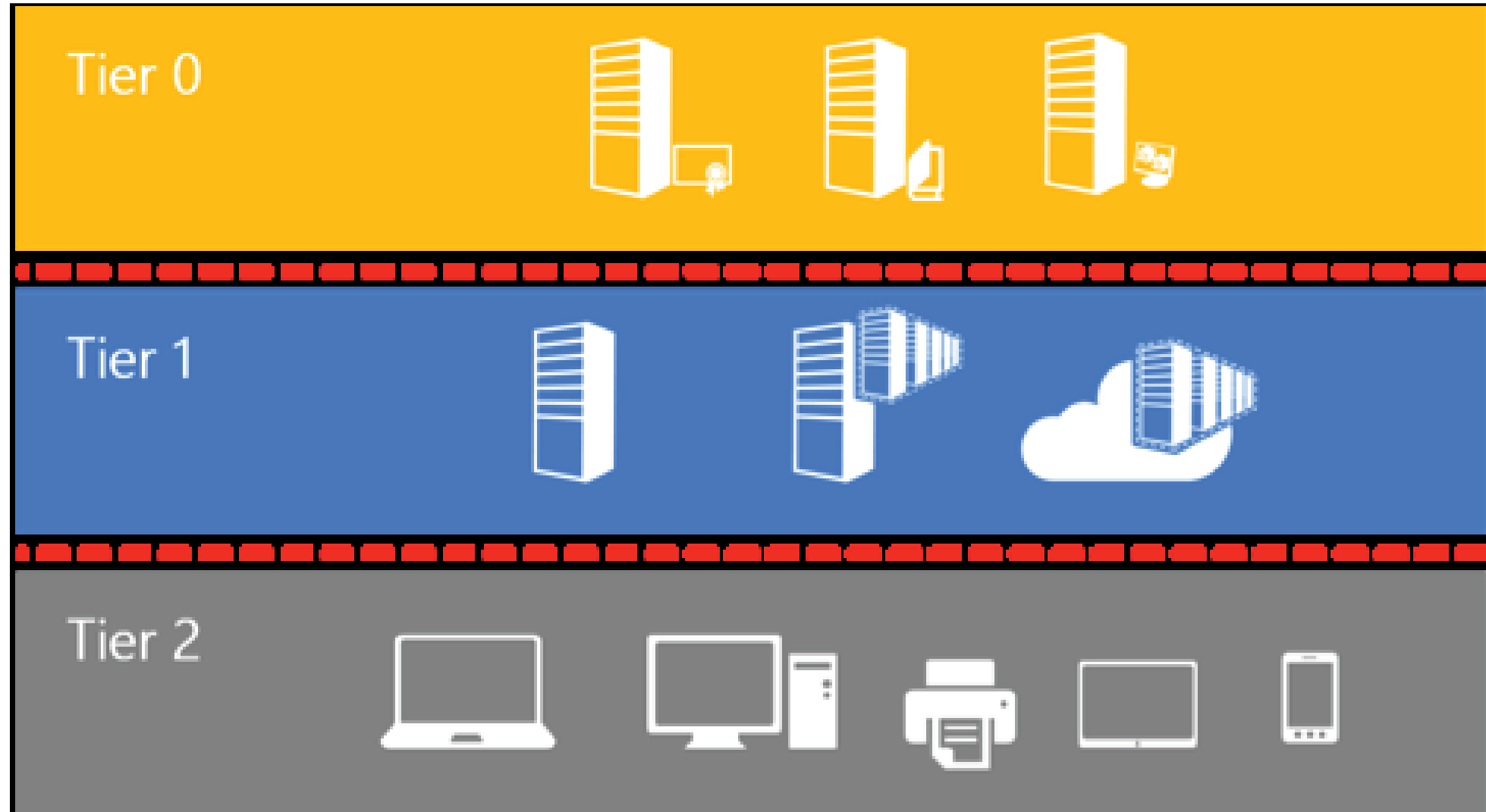
If you disable this policy setting, the device does not store the user's credentials for automatic sign-in after a Windows Update restart. The users' lock screen apps are not restarted after the system restarts.

At the bottom of the window are three buttons: "OK", "Cancel", and "Apply".

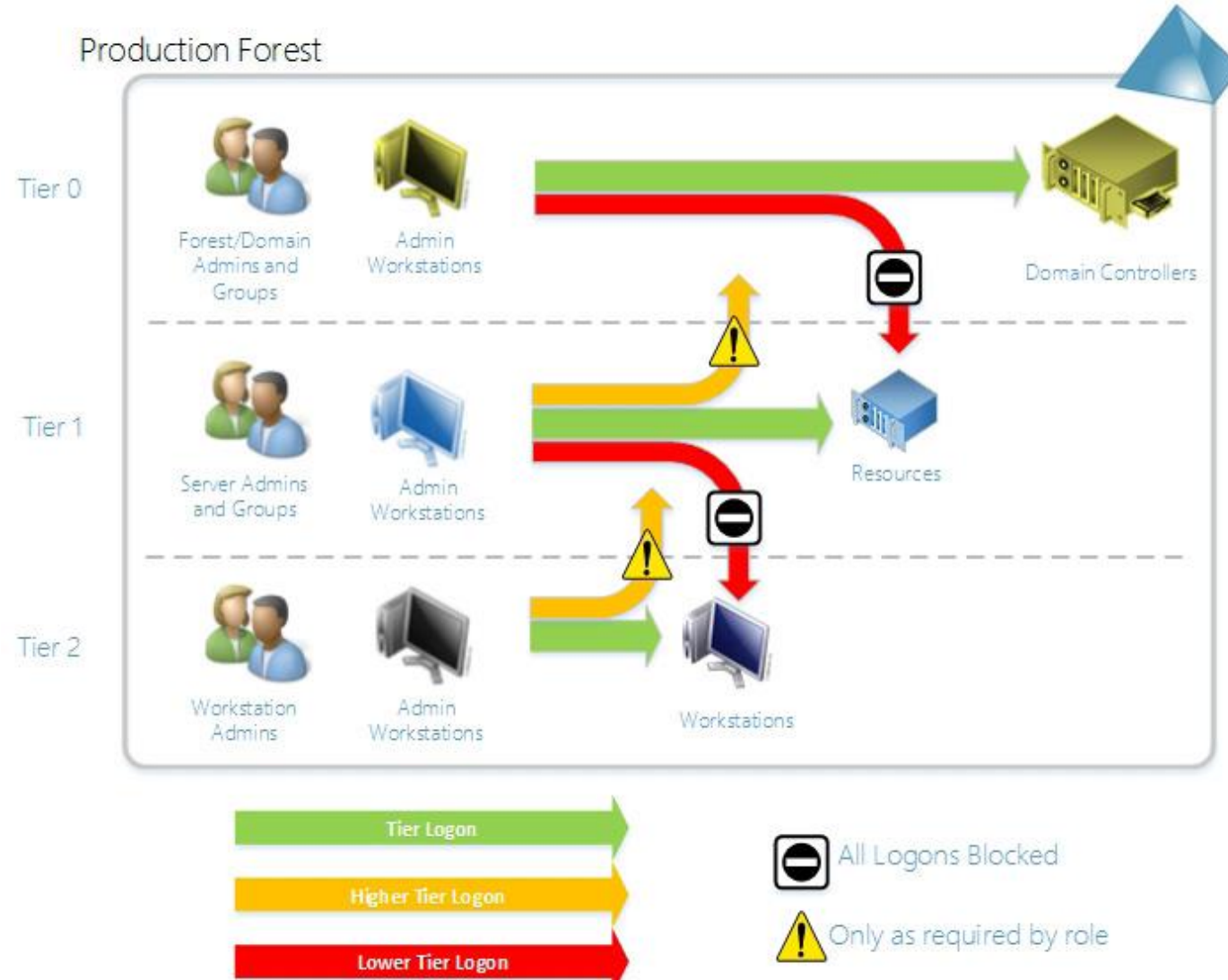
Kerberos Ticket Lifetime



Tier Model



Tier Model - Administrative logon restrictions



High-Value Accounts

- Admins
 - Domain Adminis
 - Enterprise Admin
 - Schema Adminis
 - BUILTIN\Administrators
 - BUILTIN\Hyper-V Administrators
- Service Accounts
 - SCCM, SCOM, DPM, Software Installation,...
- BMC Accounts

Authentication Policies and Silos

Restrict Access for Admins

TASKS

SECTIONS

General

Accounts

Policy

General

An authentication policy silo controls which accounts are to be protected by the silo and defines the authentication policies to be applied to members of the silo.

Display name: * Restrict Access for Admins

Description:

☐ Only audit silo policies

☒ Enforce silo policies

☒ Protect from accidental deletion

Permitted Accounts

Name	Account Type	Assigned
Admin04	Computer	
Administrator	User	
Hans Worst	User	
Jos Haarbos	User	

Add... Remove...

Authentication Policy

☒ Use a single policy for all principals that belong to this authentication policy silo.

More Information

OK

User

☒ Specify a Ticket Granting Ticket lifetime for user accounts.

Ticket Granting Ticket Lifetime (minutes): * 600

Specify access control conditions that restrict devices that can request a Ticket Granting Ticket for the user accounts assigned to this policy.

Note: NTLM authentication cannot be restricted by access control conditions. Users should be members of the Protected Users group, which does not allow NTLM.

Click Edit to define the conditions.

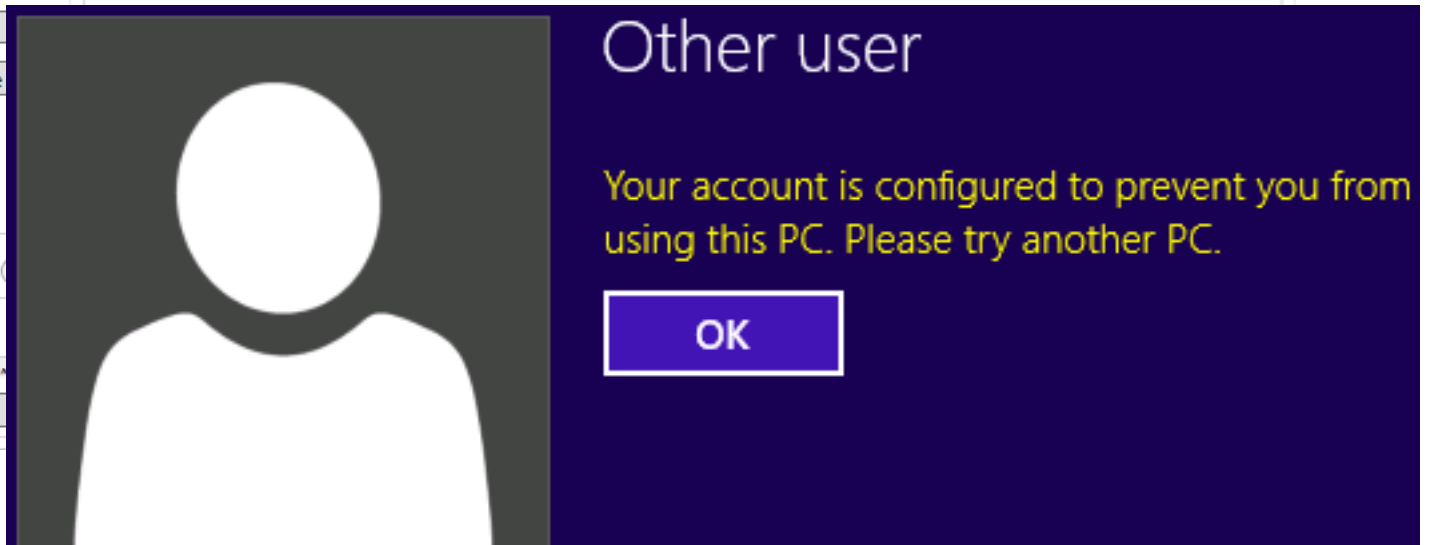
Member of any(((W8-CONTOSOW1\$-W81\W8_CONTOSOW1\$)))

Edit...

Click Edit to define the conditions.

All Resources

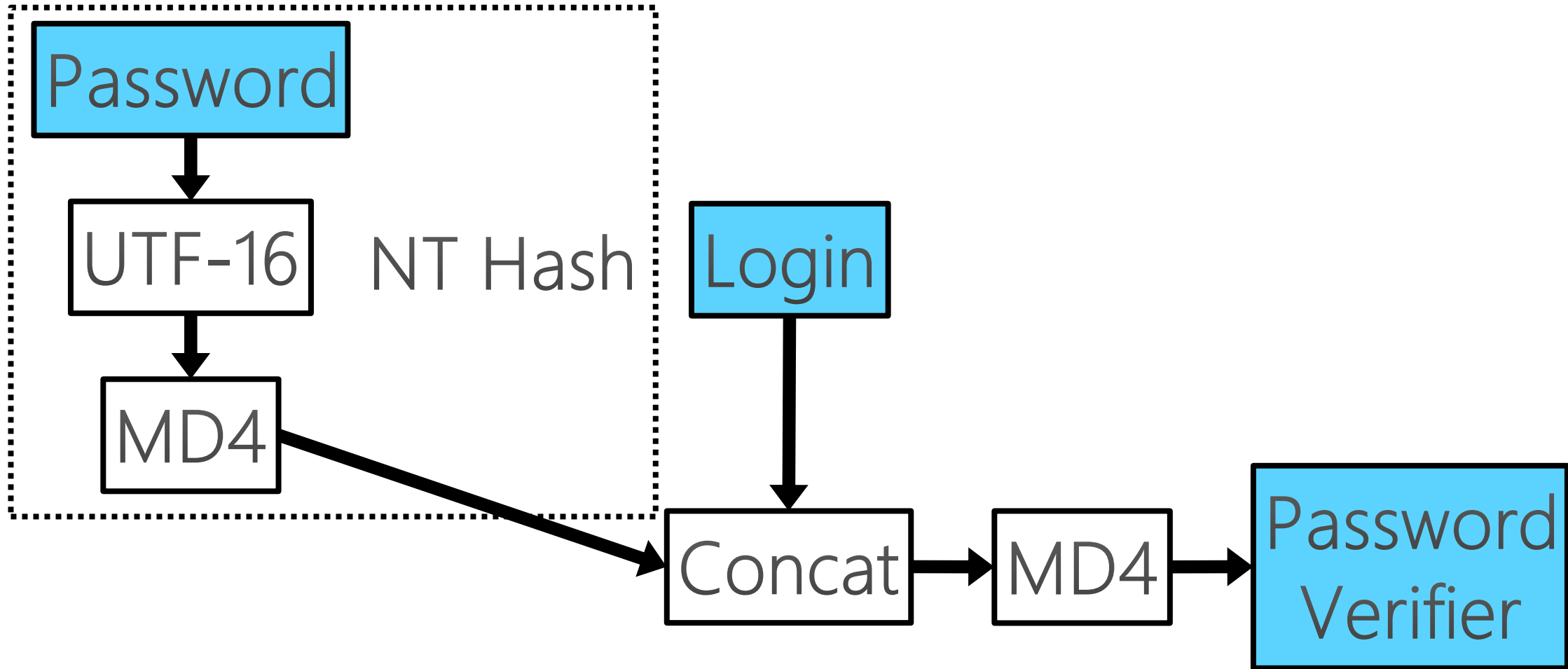
Edit...



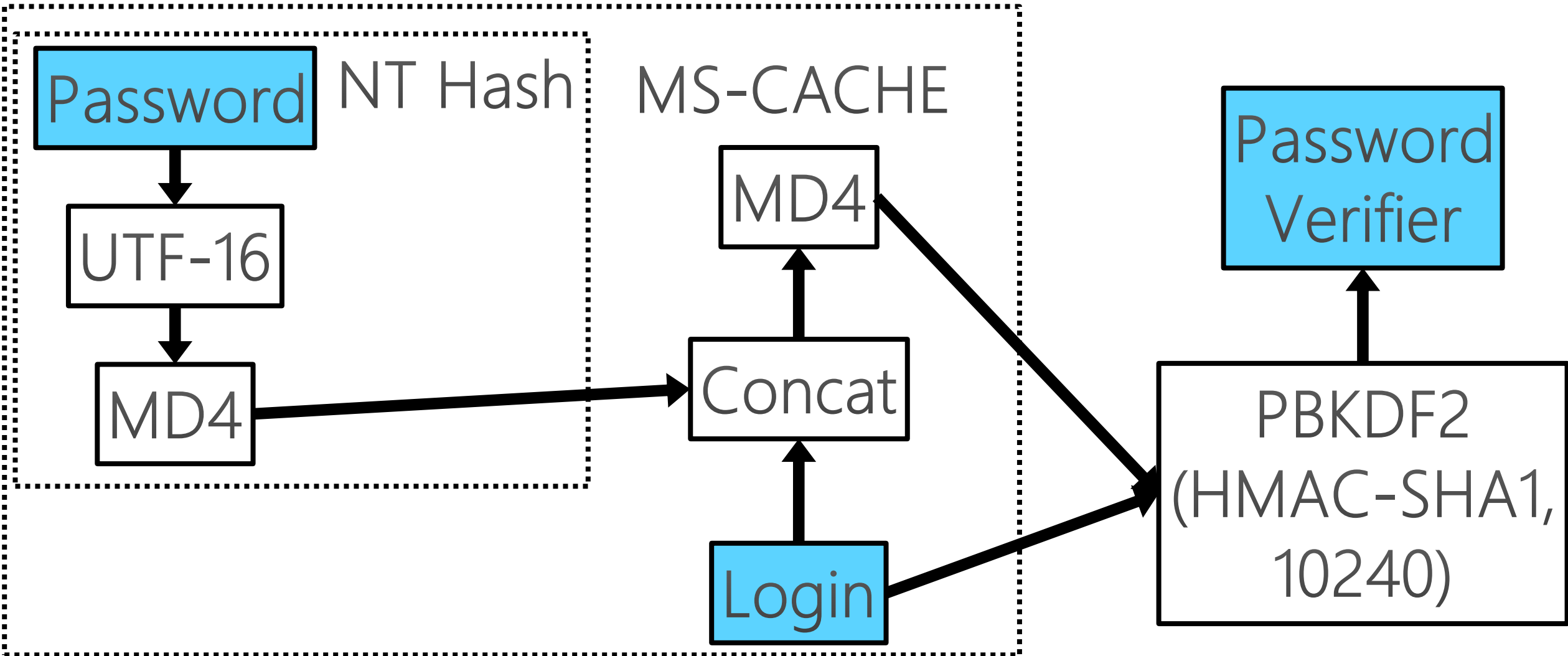
Credential Verifiers

- Windows caches AD credentials locally
- Used when DC is unavailable
- Defaults: 25 on servers, 10 on clients
- AKA MS-CACHE and MS-CACHE v2

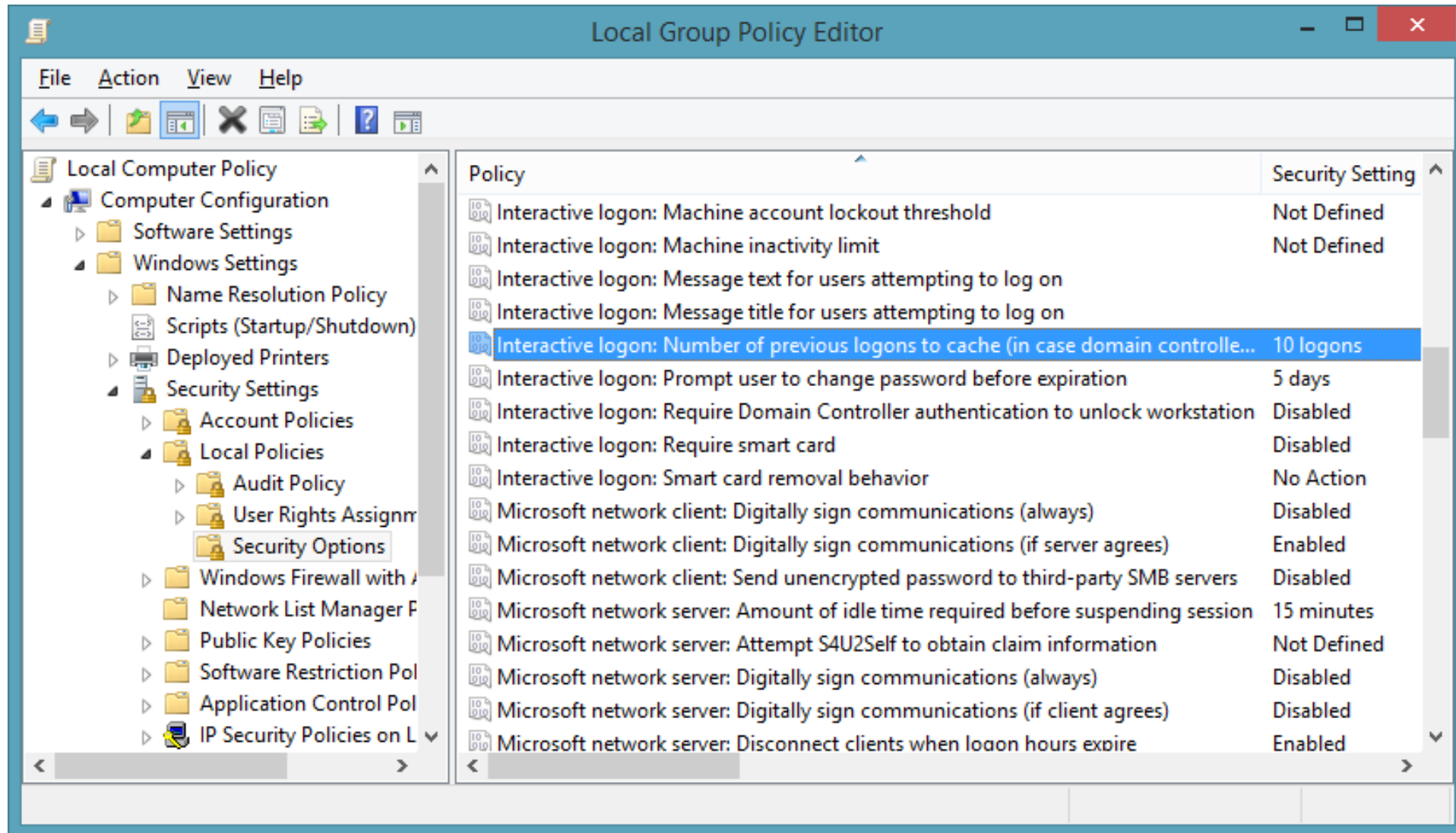
MS-CACHE Algorithm (XP)



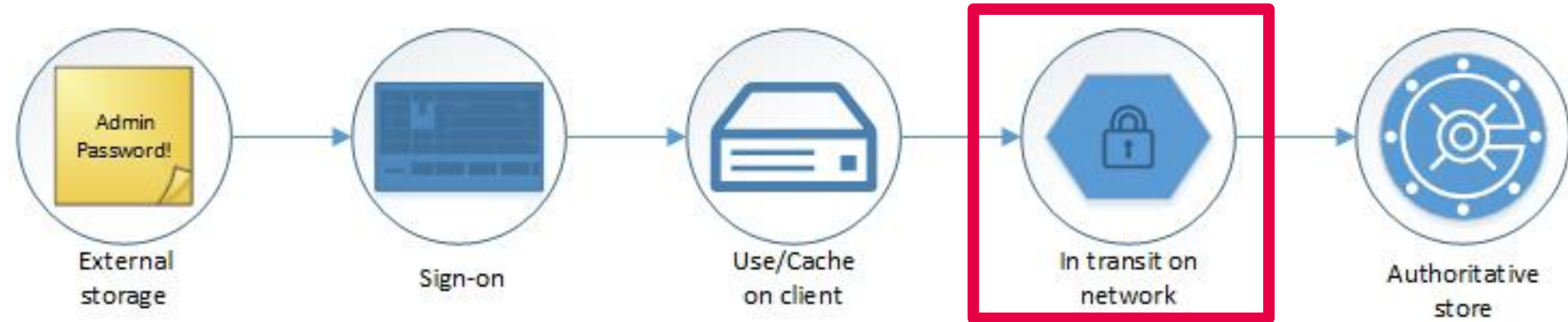
MS-CACHE v2 Algorithm (Vista+)



Configuring Credential Cache



Credentials Lifecycle / Attack Vectors



Using the Hash/Key/Ticket

DEMO

Passing the NT hash using Mimikatz

Golden Ticket

kerberos::golden

/domain:chocolate.local

/sid:S-1-5-21-130452501-2365100805-3685010670

/aes256:15540cac73e94028231ef86631bc47bd5c827847ade468d
6f6f739eb00c68e42

/user:srvcharly\$

/id:1001

/groups:513,1107

/ticket:fake_utilisateur.kirbi



GOPAS



DAQUAS



Microsoft

Proactive Measures

- Disable NTLM Authentication
- Disable Kerberos RC4-HMAC
- Implement Smartcard Authentication
- Unique local Administrator passwords
- Logon restrictions with new well-known SIDs
 - NT AUTHORITY\Local account
 - NT AUTHORITY\Local account and member of Administrators group
 - KB2871997 required on Windows 7 and 8
- Firewalls

Strengthening Kerberos Security

Steve Winfield Properties

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	
General	Address	Account	Profile
		Telephones	Organization

User login name:
 @Adatum.com

User login name (pre-Windows 2000):

☐ Unlock account

Account options:

- ☐ Use Kerberos DES encryption types for this account
- ☐ This account supports Kerberos AES 128 bit encryption.
- ☐ This account supports Kerberos AES 256 bit encryption.
- ☐ Do not require Kerberos preauthentication

Account expires:

☒ Never

☐ End of:

Network security: Configure encryption types allowed...

Security Policy Setting Explain

Network security: Configure encryption types allowed for Kerberos

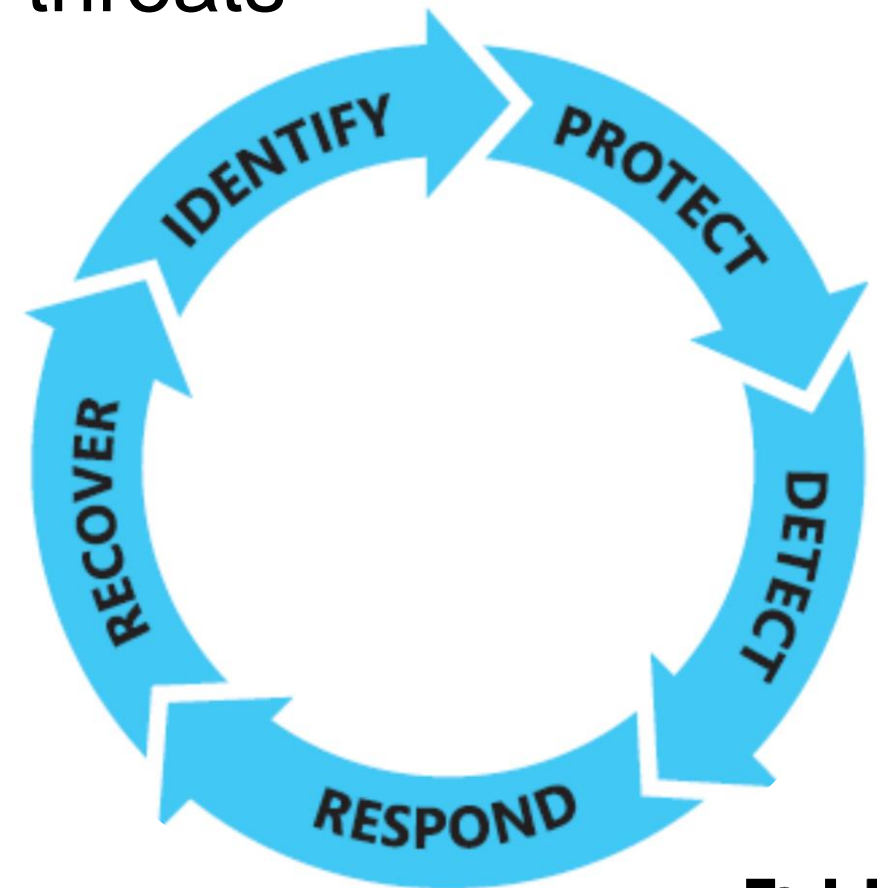
☒ Define these policy settings

DES_CBC_CRC	<input type="checkbox"/>
DES_CBC_MD5	<input type="checkbox"/>
RC4_HMAC_MD5	<input type="checkbox"/>
AES128_HMAC_SHA1	<input checked="" type="checkbox"/>
AES256_HMAC_SHA1	<input checked="" type="checkbox"/>

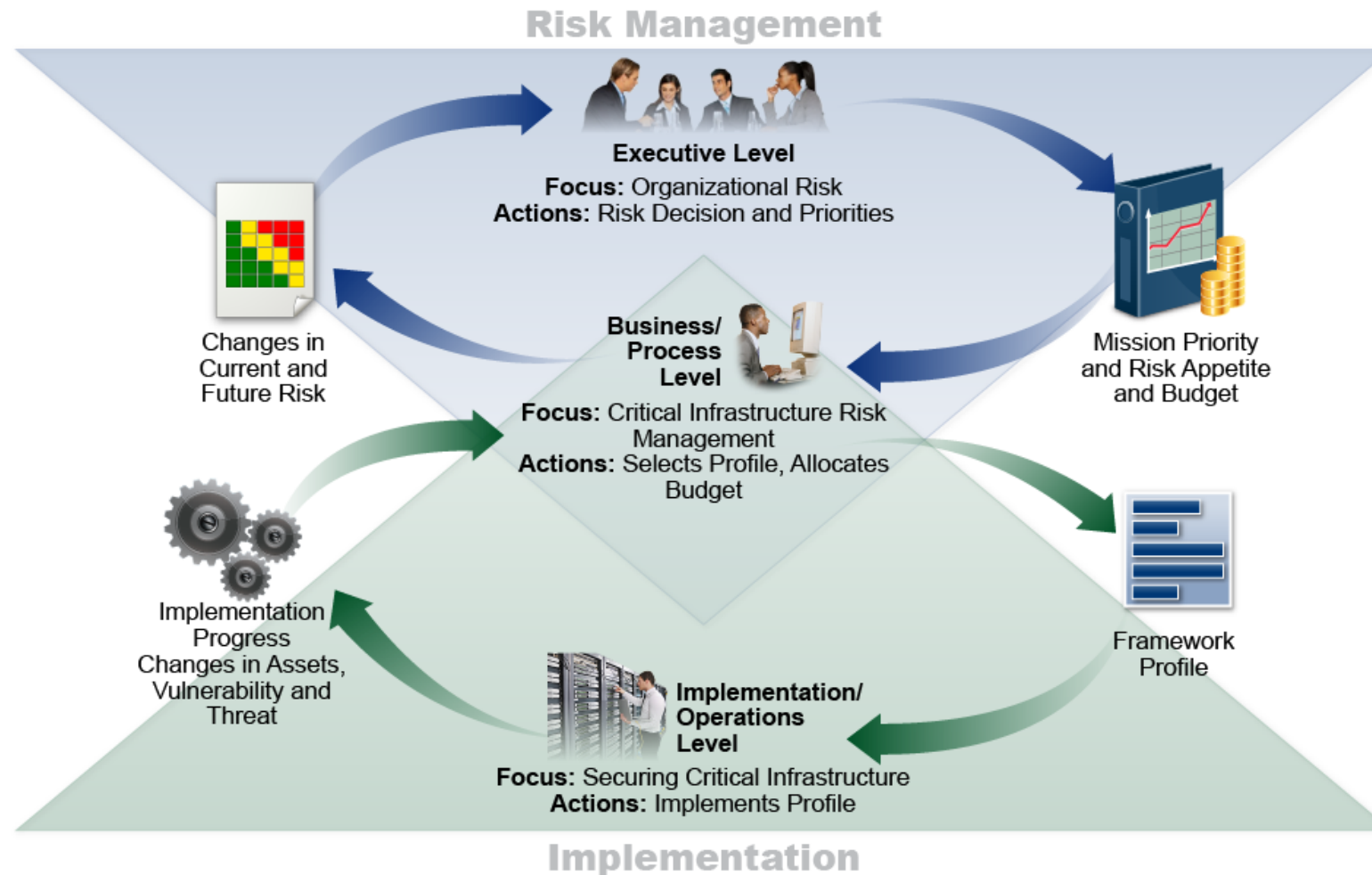
PtH Mitigation Strategies

Planning for compromise

- Identify all high-value assets
- Protect against known and unknown threats
- Detect PtH and related attacks
- Respond to suspicious activity
- Recover from a breach



NIST Framework for Improving Critical Infrastructure Cybersecurity

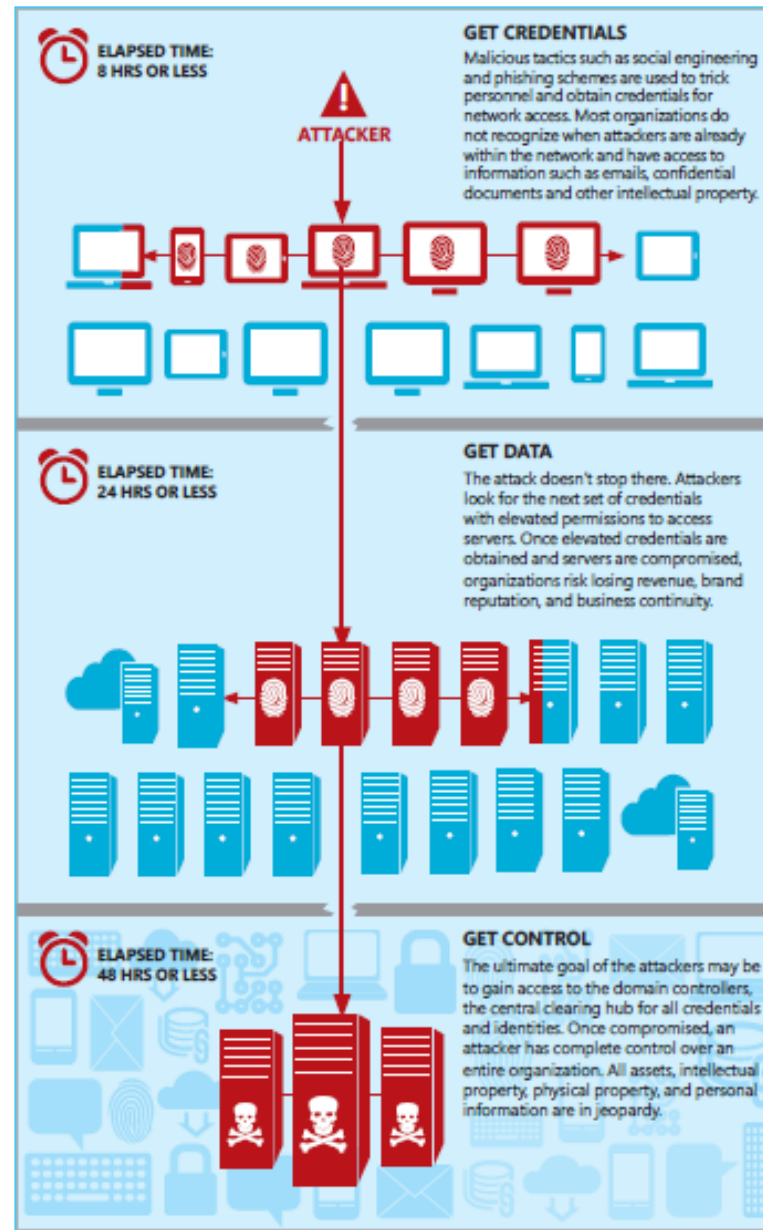


NIST Framework for Improving Critical Infrastructure Cybersecurity

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

PtH Detection

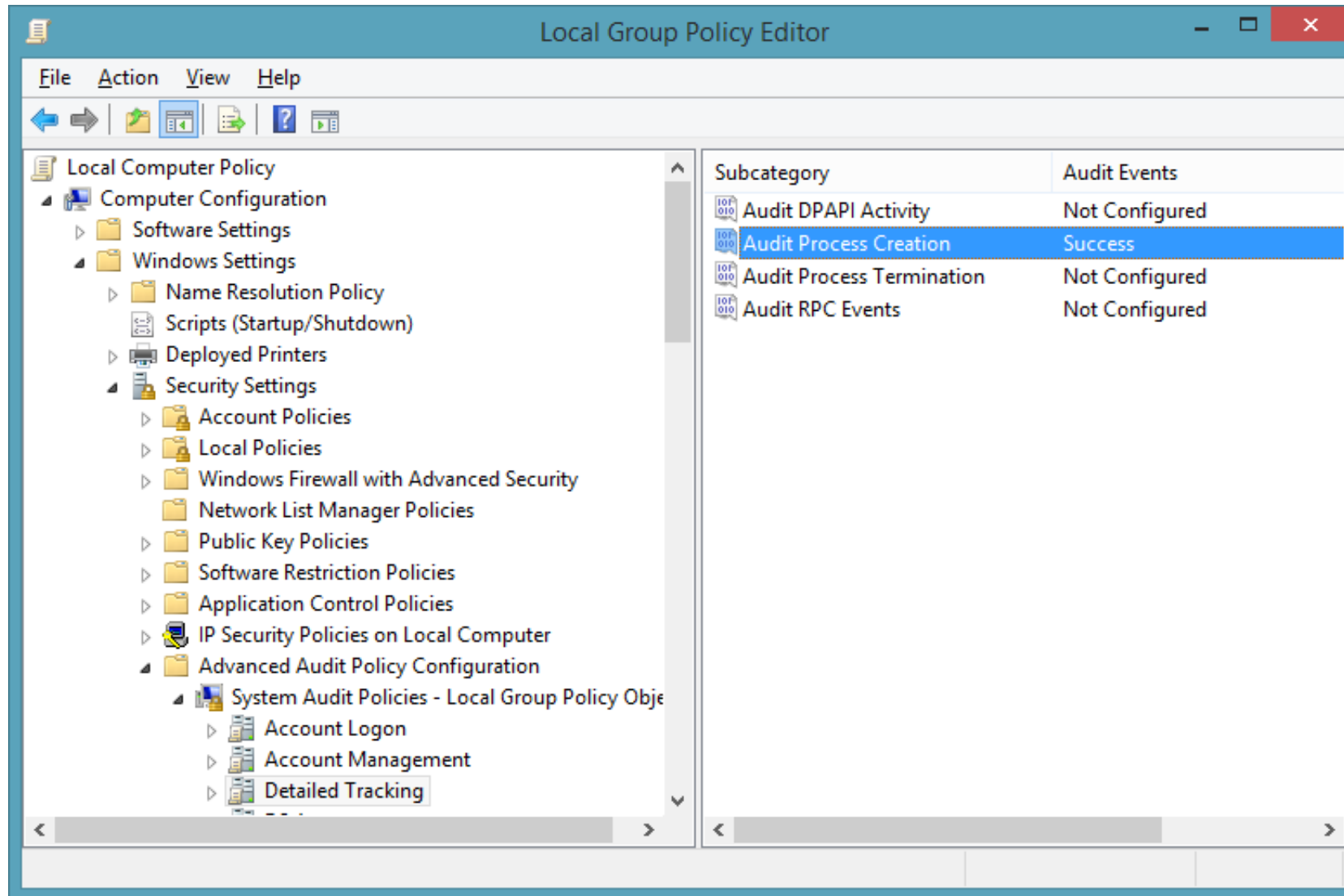
Attack Graph



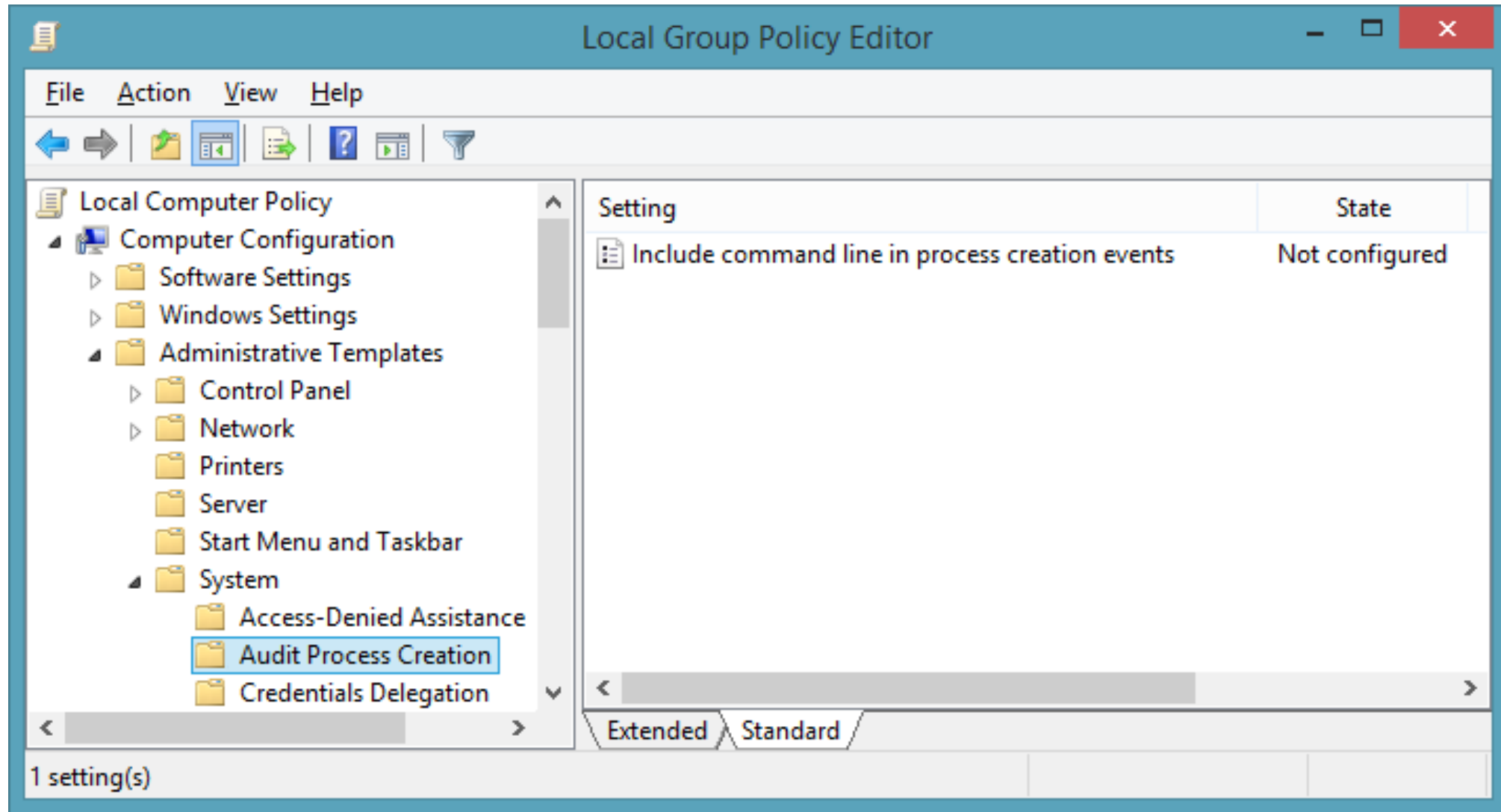
Events

- Authentication
 - Success
 - Failure
- Replication Traffic
- ...

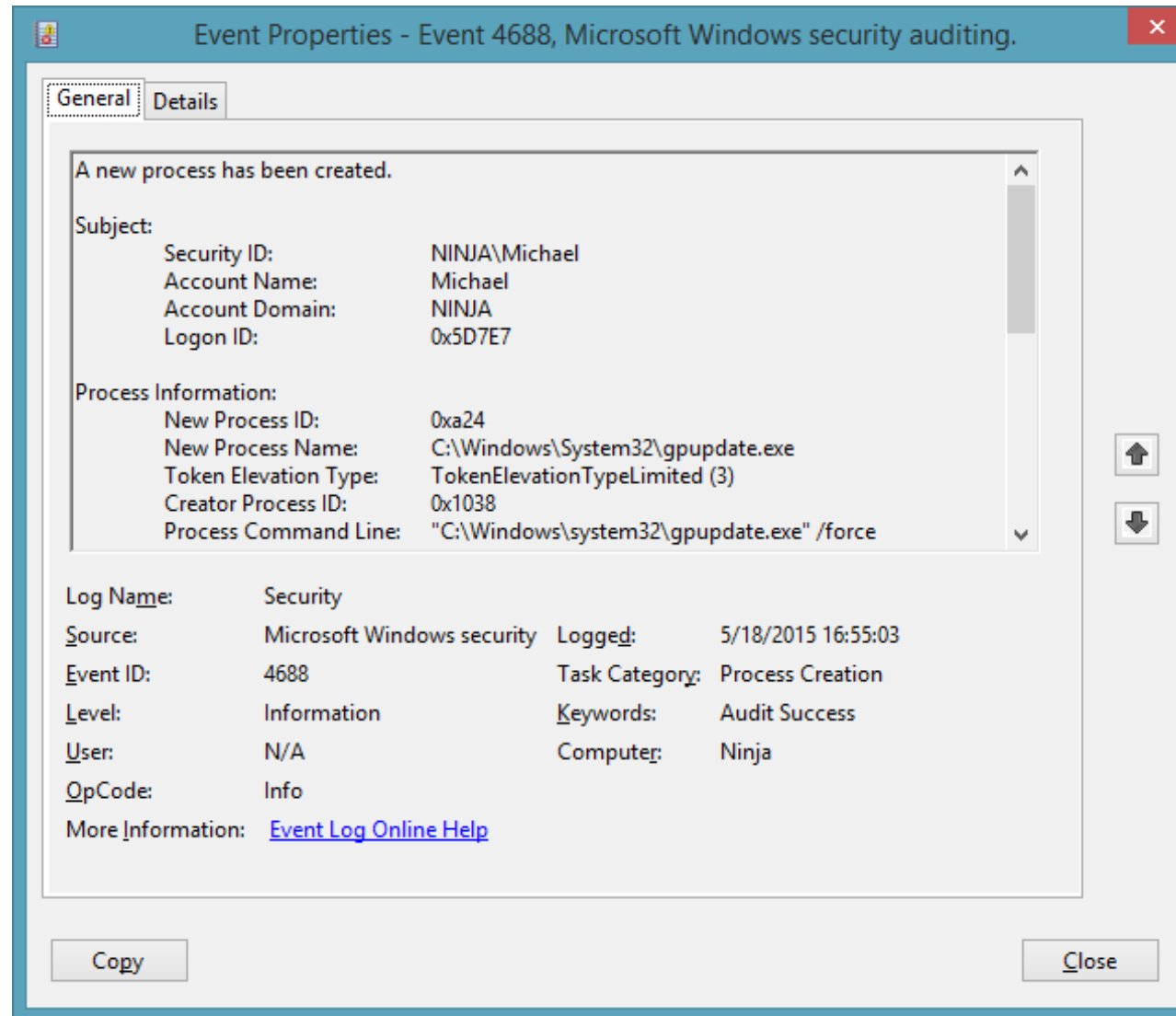
Audit Process Creation



Audit Process Creation



Audit Process Creation



Reactive Measures

- Change account passwords
- Reset computer account passwords
- Disable+Enable smartcard-enforced accounts
- Reset KRBtgt account
- Implement countermeasures

Windows 10

New Challenges Require a New Platform



Passwords theft
increasingly successful

Multi-factor solutions
too complex

Identity protection

A viable alternative
to passwords arrives

Easy and cost effective
multi-factor

A common solution everyone

Windows Hello

Microsoft Passport

Disk encryption
difficult to deploy

Use of 3rd party
solutions DLP

Data protection

Disk encryption
increasingly enabled OOB

DLP in Windows, better
with Azure and Office

BitLocker

Enterprise Data Protection

300K's+ malware
new threats per day

No way for AV
to keep up

Threat resistance

Rate of new malware
threats per day
irrelevant

Lock down Window to
only run trusted apps

Device Guard

Windows Defender

Unable to maintain
system integrity

Malware tampers with
defenses and hides

Security Hardware

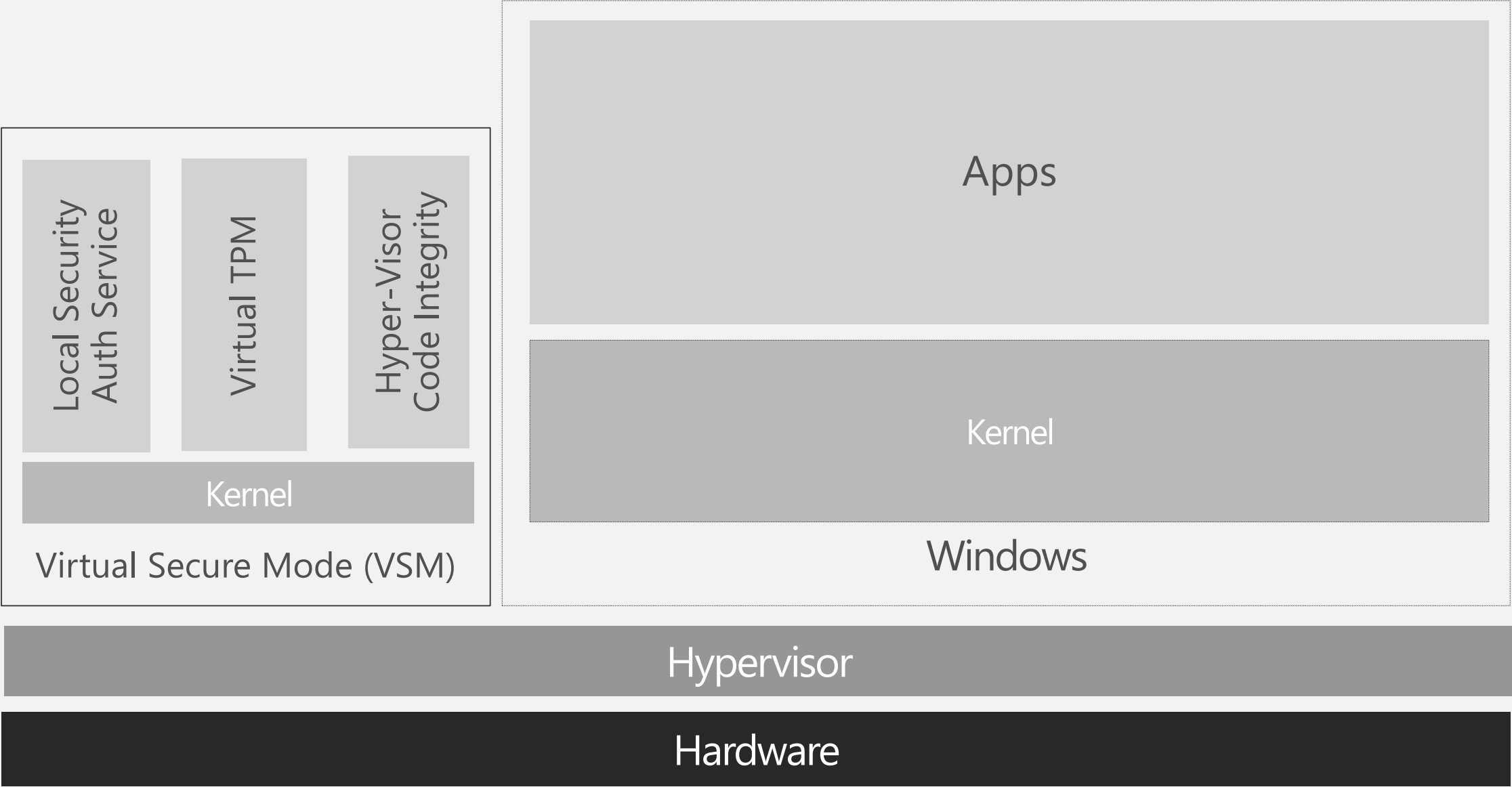
Hardware protects
system integrity

Defenses isolated
away from malware

UEFI Secure Boot

TPM 2.0, Virtualization

Hypervisor Code Integrity (HVCI) protected by VSM



DEVICE GUARD

Hardware Rooted
App Control

Enables a Windows desktop to be locked down to only run trusted apps, just like many mobile OS's (e.g.: Windows Phone)

Untrusted apps and executables such as malware are unable to run

Resistant to tampering by an administrator or malware

Requires devices specially configured by either the OEM or IT

DEVICE GUARD

Getting Apps into
the Circle of Trust

Supports all apps including Universal and Desktop (Win32)

Trusted apps can be created by IHV, ISV, and Organizations using a Microsoft provided signing service

Apps must be specially signed using the Microsoft signing service. No additional modification is required

Signing service will be made available to OEM's, IHV, ISV's, and Enterprises

MICROSOFT PASSPORT

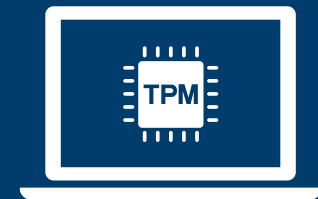


**YOUR DEVICE IS ONE OF
THE FACTORS**

USER CREDENTIAL



An asymmetrical key pair
Provisioned via PKI or created
locally via Windows 10



**SECURED BY
HARDWARE**



Hello Chris

**WINDOWS
HELLO**



Fingerprint



Iris



Facial



Gold partner:



Generální partner:



Pass-the-Hash Attacks

Michael Grafnetter
www.dsinternals.com

18. – 21. května 2015
Tech·Ed
DevCon 

Aktuální a navazující kurzy sledujte na www.gopas.cz

DÁREK PRO VÁS!

Vyplňte dotazníkové hodnocení a...

...získejte tričko **TechEd-DevCon 2015!**



SOUTĚŽ! SOUTĚŽ! SOUTĚŽ!

TechEd party!
Billiard klub Harlequin Praha, 20.5.2015

**Bud'te The Best IT Pro
nebo The Best Developer**