To Serve and Protect:
Microsoft Advanced Threat Analytics

Dennis Rietveld

Experts Live 2016

Dennis Rietveld

Freelance IT consultant
MCSA, MCSE, MCITP, CCA, VCP
activedirectory.nl
@R33dfield #ExpertsLive
dennis@rietveld-ict.nl

SECURITY

Agenda

- Wat is Microsoft ATA
  - **Introductie**
  - **Architecture**
  - **Sizing, Planning & Deployment**
- Attack Kill Chain
- Demo
- Mitigation

Home / Security

KIM ZETTER SECURITY 06.15.16 7:00 AM

THOUSANDS OF HACKED GOVERNMENT AND CORPORATE SERVERS SELLING FOR $6 ON BLACK MARKET

Inverse Path's USB armory is a secure computer squeezed onto a USB device.

AtomBombing Code Injection can potentially hack all Windows OS versions

October 28, 2016 By Pierluigi Paganini

Great Tesco Bank robbery: Hackers steal cash from 20,000 accounts as bosses freeze payments in 'emergency measure' amid fears fraudsters have cracked the codes to make new bank cards at will

- Bank CEO Benny Higgins freezes online transactions after hackers strike
- Under fire boss says 20,000 accounts have cash taken in weekend attack
- One customers says hackers may have created a new debit card in Brazil
- Another victim reported account was hit by £2,000 due to the attack
- Thousands of customers have found their bank cards have been stopped

eated "golden keys" which unlock Windows devices
ot. [Updated]

By Charlie Osborne for Zero Day | August 10, 2016 -- 10:26 GMT (11:26 BST) | Topic: Security

SECURITY

Microsoft ATA

SECURITY

Wat is Microsoft ATA

- On-premise applicatie (nog wel)
- Onderdeel van EMS
- Gedragsanalyse
- Verschillende data bronnen
- Detectie
  - Reconnaissance
  - Compromised credentials
  - Lateral movement
  - Privilege escalation
  - Domain dominance

SECURITY

Reconnaissance

Account enumeration
Net Session verkenning
Verkenning DNS
Verkenning Active Directory (SAM-R)
Afwijkend gedrag toegang resources

Lateral Movement

Pass the ticket
Pass the hash
Over-pass the hash
Afwijkende authenticatie verzoeken
Afwijkend gedrag toegang resources

Domain Dominance

Skeleton key malware
Golden ticket
Remote execution
Malicious replication request

Brute force via NTLM, Kerberos, LDAP
Gevoelige accounts in plain text authentication
Service accounts in plain text authentication
Honey Token account verdacht gedrag
Unusual protocol implementation
Malicious Data Protection Private Info Request
Afwijkend gedrag (aanwezigheid medewerker)

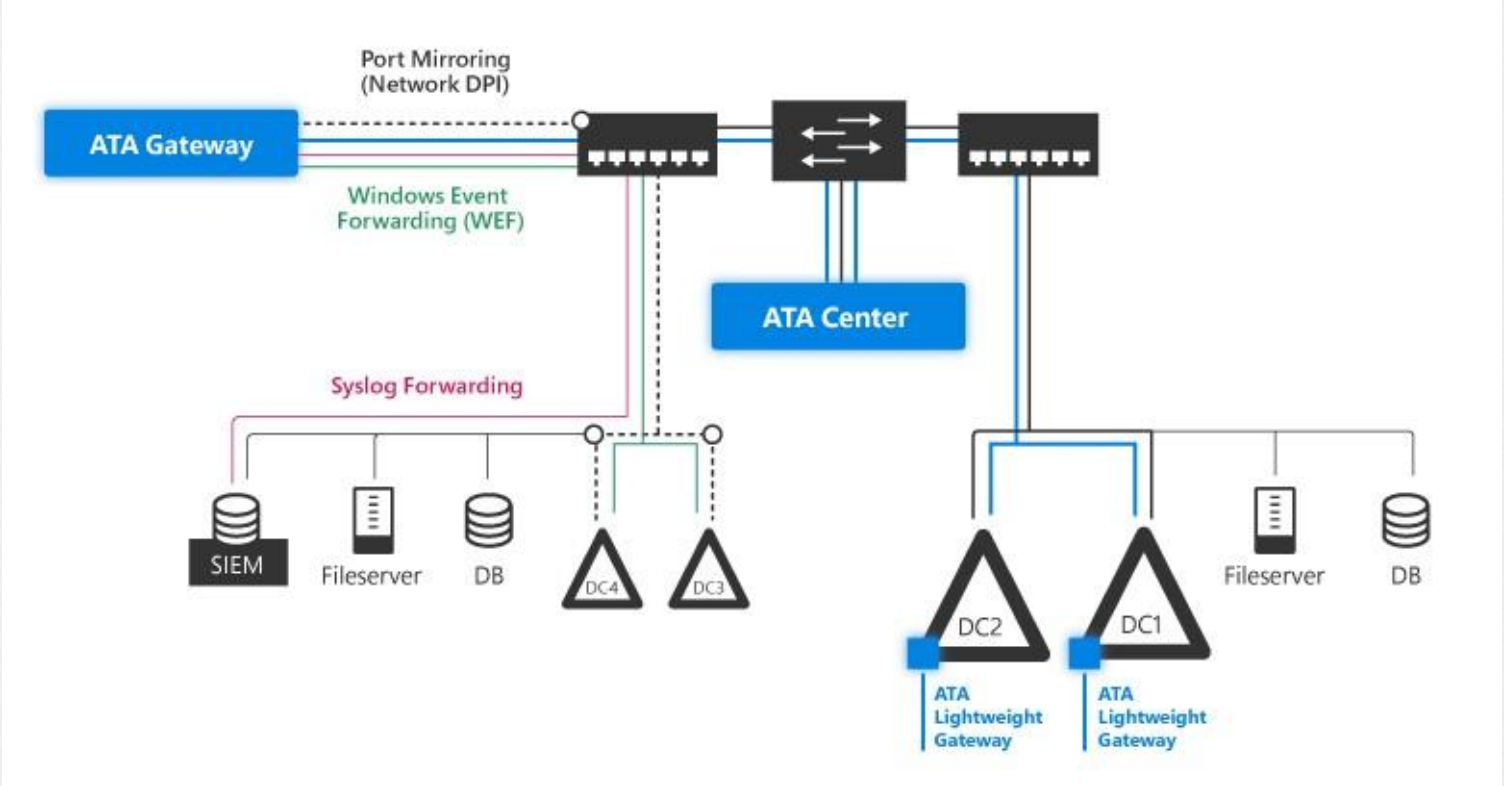
Compromised Credential

MS14-068 exploit (Forged PAC)
MS11-013 exploit (Silver PAC)

Privilege Escalation

Architecture

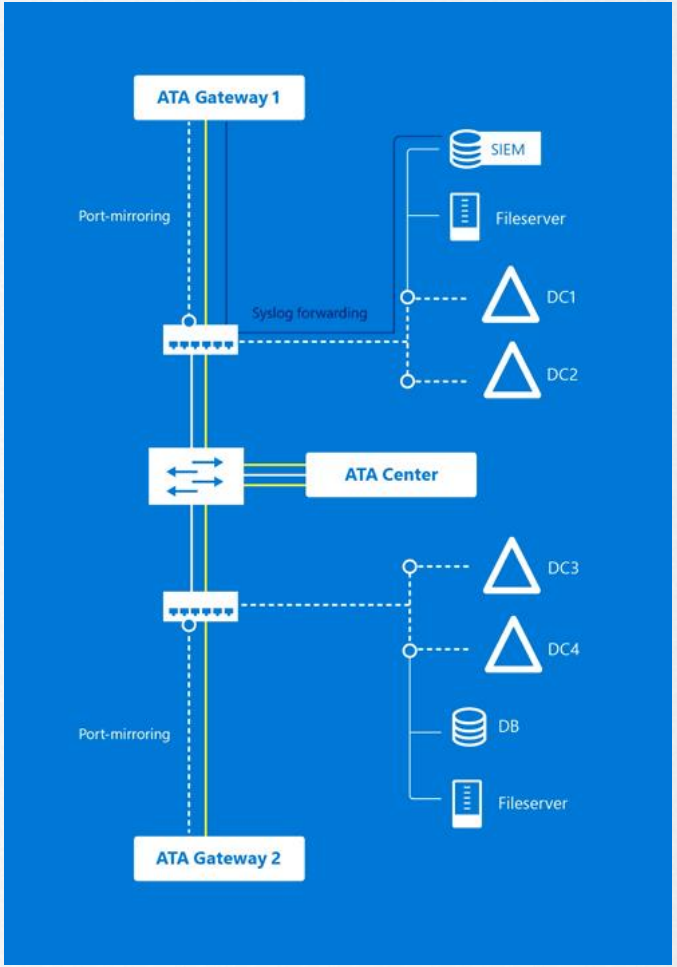
Architecture



Bron: Microsoft

Architecture

- ATA Center
- ATA Console
- ATA Gateway
- ATA Lightweight Gateway



Sizing, Planning & Deployment

System requirements

	2008 R2 SP1	2012	2012 R2	2016
ATA Center / Console			X	X
ATA Gateway			X	X
ATA Lightweight Gateway	X	X	X	X

ATA Center / Console
ATA Center Service
.NET Framework 4.6.1
MongoDB
2 IP adressen
Certificaten
KB2919355

ATA Lightweight Gateway
ATA Gateway service
ATA Gateway updater service
.NET Framework 4.6.1
Microsoft Visual C++ 2013 redist
Certificaten
KB2919355

ATA Gateway
ATA Gateway service
ATA Gateway updater service
.NET Framework 4.6.1
Microsoft Visual C++ 2013 redist
Certificaten
2 netwerk adapters
KB2919355 en KB3047154

Sizing

- ATA sizing tool
- Baseline Domain Controller

Number of DCs	4				
Number of Samples	69				
Overall Start Time UTC	2016-07-21 10:41:54				
Overall End Time UTC	2016-07-21 10:43:09				
Display DC Times as UTC/Local	Universal Time (UTC)				
Center	**Max Packets/sec**	**Avg Packets/sec**	**Busy Packets/sec**	**Busy Packets/sec Start UTC**	**Busy Packets/sec End UTC**
Grand Total	1,616	1,184	1,184	10:41:55	10:43:08
DC	**Max Packets/sec**	**Avg Packets/sec**	**Busy Packets/sec**	**Busy Packets/sec Start Time**	**Busy Packets/sec End Time**
DC1	644	457	457	10:41:54	10:43:08
DC3	334	234	234	10:41:54	10:43:08
DC4	408	249	249	10:41:54	10:43:08
DC2	405	244	244	10:41:54	10:43:08
Total	**1,792**	**1,184**	**1,184**		

Sizing tool download: https://gallery.technet.microsoft.com/Advanced-Threat-Analytics-7371c87f

Sizing ATA Center

Packets per second *	CPU (cores**)	Memory (GB)	Database storage per dag (GB)	Database storage per maand (GB)	IOPS ***
1.000	2	32	0,3	9	30 (100)
10.000	4	48	3	90	200 (300)
40.000	8	64	12	360	500 (1.000)
100.000	12	96	30	900	1.000 (1.500)
400.000	40	128	120	1.800	2.000 (2.500)

* Totaal dagelijks gemiddelde aantal packets per seconde van alle domain controllers gemonitord door alle ATA Gateways

** Aantal fysieke cores, niet hyper-threaded

*** Gemiddelde (piek)

Sizing Gateway

Packets per second	CPU (cores)*	Memory (GB)
1.000	1	6
5.000	2	10
10.000	3	12
20.000	6	24
50.000	16	48

Sizing Lightweight Gateway

Packets per second	CPU (cores)**	Memory (GB)***
1.000	2	6
5.000	6	16
10.000	10	24

* Hyper-threading moet disabled zijn
** Aantal fysieke cores, niet hyper-threaded
*** Hoeveelheid geïnstalleerd geheugen in domain controller

Planning

- ATA Center Fysiek vs Virtueel
- ATA Center domain joined of workgroup?
- Disaster Recovery
- Gateway of Lightweight Gateway

Gateway	Voordelen	Kosten	Deployment	Domain controller resources
ATA Gateway	Out-of-band oplossing, lastig vindbaar door aanvaller	Hoger	Geplaatst naast domain controller (out-of-band)	Ondersteund tot 50.000 packets/sec
ATA Lightweight Gateway	Geen fysieke of virtuele dedicated server nodig en port mirroring	Lager	Geïnstalleerd op domain controller	Ondersteund tot 10.000 packets/sec

Planning

- Certificates, self signed of CA?
- Update strategie
- SIEM of WEF?
- ATA rol groepen

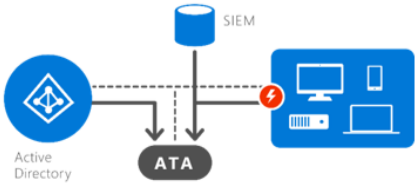
Groep	Permissies
ATA Admin	Alles
ATA Operator	Schrijf rechten maar kan geen aanpassingen maken aan de ATA configuratie
ATA Viewer	Alleen kijken

Deployment

- Active Directory forest is boundary
- Default domain user benodigd
- Deployment van ATA (lightweight) Gateway
  - Package download via ATA Center
  - Silent installatie mogelijkheden
- MongoDB

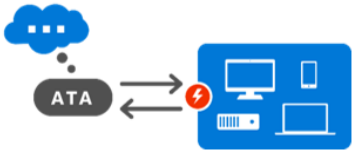
Done!

1 Analyze



Advanced Threat Analytics analyzes all Active Directory-related traffic and collects relevant events from SIEM

2 Learn



Advanced Threat Analytics automatically learns all entities' behaviors

3 Detect

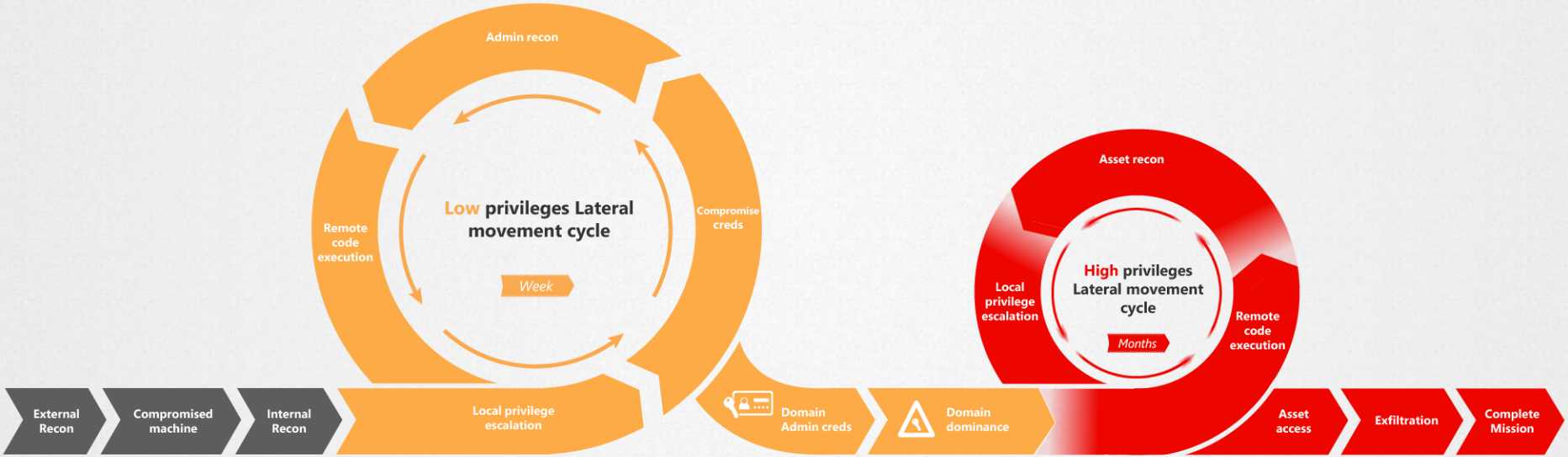
ATA builds the organizational security graph, detects abnormal behavior, protocol attacks, and weaknesses, and then constructs an attack timeline

Bron: Microsoft

Attack Kill Chain

SECURITY

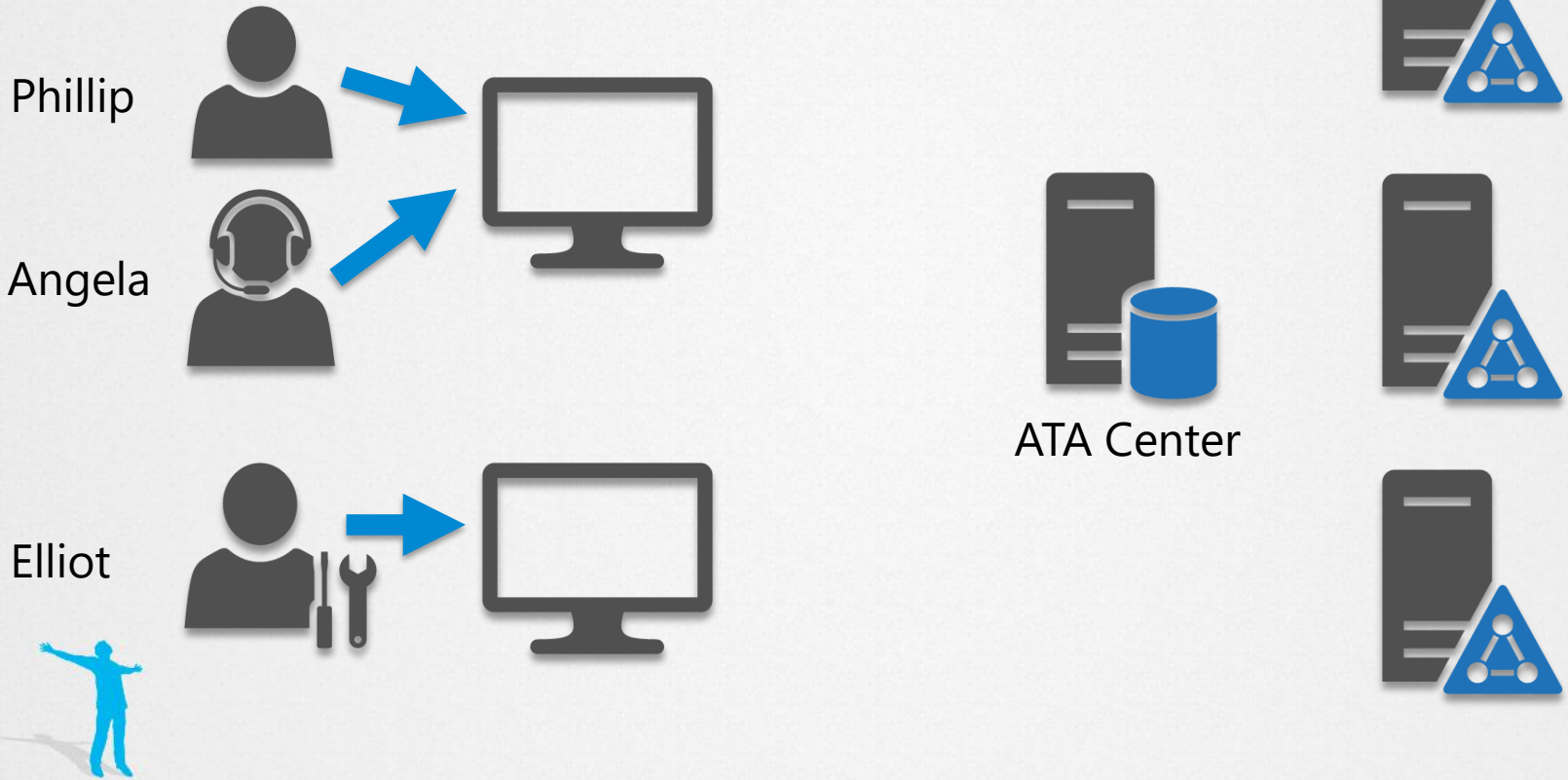
Attack Kill Chain



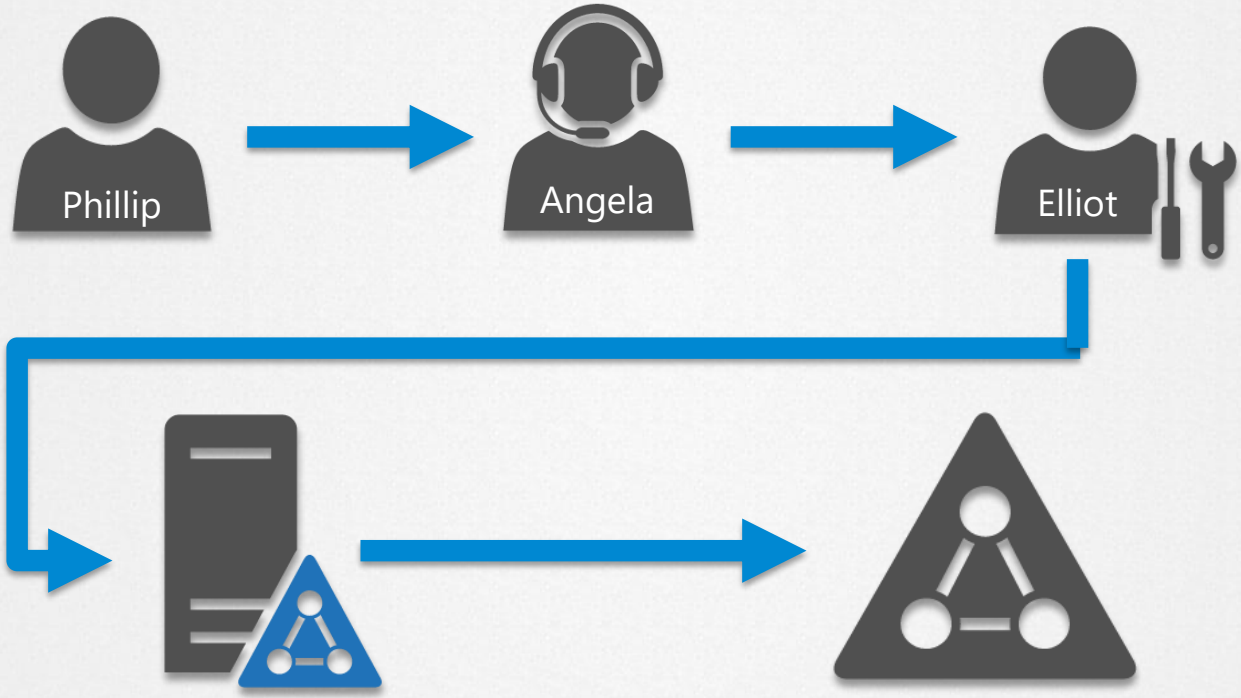
Bron: Michael Dubinsky, PM Microsoft ATA

Demo

Overview woodgrovebank.com

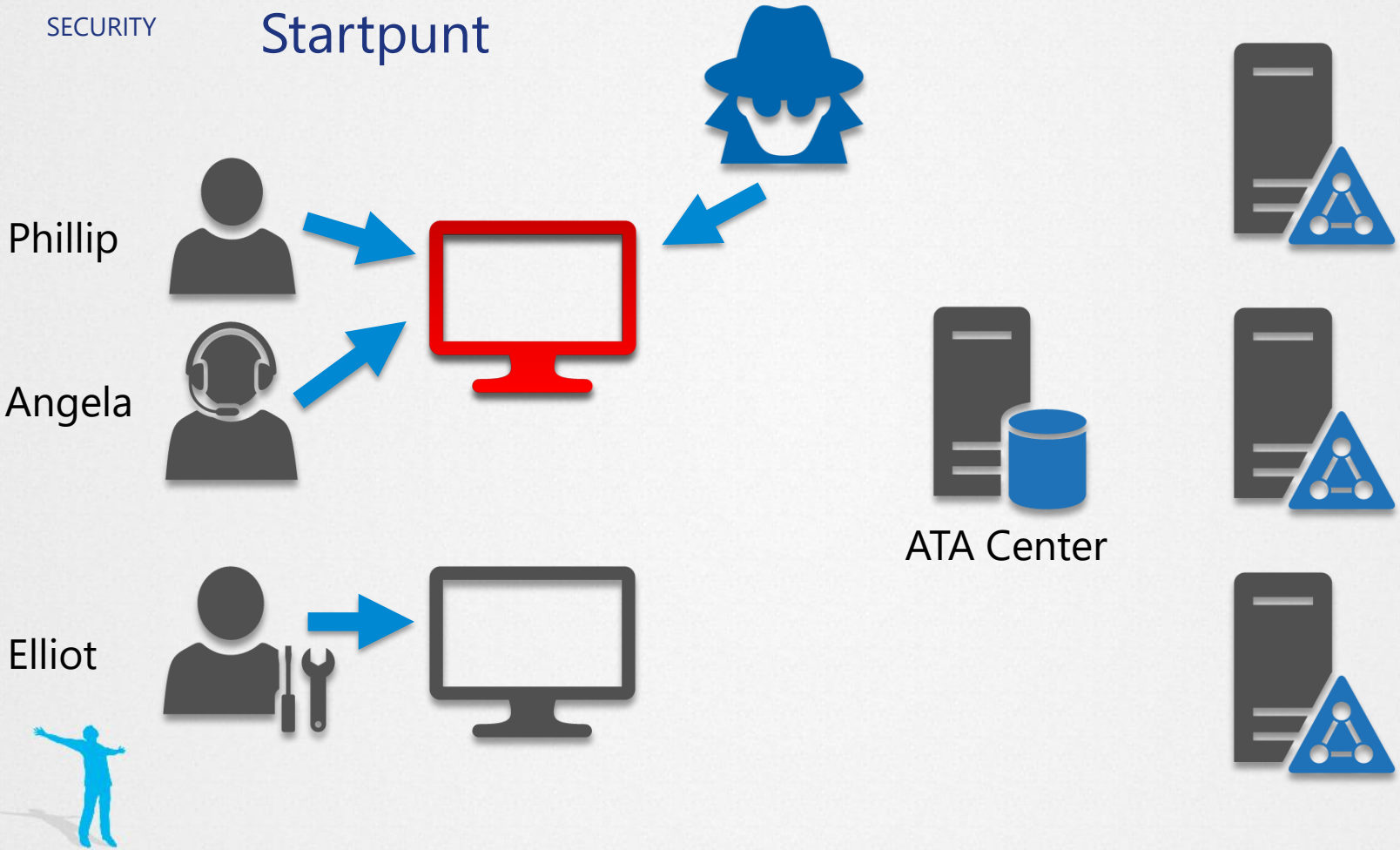


Doel? Domain Dominance



SECURITY

Startpunt

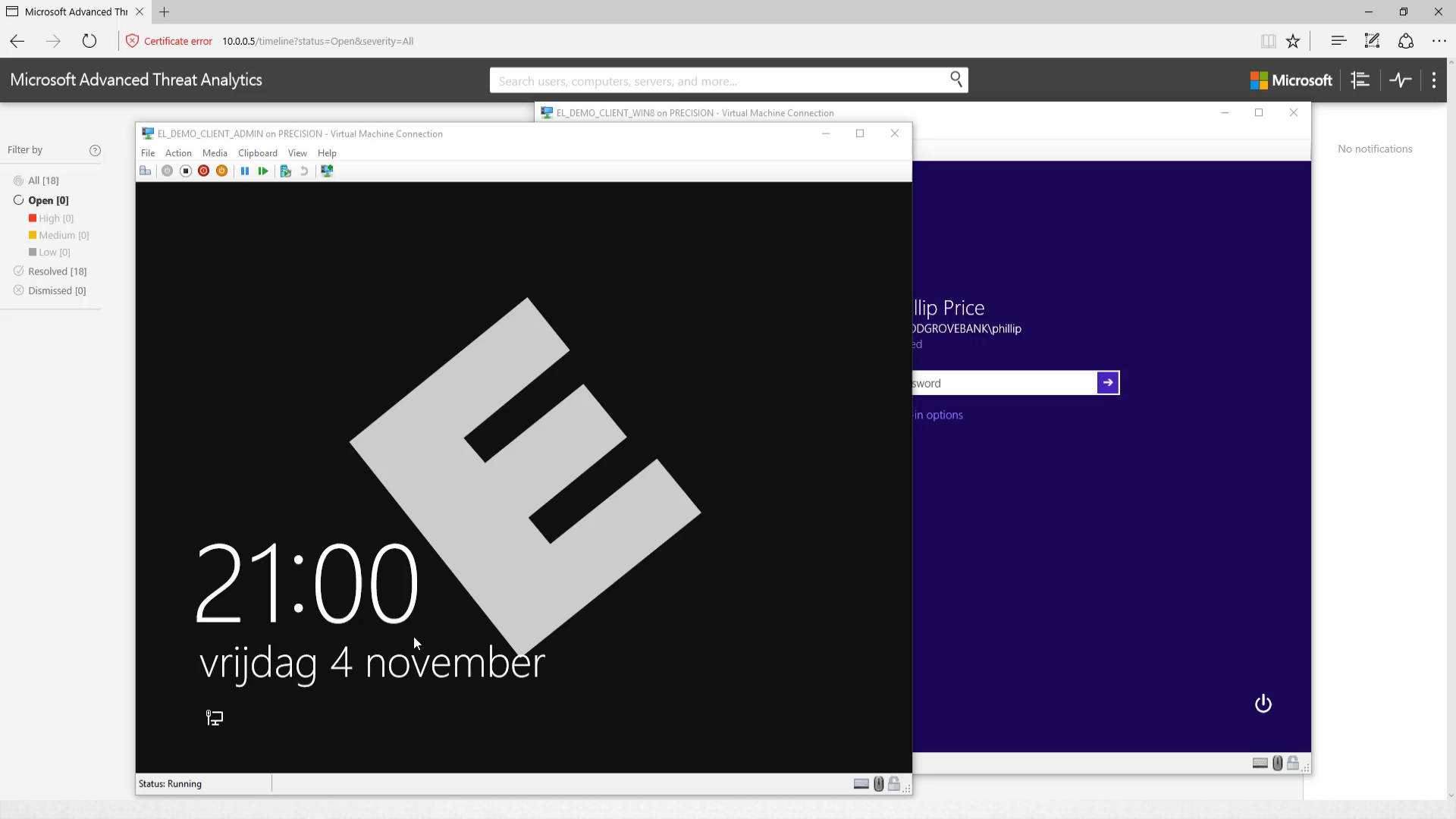


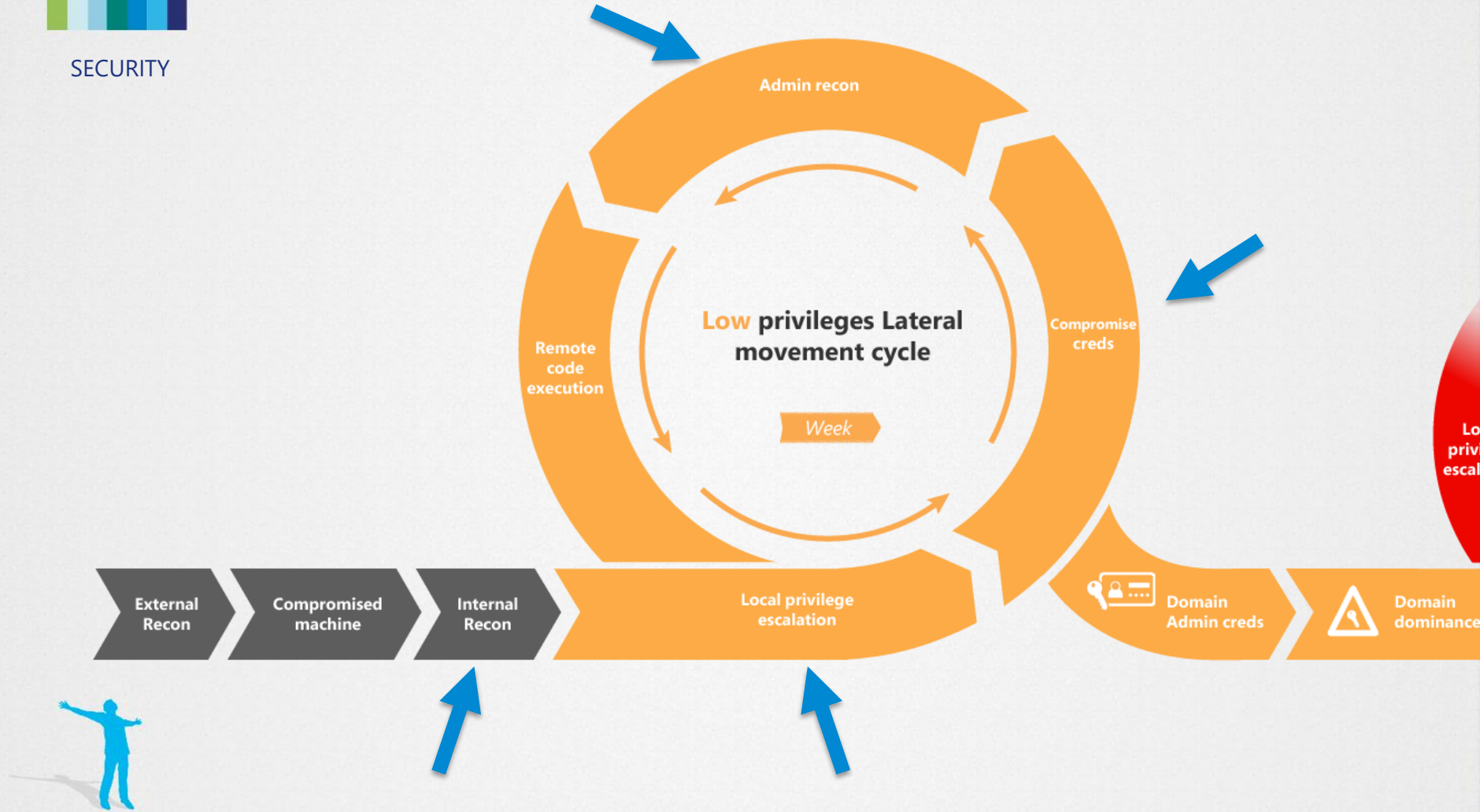
Verkenning (reconnaissance)

- Gebruiker en groep informatie (SAM-R)
- SMB sessies (Netsess)

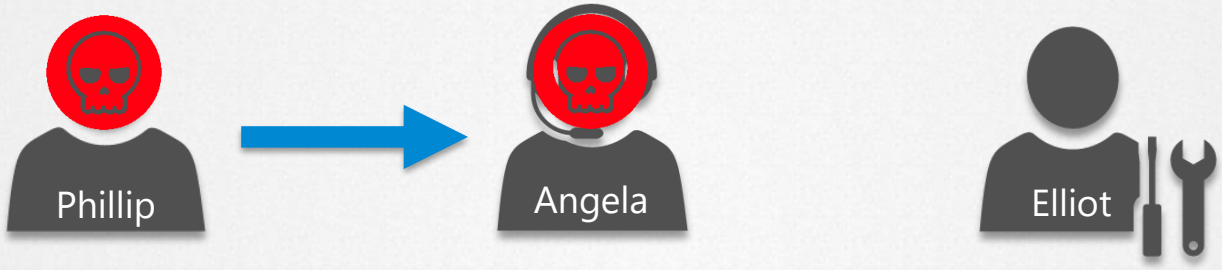
Lateral Movement

- Privileges van support stelen
- Over-pass-the-hash


Microsoft Advanced Thr
Certificate error 10.0.0.5/timeline?status=Open&severity=All
Microsoft Advanced Threat Analytics
Search users, computers, servers, and more...
Microsoft
Filter by
All [18]
Open [0]
High [0]
Medium [0]
Low [0]
Resolved [18]
Dismissed [0]
No notifications
EL_DEMO_CLIENT_ADMIN on PRECISION - Virtual Machine Connection
File Action Media Clipboard View Help
21:00
vrijdag 4 november
Status: Running
EL_DEMO_CLIENT_WIN8 on PRECISION - Virtual Machine Connection
llip Price
DGROVEBANK\phillip
sword
in options

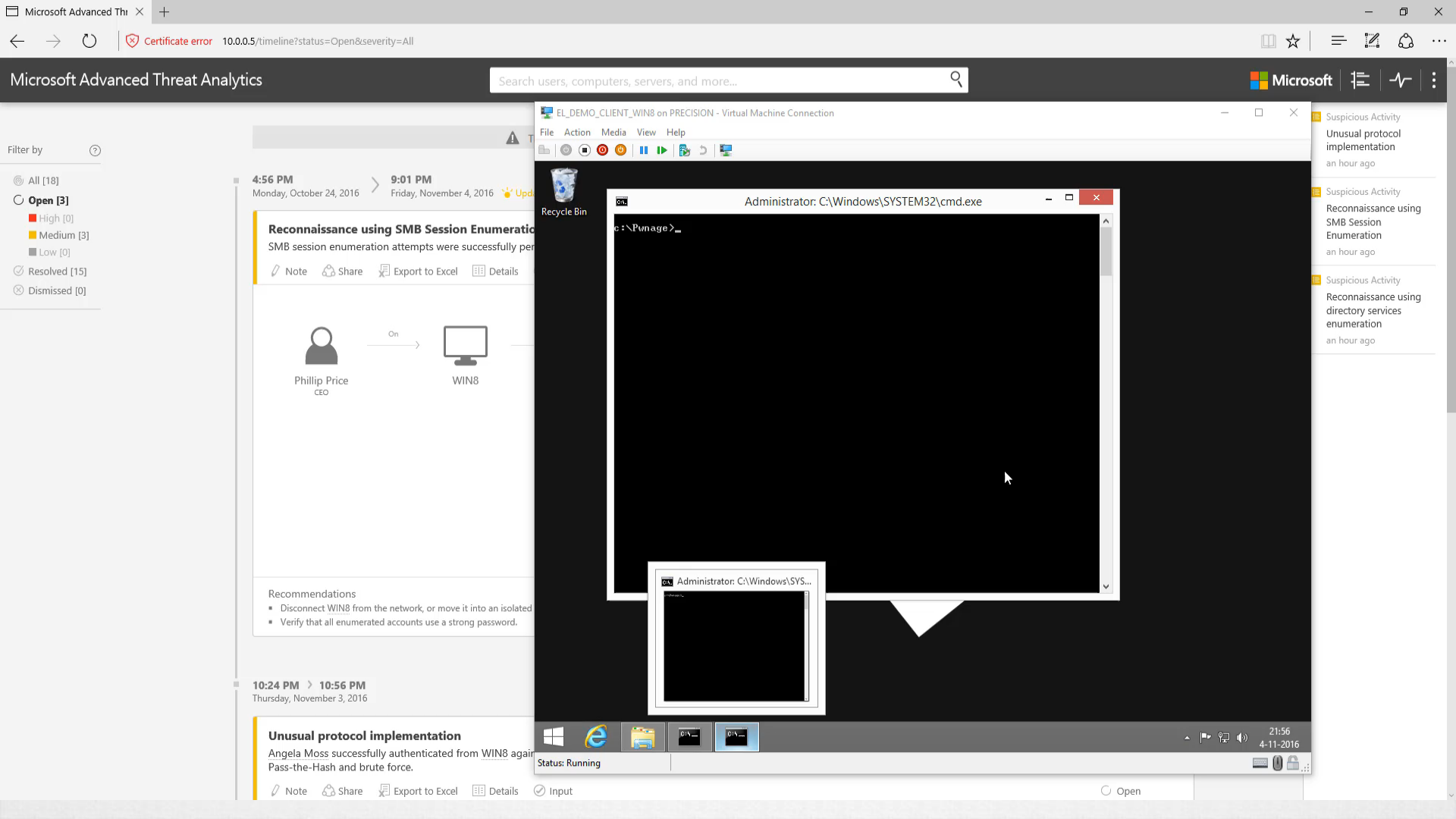

Admin recon
Compromise creds
Remote code execution
Low privileges Lateral movement cycle
Week
External Recon
Compromised machine
Internal Recon
Local privilege escalation
Domain Admin creds
Domain dominance

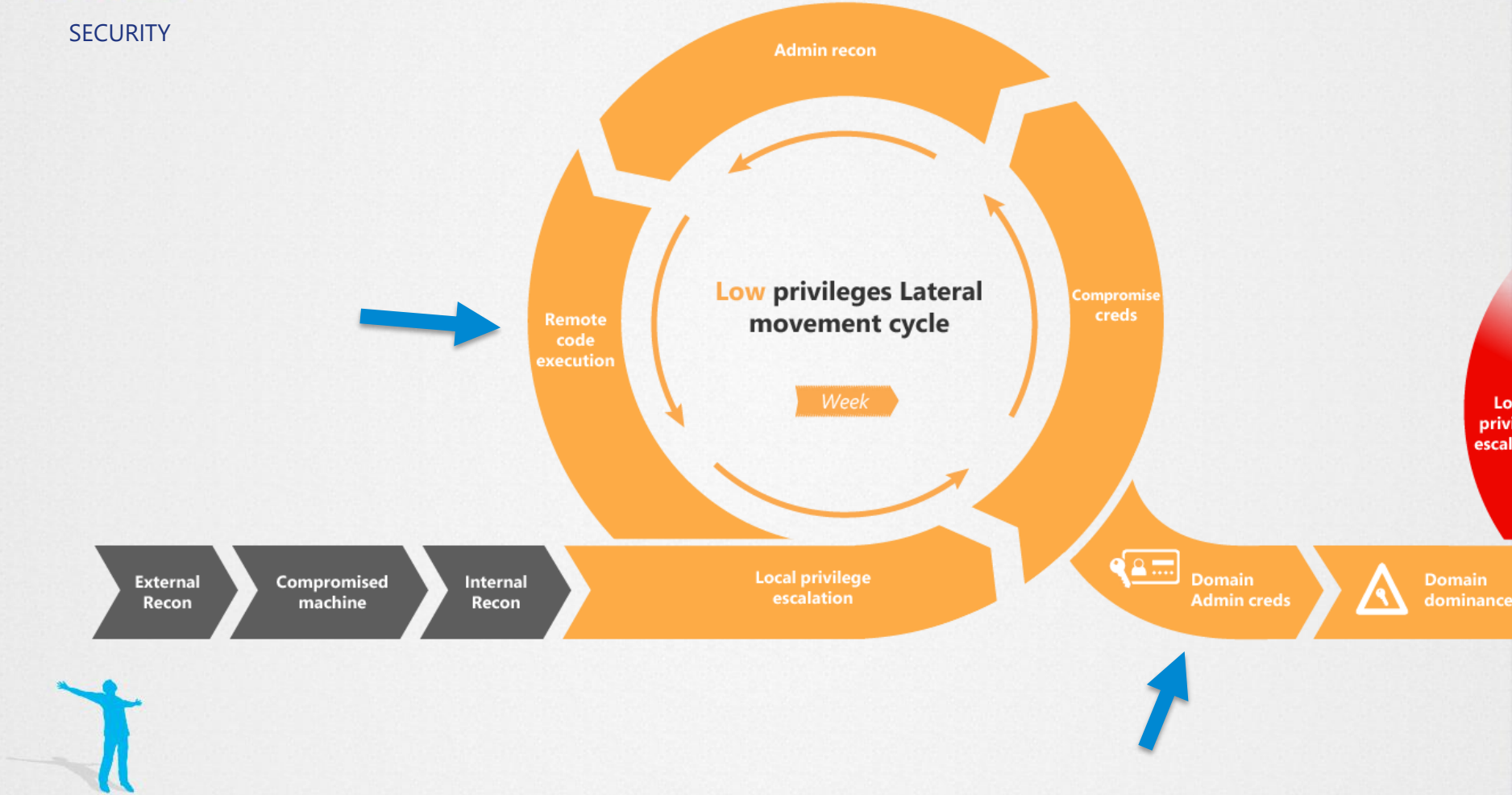
Bereikt tot zover



Lateral Movement

- Domain admin privileges stelen
- Pass-the-Ticket

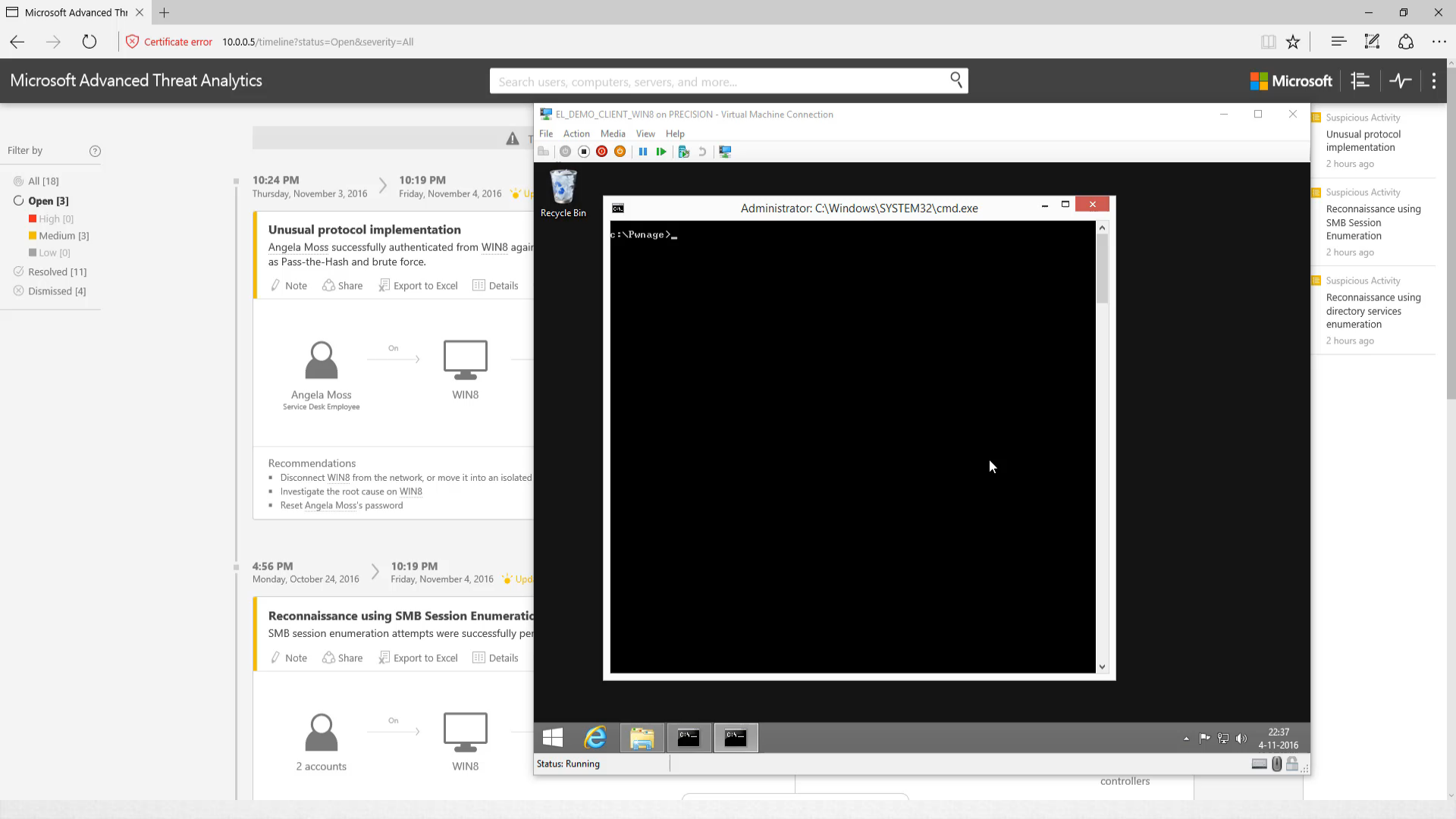

Microsoft Advanced Thr
Certificate error
10.0.0.5/timeline?status=Open&severity=All
Microsoft Advanced Threat Analytics
Search users, computers, servers, and more...
Microsoft
Filter by
All [18]
Open [3]
High [0]
Medium [3]
Low [0]
Resolved [15]
Dismissed [0]
4:56 PM
Monday, October 24, 2016
9:01 PM
Friday, November 4, 2016
Reconnaissance using SMB Session Enumeratio
SMB session enumeration attempts were successfully per
Note
Share
Export to Excel
Details
Phillip Price
CEO
On
WIN8
Recommendations
Disconnect WIN8 from the network, or move it into an isolated
Verify that all enumerated accounts use a strong password.
10:24 PM
10:56 PM
Thursday, November 3, 2016
Unusual protocol implementation
Angela Moss successfully authenticated from WIN8 agai
Pass-the-Hash and brute force.
Note
Share
Export to Excel
Details
Input
Open
EL_DEMO_CLIENT_WIN8 on PRECISION - Virtual Machine Connection
File
Action
Media
View
Help
Recycle Bin
Administrator: C:\Windows\SYSTEM32\cmd.exe
c:\Pwnage>_
Administrator: C:\Windows\SYS...
21:56
4-11-2016
Status: Running
Suspicious Activity
Unusual protocol implementation
an hour ago
Suspicious Activity
Reconnaissance using SMB Session Enumeration
an hour ago
Suspicious Activity
Reconnaissance using directory services enumeration
an hour ago

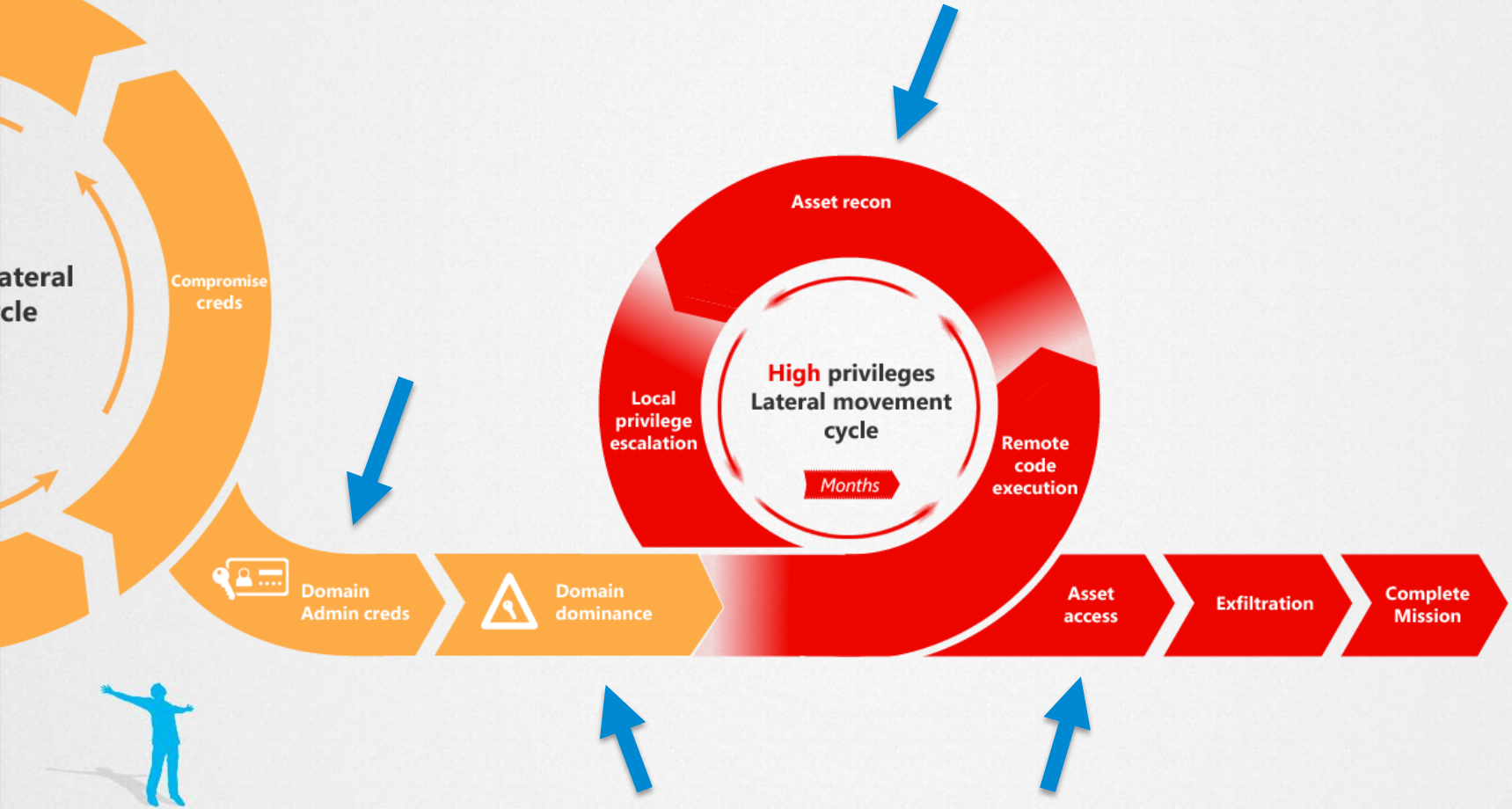

Admin recon
Low privileges Lateral movement cycle
Week
Remote code execution
Compromise creds
External Recon
Compromised machine
Internal Recon
Local privilege escalation
Domain Admin creds
Domain dominance

Bereikt tot zover

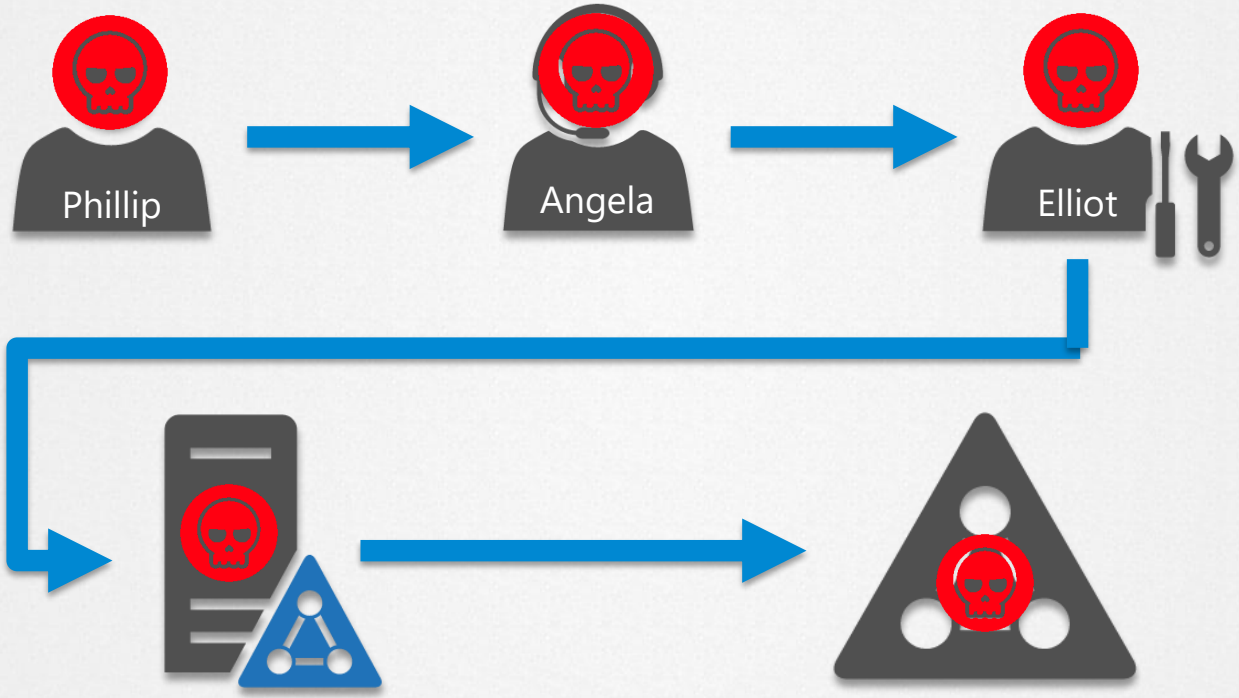
Domain Domination

- Dump hash KRBTGT account
- Creëren Golden Ticket
- Import Golden Ticket
- Toegang tot alle resources


Microsoft Advanced Thr
Certificate error
10.0.0.5/timeline?status=Open&severity=All
Microsoft Advanced Threat Analytics
Search users, computers, servers, and more...
Microsoft
Filter by
All [18]
Open [3]
High [0]
Medium [3]
Low [0]
Resolved [11]
Dismissed [4]
10:24 PM
Thursday, November 3, 2016
10:19 PM
Friday, November 4, 2016
Unusual protocol implementation
Angela Moss successfully authenticated from WIN8 agai
as Pass-the-Hash and brute force.
Note
Share
Export to Excel
Details
On
Angela Moss
Service Desk Employee
WIN8
Recommendations
Disconnect WIN8 from the network, or move it into an isolated
Investigate the root cause on WIN8
Reset Angela Moss's password
4:56 PM
Monday, October 24, 2016
10:19 PM
Friday, November 4, 2016
Reconnaissance using SMB Session Enumeratio
SMB session enumeration attempts were successfully per
Note
Share
Export to Excel
Details
On
2 accounts
WIN8
controllers
EL_DEMO_CLIENT_WIN8 on PRECISION - Virtual Machine Connection
File
Action
Media
View
Help
Recycle Bin
Administrator: C:\Windows\SYSTEM32\cmd.exe
c:\Pwnage>
22:37
4-11-2016
Status: Running
Suspicious Activity
Unusual protocol implementation
2 hours ago
Suspicious Activity
Reconnaissance using SMB Session Enumeration
2 hours ago
Suspicious Activity
Reconnaissance using directory services enumeration
2 hours ago


ateral
cle
Compromise creds
Asset recon
High privileges
Lateral movement cycle
Months
Local privilege escalation
Remote code execution
Domain Admin creds
Domain dominance
Asset access
Exfiltration
Complete Mission

Pwnage! Mission Accomplished



Filter by
All [20]
Open [7]
High [2]
Medium [5]
Low [0]
Resolved [10]
Dismissed [3]

angela
on 10.0.0.11

WIN8$
on 10.0.0.11

Recommendations
- Disconnect WIN8 from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Verify that all enumerated accounts use a strong password.

10:19 PM
Thursday, November 3, 2016

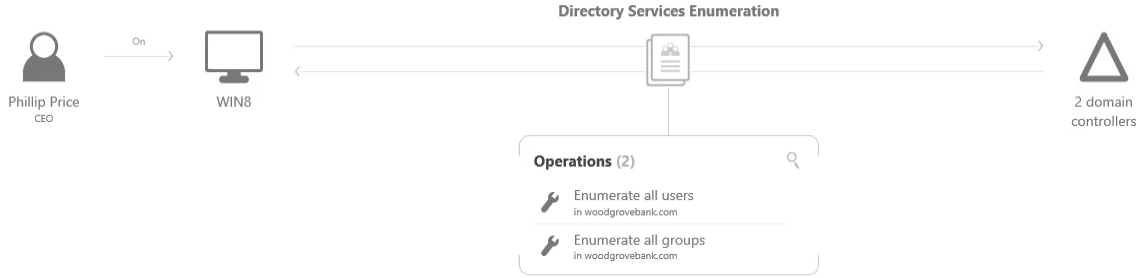
10:19 PM
Friday, November 4, 2016

Reconnaissance using directory services enumeration

The following directory services enumerations using SAMR protocol were attempted against 2 domain controllers from WIN8:

- Successful enumeration of all users in woodgrovebank.com by Phillip Price
- Successful enumeration of all groups in woodgrovebank.com by Phillip Price

Note Share Export to Excel Details Input Open



Recommendations
- Disconnect WIN8 from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more

1:17 PM

Health Issue
Gateway stopped communicating
a few seconds ago
Health Issue
Gateway stopped communicating
a few seconds ago
Suspicious Activity
Brute force attack using LDAP simple bind
4 minutes ago
Suspicious Activity
Encryption downgrade activity
4 minutes ago
Suspicious Activity
Identity theft using Pass-the-Ticket attack
4 minutes ago
Suspicious Activity
Malicious replication of directory services
4 minutes ago

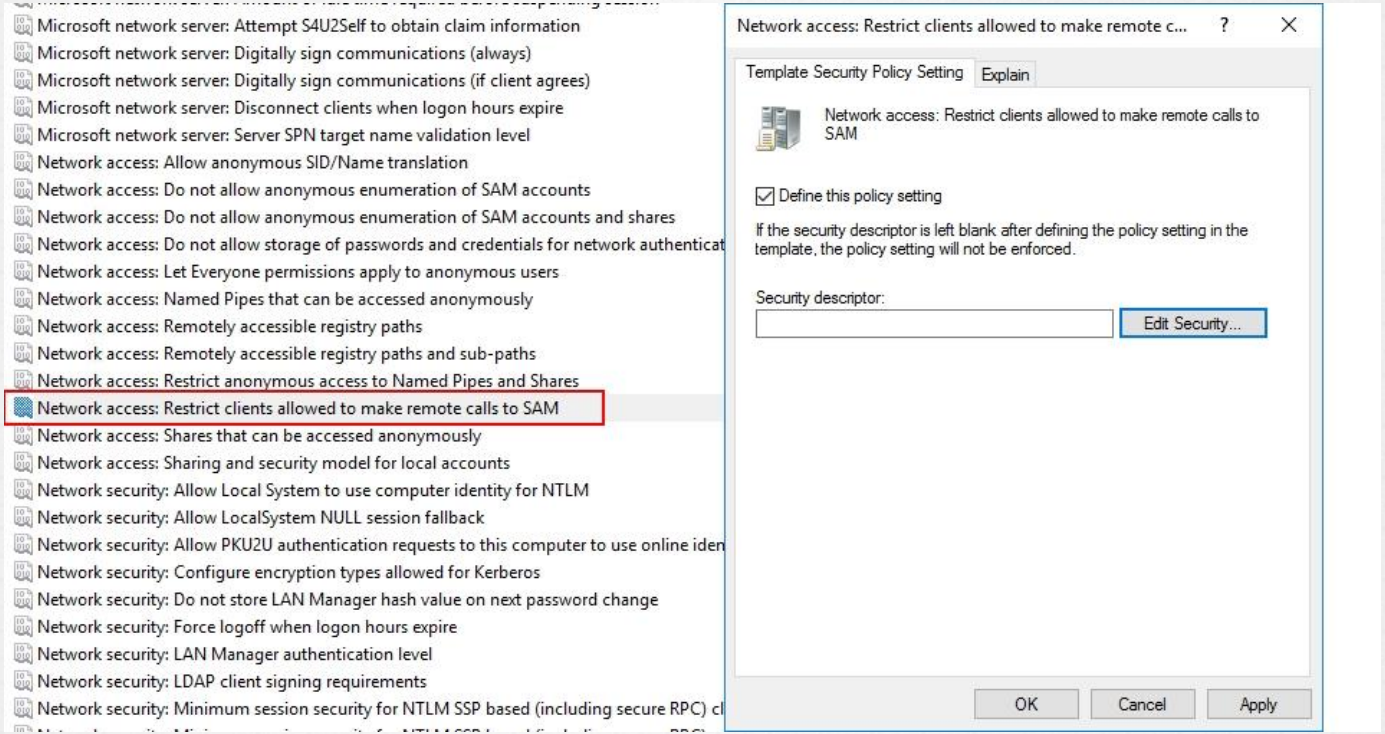
Mitigation

Verkenning (reconnaissance)

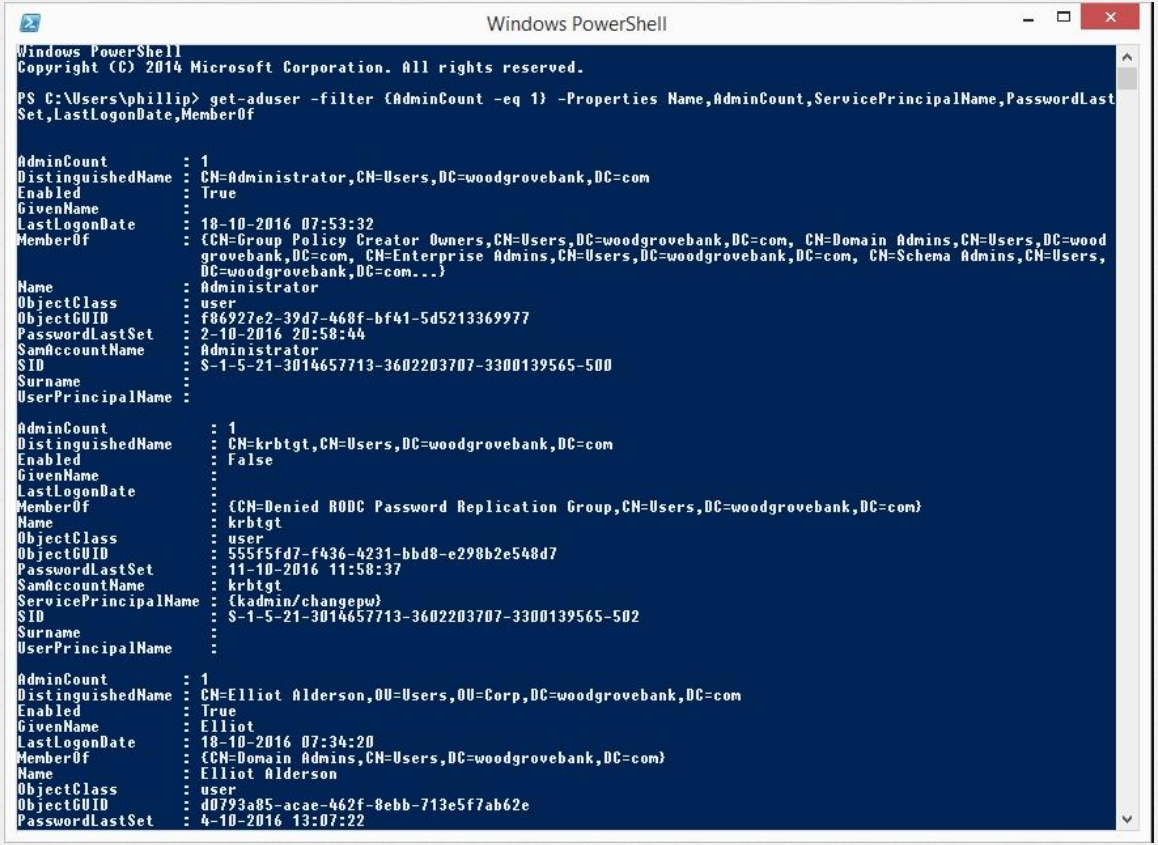
1. SAM-R

SAM-R

RestrictRemoteSAM registry (GPO) (Win10/Server 2016)



get-aduser -filter {AdminCount -eq 1} -Properties Name,AdminCount,ServicePrincipalName,PasswordLastSet,LastLogonDate,MemberOf



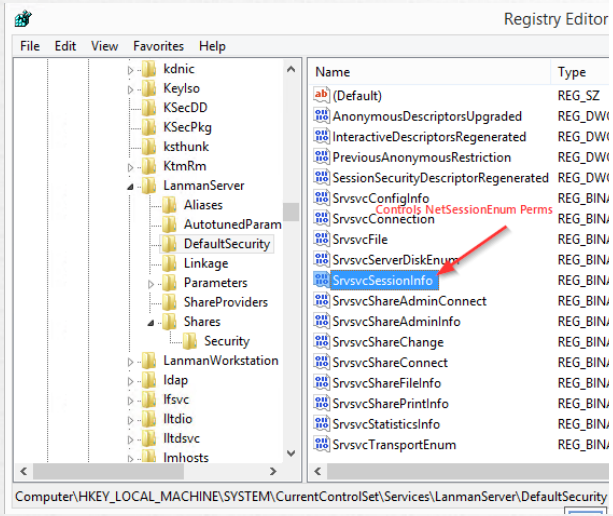
Verkenning (reconnaissance)

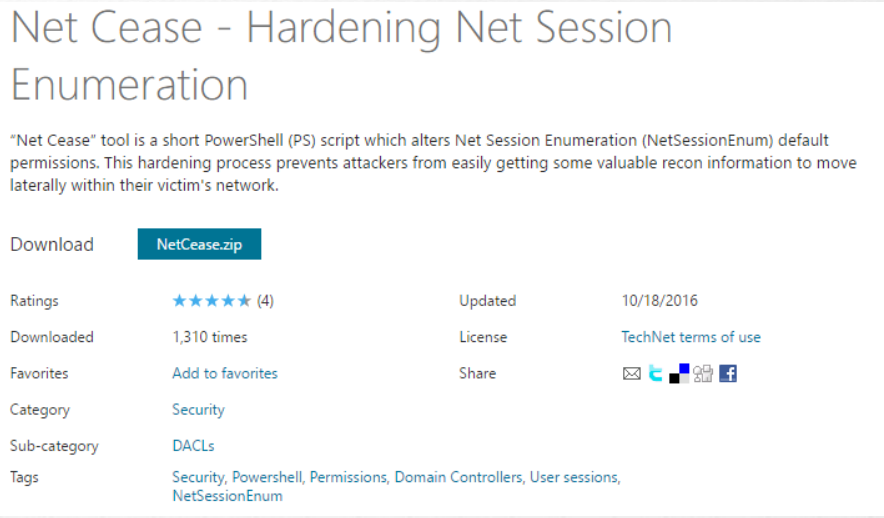
1. SAM-R
   RestrictRemoteSAM registry (GPO)
2. NetSess

SMB Session Enumeration (NetSess.exe)

- Administrators group (Security Identifier (Sid) S-1-5-32-544)
- Server Operators group (Sid S-1-5-32-549)
- Power Users group (Sid S-1-5-32-547)
- Authenticated Users group (Sid S-1-5-11)

Net Cease download: https://gallery.technet.microsoft.com/Net-Cease-Blocking-Net-1e8dcb5b





Verkenning (reconnaissance)

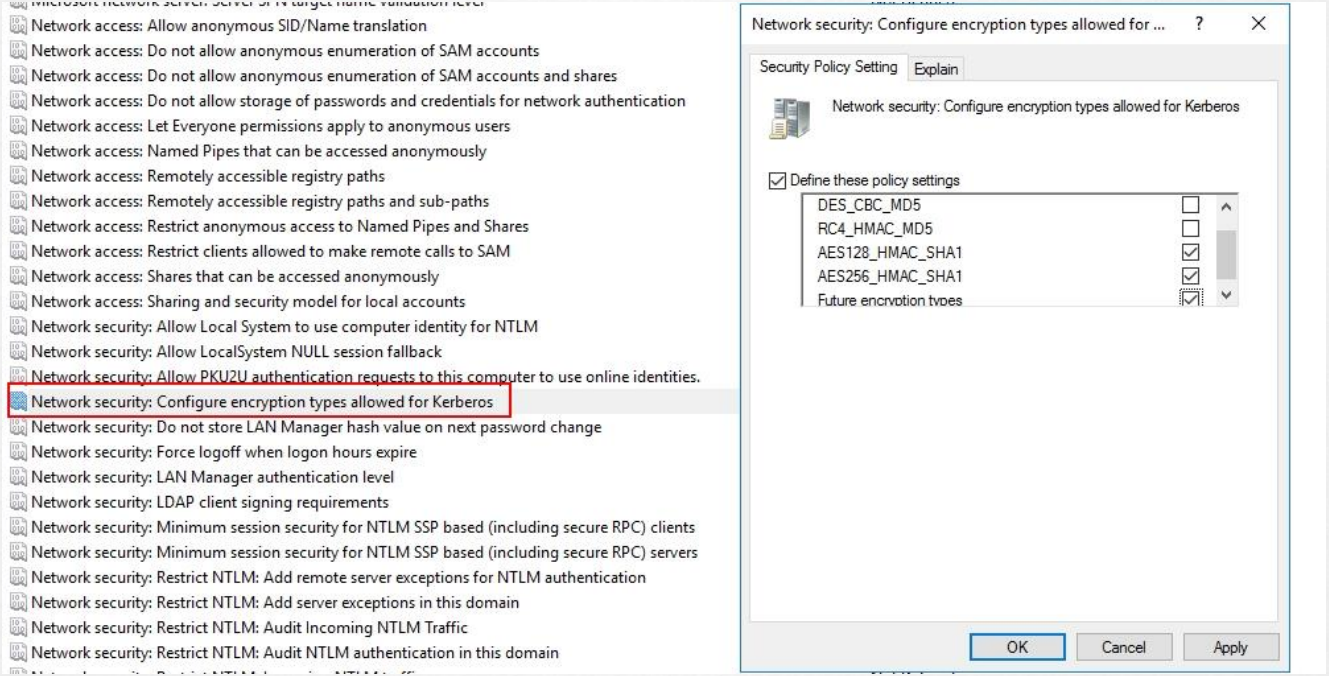
1. SAM-R
   RestrictRemoteSAM registry (GPO)
2. NetSess
   Verwijderen ‘authenticated users’ permissie

Lateral Movement

3. Over-pass-the-hash

Over-pass-the-hash

Zwakke Kerberos encryptie uitschakelen! DES, RC4. Enkel AES128/256 gebruiken



Verkenning (reconnaissance)

1. SAM-R
   RestrictRemoteSAM registry (GPO)
2. NetSess
   Verwijderen ‘authenticated users’ permissie

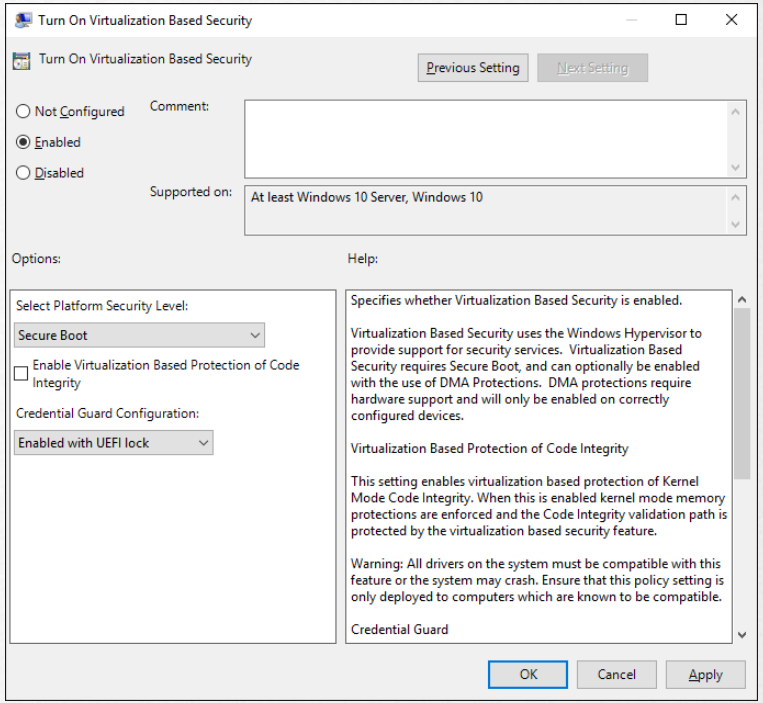
Lateral Movement

3. Over-pass-the-hash
   Zwakke Kerberos encryptie uitschakelen!
4. Pass-the-Ticket

Pass-the-Ticket

Credential Guard

- Hardware eisen
- Intel VT-D of AMD Vi IOMMU
- TPM 1.2 of 2.0
- UEFI 2.3.1c+
- UEFI Secure Boot
- Windows 10
- Lijst wordt langer



Verkenning (reconnaissance)

1. SAM-R
   RestrictRemoteSAM registry (GPO)
2. NetSess
   Verwijderen ‘authenticated users’ permissie

Lateral Movement

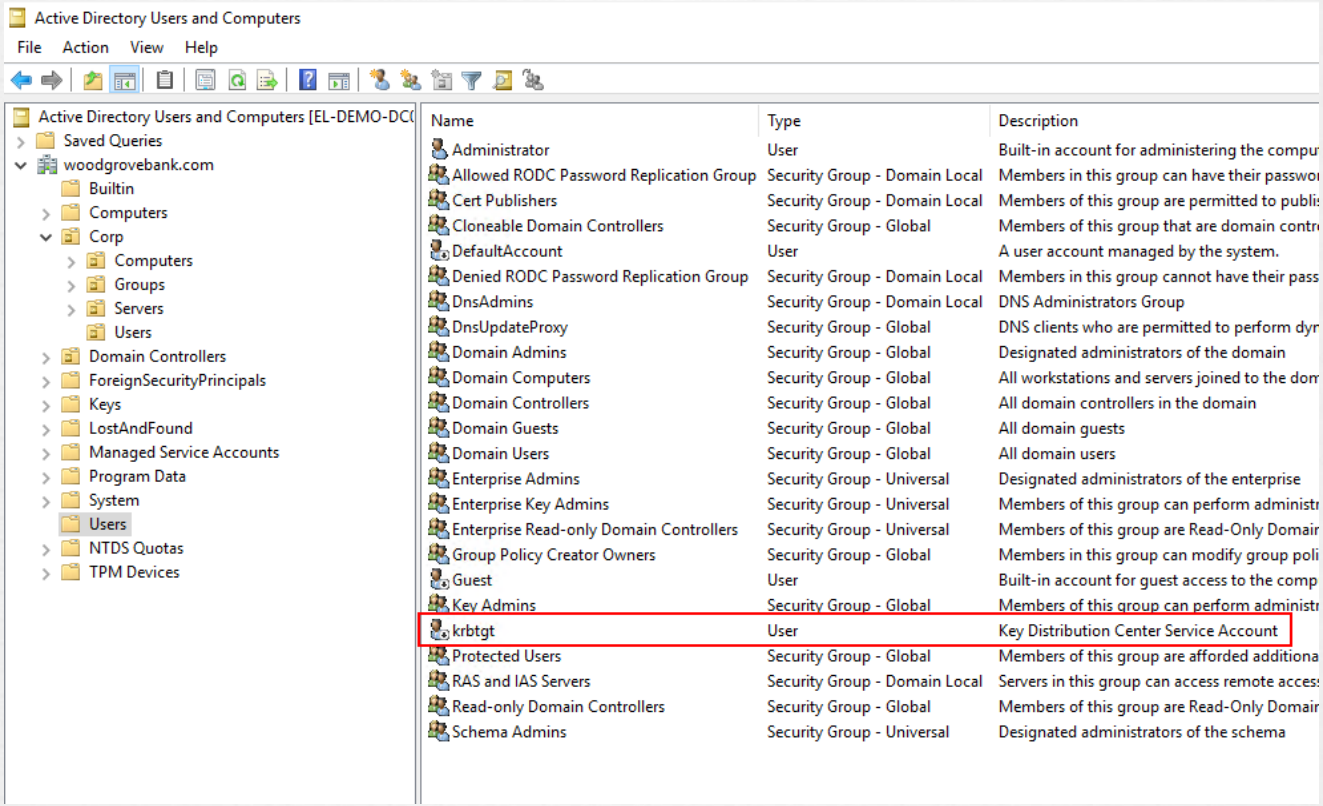
3. Over-pass-the-hash
   Zwakke Kerberos encryptie uitschakelen!
4. Pass-the-Ticket
   Credential Guard

Domain Domination

5. Compromitteren KRBTGT account (DcSync)
6. Golden Ticket

KRBTGT account, Golden Ticket

Enkel detectie



Verkenning (reconnaissance)

1. SAM-R
   RestrictRemoteSAM registry (GPO)
2. NetSess
   Verwijderen ‘authenticated users’ permissie

Lateral Movement

3. Over-pass-the-hash
   Zwakke Kerberos encryptie uitschakelen!
4. Pass-the-Ticket
   Credential Guard

Domain Domination

5. Compromitteren KRBTGT account (DcSync)
   Enkel detectie
6. Golden Ticket
   Reset KRBTGT account 2x

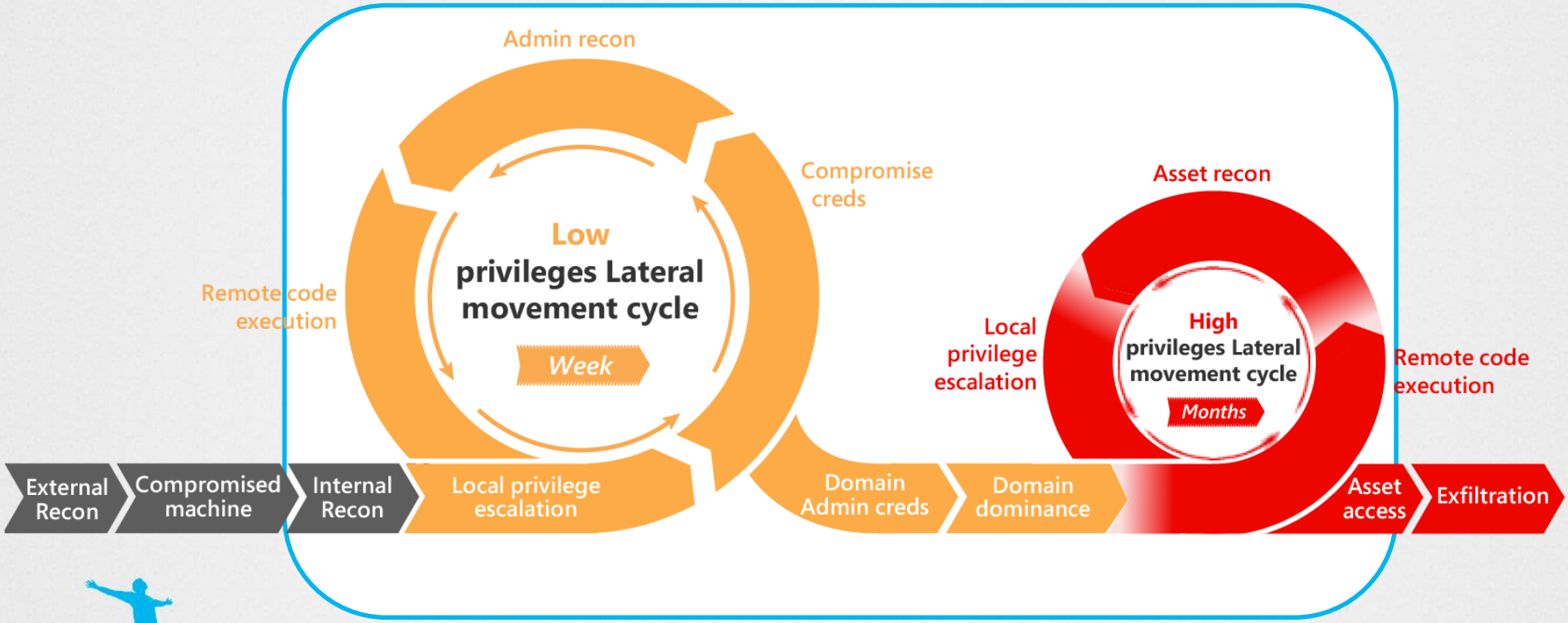
Pas bestaande technieken toe!

Protected Users Group

Kerberos Armoring (FAST)

Authentication Policies & Silos

Samenvatting



Bron: Michael Dubinsky, PM Microsoft ATA

Q&A

Volgende sessie 9:00 – 10:00 uur

Keynote: “Reinvent IT infrastructure for business agility”

Lorenzo Rizzi

Expo Theater

Experts Live 2016