
NIC
2019
Artificial Edition
6-8 February
Hasain "The Wolf of TRUESEC" @Alshakarti

Securing Privileged Access FIRST

Hasain “The Wolf” @Alshakarti

TRUESEC

Hasain “The Wolf” Alshakarti @ TRUESEC

Trusted Cyber Security Advisor

Twitter: @Alshakarti

Linkedin: https://se.linkedin.com/in/hasain

Attackers Mindset

Identify High Value Targets

- Domain controllers, certification authorities, jump servers, admin clients ...

Identify Privileged Accounts

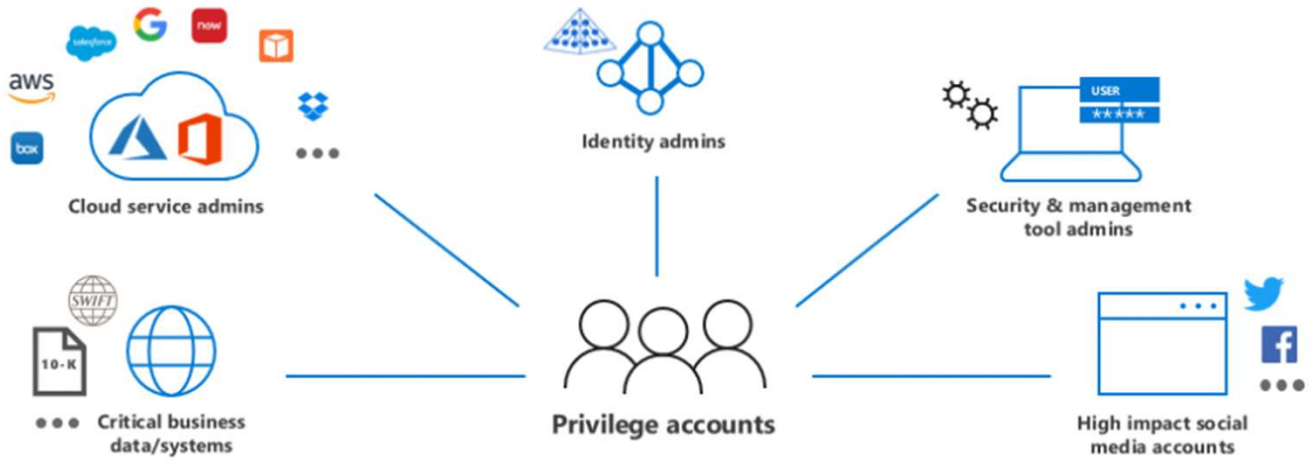
- Who are the administrators on these servers

Gain Access to Amin Credentials

- What can be compromised to get the credentials of a target user

Privileged access is more than administrators

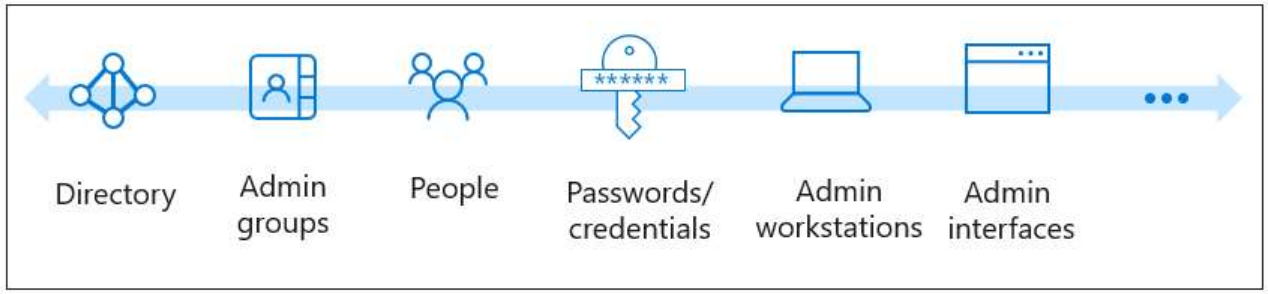
Protect high impact accounts/roles

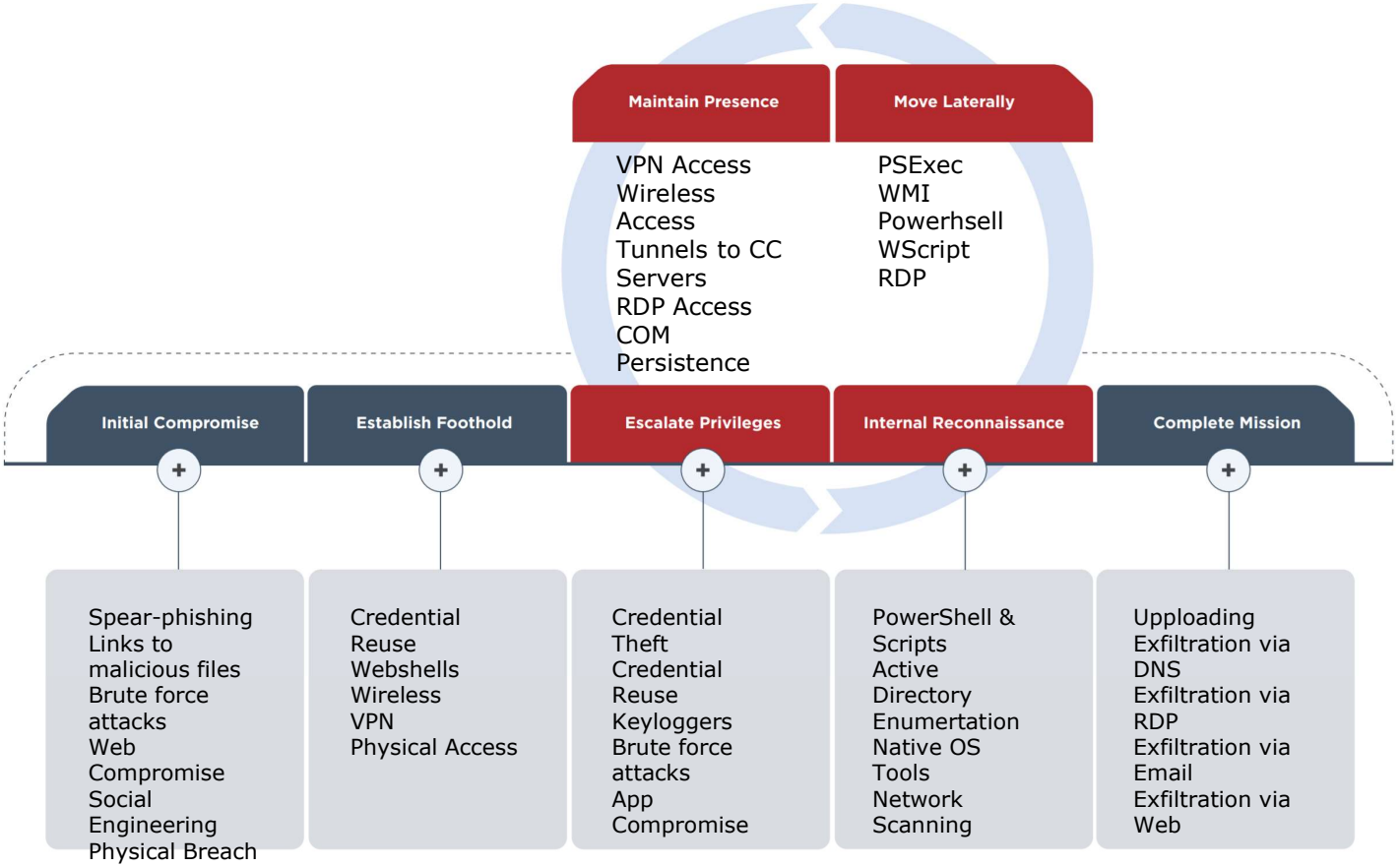


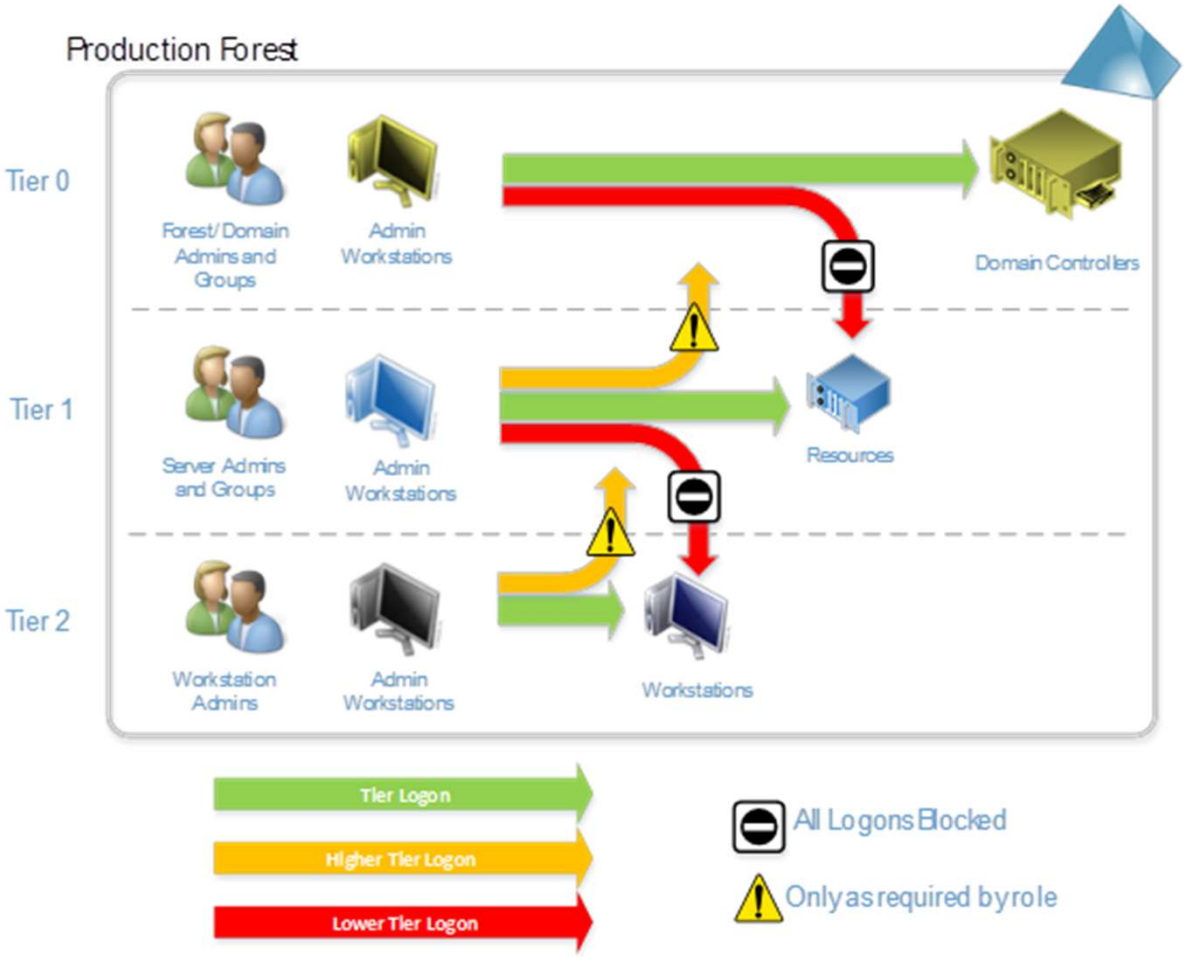
Securing privileged access

More than just vaulting admin passwords

Protect all parts of the privileged lifecycle




Maintain Presence
Move Laterally
VPN Access
Wireless Access
Tunnels to CC Servers
RDP Access
COM
Persistence
PSExec
WMI
Powerhsell
WScript
RDP
Initial Compromise
Establish Foothold
Escalate Privileges
Internal Reconnaissance
Complete Mission
Spear-phishing Links to malicious files
Brute force attacks
Web Compromise
Social Engineering
Physical Breach
Credential Reuse
Webshells
Wireless
VPN
Physical Access
Credential Theft
Credential Reuse
Keyloggers
Brute force attacks
App Compromise
PowerShell & Scripts
Active Directory Enumertation
Native OS Tools
Network Scanning
Uppoading
Exfiltration via DNS
Exfiltration via RDP
Exfiltration via Email
Exfiltration via Web


Production Forest
Tier 0
Forest/Domain Admins and Groups
Admin Workstations
Domain Controllers
Tier 1
Server Admins and Groups
Admin Workstations
Resources
Tier 2
Workstation Admins
Admin Workstations
Workstations
Tier Logon
Higher Tier Logon
Lower Tier Logon
All Logons Blocked
Only as required by role

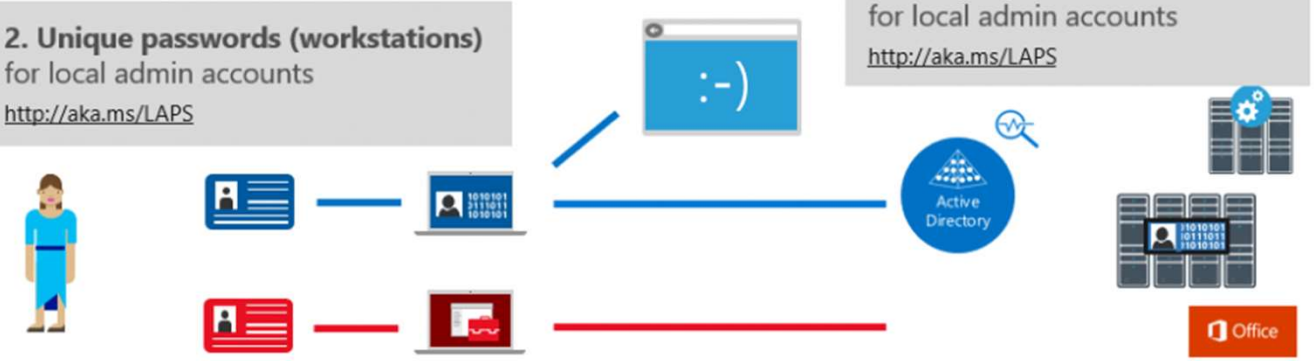
First month - securing privileged access for on-premises AD

30 Days | 90 Days | Beyond

Quick wins with significant impact

2. Unique passwords (workstations)
for local admin accounts
http://aka.ms/LAPS

3. Unique passwords (servers)
for local admin accounts
http://aka.ms/LAPS



1. Separate accounts
for admin vs. productivity tasks

4. PAW stage 1 – Perform admin work from higher security device
http://aka.ms/HighSecWin10

5. Identity attack detection
http://aka.ms/azureatp or 3rd party

First quarter - securing privileged access for on-premises AD

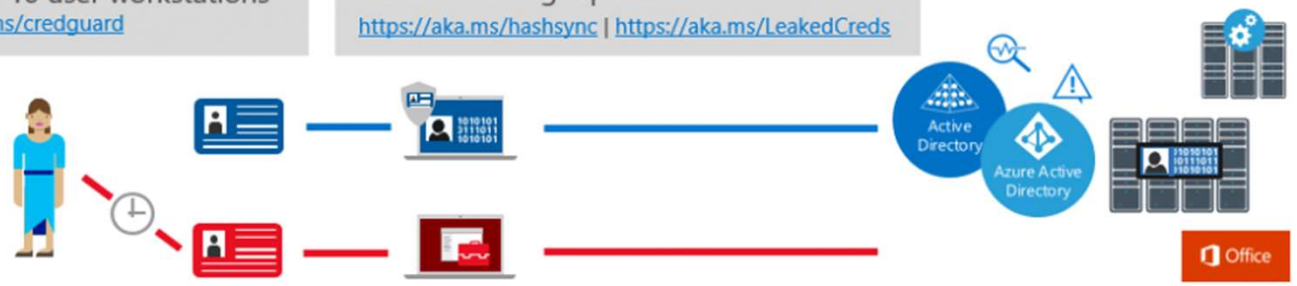
30 Days | 90 Days | Beyond

Key protections that provide significant mitigation

4. Enable credential guard on Windows 10 user workstations
http://aka.ms/credguard

5. Leaked credentials 1 - Detect risk by synchronizing password hashes to Azure AD & reviewing reports
https://aka.ms/hashsync | https://aka.ms/LeakedCreds

6. Lateral movement vulnerability detection
http://aka.ms/LateralMovementRisk



1. Require Windows Hello for business for administrative accounts
http://aka.ms/HelloForBusiness

2. PAW stage 2 – Require separate admin workstations for AD admins
Phase 1 Instructions of http://aka.ms/CyberPAW

3. Just in time privileges using privileged access management (PAM) solution
http://aka.ms/PAM or 3rd party

Beyond - securing privileged access for on-premises AD

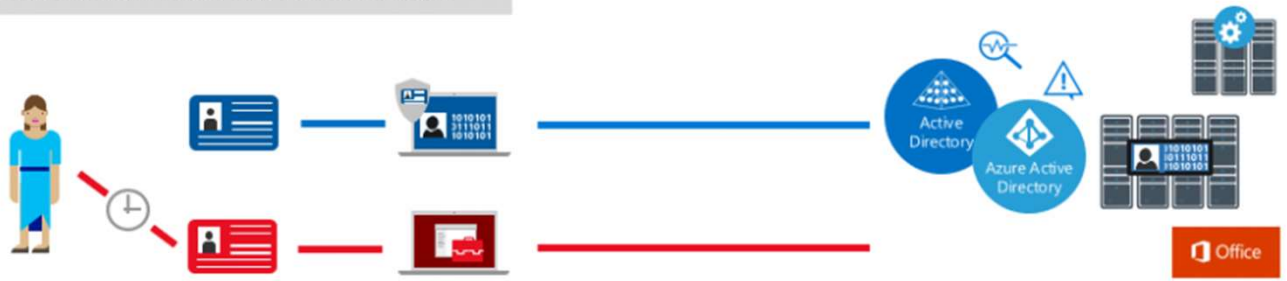
30 Days > 90 Days > Beyond

Proactively increase security posture

1. Review role-based access control (RBAC) model to reduce risk from tier combinations

4. Leaked credentials 2 - force reset of passwords using conditional access and self-service password reset

https://aka.ms/CAPolicy | https://aka.ms/selfservicepasswordreset

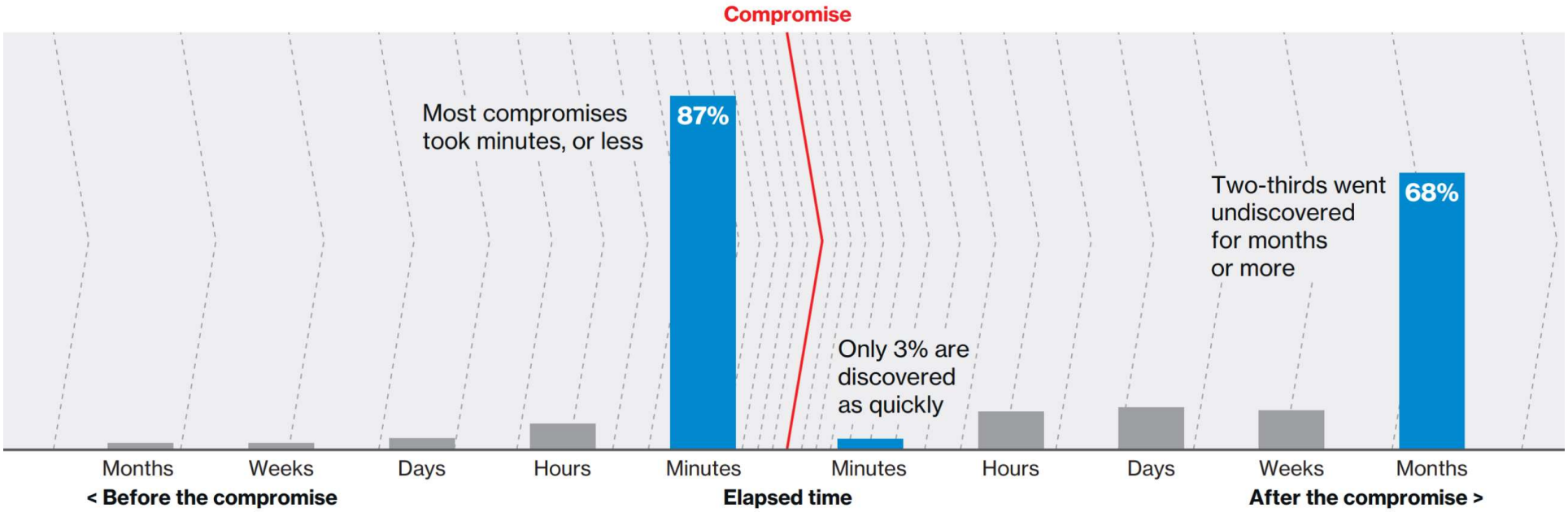


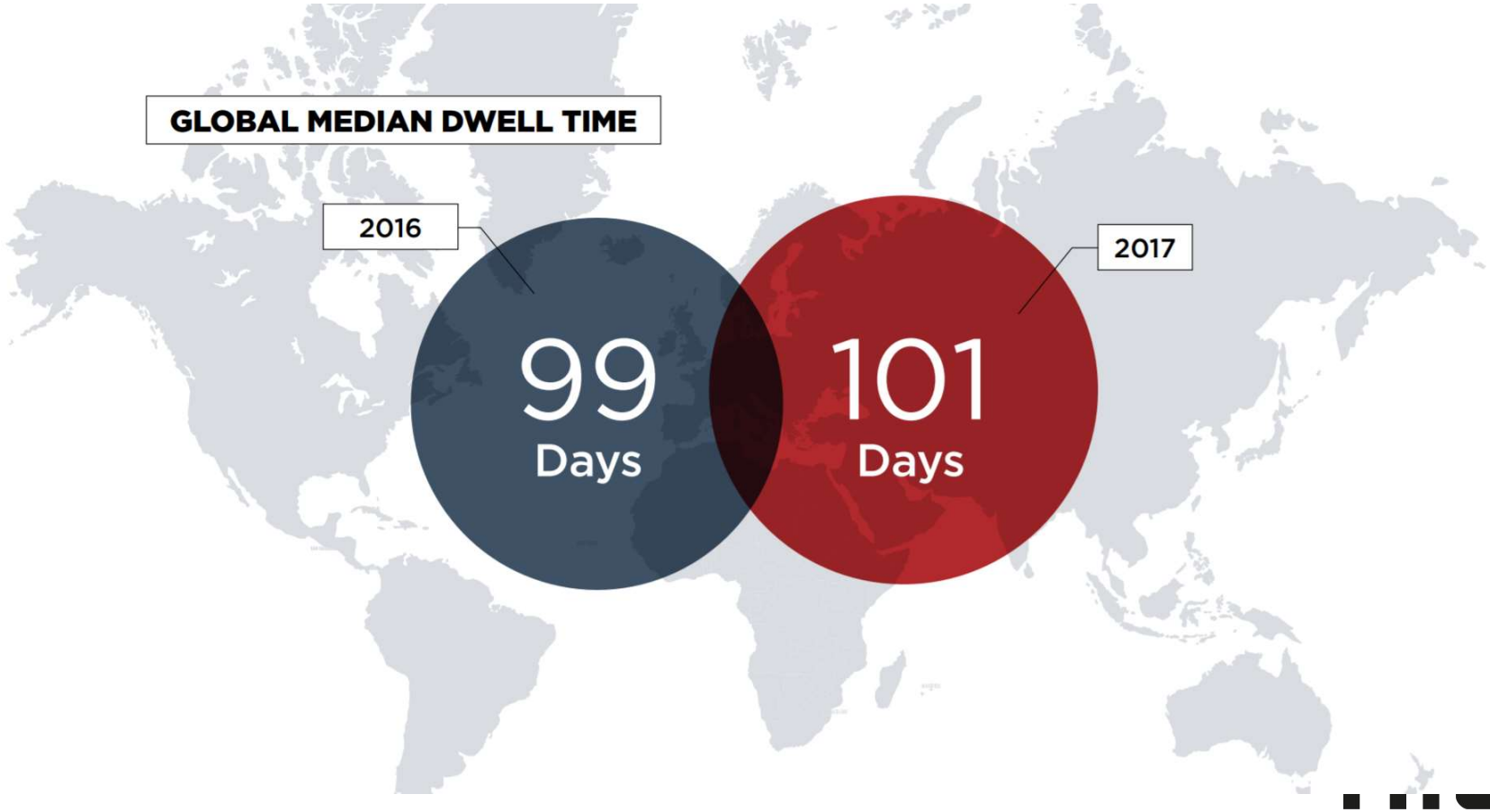
2. PAW stage 3 – Expand PAW to a program protecting all admins

Phases 2 and 3 of http://aka.ms/cyberPAW

3. Lower attack surface of domain and DC

http://aka.ms/hardenAD


Compromise
Most compromises took minutes, or less
87%
Only 3% are discovered as quickly
Two-thirds went undiscovered for months or more
68%
Months
Weeks
Days
Hours
Minutes
Minutes
Hours
Days
Weeks
Months
< Before the compromise
Elapsed time
After the compromise >


GLOBAL MEDIAN DWELL TIME
2016
99
Days
2017
101
Days

Sample Server Support

Remote server support

- **Primary (tool)** - Remote tools using network logons (type 3)
- **Primary (interactive)** RDP (RemoteGuard / RestrictedAdmin / AMA) from PAW
- **Secondary** - Logon using a local account password set by LAPS
- **Forbidden** - Standard RDP with domain account
- **Forbidden** - Using domain accounts while in the session

Physical server support

- **Primary** - Log on using a local account password set by LAPS
- **Forbidden** - Logon with a domain account
- **Forbidden** - Using domain accounts while in the session

Sample User Support

Desk-side user support

- **Primary** - "Over the shoulder" support can be provided with no tools
- **Secondary** - Logon using a local account password set by LAPS
- **Forbidden** - Logon with domain account with administrative credentials

Remote user support

- **Primary** - Remote Assistance, Skype for Business, or similar screen sharing
- **Secondary** - Logon using a local account password set by LAPS
- **Forbidden** - Logon with domain account administrative credentials

Recommended Reading

Securing Privileged Access (on-premises)
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access

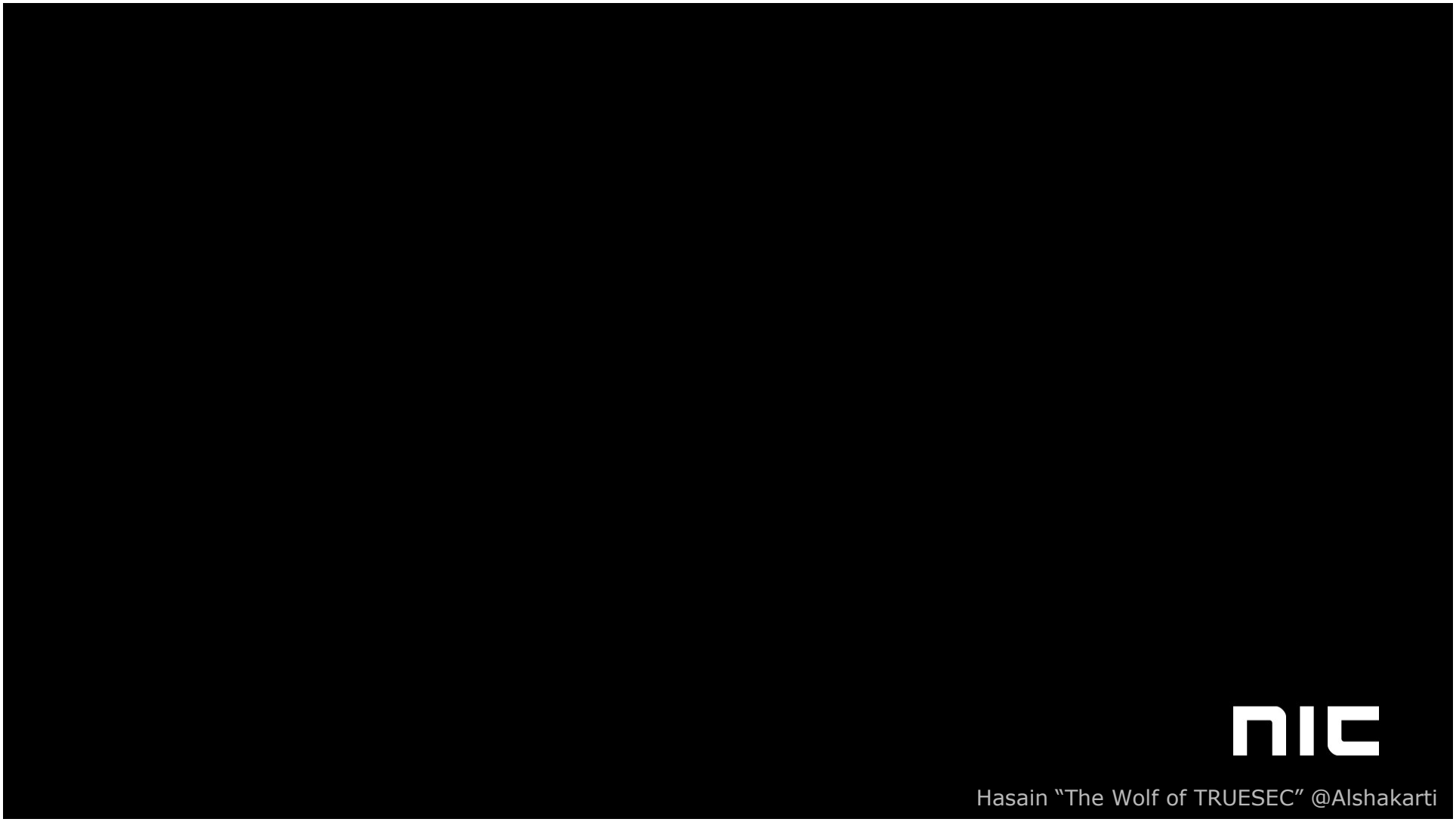
Securing privileged access for hybrid and cloud deployments in Azure AD
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-admin-roles-secure

Windows 10 Credential Theft Mitigation Guide
https://www.microsoft.com/en-us/download/details.aspx?id=54095

Privileged Account Management for the Financial Services Sector (Draft)
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/fs-pam-nist-sp1800-18-draft.pdf

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2019


Hasain “The Wolf of TRUESEC” @Alshakarti