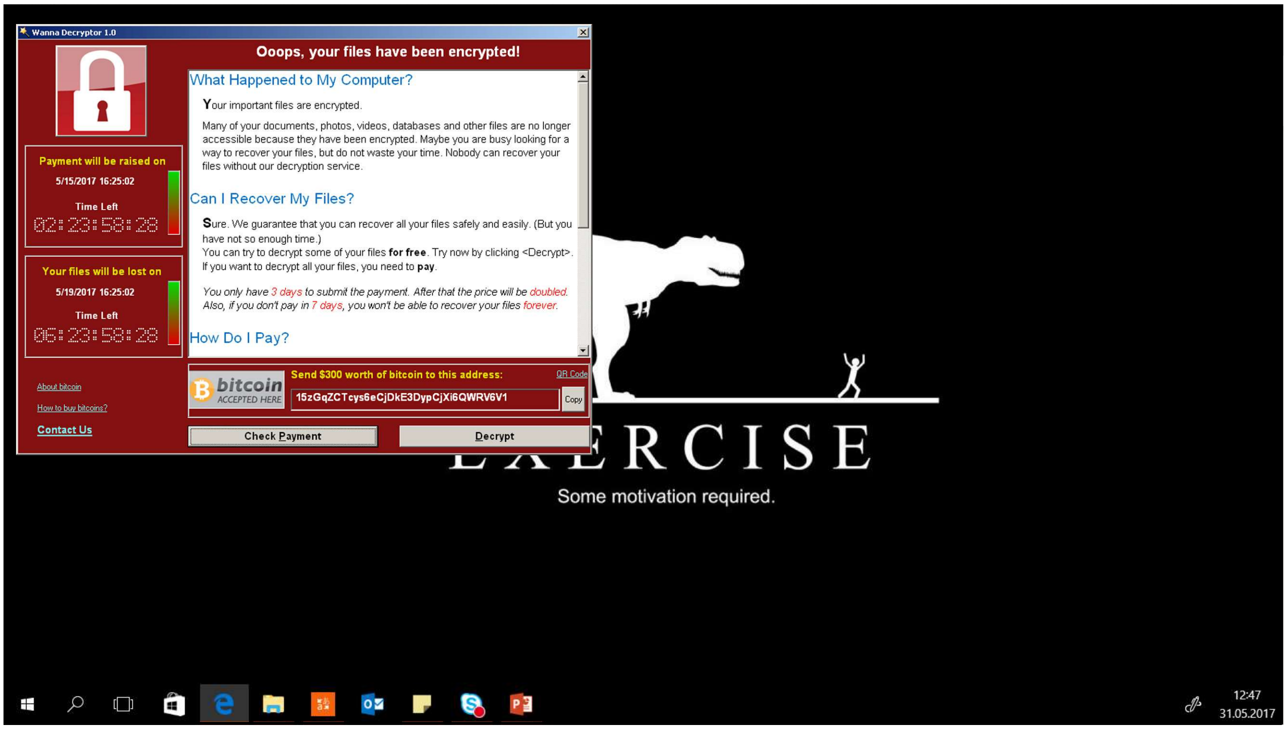


Wanna Decryptor 1.0

Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28

Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Send $300 worth of bitcoin to this address:
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

ITechDays

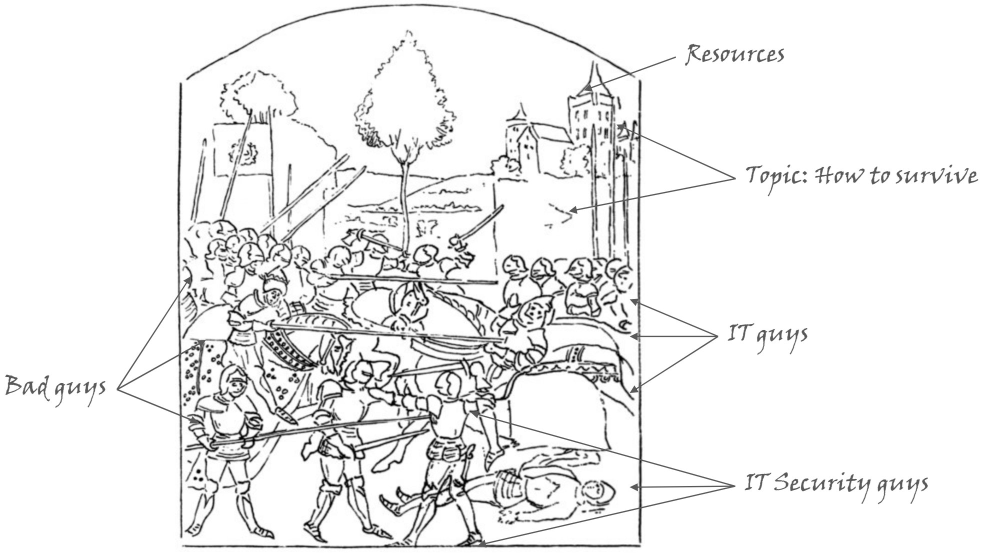
1-2 czerwca **2017**

How to build my own Castle – securing administrator access to infrastructure.
Why and How?

Marek Pyka Ph.D.
Microsoft Solutions Architect
Security and Cloud Infrastructure
mailto: marpy @ microsoft.com

AGENDA

ITechDays

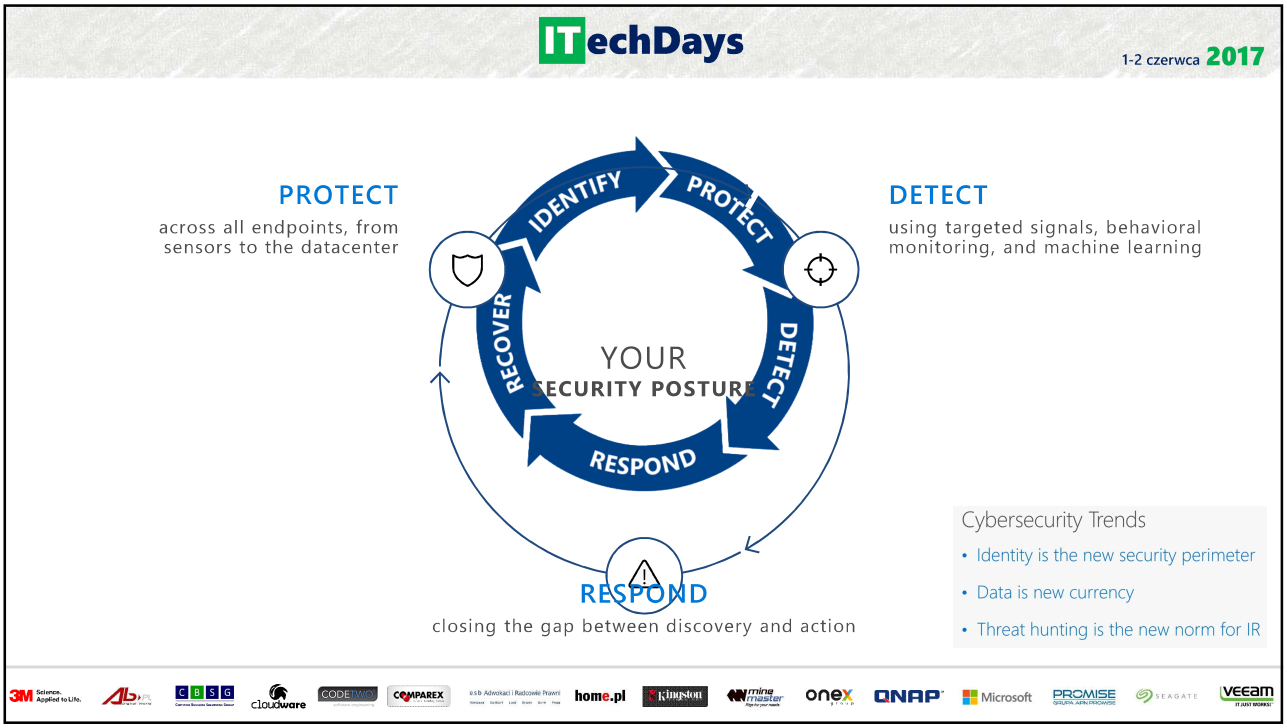


3M Science. Applied to Life. | AB.PL | CBSG | cloudware | CODETWO | COMPAREX | esb Adwokaci i Radcowie Prawni | home.pl | Kingston | mine master | onex | QNAP | Microsoft | PROMISE | SEAGATE | VEEAM IT JUST WORKS

CYBER SECURITY

THREATS

VIDEO



ITechDays

1-2 czerwca 2017

PROTECT

across all endpoints, from sensors to the datacenter

DETECT

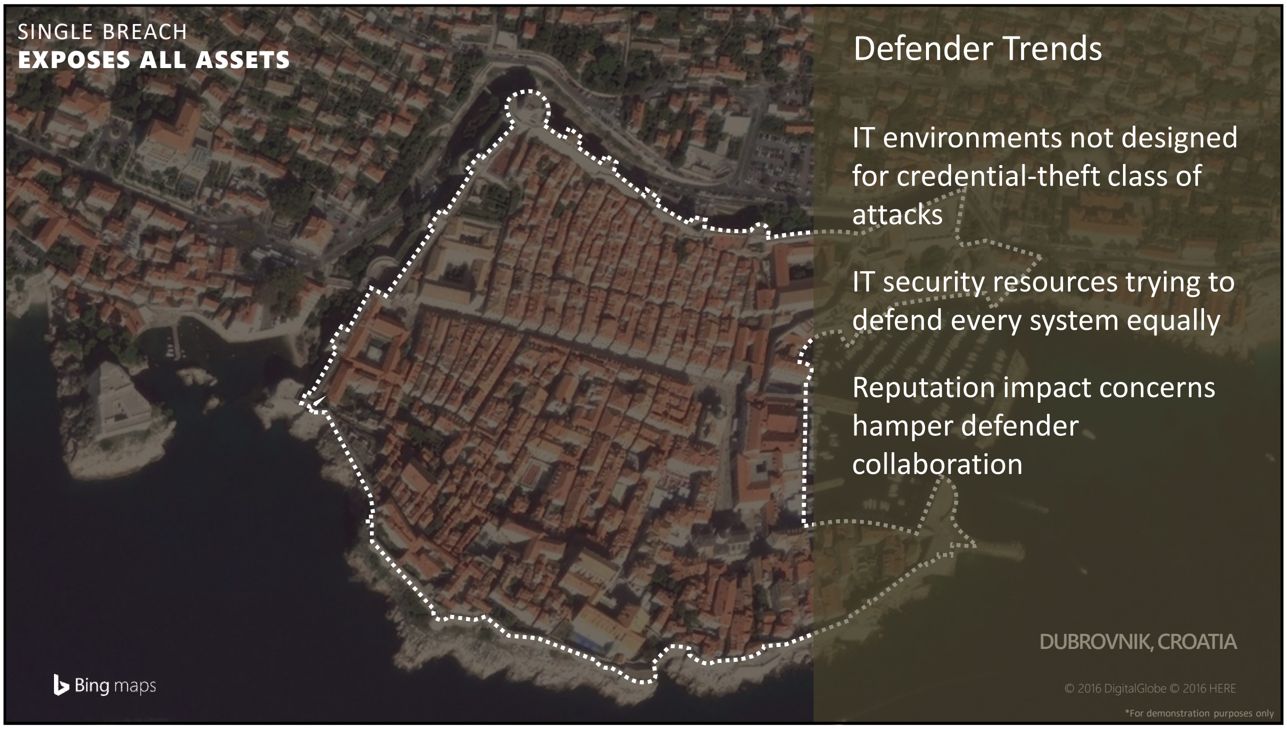
using targeted signals, behavioral monitoring, and machine learning

RESPOND

closing the gap between discovery and action

Cybersecurity Trends

- Identity is the new security perimeter
- Data is new currency
- Threat hunting is the new norm for IR



SINGLE BREACH
EXPOSES ALL ASSETS

Defender Trends

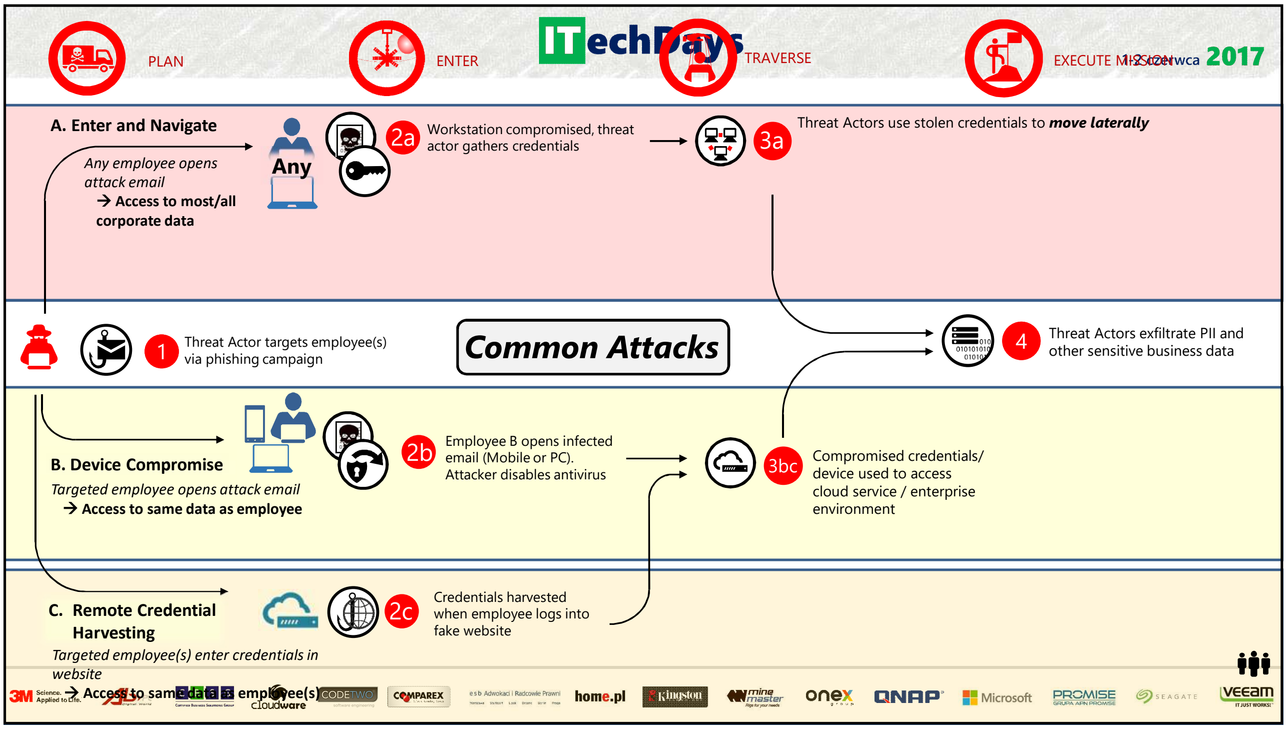
IT environments not designed for credential-theft class of attacks

IT security resources trying to defend every system equally

Reputation impact concerns hamper defender collaboration

© 2016 DigitalGlobe © 2016 HERE

*For demonstration purposes only



Common Attacks

A. Enter and Navigate

Any employee opens attack email
→ Access to most/all corporate data

2a Workstation compromised, threat actor gathers credentials

3a Threat Actors use stolen credentials to ***move laterally***

1 Threat Actor targets employee(s) via phishing campaign

4 Threat Actors exfiltrate PII and other sensitive business data

B. Device Compromise

Targeted employee opens attack email
→ Access to same data as employee

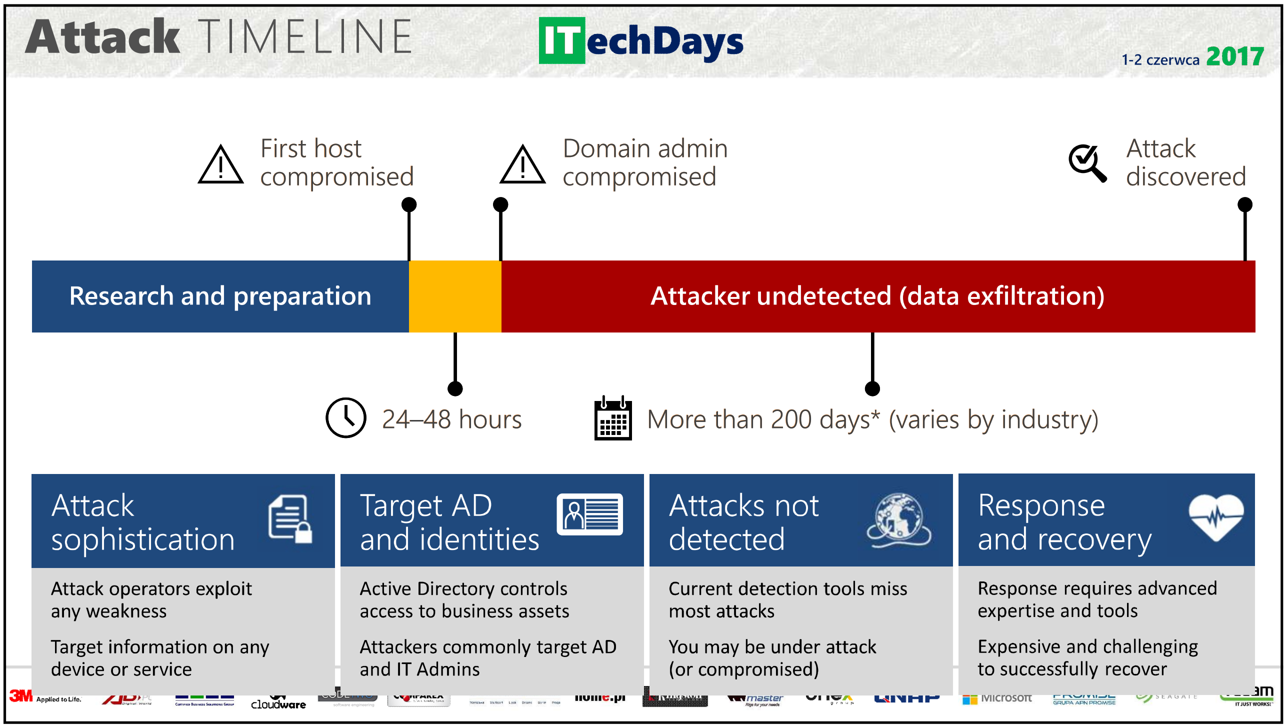
2b Employee B opens infected email (Mobile or PC). Attacker disables antivirus

3bc Compromised credentials/ device used to access cloud service / enterprise environment

C. Remote Credential Harvesting

Targeted employee(s) enter credentials in website
→ Access to same data as employee(s)

2c Credentials harvested when employee logs into fake website



Attack TIMELINE

Attack sophistication

Attack operators exploit any weakness

Target information on any device or service

Target AD and identities

Active Directory controls access to business assets

Attackers commonly target AD and IT Admins

Attacks not detected

Current detection tools miss most attacks

You may be under attack (or compromised)

Response and recovery

Response requires advanced expertise and tools

Expensive and challenging to successfully recover

Ceredential Thief

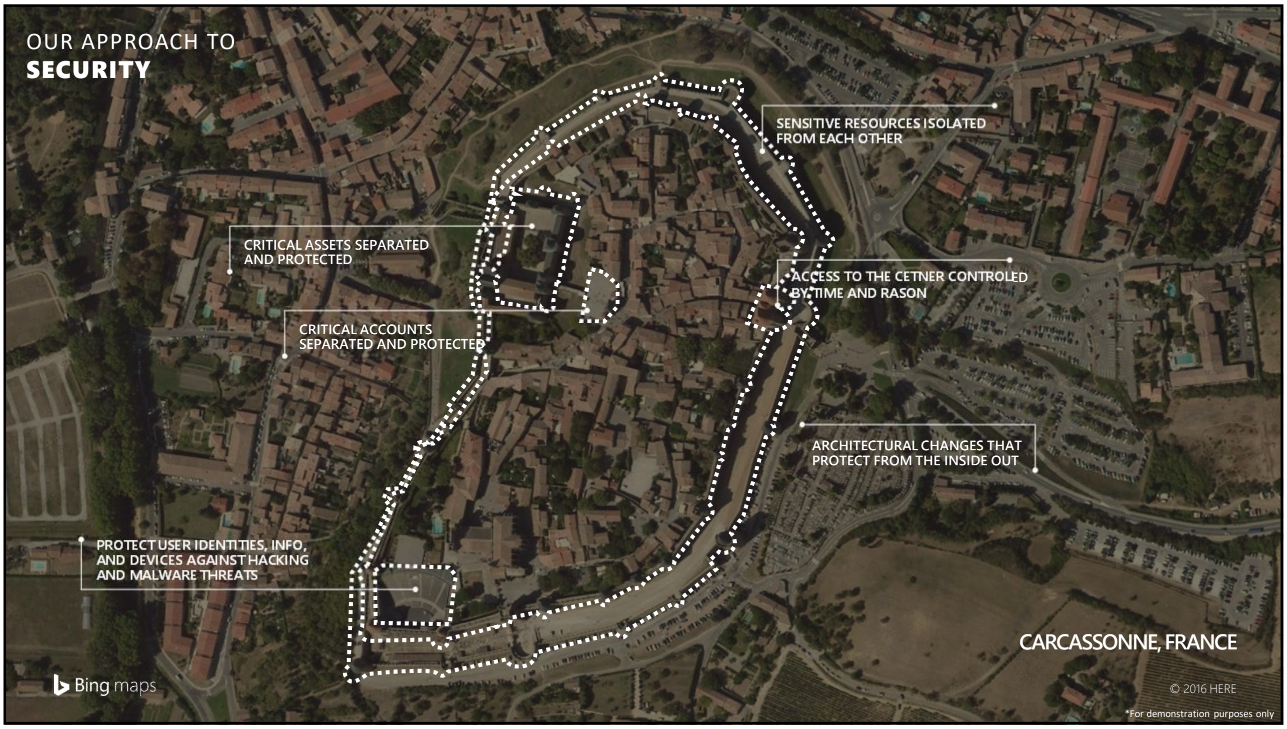
DEMO

http://aka.ms/credtheftdemo

ITechDays

SOLUTION

ITechDays



OUR APPROACH TO
SECURITY

SENSITIVE RESOURCES ISOLATED FROM EACH OTHER

CRITICAL ASSETS SEPARATED AND PROTECTED

ACCESS TO THE CETNER CONTROLED BY TIME AND RASON

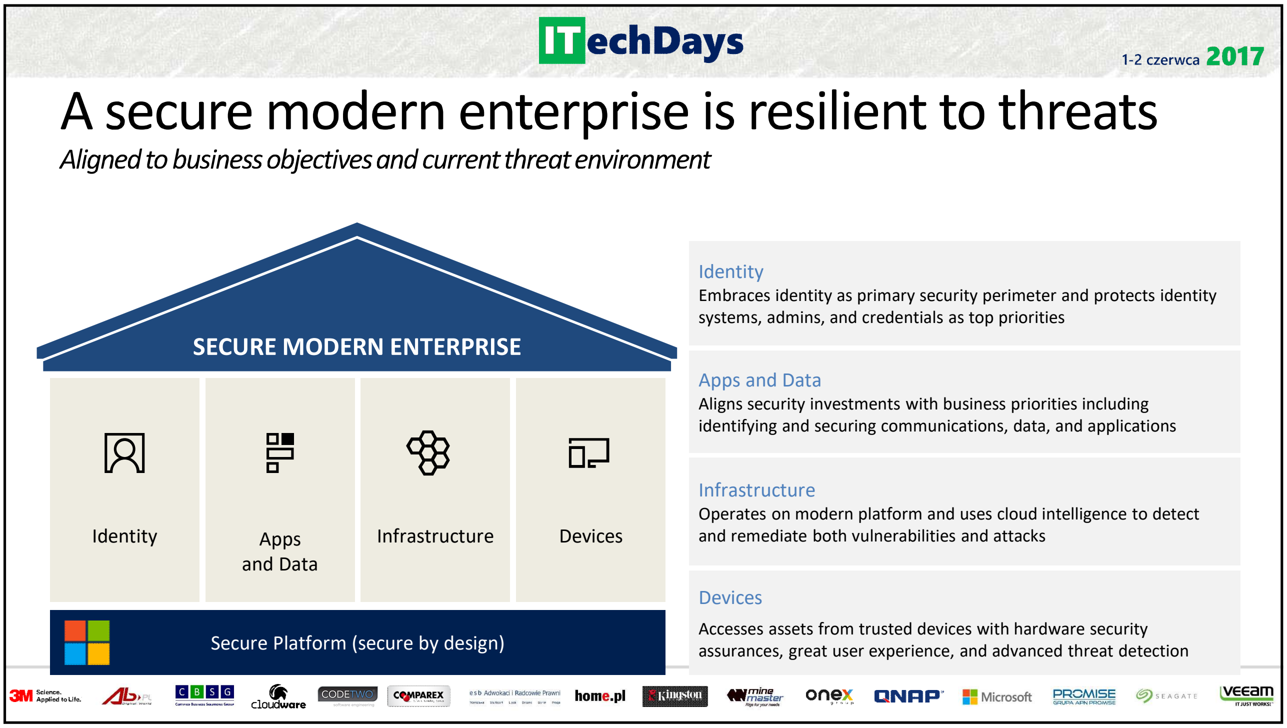
CRITICAL ACCOUNTS SEPARATED AND PROTECTED

ARCHITECTURAL CHANGES THAT PROTECT FROM THE INSIDE OUT

PROTECT USER IDENTITIES, INFO, AND DEVICES AGAINST HACKING AND MALWARE THREATS

CARCASSONNE, FRANCE

*For demonstration purposes only



A secure modern enterprise is resilient to threats

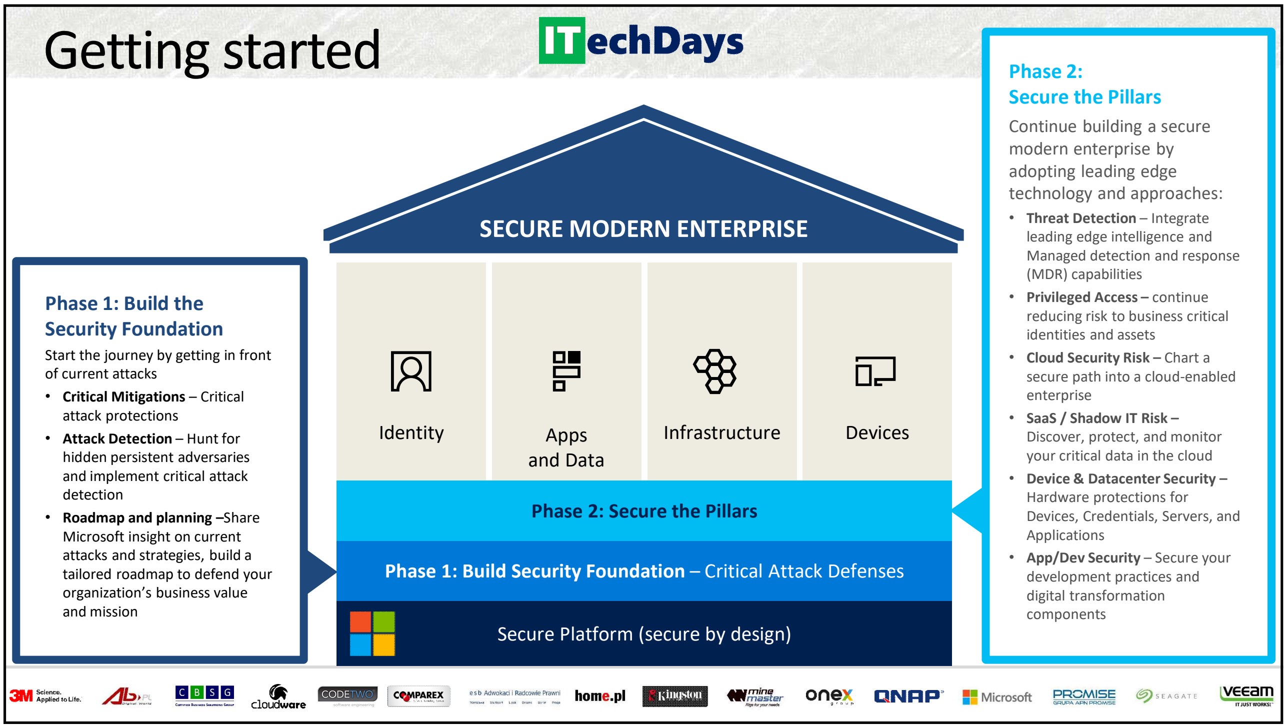
Aligned to business objectives and current threat environment

Identity
Embraces identity as primary security perimeter and protects identity systems, admins, and credentials as top priorities

Apps and Data
Aligns security investments with business priorities including identifying and securing communications, data, and applications

Infrastructure
Operates on modern platform and uses cloud intelligence to detect and remediate both vulnerabilities and attacks

Devices
Accesses assets from trusted devices with hardware security assurances, great user experience, and advanced threat detection



Getting started

ITechDays

SECURE MODERN ENTERPRISE

Identity

Apps and Data

Infrastructure

Devices

Phase 2: Secure the Pillars

Phase 1: Build Security Foundation – Critical Attack Defenses

Secure Platform (secure by design)

Phase 1: Build the Security Foundation

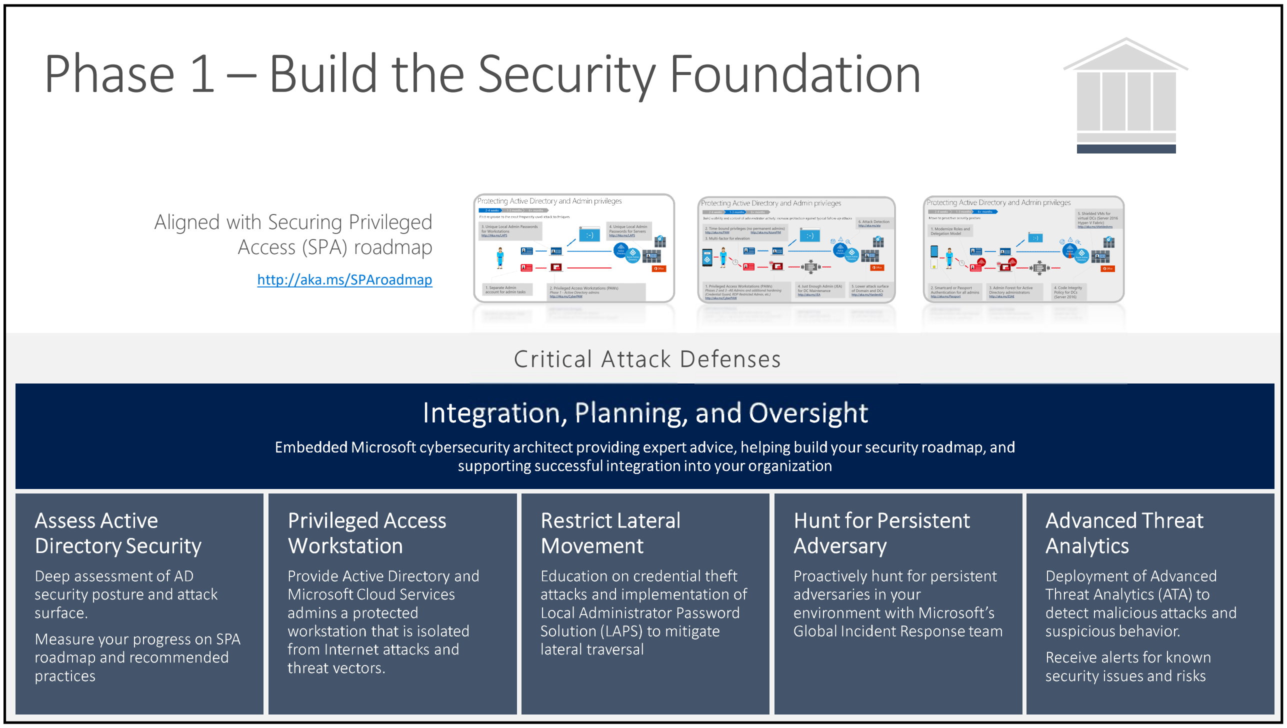
Start the journey by getting in front of current attacks

- **Critical Mitigations** – Critical attack protections
- **Attack Detection** – Hunt for hidden persistent adversaries and implement critical attack detection
- **Roadmap and planning** –Share Microsoft insight on current attacks and strategies, build a tailored roadmap to defend your organization's business value and mission

Phase 2: Secure the Pillars

Continue building a secure modern enterprise by adopting leading edge technology and approaches:

- **Threat Detection** – Integrate leading edge intelligence and Managed detection and response (MDR) capabilities
- **Privileged Access** – continue reducing risk to business critical identities and assets
- **Cloud Security Risk** – Chart a secure path into a cloud-enabled enterprise
- **SaaS / Shadow IT Risk** – Discover, protect, and monitor your critical data in the cloud
- **Device & Datacenter Security** – Hardware protections for Devices, Credentials, Servers, and Applications
- **App/Dev Security** – Secure your development practices and digital transformation components



Phase 1 – Build the Security Foundation

Aligned with Securing Privileged Access (SPA) roadmap

http://aka.ms/SPAroadmap

Critical Attack Defenses

Integration, Planning, and Oversight

Embedded Microsoft cybersecurity architect providing expert advice, helping build your security roadmap, and supporting successful integration into your organization

Assess Active Directory Security

Deep assessment of AD security posture and attack surface.

Measure your progress on SPA roadmap and recommended practices

Privileged Access Workstation

Provide Active Directory and Microsoft Cloud Services admins a protected workstation that is isolated from Internet attacks and threat vectors.

Restrict Lateral Movement

Education on credential theft attacks and implementation of Local Administrator Password Solution (LAPS) to mitigate lateral traversal

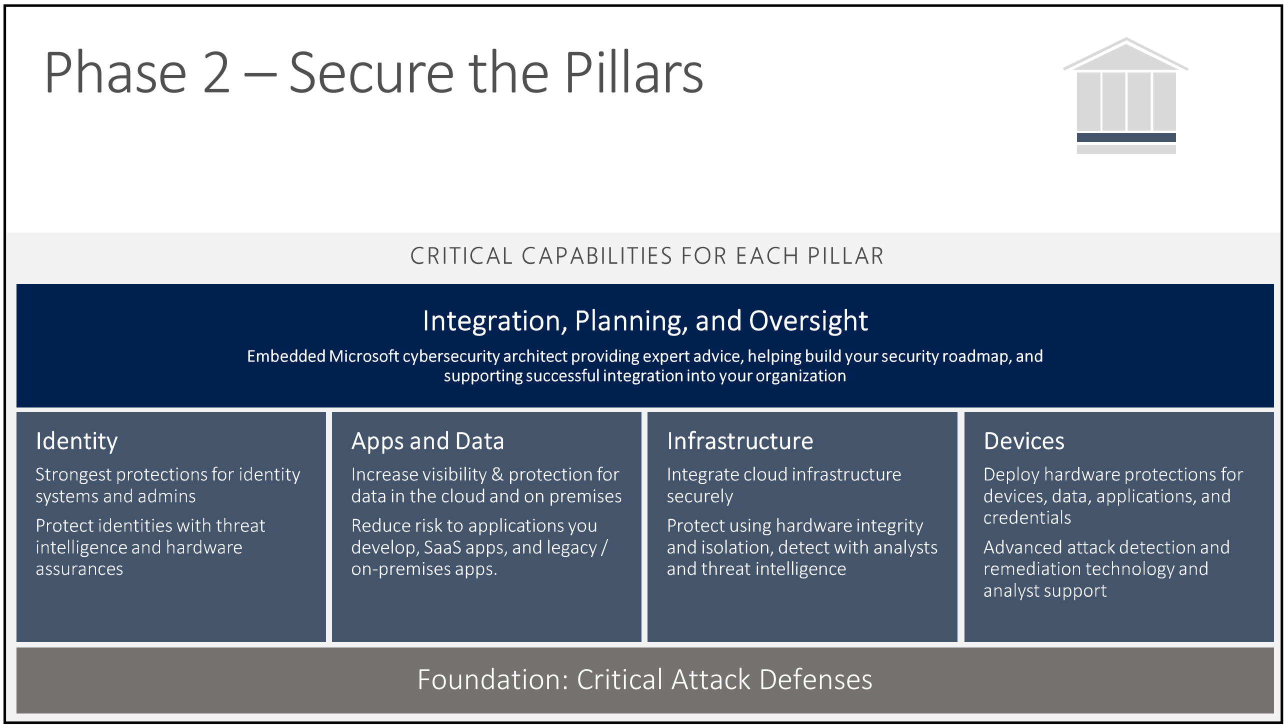
Hunt for Persistent Adversary

Proactively hunt for persistent adversaries in your environment with Microsoft's Global Incident Response team

Advanced Threat Analytics

Deployment of Advanced Threat Analytics (ATA) to detect malicious attacks and suspicious behavior.

Receive alerts for known security issues and risks



Phase 2 – Secure the Pillars

CRITICAL CAPABILITIES FOR EACH PILLAR

Integration, Planning, and Oversight

Embedded Microsoft cybersecurity architect providing expert advice, helping build your security roadmap, and supporting successful integration into your organization

Identity

Strongest protections for identity systems and admins

Protect identities with threat intelligence and hardware assurances

Apps and Data

Increase visibility & protection for data in the cloud and on premises

Reduce risk to applications you develop, SaaS apps, and legacy / on-premises apps.

Infrastructure

Integrate cloud infrastructure securely

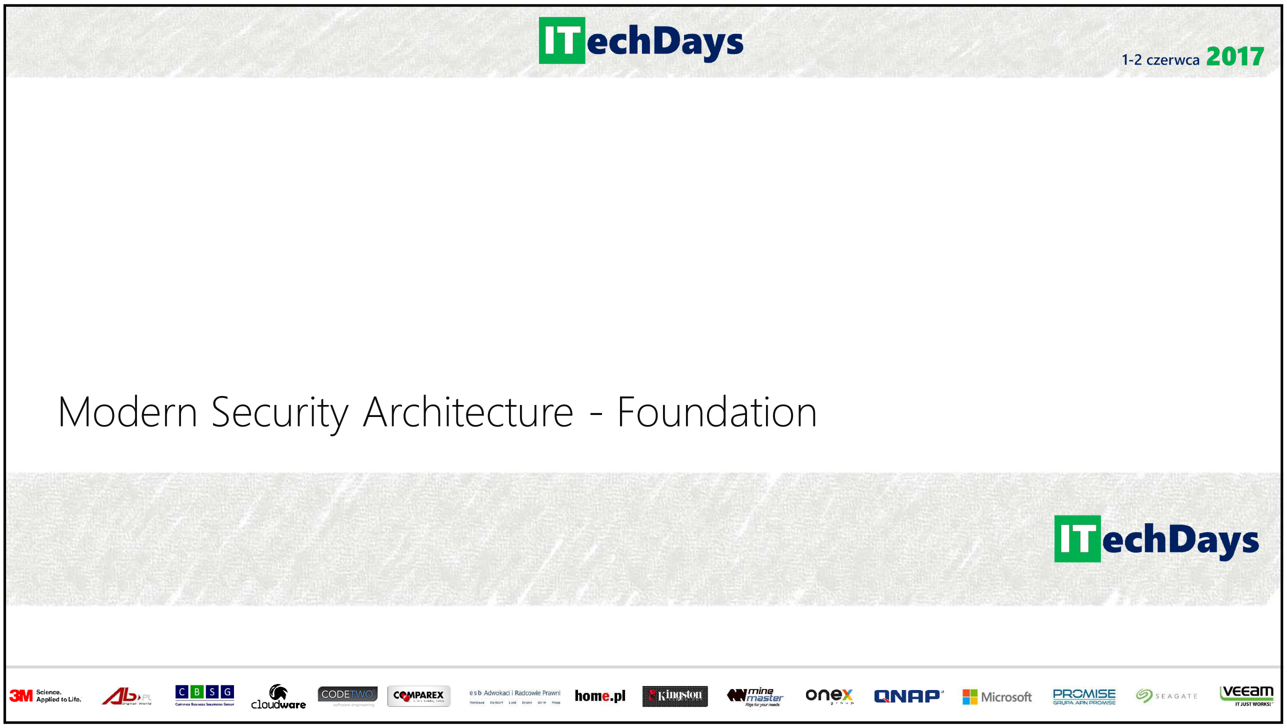
Protect using hardware integrity and isolation, detect with analysts and threat intelligence

Devices

Deploy hardware protections for devices, data, applications, and credentials

Advanced attack detection and remediation technology and analyst support

Foundation: Critical Attack Defenses

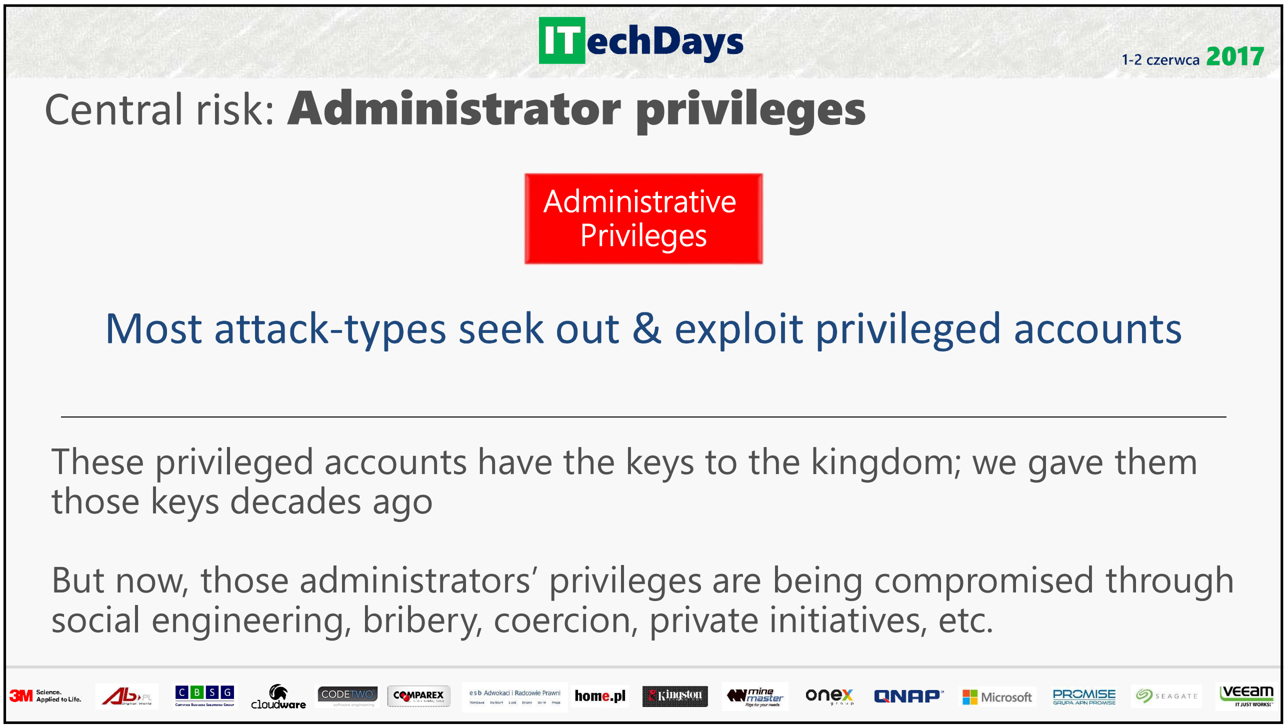


ITechDays

1-2 czerwca 2017

Modern Security Architecture - Foundation

ITechDays



ITechDays 1-2 czerwca 2017

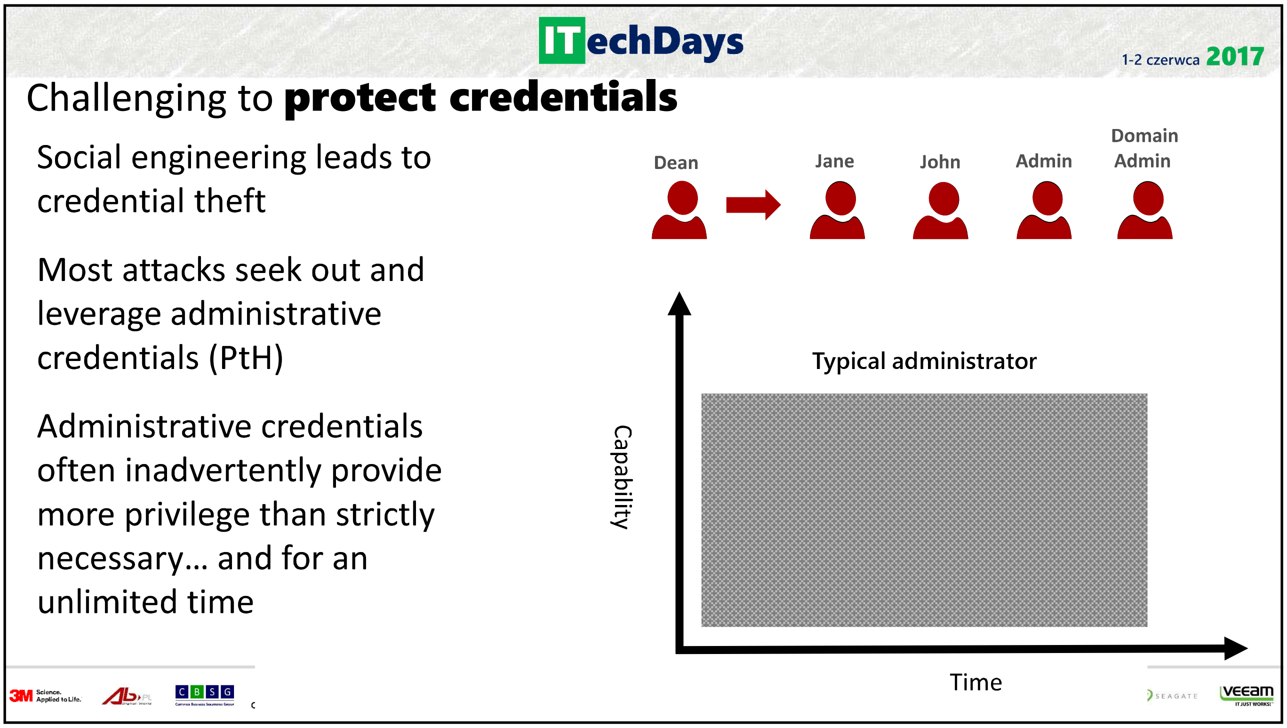
Central risk: **Administrator privileges**

Administrative Privileges

Most attack-types seek out & exploit privileged accounts

These privileged accounts have the keys to the kingdom; we gave them those keys decades ago

But now, those administrators' privileges are being compromised through social engineering, bribery, coercion, private initiatives, etc.



ITechDays 1-2 czerwca 2017

Challenging to **protect credentials**

Social engineering leads to credential theft

Most attacks seek out and leverage administrative credentials (PtH)

Administrative credentials often inadvertently provide more privilege than strictly necessary… and for an unlimited time

ITechDays 1-2 czerwca 2017

MODERN SECURITY APPROACH

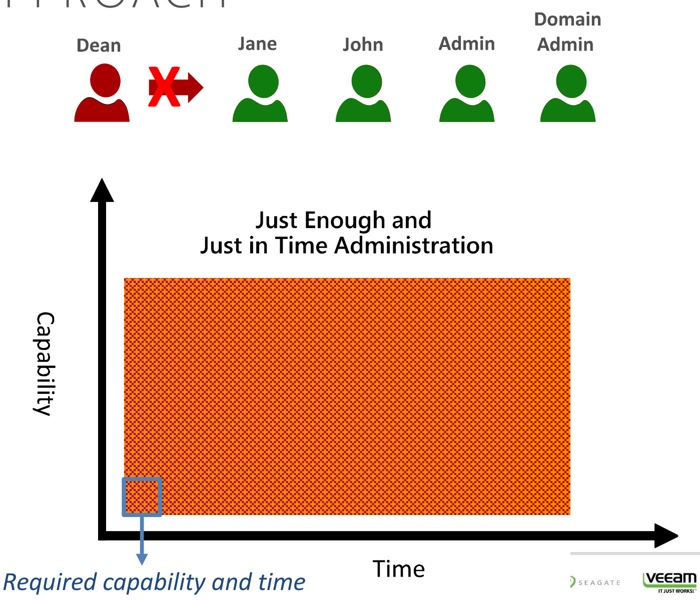
Credential Guard prevents Pass the Hash and Pass the Ticket attacks by protecting stored credentials and credential artifacts using Virtualization based Security (VBS)

Remote Credential Guard works in conjunction with Credential Guard for RDP sessions providing SSO for RDP sessions while eliminating the need for credentials to be passed to the RDP host

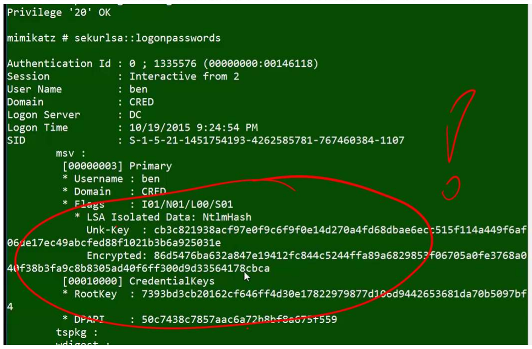
Just Enough Administration limits administrative privileges to the bare-minimum required set of actions (limited in space)

Just in Time Administration provides privileged access upon request through a workflow that is audited and limited in time

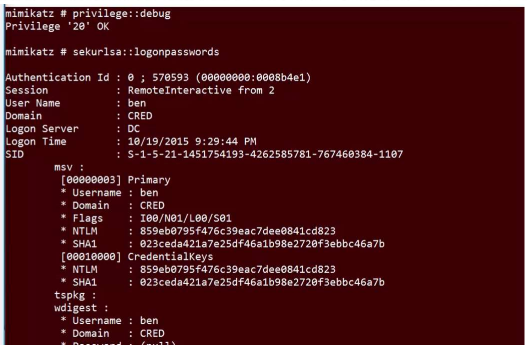
JEA + JIT = limited in time & capability



ITechDays 1-2 czerwca 2017



```
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1335576 (00000000:00146118)
Session           : Interactive from 2
User Name         : ben
Domain            : CRED
Logon Server      : DC
Logon Time        : 10/19/2015 9:24:54 PM
SID               : S-1-5-21-1451754193-4262585781-767460384-1107
        msv :
         [00000003] Primary
         * Username : ben
         * Domain   : CRED
         * Flags    : I01/N01/L00/S01
           * LSA Isolated Data: NtlmHash
             Unk-Key  : cb3c821938acf97e0f9c6f9f0e14d270a4fd68dbae6ecc515f114a449f6af
06de17ec49abcfed88f1021b3b6a925031e
             Encrypted: 86d5476ba632a847e19412fc844c5244ffa89a68298533f06705a0fe3768a0
40f38b3fa9c8b8305ad40f6ff300d9d33564178cbca
         [00010000] CredentialKeys
         * RootKey  : 7393bd3cb20162cf646ff4d30e17822979877d106d9442653681da70b5097bf
4
         * DPAPI    : 50c7438c7857aac6a72b8bf8a675f559
        tspkg :
        wdigest :
```

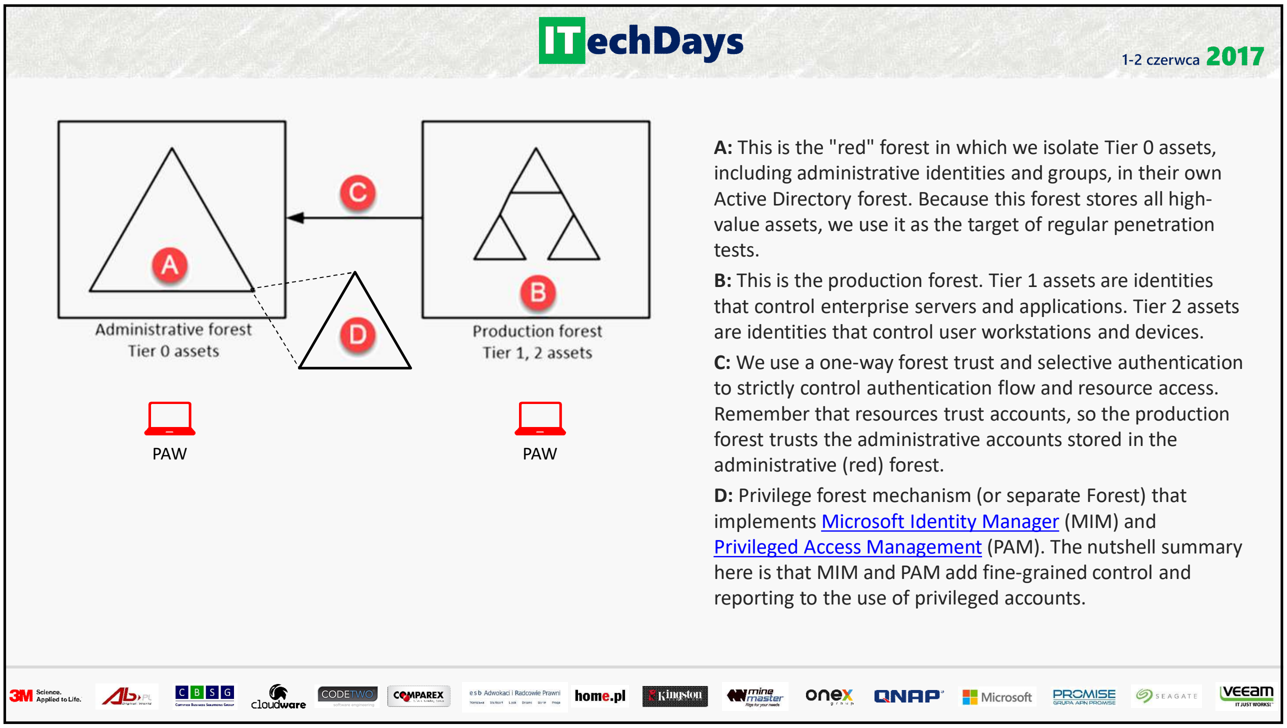


```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 570593 (00000000:0008b4e1)
Session           : RemoteInteractive from 2
User Name         : ben
Domain            : CRED
Logon Server      : DC
Logon Time        : 10/19/2015 9:29:44 PM
SID               : S-1-5-21-1451754193-4262585781-767460384-1107
        msv :
         [00000003] Primary
         * Username : ben
         * Domain   : CRED
         * Flags    : I00/N01/L00/S01
         * NTLM     : 859eb0795f476c39eac7dee0841cd823
         * SHA1     : 023ceda421a7e25df46a1b98e2720f3ebbc46a7b
         [00010000] CredentialKeys
         * NTLM     : 859eb0795f476c39eac7dee0841cd823
         * SHA1     : 023ceda421a7e25df46a1b98e2720f3ebbc46a7b
        tspkg :
        wdigest :
         * Username : ben
         * Domain   : CRED
         * Password : (null)
```

Credential Guard

DEMO

https://www.youtube.com/watch?v=urqXgBbVyWY ITechDays



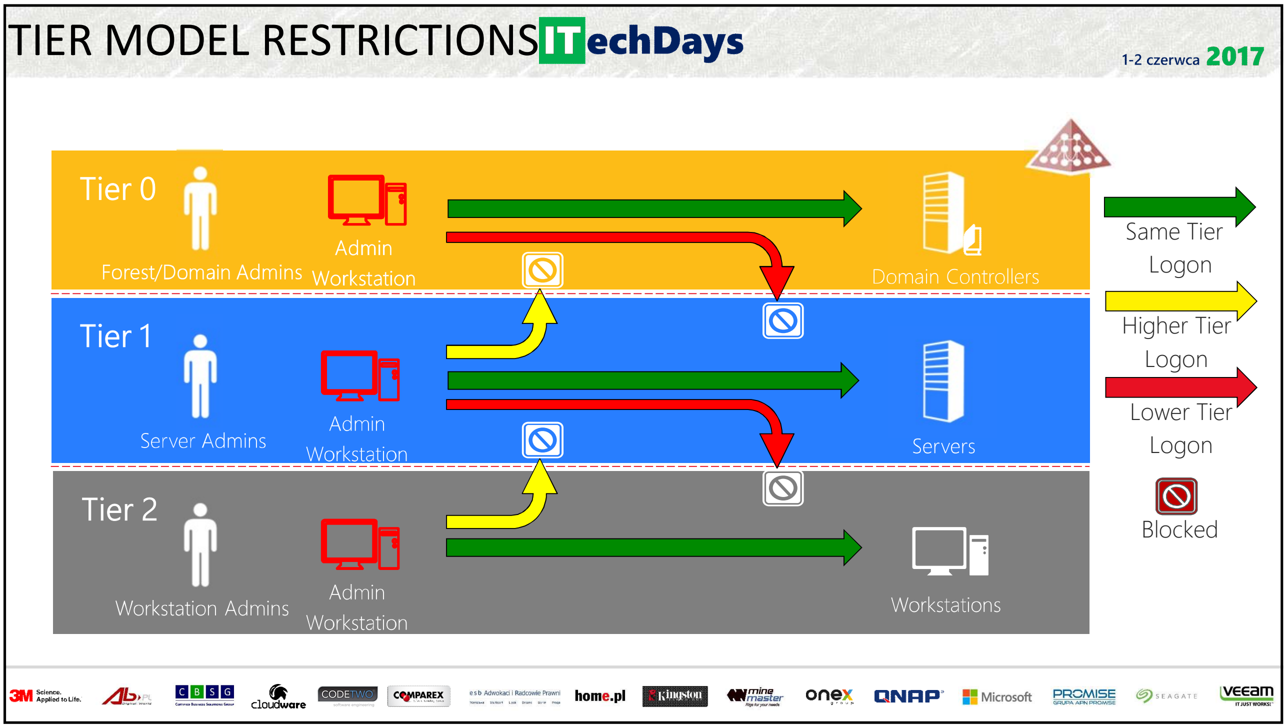
A: This is the "red" forest in which we isolate Tier 0 assets, including administrative identities and groups, in their own Active Directory forest. Because this forest stores all high-value assets, we use it as the target of regular penetration tests.

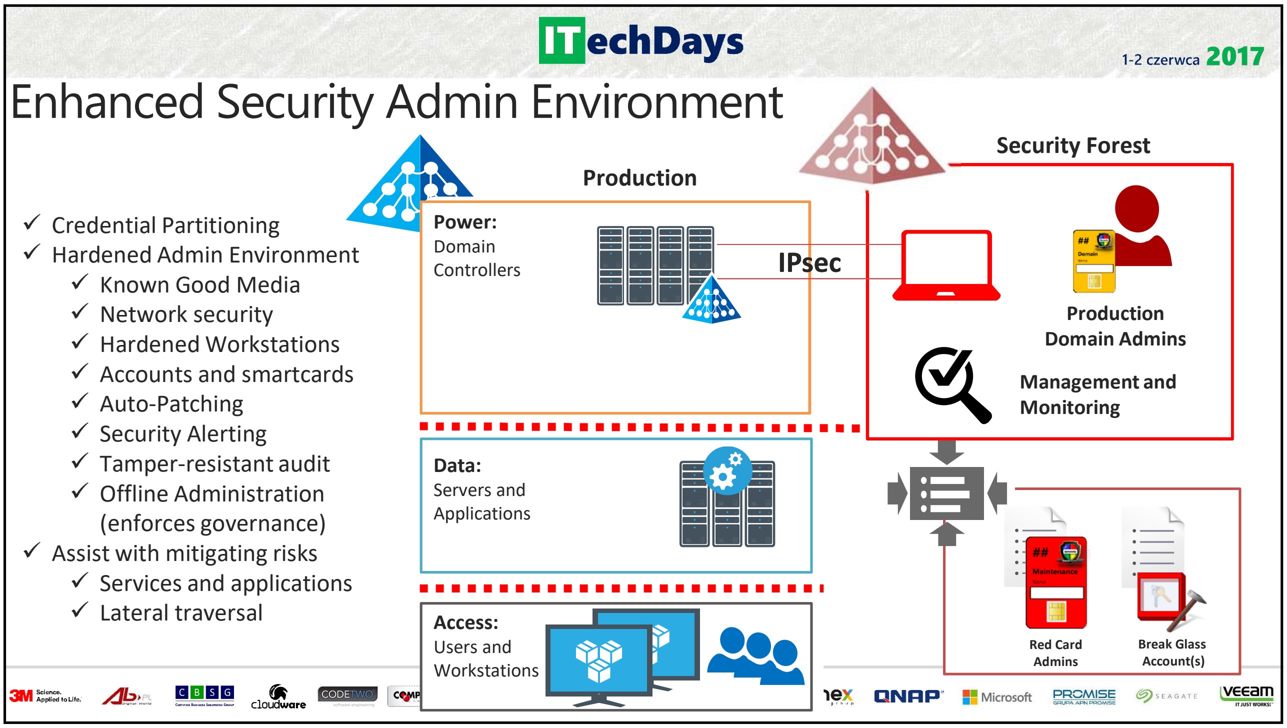
B: This is the production forest. Tier 1 assets are identities that control enterprise servers and applications. Tier 2 assets are identities that control user workstations and devices.

C: We use a one-way forest trust and selective authentication to strictly control authentication flow and resource access. Remember that resources trust accounts, so the production forest trusts the administrative accounts stored in the administrative (red) forest.

D: Privilege forest mechanism (or separate Forest) that implements Microsoft Identity Manager (MIM) and Privileged Access Management (PAM). The nutshell summary here is that MIM and PAM add fine-grained control and reporting to the use of privileged accounts.

TIER MODEL RESTRICTIONS





ITechDays

1-2 czerwca 2017

Enhanced Security Admin Environment

- ✓ Credential Partitioning
- ✓ Hardened Admin Environment
  - ✓ Known Good Media
  - ✓ Network security
  - ✓ Hardened Workstations
  - ✓ Accounts and smartcards
  - ✓ Auto-Patching
  - ✓ Security Alerting
  - ✓ Tamper-resistant audit
  - ✓ Offline Administration (enforces governance)
- ✓ Assist with mitigating risks
  - ✓ Services and applications
  - ✓ Lateral traversal

Production

Power: Domain Controllers

IPsec

Security Forest

Production Domain Admins

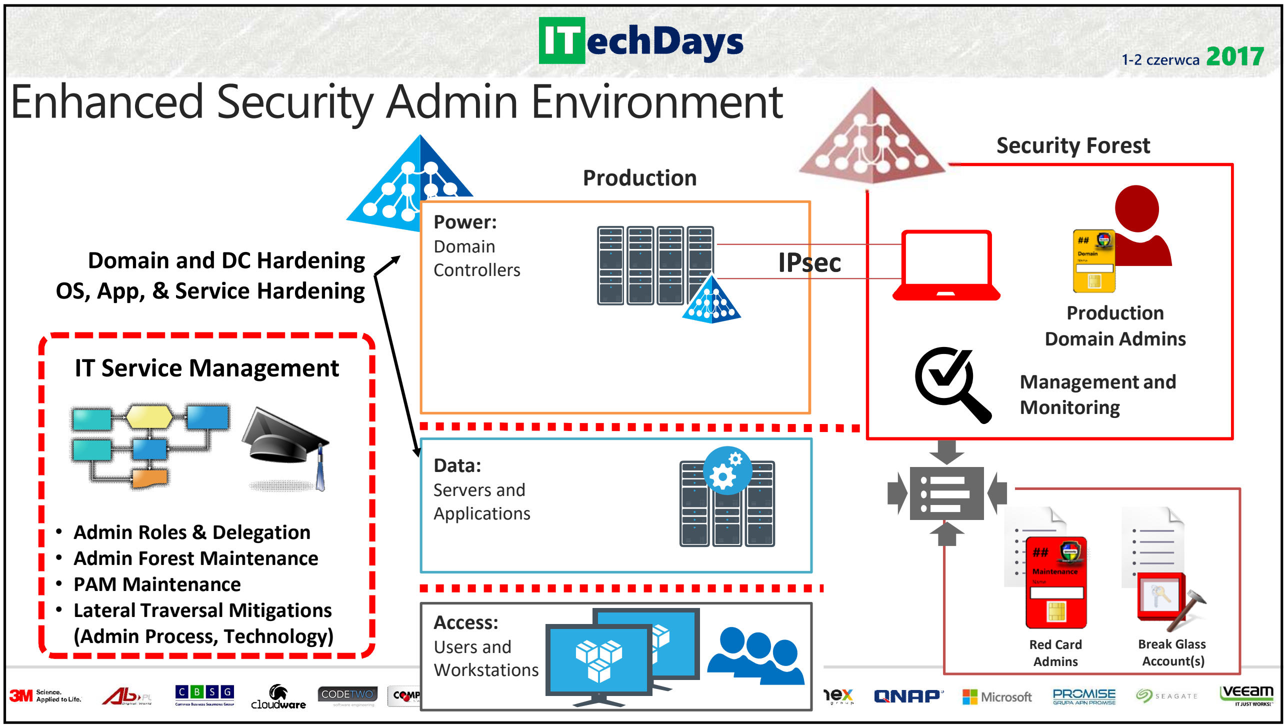
Management and Monitoring

Data: Servers and Applications

Access: Users and Workstations

Red Card Admins

Break Glass Account(s)



ITechDays

1-2 czerwca 2017

Enhanced Security Admin Environment

Domain and DC Hardening
OS, App, & Service Hardening

IT Service Management

- Admin Roles & Delegation
- Admin Forest Maintenance
- PAM Maintenance
- Lateral Traversal Mitigations (Admin Process, Technology)

Production

Power: Domain Controllers

IPsec

Security Forest

Production Domain Admins

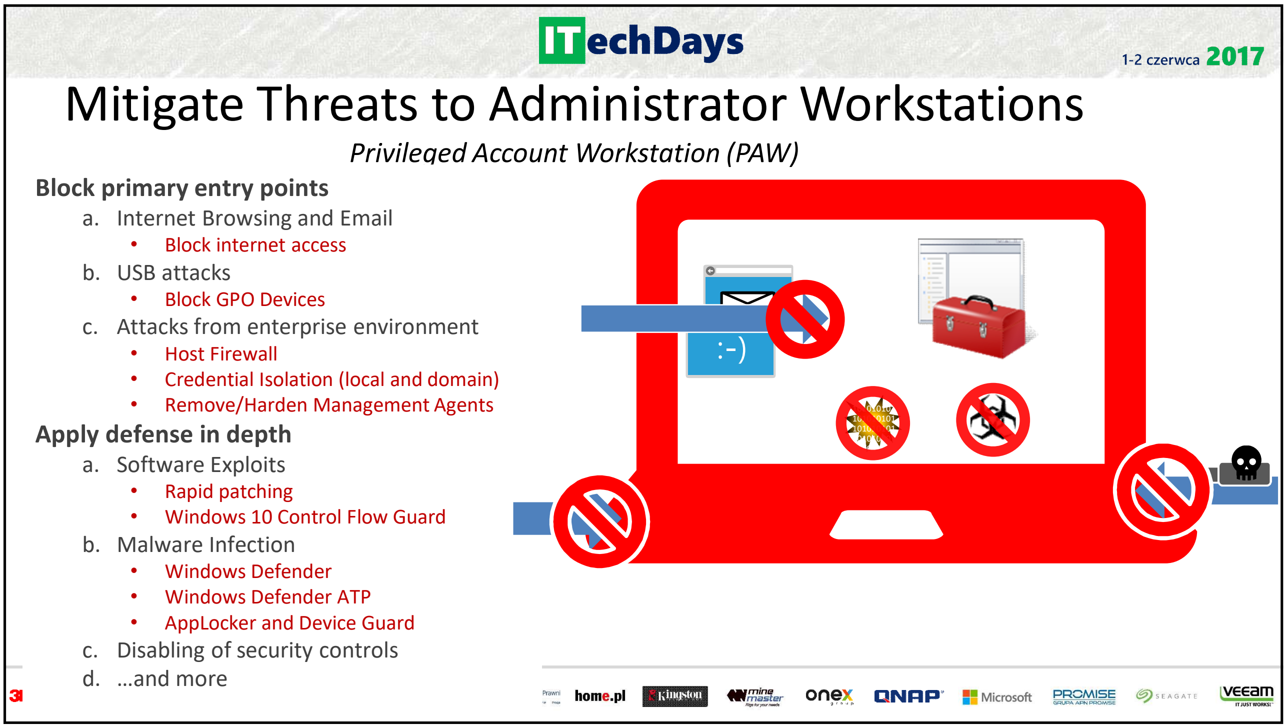
Management and Monitoring

Data: Servers and Applications

Access: Users and Workstations

Red Card Admins

Break Glass Account(s)



1-2 czerwca 2017

Mitigate Threats to Administrator Workstations

Privileged Account Workstation (PAW)

Block primary entry points

a. Internet Browsing and Email
- Block internet access

b. USB attacks
- Block GPO Devices

c. Attacks from enterprise environment
- Host Firewall
- Credential Isolation (local and domain)
- Remove/Harden Management Agents

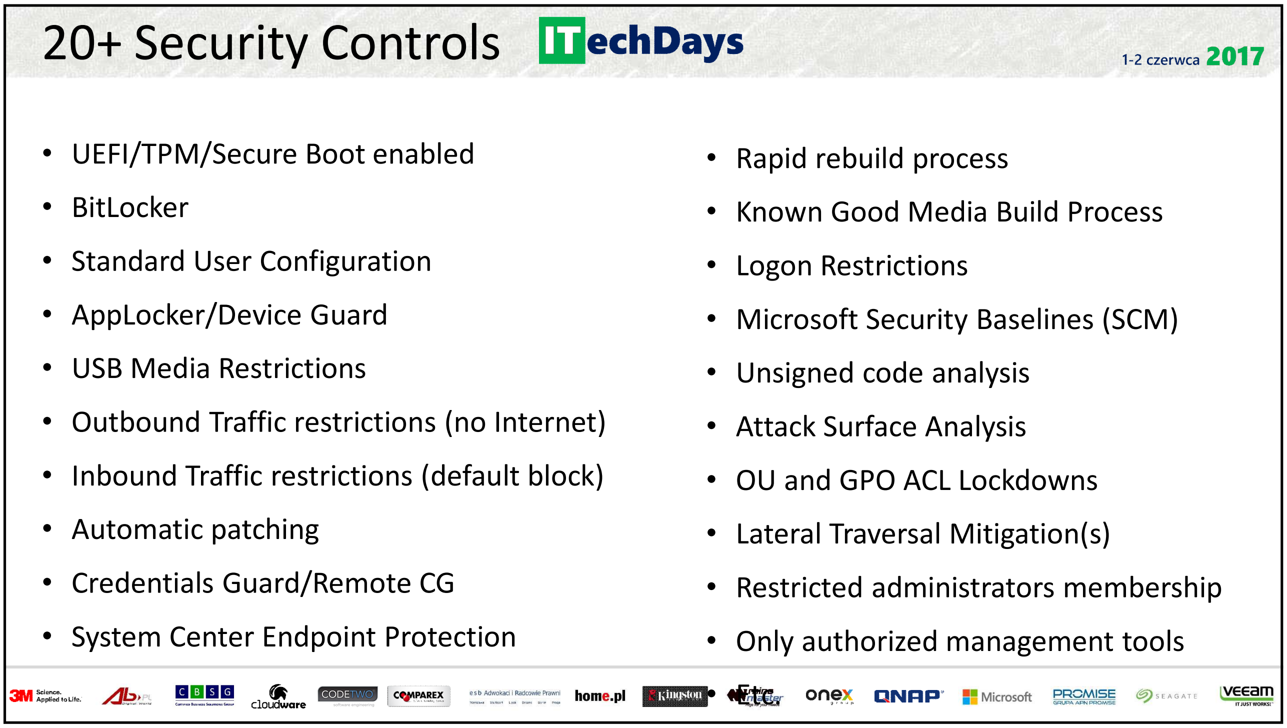
Apply defense in depth

a. Software Exploits
- Rapid patching
- Windows 10 Control Flow Guard

b. Malware Infection
- Windows Defender
- Windows Defender ATP
- AppLocker and Device Guard

c. Disabling of security controls

d. …and more

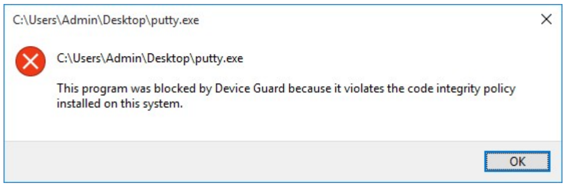


20+ Security Controls

1-2 czerwca 2017

- UEFI/TPM/Secure Boot enabled
- BitLocker
- Standard User Configuration
- AppLocker/Device Guard
- USB Media Restrictions
- Outbound Traffic restrictions (no Internet)
- Inbound Traffic restrictions (default block)
- Automatic patching
- Credentials Guard/Remote CG
- System Center Endpoint Protection
- Rapid rebuild process
- Known Good Media Build Process
- Logon Restrictions
- Microsoft Security Baselines (SCM)
- Unsigned code analysis
- Attack Surface Analysis
- OU and GPO ACL Lockdowns
- Lateral Traversal Mitigation(s)
- Restricted administrators membership
- Only authorized management tools

1-2 czerwca 2017



C:\Users\Admin\Desktop\putty.exe

C:\Users\Admin\Desktop\putty.exe

This program was blocked by Device Guard because it violates the code integrity policy installed on this system.

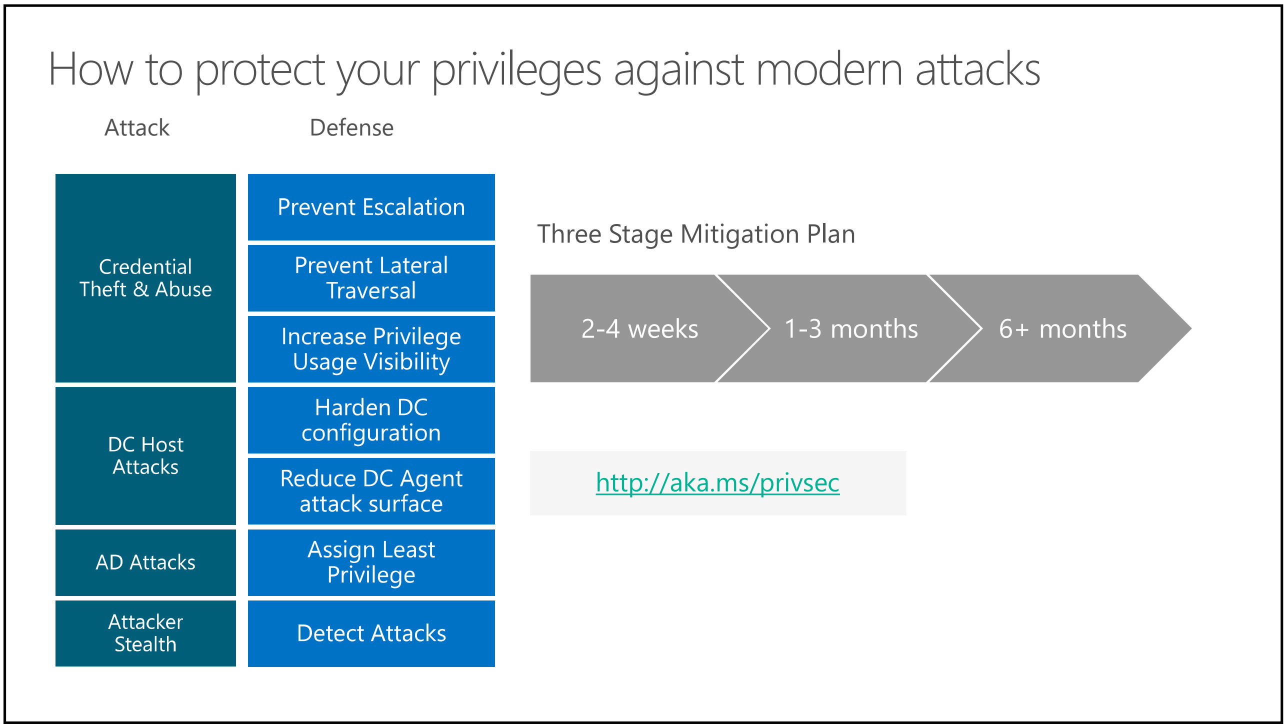
Device Guard

DEMO

https://www.youtube.com/watch?v=g24e29U97K8

1-2 czerwca 2017

Enhanced Security Admin Environment - Step-by-Step



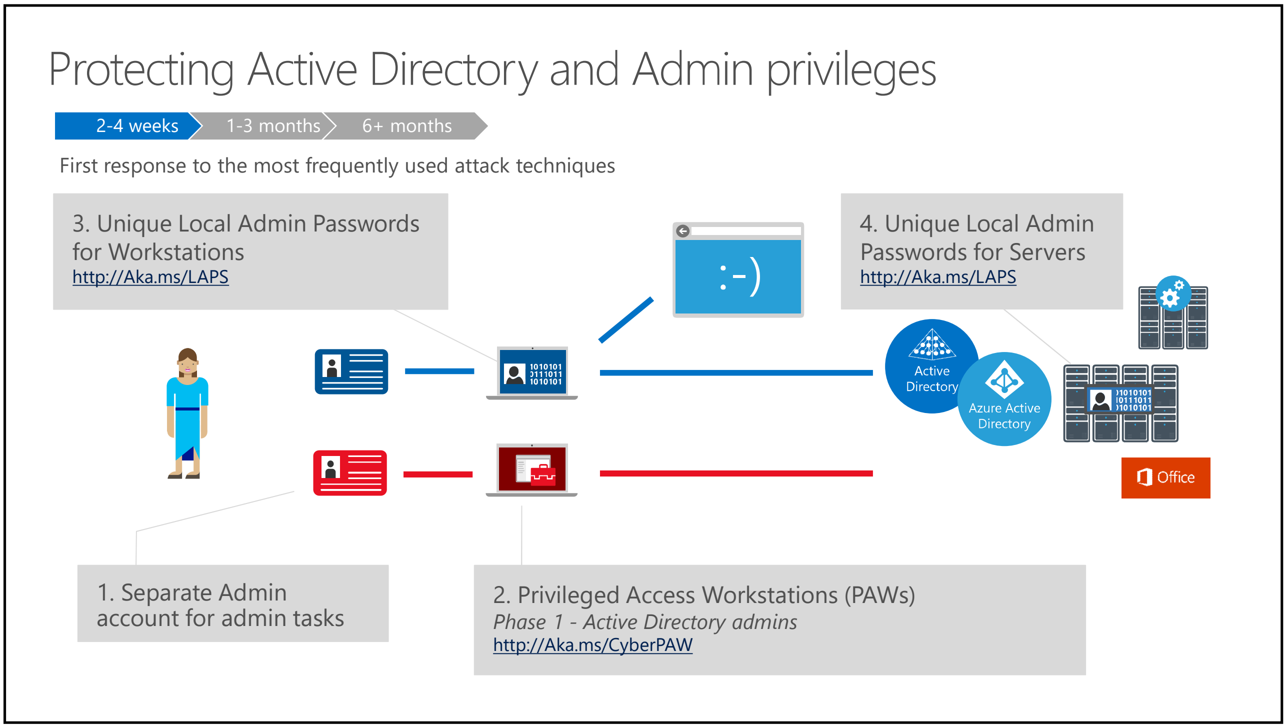
How to protect your privileges against modern attacks

Attack	Defense
Credential Theft & Abuse	Prevent Escalation
	Prevent Lateral Traversal
	Increase Privilege Usage Visibility
DC Host Attacks	Harden DC configuration
	Reduce DC Agent attack surface
AD Attacks	Assign Least Privilege
Attacker Stealth	Detect Attacks

Three Stage Mitigation Plan

2-4 weeks → 1-3 months → 6+ months

http://aka.ms/privsec



Protecting Active Directory and Admin privileges

2-4 weeks → 1-3 months → 6+ months

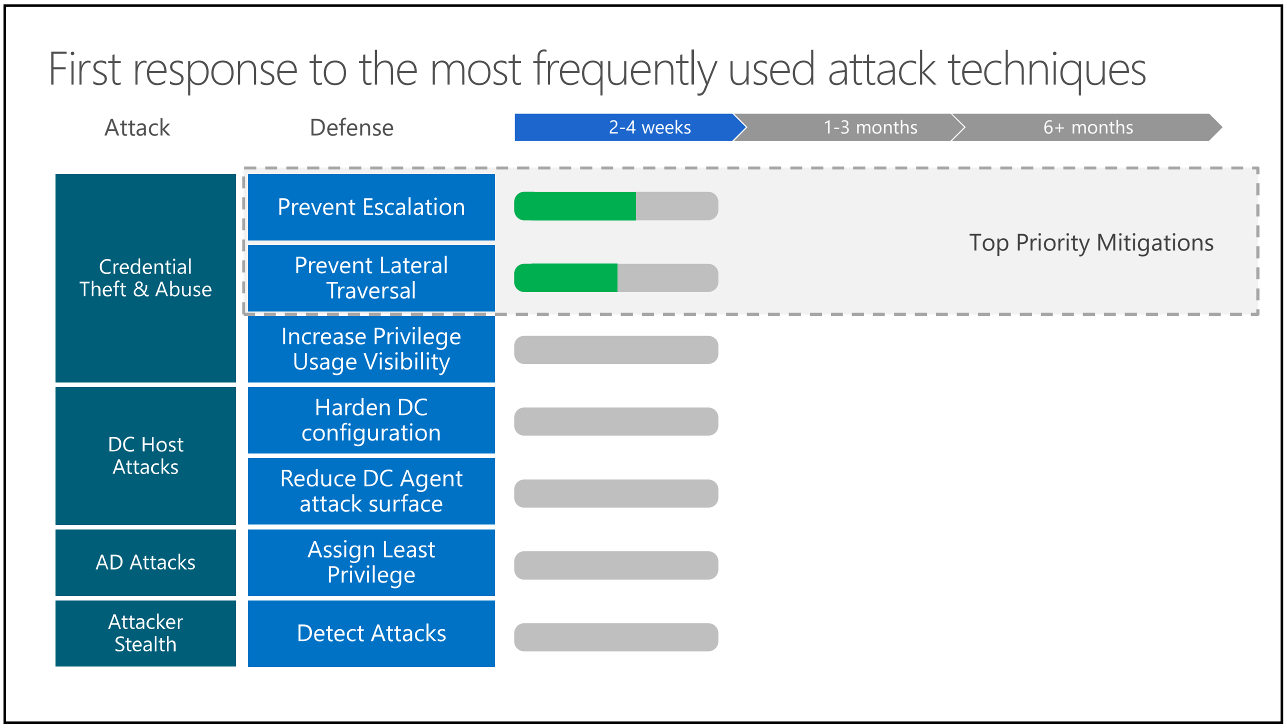
First response to the most frequently used attack techniques

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

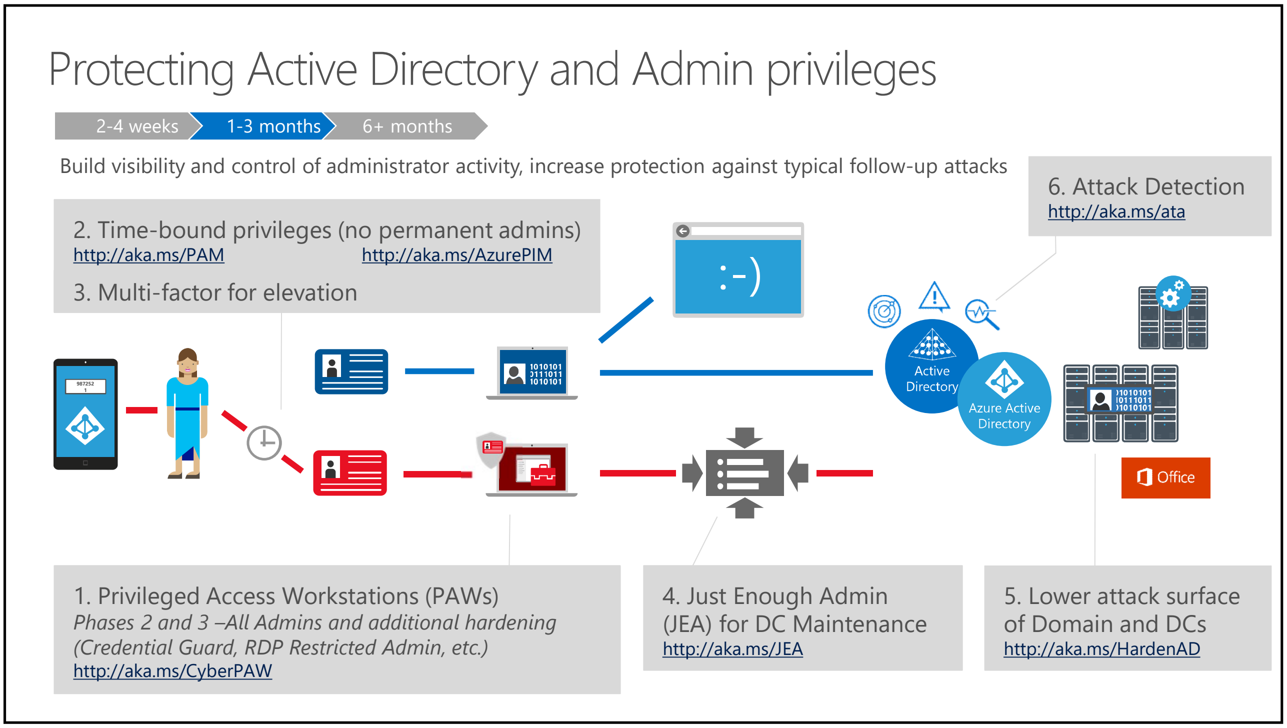


First response to the most frequently used attack techniques

2-4 weeks → 1-3 months → 6+ months

Attack	Defense
Credential Theft & Abuse	Prevent Escalation
	Prevent Lateral Traversal
	Increase Privilege Usage Visibility
DC Host Attacks	Harden DC configuration
	Reduce DC Agent attack surface
AD Attacks	Assign Least Privilege
Attacker Stealth	Detect Attacks

Top Priority Mitigations



Protecting Active Directory and Admin privileges

2-4 weeks → 1-3 months → 6+ months

Build visibility and control of administrator activity, increase protection against typical follow-up attacks

2. Time-bound privileges (no permanent admins)
http://aka.ms/PAM http://aka.ms/AzurePIM

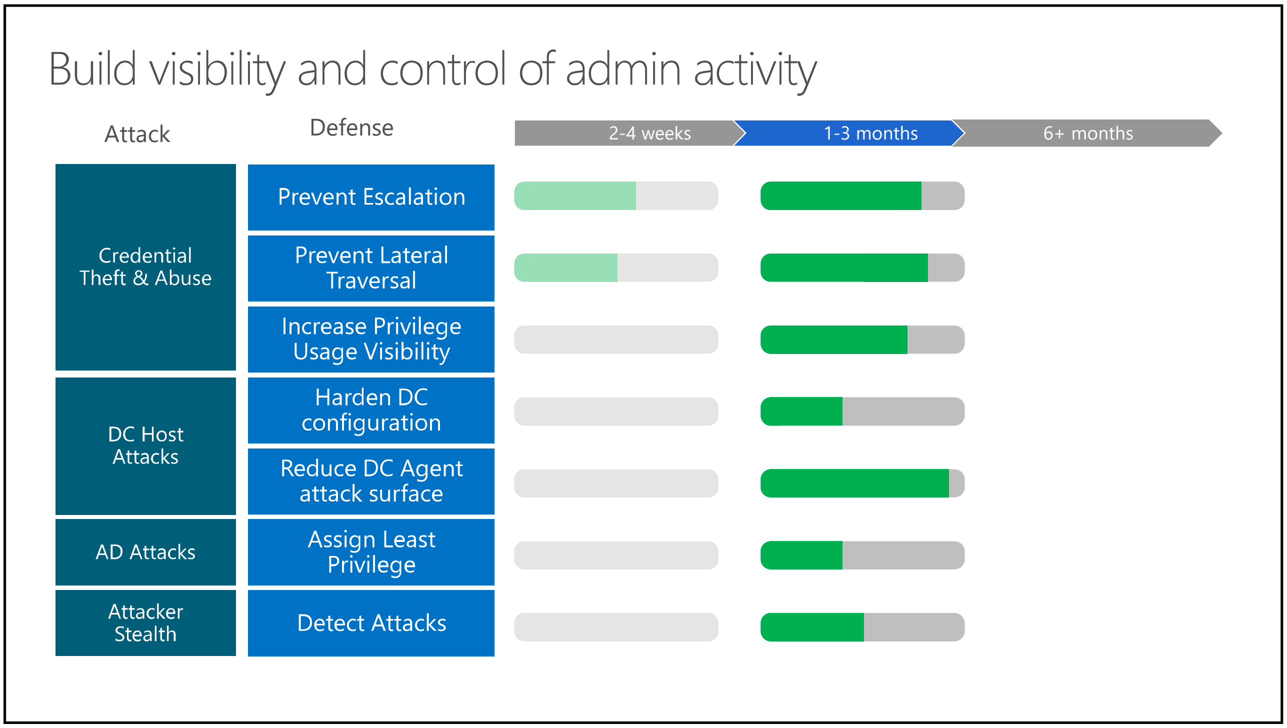
3. Multi-factor for elevation

6. Attack Detection
http://aka.ms/ata

1. Privileged Access Workstations (PAWs)
Phases 2 and 3 –All Admins and additional hardening (Credential Guard, RDP Restricted Admin, etc.)
http://aka.ms/CyberPAW

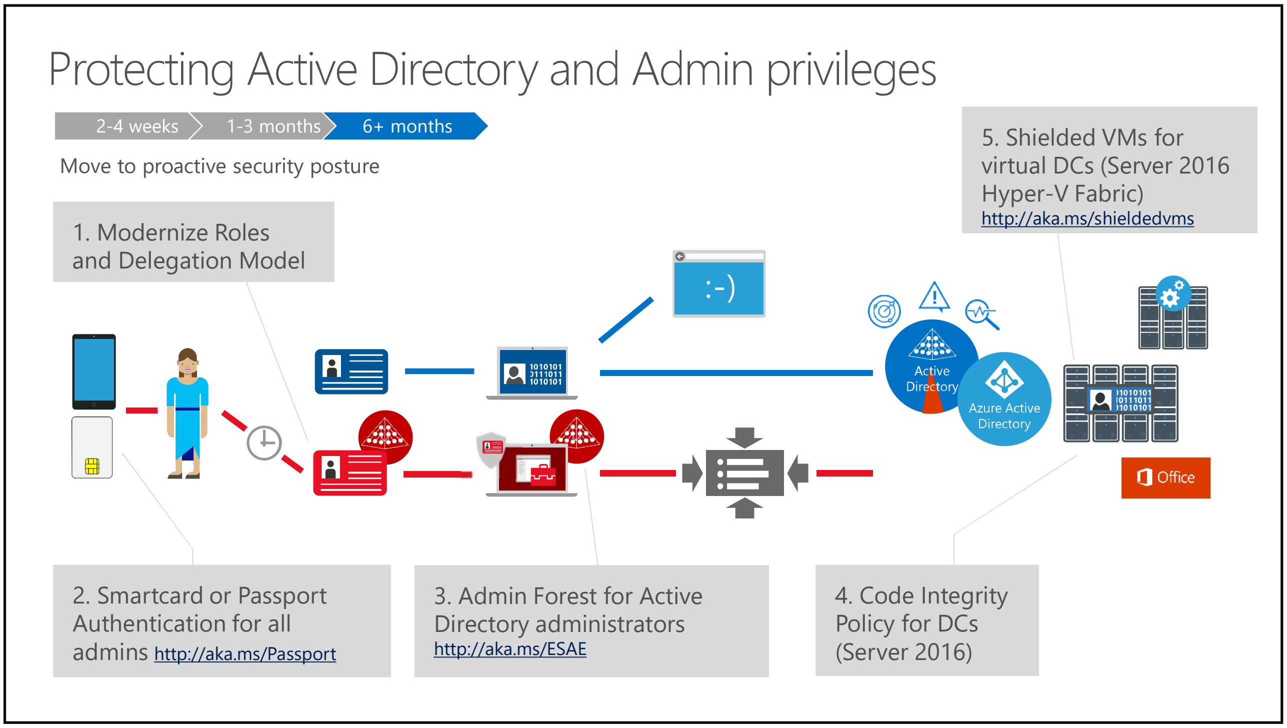
4. Just Enough Admin (JEA) for DC Maintenance
http://aka.ms/JEA

5. Lower attack surface of Domain and DCs
http://aka.ms/HardenAD



Build visibility and control of admin activity

Attack	Defense
Credential Theft & Abuse	Prevent Escalation
	Prevent Lateral Traversal
	Increase Privilege Usage Visibility
DC Host Attacks	Harden DC configuration
	Reduce DC Agent attack surface
AD Attacks	Assign Least Privilege
Attacker Stealth	Detect Attacks



Protecting Active Directory and Admin privileges

Move to proactive security posture

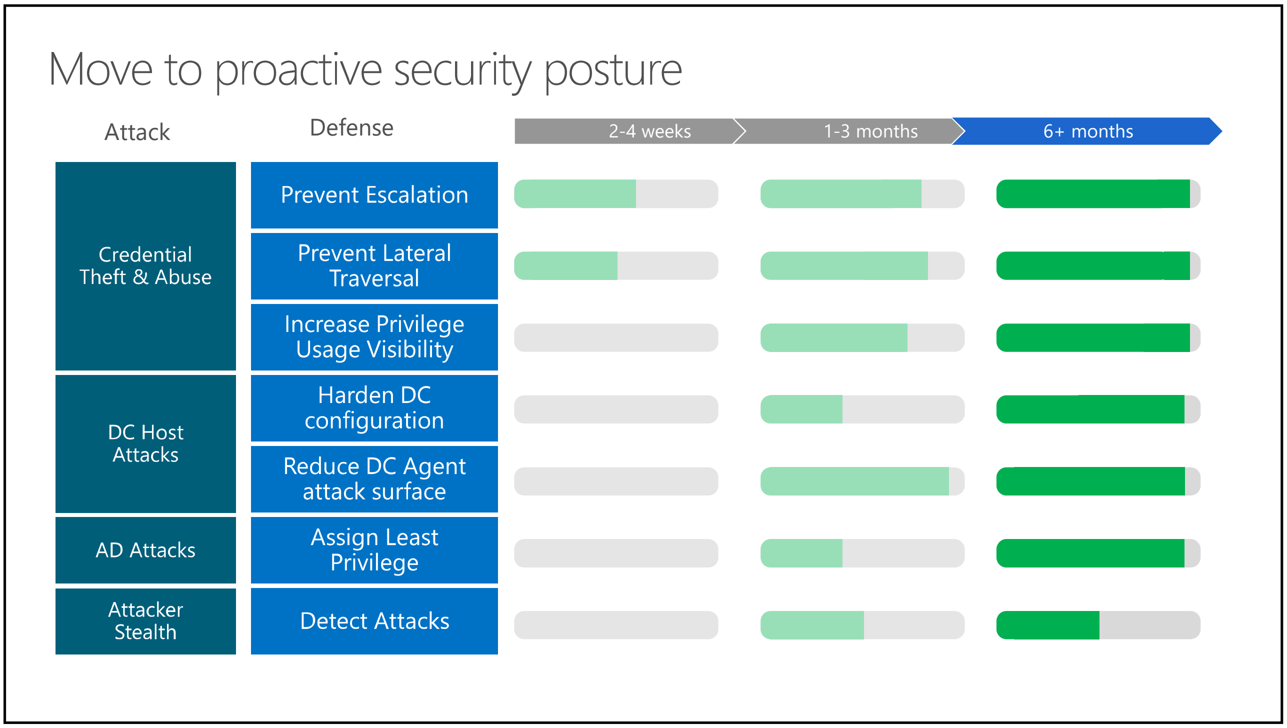
1. Modernize Roles and Delegation Model

2. Smartcard or Passport Authentication for all admins http://aka.ms/Passport

3. Admin Forest for Active Directory administrators http://aka.ms/ESAE

4. Code Integrity Policy for DCs (Server 2016)

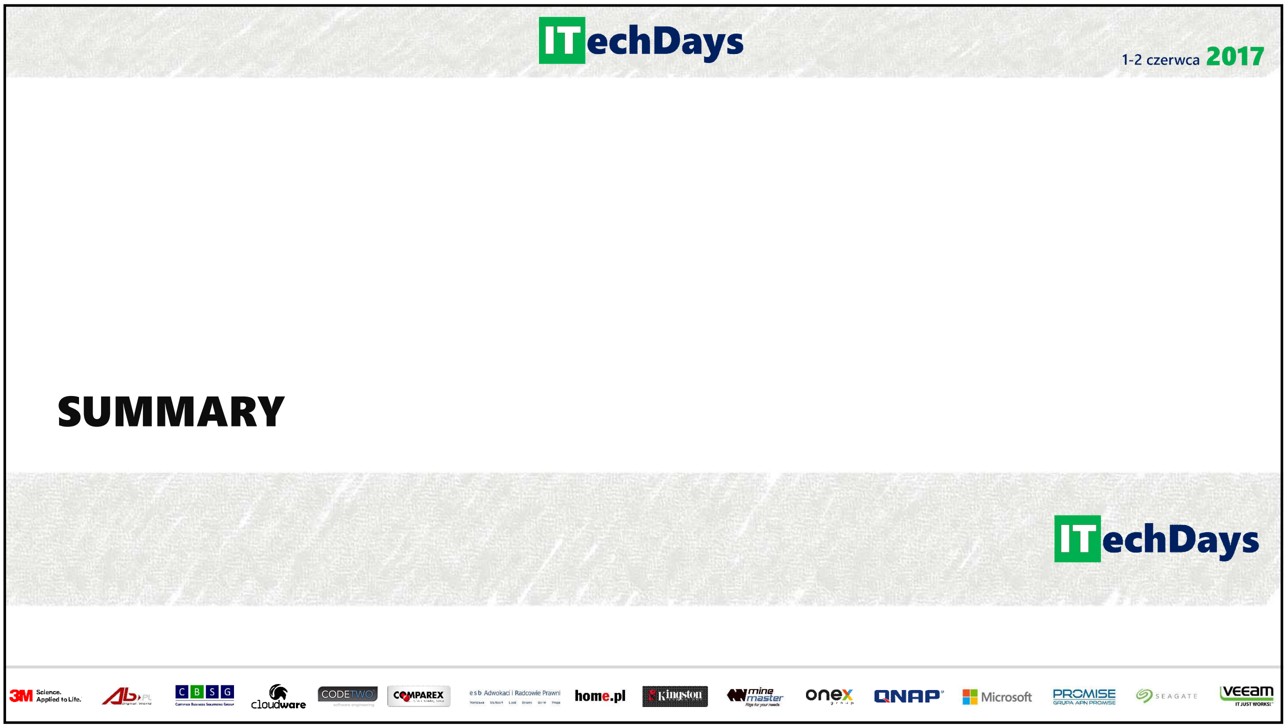
5. Shielded VMs for virtual DCs (Server 2016 Hyper-V Fabric) http://aka.ms/shieldedvms



Move to proactive security posture

2-4 weeks → 1-3 months → 6+ months

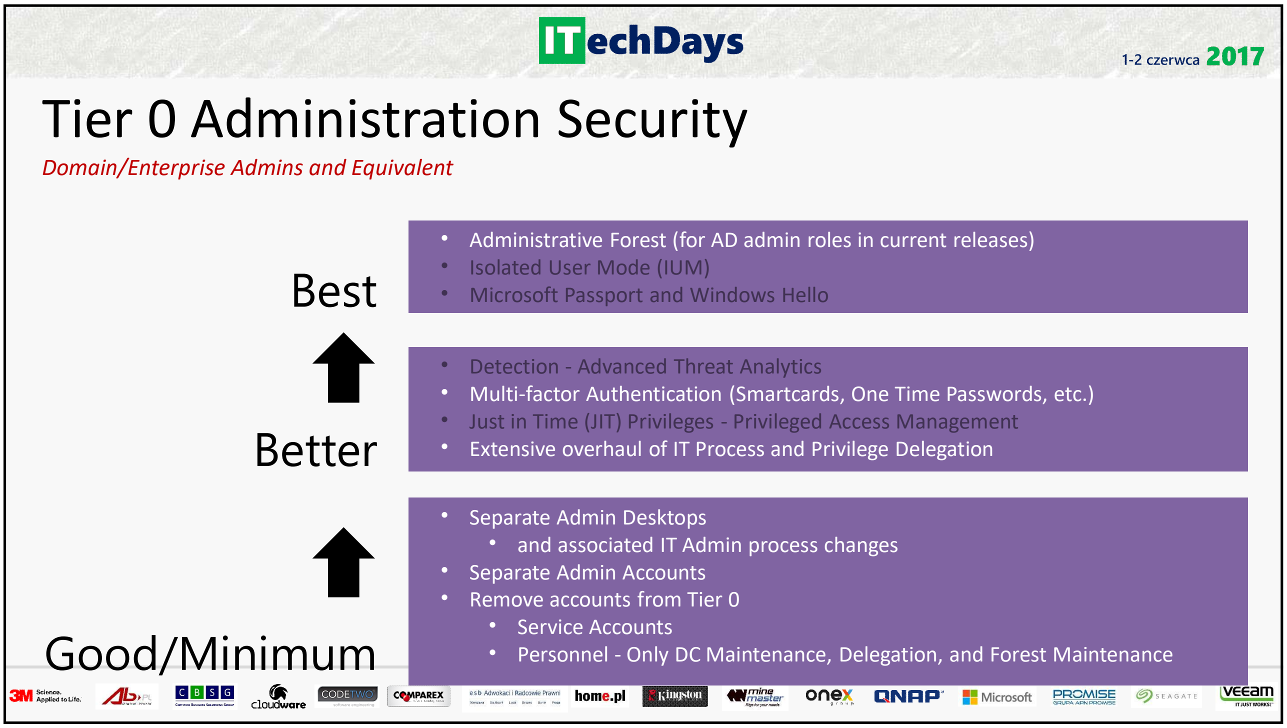
Attack	Defense
Credential Theft & Abuse	Prevent Escalation
	Prevent Lateral Traversal
	Increase Privilege Usage Visibility
DC Host Attacks	Harden DC configuration
	Reduce DC Agent attack surface
AD Attacks	Assign Least Privilege
Attacker Stealth	Detect Attacks



ITechDays 1-2 czerwca 2017

SUMMARY

ITechDays



ITechDays 1-2 czerwca 2017

Tier 0 Administration Security

Domain/Enterprise Admins and Equivalent

Best

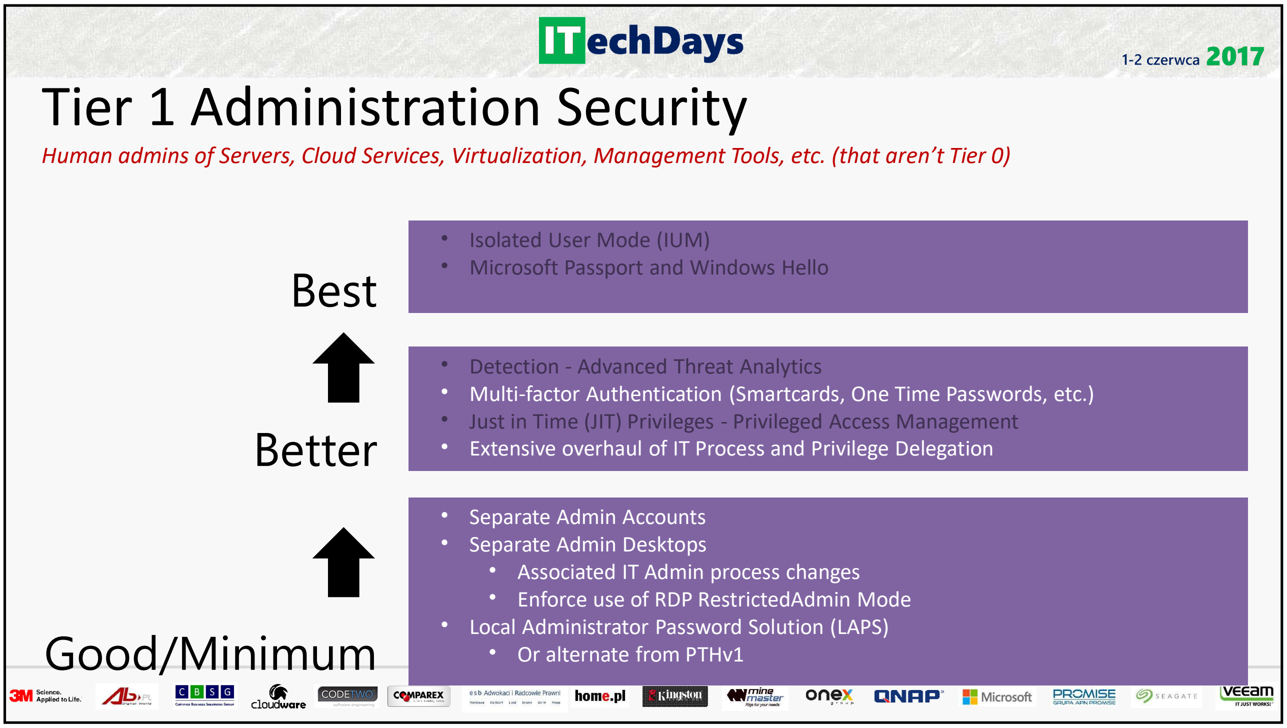
- Administrative Forest (for AD admin roles in current releases)
- Isolated User Mode (IUM)
- Microsoft Passport and Windows Hello

Better

- Detection - Advanced Threat Analytics
- Multi-factor Authentication (Smartcards, One Time Passwords, etc.)
- Just in Time (JIT) Privileges - Privileged Access Management
- Extensive overhaul of IT Process and Privilege Delegation

Good/Minimum

- Separate Admin Desktops
  - and associated IT Admin process changes
- Separate Admin Accounts
- Remove accounts from Tier 0
  - Service Accounts
  - Personnel - Only DC Maintenance, Delegation, and Forest Maintenance



ITechDays 1-2 czerwca 2017

Tier 1 Administration Security

Human admins of Servers, Cloud Services, Virtualization, Management Tools, etc. (that aren't Tier 0)

Best

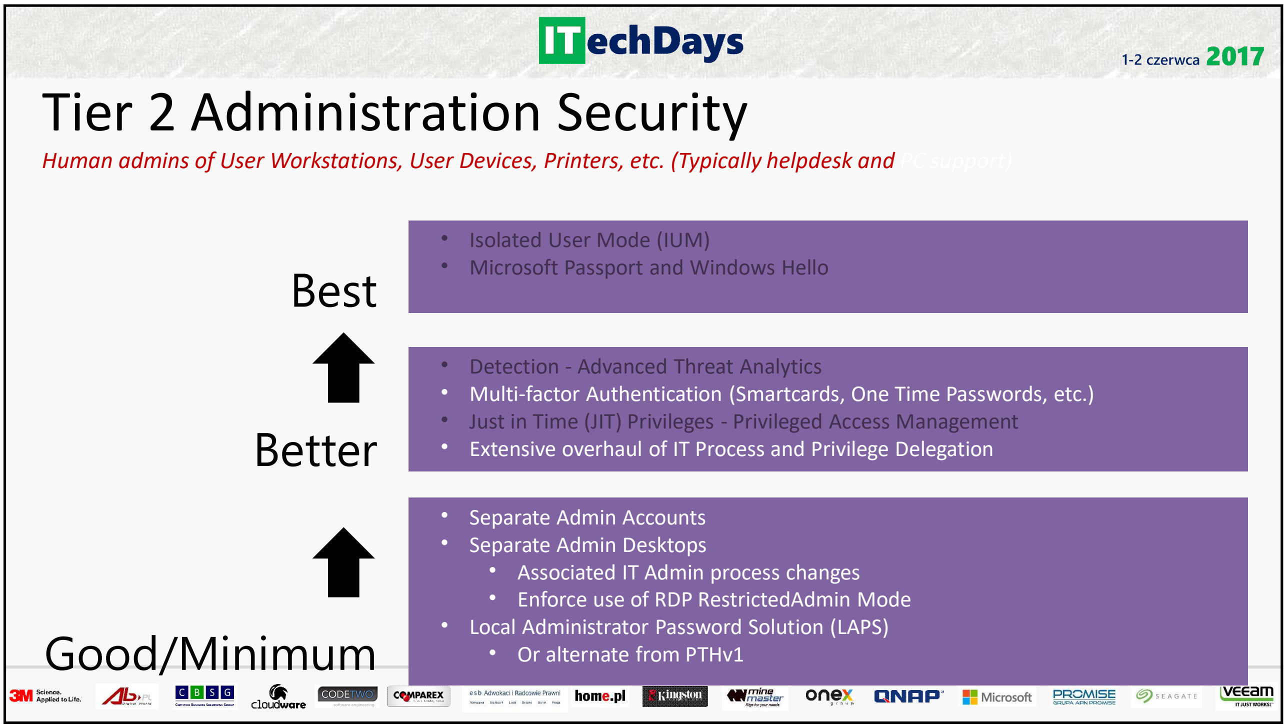
- Isolated User Mode (IUM)
- Microsoft Passport and Windows Hello

Better

- Detection - Advanced Threat Analytics
- Multi-factor Authentication (Smartcards, One Time Passwords, etc.)
- Just in Time (JIT) Privileges - Privileged Access Management
- Extensive overhaul of IT Process and Privilege Delegation

Good/Minimum

- Separate Admin Accounts
- Separate Admin Desktops
  - Associated IT Admin process changes
  - Enforce use of RDP RestrictedAdmin Mode
- Local Administrator Password Solution (LAPS)
  - Or alternate from PTHv1



ITechDays 1-2 czerwca 2017

Tier 2 Administration Security

Human admins of User Workstations, User Devices, Printers, etc. (Typically helpdesk and PC support)

Best

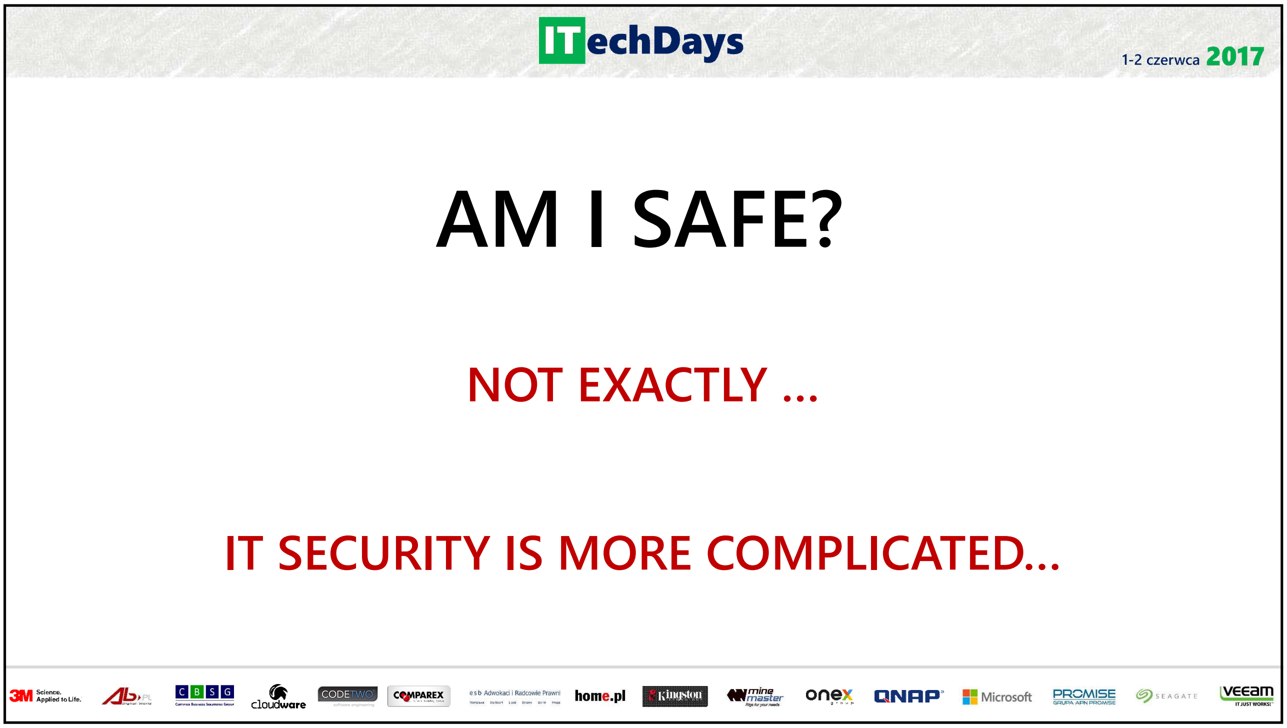
- Isolated User Mode (IUM)
- Microsoft Passport and Windows Hello

Better

- Detection - Advanced Threat Analytics
- Multi-factor Authentication (Smartcards, One Time Passwords, etc.)
- Just in Time (JIT) Privileges - Privileged Access Management
- Extensive overhaul of IT Process and Privilege Delegation

Good/Minimum

- Separate Admin Accounts
- Separate Admin Desktops
  - Associated IT Admin process changes
  - Enforce use of RDP RestrictedAdmin Mode
- Local Administrator Password Solution (LAPS)
  - Or alternate from PTHv1



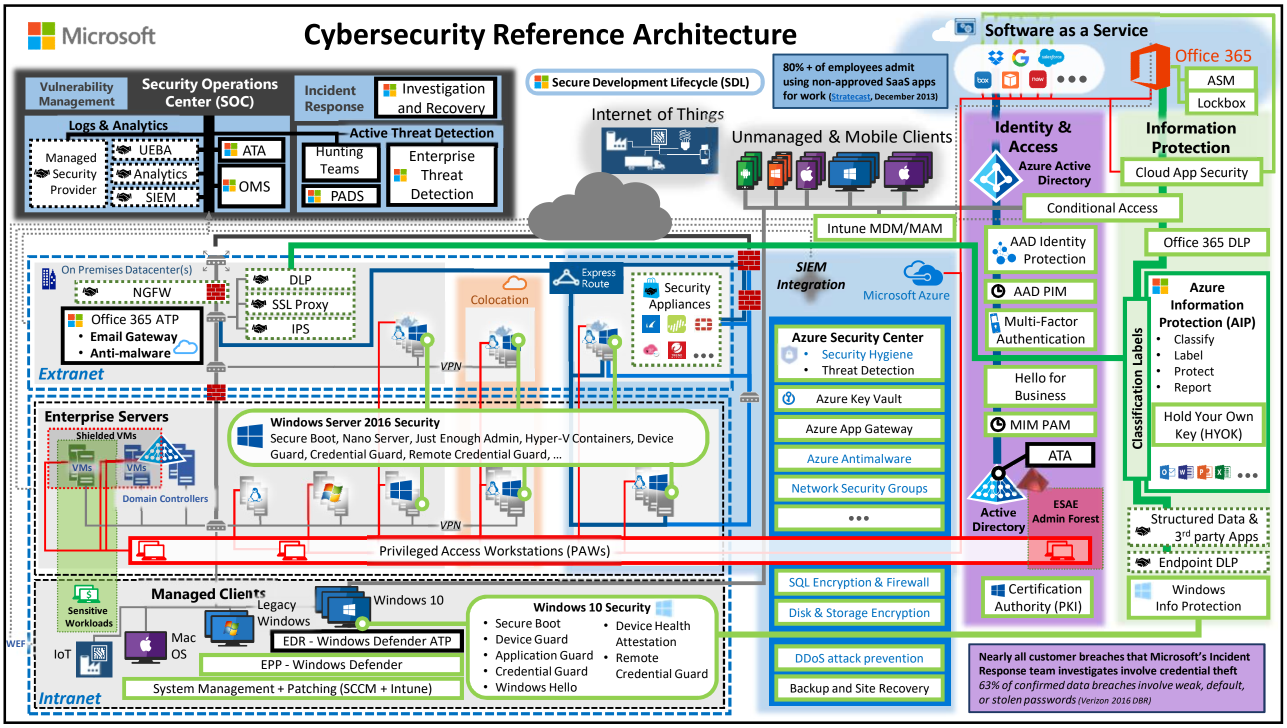
ITechDays 1-2 czerwca 2017

AM I SAFE?

NOT EXACTLY …

IT SECURITY IS MORE COMPLICATED…

Cybersecurity Reference Architecture



Microsoft

Vulnerability Management

Security Operations Center (SOC)

Incident Response

Investigation and Recovery

Logs & Analytics

Managed Security Provider

UEBA

Analytics

SIEM

ATA

OMS

Active Threat Detection

Hunting Teams

PADS

Enterprise Threat Detection

Secure Development Lifecycle (SDL)

80% + of employees admit using non-approved SaaS apps for work (Stratecast, December 2013)

Internet of Things

Unmanaged & Mobile Clients

Software as a Service

Office 365

ASM

Lockbox

Identity & Access

Azure Active Directory

Information Protection

Cloud App Security

Conditional Access

Intune MDM/MAM

AAD Identity Protection

Office 365 DLP

On Premises Datacenter(s)

NGFW

DLP

SSL Proxy

IPS

Office 365 ATP
- Email Gateway
- Anti-malware

Extranet

Colocation

Express Route

Security Appliances

VPN

SIEM Integration

Microsoft Azure

Azure Security Center
- Security Hygiene
- Threat Detection

Azure Key Vault

Azure App Gateway

Azure Antimalware

Network Security Groups

•••

AAD PIM

Multi-Factor Authentication

Hello for Business

MIM PAM

ATA

Active Directory

ESAE Admin Forest

Classification Labels

Azure Information Protection (AIP)
- Classify
- Label
- Protect
- Report

Hold Your Own Key (HYOK)

Enterprise Servers

Shielded VMs

VMs

VMs

Domain Controllers

Windows Server 2016 Security

Secure Boot, Nano Server, Just Enough Admin, Hyper-V Containers, Device Guard, Credential Guard, Remote Credential Guard, …

VPN

Privileged Access Workstations (PAWs)

Structured Data & 3rd party Apps

Endpoint DLP

Sensitive Workloads

Managed Clients

Legacy Windows

Windows 10

Mac OS

IoT

WEF

EDR - Windows Defender ATP

EPP - Windows Defender

System Management + Patching (SCCM + Intune)

Intranet

Windows 10 Security
- Secure Boot
- Device Guard
- Application Guard
- Credential Guard
- Windows Hello
- Device Health Attestation
- Remote Credential Guard

SQL Encryption & Firewall

Disk & Storage Encryption

DDoS attack prevention

Backup and Site Recovery

Certification Authority (PKI)

Windows Info Protection

Nearly all customer breaches that Microsoft's Incident Response team investigates involve credential theft

63% of confirmed data breaches involve weak, default, or stolen passwords (Verizon 2016 DBR)

ITechDays

1-2 czerwca **2017**

```
            uu$:$:$:$:$:$uu
         uu$$$$$$$$$$$$$$$$$uu
        u$$$$$$$$$$$$$$$$$$$$$u
        u$$$$$$$$$$$$$$$$$$$$$$$u
      u$$$$$$$$$$$$$$$$$$$$$$$$$u
      u$$$$$$$$$$$$$$$$$$$$$$$$$u
      u$$$$$$*   *$$$*   *$$$$$$u
      *$$$$*      u$u       $$$$*
       $$$u       u$u       u$$$
       $$$u      u$$$u      u$$$
        *$$$$uu$$$   $$$uu$$$$*
         *$$$$$$$*   *$$$$$$$*
           u$$$$$$$u$$$$$$$u
            u$*$*$*$*$*$*$u
 uuu        $$u$ $ $ $ $u$$       uuu
u$$$$        $$u$u$u$u$u$$       u$$$$
 $$$$$uu      *$$$$$$$$$*     uu$$$$$$
u$$$$$$$$$$$      *****    uuuu$$$$$$$$$
$$$$***$$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
         uuuu **$$$$$$$$$$uuu
 u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
 $$$$$$$$$$****           **$$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
     $$$*     PRESS ANY KEY!       $$$$*
```

QUESTIONS?

ITechDays