Microsoft

The security philosophy

Threats targeting the hybrid & cloud identity platform

External resources disclaimer

This material includes links to external publicly available articles, projects, and research papers which are provided to you as a convenience and for informational purposes only.

Microsoft bears no responsibility for the accuracy, legality, content or any other aspect of the external site. Use of external hyperlinks does not constitute an endorsement by Microsoft of the linked content.

The external content referenced in this document belongs exclusively to their respective author(s). Inclusion in this presentation does not grant you with any right on the external content. You must comply with the original source’s applicable policies.

How to use this document

Why this document?

This document is provided as a companion of the video lessons. Additional information is included here which would not fit the video format or would exaggeratedly lengthen the videos. As you are watching the videos, the instructor will point you to additional content in this document.

Structure

The structure of this slide deck follows the structure of the lessons. One slide deck is provided for each module. The slide deck has the same structure (naming of chapters and sections) as the associated video so that you can quickly jump to the slides of the lesson you are currently watching.

Foreword

This deck contains some design artefacts which all have their importance…

This sticky note icon is used to introduce the **abbreviation** of a concept or a technical word. Once the abbreviation has been introduced, the full version is no longer mentioned.

You will also find a list of all abbreviations at the end of the deck.

We were all young once. A section with this icon will tell you the **history** you might have missed by not working with the technology for the last 20 years.

Just because you are new does not mean you do not have to know how we got here!

Professor Useful will introduce some **tricky technical details** which might not seem relevant at first but could end up being really useful if you want to dig deeper in the technology.

This frame contains…

- Takeaways so important that we framed them

How to know the slide level

This deck contains 3 different content levels:

1. Regular level, the common slide
2. Advanced level, a slide with this indicator at the top left 

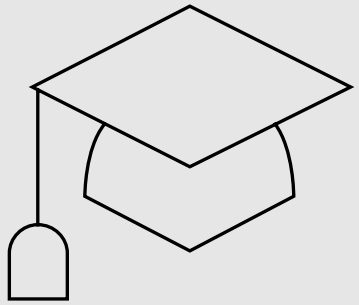
3. Additional content, all hidden slides

Sequence

1

The security philosophy

Learning Objectives



Identify important concepts to follow when working on projects to enhance the security of an environment

Agenda

1. AD and Azure AD: perfect targets
2. Defense in depth
3. The initial breach
4. The attacker's perspective
5. Introduction to the phases of an attack

Chapter

2.1.1

AD and Azure AD: perfect targets

🎯 Explain why identity platforms are targets

Is AD or AAD really the target?

AD/AAD is targeted but not for what it is, but for what it gives access to

AD or AAD is not the initial breach

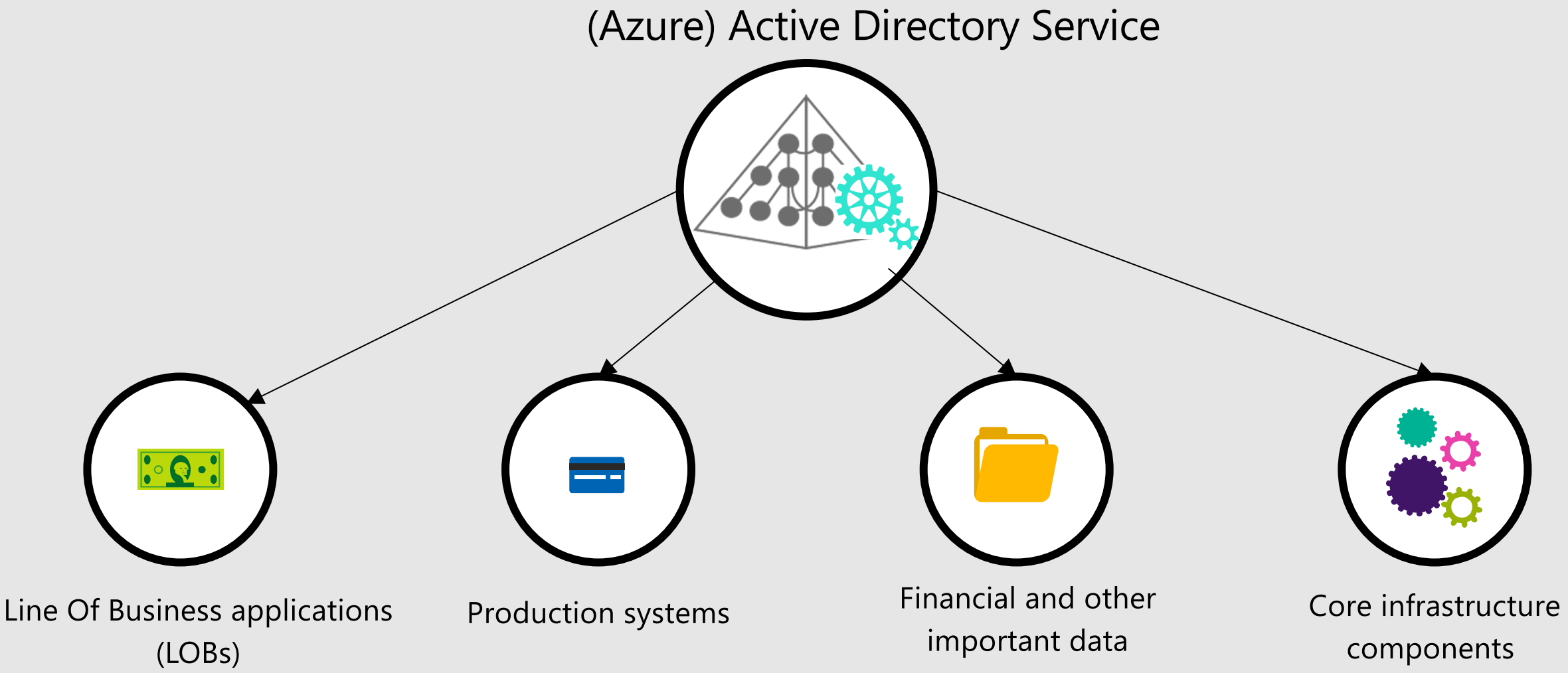
The user' device is the battlefield

- And by extension, the identities on these devices are the targets

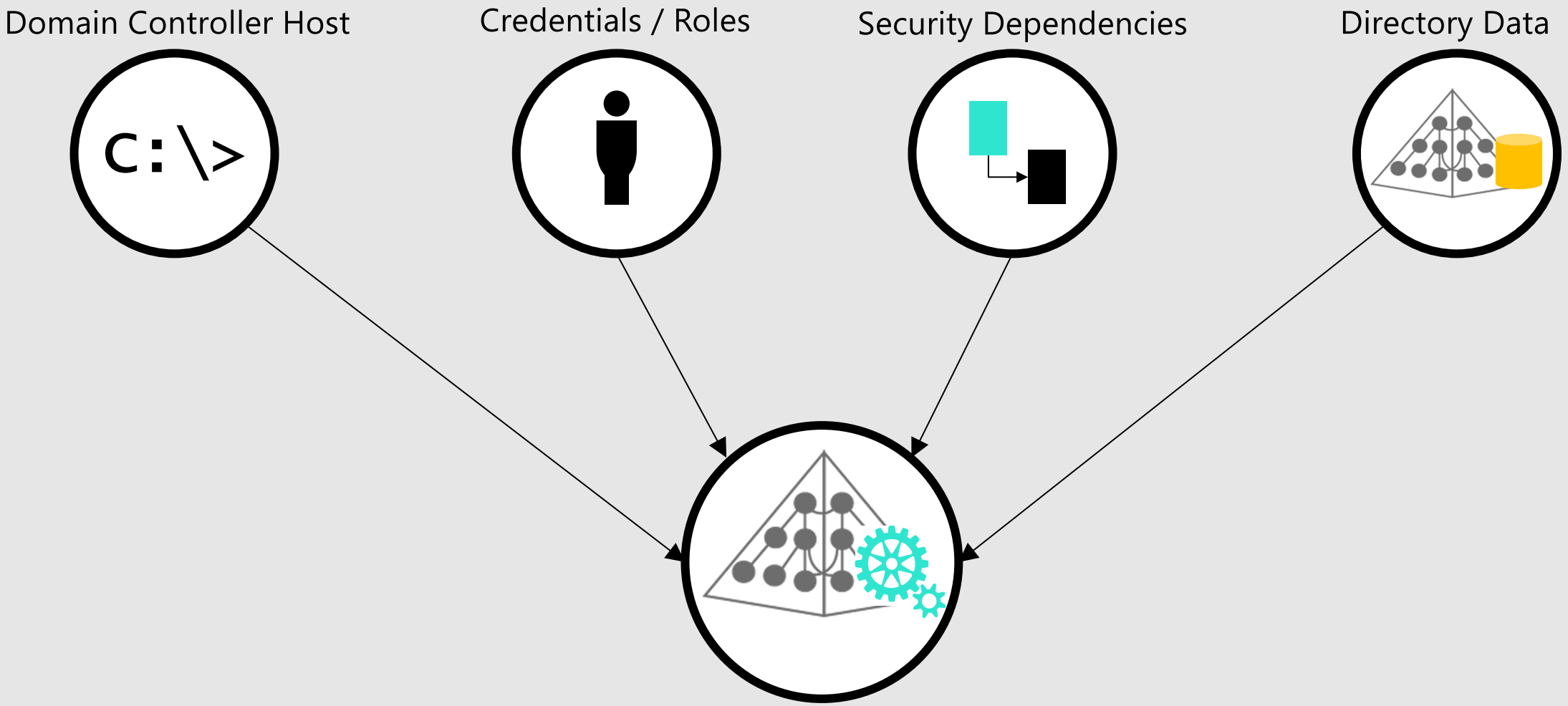
Initial breaches can have various forms

- 0-day
- Phishing
- Password discovery attacks

Identities have power over…

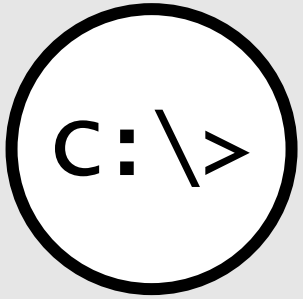


Means of control over AD



Gain control of the Domain Controller host

Domain Controller Host



- If you have physical access to a DC
  - Or its hard drive
  - Or its backup
- If you have physical access to the virtual platform of a virtual DC
  - Or are an admin of this platform

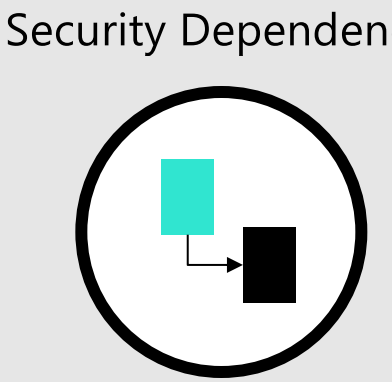
Then you control the environment!

Gain control of the privileged identities

Credentials / Roles

- If you found the password of an admin account, you can control the platform
- If you stole the credentials of a privileged account, then you can control the platform

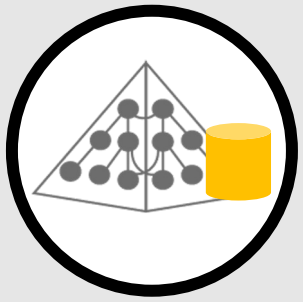
Gain control of security dependencies



- If you have agents running on DCs, whoever owns these agents - owns the DCs
  - Backup agents
  - Monitoring agents
  - Threat detection agents
  - Software deployment agents
  - …
- If integrated applications have privileges in AD, then the admins of those applications own AD

Gain control through directory data

Directory Data



- Incorrect and permissive delegations will allow new control paths
  - Incorrect Group Policy permissions
  - Incorrect OU permissions
  - Incorrect privileges on applications

- When permissions are given to non-privileged accounts, they become unsuspected privileged accounts

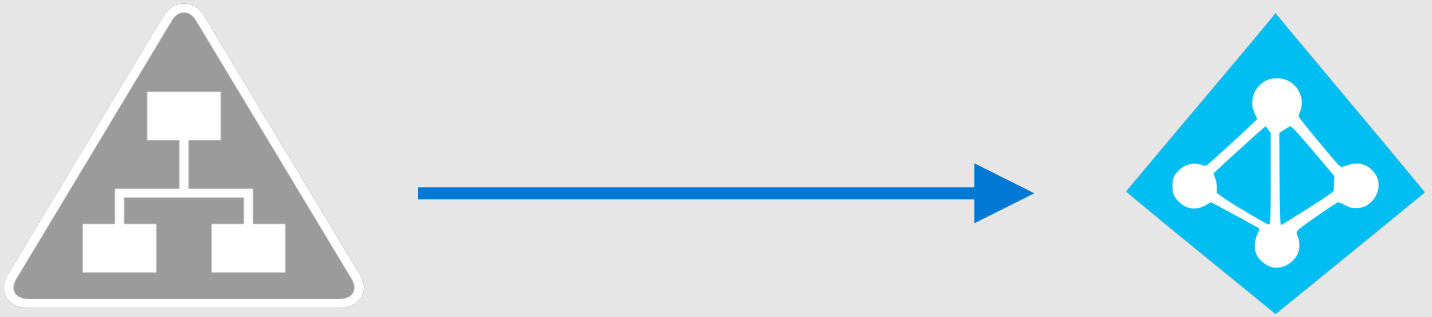
Adv.

Install from Media

IFM

- Feature that allows promotion of new domain controllers from pre-seeded set of files
- Created to speed up promotion time in high latency environments
- IFM contains the database and SYSVOL
- IFM are as sensitive as a domain controllers' backups
- You need to monitor if IFM are being created on your domain controllers

Is your Azure AD platform safe by default?



- Azure AD Connect Sync
- AD FS
- PTA agent

🔒 Your cloud environment is as safe as your on-premises environment

Chapter

2.1.2

Defense strategy

🎯 Describe the concept of defense in depth

What's the plan?

1. Assume breach
2. Defense in depth

Assume breach

You don’t know what you don’t know

- ? An attacker might have gotten into the system in the past
- ? An attacker may currently be in the system
- ? We can’t expect to protect our environment against attack techniques which do not exist yet

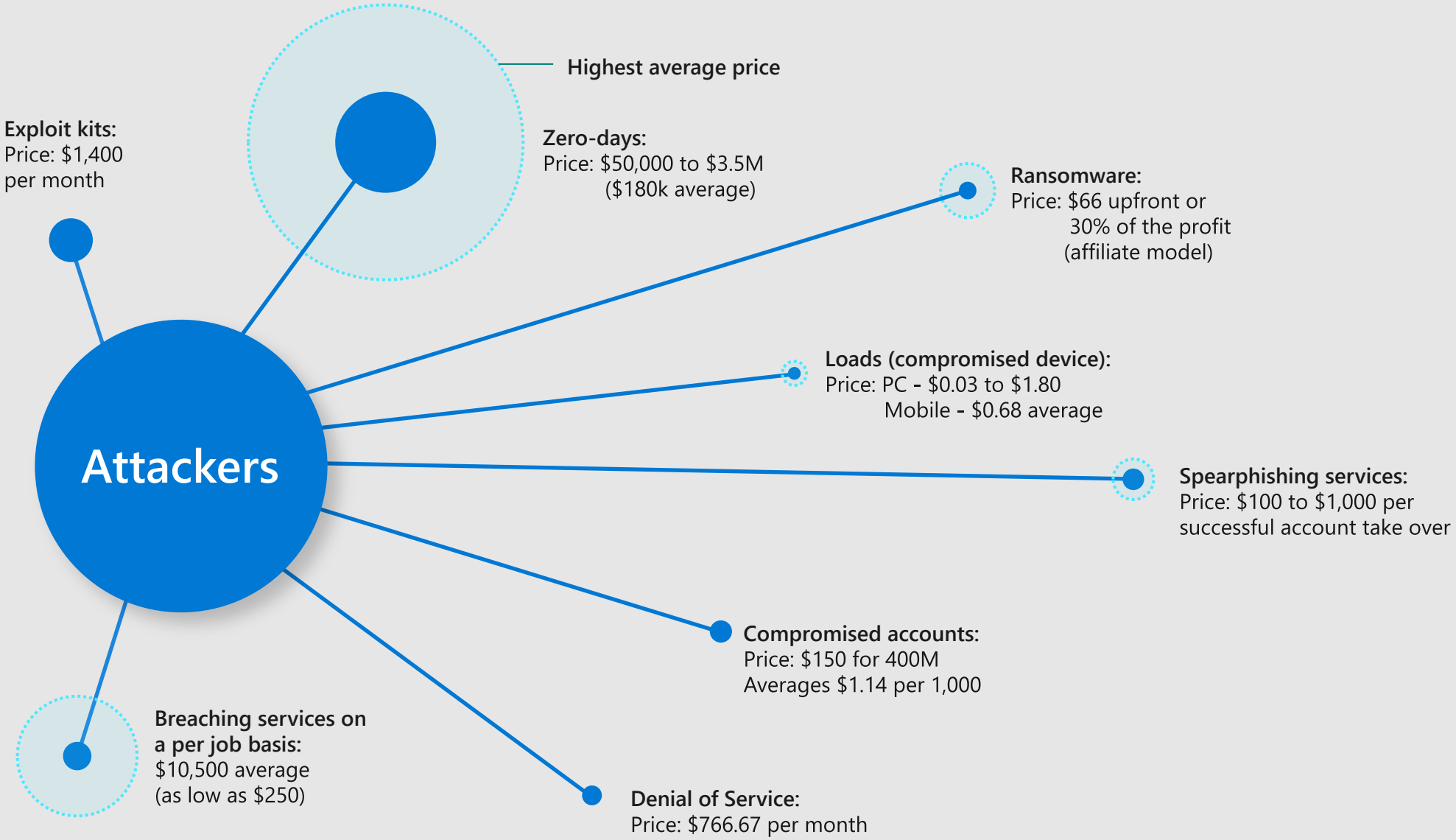
Defense in depth

- You want to make it…
  - 💪 Harder
  - ⏱️ Longer
  - 📢 Louder

  … for the attacker

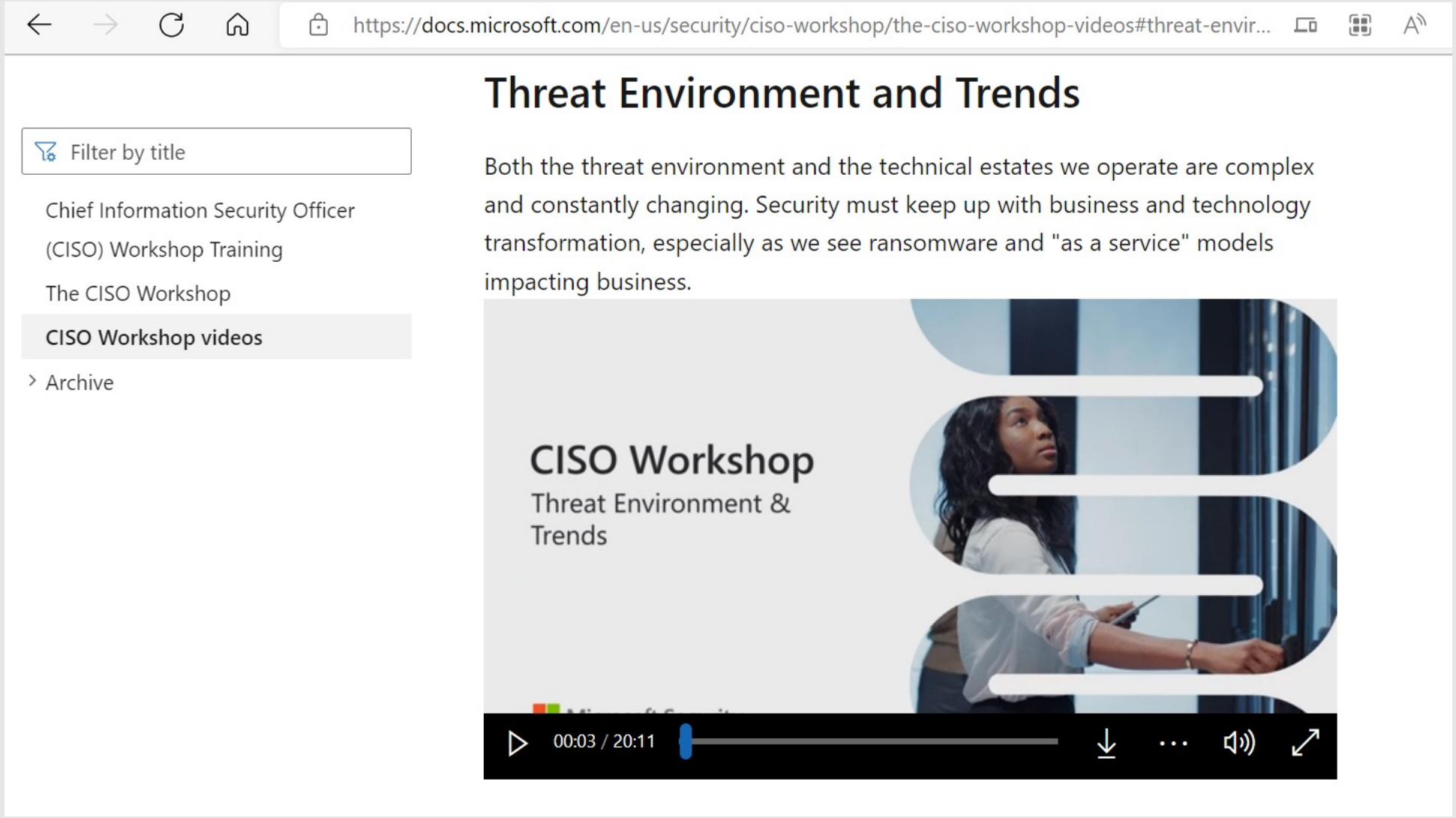
- You want to be an unattractive target

Attack services are cheap

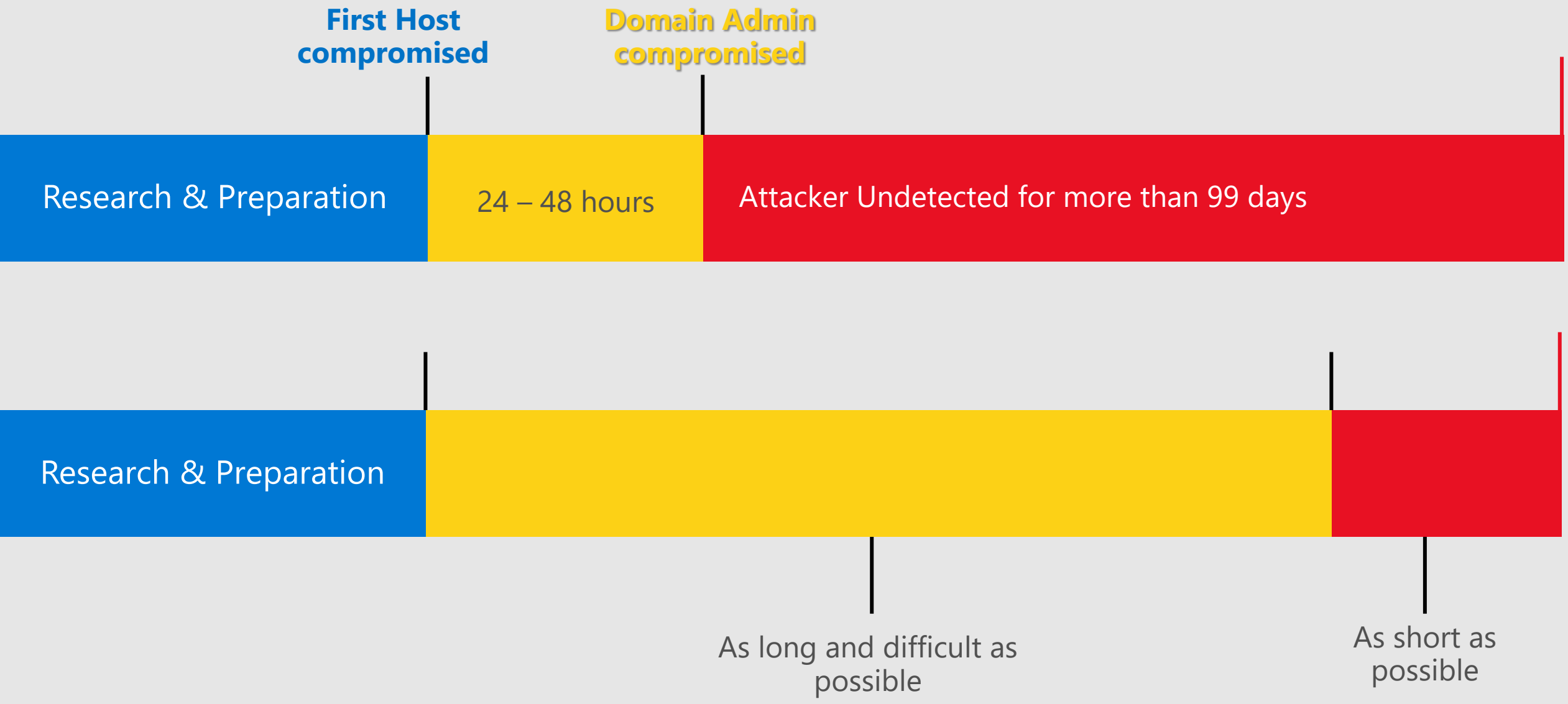


Adv.

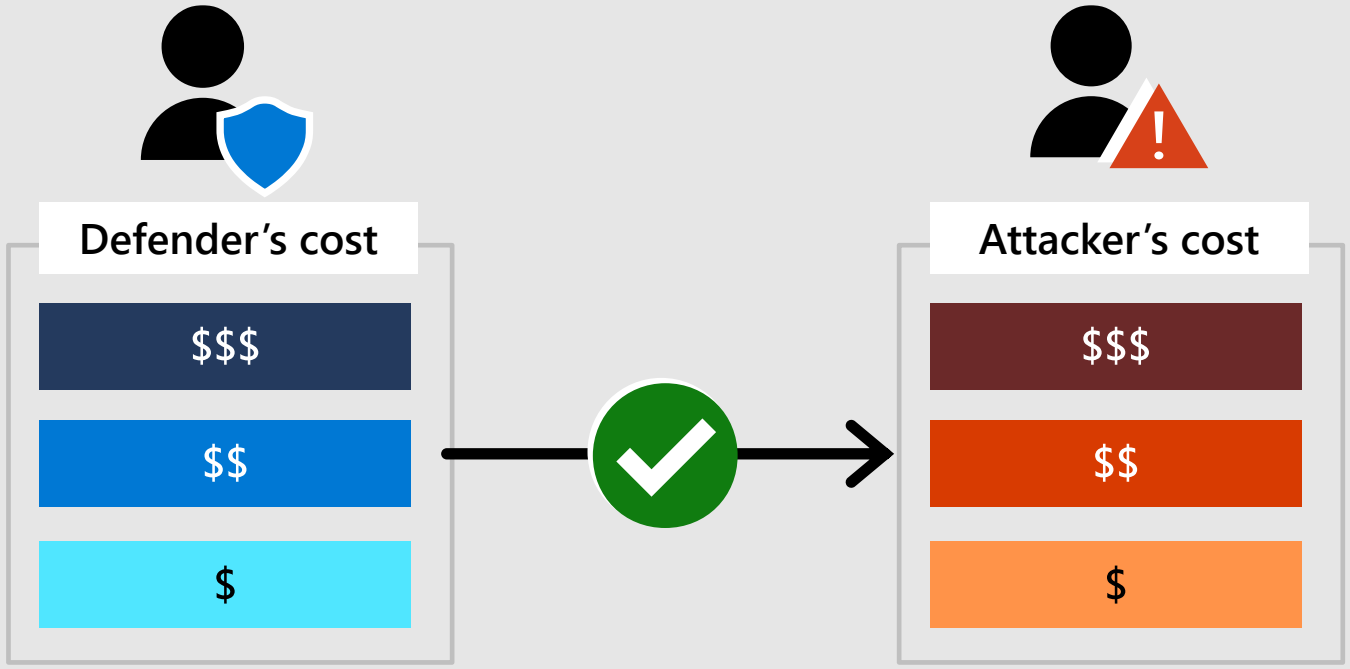
Threat Environment and Trends



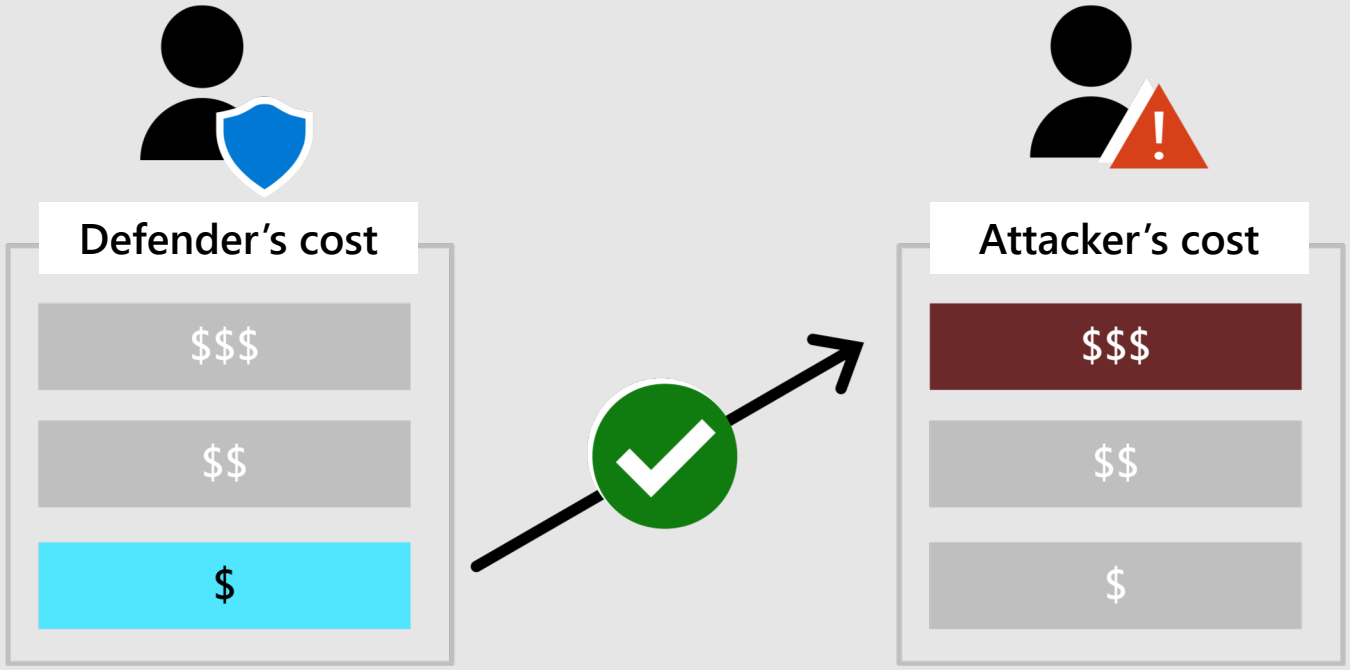
Disrupt the attack timeline



Disrupt Attackers



Disrupt Attackers



Adv.

A layered approach to Security

- Physical Security

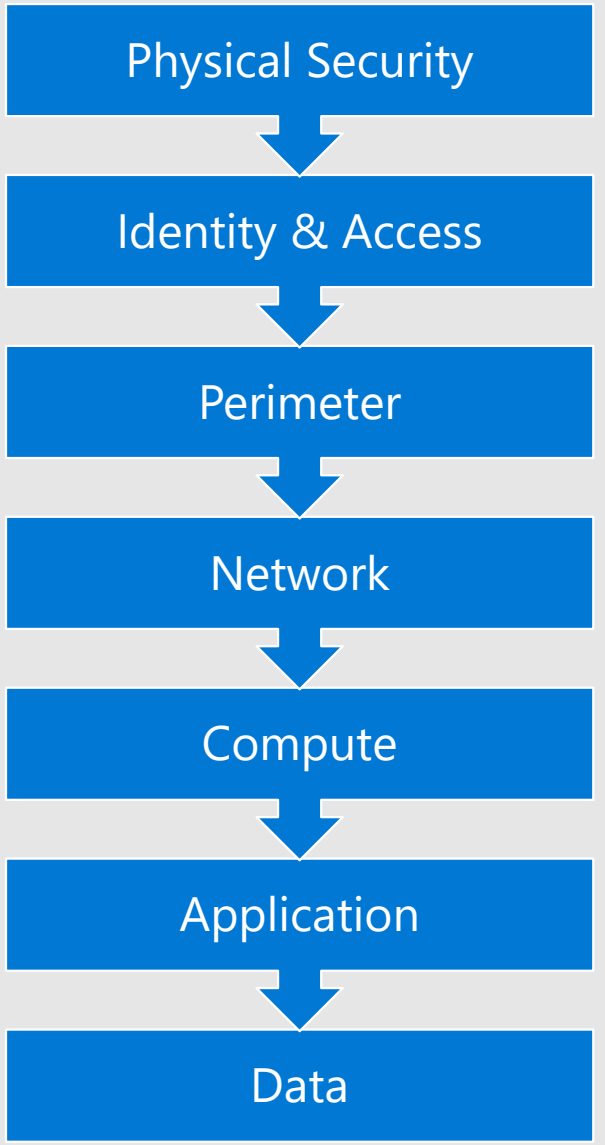
  Physical building security and controlling access to computing hardware within the data center is the first line of defense.

- Identity & Access

  Control access to infrastructure, change control
  Use single sign-on and multi-factor authentication
  Audit events and changes

- Perimeter

  Use distributed denial-of-service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for end users
  Use perimeter firewalls to identify and alert on malicious attacks against your network



A layered approach to Security

- Networking

  Limit communication between resources through segmentation and access controls

  Deny by default

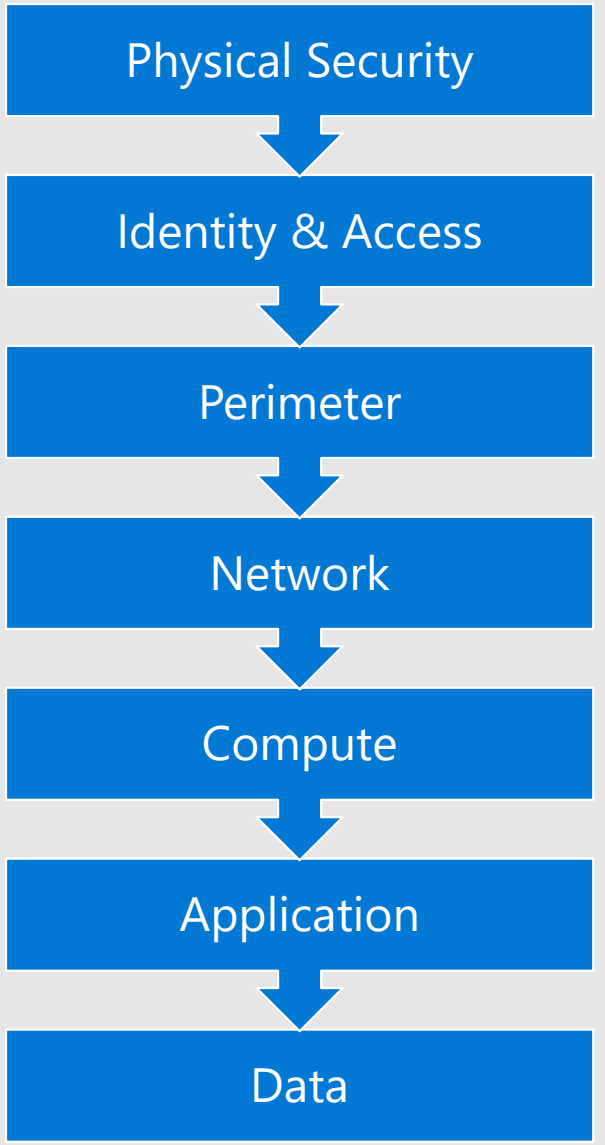
  Restrict inbound internet access and limit outbound where appropriate

  Implement secure connectivity to on-premises networks

- Compute

  Secure access to virtual machines

  Implement endpoint protection and keep systems patched and current



A layered approach to Security

In almost all cases, attackers are after data!

- Application

  Ensure applications are secure and free of vulnerabilities

  Store sensitive application secrets in a secure storage medium

  Make security a design requirement for all application development

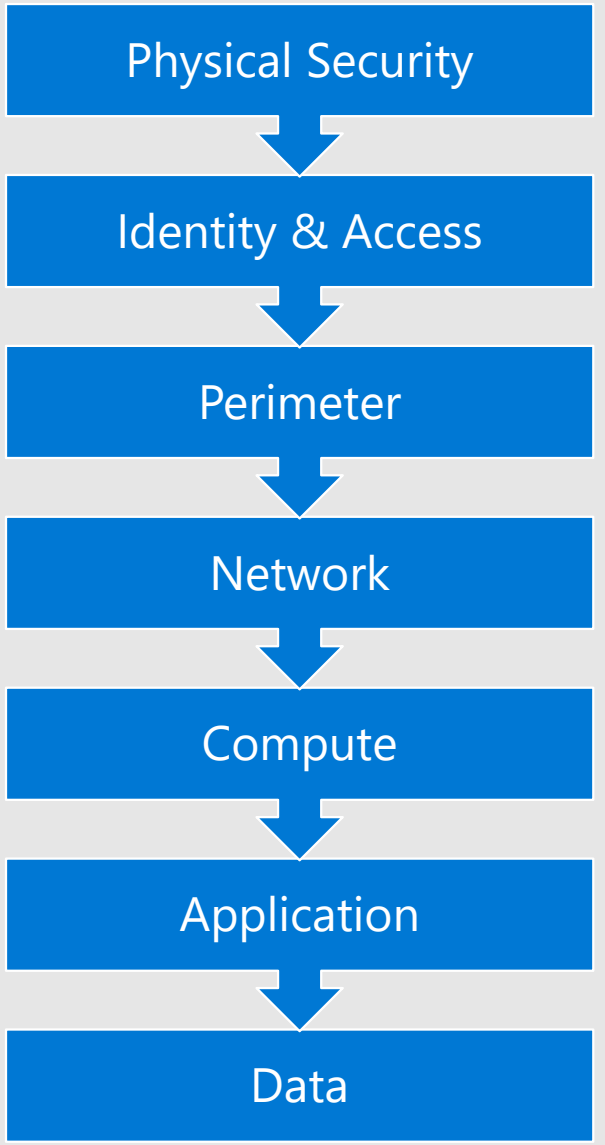
- Data

  Stored in a database

  Stored on disk inside virtual machines

  Stored on a SaaS application such as Office 365

  Stored in cloud storage



Chapter

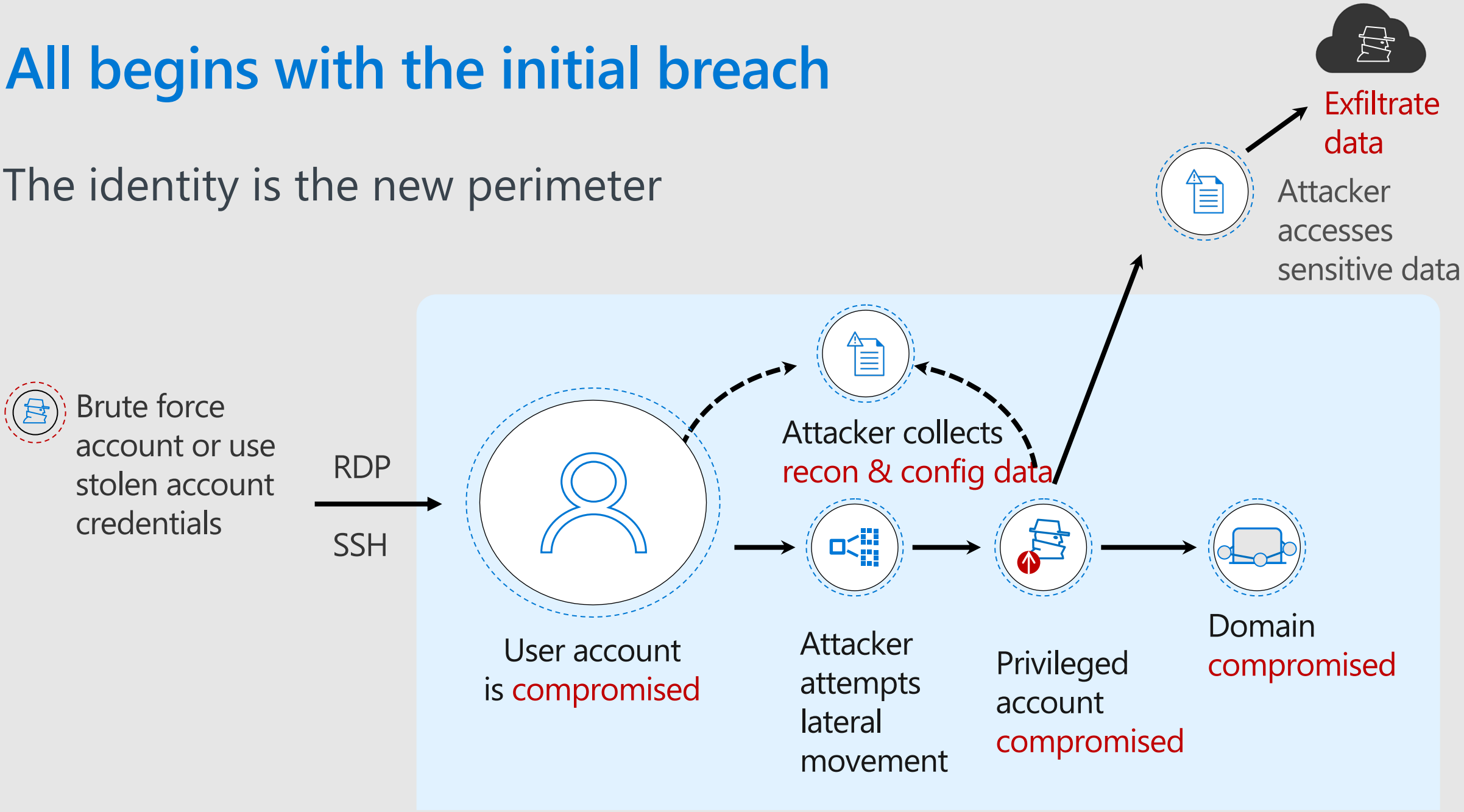
2.1.3

The initial breach

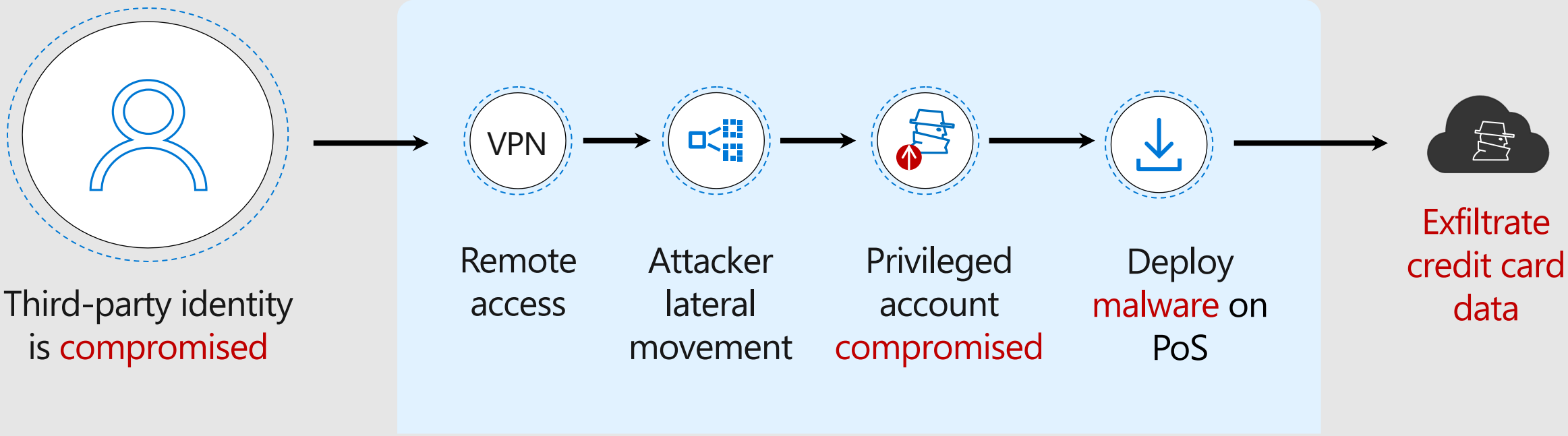
🎯 Explain the concept of the initial breach

All begins with the initial breach

The identity is the new perimeter



Real life examples



Real life examples

- Supply chain attacks

  The goal is to access source codes, build processes, or update mechanisms by infecting legitimate apps to distribute malware.

Advanced Persistent Threats

APT

- IT's a cyber attack where the attacker gains and maintains unauthorized access to the target environment
  - Remains undetected for a significant period

- The attacker will monitor, recognize and relay information and sensitive data.
  - The intention of an APT is often to exfiltrate or steal data

- Use two primary methods of persistence
  - Compromised endpoints and compromised credentials.

Chapter

2.1.4

The attacker's perspective

🎯 Describe an attacker's perspective

Think like an attacker

Which nodes contain harvestable privileged credentials?

Which nodes can attacker access using these credentials?

What is the cost of reaching a node?

Bloodhound

- Open-source tool used by attackers to visualize control paths leading to identified targets using a Graph database (Neo4j)
  - Ideally to domain admin accounts
- It shows control path for both AD DS and Azure AD
- The collection tool is called Sharpound
  - But you can also inject data collected by other tools

Defensive teams should also use it!

Stormspotter

- Open-source tool developed by Microsoft Security Teams to visualize control paths of Azure objects using a graph database (neo4j)
- It shows control path for Azure resources
- The collection tool is called Stormcollector

Defensive teams should also use it!

Adv.

Thinking Like an Attacker

Servers

Server Administrator

All Local Data

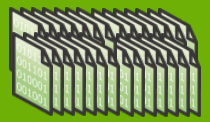
Active User Credentials

SAM: NT Hashes

Domain Admin

PtH

Domain Admin Access



All Credentials (NT Hashes)

All Active Directory Data (Full Control)

All Data

Domain Controllers

User Access

PtH

Server Admin

PtH

Domain Admin

PtH

Domain Admin Logon

Access Data

Patient Zero

Workstation Administrator

All Local Data

Active User Credentials

Secure Accounts Manager (SAM): NT Hashes

Service Account Credentials

PtH (Local accounts)

Credential Re-use

All Local Data

Active User Credentials

SAM: NT Hashes

SYSTEM or Administrator

Establish Beachhead

User Access

User Action

Malware Install

Beacon, C&C

All Active Directory Data (Read)

User's Data and Keystrokes

User Credential

- Vuln and Exploit
- User = Admin

Elevation

All Workstations

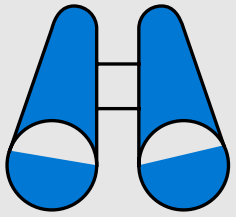
Chapter

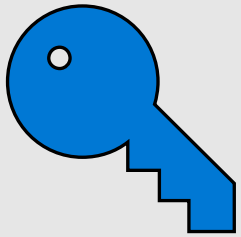
2.1.5

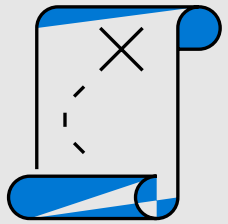
Introduction to the phases of an attack

🎯 Describe the different phases of an attack

Attacks generic phases







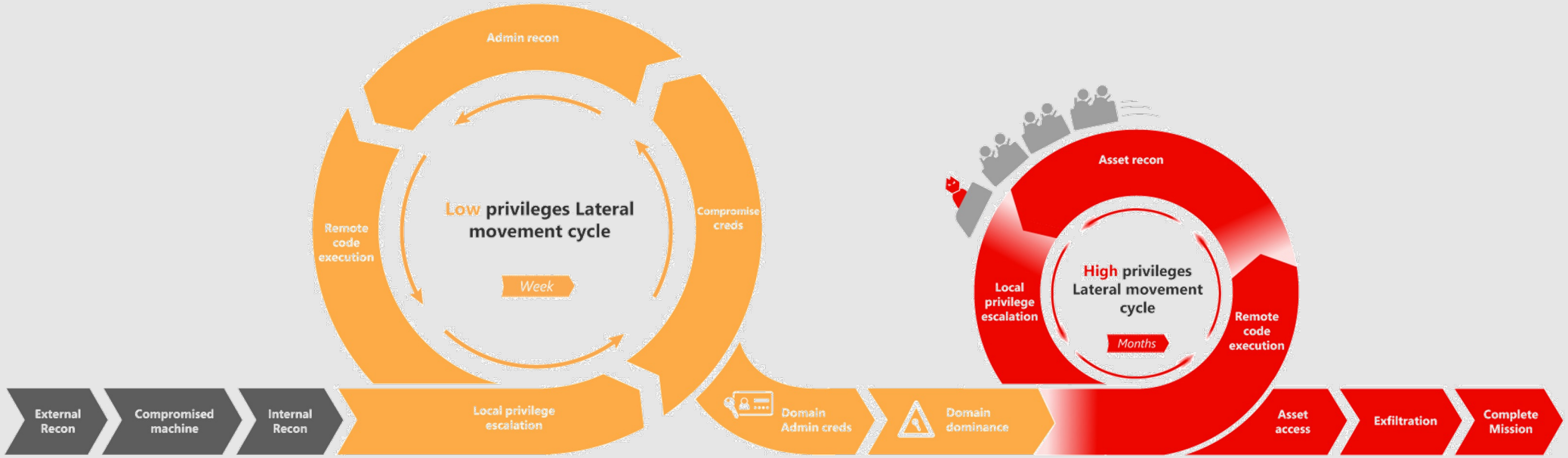
Reconnaissance

Compromised credentials

Lateral movement

Domination

Attack Kill Chain model



1. **External reconnaissance:** Attempts to locate potential penetration point to map and understand the layout and structure of victim's environment.
2. **Compromise machine/Initial foothold:** Gains access to victim's network.
3. **Initial internal reconnaissance:** Works on "mapping" the internal network layout and identifying "interesting" areas.
4. **Low privileges "Lateral movement" cycle:** Begins to move across devices in the network to "improve position" to reach privileged credentials.
5. **Domain admin credentials:** Gains access to privileged credentials by moving "enough" to get to a machine where these credentials exist.
6. **Domain persist:** they want, whenever and however within the environment.
7. **High privileges "Lateral movement" cycle:** Uses previously compromised privileged credentials to move towards the area that includes the asset of interest to the attacker.
8. **Asset access:** Accesses high-value assets.
9. **Exfiltration:** Transfers the collected information outside of the victims' network
10. **Persistence:** Gains full control of the domain and the ability to do whatever used for the attackers goals.

What is MITRE ATT&CK?

- Adversarial Tactics, Techniques and Common Knowledge (ATT&CK)
- Designed to document common Techniques, Tactics, and Procedures (TTP) of Advanced Persistent Threats (APT)
- Provides matrices of known adversary techniques cataloged by tactics, techniques, and sub-techniques
- Can document detections and behaviors from security products and map to MITRE ATT&CK
- Assists in identifying and prioritizing gaps in security detection and protection

MITRE phases

1. Reconnaissance
2. Resource Development
3. Initial Access
4. Execution
5. Persistence
6. Privilege Escalation
7. Defense Evasion
8. Credential Access
9. Discovery
10. Lateral Movement
11. Collection
12. Command and Control
13. Exfiltration
14. Impact

Adv.

Tactics and Techniques

Tactics

Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		System Shutdown/Reboot
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		Stored Data Manipulation
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Scheduled Task	Hooking	Port Monitors	Extra Window Memory Injection	Two-Factor Authentication Interception	System Service Discovery			Uncommonly Used Port		
	Scripting	Hypervisor	PowerShell Profile	File and Directory Permissions Modification		System Time Discovery			Web Service		
	Service Execution	Image File Execution Options Injection	Process Injection	File Deletion		Virtualization/Sandbox Evasion					
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Scheduled Task	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Service Registry Permissions Weakness	Gatekeeper Bypass							
	Source	Launch Daemon	Setuid and Setgid	Group Policy Modification							
	Space after Filename	Launchctl	SID-History Injection	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Startup Items	Hidden Users							
	Trap	Local Job Scheduling	Sudo	Hidden Window							
	Trusted Developer Utilities	Login Item	Sudo Caching	HISTCONTROL							
	User Execution	Logon Scripts	Valid Accounts	Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver	Web Shell	Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		PowerShell Profile		Modify Registry							
		Rc.common		Mshta							
		Re-opened Applications		Network Share Connection Removal							
		Redundant Access		NTFS File Attributes							
		Registry Run Keys / Startup Folder		Obfuscated Files or Information							
		Scheduled Task		Parent PID Spoofing							
		Screensaver									
		Security Support Provider									

- **Tactics** - High Level Objectives
- **Techniques** – attack method used

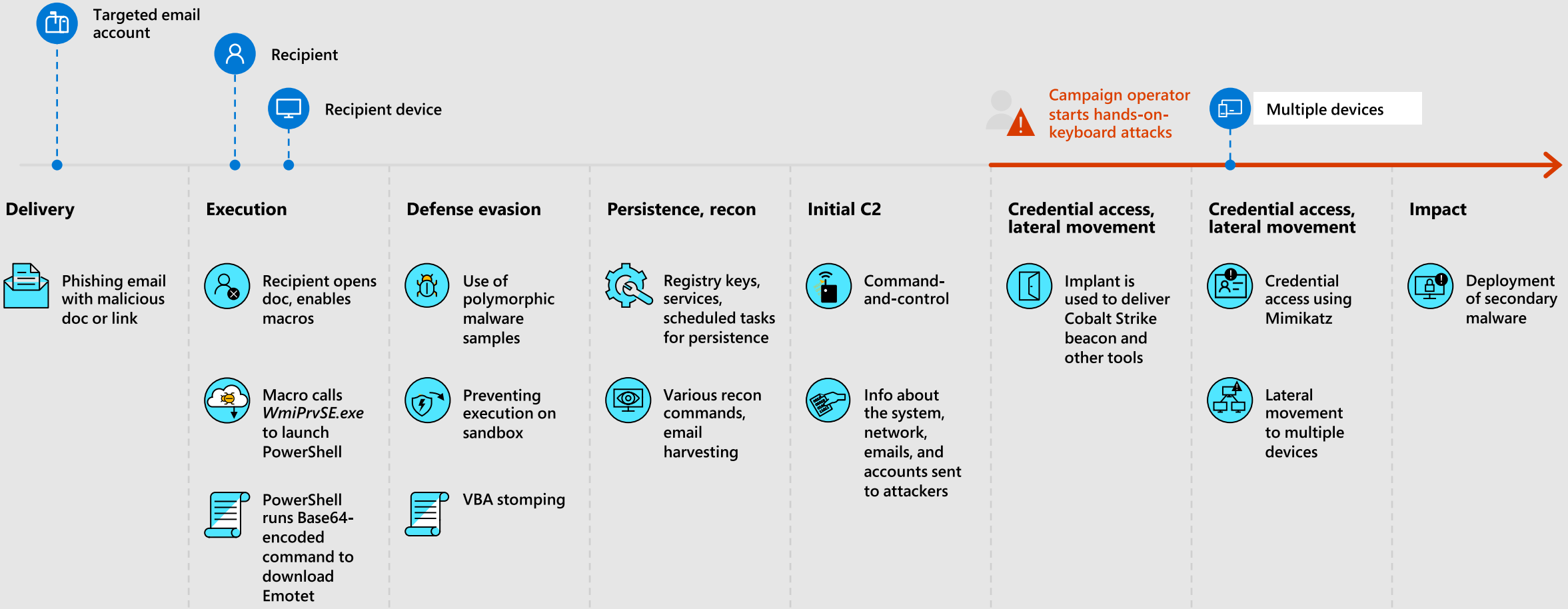
Why use MITRE ATT&CK?

- Determine the effectiveness of cybersecurity capabilities in preventing, detecting and responding to events
- Identify gaps in security coverage
- Build a common language and approach across all tools and services
- Build defensive controls roadmap
- Provide evidence for cost effective mitigations
- Facilitate cybersecurity conversations

Adv.

I want Money – Story of a Ransomware

Emotet/Ryuk Ransomware campaign



Detections by Microsoft

SIEM

SOAR

- We highly recommend deploying **Security Information and Event Management /Security Automation and Automated Response** and deploying an e**X**tended **D**etection and **R**esponse solution

XDR

- Microsoft offers solutions in this space

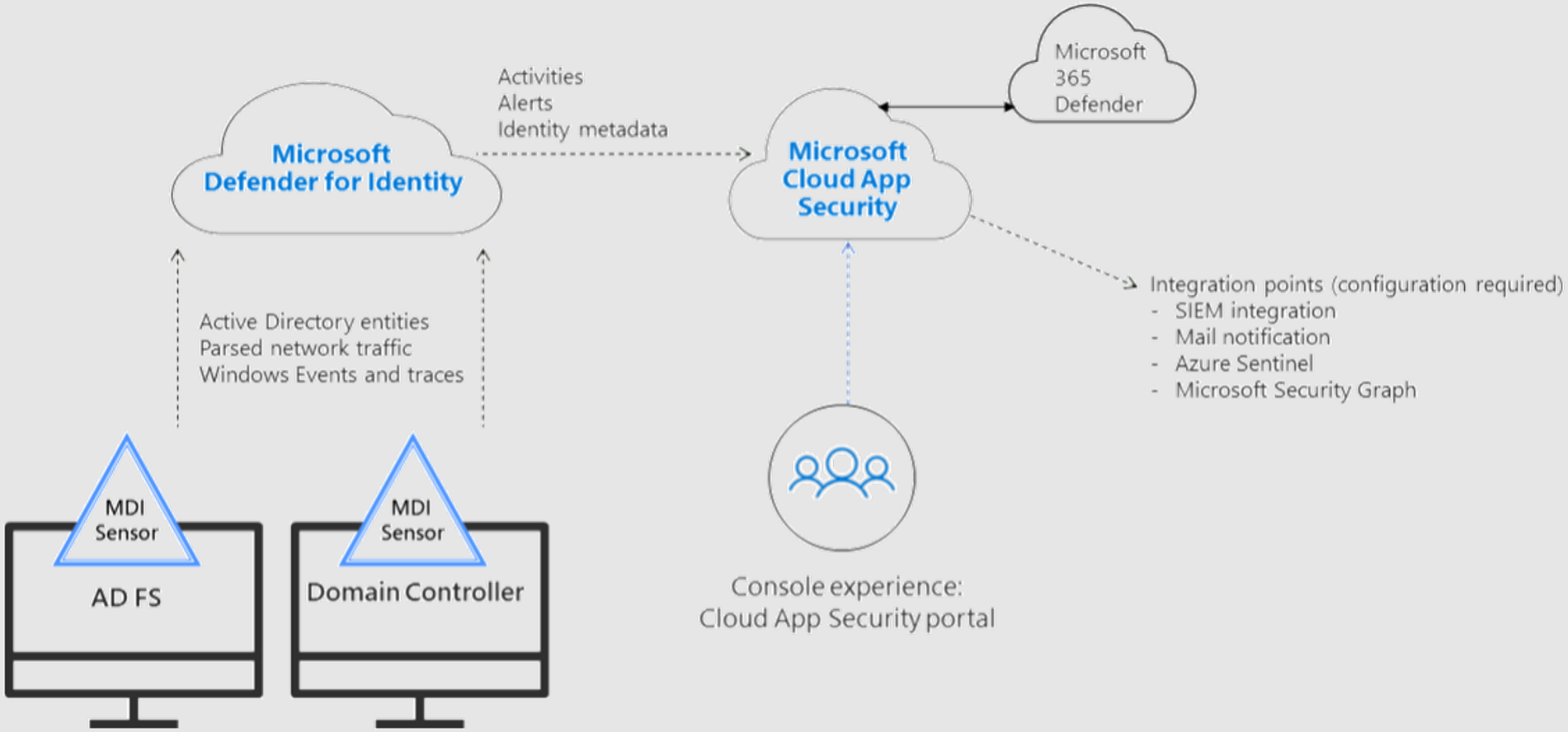
- Focus on Microsoft Defender for Identity

Microsoft Defender for Identity

MDI

- Monitor your domain controllers and AD FS servers
- A platform to **identify** advanced security attacks **before** they cause damage

Microsoft Defender for Identity Architecture



Microsoft

List of abbreviations

AD DS – Active Directory Domain Services
AAD – Azure Active Directory
SCCM – System Center Configuration Manager
SCOM – System Center Operation Manager
IFM – Install From Media
XDR – eXtended Detection and Response
SIEM - Security information and event management
SOAR - Security orchestration automated response
MDI – Microsoft Defender for Identity