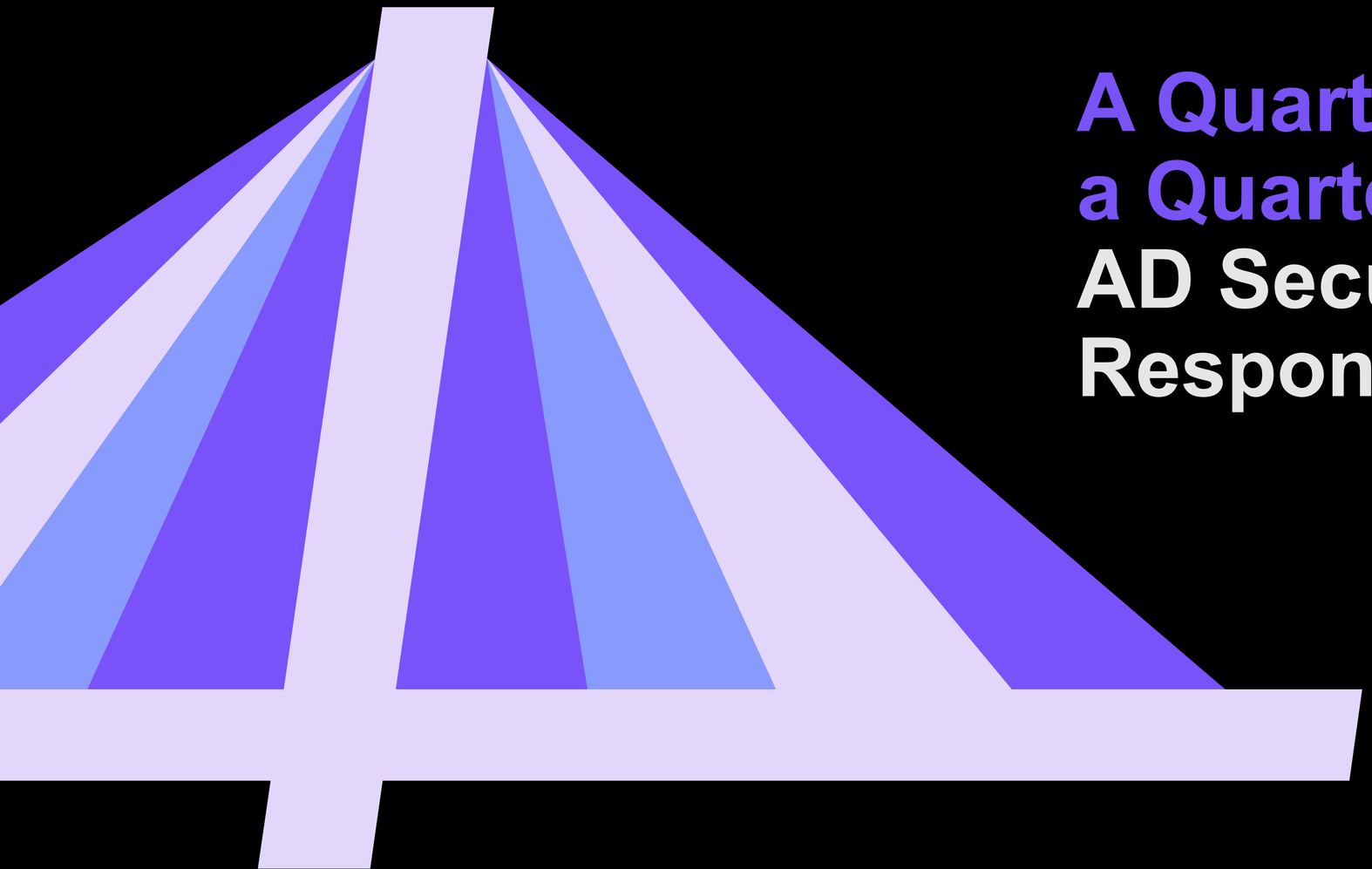
HYBRID IDENTITY PROTECTION conf25

CHARLESTON



# A Quarter Century, a Quarter Million Breaches: AD Security & Incident Response in 2025

HYBRID IDENTITY PROTECTION conf25
CHARLESTON

# Michael Van Horenbeeck

CEO @ The Collective

*Microsoft Security MVP*

*Author of Microsoft 365 Security for IT Pros*

*Zero Trust Zone Podcast*

*Labeled by employees as dinosaur **

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

# The Challenge

Mandiant Reports

**90%**

of incidents involve directly or indirectly Active Directory.

IBM Data Breach Report (2025):

**241 days**

is the average time to identify (detect) and contain a breach

IBM Reports:

**IAM**

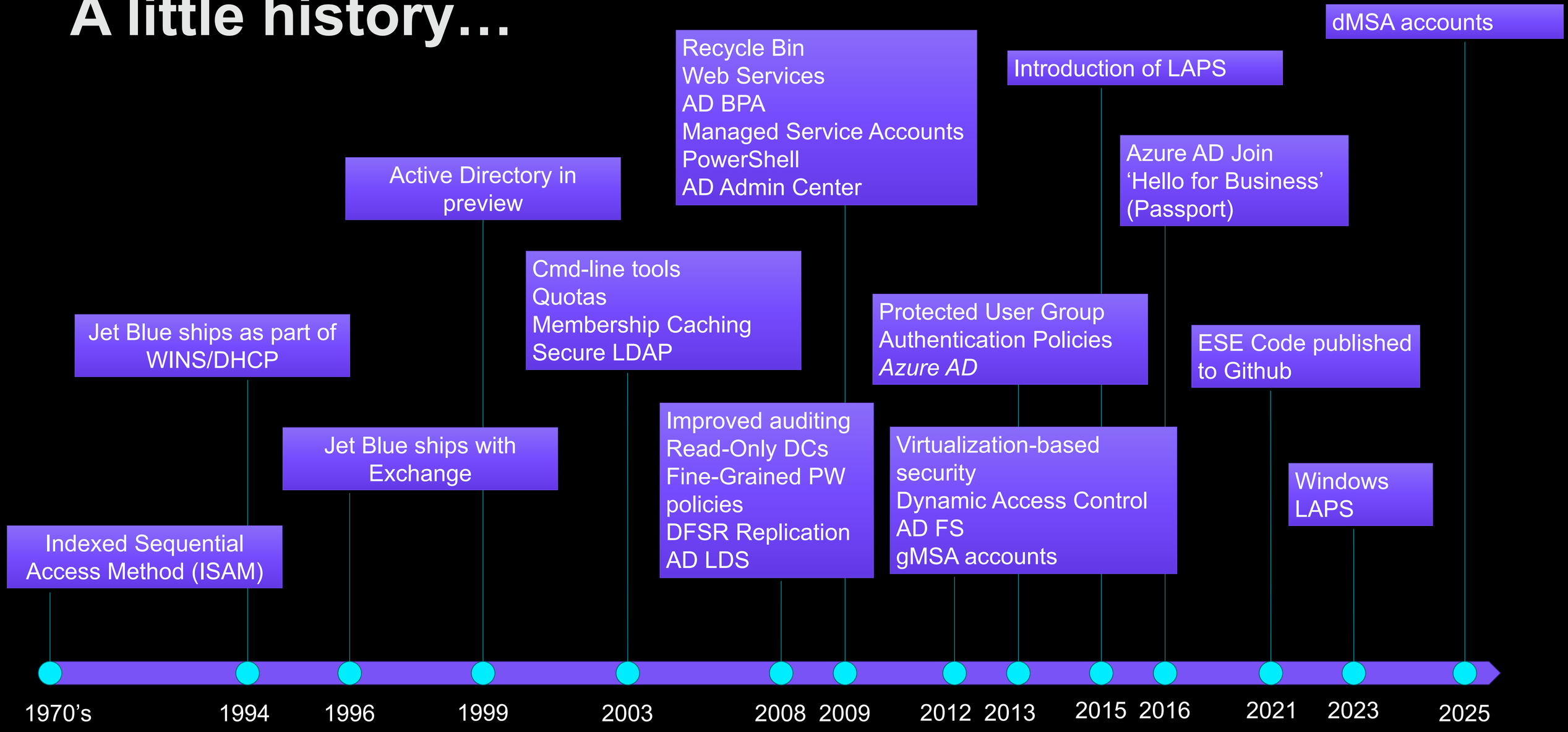
identified as the top cost-reducing investment; especially non-human identities.

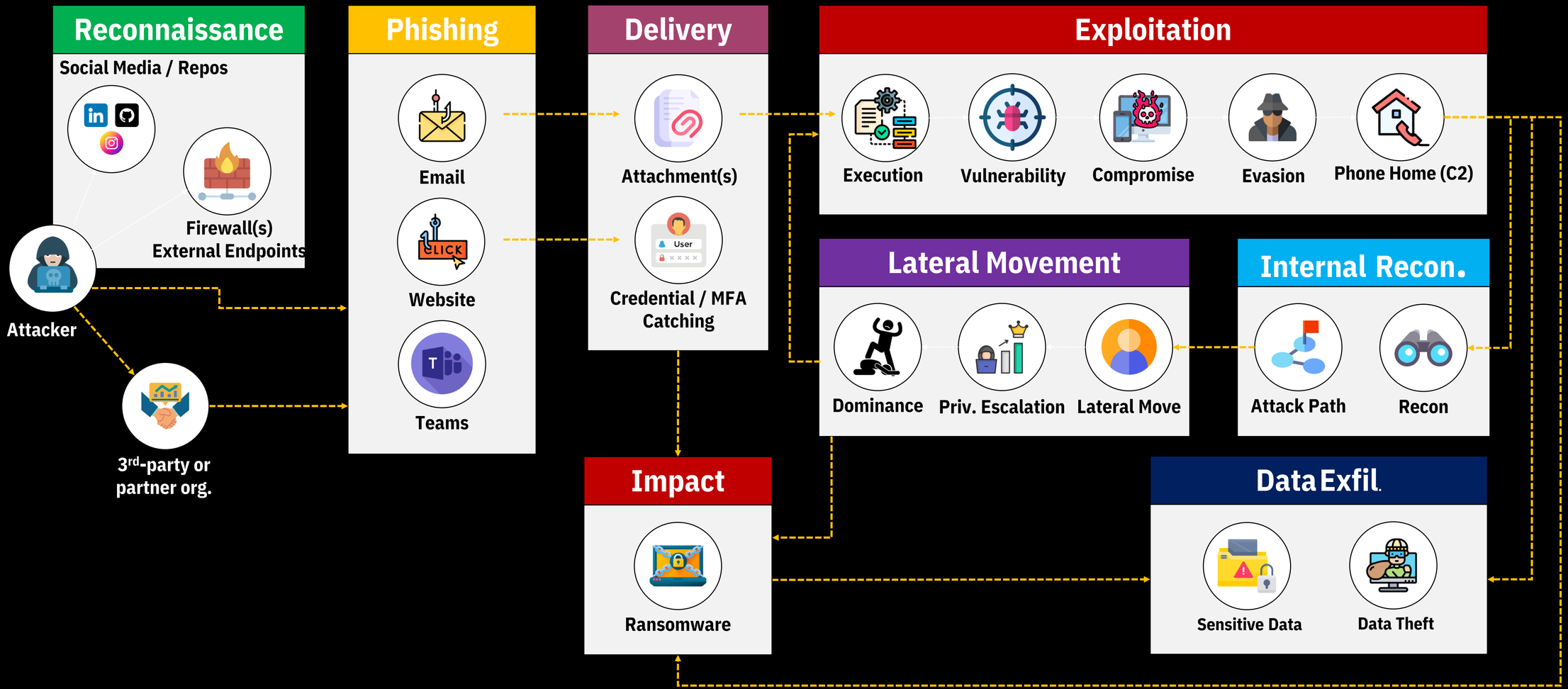
Microsoft Reports (2024 Digital Defense Report)

**11 hours**

Being the median time for attackers to compromise AD from initial access (*though being as low as several minutes*)

# A little history…




Reconnaissance
Social Media / Repos
Firewall(s)
External Endpoints
Attacker
3rd-party or
partner org.
Phishing
Email
Website
Teams
Delivery
Attachment(s)
Credential / MFA
Catching
Exploitation
Execution
Vulnerability
Compromise
Evasion
Phone Home (C2)
Lateral Movement
Dominance
Priv. Escalation
Lateral Move
Internal Recon.
Attack Path
Recon
Impact
Ransomware
Data Exfil.
Sensitive Data
Data Theft

# Shortened Kill Chain

Attacker

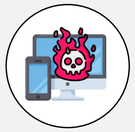
**Target**

Targeted Appliance

**Exploitation**

Vulnerability

**Result**



Compromise

*e.g. Service Account w/ Domain Admin*

**Result**

Dominance

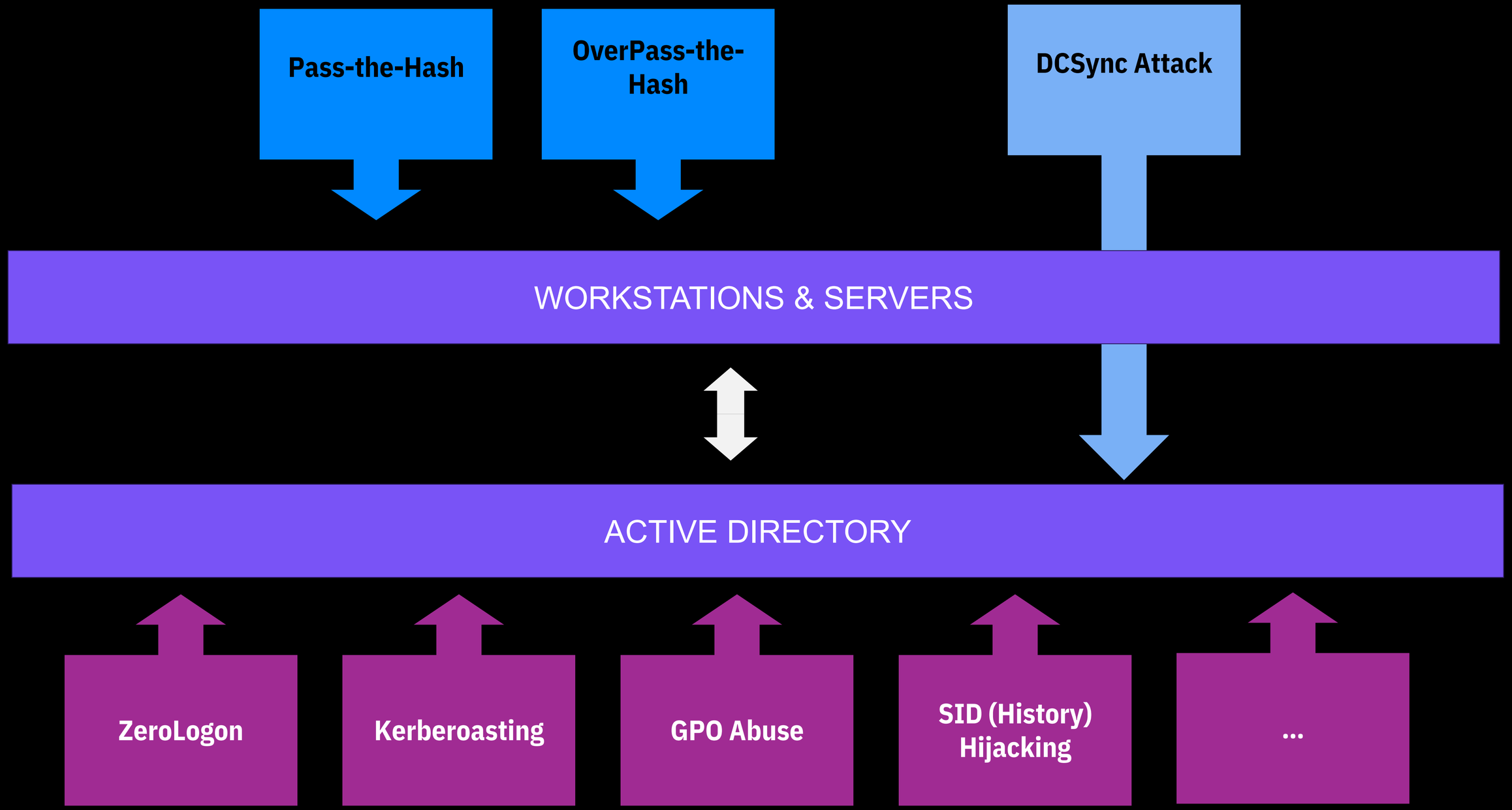
**Impact**

Ransomware

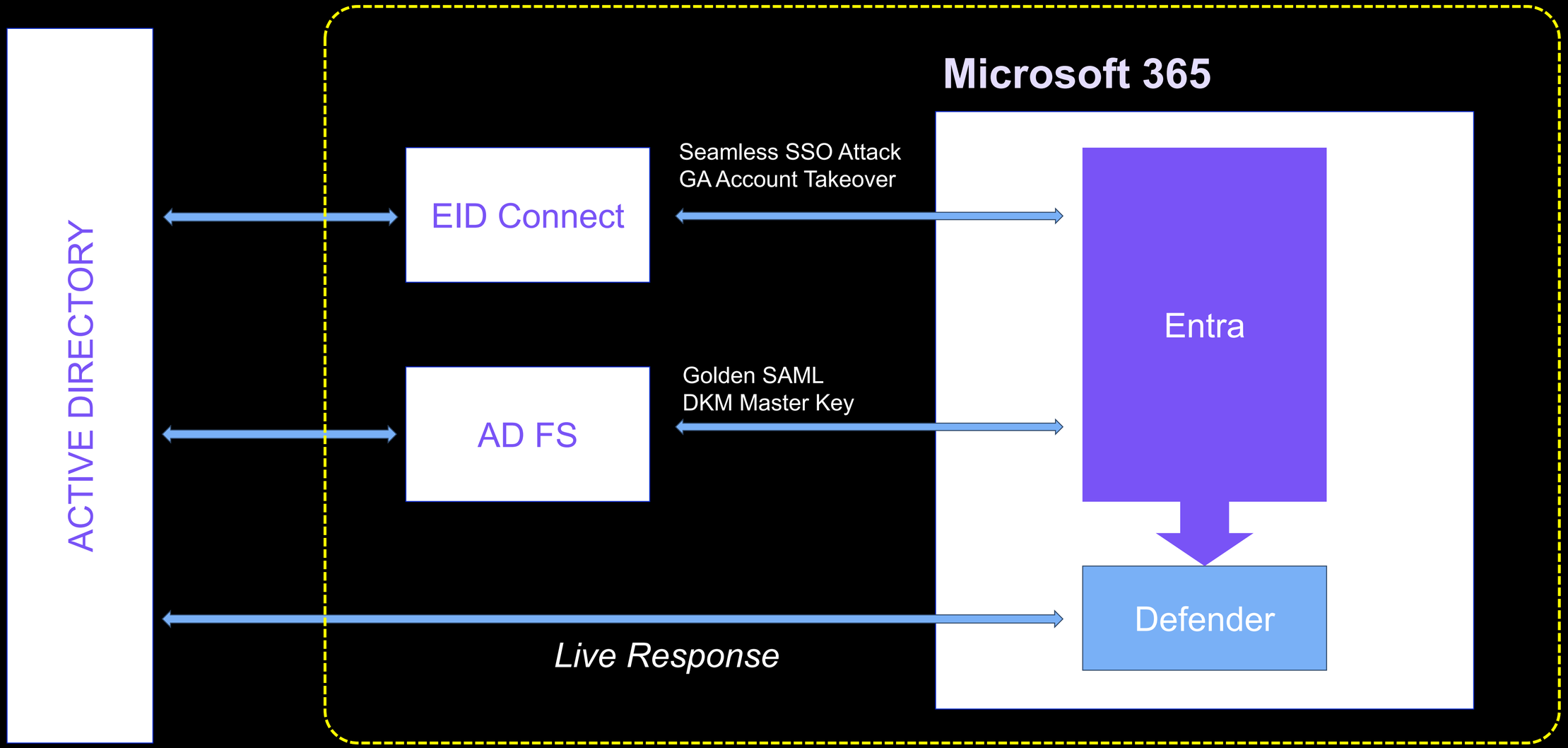
**Data Exfil.**

Sensitive Data

Data Theft


Pass-the-Hash
OverPass-the-Hash
DCSync Attack
WORKSTATIONS & SERVERS
ACTIVE DIRECTORY
ZeroLogon
Kerberoasting
GPO Abuse
SID (History) Hijacking
...

# Extended Attack Surface



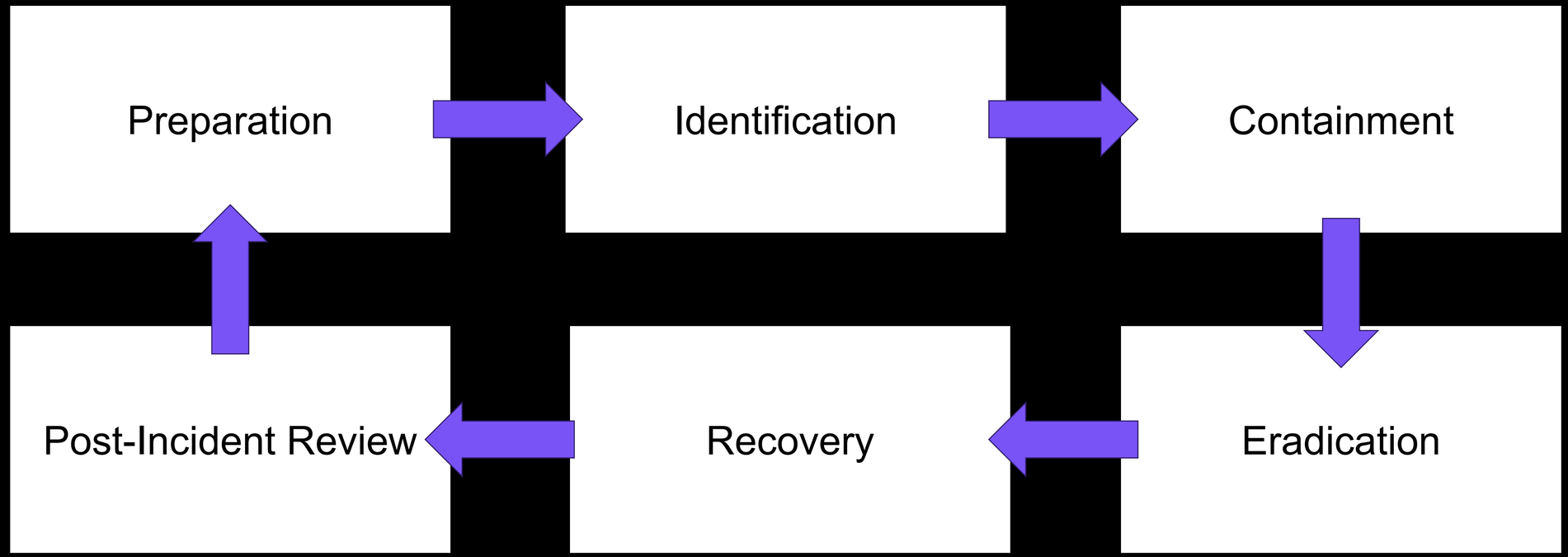
# Active Directory Security – It’s a journey

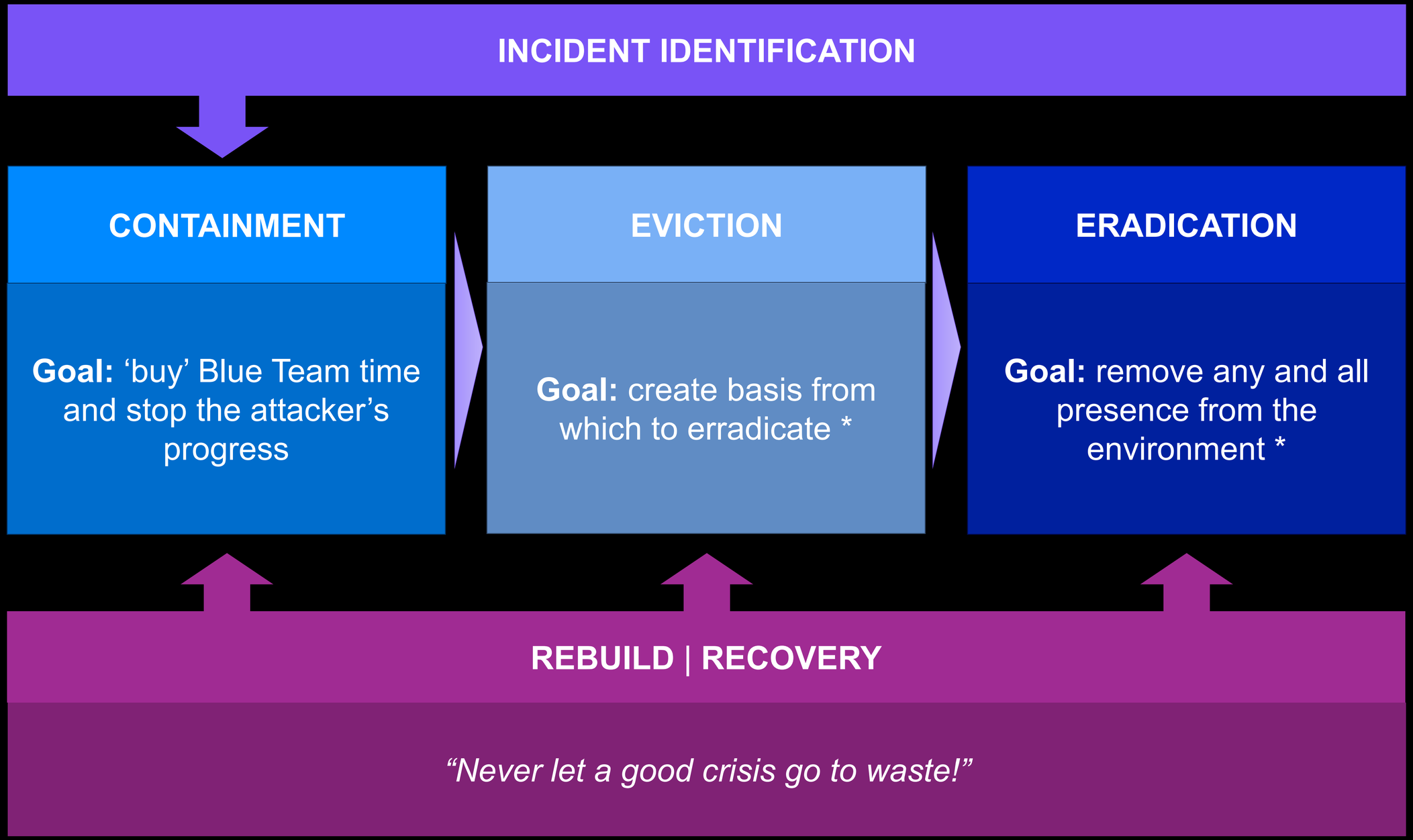
HYBRID IDENTITY PROTECTION conf25

CHARLESTON

# Incident Response

# Incident Response steps




INCIDENT IDENTIFICATION
CONTAINMENT
Goal: ‘buy’ Blue Team time and stop the attacker’s progress
EVICTION
Goal: create basis from which to erradicate *
ERADICATION
Goal: remove any and all presence from the environment *
REBUILD | RECOVERY
“Never let a good crisis go to waste!”

# Identification

## DO NOT

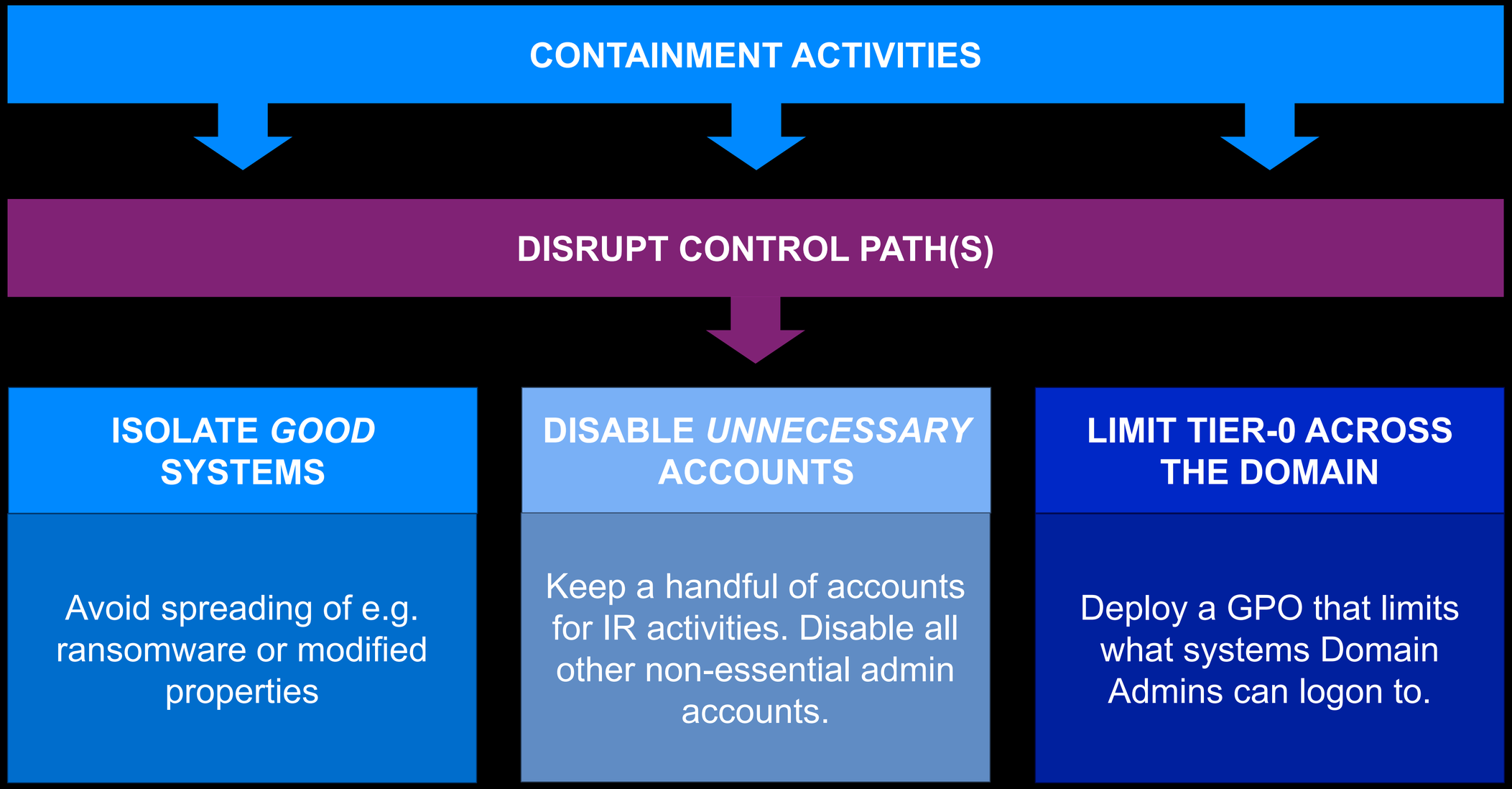
jump to conclusions and start resetting random stuff…

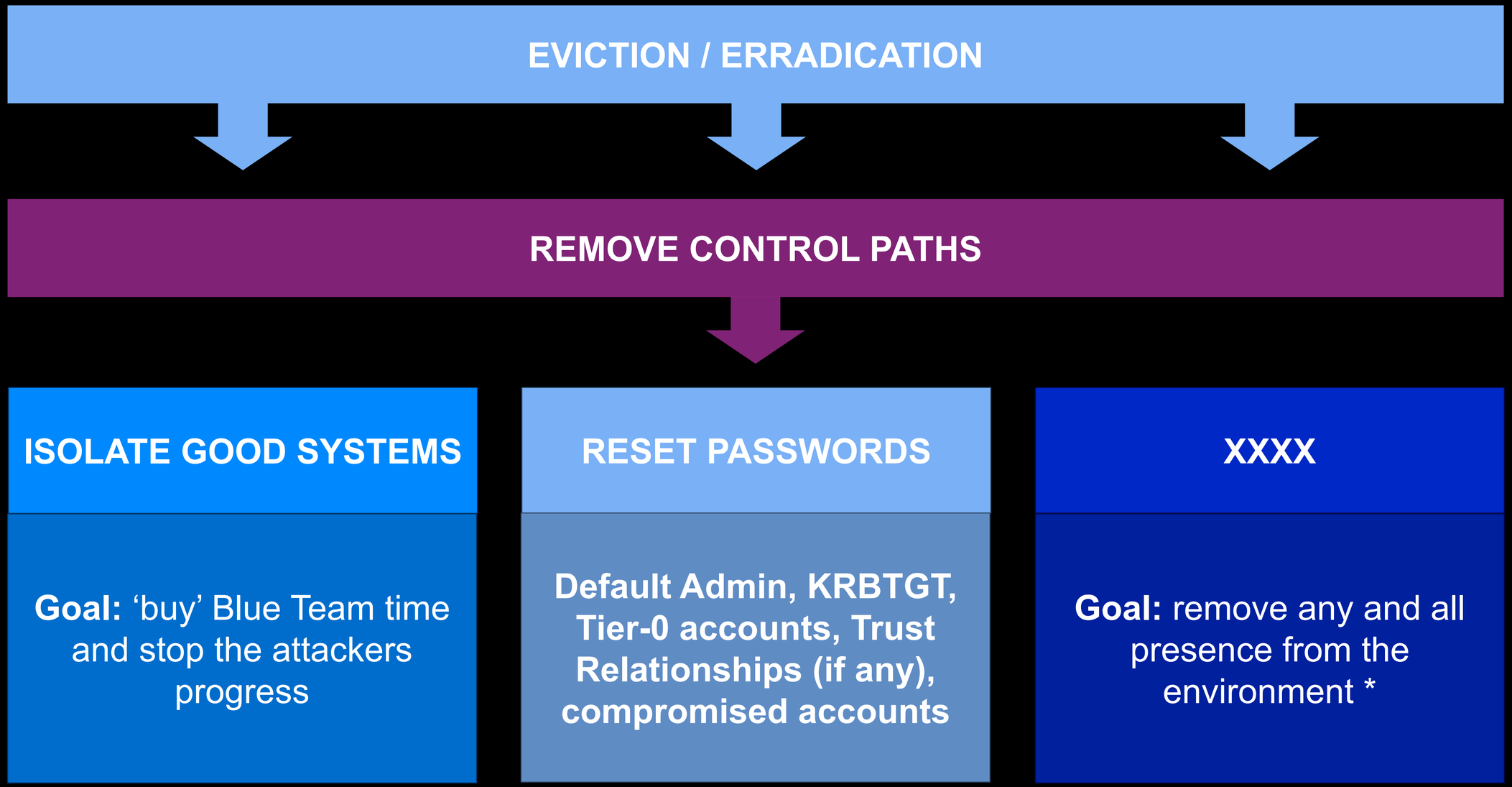
## DO

- Understand the scope of the breach
- Check for (other) unusual activity
- Check what logs you have available
- Collect (and document) evidence

## WHY?

*IDENTIFY CONTROL PATHS*

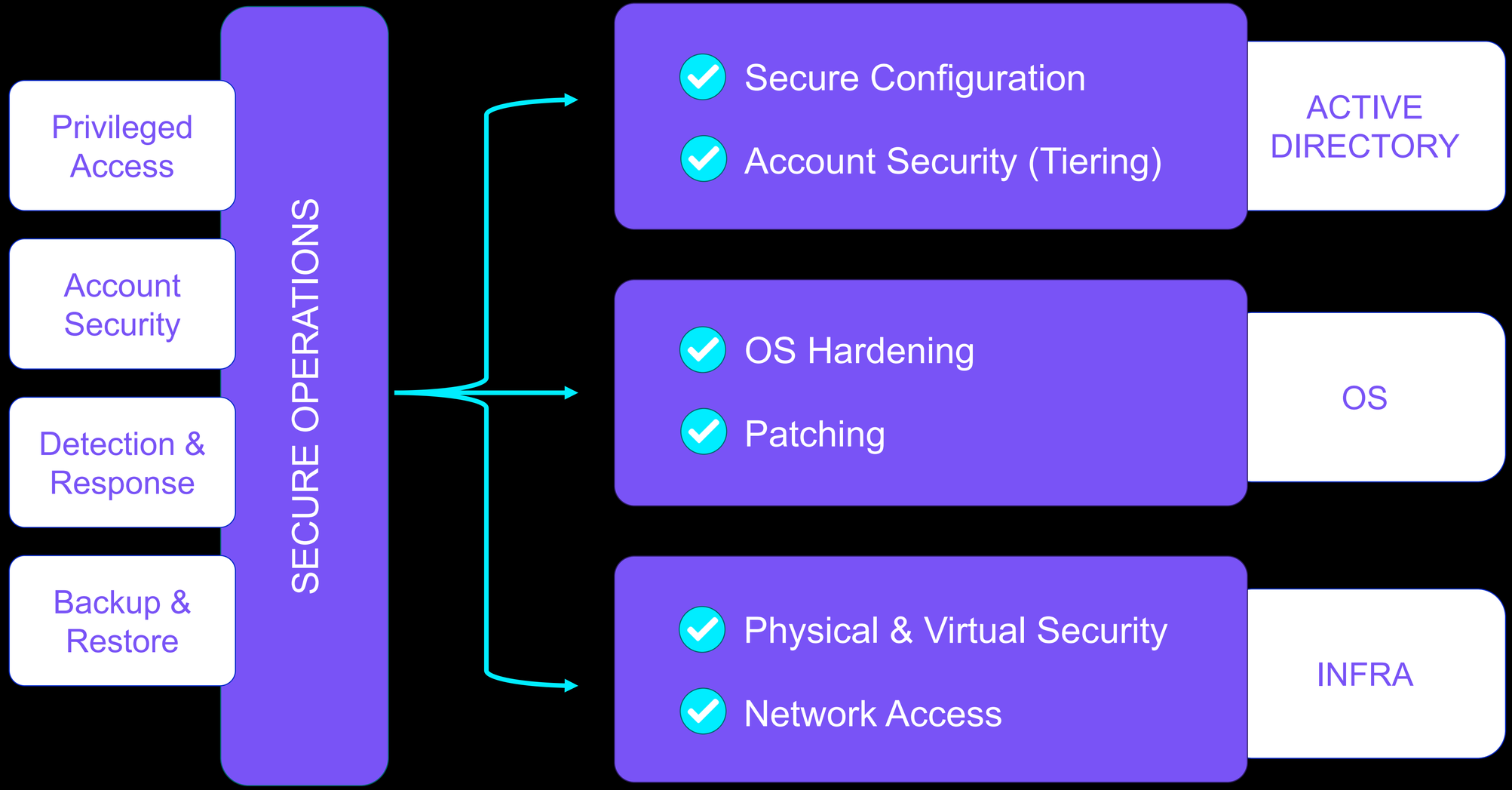

CONTAINMENT ACTIVITIES
DISRUPT CONTROL PATH(S)
ISOLATE *GOOD* SYSTEMS
Avoid spreading of e.g. ransomware or modified properties
DISABLE *UNNECESSARY* ACCOUNTS
Keep a handful of accounts for IR activities. Disable all other non-essential admin accounts.
LIMIT TIER-0 ACROSS THE DOMAIN
Deploy a GPO that limits what systems Domain Admins can logon to.

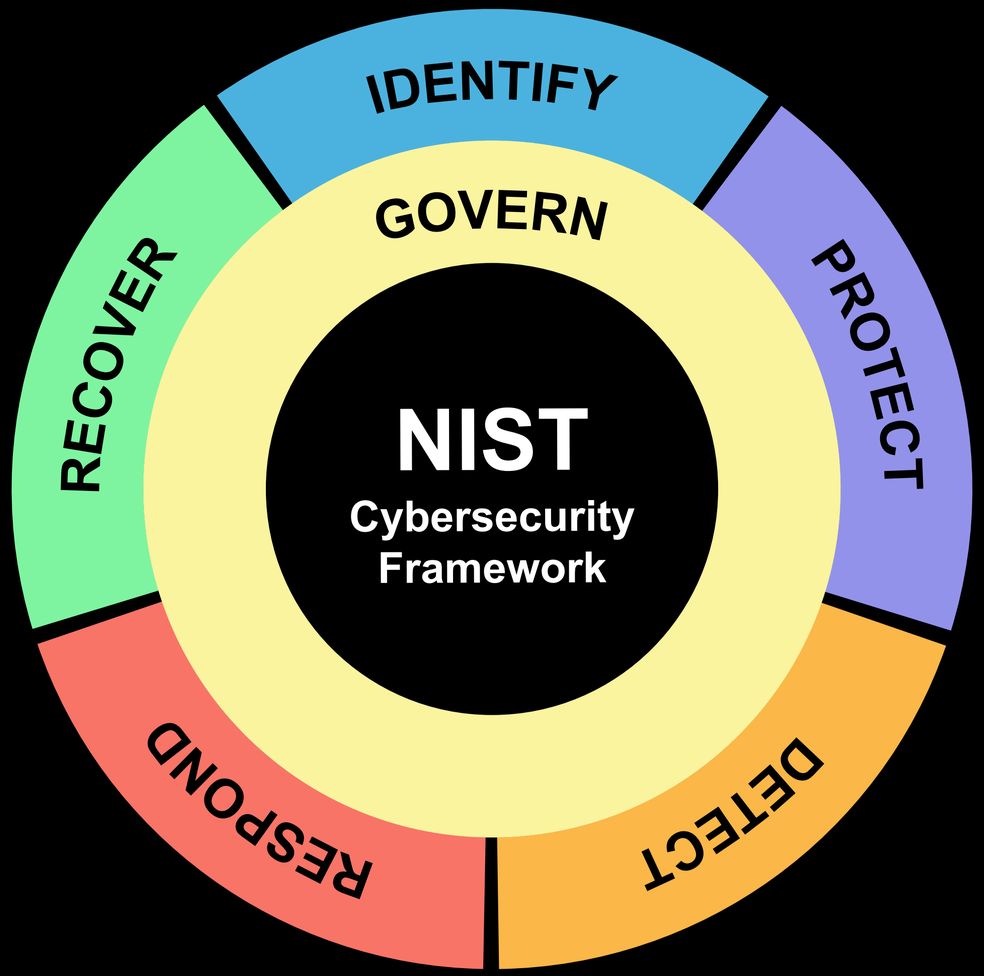

EVICTION / ERRADICATION
REMOVE CONTROL PATHS
ISOLATE GOOD SYSTEMS
Goal: ‘buy’ Blue Team time and stop the attackers progress
RESET PASSWORDS
Default Admin, KRBTGT, Tier-0 accounts, Trust Relationships (if any), compromised accounts
XXXX
Goal: remove any and all presence from the environment *

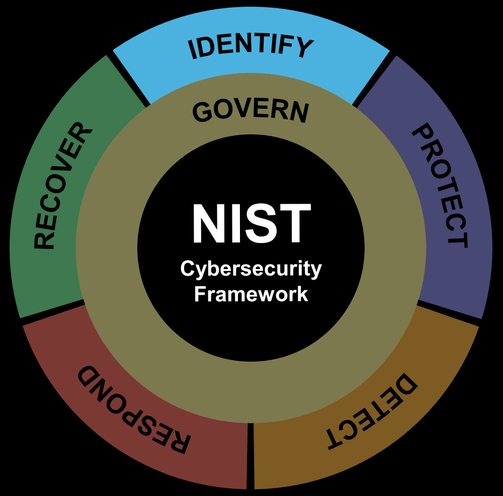
HYBRID IDENTITY PROTECTION conf25 CHARLESTON

# Post-breach activities

# A multi-layered approach



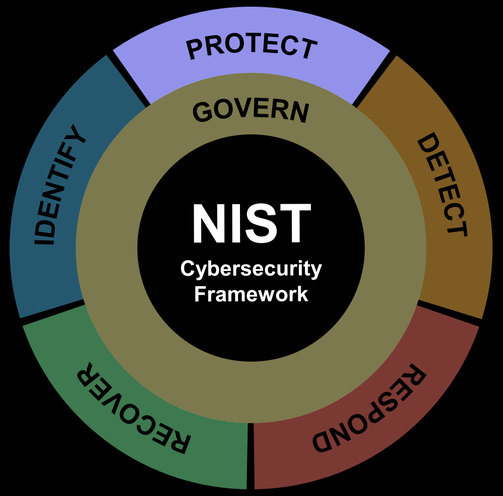

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
GOVERN
NIST
Cybersecurity
Framework




1. Increase Visibility through monitoring (ITDR)

2. Collect logs, establish a baseline of ‘regular’ operations

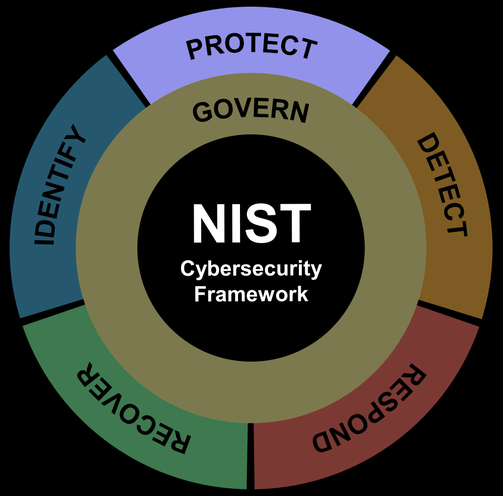
3. Regularly check configuration drift (e.g. Purple Knight)

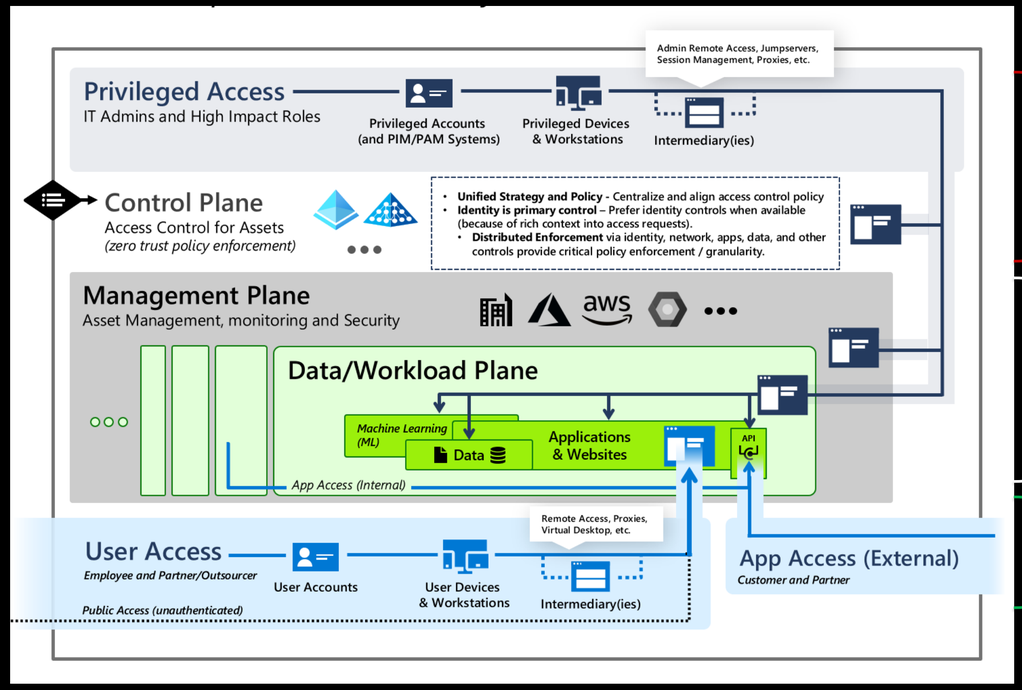



1. Secure Privileged Access

2. Secure Configuration & Best Practices

3. Account Security (e.g. Non-Human Identities (NHI))

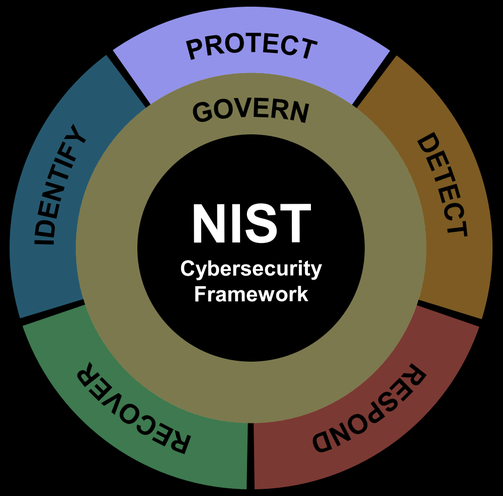


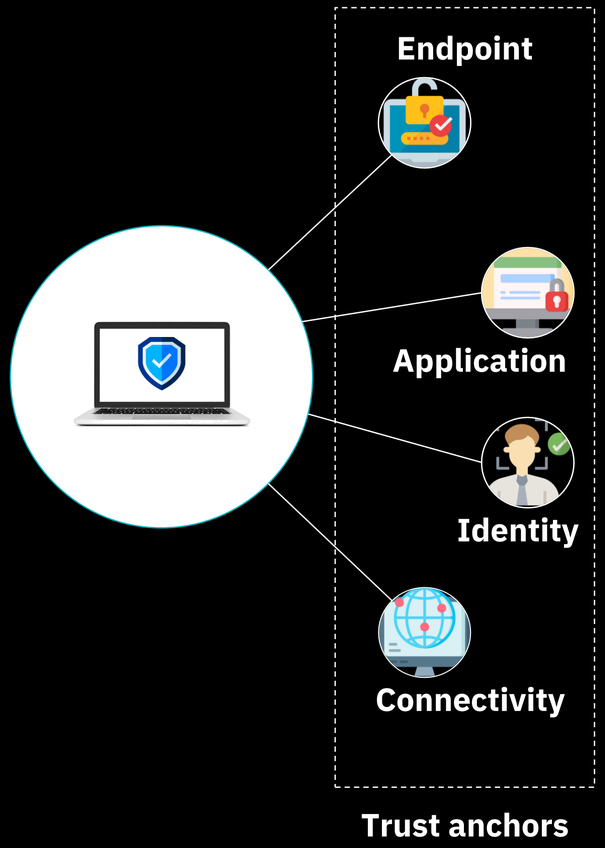




**Tier 0 – Critical Management Activities**

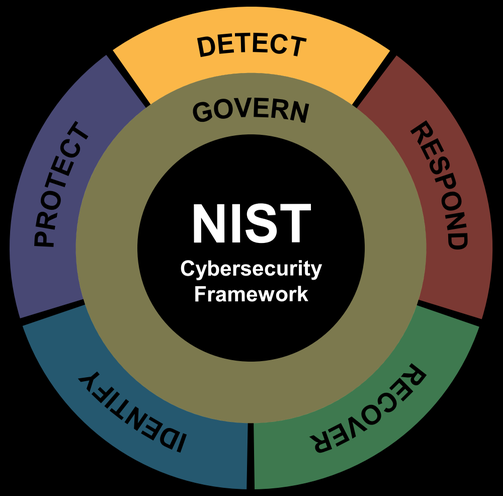
**Tier 1 – General (platform) Administration**

**Tier 2 – User Access**



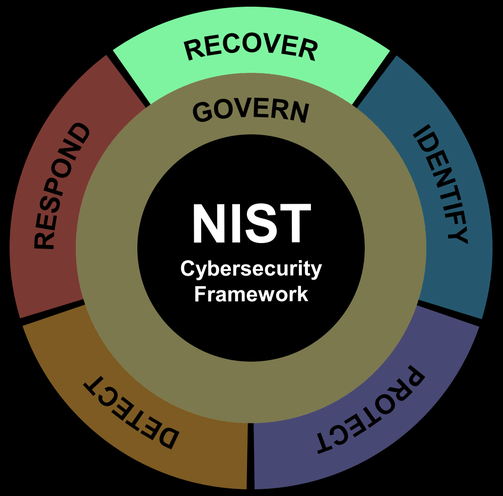

“Trust but verify”.
Explicit verification
of trust anchors.



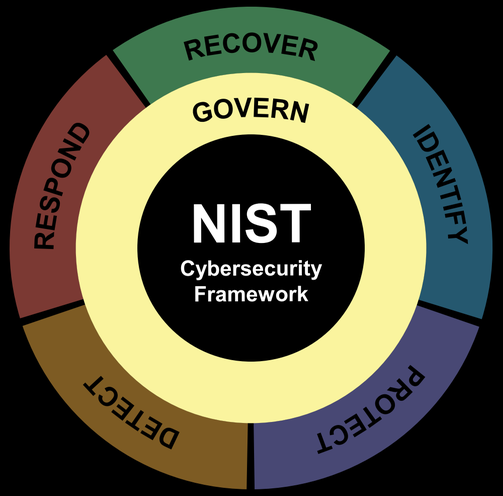

1. ITDR + EDR = Where the magic happens

2. Ensure sufficient logging, auditing (and retention thereof)

3. Get help where needed ☺




1. Establish BCP and resulting DRP
2. Take backups and store securely
3. Regularly test backups and recovery strategy




1. Establish a forward-looking IAM policy (ground rules)

2. Stick to the policy and process!

3. Review innovations, understand their use and implications; implement if useful.

# Key Takeaways

**1**

Preparation is (more than) half of the work. A solid governance process will reduce the risk significantly and drive down the MTTR for an incident.

**2**

Understanding the correct scope of an incident is primordial as it shapes the response strategy and actions.

**3**

Identity Security is a multi-layered approach. Even with a solid configuration, 3rd-party tools and automation(s) are critical elements in your protection strategy.

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

# Questions?