

# **The Whole Nine Yards: Establish a Comprehensive Identity Security Stack for Your Business**



# Derek Melber

VP of Product Engagement and Outreach

QOMPLX

[derek.melber@qomplx.com](mailto:derek.melber@qomplx.com)

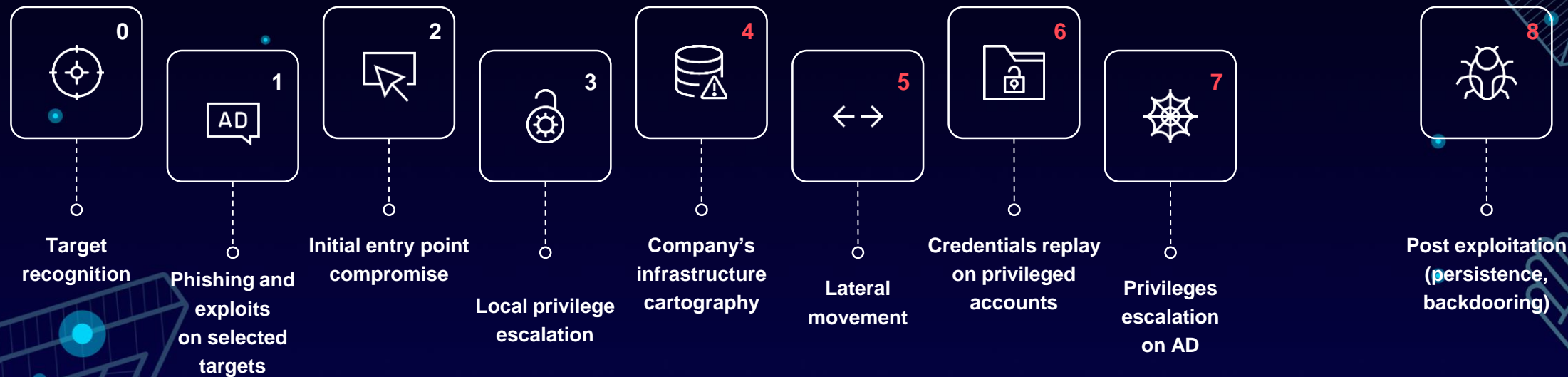
# Identity is the main target for attackers

Verizon DBIR:

Stolen credentials  
led to nearly  
**50%** of attacks



# Typical Attack Tactics



## Attacker Tactics:

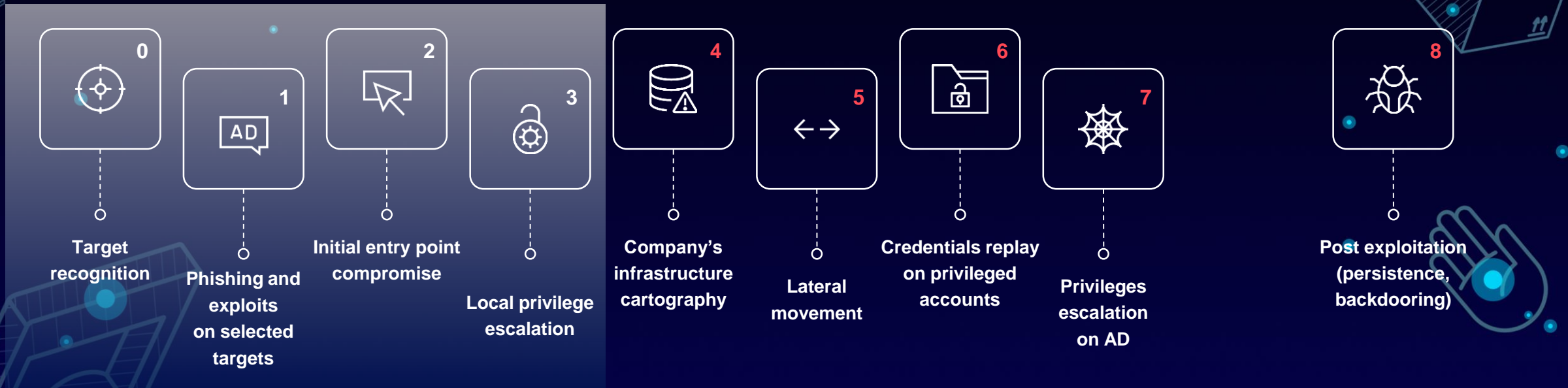
- Exploit vulnerabilities and misconfigurations
- Mine credentials
- Install enumeration tools



# Current identity solutions

SECURITY TECHNOLOGIES:

PAM / MFA / IGA / AM / CIEM



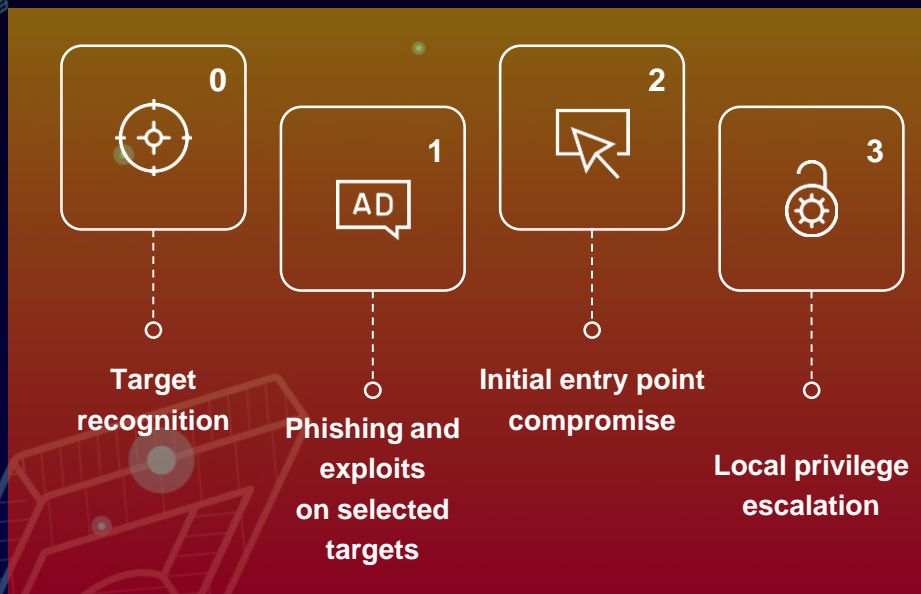
## Attacker Tactics:

- Exploit vulnerabilities and misconfigurations
- Mine credentials
- Install enumeration tools

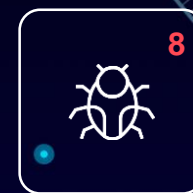
# Current identity solutions

SECURITY TECHNOLOGIES:

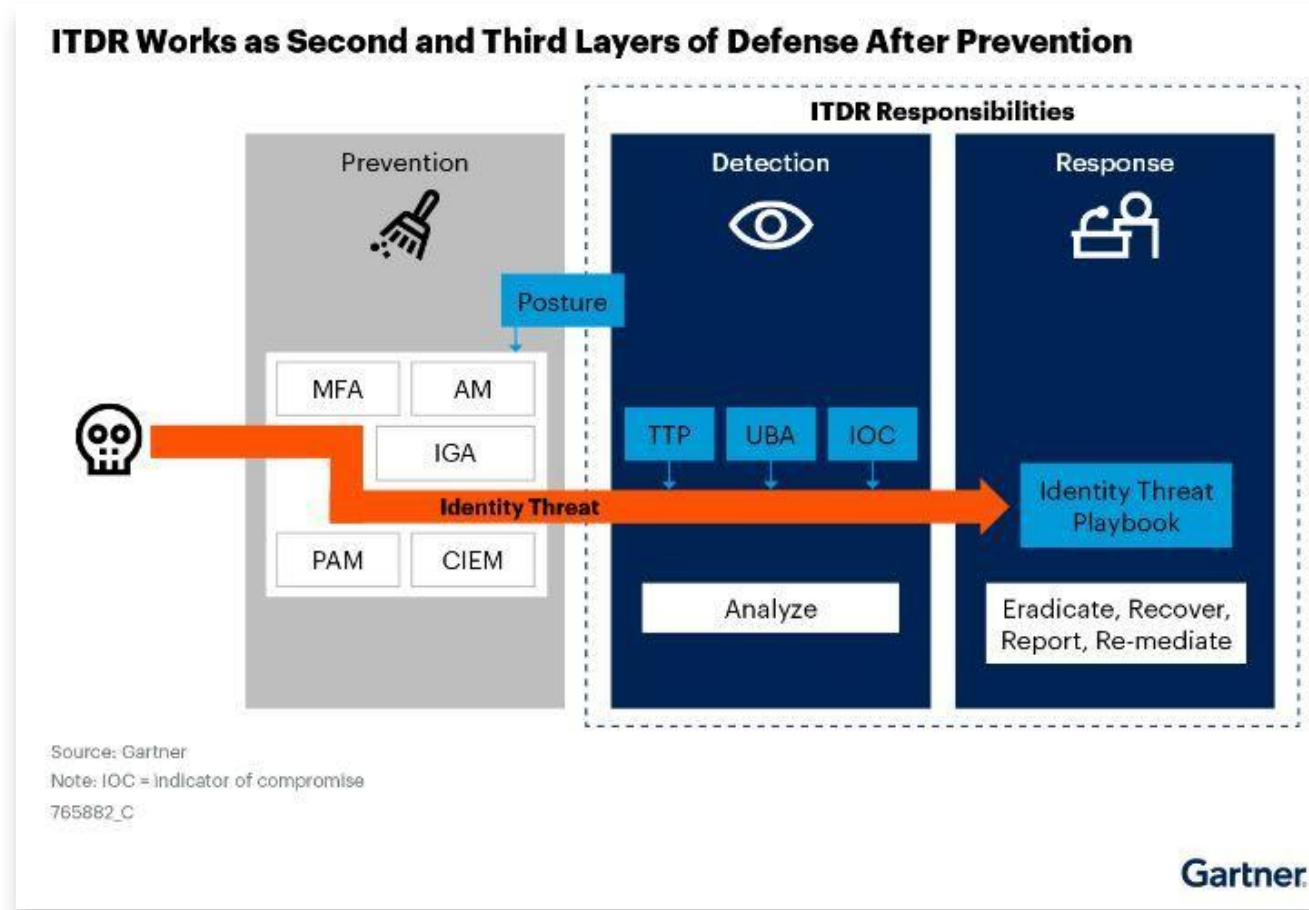
PAM / MFA / IGA / AM / CIEM



Identities not secured



# Gartner – Identity Threat Detection & Response (ITDR)



\*Source: Gartner®, Enhance Your Cyberattack Preparedness With Identity Threat Detection and Response, 20 October 2022  
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

# Comprehensive Identity Security: Prevent, Detect & Respond

QOMPLX

## IDENTITY THREAT DETECTION & RESPONSE



### IDENTITY PREVENT

AUTHENTICATION  
KERBEROS, NTLM, SAML

ON-PREM AD SECURITY AND  
IDENTITY HYGIENE

AZURE AD SECURITY AND  
IDENTITY HYGIENE

AWS, GCP, OKTA, PING,  
SECURITY & IDENTITY HYGIENE



### ATTACK DETECTION

PASSWORDS

ENUMERATION

PRIVILEGED ACCOUNTS

LATERAL MOVEMENT

PRIVILEGE ESCALATION

CREDENTIAL THEFT



### GUIDANCE & RESPONSE

ATTACK INSIGHTS AND DETAILS

ACTION RECOMMENDATIONS

TASKS & COMMANDS

BACKDOOR DETECTIONS

PERSISTENT DETECTIONS



# Identity Security - Prevent

## On-prem identity

- Visibility of existing AD security issues
- 24x7 real-time and automatic analysis of every AD change for new security issues

## Cloud identity

- Visibility of existing cloud identity security issues
- 24x7 real-time and automatic analysis of every change for new security issues

## Guidance and remediation

- Insights and summaries of issues
- Contextual guidance for remediation



### IDENTITY PREVENT

AUTHENTICATION  
KERBEROS, NTLM, SAML

ON-PREM AD SECURITY AND  
IDENTITY HYGIENE

AZURE AD SECURITY AND  
IDENTITY HYGIENE

AWS, GCP, OKTA, PING,  
SECURITY & IDENTITY HYGIENE

# Identity Security - Detect

## Assume breach

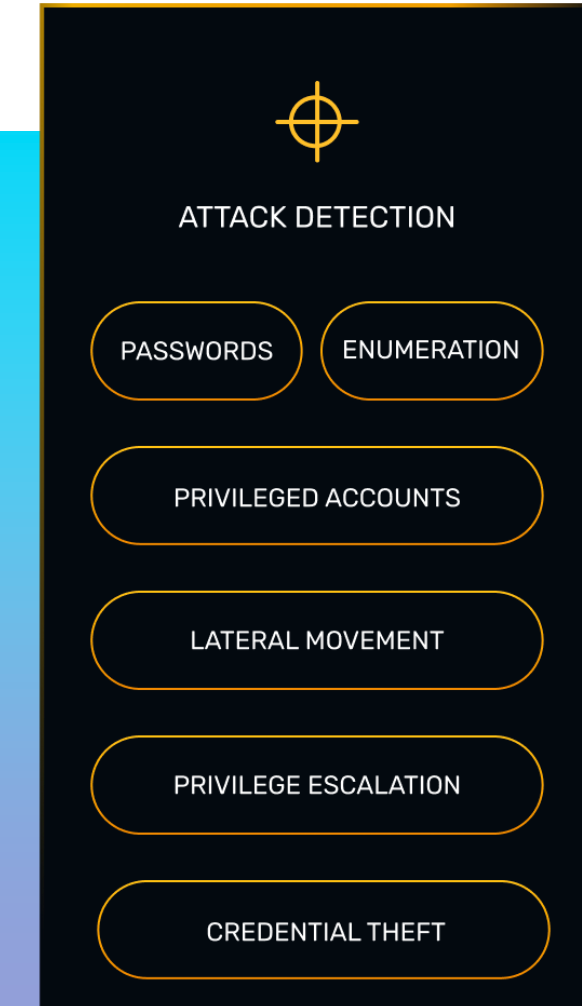
- Must take the approach that the network is already breached
- Basic and complex attacks must be detected where identities reside (on-prem and cloud)

## Deep and wide attack detections

- Password attacks, lateral movement, privilege escalation, etc.
- Object, attribute, kerberoasting, impersonation, etc

## Zero Trust related attack detections

- On-prem credential abuse and forgeries (Golden Ticket, Silver ticket, Diamond ticket, Sapphire ticket, etc.)
- Cloud credential abuse and forgeries (SAML and AAD Kerberos)



# Identity Security - Response

## Guidance and insights

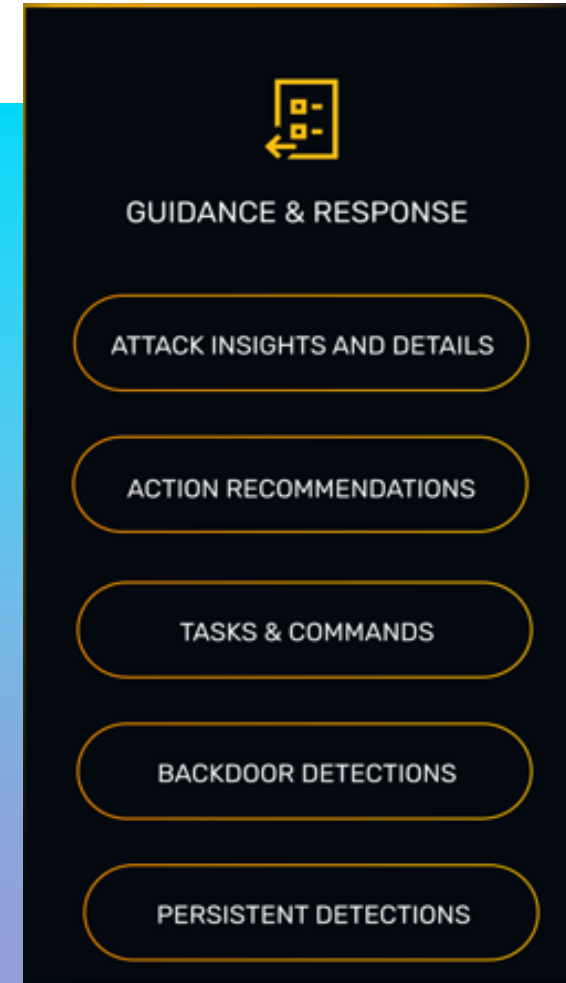
- Not everyone understands the technical aspects of an attack
- Time is of the essence... no time to research

## Direction and examples

- Attacks can be complicated - knowing where to go in GUI is key
- PowerShell is powerful, but also complicated – examples make a difference

## Playbooks for attack response

- Overview of the attack and consequences
- Step-by-step incident response tasks





# THANK YOU!

Derek Melber

[derek.melber@qomplx.com](mailto:derek.melber@qomplx.com)