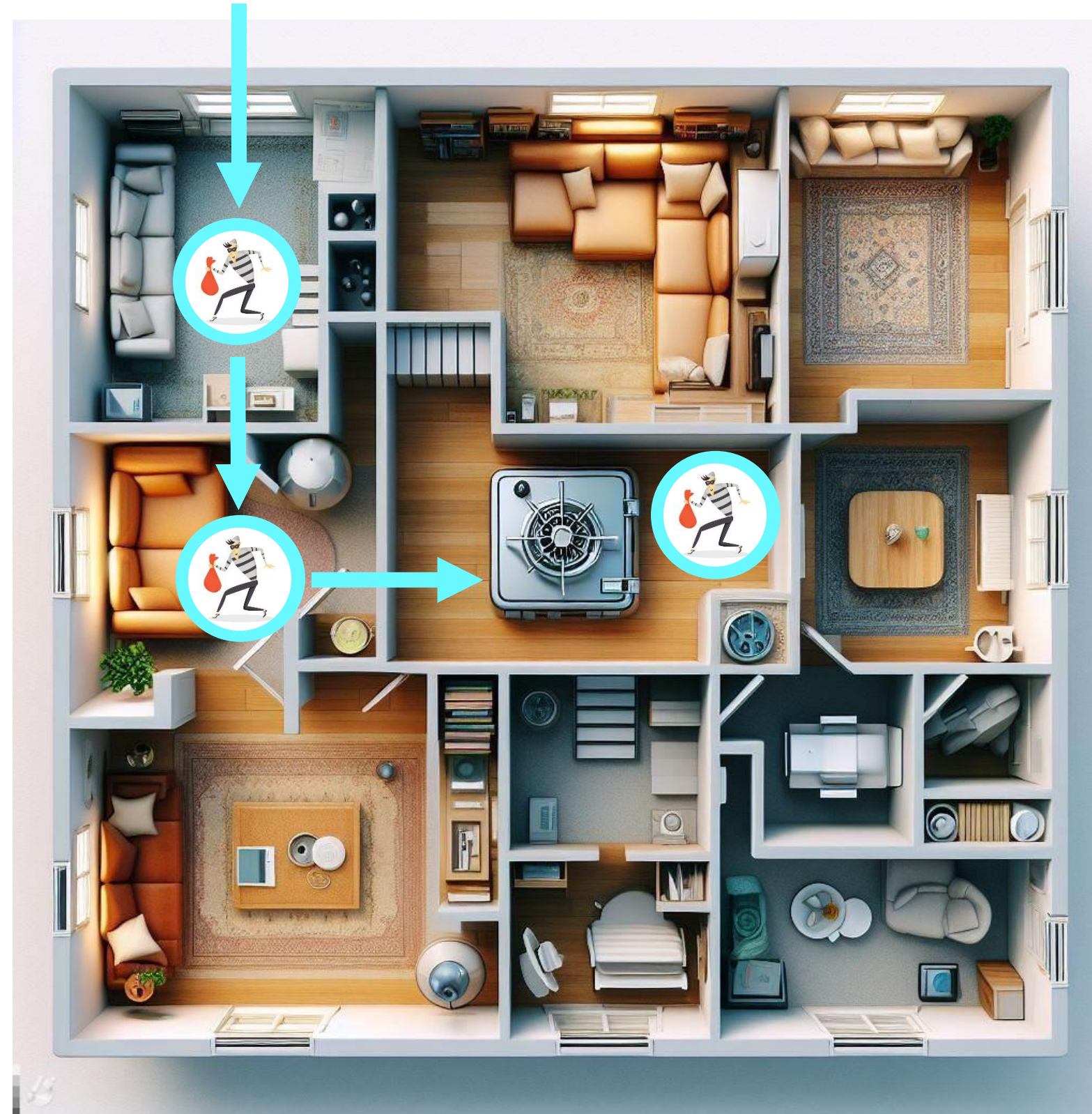# Lateral Movement

— There is no attack without lateral movement

— In most cases the crown jewels are not exposed directly

— Crown jewels are not put on a table in a room with an open window to the street

— They are kept at a safe place

— That's why a burglar must move laterally through the rooms of a building

glueck kanja

glueckkanja.com

MITRE ATTACK

glueck·kanja

glueckkanja.com

Initial Access

External Remote Services

Phishing

Drive-by Compromise

Remote Code Execution

glueckkanja.com

Privilege Escalation

Remote Code Execution

Admin Credentials

User Credentials

User

Lateral Movement through Privilege Escalation

"
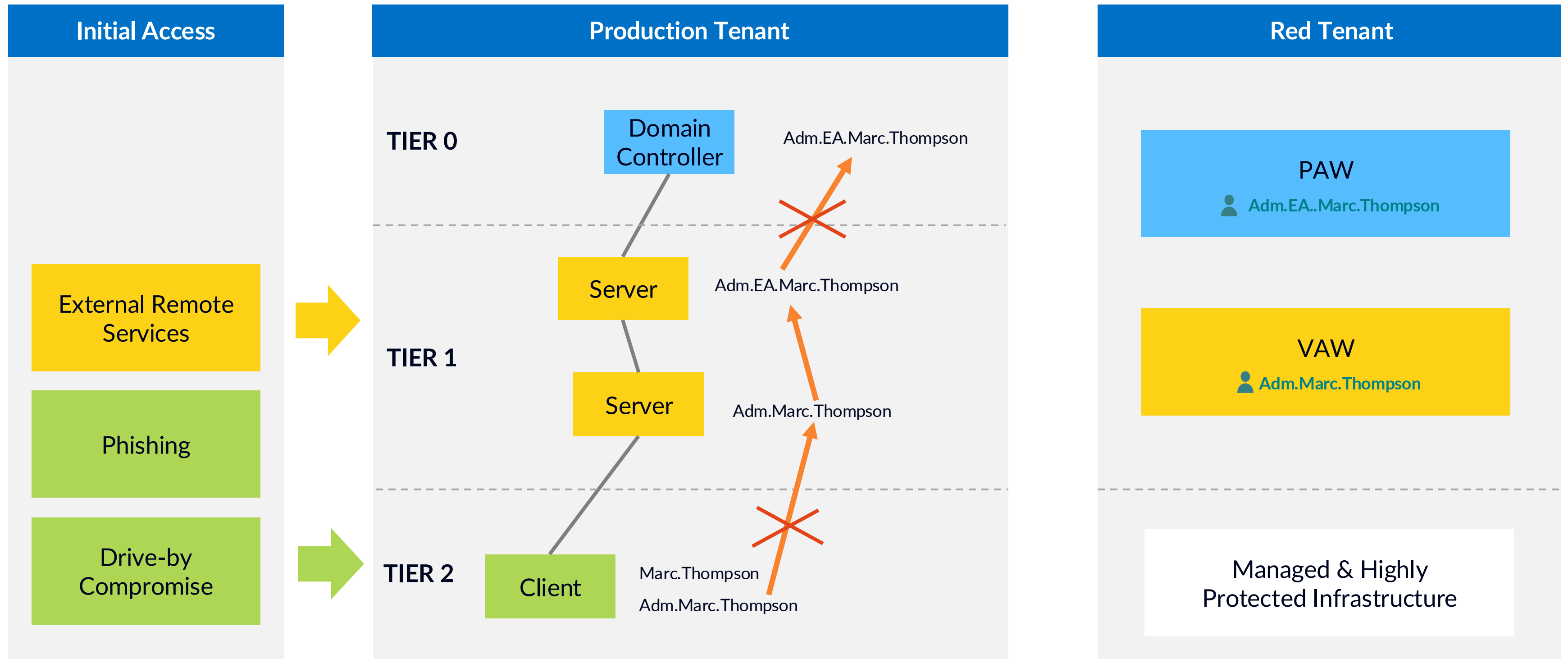
93% of our ransomware incident response engagements revealed insufficient controls on privilege access and lateral movement.

Source: 2022 Microsoft Digital Defence Report

PAW & VAW

PAW Scenario

Resource Tenant

Azure Management   Entra Portal   Security Portal

Conditional Access: PAW Access Only

Red Tenant

PAW   FIDO 2

Office PC

✓ Physical isolation (clean keyboard)   ✗ Second Device to carry

✓ 1:1 User to Device Binding   ✗ Hardware procurement process

VAW Scenario

Resource Tenant

Azure Management   Entra Portal   Security Portal

Conditional Access: Compliant Devices Only

Conditional Access: VAW Access Only

Red Tenant

Office PC   VAW (based on AVD)   FIDO 2

✓ No additional Hardware needed   ✗ Virtual separation (remaining risk)

✗ No 100% isolation between Tiers   ✓ 100% scalable through cloud technology

glueck kanja

glueckkanja.com

Highly Secure Working Environment PAW

Resource Tenant

Resource Tenant

Resource Tenant

B2B Access

B2B Access

B2B Access

Managed Red Tenant

PAW

– Restricted Web Access
– Application Control (App-Locker)
– No Local Admin Access
– TPM, VBS, Code Integrity, Secure Boot
– XDR & SIEM Monitoring
– Strict Separation of Duties
– Dedicated PW Management

Admins login via FIDO2 only

glueck▪kanja

Thanks!

glueckkanja.com