

FROM ENDPOINT ACCESS TO IDENTITY

Understanding Today's Attack Paths

CYBEROPS 2026



MEET YOUR PRESENTER

JIMMY COLVIN

Technical Account Manager II | Huntress

- 27+ years of experience across technology and security
- Previously built the Technical Implementation Manager function at Red Canary
- U.S. Army veteran



THE TERMS, IN PLAIN LANGUAGE

Endpoint

A computer or server someone uses or manages.

MFA multi-factor authentication

Sign-in that requires more than one kind of proof.

Session token

Digital proof that keeps you signed in.

AiTM adversary-in-the-middle

An attacker relays a sign-in and can capture its session.

RMM remote monitoring and management

Software IT uses to manage devices remotely.

EDR endpoint detection and response

Tools that watch device activity and help investigate and respond.

SIEM security information and event management

A system that brings security logs together for investigation.

SOC security operations center

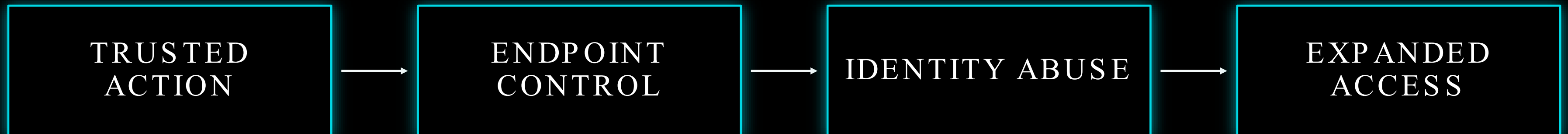
The team that investigates security alerts and coordinates response.

THE FILE IS NOT THE WHOLE STORY

OLD VIEW



BROADER VIEW



The links between events reveal the attack.

CLICKFIX MAKES THE USER RUN THE COMMAND

SAFE TRAINING SIMULATION

Representative example // not case evidence

FRAME 1 / 3

STATIC TRAINING MOCKUP // OFFLINE // NON-FUNCTIONAL

Verify You Are Human

Please verify that you are a human to continue.

 I'm not a robot

01 THE LURE

A webpage asks you to verify

A familiar CAPTCHA style check appears on an ordinary site.

DEFENDER TAKEAWAY

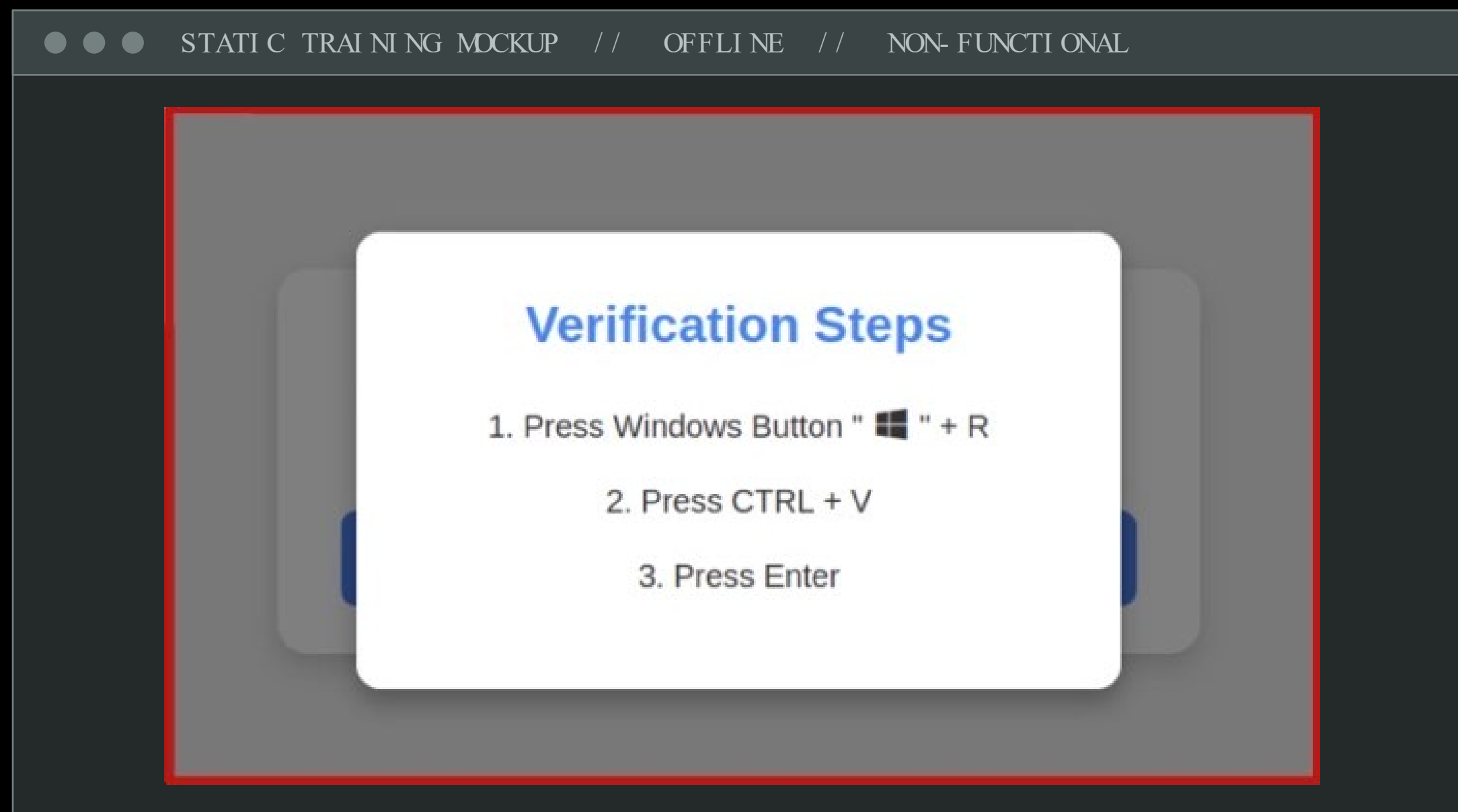
Real CAPTCHAs never ask you to run anything.

CLICKFIX MAKES THE USER RUN THE COMMAND

SAFE TRAINING SIMULATION

Representative example // not case evidence

FRAME 2 / 3



02 THE INSTRUCTIONS

Verification asks for keystrokes

Open Run, paste, press Enter. The page already filled the clipboard.

DEFENDER TAKEAWAY

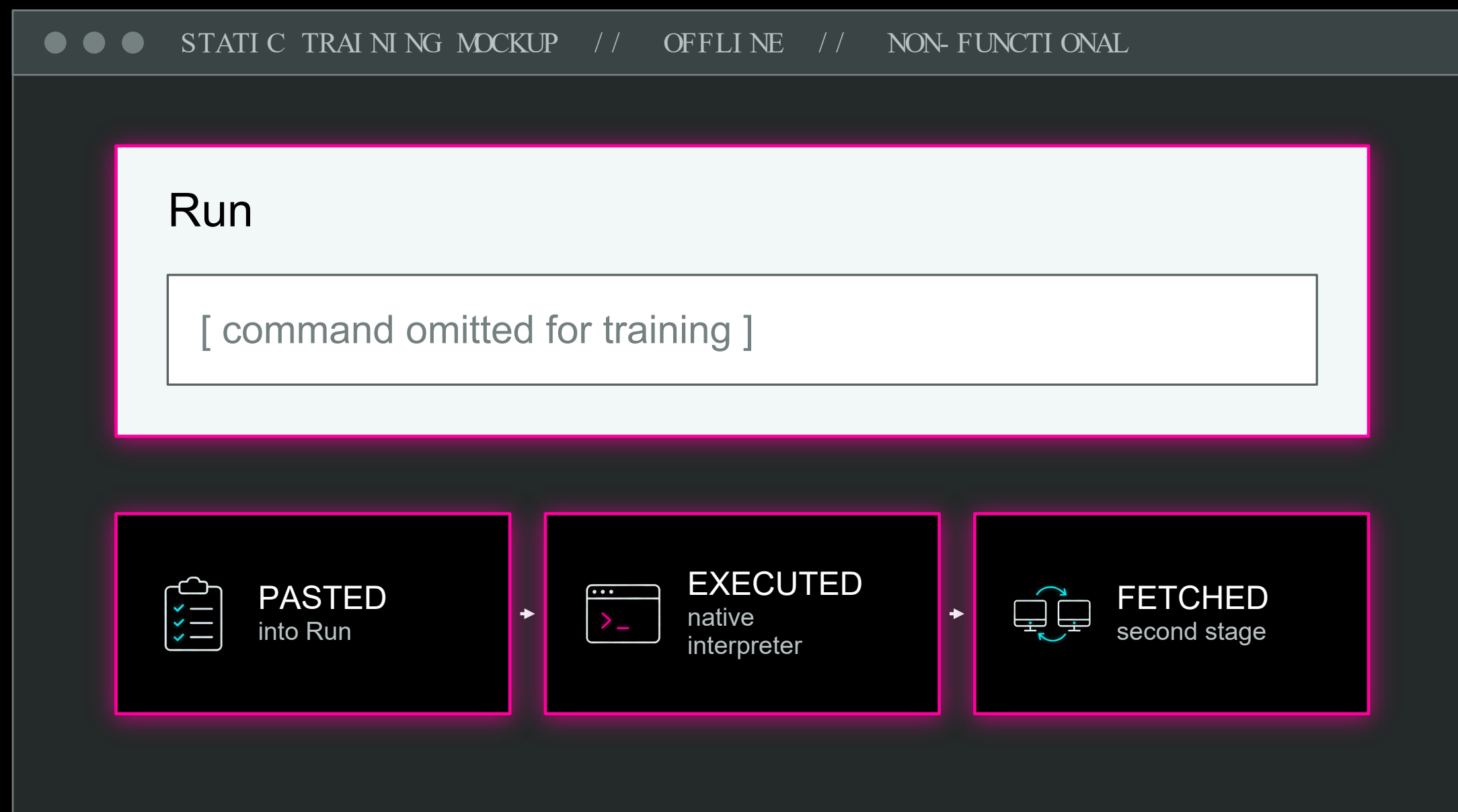
Any prompt to open Run or a terminal is a stop sign. Report it.

CLICKFIX MAKES THE USER RUN THE COMMAND

SAFE TRAINING SIMULATION

Representative example // not case evidence

FRAME 3 / 3



03 THE OUTCOME

One paste becomes code execution

The user runs the attacker's command.
No exploit required.

DEFENDER TAKEAWAY

Hunt the behavior: Run history, interpreter launch, outbound retrieval.

HUNT THE BEHAVIOR, NOT THE LURE

Lures vary: ClickFix, FileFix, TerminalFix

01

USER-DRIVEN
EXECUTION

02

INTERPRETER
ACTIVITY

03

OUTBOUND
PAYLOAD
RETRIEVAL

Useful investigation chokepoints across the variants studied.

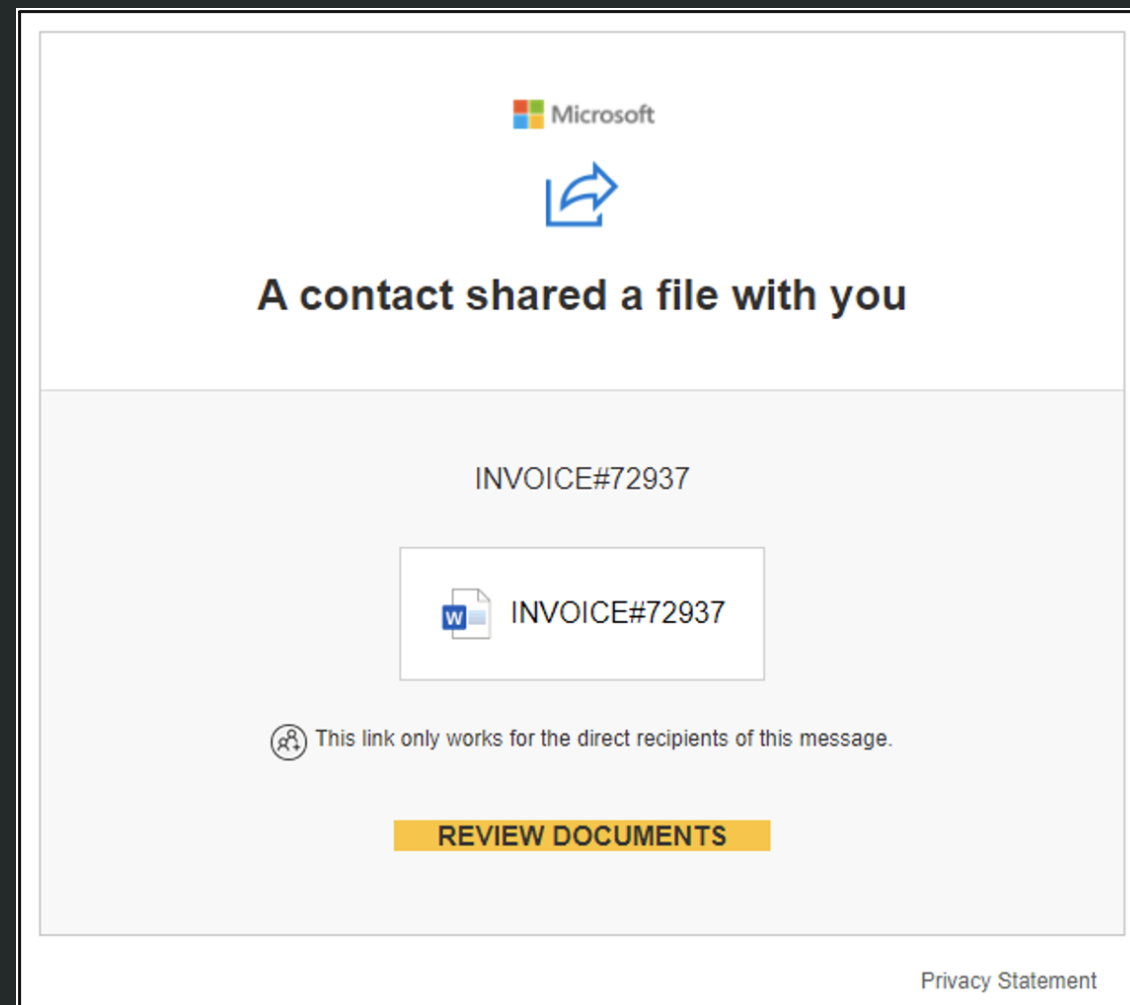
MFA SUCCESS DOES NOT PROVE A SAFE SESSION

SAFE TRAINING SIMULATION

Representative example // not case evidence

FRAME 1 / 3

STATIC TRAINING MOCKUP // OFFLINE // NON-FUNCTIONAL



01 THE LURE

A contact shared a file with you

A familiar file-share notice urges: review documents.

DEFENDER TAKEAWAY

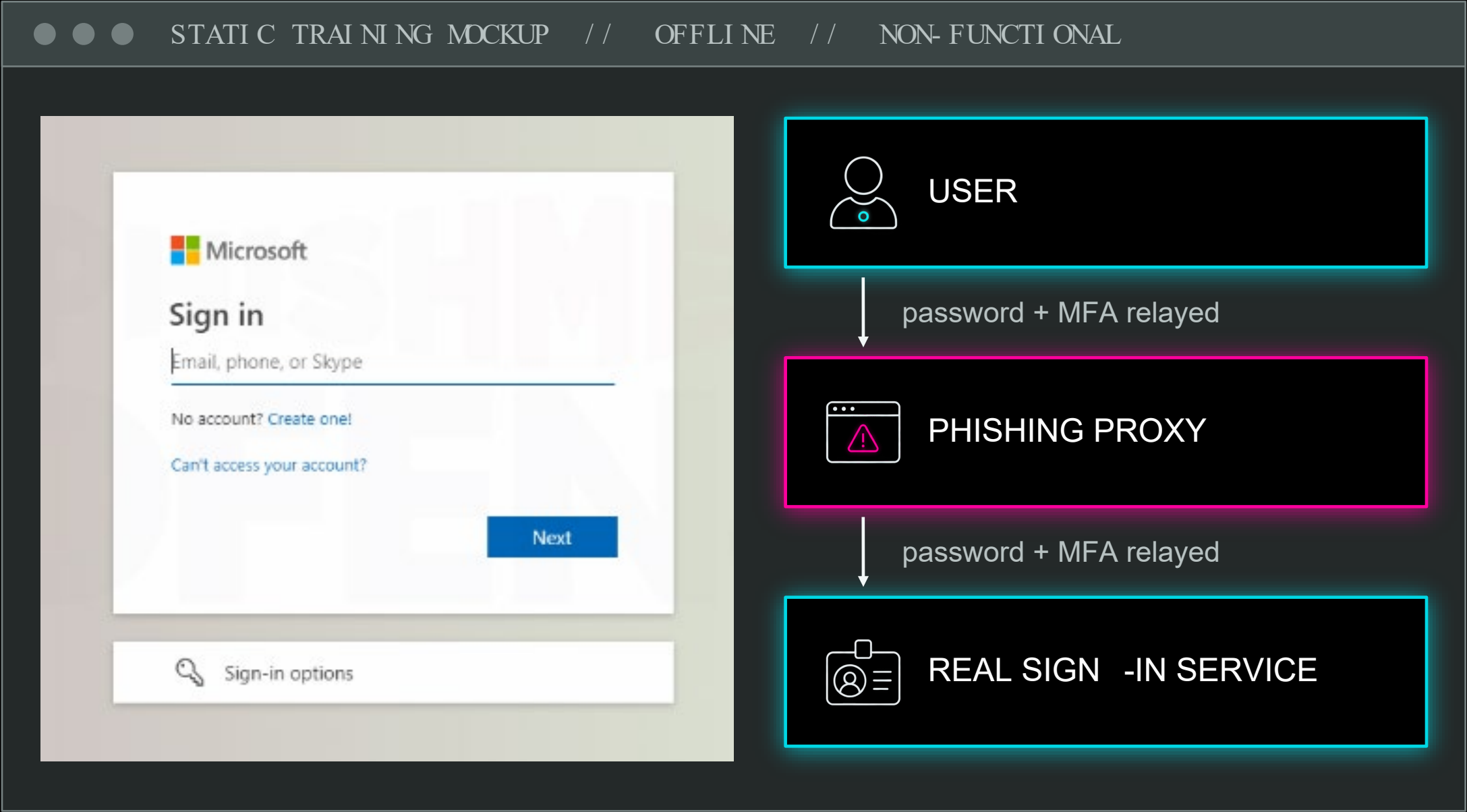
Verify unexpected shares through a separate channel.

MFA SUCCESS DOES NOT PROVE A SAFE SESSION

SAFE TRAINING SIMULATION

Representative example // not case evidence

FRAME 2 / 3



02 THE SIGN-IN

The sign-in page looks real

A proxy relays the real page. Password and MFA pass through live.

DEFENDER TAKEAWAY

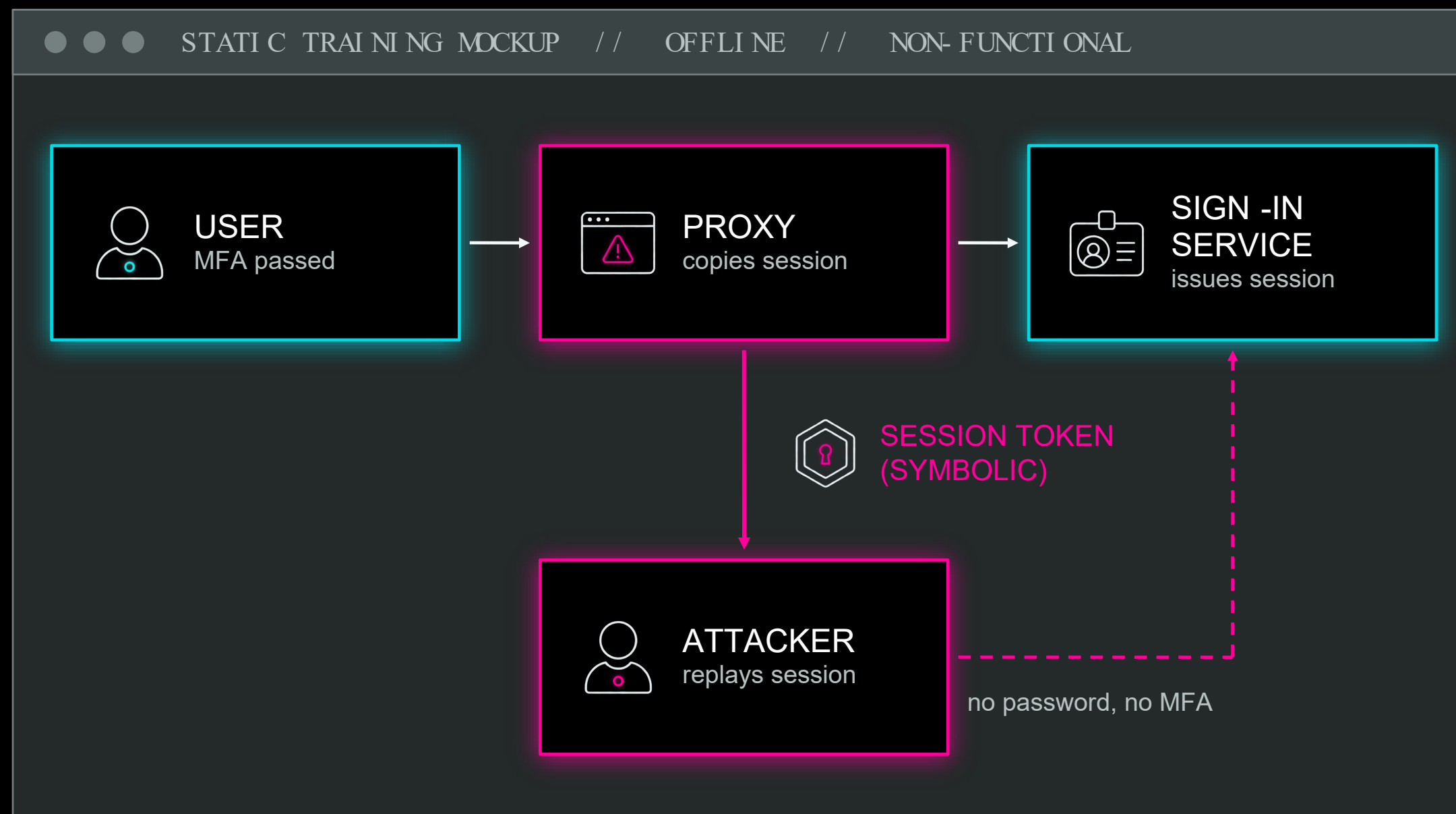
Prefer phishing-resistant MFA. A passed prompt is not proof of safety.

MFA SUCCESS DOES NOT PROVE A SAFE SESSION

SAFE TRAINING SIMULATION

Representative example // not case evidence

FRAME 3 / 3



03 THE THEFT

The attacker leaves with the session

The proxy keeps the signed-in session and replays it elsewhere.

DEFENDER TAKEAWAY

Hunt after login: token replay, new device, inbox rules. Revoke sessions.

THE LOGIN IS ONLY THE START

CASE EVIDENCE // REDACTED REPORT SCREENSHOTS

TOKEN THEFT DETECTION



Rule Name: Token Theft

Country: <REDACTED>

VPN: <REDACTED>

Activity Occurred At: <REDACTED>

OAuth2 ACTIVITY FROM ONE IP

OAuth2:Authorize	139.28.218.17
------------------	---------------

OAuth2:Token	139.28.218.17
--------------	---------------

OAuth2:Token	139.28.218.17
--------------	---------------

OAuth2:Authorize	139.28.218.17
------------------	---------------

Connect the session to what changed afterward.

Also in this case: device fingerprint mismatch; messages moved to Conversation History.

SHOULD THIS REMOTE TOOL BE HERE?

RMM = remote monitoring and management

- 01 Who owns this installation?
- 02 Is this endpoint approved to run it?
- 03 Does the activity fit the support workflow?

SAFE MODE CAN REDUCE SECURITY VISIBILITY

NORMAL WINDOWS

- Security services running

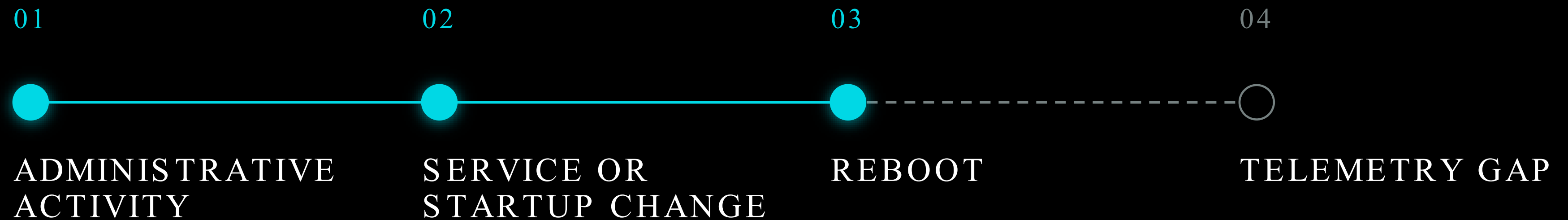
REBOOT
→

SAFE MODE

- Reduced service set; protection may not run

In the observed Akira incident, encryption failed, but data had already been stolen.

INVESTIGATE WHAT CHANGED BEFORE THE SILENCE



Unexpected silence deserves context, not an assumption.

A VALID LOGIN CAN STILL BE ATTACKER ACCESS

SIEM = security information and event management

CASE EVIDENCE // REDACTED SIEM DETECTION REPORT

2026-01-09 08:30:29 UTC

Expedited

Critical

Rule Name: [SIEM Detection 1](#)

Event Category: authentication

Event Provider: Microsoft-Windows-Security-Auditing

Event Code: 4778

Remote IP Lookup:

Remote IP Logs:

SIEM Logs: [SIEM Dashboard](#)

Source Host Name: WIN-<REDACTED>

Source IP: IP

User Name: User

Investigate source context

Connect the session to endpoint activity.

SOURCE HOST NAME

Redacted; context comes from the case

EVENT CODE 4778

Session reconnect, commonly Remote Desktop

ENDPOINT EVIDENCE FOLLOWS THE ACCESS

08:36:11 UTC | EDR detections

2026-01-09 08:36:11 UTC	Expedited	High		Rule Name: EDR Detection 1 </> Username: User Process Name: C:\Windows\system32\NOTEPAD.EXE  Command Line: "C:\Windows\system32\NOTEPAD.EXE" C:\ProgramData\AdUsers.txt 
2026-01-09 08:36:11 UTC	Expedited	Critical		Rule Name: EDR Detection 3 </> Username: User Process Name: C:\Windows\system32\NOTEPAD.EXE  Command Line: "C:\Windows\system32\NOTEPAD.EXE" C:\ProgramData\AdUsers.txt 
2026-01-09 08:36:11 UTC	Expedited	Critical		Rule Name: EDR Detection 2 </> Username: User Process Name: C:\Windows\system32\NOTEPAD.EXE  Command Line: "C:\Windows\system32\NOTEPAD.EXE" C:\ProgramData\AdUsers.txt 
2026-01-09 08:36:11 UTC	Expedited	High		Rule Name: EDR Detection 4 </> Username: User Process Name: C:\Windows\system32\nltest.exe  Command Line: "C:\Windows\system32\nltest.exe" /domain_trusts 

About six minutes between the SIEM and EDR detections.



AN INVESTIGATION SHOULD END WITH NEXT STEPS

FINDINGS

What happened?

SCOPE

What was affected?

ACTIONS

What must happen next?

Evidence should become a timeline and a response plan.



FIVE QUESTIONS FOR YOUR TEAM

- 01 Which remote tools belong here?
- 02 Can we connect endpoint, identity, and access activity?
- 03 Who investigates unexpected service changes and reboots?
- 04 Who reviews high-risk access after hours?
- 05 Can we contain both the endpoint and the identity?

QUESTIONS

THANK YOU

CyberOps 2026

