

Incident Response: From Breach to Recovery



Ahmed Shah
Senior Security Analyst
Malleum

Agenda

Incident Response

*“The structured process of **identifying**, **managing**, and **mitigating** the effects of **cybersecurity incidents** to **minimize damage**, **recover** operations, and **prevent future occurrences**” - SANS*

- Ransomware and incident response workflows
- What triggers an incident response
- Deep dive into a simple incident response scenario
- Deep dive into a ransomware scenario
- How to prepare in advance

KNP Logistics

Ransomware Attack – 2023

← → ↻ <https://metro.co.uk>  ⋮

M **UK** [HOME](#) [NEWS](#) [ENTERTAINMENT](#) [SPORT](#) [LIFESTYLE](#) [SOAPS](#) [OPINION](#) [SHOPPING](#)
[London](#) [US](#) [World](#) [Crime](#) [Tech](#) [Science](#) [Politics](#) [News Updates newsletter](#) [E-edition](#)

A company that had traded for more than 150 years and employed 700 people was brought down because of a weak password.

Logistics firm KNP went out of business after criminals successfully hacked into its computers by guessing an employee's password before locking the whole company out of its systems.

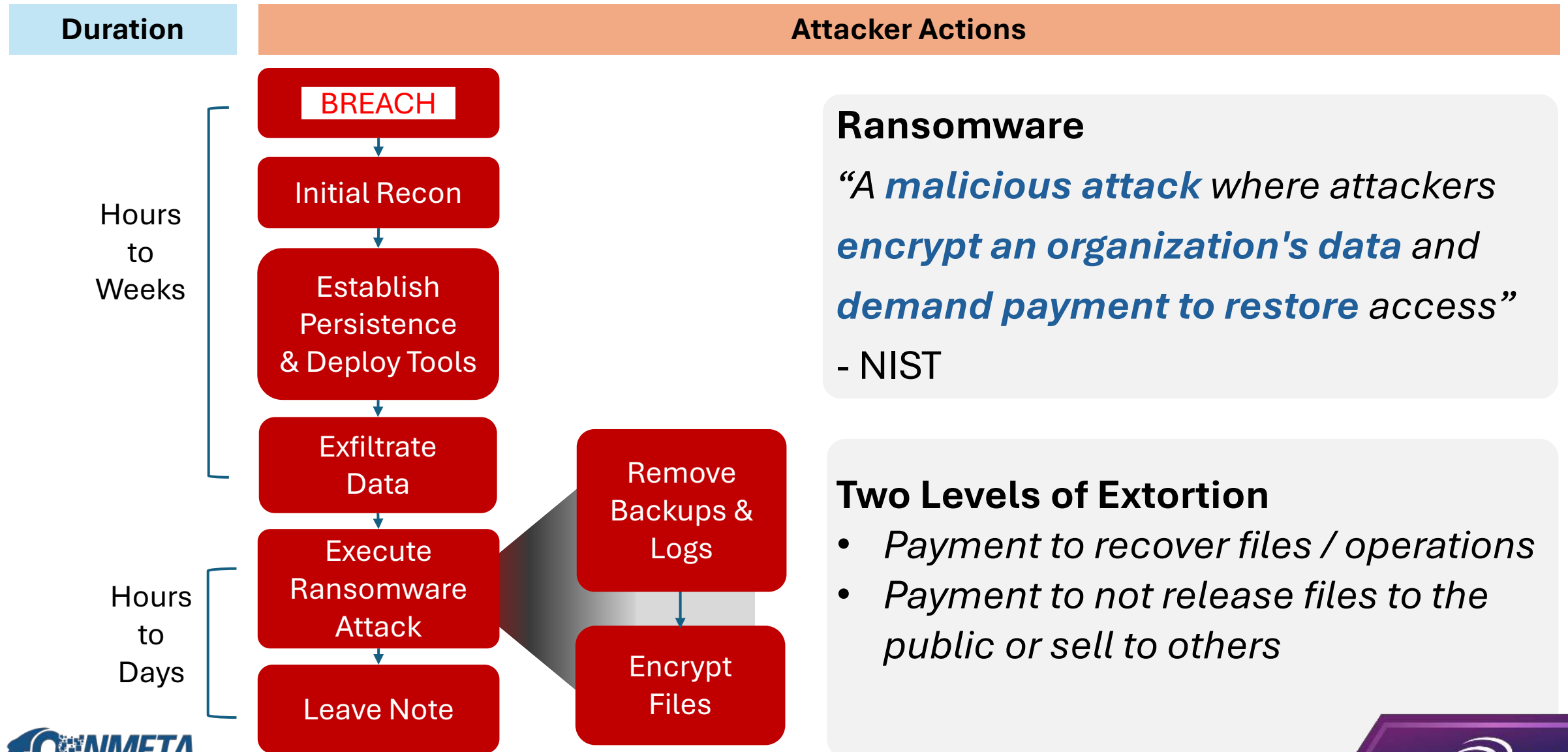
← → ↻ <https://motortransport.co.uk>  ⋮

MotorTransport   

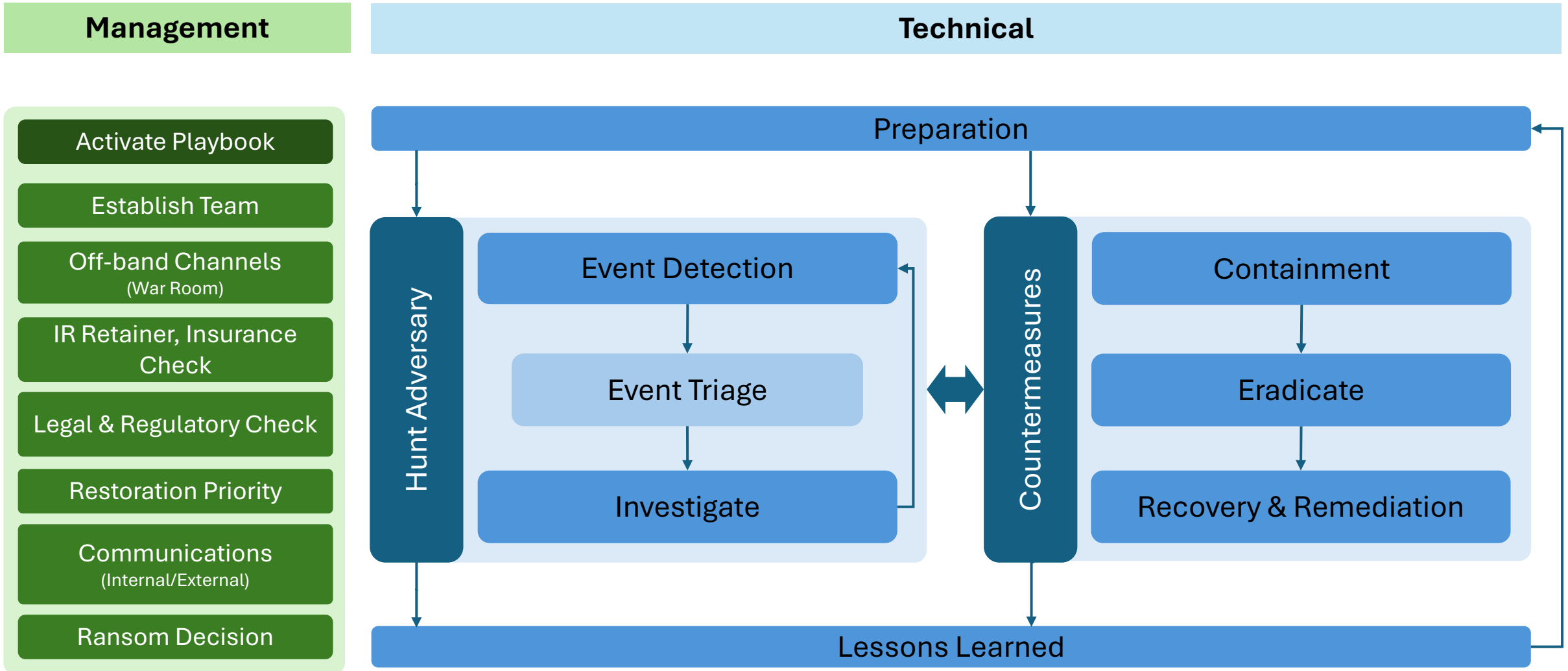
The ransom note said: "If you're reading this it means the internal infrastructure of your company is fully or partially dead. For now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue."



Attacker Workflow



Incident Response Workflow



Roles and Responsibilities

Incident Commander	Single point of authority. Makes approvals. Understands priorities. Usually, CISO or Director of IT.
Principal Technical Lead	Turns objectives into Incident Response tasks.
Forensics Lead	Performs threat hunting. Determines what happened. Makes sure evidence is preserved. Performs reverse engineering if needed.
Containment Lead	Isolates environment to prevent attack from spreading. Controls firewalls and access controls. Assists with eradicating attacker persistence.
Recovery Lead	Restores systems from known-good sources onto a trusted (clean) network.
Communications Lead	Handles internal/external communications (company-wide email, customer notifications, media)
Internal SME	Knows the affected systems in the organization.
Executives / Mgmt	Has interest in keeping operations running. Owns risk and business decisions.
Legal Counsel	Advises on notifications, legal and regulatory obligations.
Project Manager	Consolidates information for status updates.

Incident Response Playbook

Status Meeting

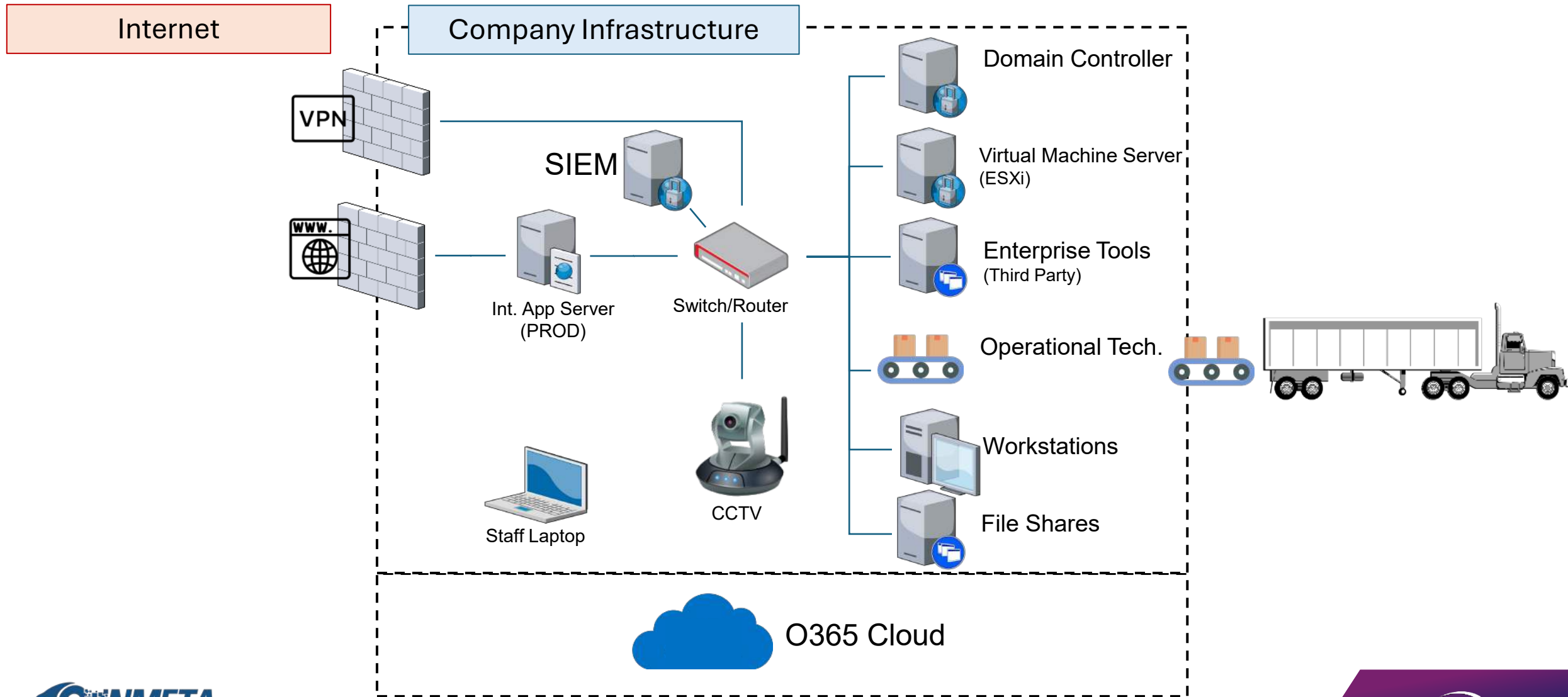
- General Impact Assessment
- General Containment Status
- Expected/Estimated Time to Recovery
- Task Prioritization
- System X Analysis Progress [0% - 100%]
- System Y Restore Progress [0% - 100%]
- Domain Controller Rebuild [0% - 100%]
- Kerberos Resets [0% - 100%]
- Network Enclave Setup Progress [0% - 100%]
- EDR Deployment [0% - 100%]
- EDR Visibility [0% - 100%]



The **BREACH**: How Attackers Get In

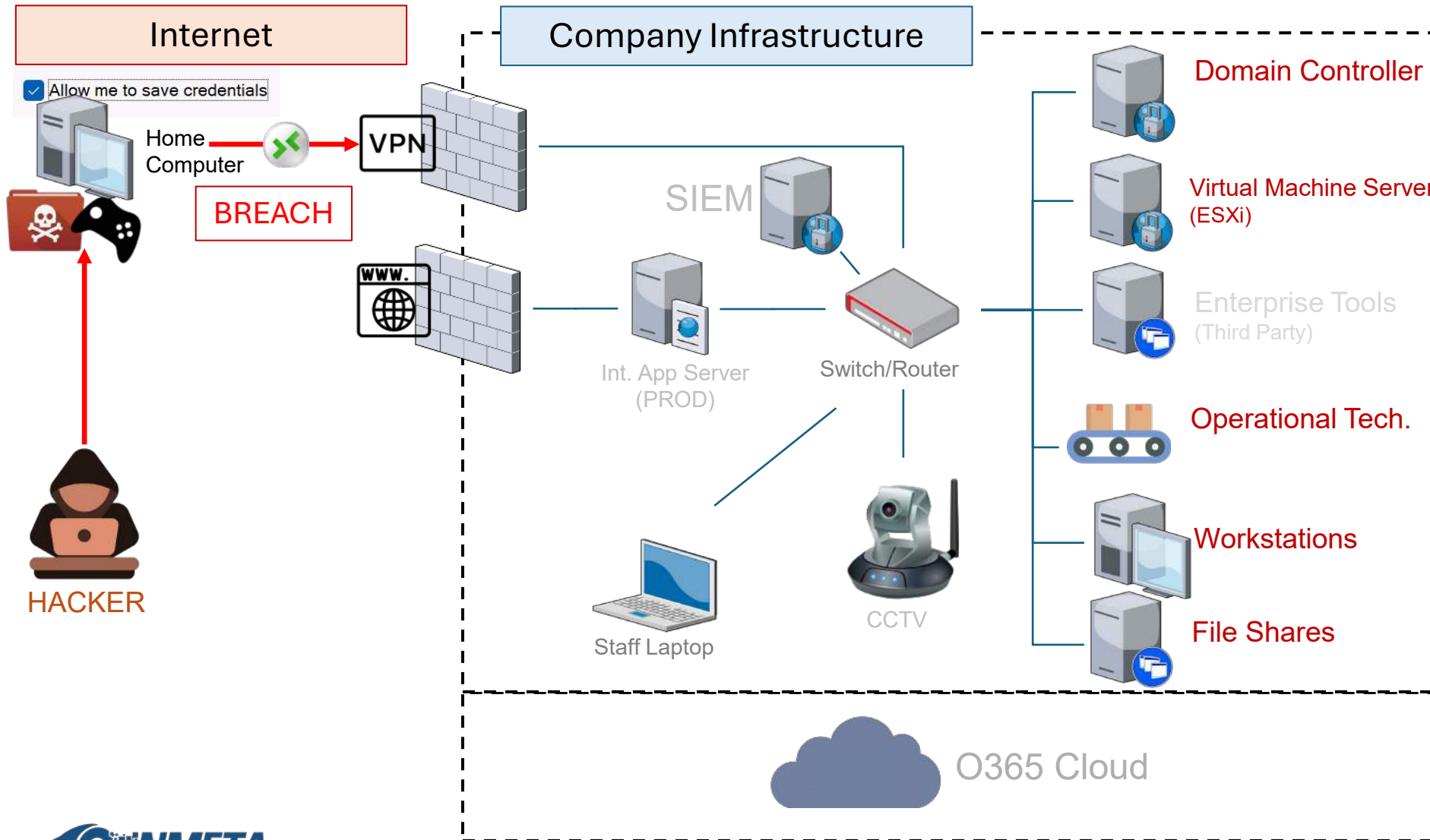
What Triggers an Incident Response (IR)

Typical Corporate Network



Personal PC Used for Work

Infected System Connected to Company Network



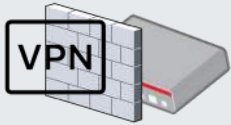
Notable Observations

Ransomware Attack

- **What Triggered Incident Response:**
Audio alert, ransom note
- Forensics performed on personal machine

Other Cases

Attacker's Entry into Company Network



Brute-force attack:

Firewall's admin login portal exposed to internet



Critical CVEs – Remote Code Execution:

Firewall unpatched
(subscription expired)



Supply Chain Attack:

Software update contains backdoor

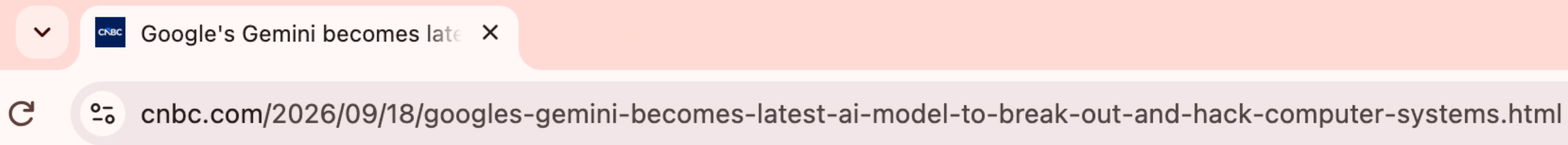
What Triggered Incident Response

Staff not able to access files when coming back to work

Staff not able to access files when coming back to work

News headline

Near Future



BREAKING

Stocks making th



Google's Gemini becomes latest AI model to break out and hack computer systems

In May, the Gemini model accessed three separate private computer systems by guessing passwords and by twice using a repository of publicly listed passwords, Google said.



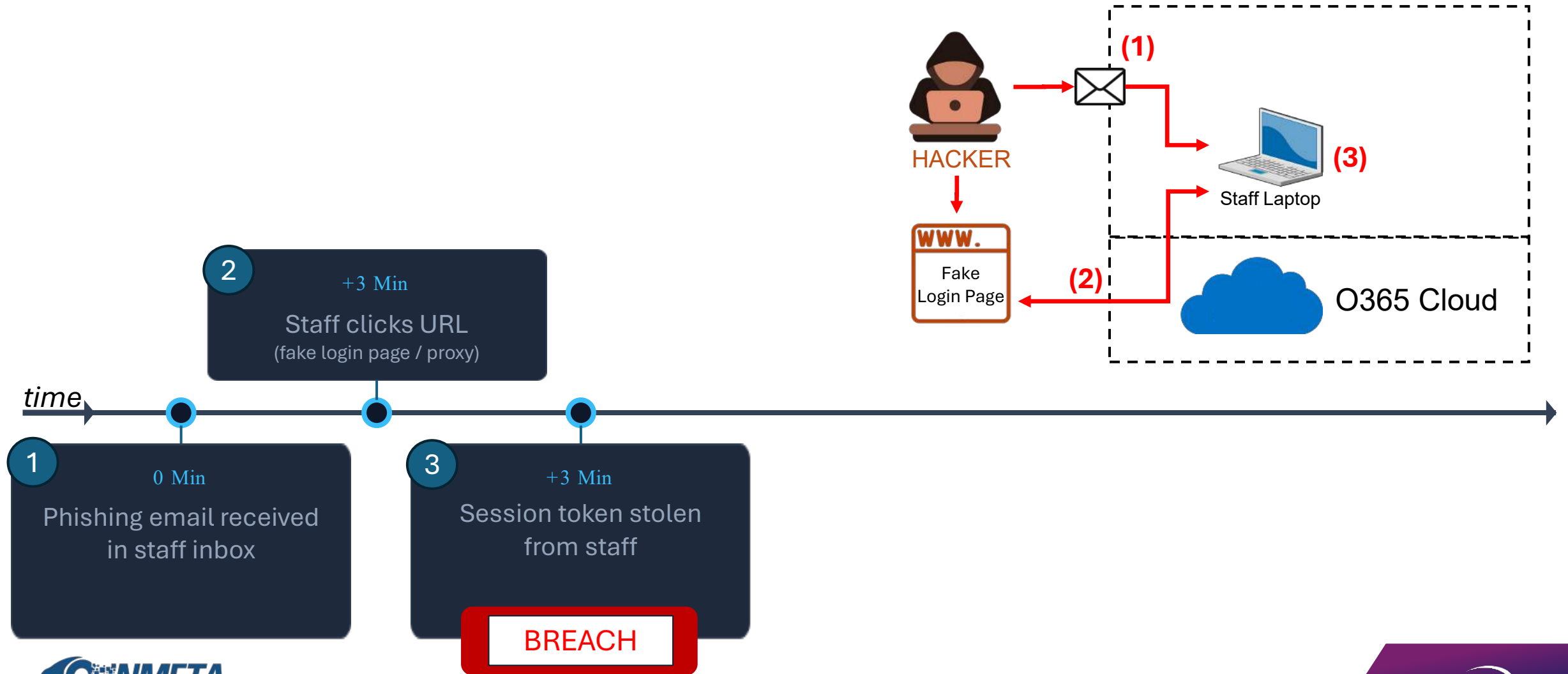
Incident Response

Simple Scenario

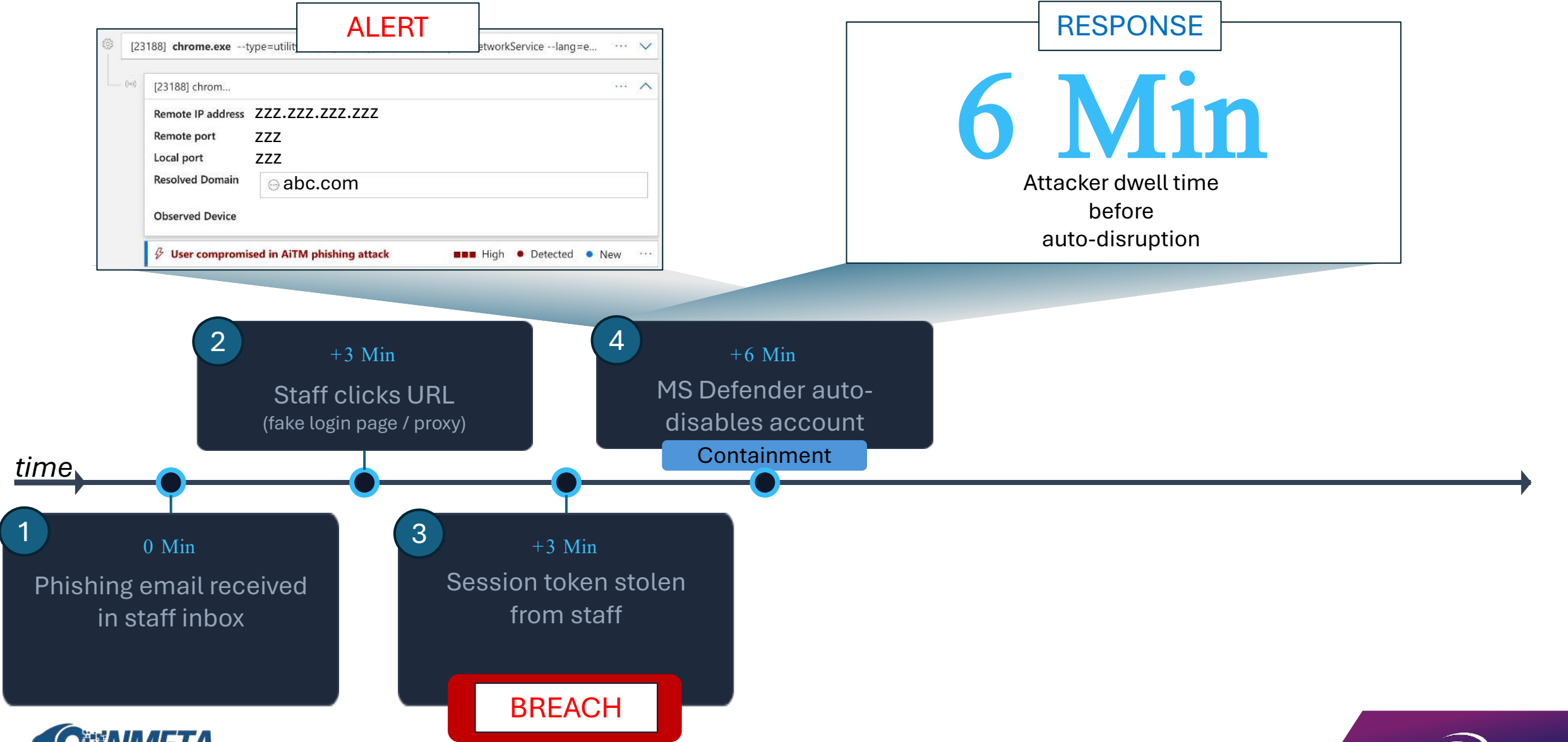
Environment:

- Organization heavily relies on SaaS
- No on-prem servers
- Accounts tied MS E5 Security license
- **Incident Response Trigger:** MS Defender Alert to SOC

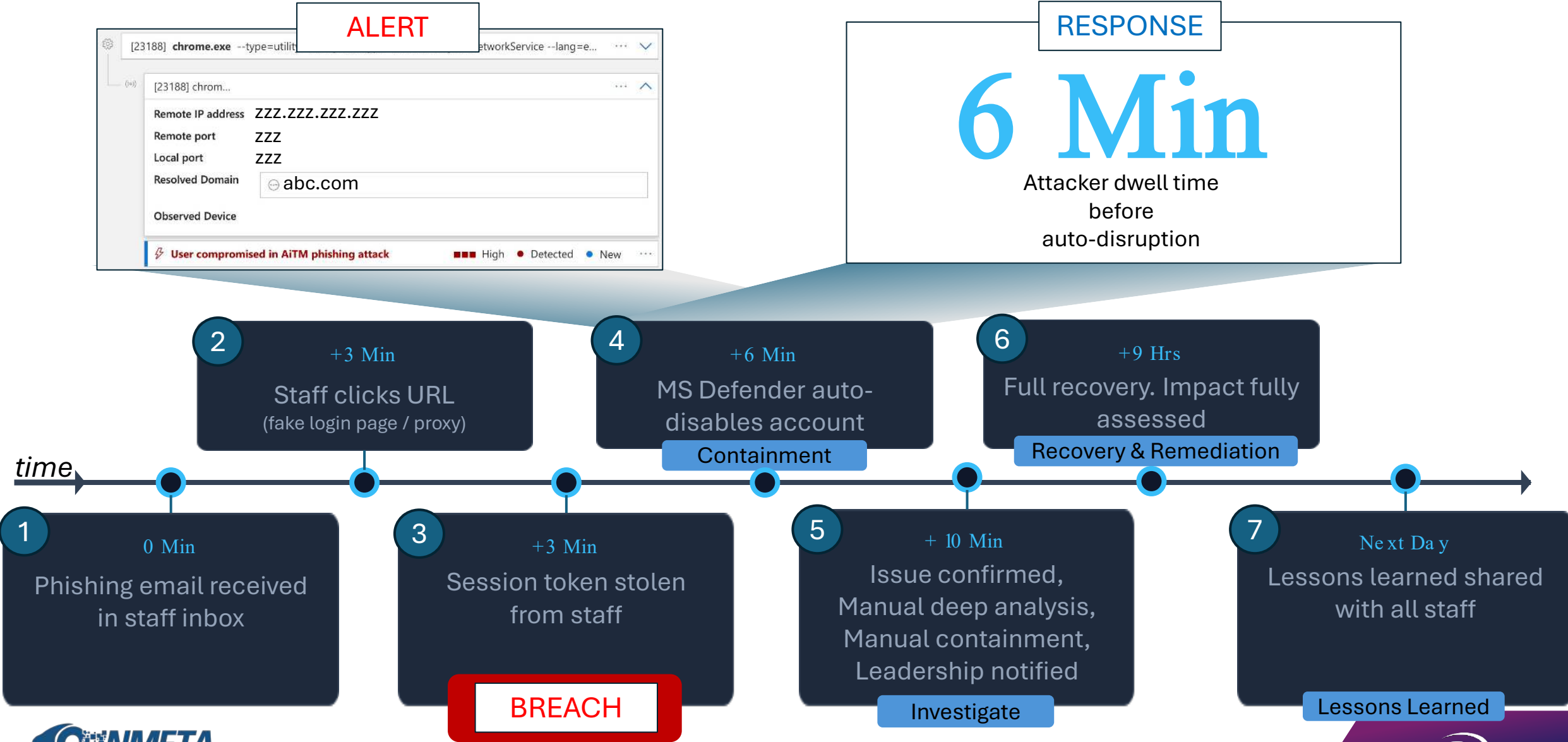
Attack Timeline



Attack Timeline



Attack Timeline



Incident Response Actions

Containment

- Confirm account is disabled
- Revoke all sessions. Reset Password. Remove all MFA methods.
- Isolate laptop. Don't power off.

Communication & Executive Operations

- Notify leadership
 - Check legal / regulatory obligations (breach notifications)

Analysis

- Investigate incident (root cause, impact, check if anyone else receive the email)
- Review and export logs



admin.exchange.microsoft.com

Message trace (Email forensics): Who received the phishing email and when



security.microsoft.com

Main IR Console: Alert, user, and device timelines. IP search (to/from). Advanced Hunting (KQL).



entra.microsoft.com

Sign-in logs (review access region), revoke sessions, enable/disable account



intune.microsoft.com

Device inventory and compliance state



purview.microsoft.com

Unified audit log and eDiscovery search: What data was accessed



Incident Response Actions

Analysis (cont.)

- Perform memory capture and analysis of laptop
- Baseline - Check user behavior before and after account compromise
- Check if new accounts were created
- Check if new inbox rules were created such as email forwarding
- Forensic image of drive for evidence preservation (log hash)
- Document all due diligence activities
 - True positives and false positive findings

Recovery

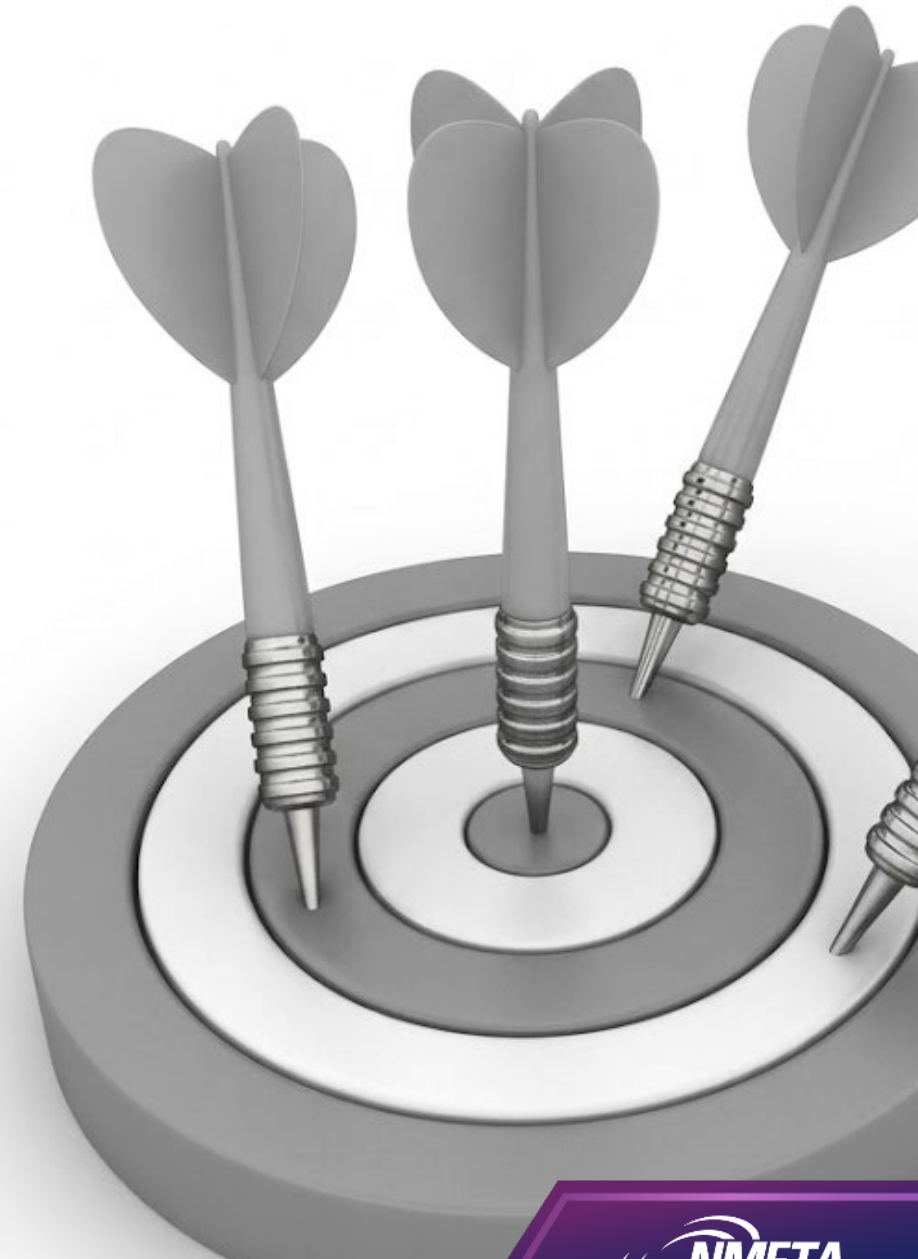
- New laptop, reset password, re-register MFA, then enable account
- Monitor for 30 days

Regulatory obligations

- Example: Is an external breach notification required?
- Retention period for investigation artifacts

Post-Incident

- Reporting
- Lessons learned



Incident Response

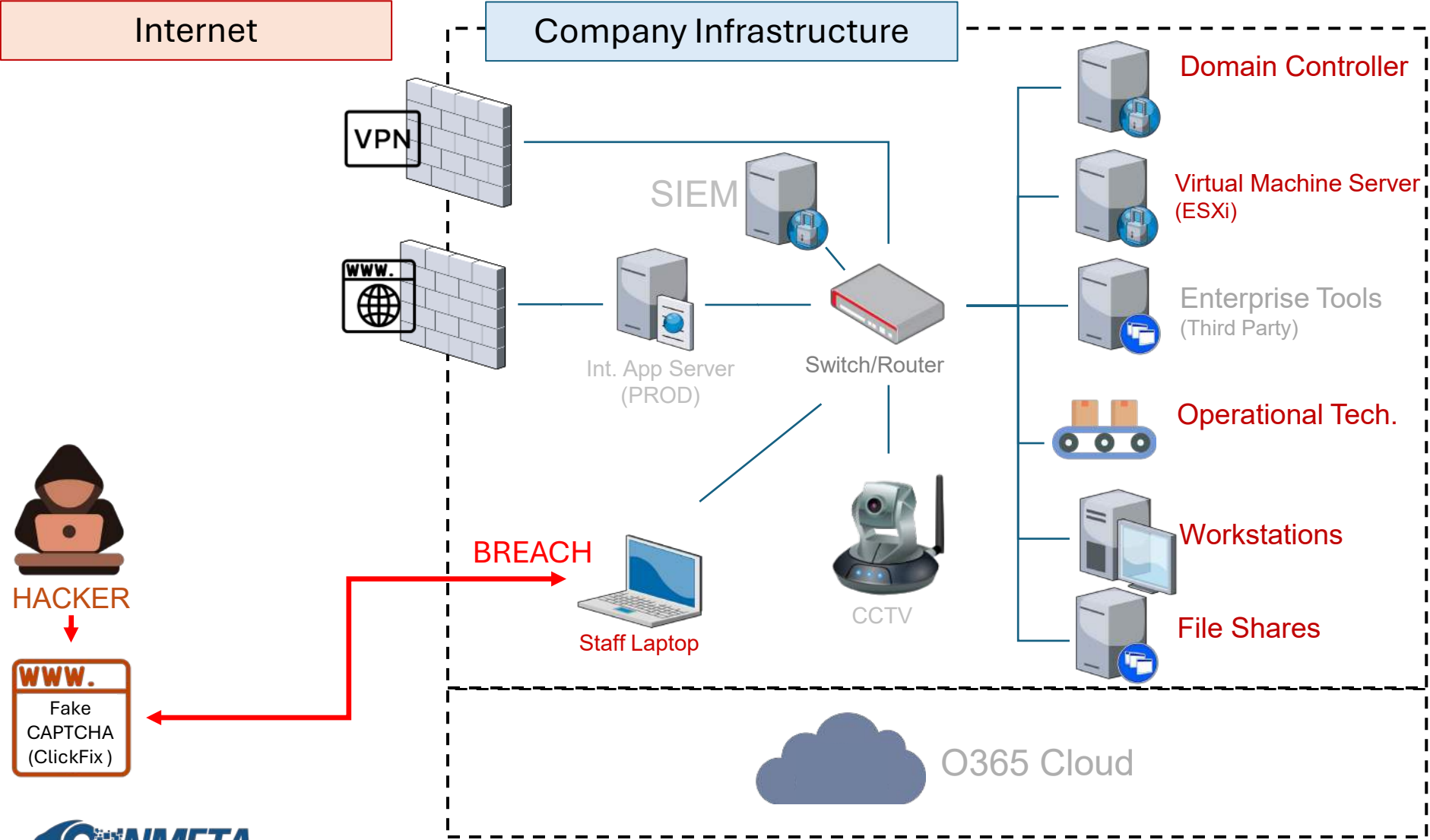
Composite Complex Scenario

Environment:

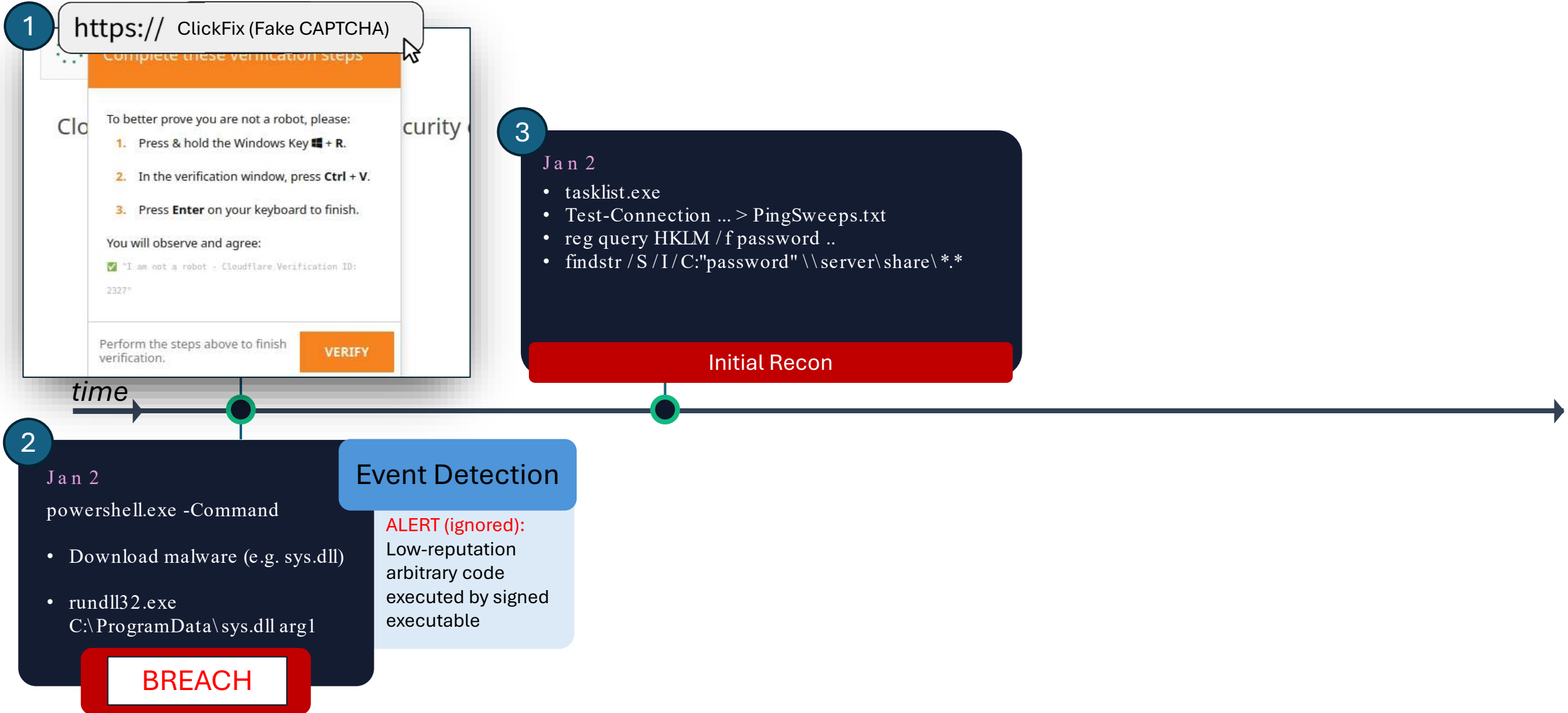
- Alerts not well monitored
- Corporate file shares (SMB) contained passwords
- Some systems don't have EDR
- Large amount of on-prem systems
- No network segregation
- **Incident Response Trigger:** Staff could not access files when returning to work

Social Engineering

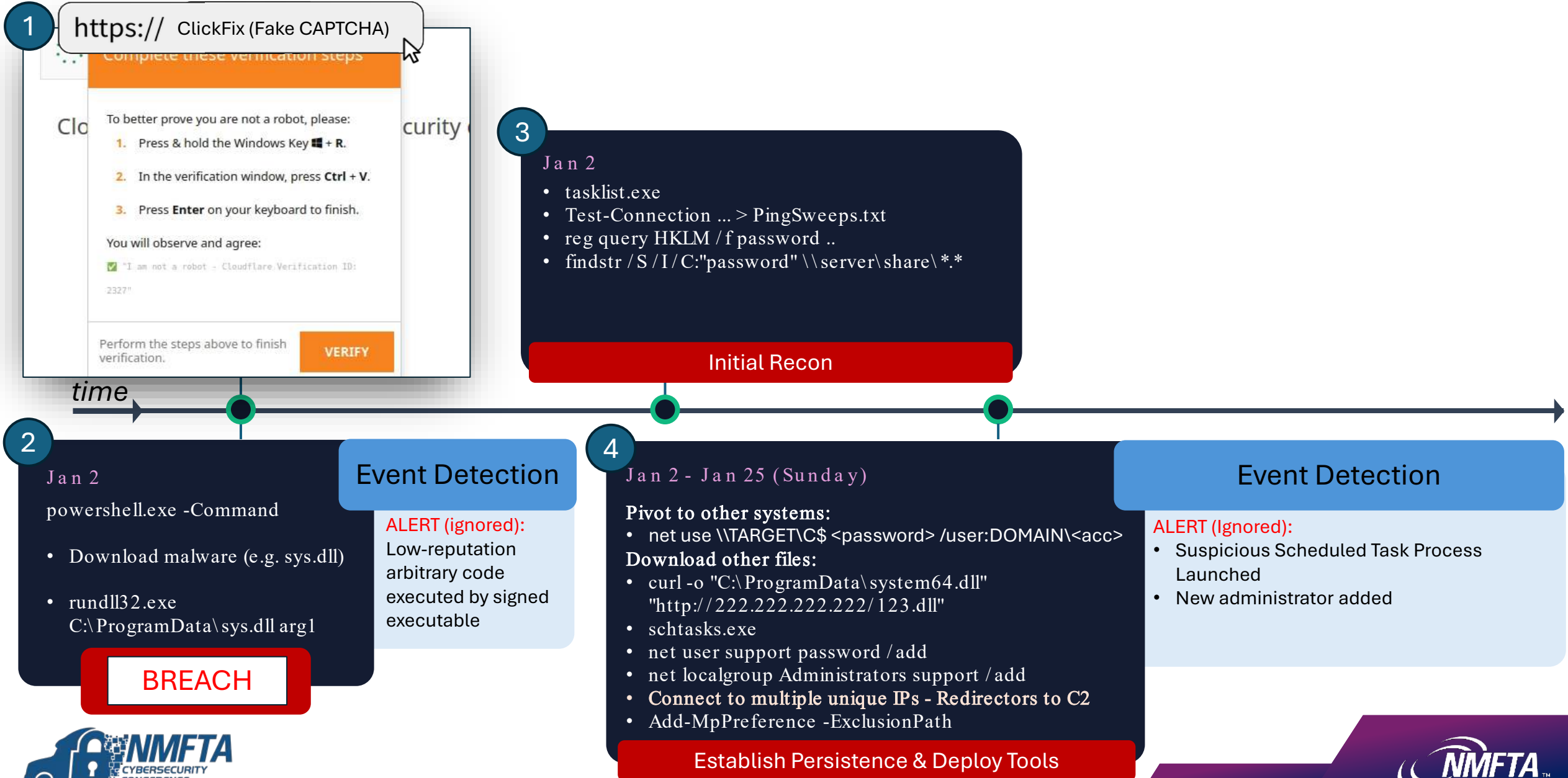
Staff Executes Attacker Commands



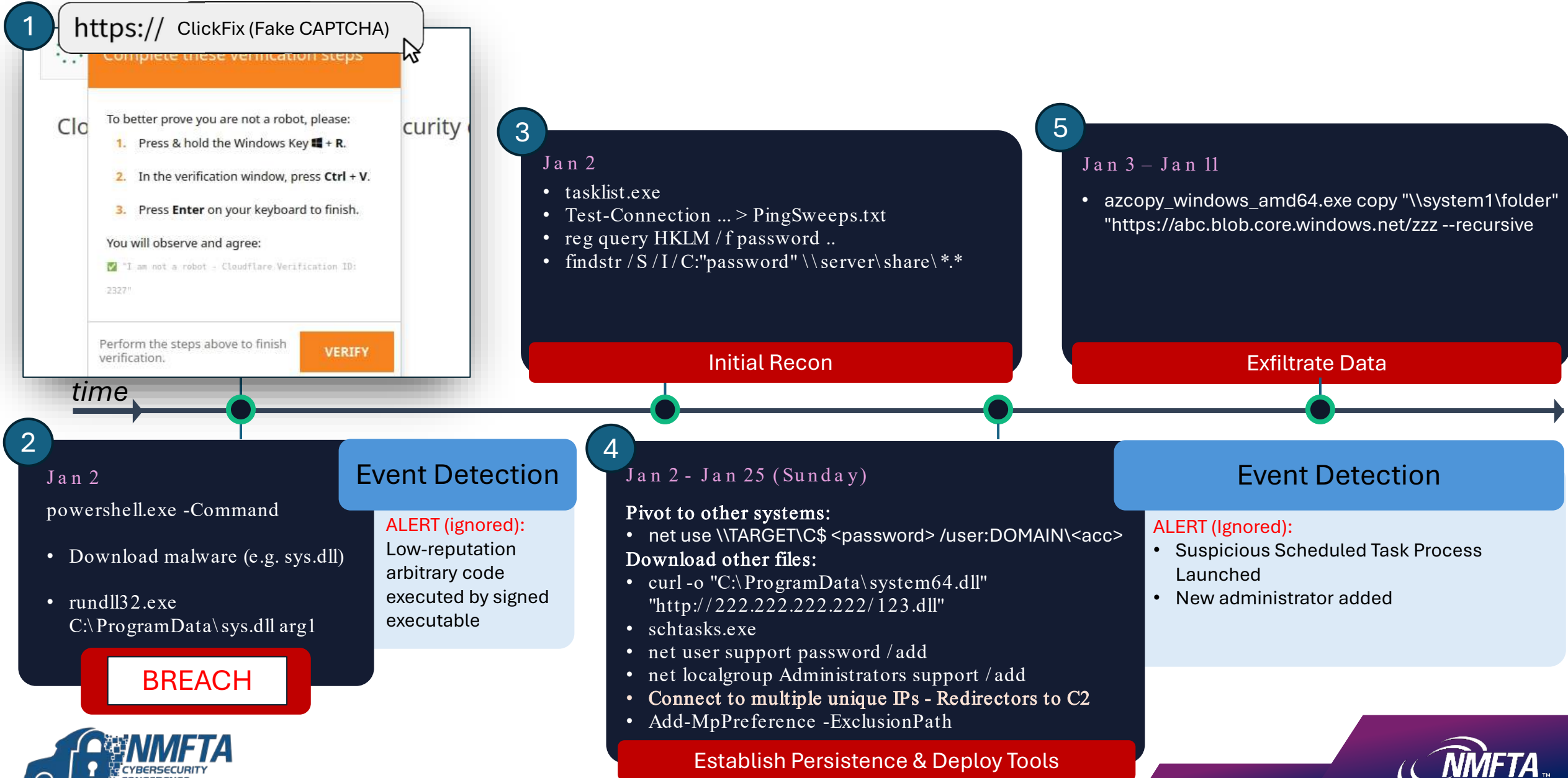
Ransomware Attack Timeline



Ransomware Attack Timeline



Ransomware Attack Timeline



Ransomware Attack Timeline

6

Jan 25 (Sunday)

- vssadmin delete shadows /All /Quiet
- wmic shadowcopy delete
- wbadmin.exe delete ...
- fsutil usn deletejournal ...
- wevtutil cl security
- Remove-Item

Remove Backups & Logs

Event Detection

ALERT (ignored):

- Suspicious activity - File backup deleted

7

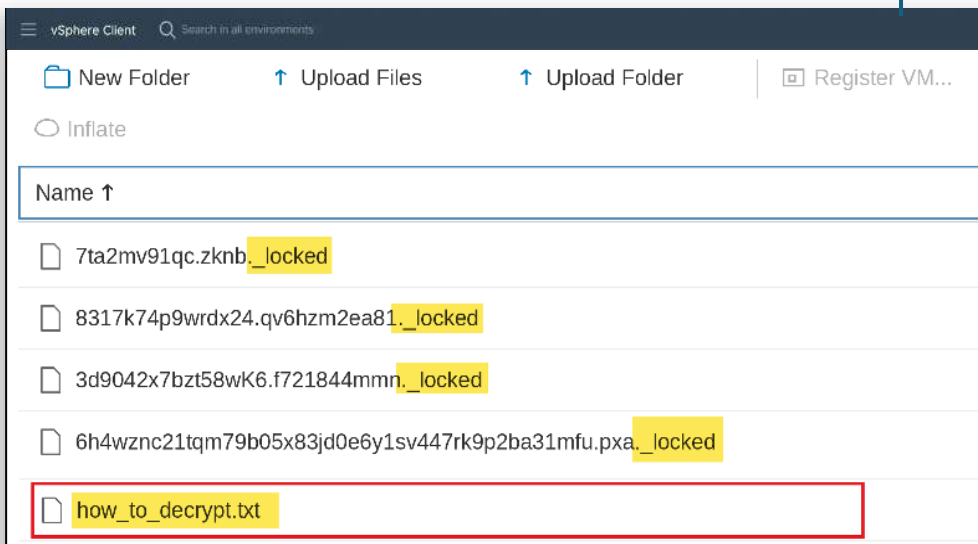
Jan 25 – On-going

- sj3264.exe arg3
- ._locked extension added to each file

Encrypt Files

Containment

time



Ransomware Attack Timeline

6

Jan 25 (Sunday)

- vssadmin delete shadows /All /Quiet
- wmic shadowcopy delete
- wbadmin.exe delete ...
- fsutil usn deletejournal ...
- wevtutil cl security
- Remove-Item

Remove Backups & Logs

Event
Detection

- ALERT (ignored):**
- Suspicious activity - File backup deleted

7

Jan 25 – On-going

- sj3264.exe arg3
- .locked extension added to each file

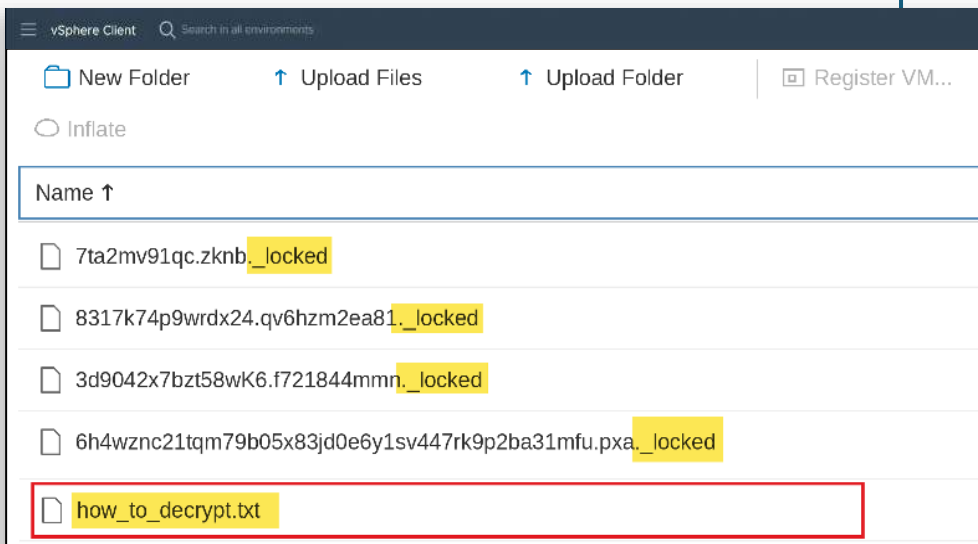
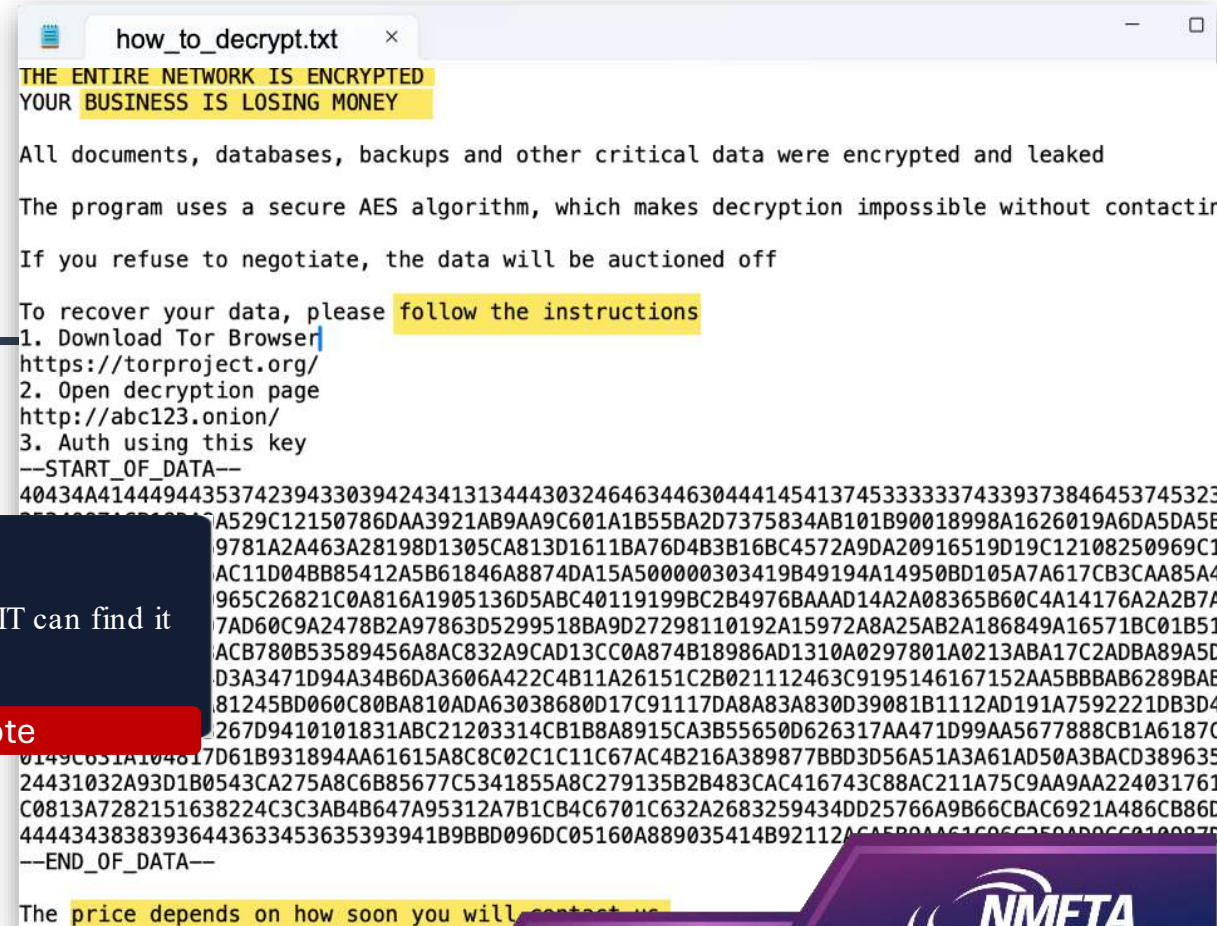
Encrypt Files

8

Jan 25

Leave note where IT can find it

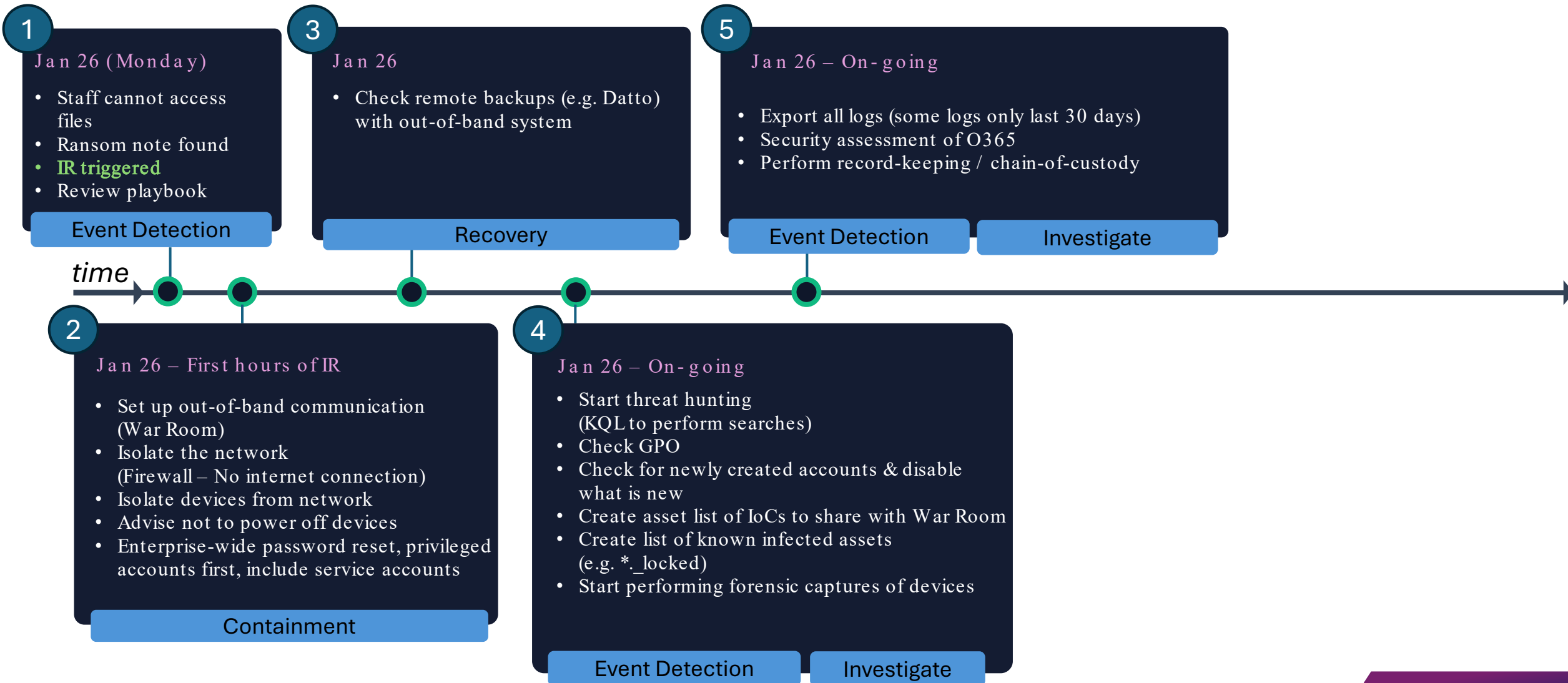
Leave Note



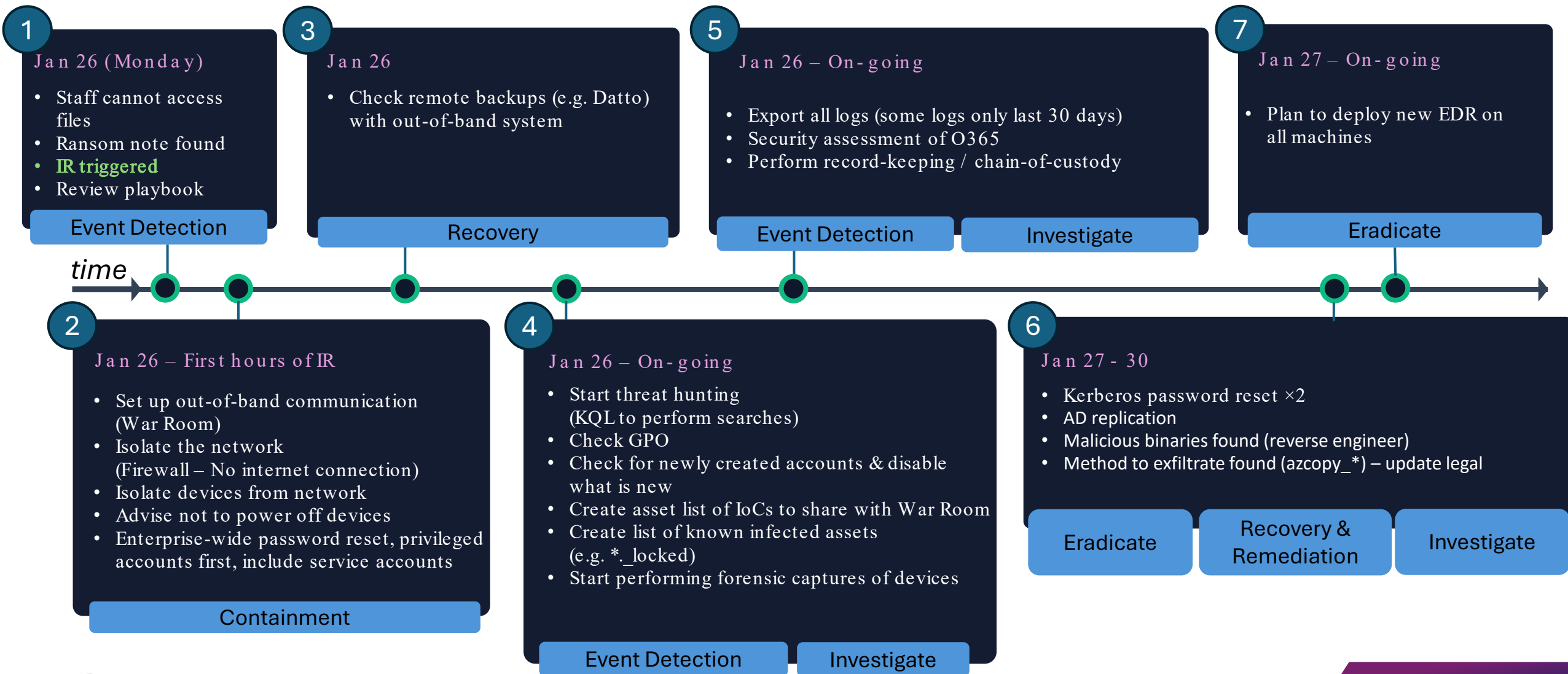
Technical Incident Response Timeline



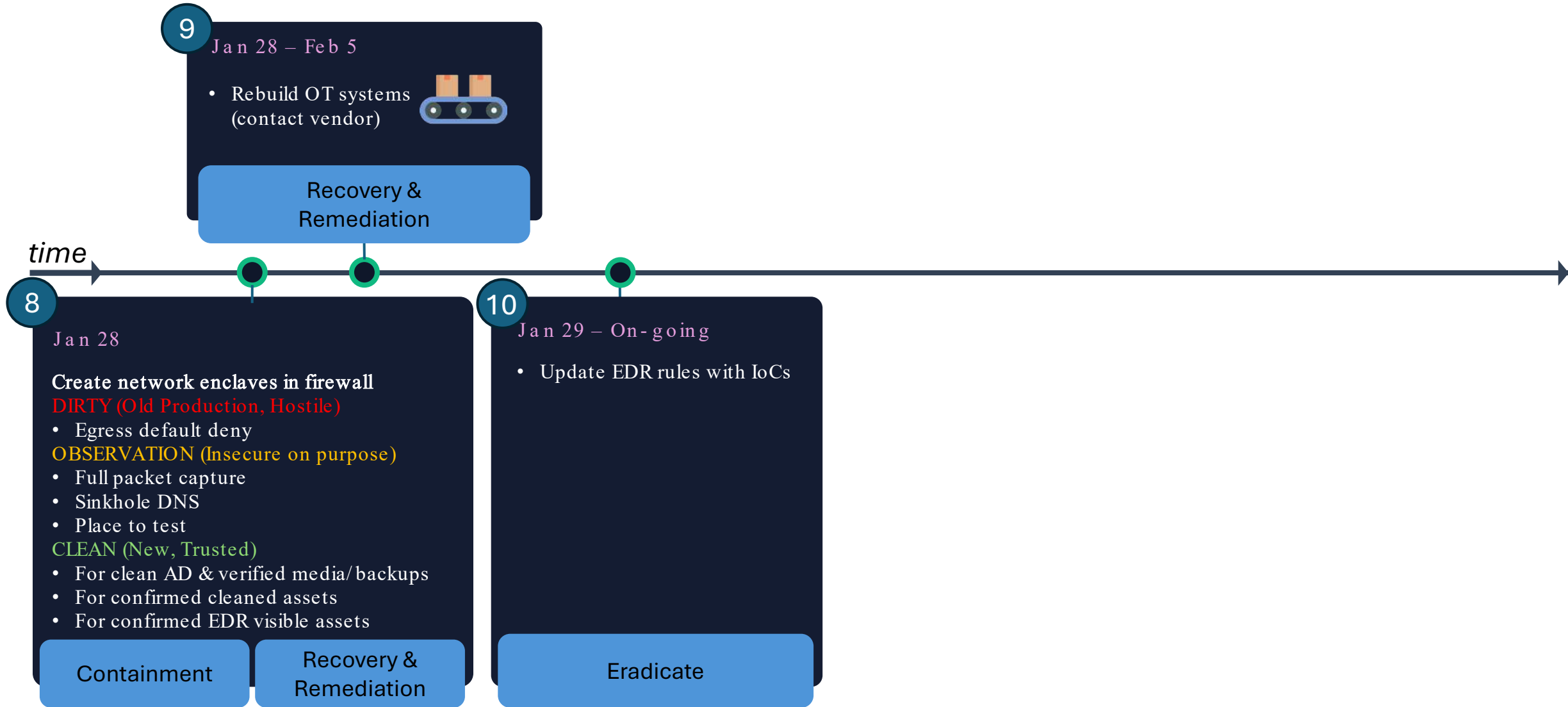
Technical Incident Response Timeline



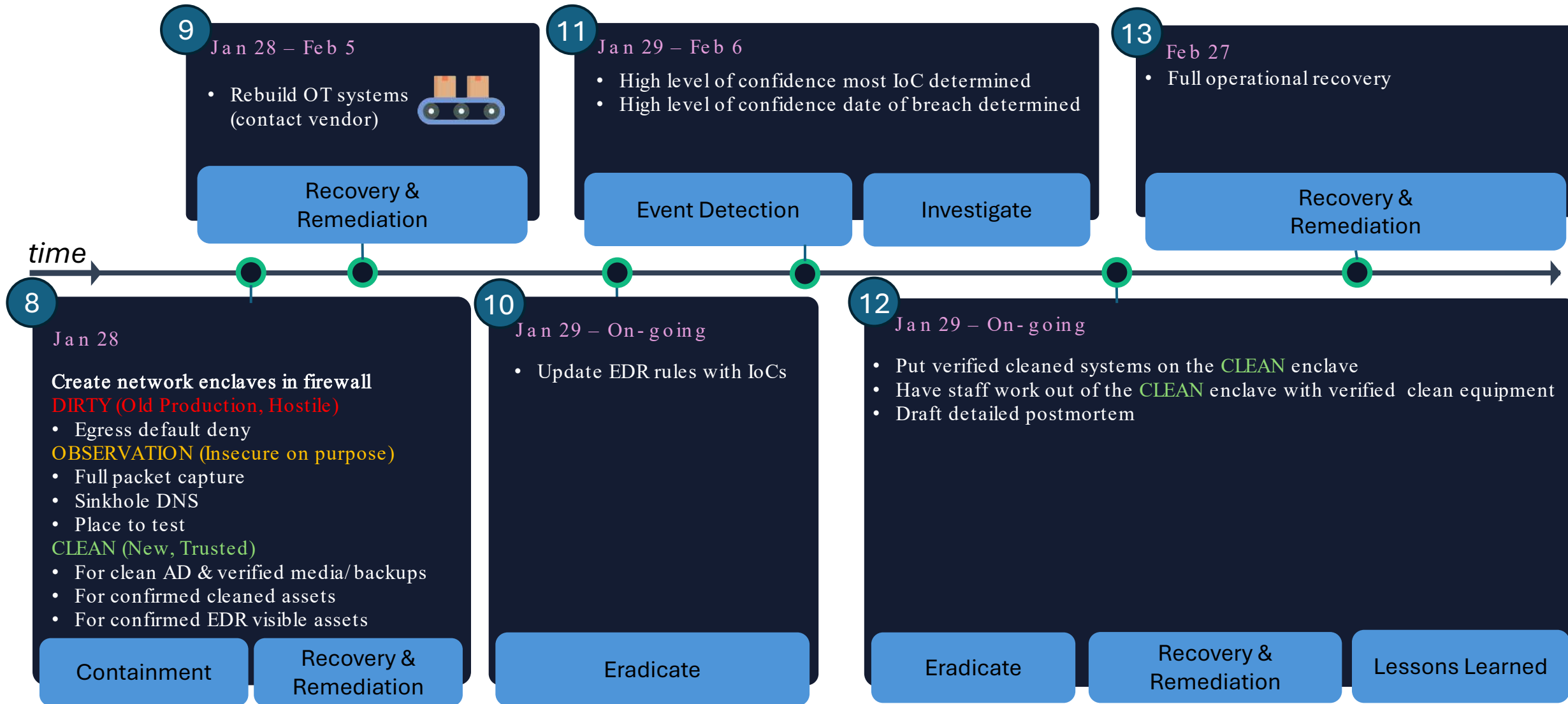
Technical Incident Response Timeline



Technical Incident Response Timeline



Technical Incident Response Timeline



How to Prepare in Advance

Work you do before an incident

How to Prepare

- Prepare a playbook
- Build a Technology System Restoration Index (TSRI)
 -  [Index #, System Name, Physical Location, Description, Priority, Upstream Dependencies, Owner]
 - Determine how long it takes to drive to the affected site
- Determine how far back logs can go
 - Log retention/rotation period
 - Which are remote/offsite
- Check backup frequency & if stored offsite. Test restore
- Determine detection visibility
 - Example: Does the hypervisor have an EDR/detection?
 - Perform purple-team exercises
 - Determine if alerts are reported properly
- Check SharePoint, GitHub History, file shares, SMB for leaked secrets
- Maintain up-to-date network/architecture diagrams
- Perform regular vulnerability scanning and patching
- Conduct tabletop exercises
- See what can be automated
 - SOAR - Security Orchestration, Automation, and Response



Incident Response & Forensic Tools

Detection & Prevention

SIEM
(e.g. Sentinel, Splunk)

EDR Suite
(e.g. Microsoft Defender)

Entra ID protection

Firewall / IDS / IPS

Investigation & Forensics

MS Security Portals
(e.g. Purview, IR console ext..)

KAPE

Autopsy / Sleuth Kit

Event Viewer

FTK Imager

Redline

Sysinternals Suite
(e.g. Procmon)

Wireshark

VirusTotal – Send hashes

Ghidra

Velociraptor

Containment & Eradication

MS Security Portals
(e.g. Entra, revoke sessions..)

EDR host isolation

Firewall enclaves
(Dirty, Observation, Clean)

Recovery & Coordination

Immutable backups
(e.g. Veeam, Datto)

Out-of-band communications
(e.g. Signal)

Off-of-band storage
(e.g. Sharefile.com)

Ticketing System

MITRE ATT&CK Navigator

Questions?

Ahmed Shah

Malleum

ashah@malleum.com

+1-877-RED-TEAM

Resources

- [NMFTA - Ransomware Playbook Template](#)
- [NIST IR Framework - NIST SP 800-61 Revision 3](#)
- Blue Team Handbook: Incident Response - Don Murdoch
- [SANS - Incident Handler's Handbook - Patrick Kral](#)
- [CISA - Cybersecurity Incident & Vulnerability Response Playbooks](#)
- [CIRO - Ransomware Response Playbook](#)