COHESITY

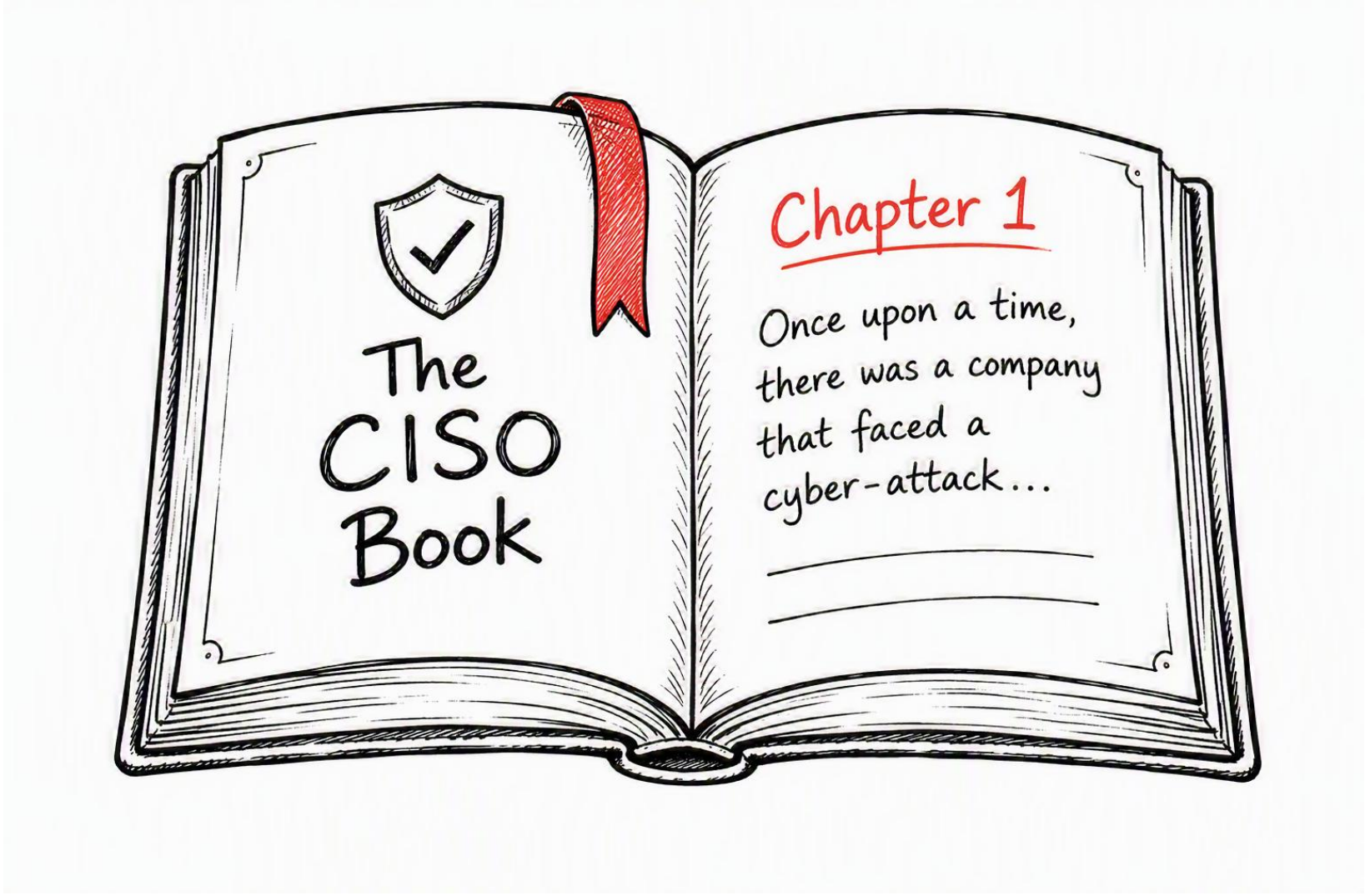
From Panic to Control

How to respond to a cyber attack

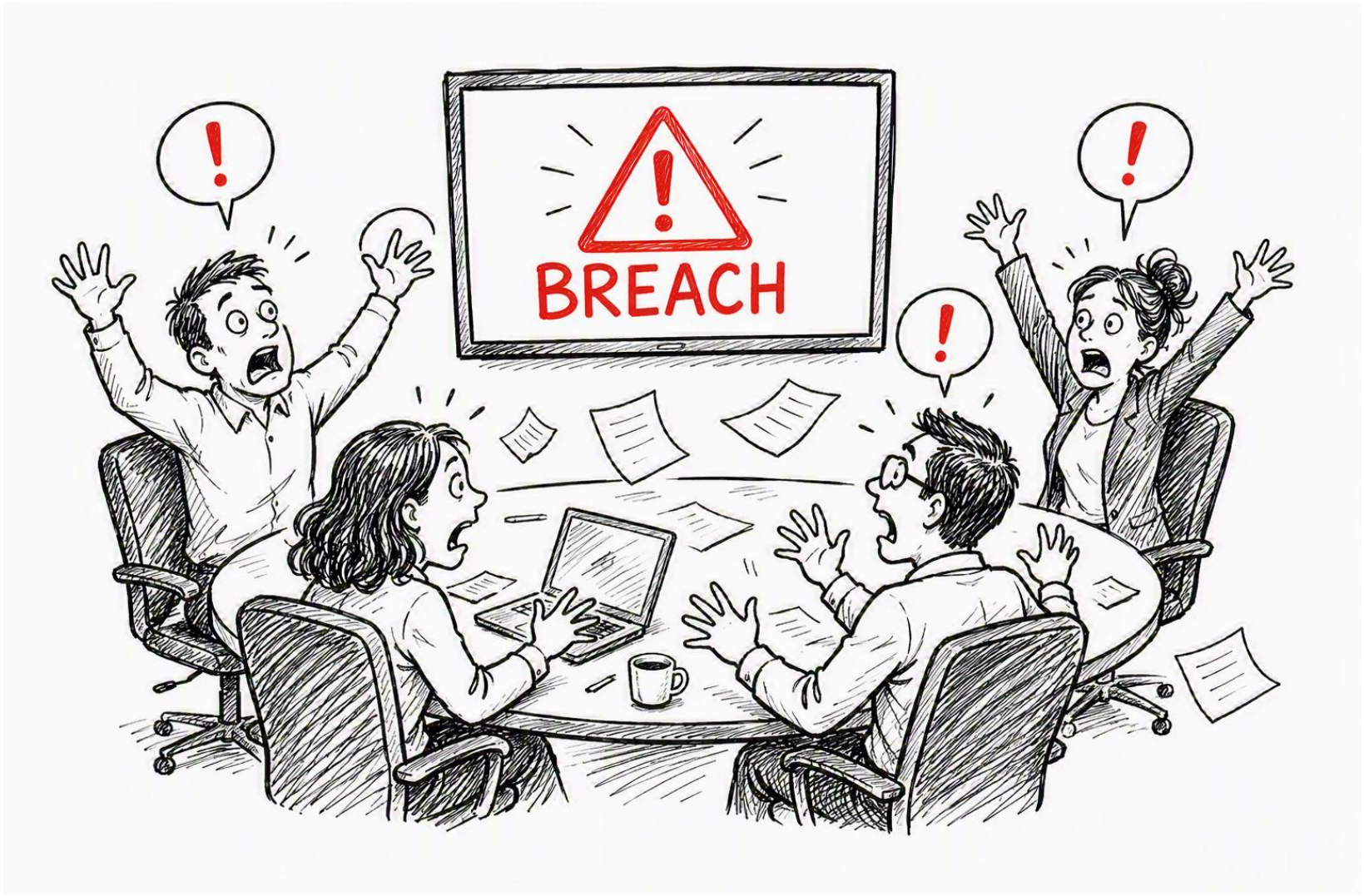
Petter Sveum
Field CTO Europe & Emerging

2026-11-06, NetNordic, Uppsala, Sweden

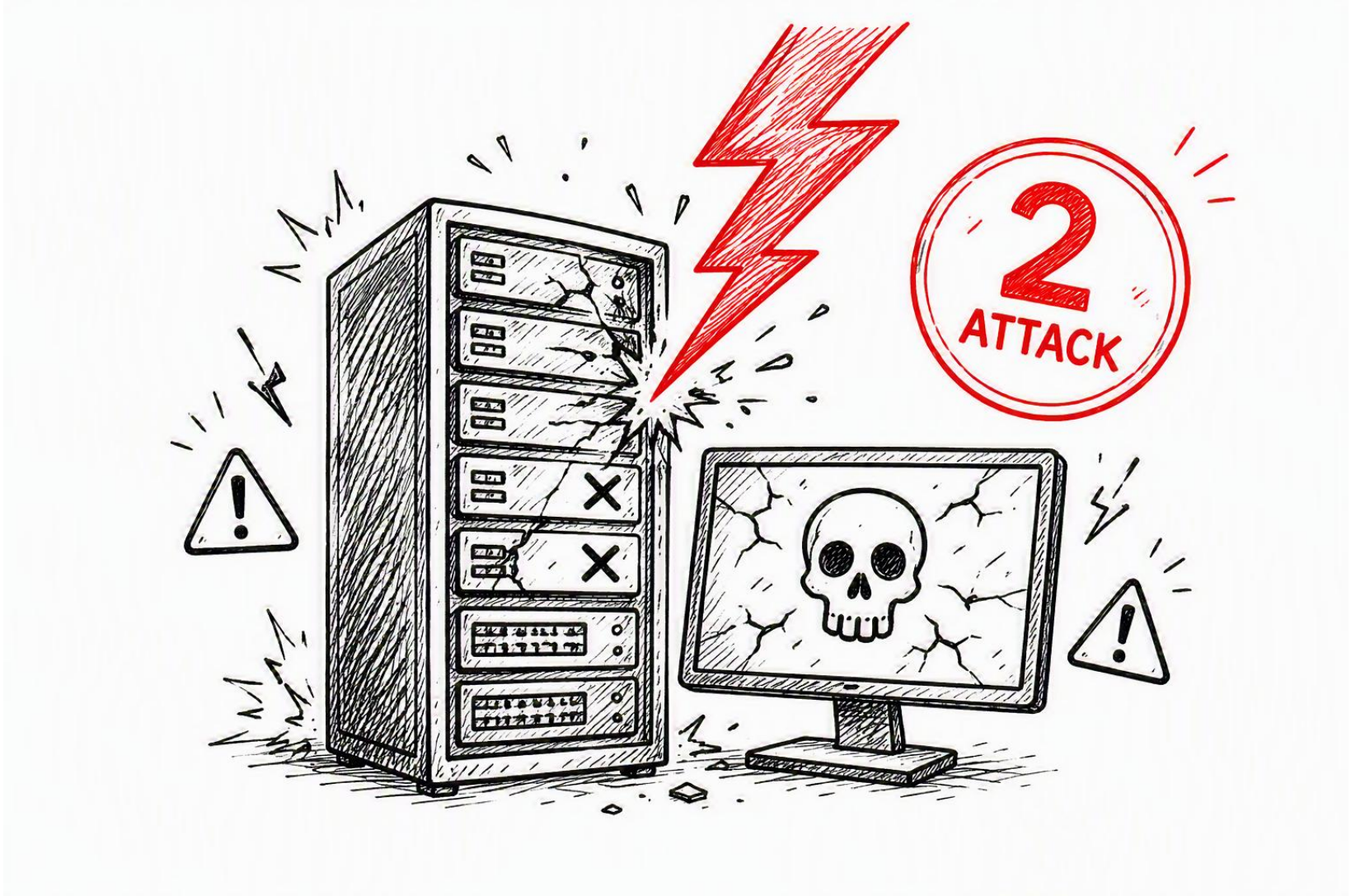




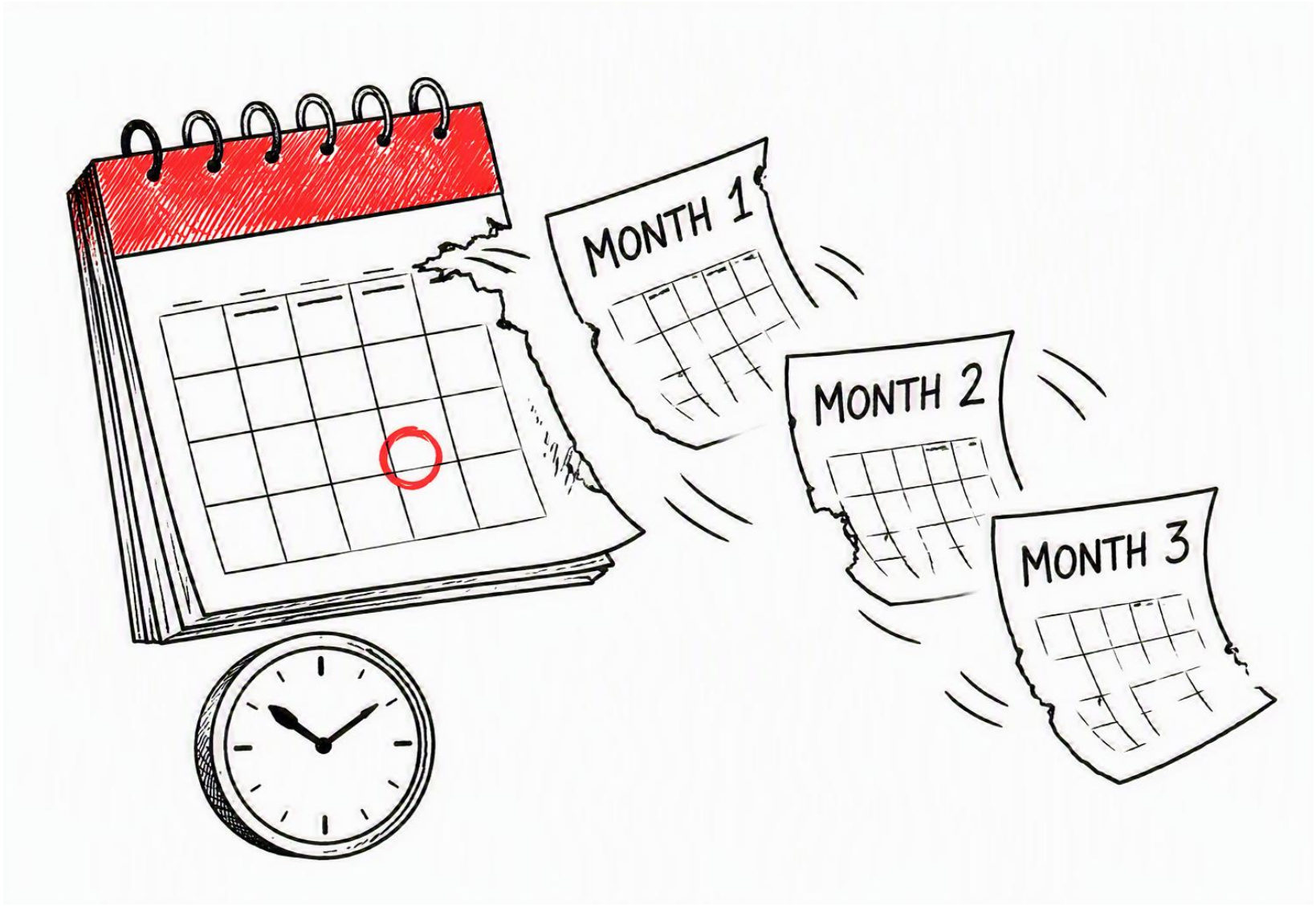
COHESITY © 2026 Cohesity Inc. All rights reserved.



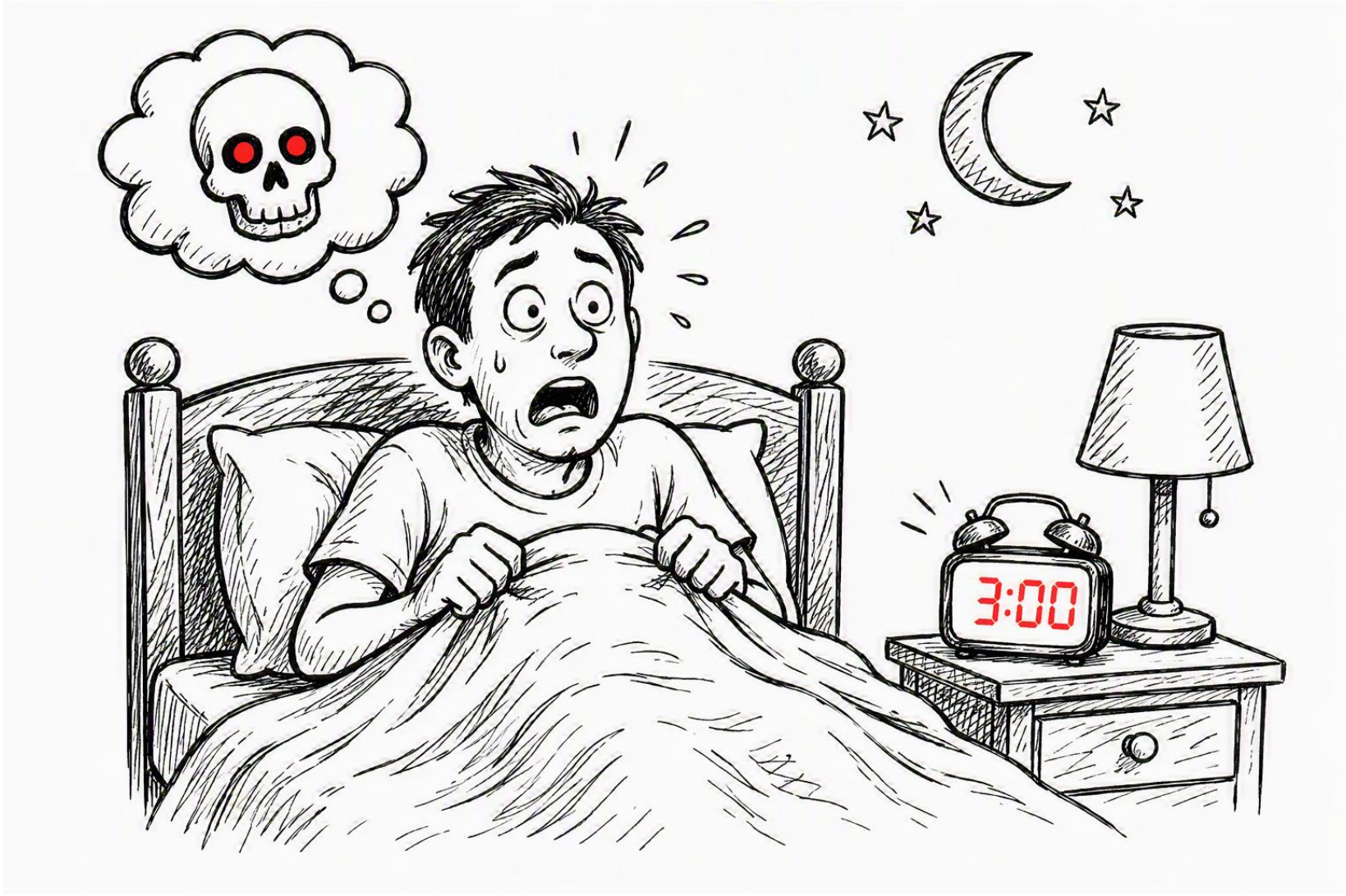
© 2026 Cohesity Inc. All rights reserved.



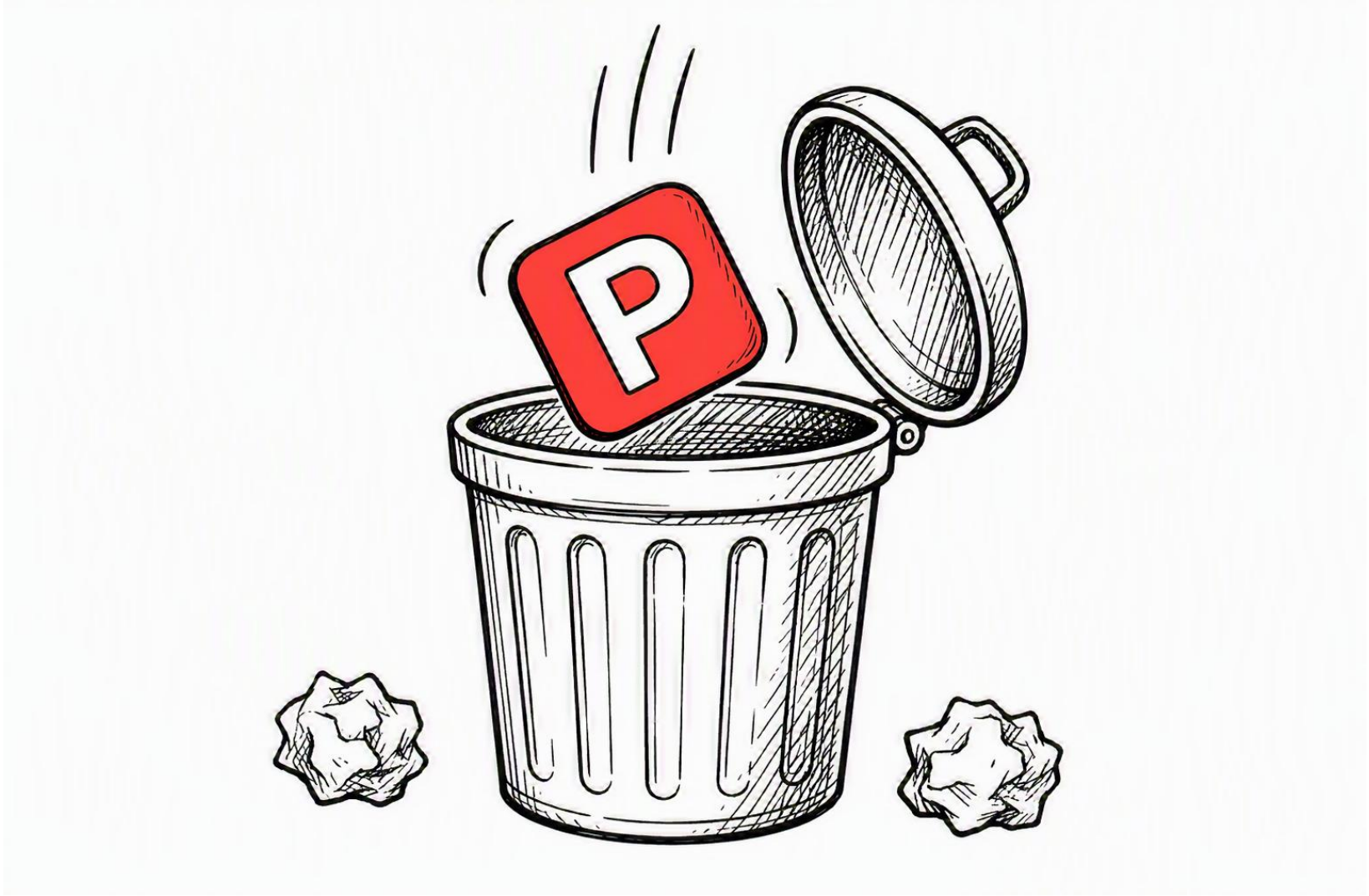
© 2026 Cohesity Inc. All rights reserved.



© 2026 Cohesity Inc. All rights reserved.



© 2026 Cohesity Inc. All rights reserved.



© 2026 Cohesity Inc. All rights reserved.

Lessons from real-world cyber attacks

Identity is under attack

Stolen credentials, social engineering (phishing), and brute force methods

IT is fragmented

Complex, heterogeneous environments with multiple teams, tools, & processes



Backups are vulnerable

Without immutability and zero trust access controls, backups are exposed to attack

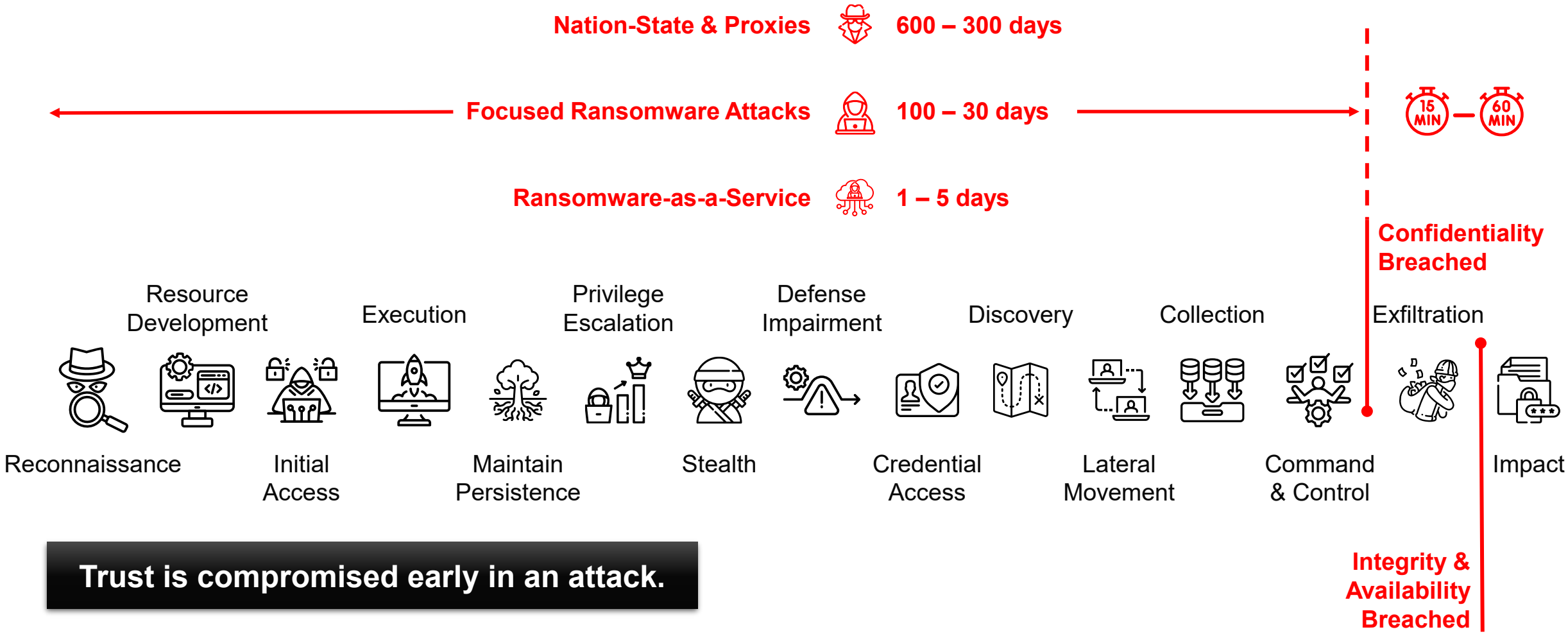
Most aren't prepared

Insufficient plans and testing; no line of sight for what happens during an attack

© 2026 Cohesity Inc. All rights reserved.

What really happens during a Ransomware / Wiper attack?

MITRE ATT&CK: 15 stages or tactics



Trust is compromised early in an attack.

Data is encrypted or wiped at the end of an attack.

© 2026 Cohesity Inc. All rights reserved.

Cyber Incident Impacts

Common Ransomware / Wiper Responses

CISO

Cyber Incident

Data Theft

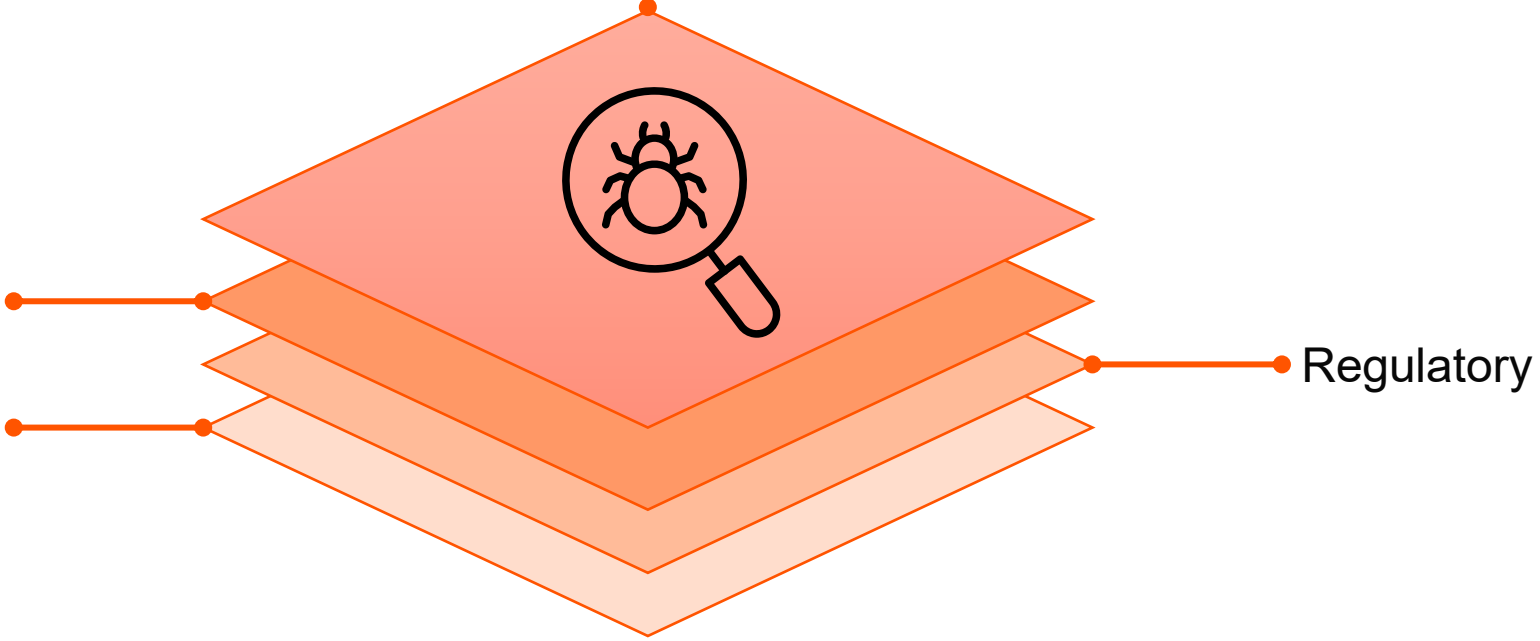
Loss of Trust

Operational

CIO/CTO

BC/DR

System Down
Data Loss



Legal

Reputational

Regulatory

© 2026 Cohesity Inc. All rights reserved.

BCDR vs Cyber Incident Response Timelines

Business Continuity & Disaster Recovery



Cyber Response & Recover

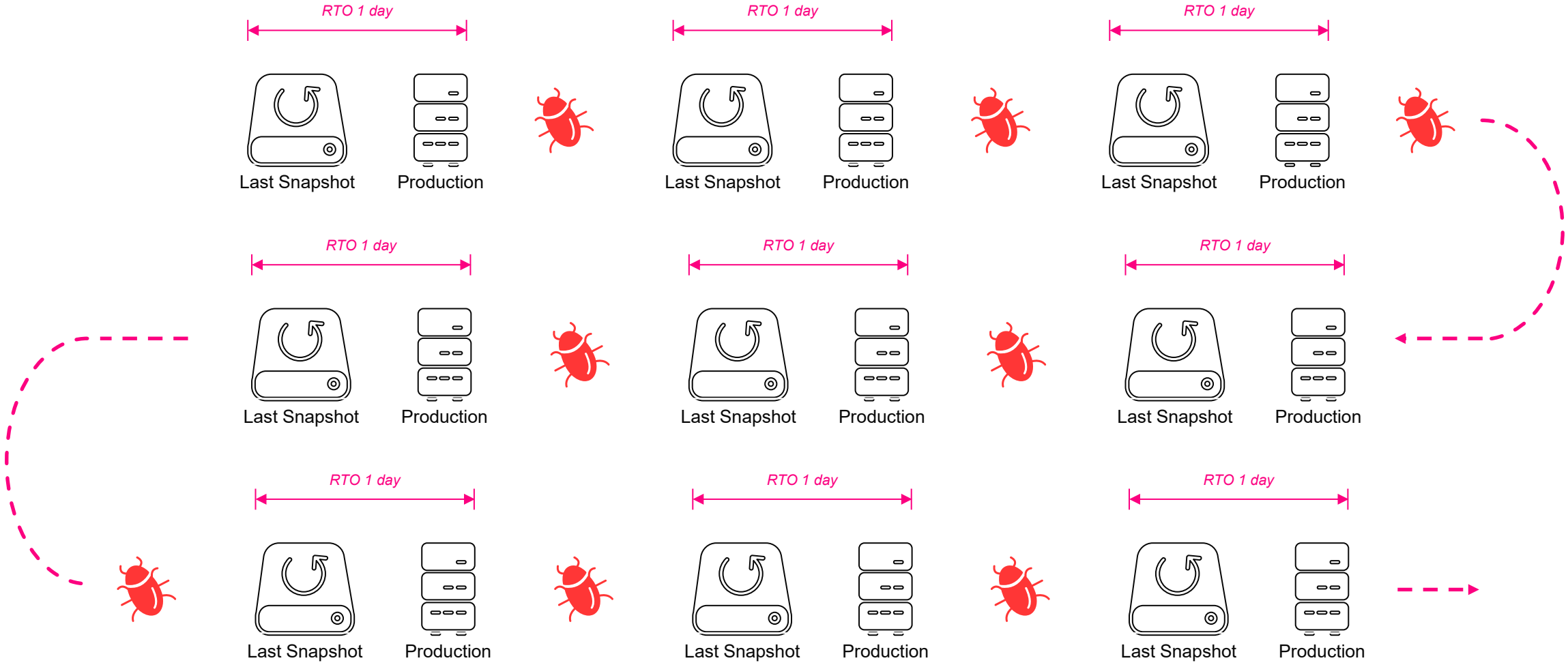




Cyber Resiliency Require Re-Establishing Trust

© 2026 Cohesity Inc. All rights reserved.

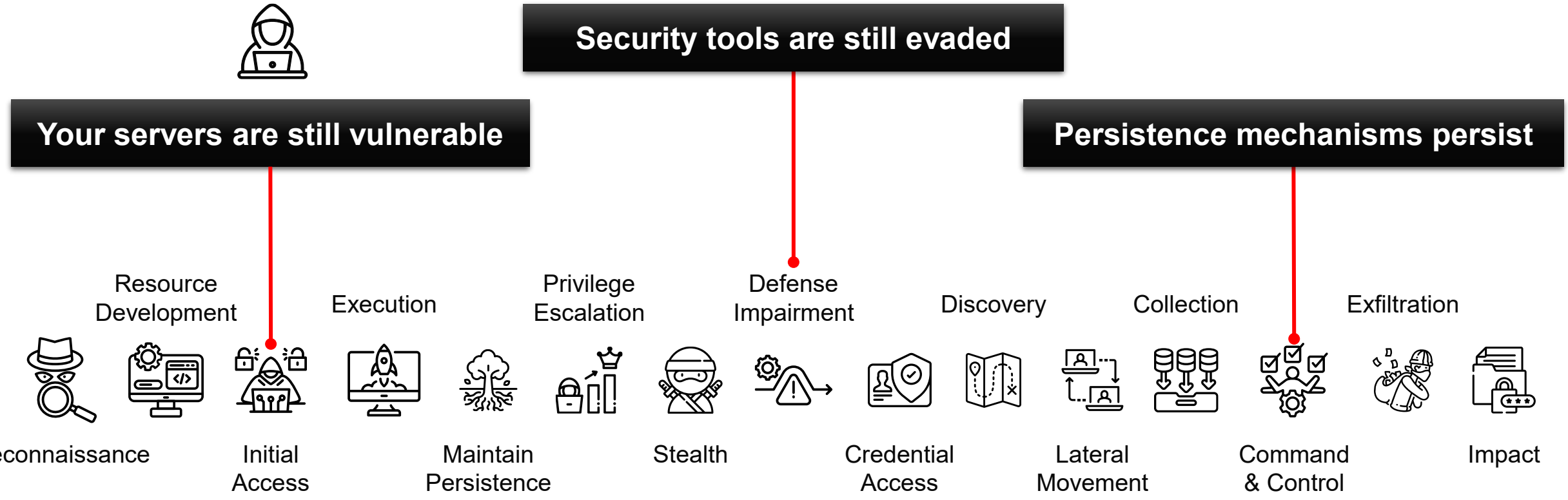
Cyber Recovery with a classic BC/DR approach



© 2026 Cohesity Inc. All rights reserved.

The Effect of Restoring without investigation and mitigation

MITRE ATT&CK: 15 stages or tactics



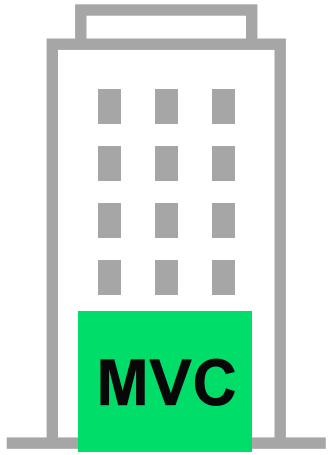
© 2026 Cohesity Inc. All rights reserved.

Cohesity 5 steps of cyber resilience©

1 Data protection & identity resilience	2 Cyber vaulting	3 Threat protection	4 Cyber recovery orchestration	5 Data & AI security posture management
Discover and protect all data Cohesity DataProtect Cohesity NetBackup Cohesity Identity Resilience	**Ensure data is always recoverable** Cohesity FortKnox Cohesity NetBackup IRE	**Detect and investigate threats** Threat Protection	**Practice application resilience** RecoveryAgent	**Optimize data risk posture** Cohesity DSPM Cohesity Data Classification
• On-prem • Cloud • BaaS • IAM	• Platform Security • Immutability & WORM • Cyber Vault	• Anomaly & Threat Detection • Threat Hunting • SIEM Integration	• Clean Room • Recovery Orchestration • CERT	• Data Classification • DSPM

© 2026 Cohesity Inc. All rights reserved.

Prepare: define your Minimum Viable Company quickly



Identify
critical services

Protect
recovery assets

Establish
trusted foundation

Restore
to a clean room

Prove
viability

COHESITY © 2026 Cohesity Inc. All rights reserved.

Prepare: Ensure access to critical resources and trusted tooling in minutes

Cohesity Digital Jump Bag keeps the required resources beyond the reach of attackers and provides rapid access to the response team after an incident



- Networking
- Security & IT Tooling
- Stakeholder Contact List
- Cyber Insurance Policy
- Voice-over-IP
- Incident Playbooks
- DNS
- Contracts with MSP or Retained Incident Response
- Email
- Logical Access Control
- Physical Access Control

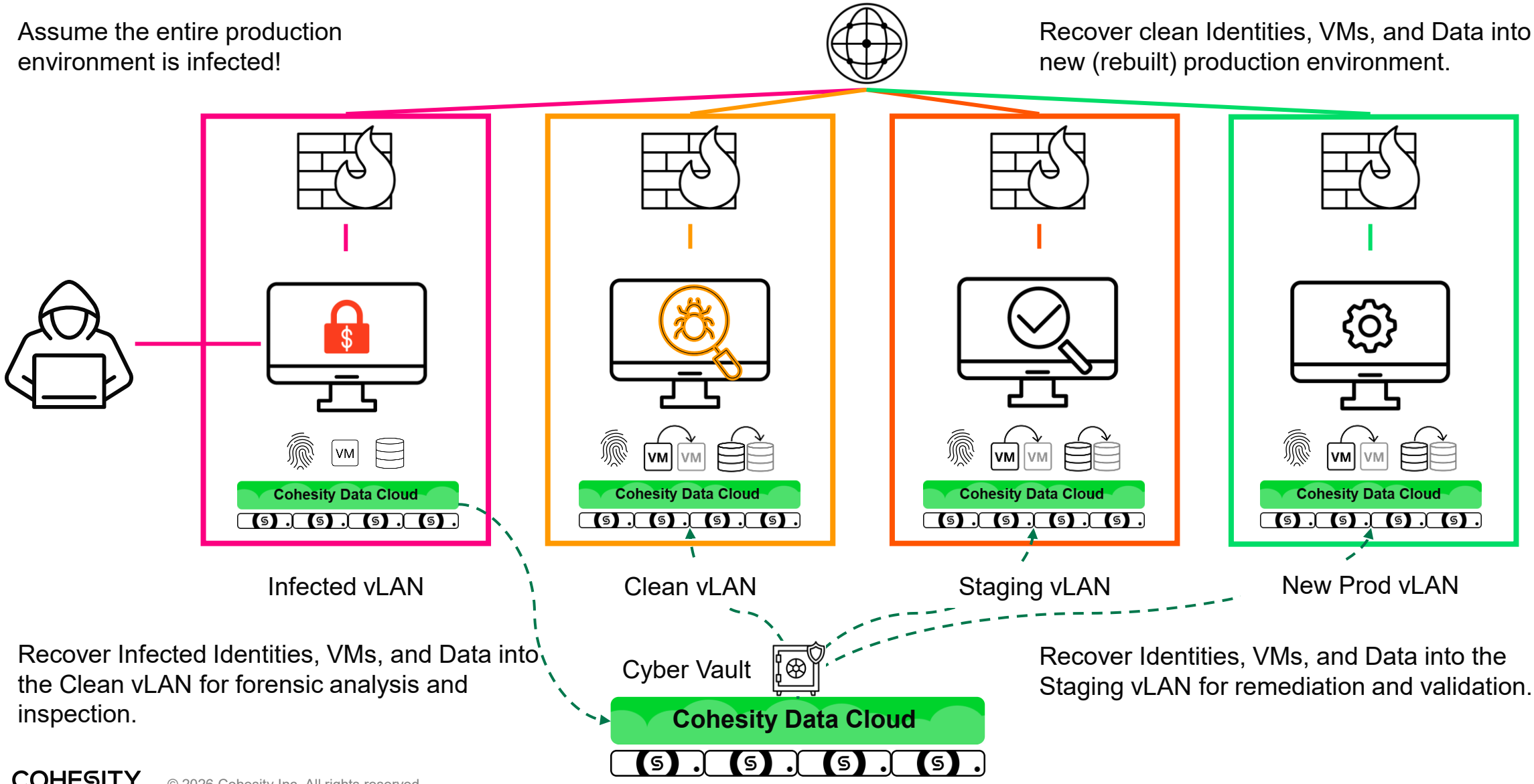
COHESITY © 2026 Cohesity Inc. All rights reserved.

Prepare A Clean Room Architecture

to drive the Cyber Incident Response and Recovery Process

Assume the entire production environment is infected!

Recover clean Identities, VMs, and Data into the new (rebuilt) production environment.



Recover Infected Identities, VMs, and Data into the Clean vLAN for forensic analysis and inspection.

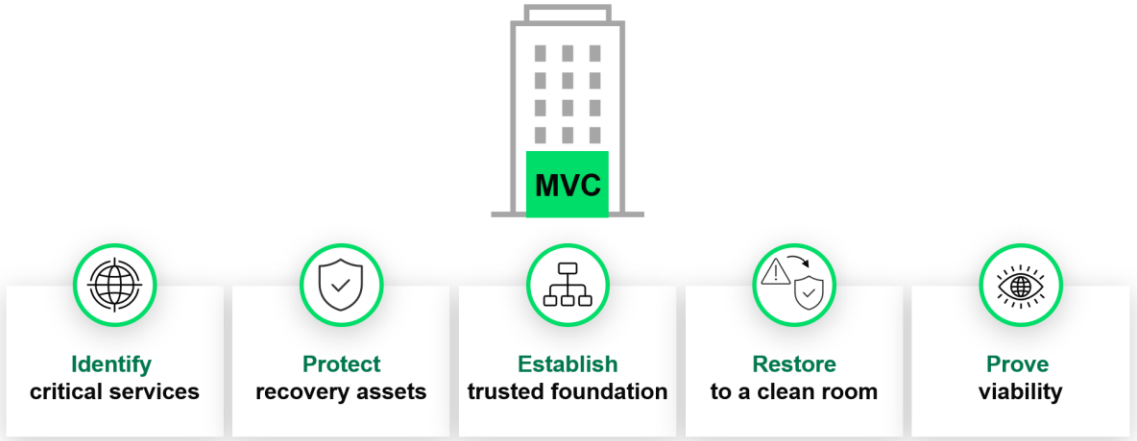
Recover Identities, VMs, and Data into the Staging vLAN for remediation and validation.

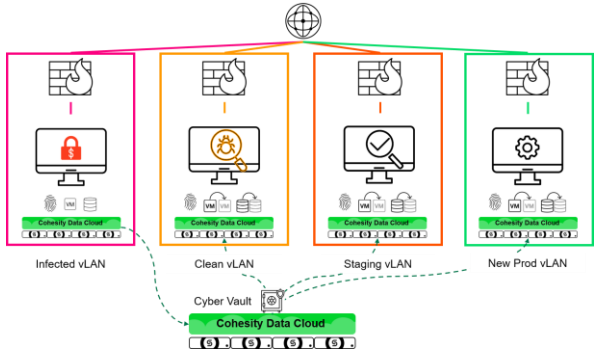
© 2026 Cohesity Inc. All rights reserved.

Minimum Viable Company, Digital Jump Bag and Clean Room

Building the Operational Framework for Trusted Cyber Recovery

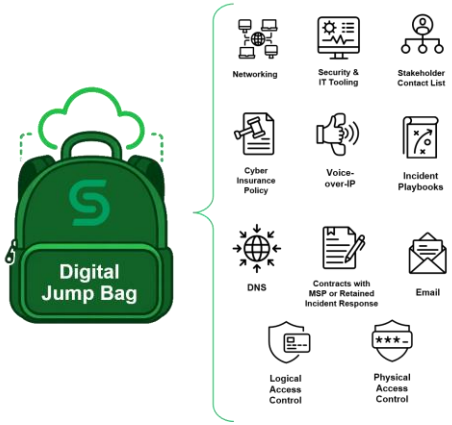
Minimum Viable Company

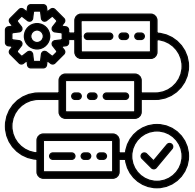




Clean Room Architecture

Digital Jump Bag Contents

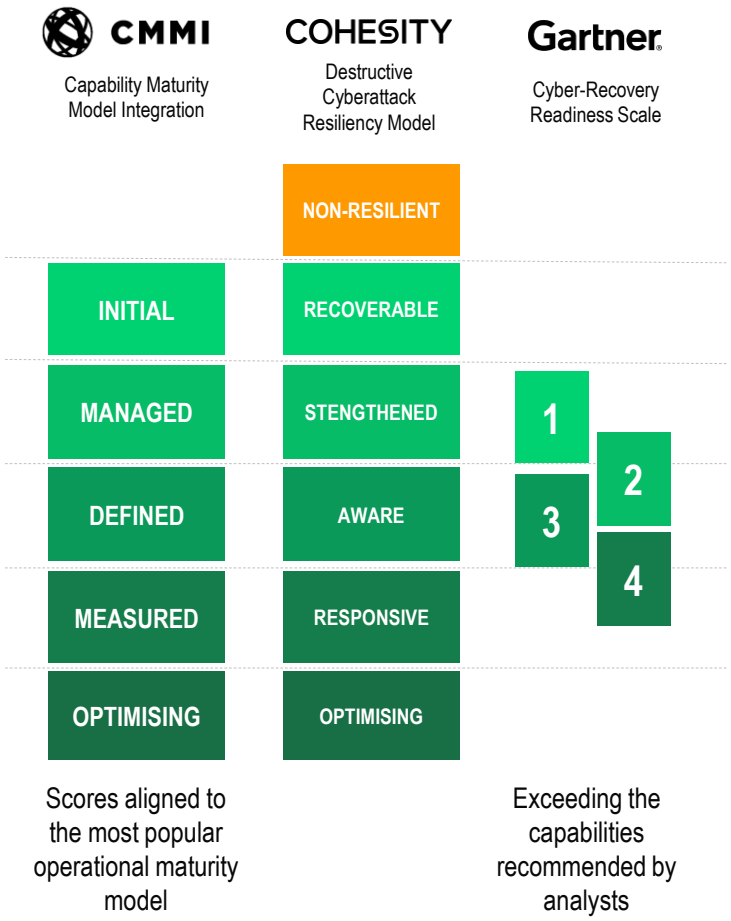


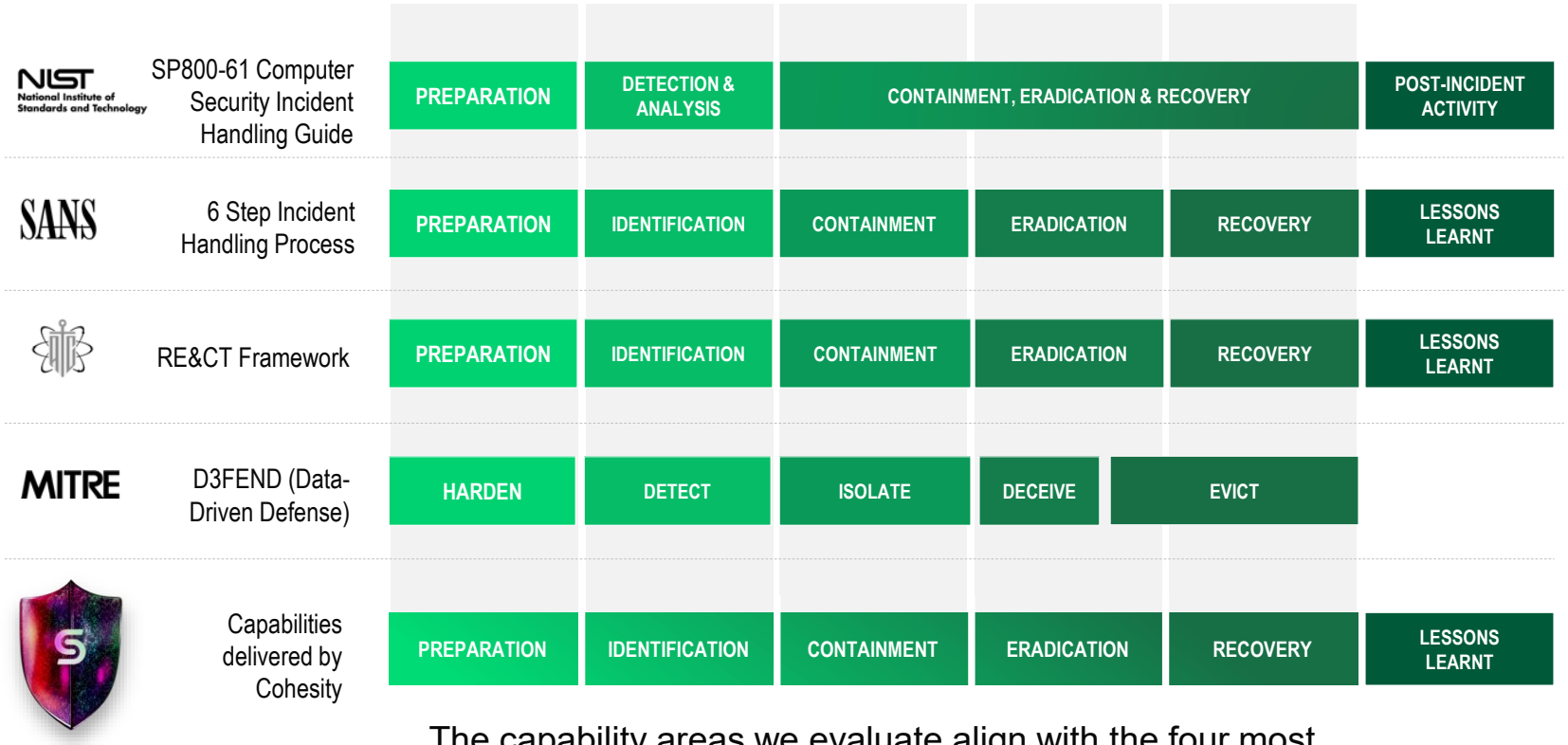


Required Workflows, RACI, and Orchestration Automation

© 2026 Cohesity Inc. All rights reserved.

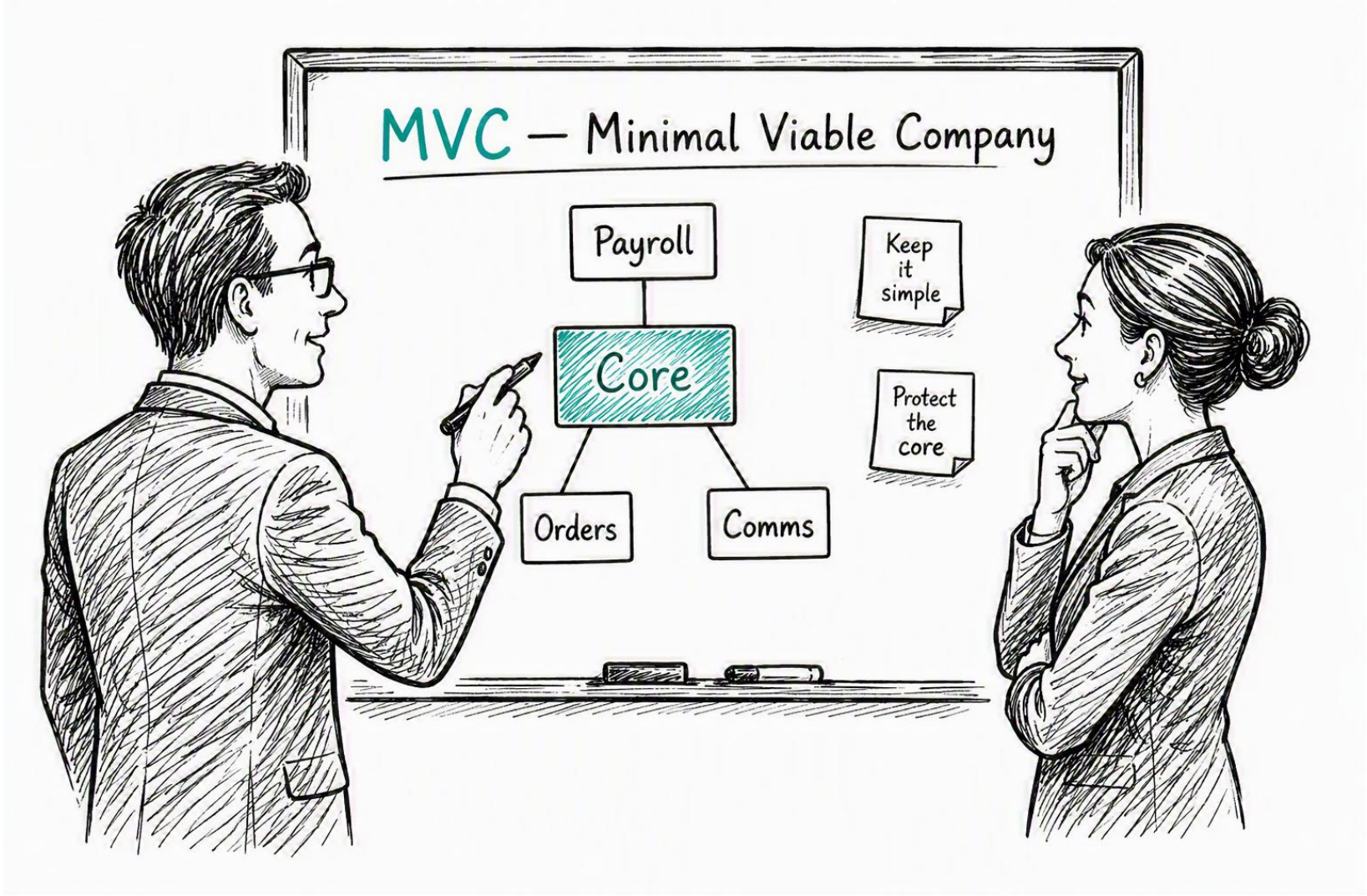
Comprehensive Cyber Resiliency



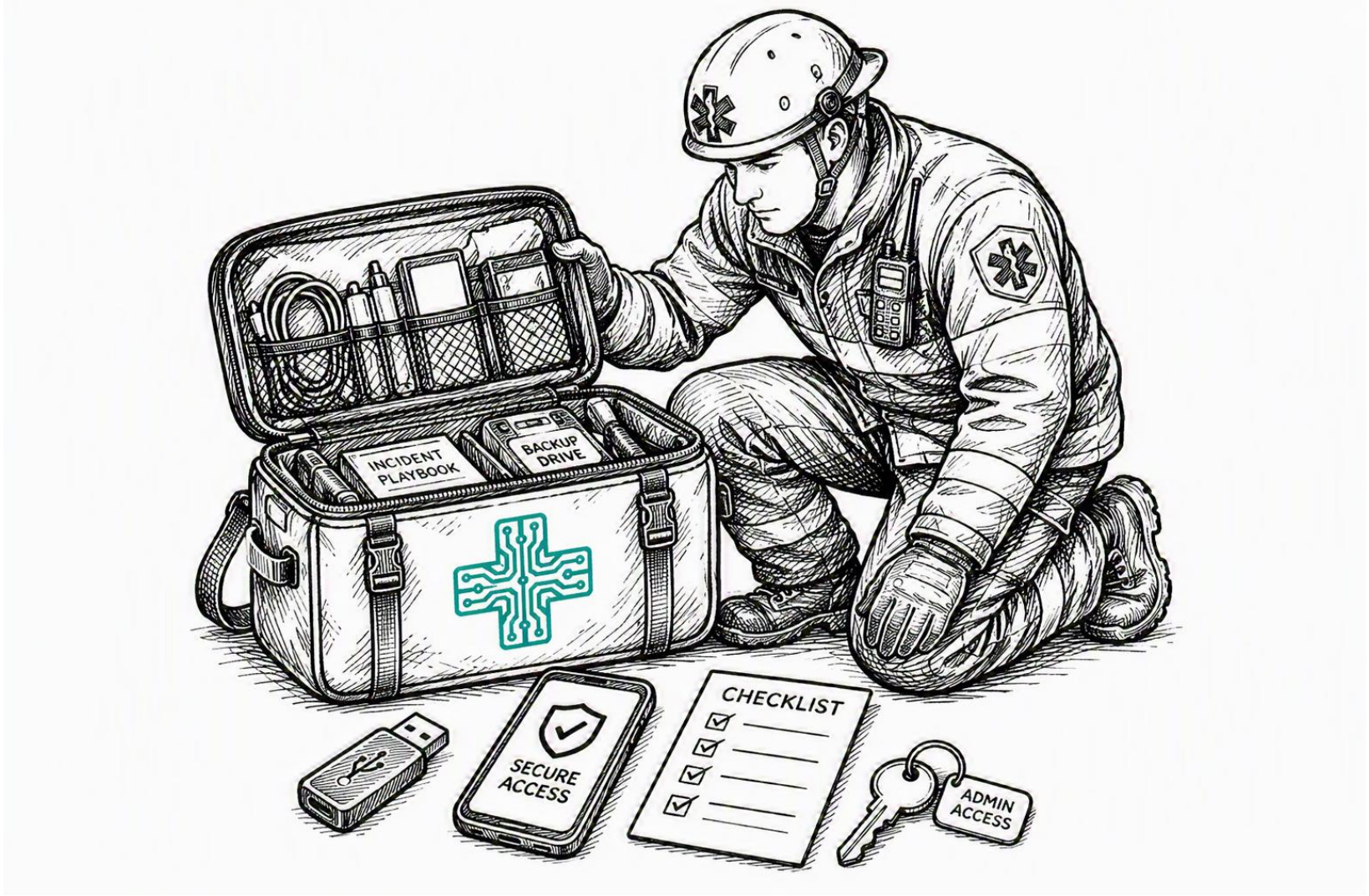


The capability areas we evaluate align with the four most popular cyber incident response and recovery frameworks

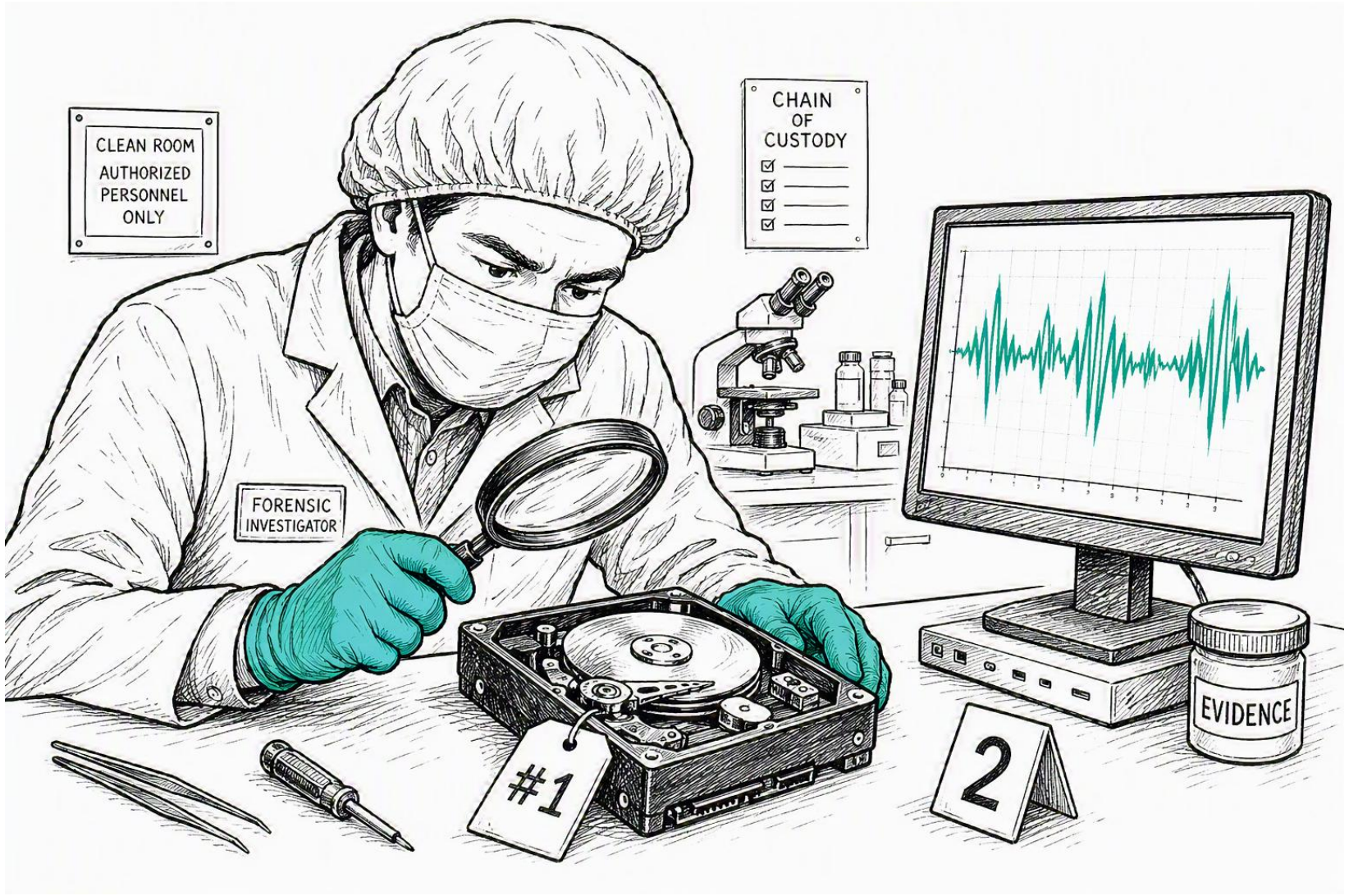
© 2026 Cohesity Inc. All rights reserved.



COHESITY © 2026 Cohesity Inc. All rights reserved.



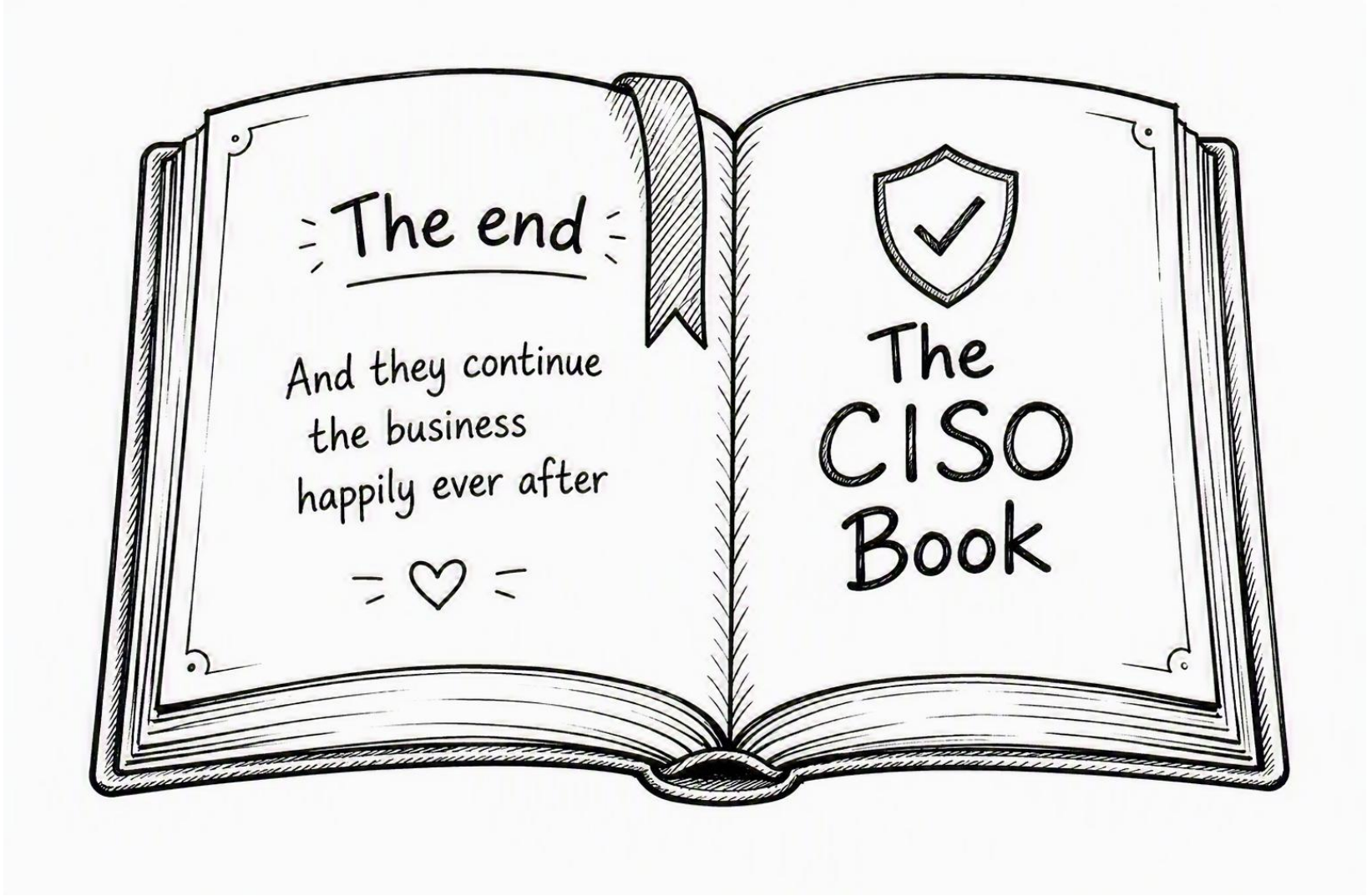
© 2026 Cohesity Inc. All rights reserved.



© 2026 Cohesity Inc. All rights reserved.



© 2026 Cohesity Inc. All rights reserved.



COHESITY © 2026 Cohesity Inc. All rights reserved.

Thank You!

petter.sveum@cohesity.com

COHESITY

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, the Helios logo, DataGovern, SiteContinuity, DataHawk, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.