COHESITY

COHESITY

Ismo Puuronen – Sr. Sales Engineer
2026 - March

Our Mission:

To protect, secure & provide insights into the world's data.

Data Protection

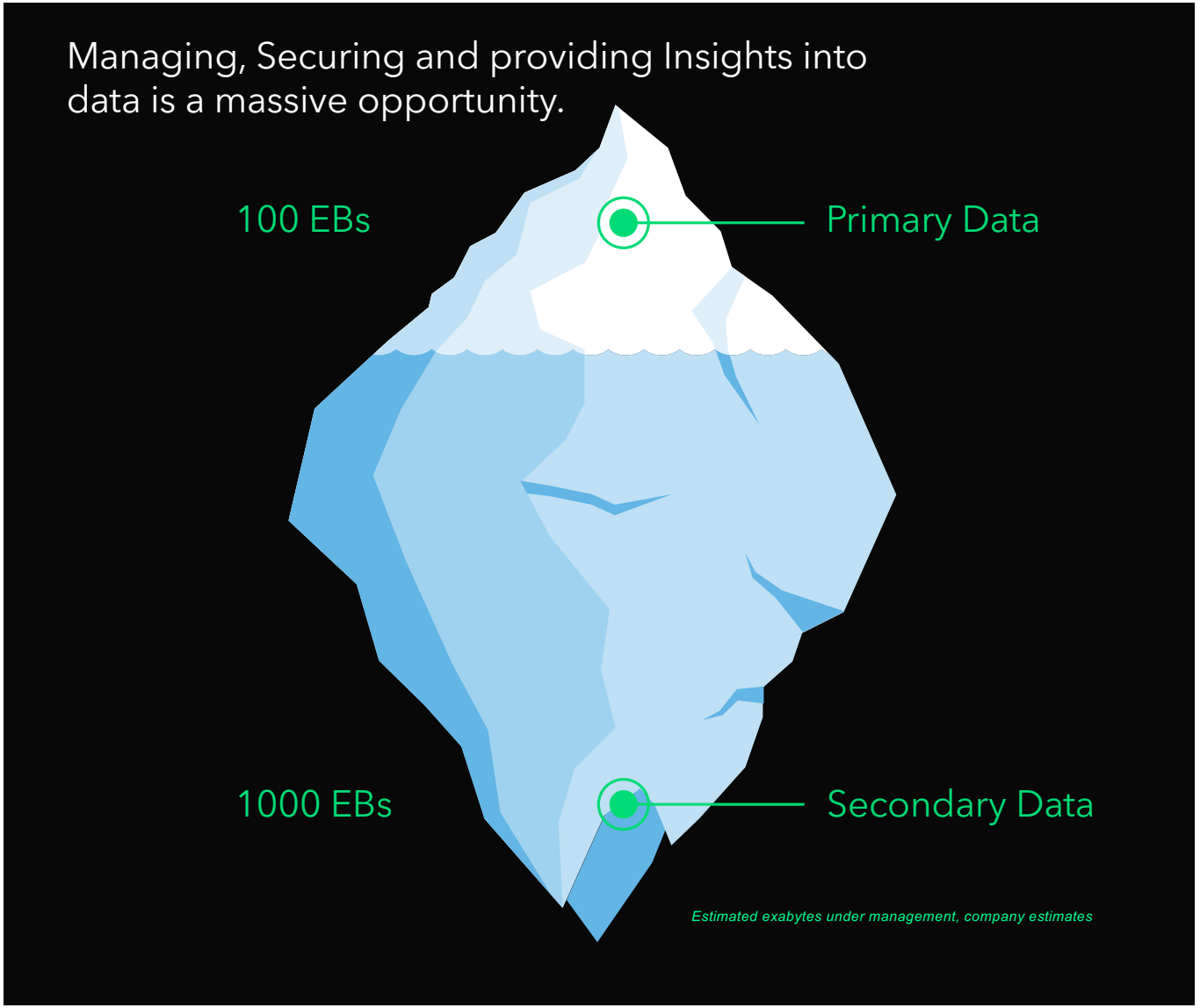
- Broad Workloads
- Enterprise Scale
- Flexible Consumption

Data Security

- Threat Detection
- Posture Management
- Cyber Recovery

Data Insights

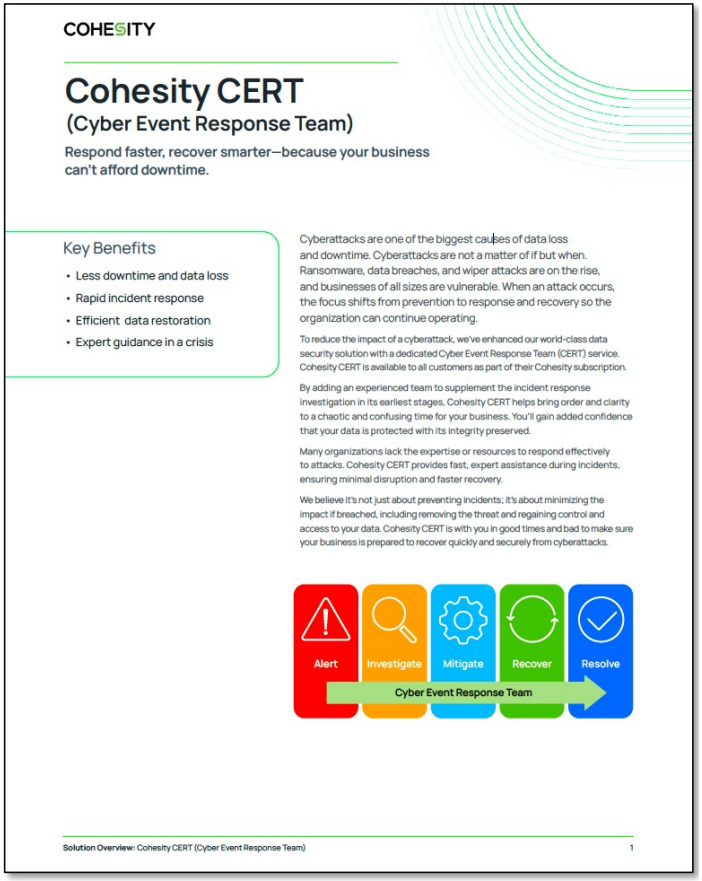
- GenAI Engine
- Search & Analytics
- Operational Insights



Cohesity – Cyber Event Response Team

https://www.cohesity.com/support/cyber-events-response-team/

- **CERT** is always part of the support.
- **Rapid Ransomware Response** – Expert assistance from Cohesity to quickly assess, contain, and recover from cyberattacks using immutable snapshots and clean backups.
- **Forensic Analysis & Guidance** – Help identifying the scope of impact, validating clean recovery points, and providing best practices for secure restore.
- **Minimized Downtime & Risk** – Accelerated recovery workflows and close coordination with your IT/security teams to reduce business disruption



COHESITY

Cohesity CERT

(Cyber Event Response Team)

Respond faster, recover smarter—because your business can't afford downtime.

Key Benefits

- Less downtime and data loss
- Rapid incident response
- Efficient data restoration
- Expert guidance in a crisis

Cyberattacks are one of the biggest causes of data loss and downtime. Cyberattacks are not a matter of if but when. Ransomware, data breaches, and wiper attacks are on the rise, and businesses of all sizes are vulnerable. When an attack occurs, the focus shifts from prevention to response and recovery so the organization can continue operating.

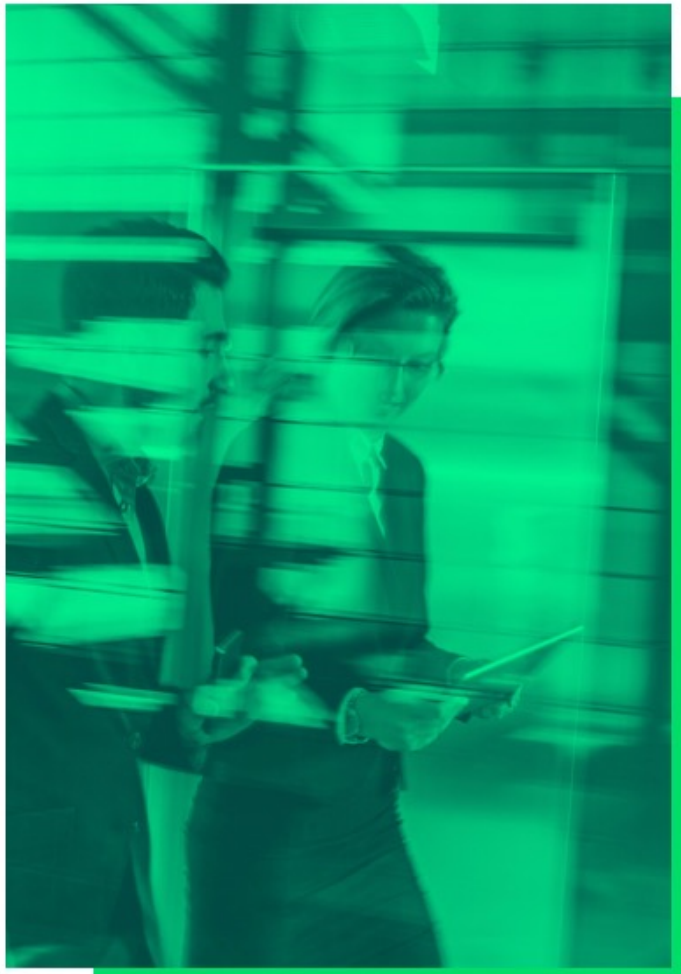
To reduce the impact of a cyberattack, we've enhanced our world-class data security solution with a dedicated Cyber Event Response Team (CERT) service. Cohesity CERT is available to all customers as part of their Cohesity subscription.

By adding an experienced team to supplement the incident response investigation in its earliest stages, Cohesity CERT helps bring order and clarity to a chaotic and confusing time for your business. You'll gain added confidence that your data is protected with its integrity preserved.

Many organizations lack the expertise or resources to respond effectively to attacks. Cohesity CERT provides fast, expert assistance during incidents, ensuring minimal disruption and faster recovery.

We believe it's not just about preventing incidents; it's about minimizing the impact if breached, including removing the threat and regaining control and access to your data. Cohesity CERT is with you in good times and bad to make sure your business is prepared to recover quickly and securely from cyberattacks.

Solution Overview: Cohesity CERT (Cyber Event Response Team) 1



The leading brands in enterprise and public sector rely on us

~70%

OF THE GLOBAL 500

10/10
Top Financial Services Companies

10/10
Top Manufacturing Companies

9/10
Top Technology Companies

8/10
Top Healthcare Companies

8/10
Top Retail Companies

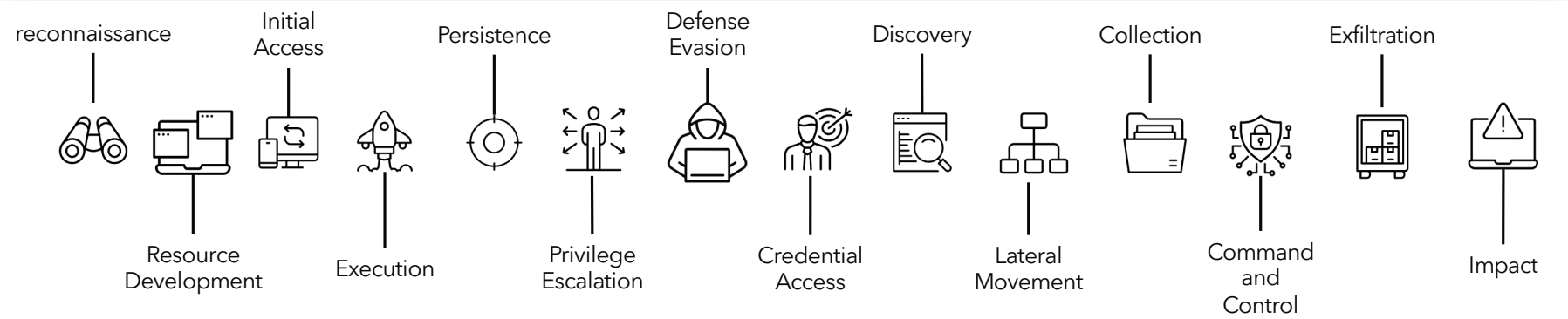
7/10
Top Energy Companies

The leading brands in enterprise and public sector rely on us

Federal/SLED

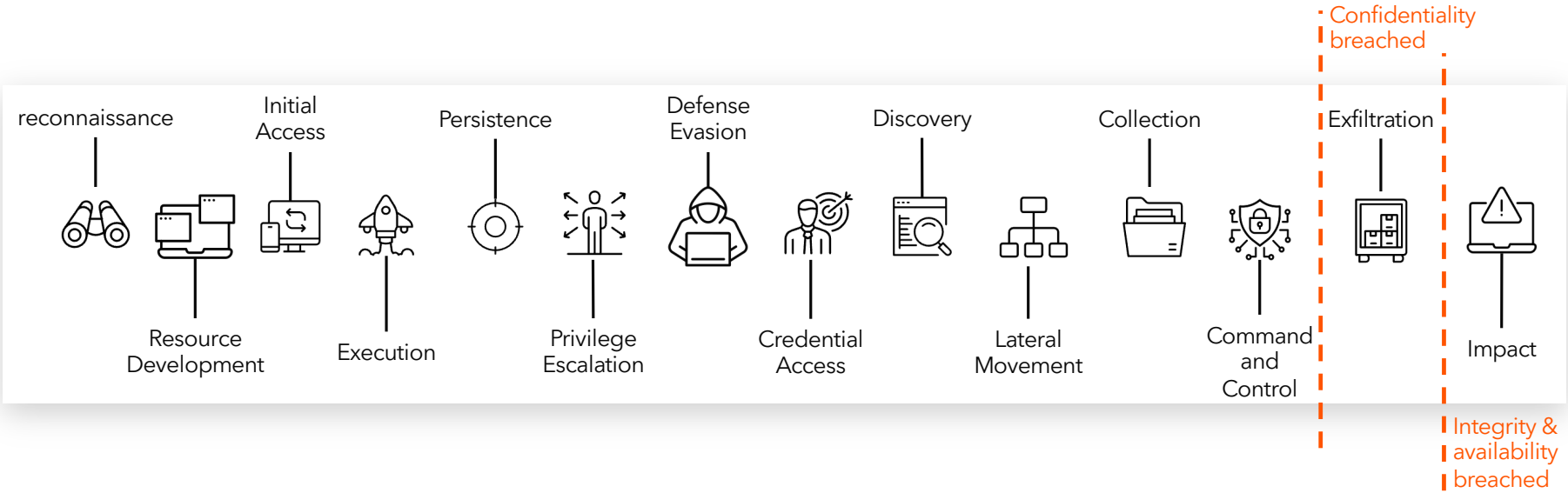
MITRE ATT&CK

- Globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
- 14 “tactics” or stages the attacker goes through to steal and encrypt or wiper your data.
- Over 300 different “techniques” available to team to achieve each outcome

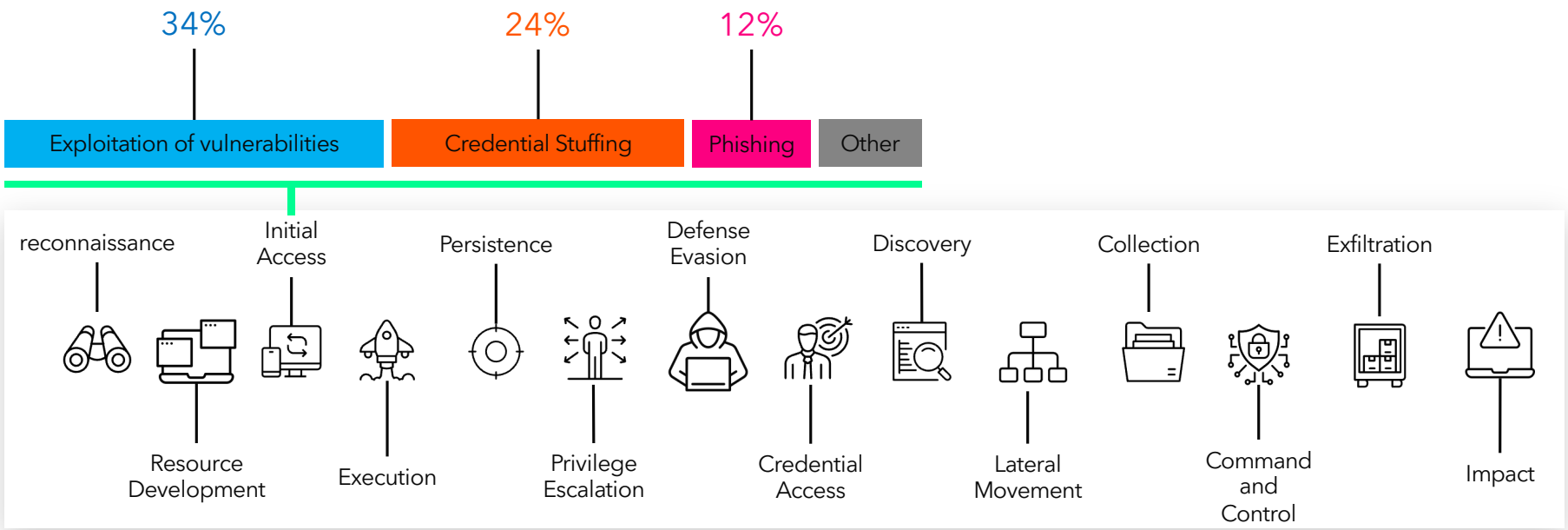


When damage is done

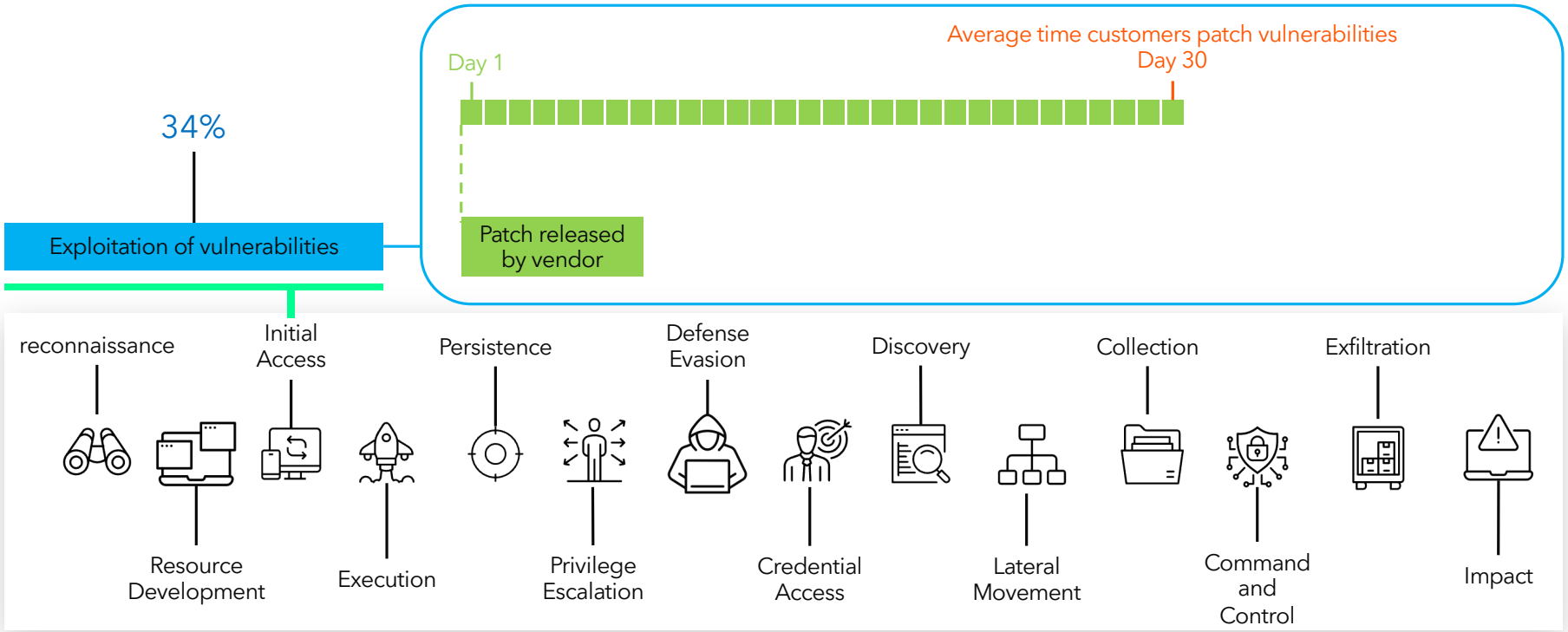
- It is only in the last two tactics that there is impact



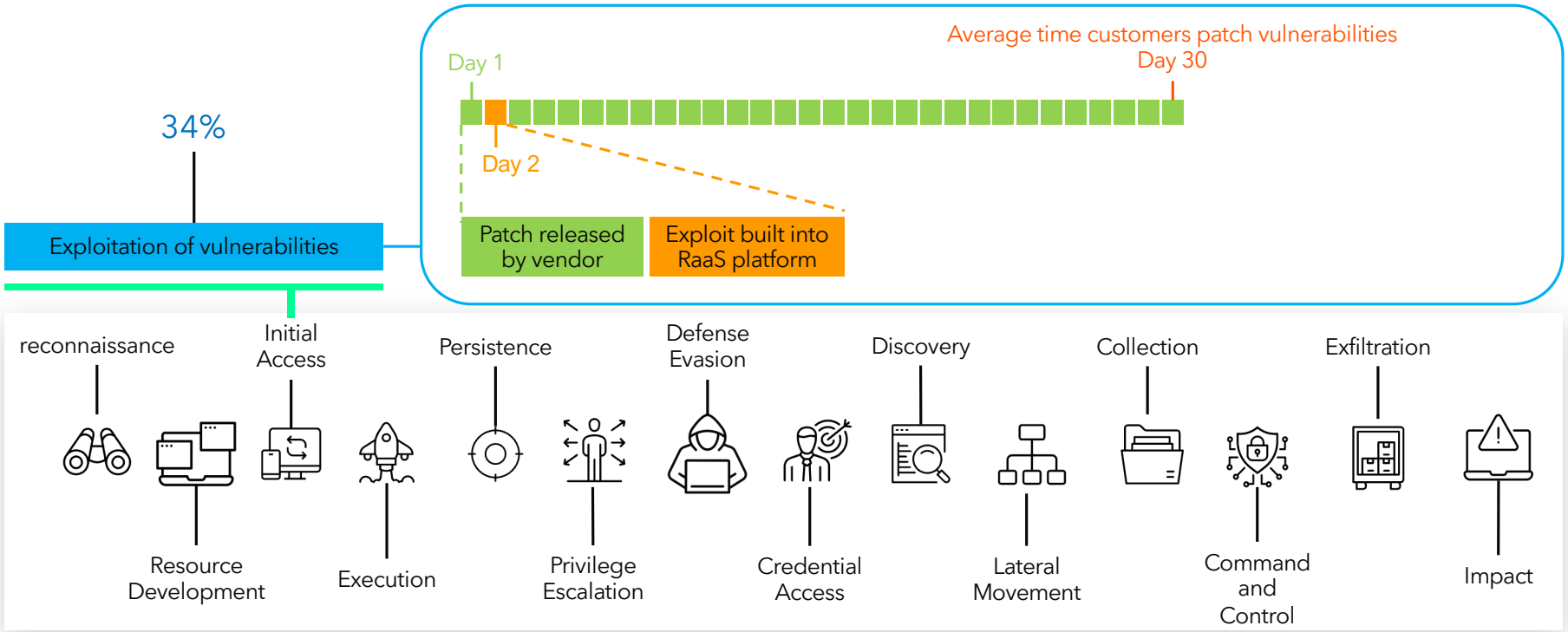
Vulnerability exploitation is most common way into organizations



…and the pace of weaponization is increasing



…and the pace of weaponization is increasing



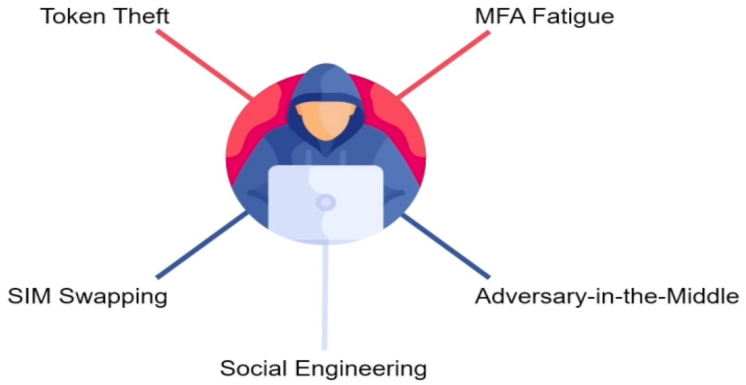
AD / IDP under siege

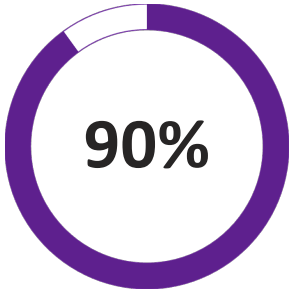
What does Active Directory do?

Handles the **4 A's** of IAM
(Identity and Access Management)

- ✓ **Authentication**: Who you are
- ✓ **Authorization**: What you're allowed to access
- ✓ **Account:** management
- ✓ **Audit**: Proving who did what (sign-in logs, etc.)

AD / IDP under siege





Incident Response Cases

IR engagements that involve Active Directory compromise (Mandiant Consulting)

Jaguar Land Rover

Sep 25, 2025

When the Hack Hits the Boardroom: How Jaguar Land Rover's Cyber Crisis Becomes a C-Suite Test

By: Zenia Pearl V. Nicolas

Jaguar Land Rover's Midnight Cyberattack

At 2:07 a.m., the phone rings. On the other end, the operations chief's voice is tight: *"The lines are down. Systems are locked. We can't ship tomorrow."*

For Jaguar Land Rover (JLR), this was not a simulation — it was reality. Following a 31 August 2025 cyberattack, the company confirmed its production halt would last *"until 1 October"* (Reuters, 2025a). In its statement, JLR explained: *"We have made this decision to give clarity for the coming week as we build the timeline for the phased restart of our operations and continue our investigation"* (Reuters, 2025a).

The Guardian added that JLR teams were *"working around the clock alongside cybersecurity specialists, the NCSC, and law enforcement"* to contain the breach (The Guardian, 2025a).

- **Attack was disclosed early September 2025 -> JLR did not produce single vehicle for 5 weeks.**
- **Phased restart of production in October, normal operations mid-November**
- **JLR initially stated there was no evidence of customer data theft, it later admitted that some internal data might have been affected.**

Jaguar Land Rover

How Did Attackers Breach JLR?

Jaguar Land Rover has not released a comprehensive technical post-mortem of the September 2025 breach; however, security researchers and leaked information from the attackers themselves provide a clear picture.

The **JLR breach breakdown** reveals that the intrusion was not the result of a sophisticated zero-day exploit, but rather the execution of well-known tactics: social engineering, credential abuse, weak segmentation, and inadequate detection.

Lateral Movement and System Sabotage

After breaching the perimeter, attackers expanded their access through **lateral movement**. They escalated privileges, navigated through JLR's IT environment, and eventually reached core infrastructure. Reports indicate that once entrenched, they deployed ransomware or destructive malware, crippling servers and halting factory operations.

The fact that JLR felt forced to **disconnect entire systems worldwide**, from dealer platforms to factory lines, demonstrates how deeply attackers had penetrated. Instead of isolating a compromised segment, JLR had to hit the emergency brake across its global operations.

COHESITY

Jaguar Land Rover

Insufficient Network Segmentation

The scale of disruption also points to a lack of **network segmentation**. As a modern automaker, JLR had tightly integrated IT systems with factory automation and logistics. This "everything connected" model maximizes efficiency but leaves no firebreaks against cyberattacks.

Once attackers infiltrated corporate IT, they could potentially pivot toward operational systems, forcing JLR to shut down plants worldwide as a precaution. In a properly segmented environment, breaches in one area should not cascade into total production stoppages.

Lack of Monitoring and Anomaly Detection

The attackers were able to **exfiltrate massive volumes of data**, in one case, an additional 350 GB dump, without immediate detection. This highlights a failure of monitoring and anomaly detection. Abnormal behaviors such as:

- A single user account retrieving hundreds of gigabytes of records,
- connections tunneling data through Tor,
- or sudden traffic spikes from unusual IP ranges,

COHESITY

Jaguar Land Rover

- JLR – virallista vahvistusta ei ole, mutta merkit viittaavat vahvasti siihen, että indetity provider oli joutunut hyökkäyksen kohteeksi:
  - Pääsy:
    - IT-ympäristöihin
    - Tuotantoympäristöihin
    - Applikaatioihin

- Hyökkäystapa viittaa muutamaan ryhmään, nämä ryhmät ovat tunnettuja siitä, että he hyödyntävät:
  - Indentity-based intrusions (not exploits)
  - Social engineering + credential theft
  - Targeting SSO / IAM systems
  - Steal credentials / session tokens
  - Bypass MFA
  - Take over cloud identity (Entra ID / Okta)
  - Pivot into on-prem AD

JPM

JP Morgan Chase Data Breach Explained: What Happened?

The JP Morgan Chase data breach was discovered in May 2025, exposing sensitive customer data, including personally identifiable information (PII) and account details. Initial evidence suggests the breach stemmed from a phishing attack that escalated into unauthorized access to critical systems. While not confirmed, some speculate it may tie into a broader, coordinated campaign targeting financial institutions.

When did the JP Morgan Chase Data Breach happen?

The breach was identified on May 15, 2025, but investigations suggest the compromise began as early as April 2025, giving attackers extensive time to access sensitive systems before detection.

Who hacked JP Morgan Chase?

The identities and motivations behind the JP Morgan Chase data breach remain unknown. Investigators have not attributed the attack to a specific threat actor at this time.

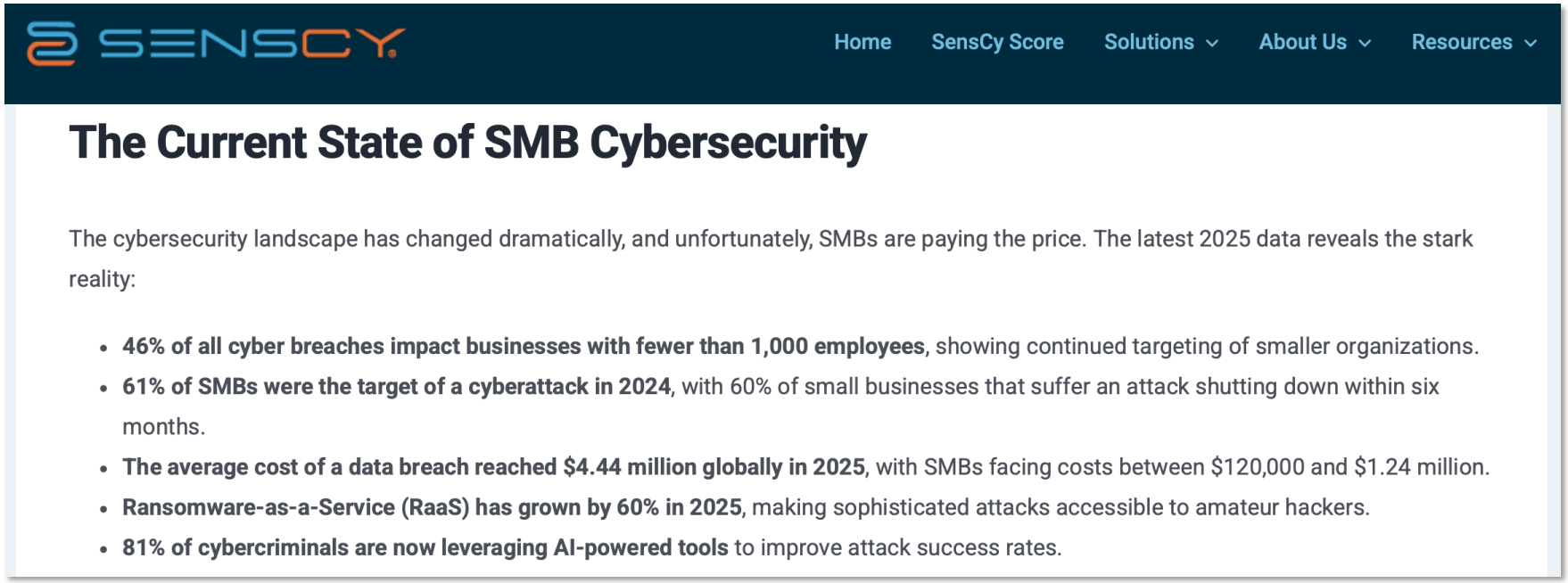
May 2025 – over 25 million customers were affected, compromised data including personal information.

JPMorgan cyberattack hits 76M households

PUBLISHED FRI, OCT 3 2014•1:51 AM EDT | UPDATED FRI, OCT 3 2014•9:41 AM EDT

September - 2014 – Attack was discovered late July, halted middle August - one of the largest in history, affecting 76 million households & 7 million small businesses.

State of Cybersecurity

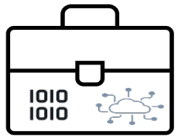


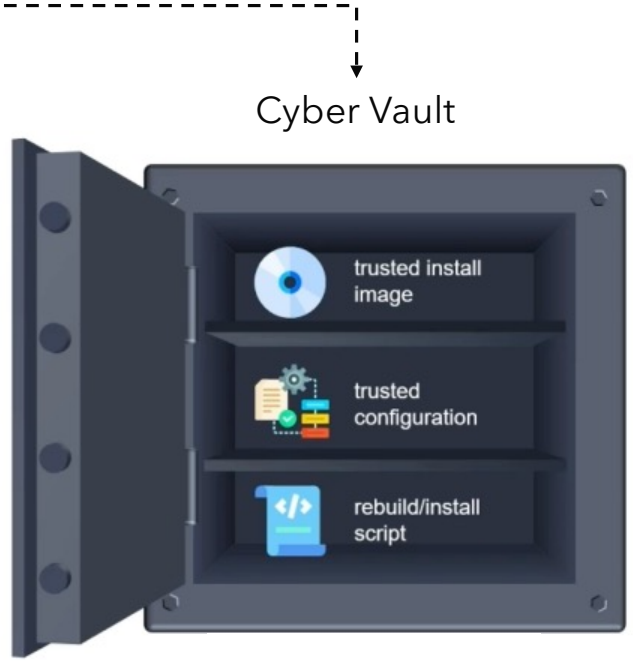
Cyber Resiliency: Bouncing Back!

- Immutable backup
- RTO requirement -> Recover vs rebuild?

- Archive is not Cyber Vault

- **Digital Jump Bag**
  - ISO images
  - Base network configurations
  - Application installers
  - License keys
  - Manuals
  - Contact persons
  - DNS, AD, etc. configs
  - Playbook/Recovery plan
  - …





Summary

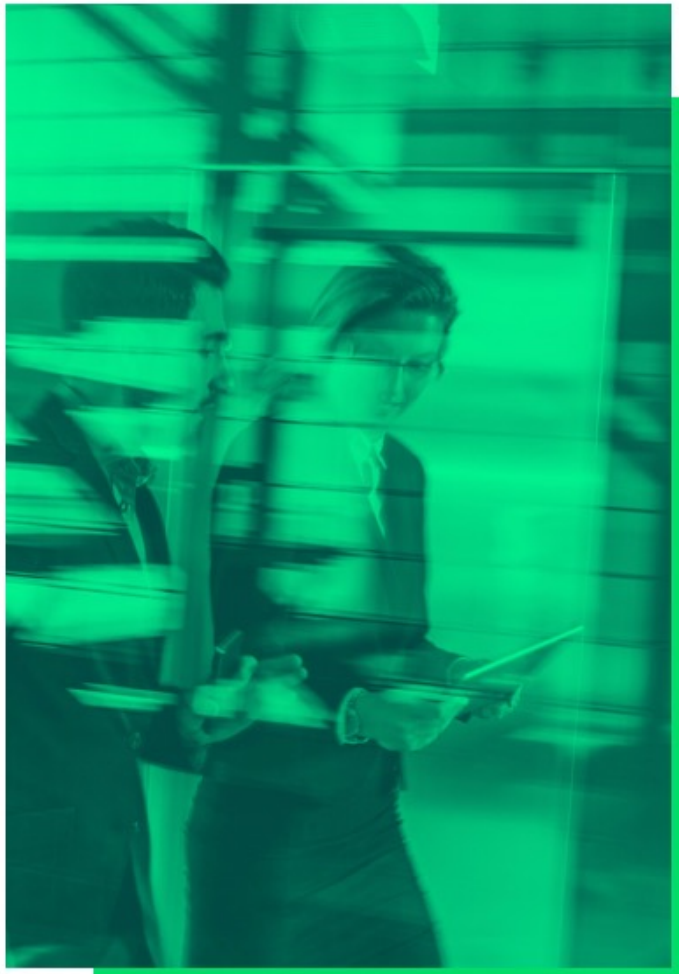
1. **Successful cyber attacks cannot be prevented, even largest corporations with largest security budgets faces them:**
   - Focus on how to bounce back.

2. **AD/IDP compromise is the case in 90% of the time in cyber events:**
   - Make sure to have immutable backups in place regarding your business-critical workloads & applications, including AD & EntraID

3. **Playbook/recovery plan & Digital Jump Bag:**
   - Have them & keep them safe and isolated.

4. **Cyber Vault:**
   - Off-site copy of the critical data, including recovery plan & DJB.

5. **Recover vs Rebuild:**
   - Prepare to rebuild instead recover.



THANK YOU

COHESITY