JUDGMENT Day by Alanata

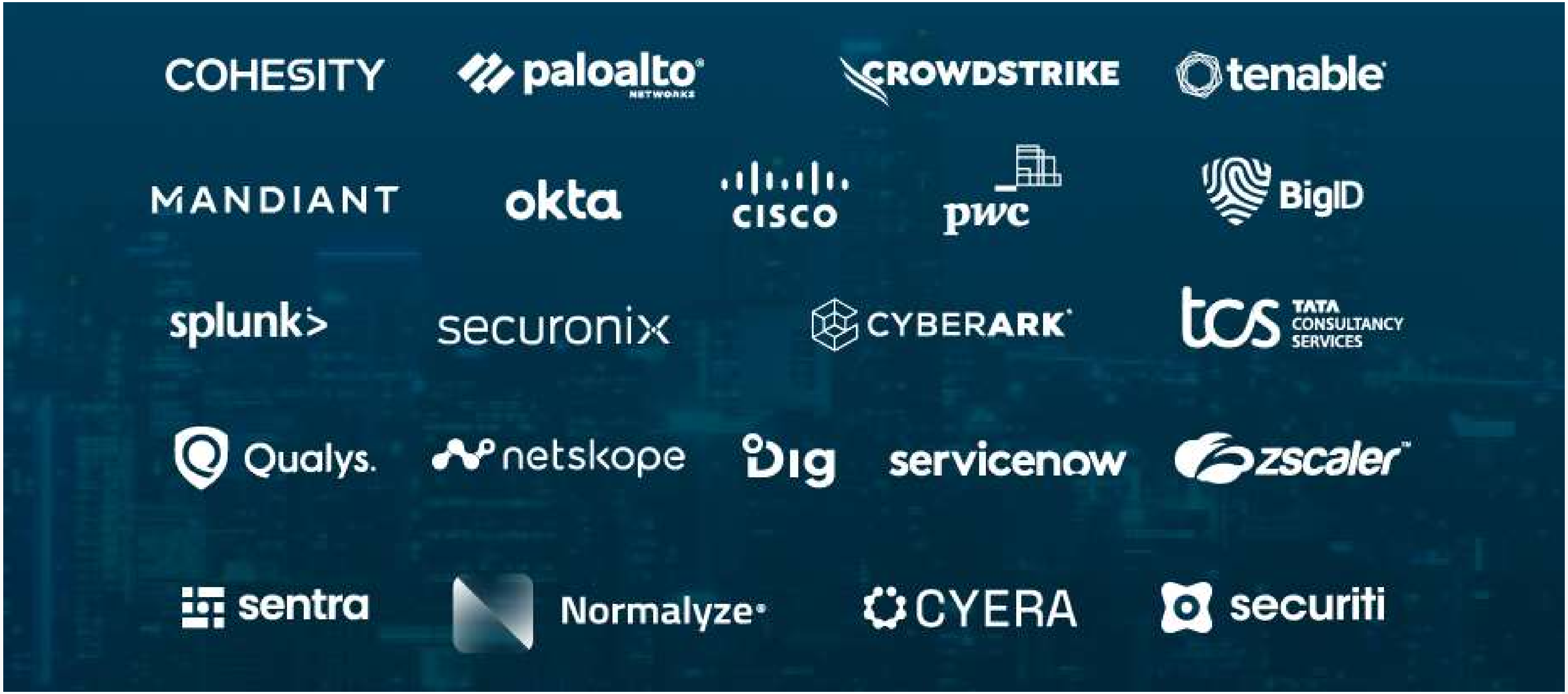
Realita obnovy dát pri kybernetickom útoku

Josef Honc
Senior Principal Sales Engineer

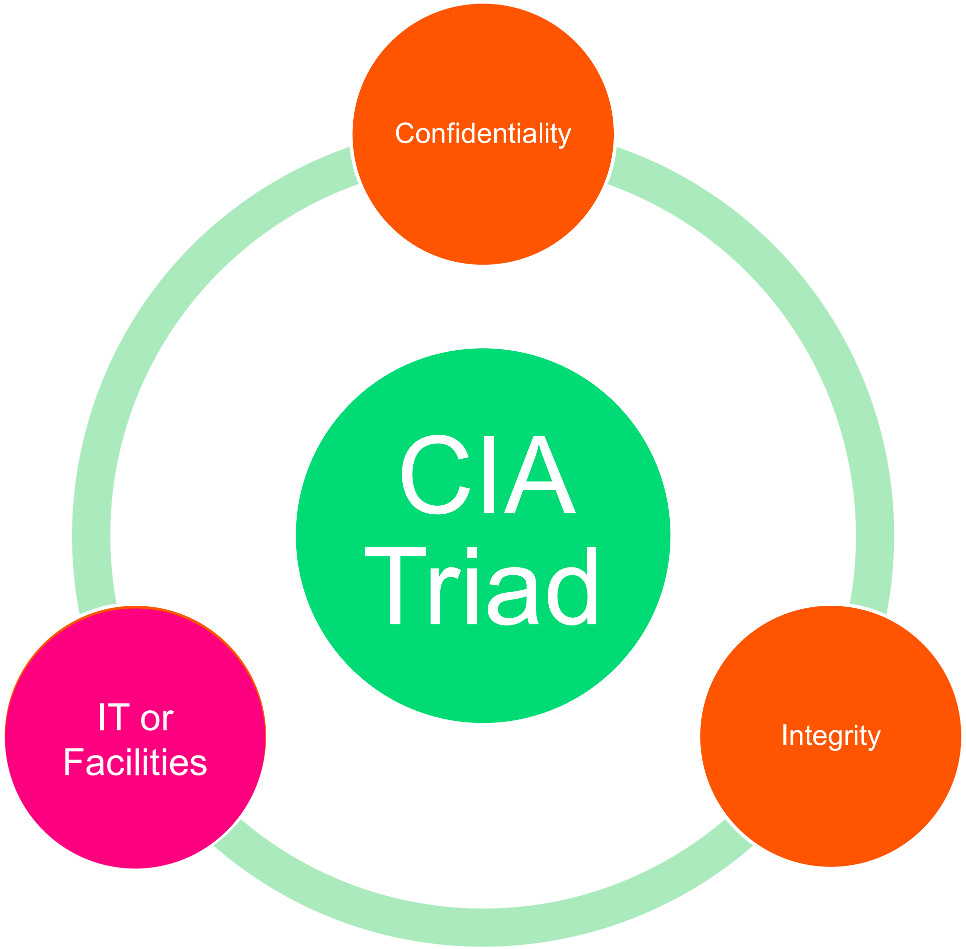
COHESITY

All Roads Pass Through Your Data

The Industry’s ONLY Data Security Alliance

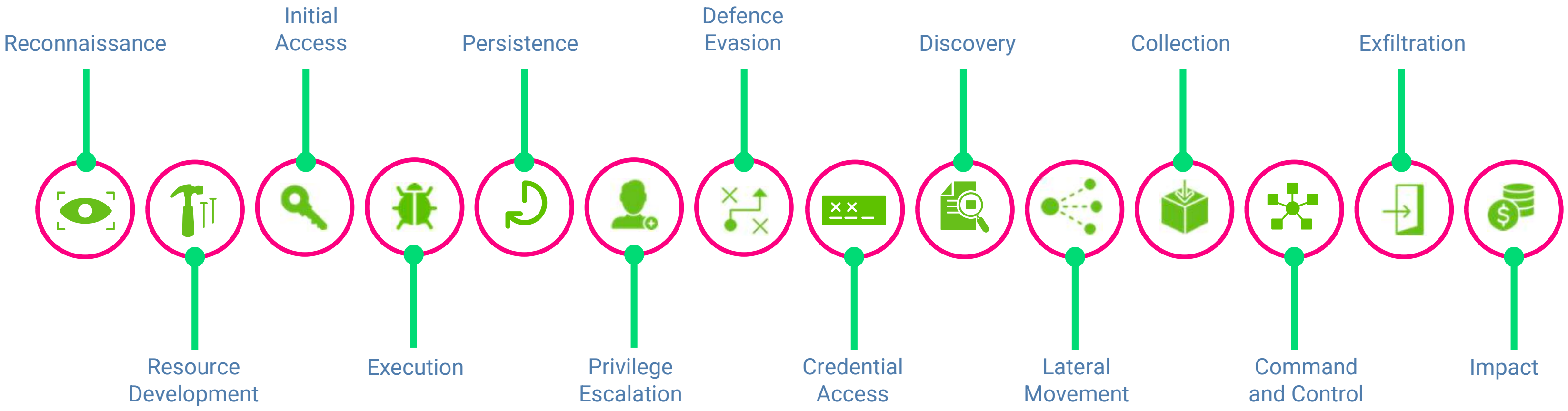


What risks are we managing?



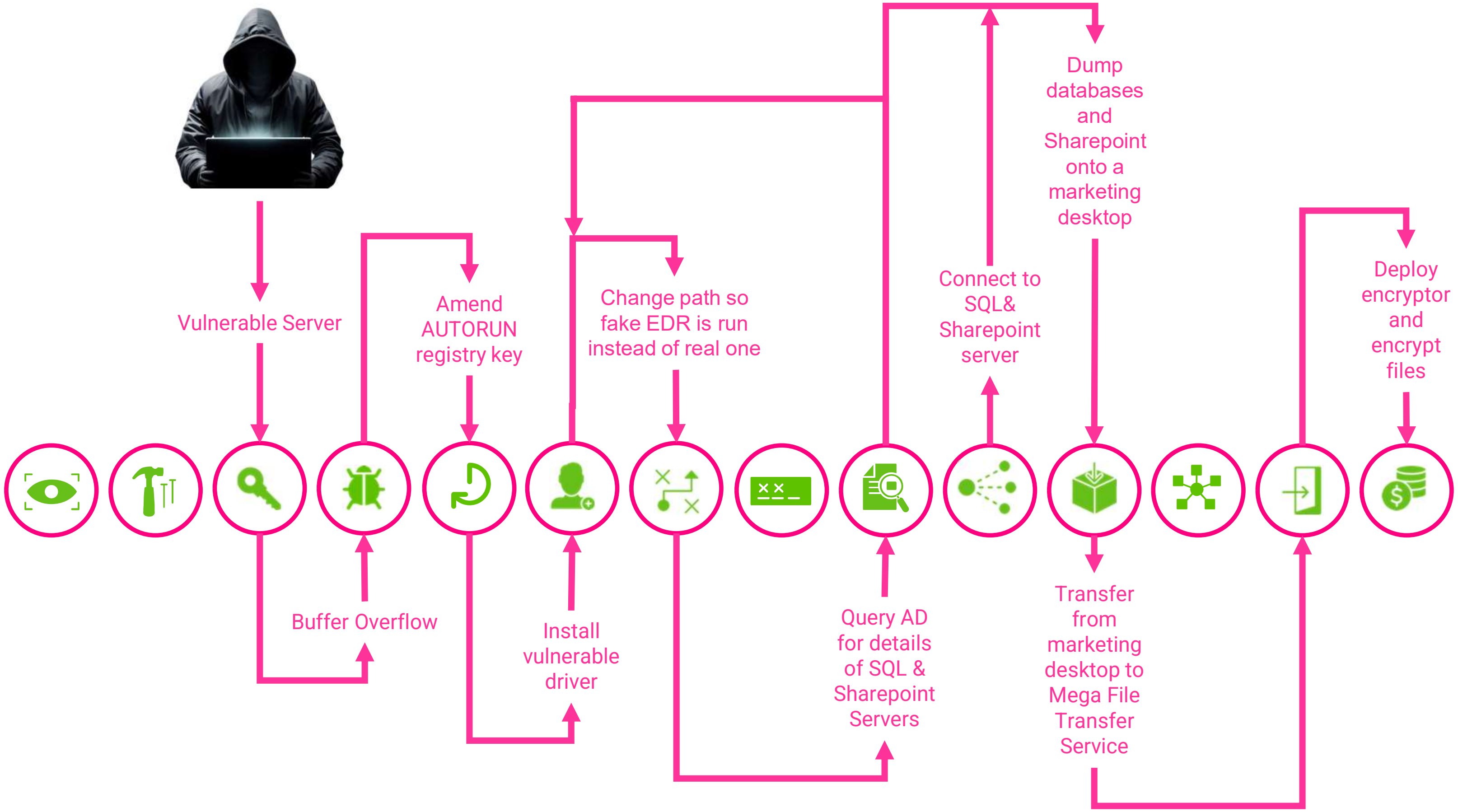
https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html

MITRE ATT&CK



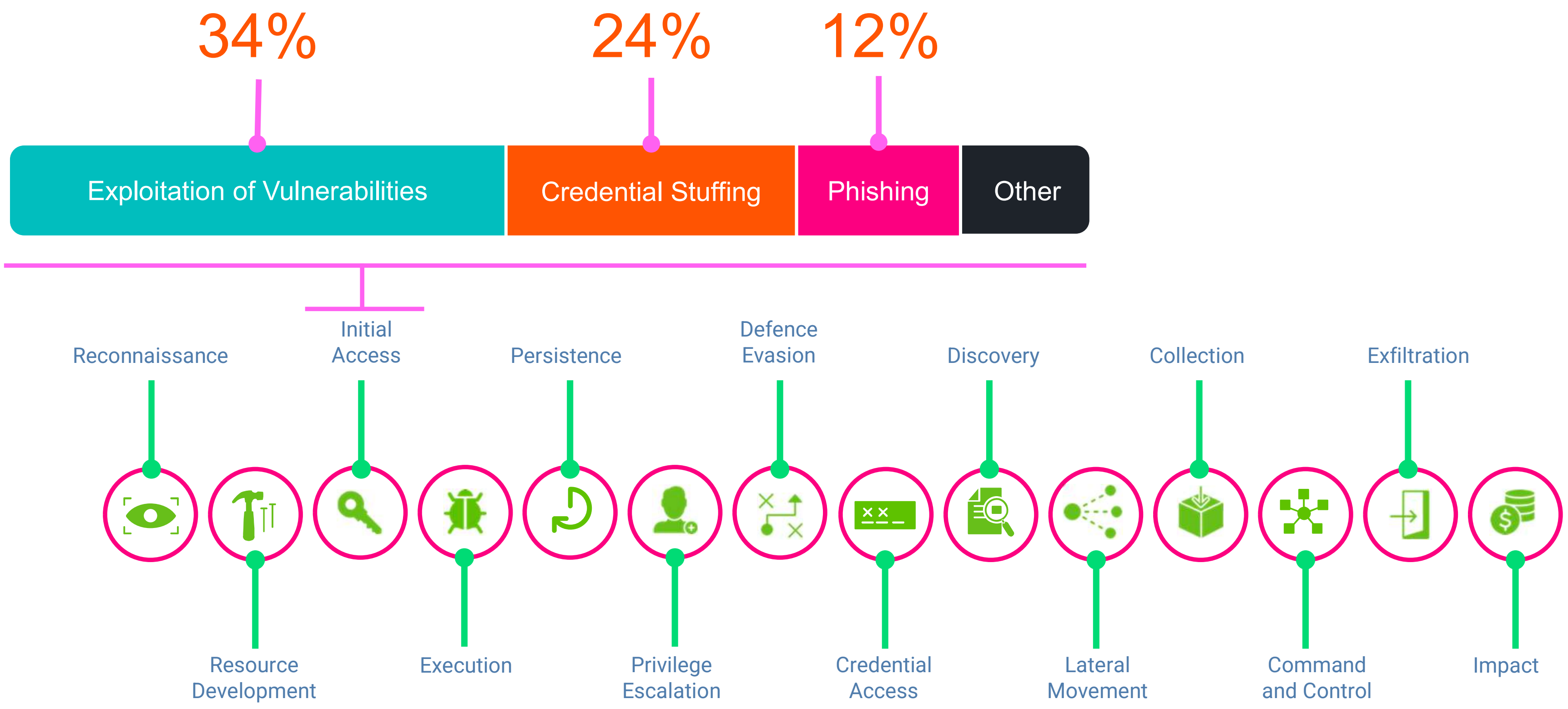
COHESITY

Ransomware isn’t a single malware binary


Vulnerable Server
Buffer Overflow
Amend AUTORUN registry key
Install vulnerable driver
Change path so fake EDR is run instead of real one
Query AD for details of SQL & Sharepoint Servers
Connect to SQL& Sharepoint server
Dump databases and Sharepoint onto a marketing desktop
Transfer from marketing desktop to Mega File Transfer Service
Deploy encryptor and encrypt files

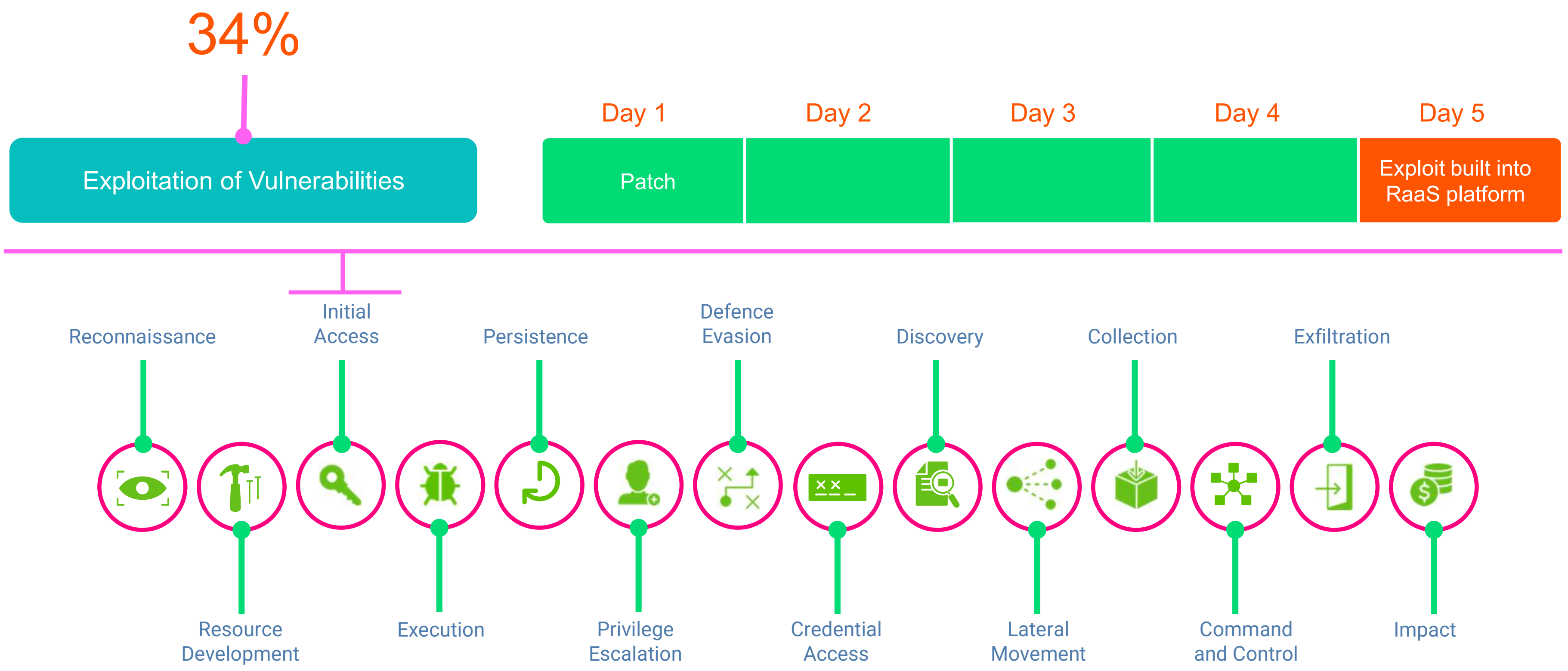
COHESITY

Business Continuity & Disaster Recovery vs Cyber Recovery

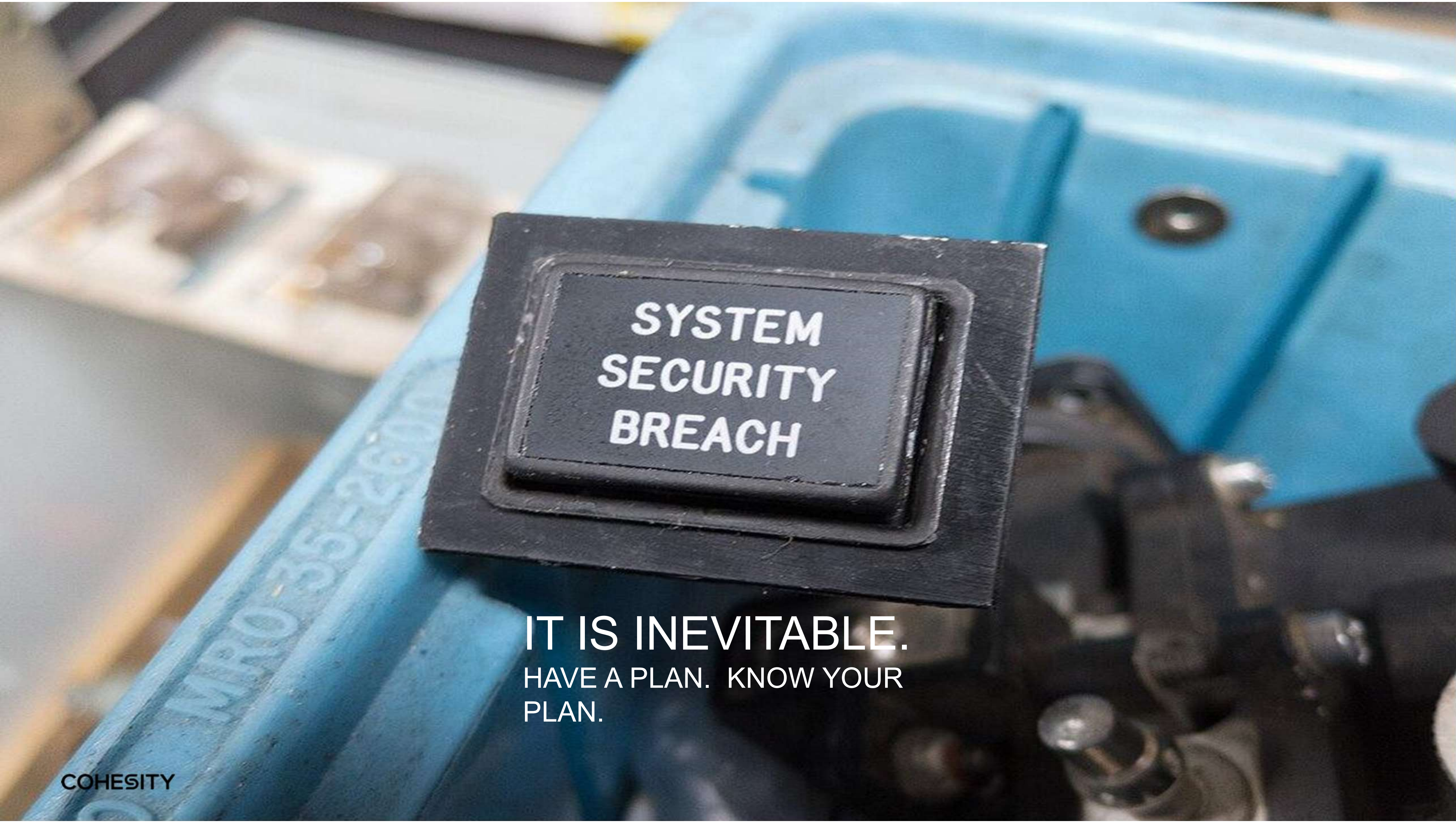


COHESITY

Business Continuity & Disaster Recovery vs Cyber Recovery



COHESITY



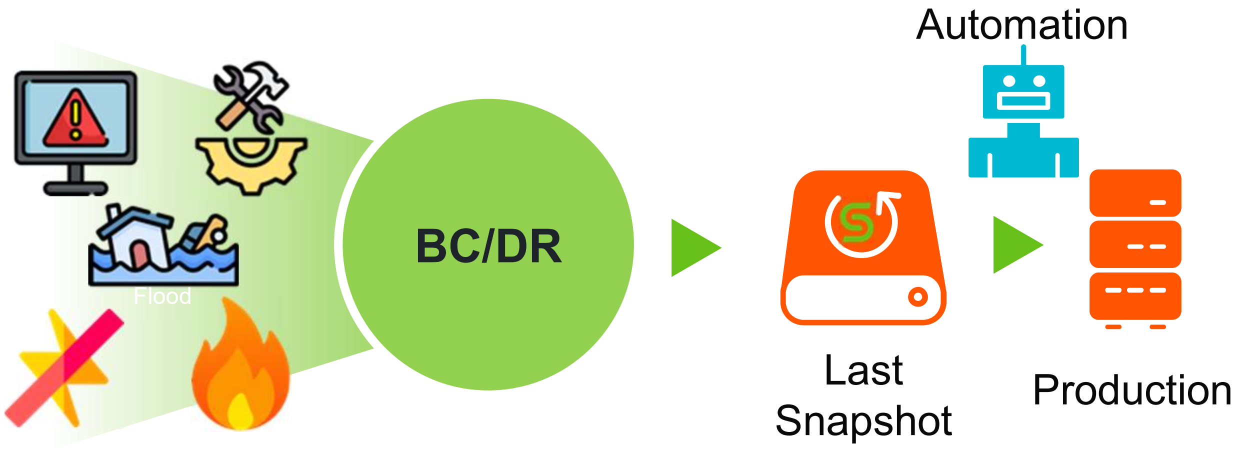
IT IS INEVITABLE.

HAVE A PLAN. KNOW YOUR PLAN.

COHESITY

Business Continuity & Disaster Recovery vs Cyber Recovery

Business Continuity & Disaster Recovery



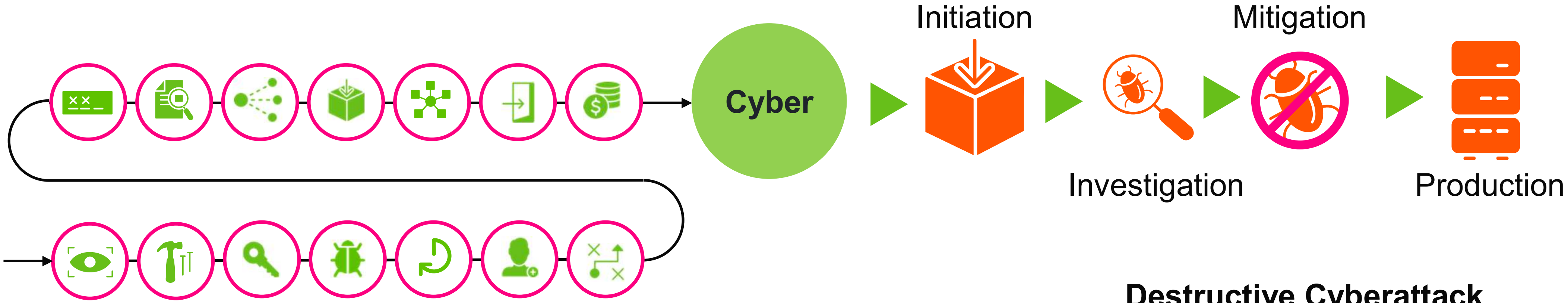
Flood

BC/DR

Automation

Last Snapshot

Production



Cyber

Initiation

Investigation

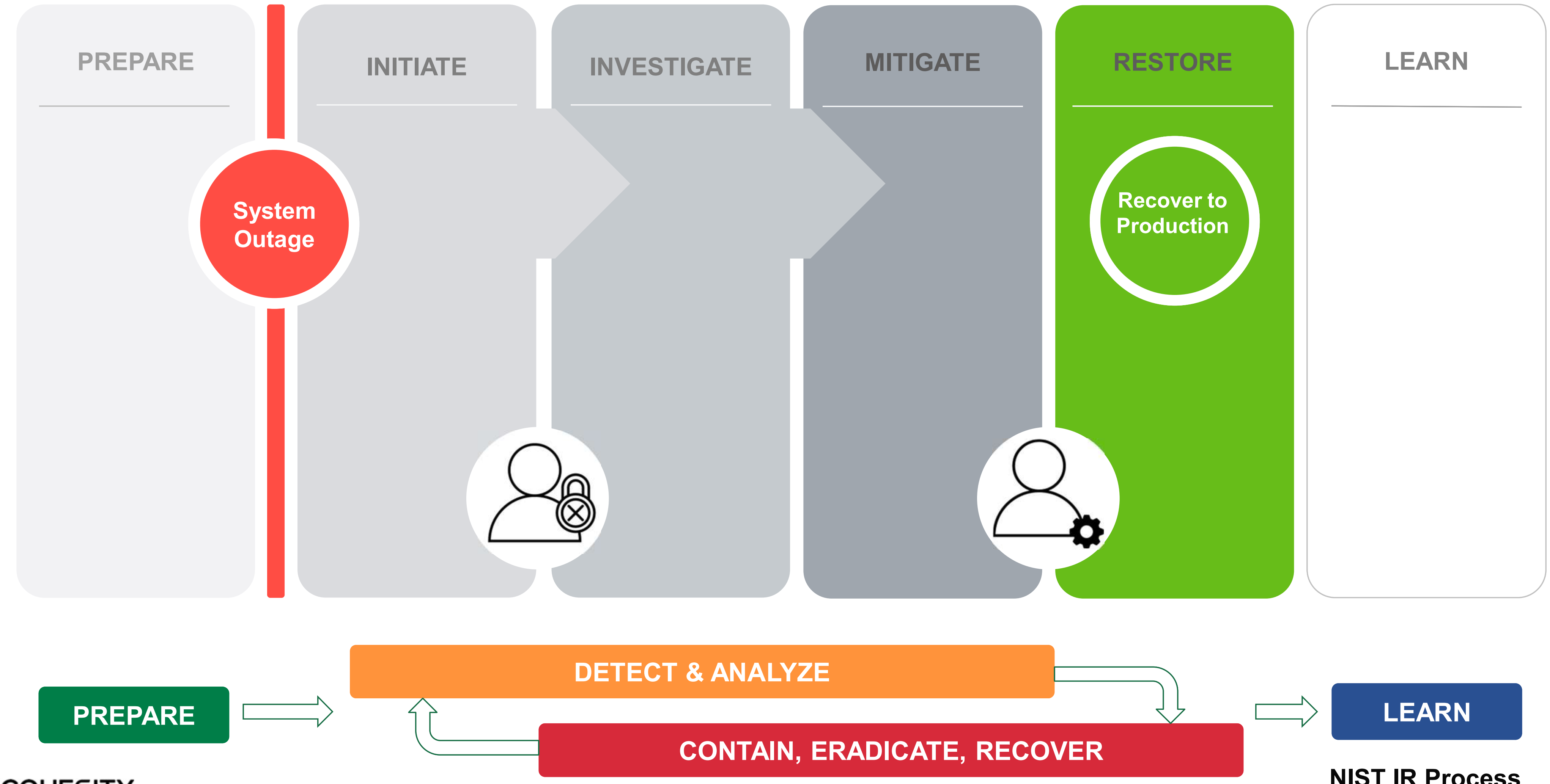
Mitigation

Production

Destructive Cyberattack

COHESITY

Cohesity Incident Response Perspective

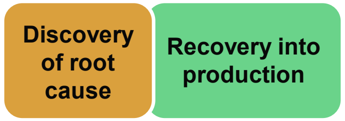


NIST IR Process

COHESITY

Business Continuity & Disaster Recovery vs Cyber Recovery

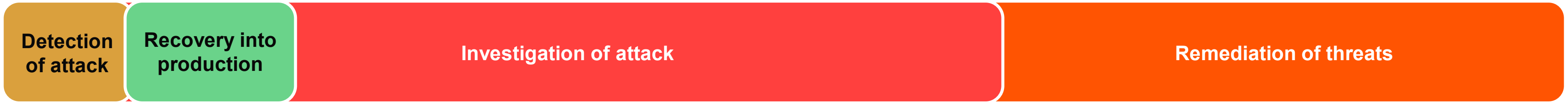
Business Continuity & Disaster Recovery



Discovery of root cause

Recovery into production

Cyber Response & Recover



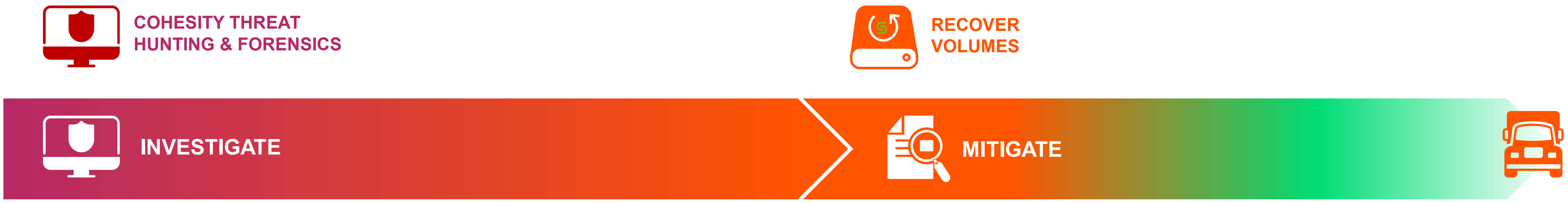
Detection of attack

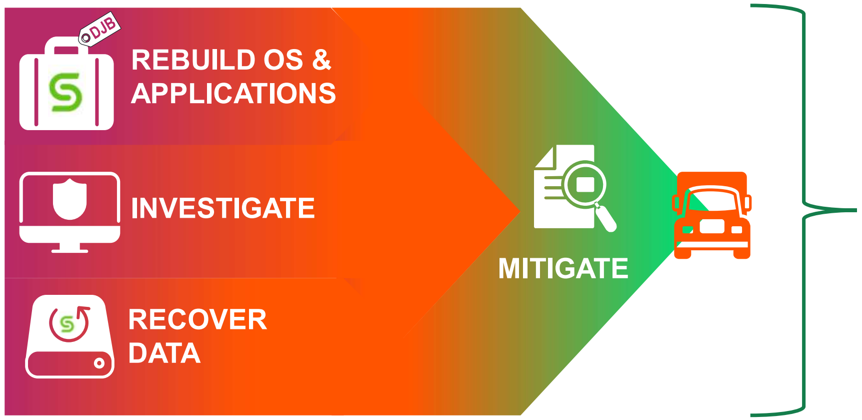
Recovery into production

Investigation of attack

Remediation of threats

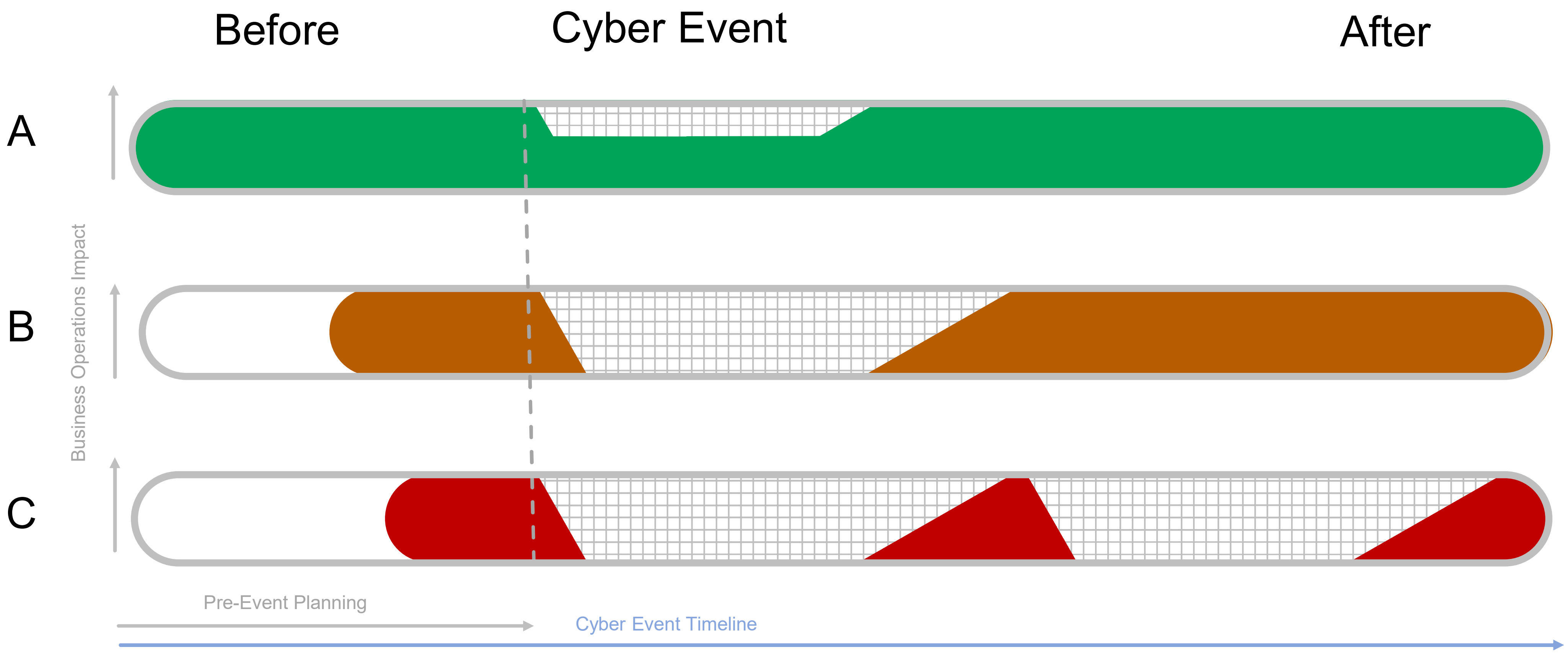
Recover/Clean vs. rebuild: speeding RTO





- Parallel activities
- Reduced investigatory & mitigated overhead

Same Attack, Different Outcomes



COHESITY

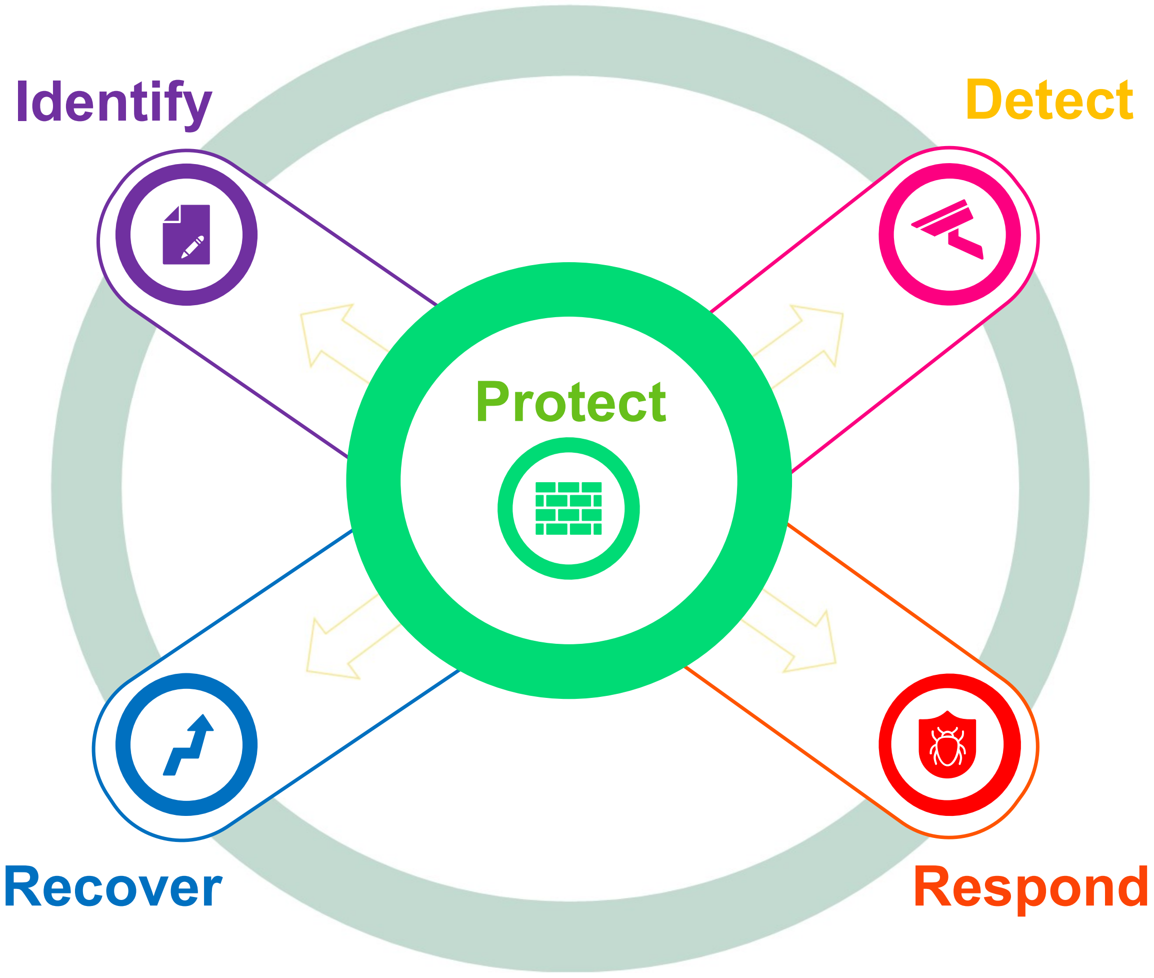
Cyber Resilience Capabilities

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
DSPM - Sensitive Data Discovery	Encryption	SIEM Integration	SOAR Integration	Instant Mass Restore
Vulnerability Scanning	Immutability	3rd Party Threat Feeds	Proactive Threat Response	Clean Room Recovery
Proactive Data Classification	Data Isolation	EDR/XDR Detection Ingest	Instant Clean Room	Cloud Vault Recovery
Data Asset Discovery	Zero Trust Principals	Reactive Hunting	Forensic Threat Hunting	
Posture Advisor	Separation of Duties	Comprehensive IOC Scanning	Point in Time Vulnerability Scanning	
		Ransomware Anomaly Analysis	Incident Timeline Analysis	
		Malware Scan on Access (ICAP)	Business & Regulatory Assessment	

S Cohesity capabilities

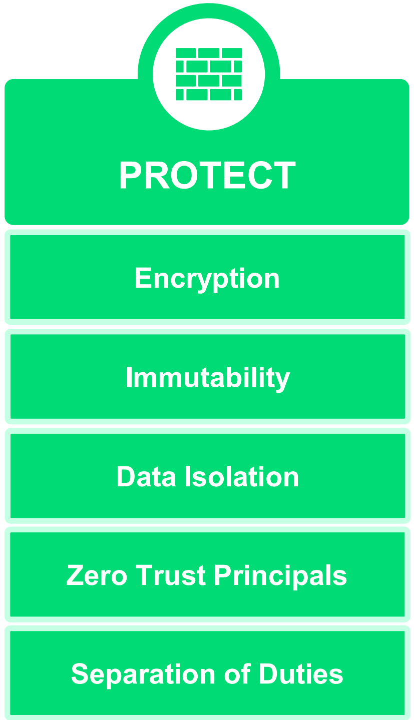
A Cohesity enabled Alliance capabilities

Cyber Resilience Infrastructure is Hub and Spoke



COHESITY

Data Protection Is the Core of Cyber Security



PROTECT

Encryption

Immutability

Data Isolation

Zero Trust Principals

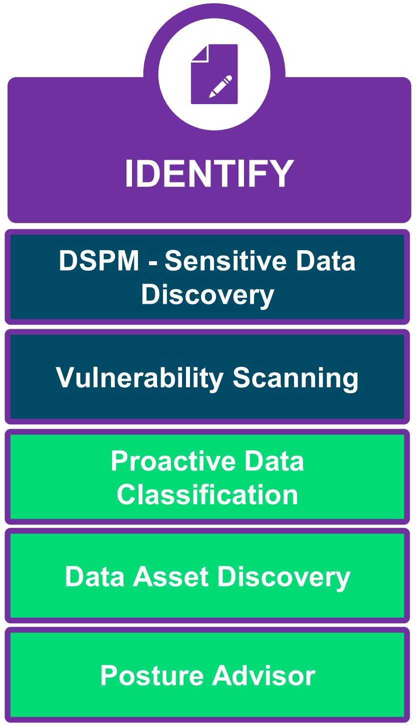
Separation of Duties

Intrinsic properties

- Read only file system
- Immutability by design

- Zero Trust principles
- Multi-factor authentication
- SSO integration SAMLv2
- Separation of duties (missile keys + who)

Know The Mission Before You Begin



IDENTIFY

DSPM - Sensitive Data Discovery

Vulnerability Scanning

Proactive Data Classification

Data Asset Discovery

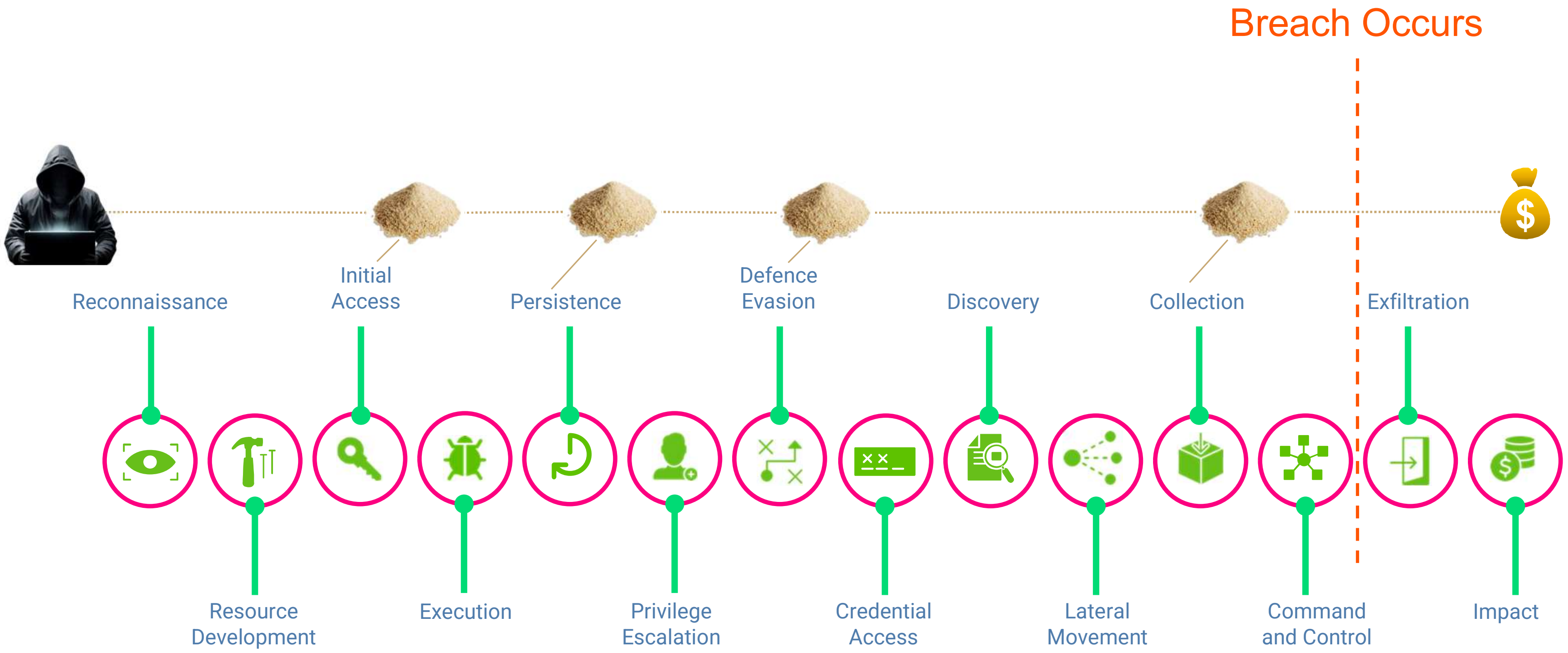
Posture Advisor

1. People, process and platforms
   1. Application owners
   2. Nontechnical too
2. What is your minimum viable company?
   1. What are your most critical applications and data?
   2. Scan and classification of data
3. Pressure testing
   1. Vulnerability and IoC scanning
   2. Highlight Configuration Drift
   3. Detect malicious re-configuration

S Cohesity capabilities

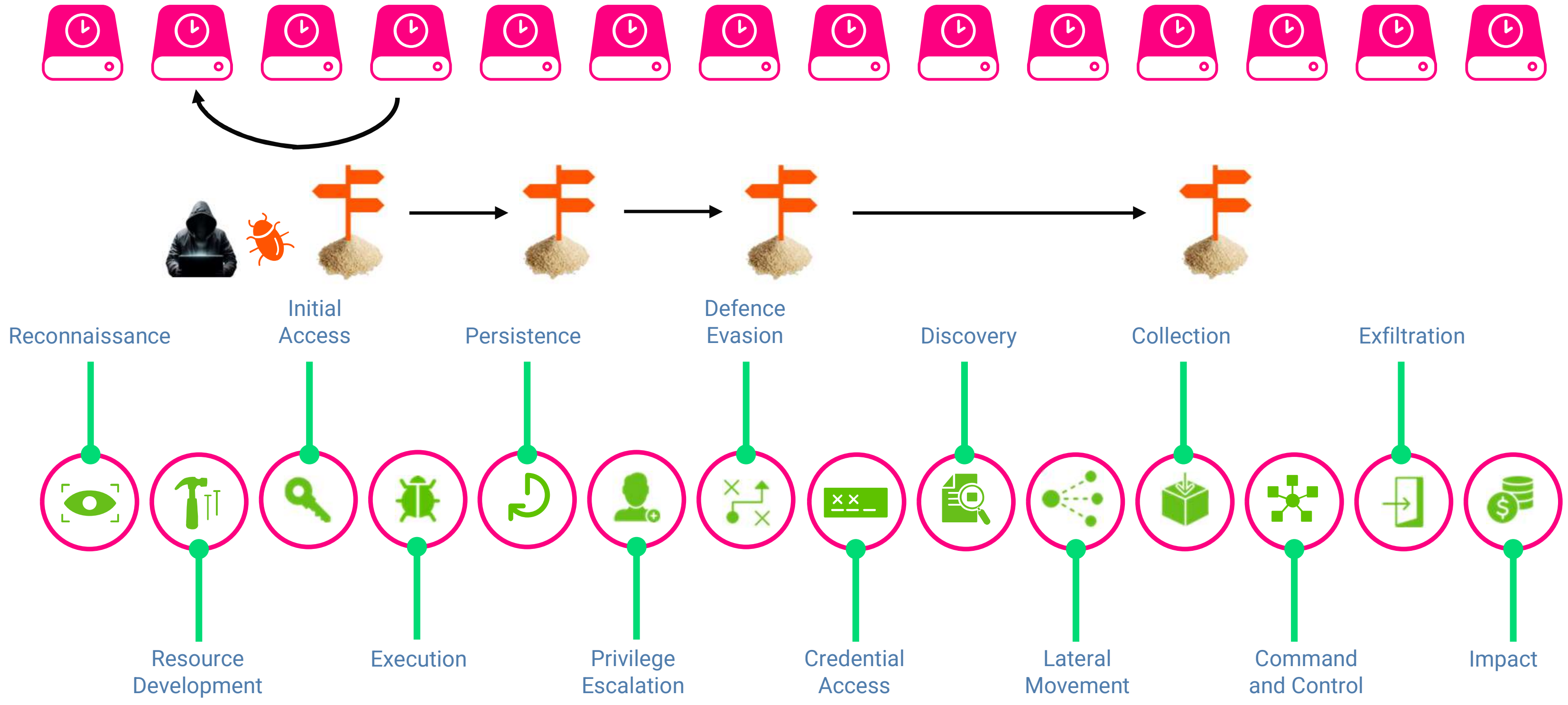
A Cohesity enabled Alliance capabilities

Indicators of Compromise



COHESITY

Indicators of Compromise

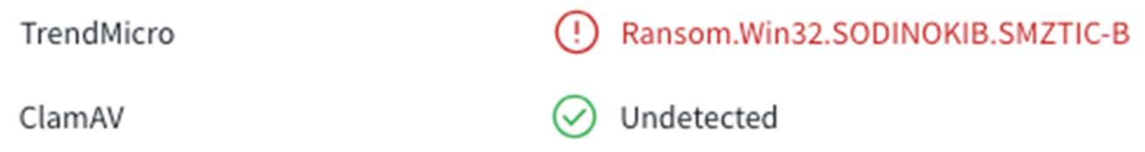


PUSH TO OPEN
PUSH TO OPEN

Hashing it out

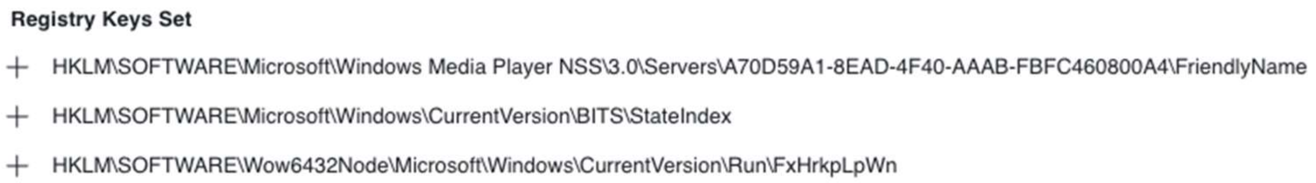
334776db4ec6ff535f8ee96a6b7da83ca51b320cef4ba102d0da12660524a846

Which tools can see the threat?



TrendMicro	! Ransom.Win32.SODINOKIB.SMZTIC-B
ClamAV	✓ Undetected

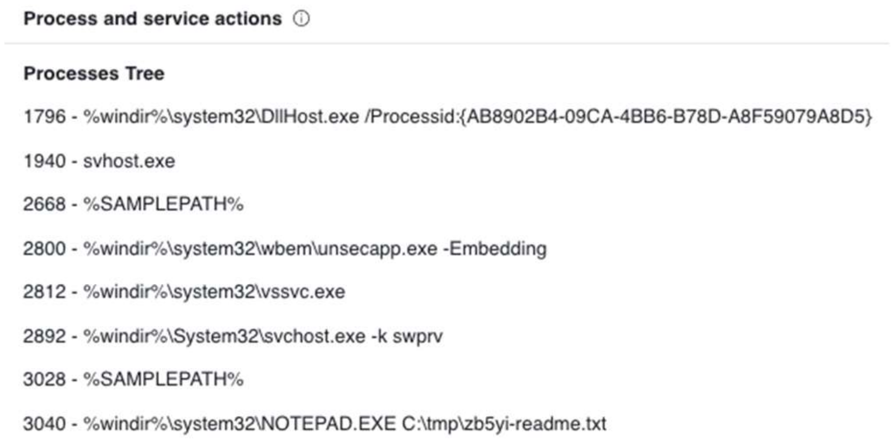
How does it hide?



Registry Keys Set

- HKLM\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Servers\A70D59A1-8EAD-4F40-AAAB-FBFC460800A4\FriendlyName
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\BITS\StateIndex
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\FxHrkpLpWn

What processes run?



Process and service actions ⓘ

Processes Tree

```
1796 - %windir%\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
1940 - svhost.exe
2668 - %SAMPLEPATH%
2800 - %windir%\system32\wbem\unsecapp.exe -Embedding
2812 - %windir%\system32\vssvc.exe
2892 - %windir%\System32\svchost.exe -k swprv
3028 - %SAMPLEPATH%
3040 - %windir%\system32\NOTEPAD.EXE C:\tmp\zb5yi-readme.txt
```

Detection, Smoke or Fire

DETECT

- SIEM Integration
- 3rd Party Threat Feeds
- EDR/XDR Detection Ingest
- Reactive Hunting
- Comprehensive IOC Scanning
- Ransomware Anomaly Analysis
- Malware Scan on Access (ICAP)

Smoke or Fire

Anomalies detected before destination with active systems or, tailing indicators discovered by your backup threat detection

S Cohesity capabilities

A Cohesity enabled Alliance capabilities

Speed and Confidence in Your Response

RESPOND

SOAR Integration

Proactive Threat Response

Instant Clean Room

Forensic Threat Hunting

Point in Time Vulnerability Scanning

Incident Timeline Analysis

Business & Regulatory Assessment

Speed & Confidence

1. Which is faster? Build vs. Restore
2. What is your incident termination criteria?

There will be chaos

- Legal, chain of custody
- Who has the authority?
- Hot, warm or cold site
- Eradication and exit criteria
- How much is a manual process?

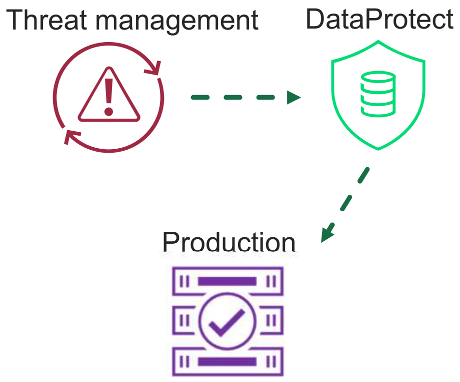
OS | Apps | Files & Data

Incident Response Flows

Example A

RESPOND

- SOAR Integration
- Proactive Threat Response
- Instant Clean Room
- Forensic Threat Hunting
- Point in Time Vulnerability Scanning
- Incident Timeline Analysis
- Business & Regulatory Assessment



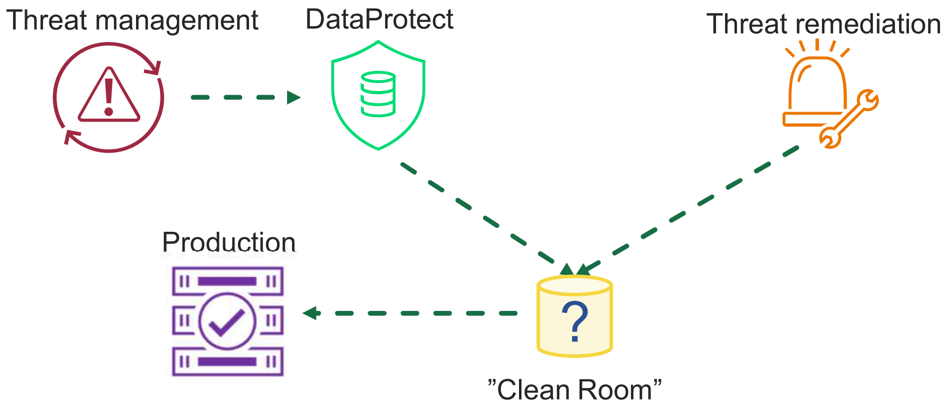
OS | Apps | Files & Data

Incident Response Flows

Example B

RESPOND

- SOAR Integration
- Proactive Threat Response
- Instant Clean Room
- Forensic Threat Hunting
- Point in Time Vulnerability Scanning
- Incident Timeline Analysis
- Business & Regulatory Assessment



OS | Apps | Files & Data

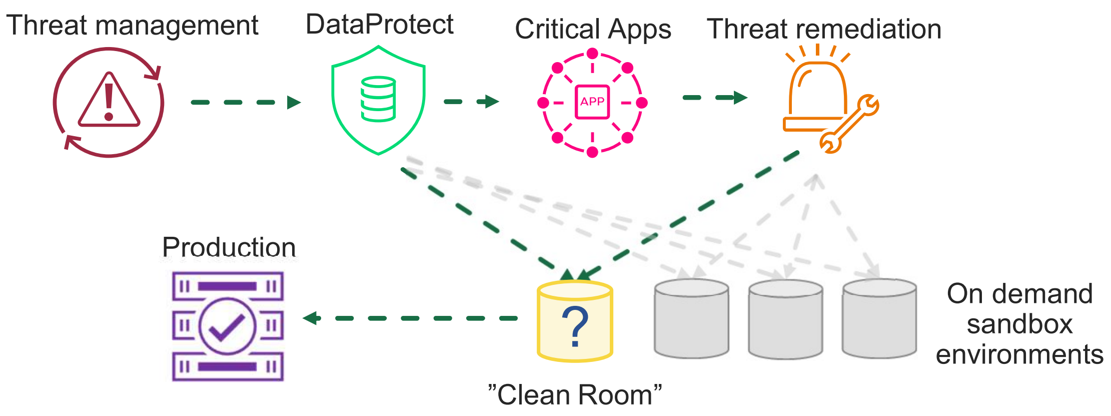
COHESITY

Incident Response Flows

Example B

RESPOND

- SOAR Integration
- Proactive Threat Response
- Instant Clean Room
- Forensic Threat Hunting
- Point in Time Vulnerability Scanning
- Incident Timeline Analysis
- Business & Regulatory Assessment



OS

Apps

Files & Data

Recovery, The Last Mile

RECOVER

Instant Mass Restore

Clean Room Recovery

Cloud Vault Recovery

1. All data has been returned to associated primary systems
2. Getting all business owners to sign off on back to normal operations
3. Many point operations / surgical recoveries
4. Meeting all SLA for applications and customers
5. Data Protection SLA back to normal

Data Security Posture Checklist

Criteria	Rationale	Response
Are your backups **immutable**?	Prevent premature deletion of backups.	Y / N
Are your backups **air-gapped**?	Gold copy of last resort if primary is lost.	Y / N
Do you have an **offsite** copy of your backups?	Adhere to 3:2:1 rule for backup copies.	Y / N
Are your **backup servers and infrastructure hardened** (OS, application)?	Prevent attackers from accessing backup servers.	Y / N
Does the system **detect insecure configurations** automatically?	Avoid configuration drift and insecure options.	Y / N
Do you use **RBAC**, **MFA**, and **quorum** to control access to backups?	Prevent a single privileged user from taking malicious action on backups.	Y / N
Is the **RPO** and **RTO** for workloads formally defined?	Understand business requirements for recovery SLAs.	Y / N
Are cyber recovery scenarios **tested** on a regular basis?	Prove that recovery infrastructure and processes are viable.	Y / N

THANK YOU

josef.honc@cohesity.com

COHESITY

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.

COHESITY