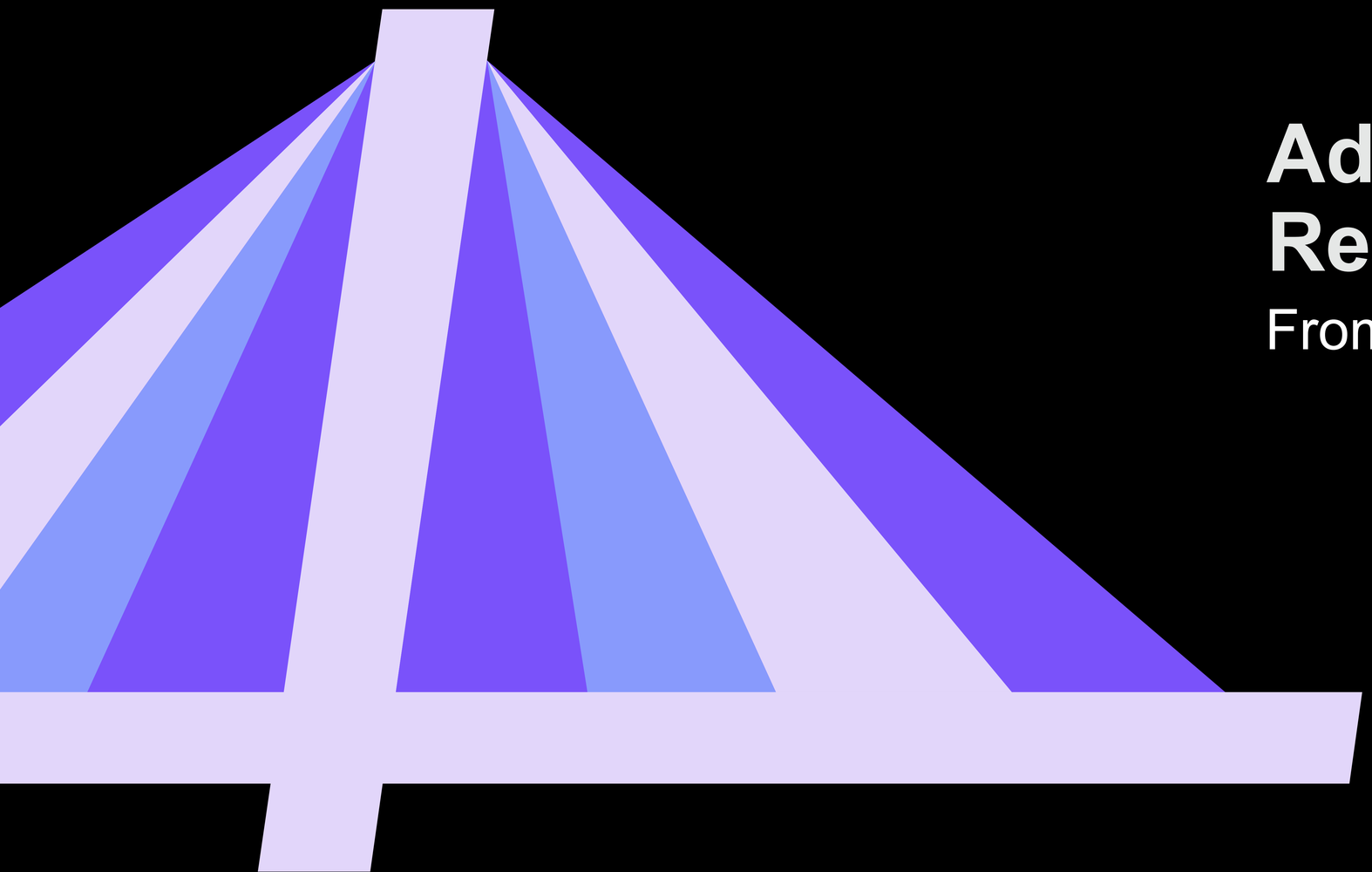


HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Advancing Cyber Resilience

From Identity to Data and Beyond

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Jonathon Mayor

Principal Security Consultant, Cohesity

Responder, Coach, Maker, Learner (Breaker), Inventor

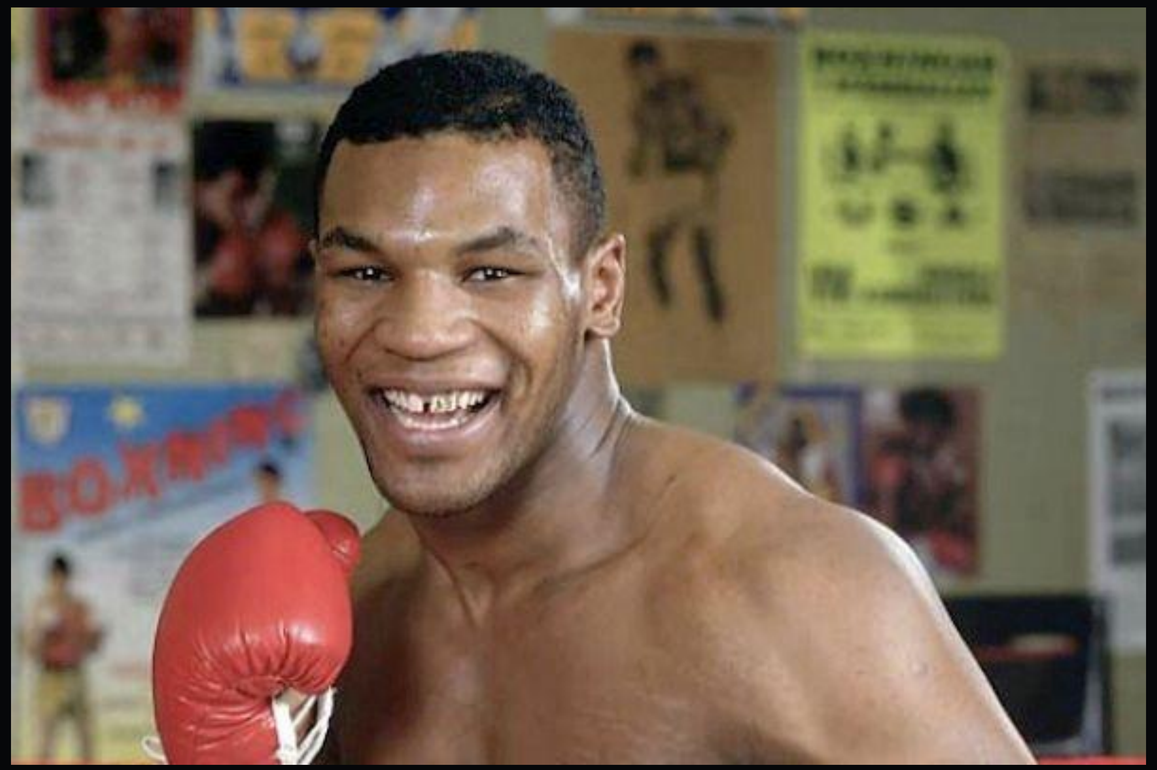
IT IS INEVITABLE.
HAVE A PLAN. TEST THE PLAN.

No plan of operations extends with any certainty beyond the first encounter with the main enemy forces."

Helmuth von Moltke

In Other Words

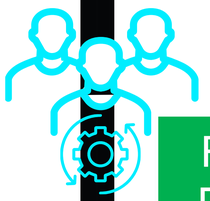
“Everyone has a plan until. . . “



Cohesity Incident Response Perspective

Prepare	Initiate	Investigate	Mitigate	Restore	Learn
Are trusted assets and information available?	Is a response possible with available tools?	What is the scope and timeline of events?	What needs to happen before restoring?	**How long to restore critical services?**	What worked and what needs improvement?

Destructive Cyber Attack

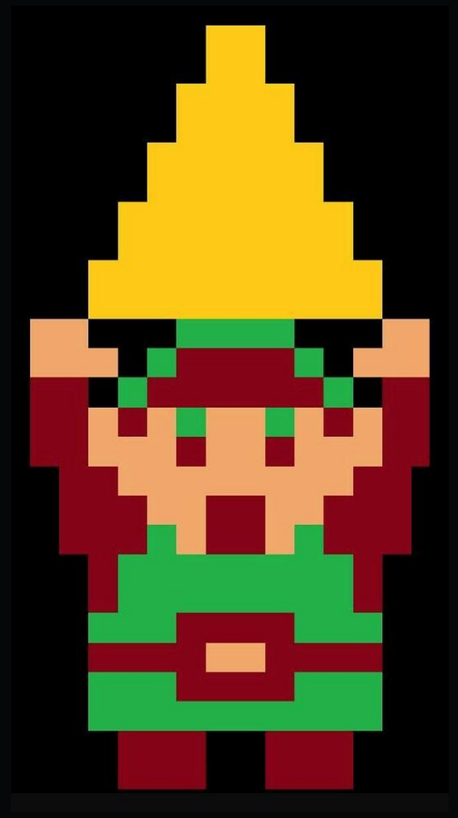


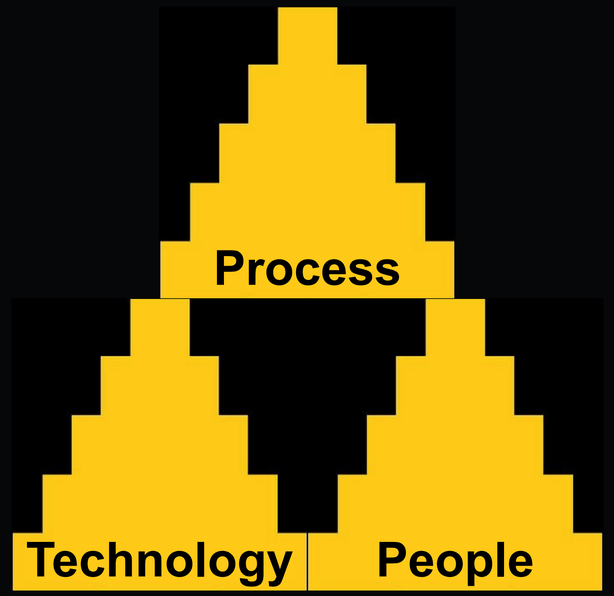
Restore to Production

Response

Recovery

The CIA Tri. . . force?





Houston, we have a problem.

Signs things may not be going well

> We successfully rotated all keys, but now we are having issues logging in to critical systems."

Active Directory Admin

> The threat is contained, and the backup infrastructure does not appear to be impacted. However, the core network devices have been compromised, and all systems have been unplugged."

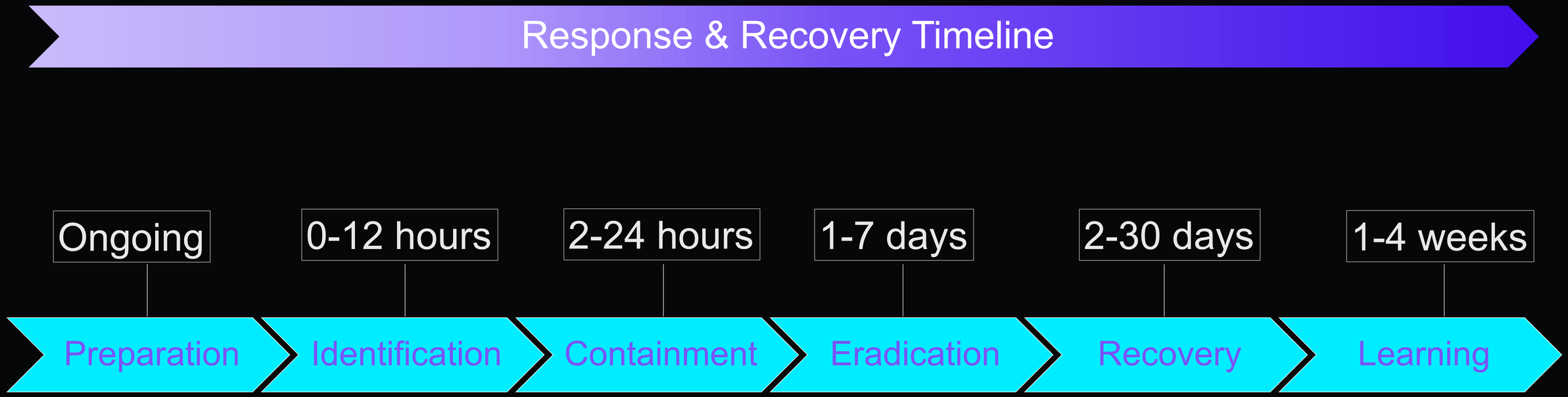
Infrastructure Lead

> It is confirmed that Active Directory has been compromised. No systems are released to be restored until the full investigation has been completed."

DFIR Lead

The Challenge

Shorten “mean time to recover” MTTR



The Waiting

How it started

How its going

Impacts to the Timeline

Initial delays have a lasting effect

- Communication
- Authentication (Access)

Longer restore times have a multiplying effect

- Repeated restores add time
- Latency in data movement has a compounding effect

Access to resources is limited

- Primary systems are full, isolated, or unavailable

Process gaps introduce risk

- Ad hoc actions compound undesired outcomes

Detection

User login errors, then alerts through endpoint scanning

Ransom note

Impact

Core network devices, Active Directory, Exchange, virtual systems, file shares, databases

Response Challenges

Initial communication and authentication to unaffected systems was impeded

Outcome & Learnings

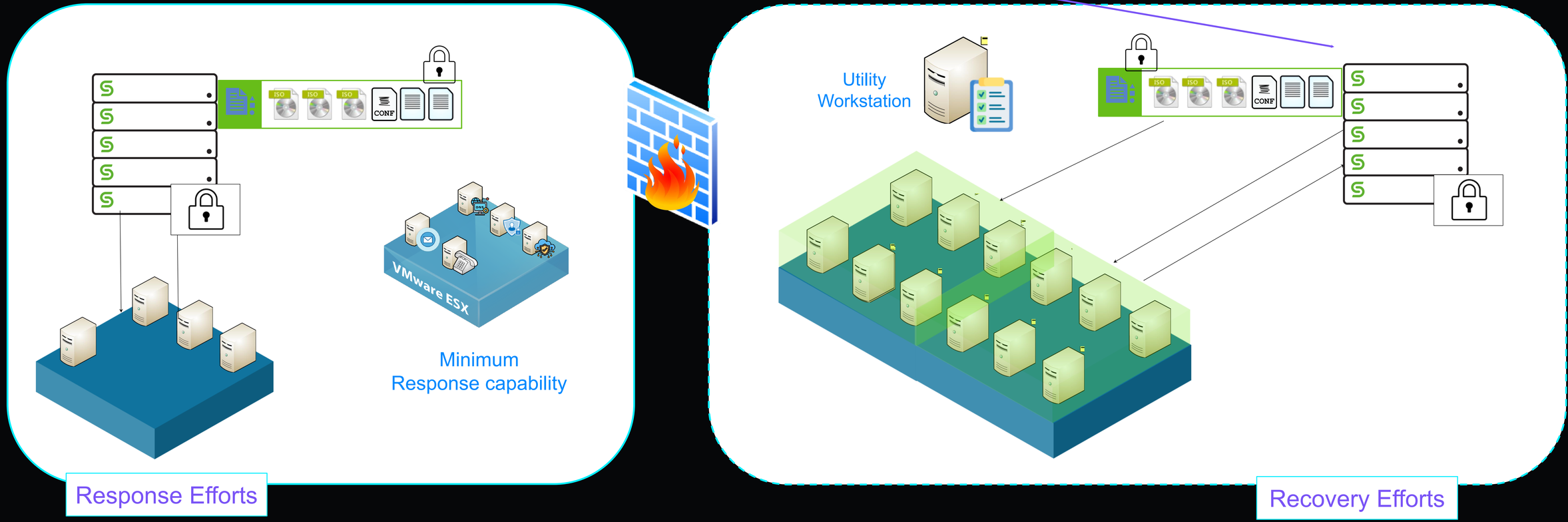
Backup platform withstood the attack

Directory was restored into isolated environment for analysis

Workflow Architecture Diagram: High Impact

- Identification
- Containment

- Eradication
- Recovery



Impact

Production VMware environment (including Cohesity VE) was encrypted.

Response

Customer contacted CERT and Fenix24 for coordinated eradication, restores, and validation.

Cohesity Relevance

FortKnox was unaffected, so all critical systems were able to be restored.

Outcome

Manufacturing operations were able to resume within 4 days.

Observed Attack Patterns

Cohesity Cyber Events Response Team – Trailing 9 months

Persistence, Privilege Escalation	Resource Development, Defense Evasion	Exfiltration	Credential Access
AI-supported phishing and social engineering	EDR evasion built into RaaS platforms	Data exfiltration without encryption	IAM compromise (Active Directory)

Mitigations

Network Segmentation, Role-based Access	Execution Prevention, Audit, Restrict Permissions	Data Loss Prevention, Restrict Web Content	AD Configuration, Privileged Access Manager

Foundation of Resilience

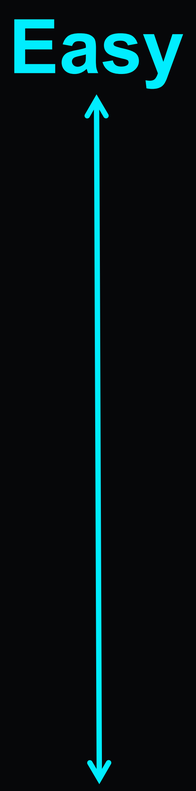
Getting from Here. . . to There

Incident Response & Recovery – Target Outcomes

Preparation	Identification	Containment	Eradication	Recovery	Learning
Improve resilience maturity	Get from signal to action quickly	Control and minimize impact	Manage risk to an acceptable level	Quick, flexible access to data and systems	Continuous improvement

THE BASICS

People | Process | Technology



TE - Enforce the use of phishing-resistant MFA
TE - Use WORM technology on backups
PR - Use principle of least privilege access
PR - Create separation of duties for destructive or mission critical actions
PE - Use unique, local accounts for elevated access to critical systems
TE - Ensure systems have backups using 3-2-1+
PE - Use network segmentation to limit access between clients, critical systems, response/recovery systems
TE - Alerting for logins to out-of-band and administrative interfaces of critical systems
PR - Establish chain of custody for trusted and validated access to system images, install media, contracts, contacts, etc.
PE - Validated ability to rebuild response communications, authentication, security tooling, (minimum response capability)
PR - Optimized processes for investigation in isolation as required

HYBRID IDENTITY PROTECTION conf25

CHARLESTON

Questions?

HYBRID IDENTITY PROTECTION conf25 CHARLESTON

Thank You

Stay safe out there

HYBRID
IDENTITY
PROTECTION

conf25

CHARLESTON