Airiam

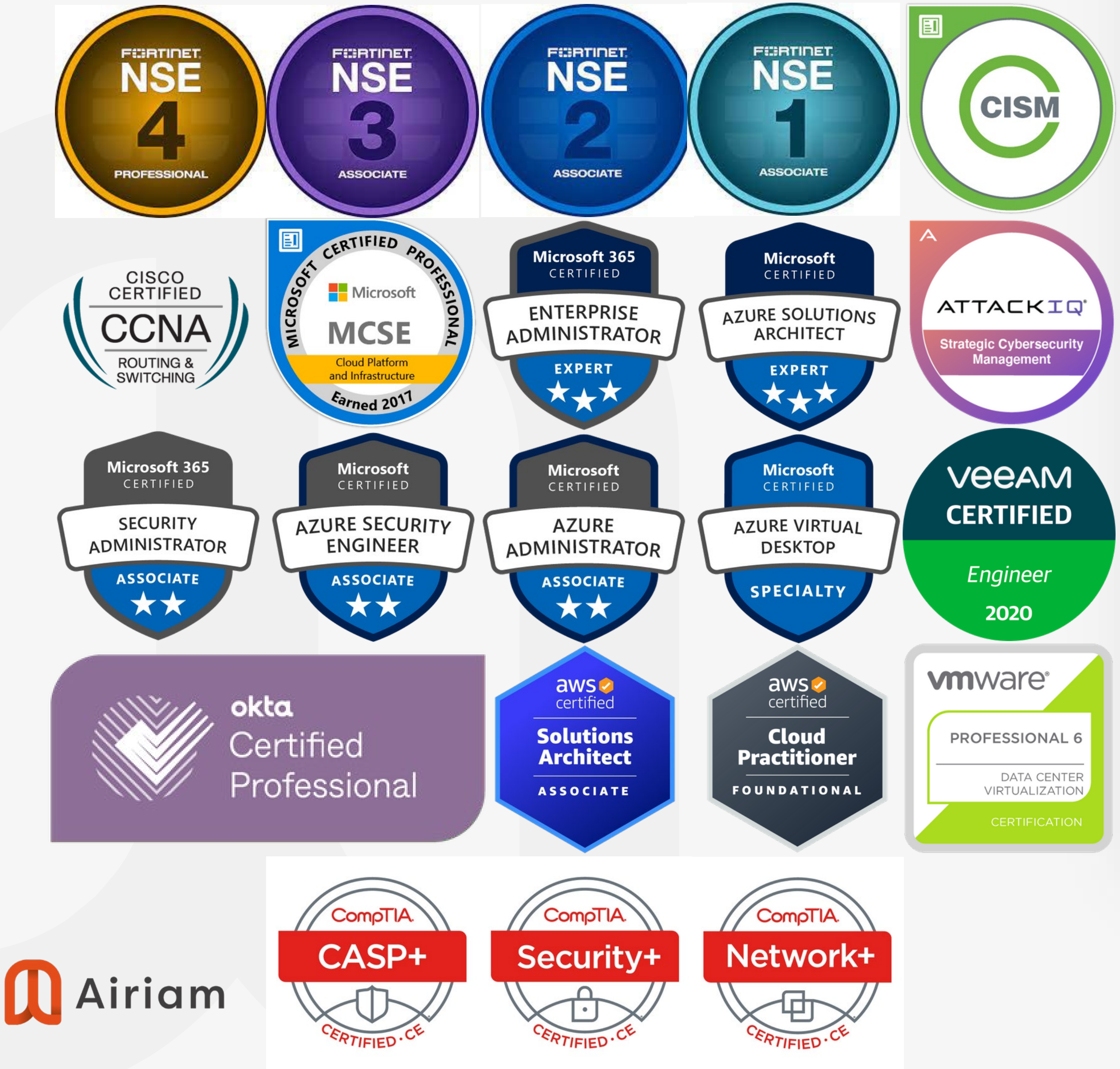
# Resiliency
for Logistics Companies

by Art Ocain, Vice President of Service Delivery at Airiam

art@airiam :~$ whoami

Information Security & Incident Response

- Lead Incident Response
- Sys admin background with detours through network admin and cloud admin
- Cybersecurity enthusiast & evangelist


FORTINET NSE 4 PROFESSIONAL
FORTINET NSE 3 ASSOCIATE
FORTINET NSE 2 ASSOCIATE
FORTINET NSE 1 ASSOCIATE
CISM
CISCO CERTIFIED CCNA ROUTING & SWITCHING
MICROSOFT CERTIFIED PROFESSIONAL Microsoft MCSE Cloud Platform and Infrastructure Earned 2017
Microsoft 365 CERTIFIED ENTERPRISE ADMINISTRATOR EXPERT
Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT
ATTACKIQ Strategic Cybersecurity Management
Microsoft 365 CERTIFIED SECURITY ADMINISTRATOR ASSOCIATE
Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE
Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE
Microsoft CERTIFIED AZURE VIRTUAL DESKTOP SPECIALTY
veeam CERTIFIED Engineer 2020
okta Certified Professional
aws certified Solutions Architect ASSOCIATE
aws certified Cloud Practitioner FOUNDATIONAL
vmware PROFESSIONAL 6 DATA CENTER VIRTUALIZATION CERTIFICATION
CompTIA CASP+ CERTIFIED · CE
CompTIA Security+ CERTIFIED · CE
CompTIA Network+ CERTIFIED · CE

Airiam

Front Line Observations

All companies experience cyber attack

Most companies will experience ransomware

Most companies have recovery problems

Airiam

Key for **Managed Service Provider** or Managed Security Service Provider

IT Management

- Manage stability and performance of networks, systems, data
- Keep technology in alignment with best practices
- Keep technology up to date
- Improve business operations through IT

Security Management

- Identify
- Protect
- Detect
- Respond
- Recover

- Manage risk through cyber
- Plan and implement controls
- Layer defenses
- Monitor
- Identify and fix vulnerabilities
- Identify and respond to threats

Resilience

- Anticipate
- Withstand
- Recover
- Adapt

- Contain and stop damage from attacks
- Plan & manage Disaster Recovery
- Stand back up quickly after an attack
- Improve systems after an attack (using what was learned)

Airiam

Key for **Managed Service Provider** or Managed Security Service Provider

Automation

- Backup Remediation
- IT Constraint Management
- IT Ops → CI/CD
- Automated incident creation
- Continuous monitoring and correlation
- Continuous vulnerability management & patching
- Continuous pentesting

Continuous Patching

- Patching should happen
  - Immediately
  - Daily
  - With minimal downtime
- Frequent patching is a sign of resilience

Short Feedback Loops

- Enable rapid feedback loops between clients and service providers.
  - Users
  - Executives
  - Incident Response (IR)
  - Security Operations (SOC)
  - Network Operations (NOC)
  - IT Operations (Server, Endpoint, Cloud, IAM, etc.)
  - Development / DevOps
  - Risk Management

Cyber Resilience for Logistics Companies

Think about the range of tools your business uses to get the job done:

- **Software**: mapping and load management software, truck management software, driver logging systems, warehouse management systems, fuel systems, customs and insurance compliance, tracking technology, rate management, billing, accounting systems, fleet management software, etc.

- **Hardware**: connected vehicle/truck GPS, server infrastructure, cloud, workstations/laptops, fuel pumps, operational tech

Cyber Resilience for Logistics Companies

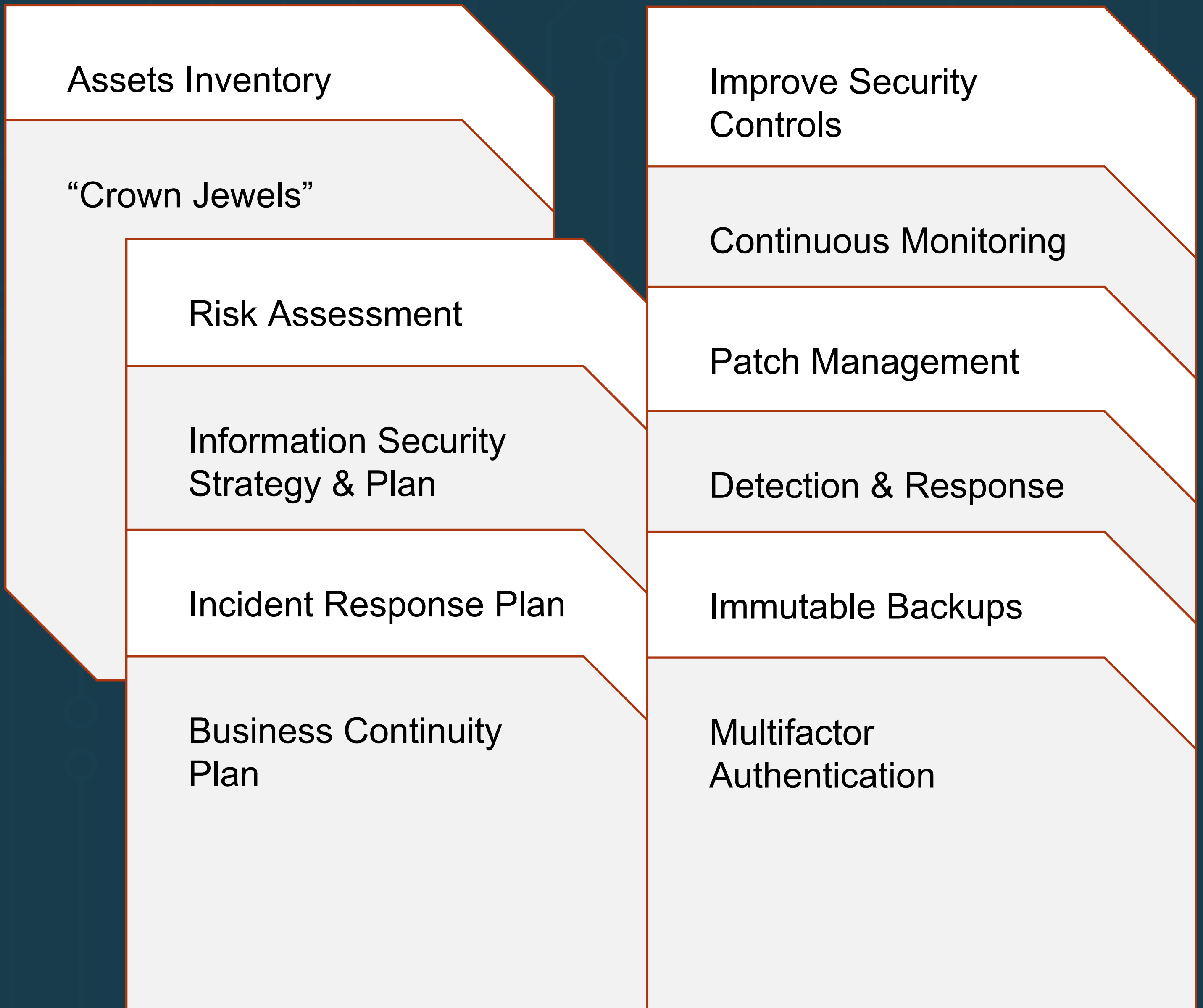
The complexity of your systems requires careful monitoring and support to stop unauthorized access and data breaches.

- Develop and practice an cybersecurity program, incident response plan, and disaster recovery plan
- Ensure systems are patched, preventing hackers from targeting known vulnerabilities
- Monitor your networks for suspicious activity to take preventive steps before a full breach occurs
- Design and manage immutable backups and ensure credentials to those backups are secure
- Support and create multi-factor authentication (MFA) options to stop attackers from breaking in
- Pentest your systems to find vulnerabilities before hackers do, allowing fixes to occur so breaches don't
- Train your team members to prevent phishing attacks - one of the most common ways hackers initially gain access to networks

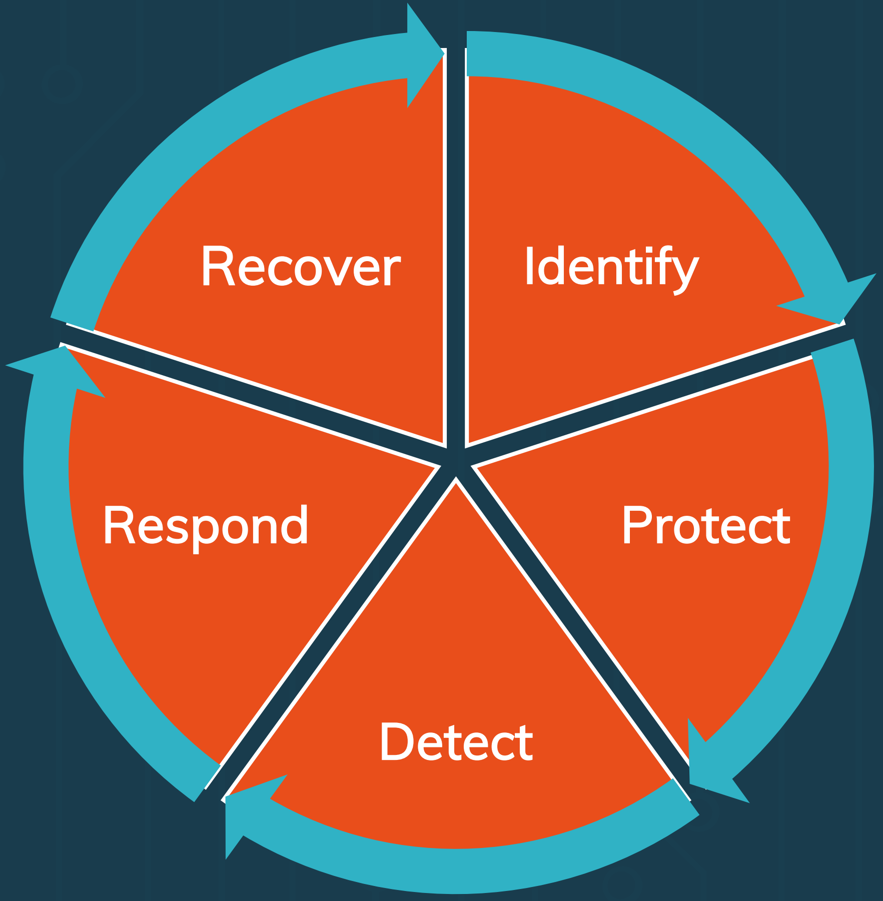
Cybersecurity & Resilience

- Protect, but EXPECT attack and EXPECT that you won't be successful in preventing all attacks.

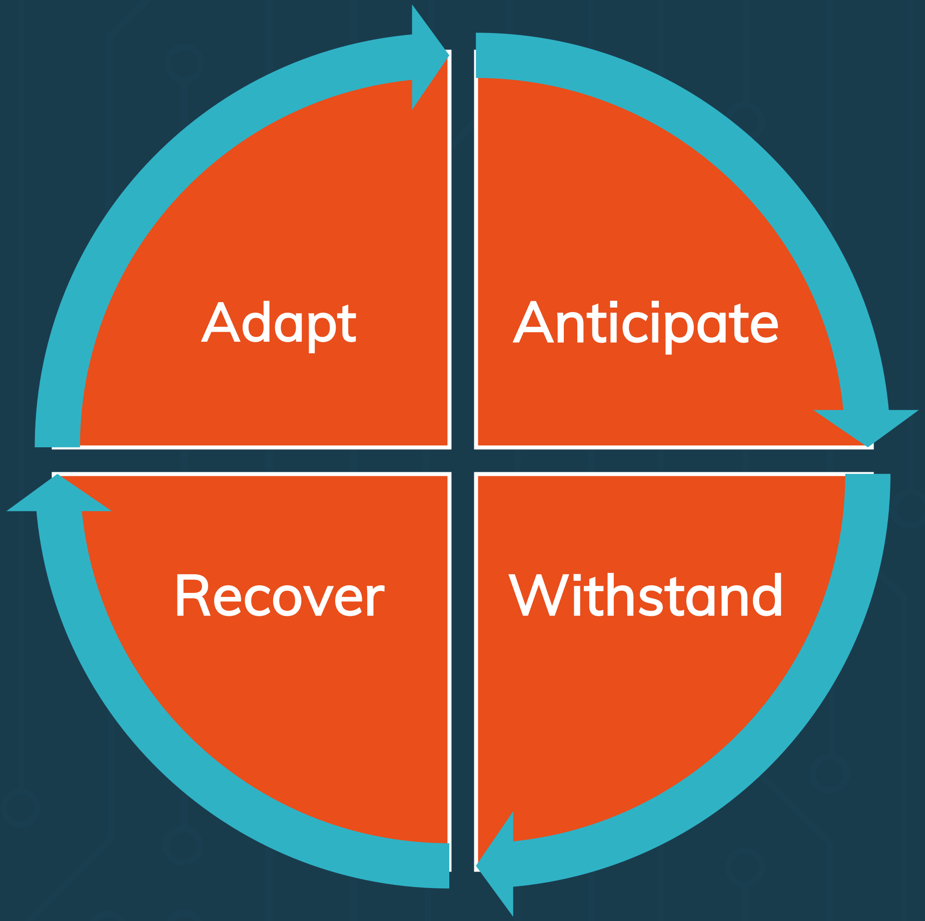
- Plan to recover from attacks, especially destructive attacks (Wiper & Ransomware).



Cybersecurity & Resilience



NIST Cybersecurity Framework



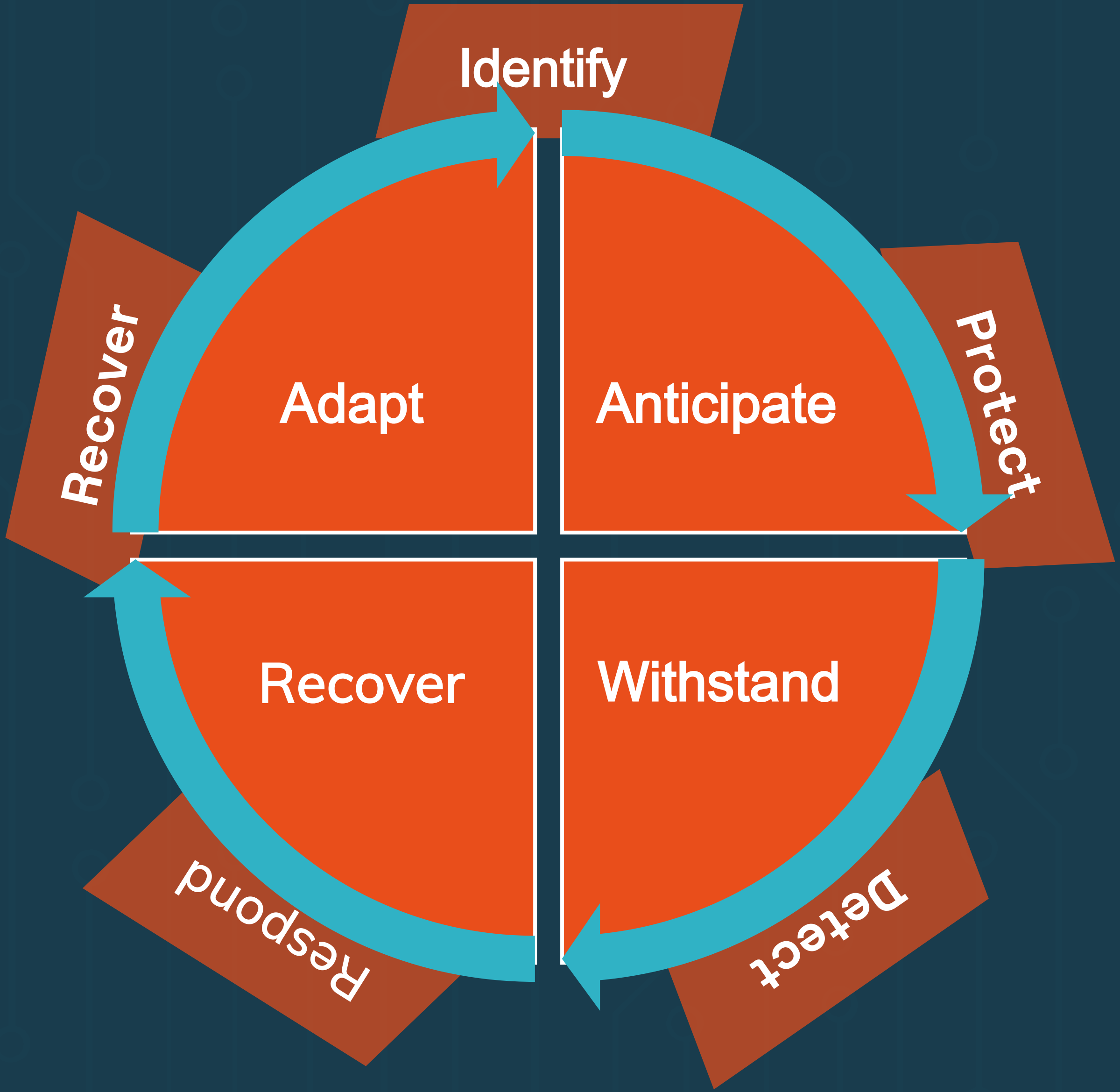
MITRE Cyber Resiliency Engineering Framework

Airiam

Cybersecurity & Resilience

Technology is at the heart of nearly every successful business or organization. Keeping that technology up and running is vital for a company to succeed.

A **resilient company** succeeds when things get tough. Building **resiliency** into your organization is accomplished with the right people, processes, and technology.

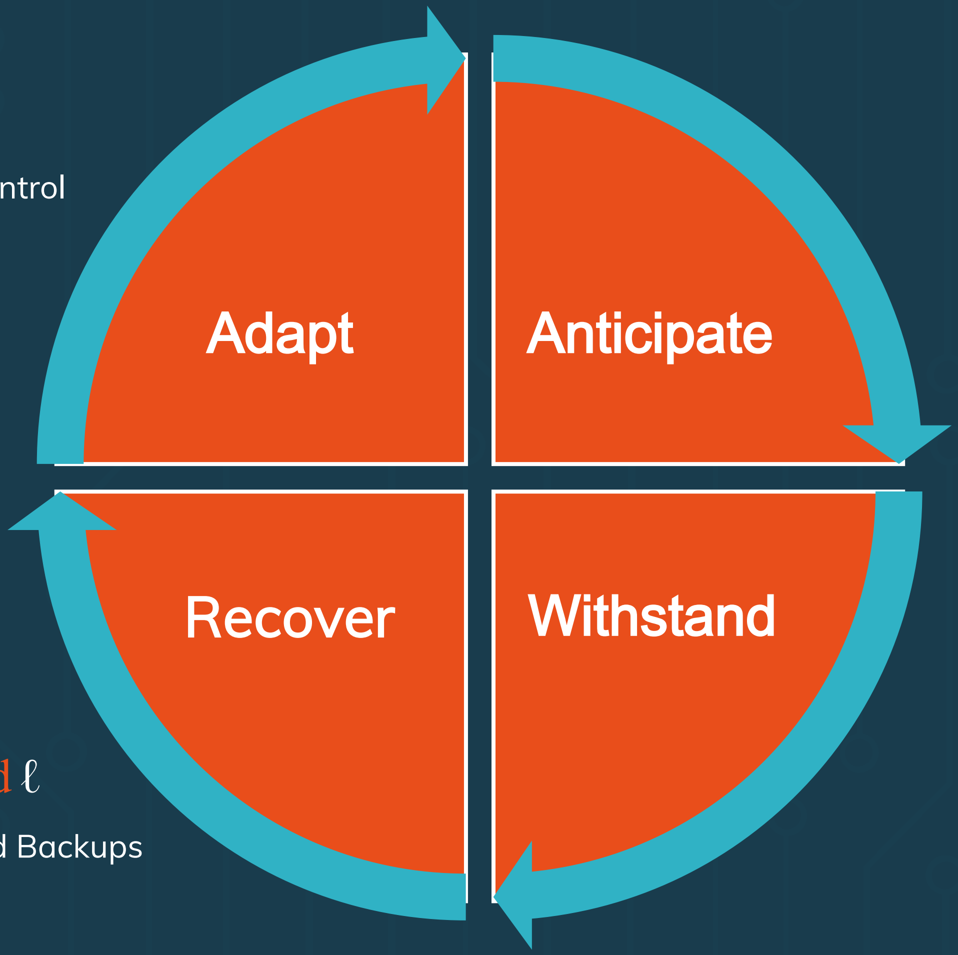


Airiam

Cybersecurity & Resilience

AirCTRLℓ

IT Asset Management and Control



Adapt

Anticipate

Recover

Withstand

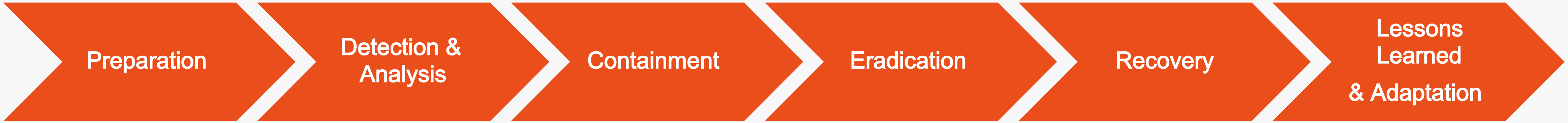
AirGuardℓ

Cybersecurity Protection and Response

AirGapdℓ

Disaster Recovery and Backups

Incident Response Process



The structure that Airiam's AirRescue Incident Response follows is based on the [NIST 800-61 Incident Response Cycle]() and the [SANS Incident Response Process]().

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

SANS

Incident Response
Insights
Managed IT Operations
Managed Cybersecurity