Zero Trust Industry Days 2024

Software Engineering Institute - Carnegie Mellon

Mark Allers
VP of Business Development, Cimcor

CIMTRAK
INTEGRITY, TRUST & RESILIENCY

LEVEL SET

ZTA Is More Than a Buzzword & More Than a Product Suite

- The current administration has executed the appropriate strategy – Zero Trust and Executive Order 14028.

- Zero Trust Architecture (ZTA) means the ENTIRE end-to-end approach to build, configure, deliver, and maintain cybersecurity solutions that claim to offer "Zero Trust"…or better known as the 7 Tenets.

- ZTA encompasses products and the controls that need to be in place to deliver high-quality and dependable solutions.

- Only a small set of technology companies can deliver against the expectations of ZT as defined in Executive Order 14028, M-22-09, and M-21-31.

- ZT is more than just authentication and authorization.

A Multitude of Zero Trust Efforts

- NIST SP 800-207
- White House – EO 14028
- DoD - ZT Capabilities Statement
- CISA - Zero Trust Maturity Model
- DHS - Zero Trust Implementation Strategy
- Institute of Electrical and Electronics Engineers (IEEE)
- Cloud Security Alliance (CSA)
- Information Sharing and Analysis Centers (27 ISACs)
- Software Engineering Institute
- Gartner

Current Thinking vs Zero Trust Principals

Current Thinking

- After a single authentication, users, devices, services, and workloads are trusted to be legitimate and are granted access to a broad range of resources.
- The ubiquitous use of denylists in security tools inherently trusts that all activity is legitimate unless known to be malicious

Zero Trust (800-207)

1. Assume Breach - Organizations should assume at all times that there is a malicious presence inside their environment and implement security controls to minimize the impact.
2. Verify, Don't Trust - Instead of assuming legitimacy, organizations should continuously verify all components within their IT infrastructure to ensure they haven't been compromised.
3. Least Privilege - Once verified, users, devices, and services should be granted the minimum possible access required to complete their function—and for the shortest possible period. This minimizes the potential impact of malicious activity

INTEGRITY is the confidence and certainty that the appropriate controls and compliance requirements are in place and operating as expected to ensure the accuracy, consistency, and trustworthiness of the network, system, user, and application layers throughout its entire life-cycle of operation.

NIST 800-207 (the 7 Tenets)

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the ***INTEGRITY*** and ***SECURITY POSTURE*** of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture (M-21-31)

Tenet #5 Is Ambiguous

- The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
    - No formal “ Integrity “ definition or control(s) specific has ever been established.
    - Security posture is making reference to compliance.
    - Without integrity assurance, how can one ensure that the workload of solutions providing authorization platforms isn’t and can’t be compromised?
    - Tenet 5 is often overshadowed by the topic of authentication and authorization and lost in discussions.

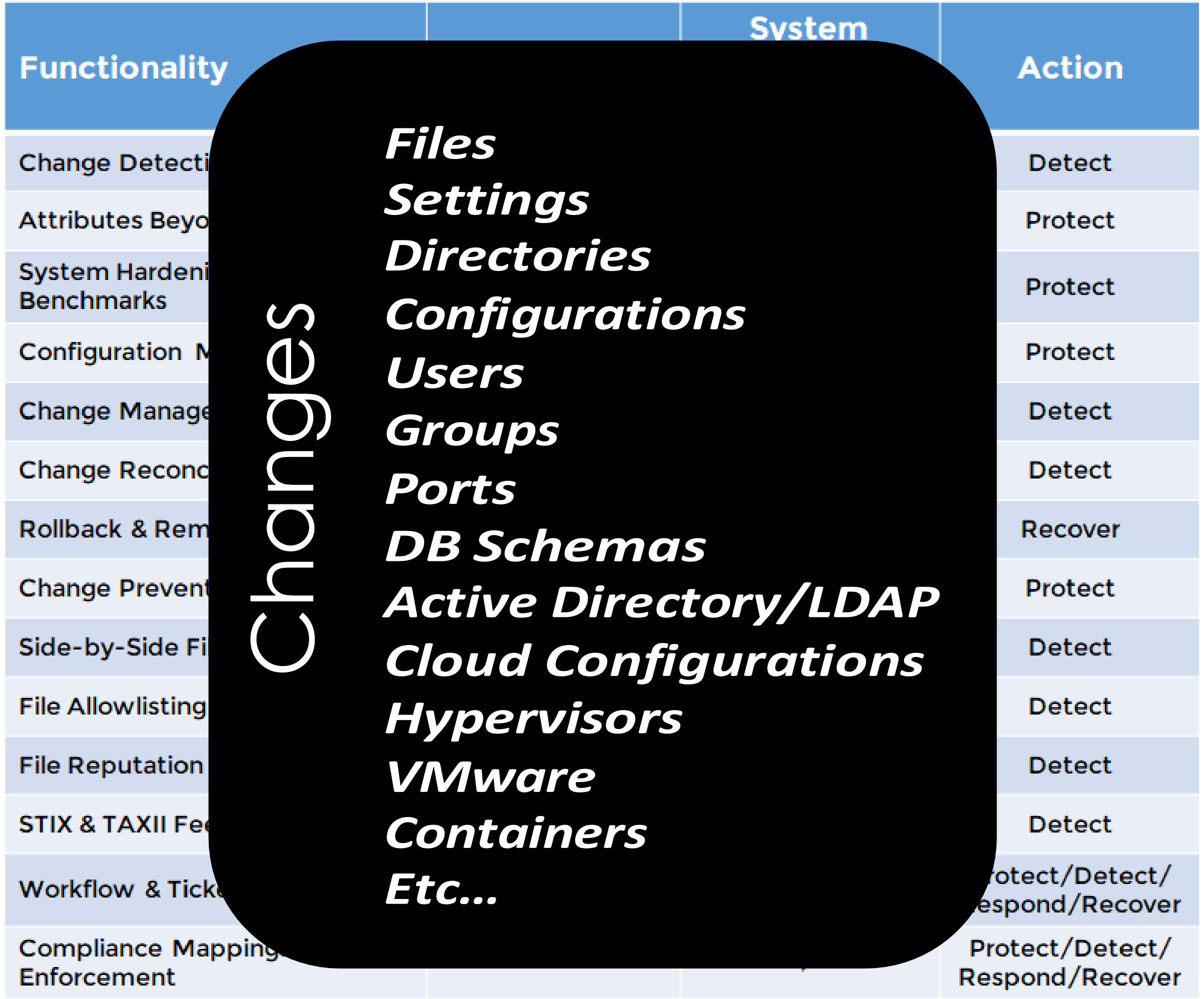
CIMCOR

So…What Is Integrity & Security Posture?

- Integrity is NOT File Integrity Monitoring (FIM)

- Integrity functionality and controls are found in multiple best practice domains and compliance mandates.
- 24% of best practices and compliance controls are integrity controls or
- “Security Posture” refers to the ongoing assurance and attestation that the infrastructure is in a known, authorized, and expected state of operation.

Integrity Is More Than Simply Detecting Change In The Case of FIM!



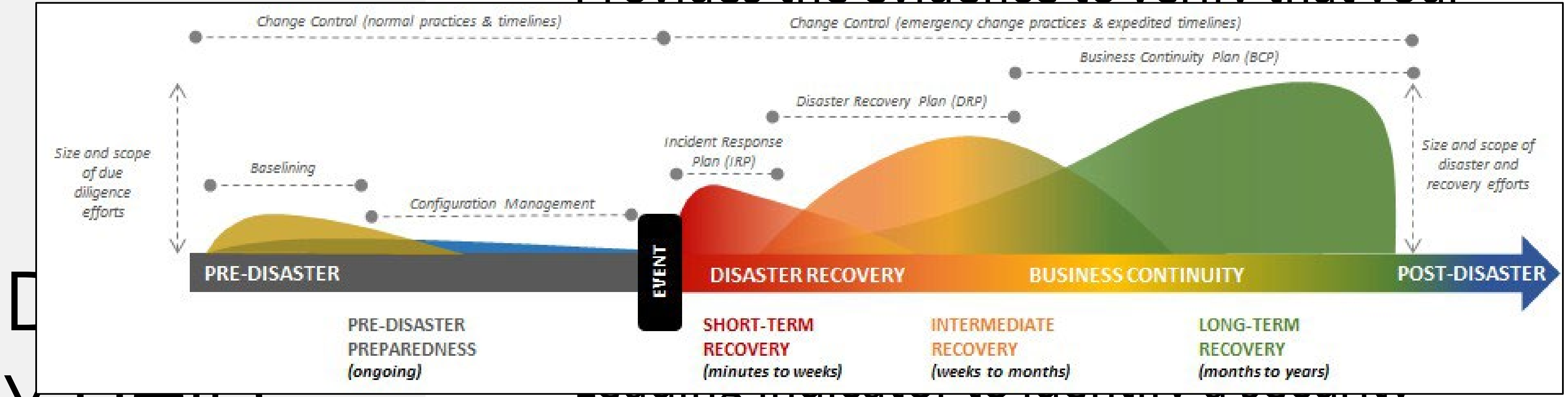
Functionality		System	Action
Change Detecti			Detect
Attributes Beyo			Protect
System Hardeni Benchmarks			Protect
Configuration M			Protect
Change Manage			Detect
Change Reconc			Detect
Rollback & Rem			Recover
Change Prevent			Protect
Side-by-Side Fi			Detect
File Allowlisting			Detect
File Reputation			Detect
STIX & TAXII Fe			Detect
Workflow & Tick			otect/Detect/ espond/Recover
Compliance Mapping Enforcement			Protect/Detect/ Respond/Recover

Changes

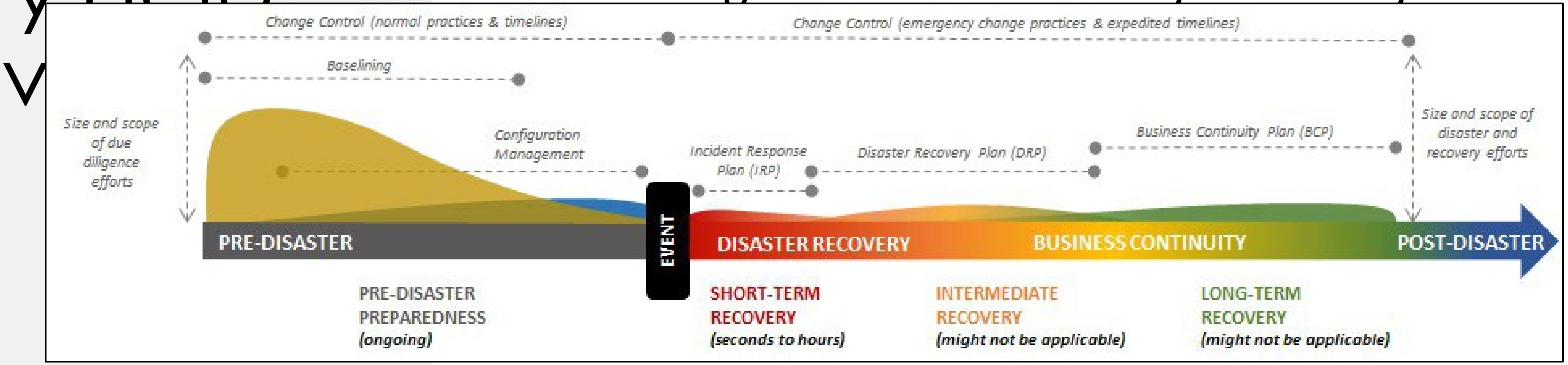
Files
Settings
Directories
Configurations
Users
Groups
Ports
DB Schemas
Active Directory/LDAP
Cloud Configurations
Hypervisors
VMware
Containers
Etc…

What D
Integrity
Solv

- Critical to achieving a Zero Trust framework and Tenet #5.
- Provides the evidence to verify that your


Change Control (normal practices & timelines)
Change Control (emergency change practices & expedited timelines)
Business Continuity Plan (BCP)
Disaster Recovery Plan (DRP)
Incident Response Plan (IRP)
Size and scope of due diligence efforts
Baselining
Configuration Management
Size and scope of disaster and recovery efforts
PRE-DISASTER
EVENT
DISASTER RECOVERY
BUSINESS CONTINUITY
POST-DISASTER
PRE-DISASTER PREPAREDNESS (ongoing)
SHORT-TERM RECOVERY (minutes to weeks)
INTERMEDIATE RECOVERY (weeks to months)
LONG-TERM RECOVERY (months to years)

Leading indicator to identify a security

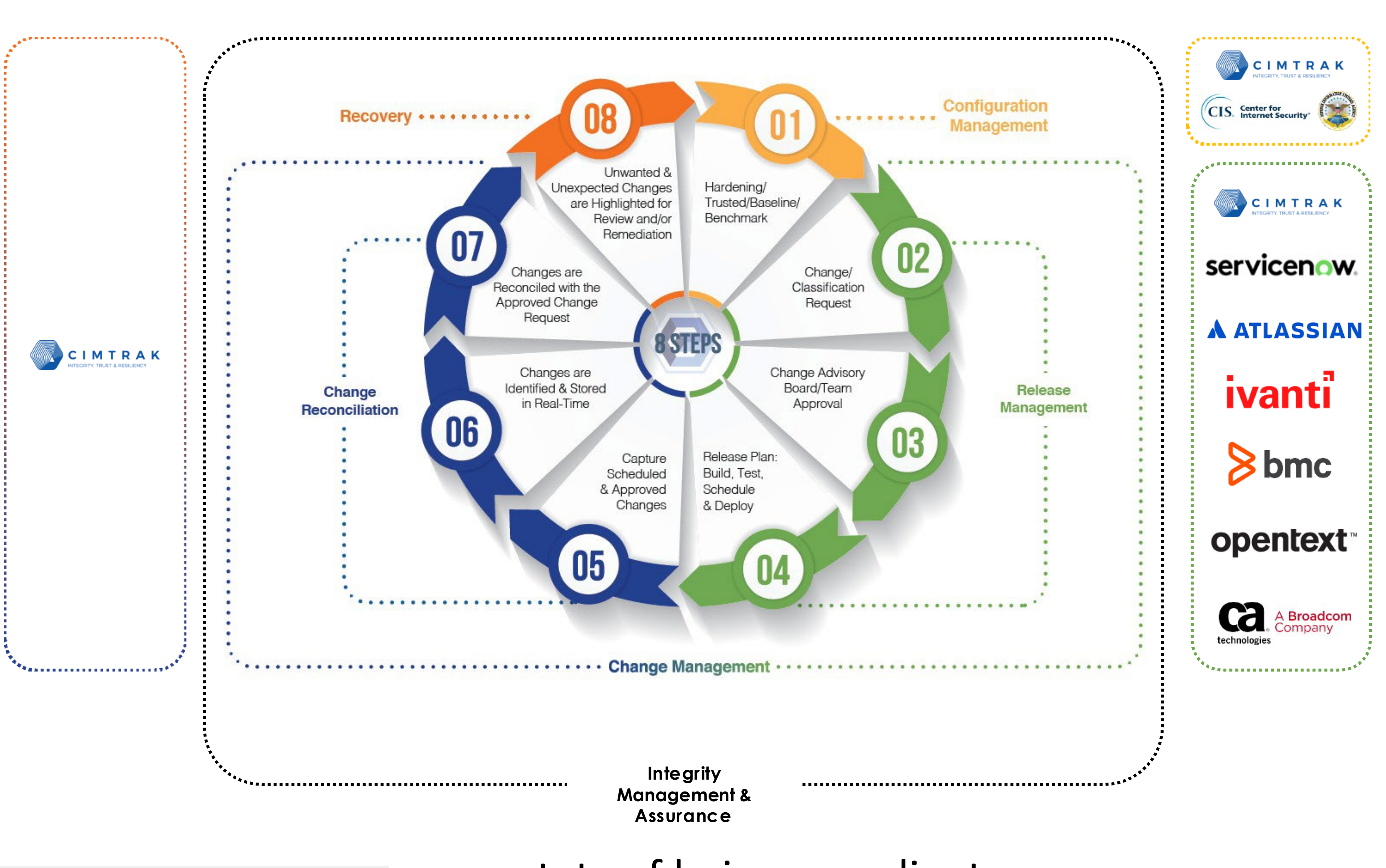

Change Control (normal practices & timelines)
Change Control (emergency change practices & expedited timelines)
Baselining
Size and scope of due diligence efforts
Configuration Management
Incident Response Plan (IRP)
Disaster Recovery Plan (DRP)
Business Continuity Plan (BCP)
Size and scope of disaster and recovery efforts
PRE-DISASTER
EVENT
DISASTER RECOVERY
BUSINESS CONTINUITY
POST-DISASTER
PRE-DISASTER PREPAREDNESS (ongoing)
SHORT-TERM RECOVERY (seconds to hours)
INTERMEDIATE RECOVERY (might not be applicable)
LONG-TERM RECOVERY (might not be applicable)

- Enables a closed-loop process!
- Leading indicator you have drifted from a state of being compliant.

CIMCOR

Wha
Integr
So

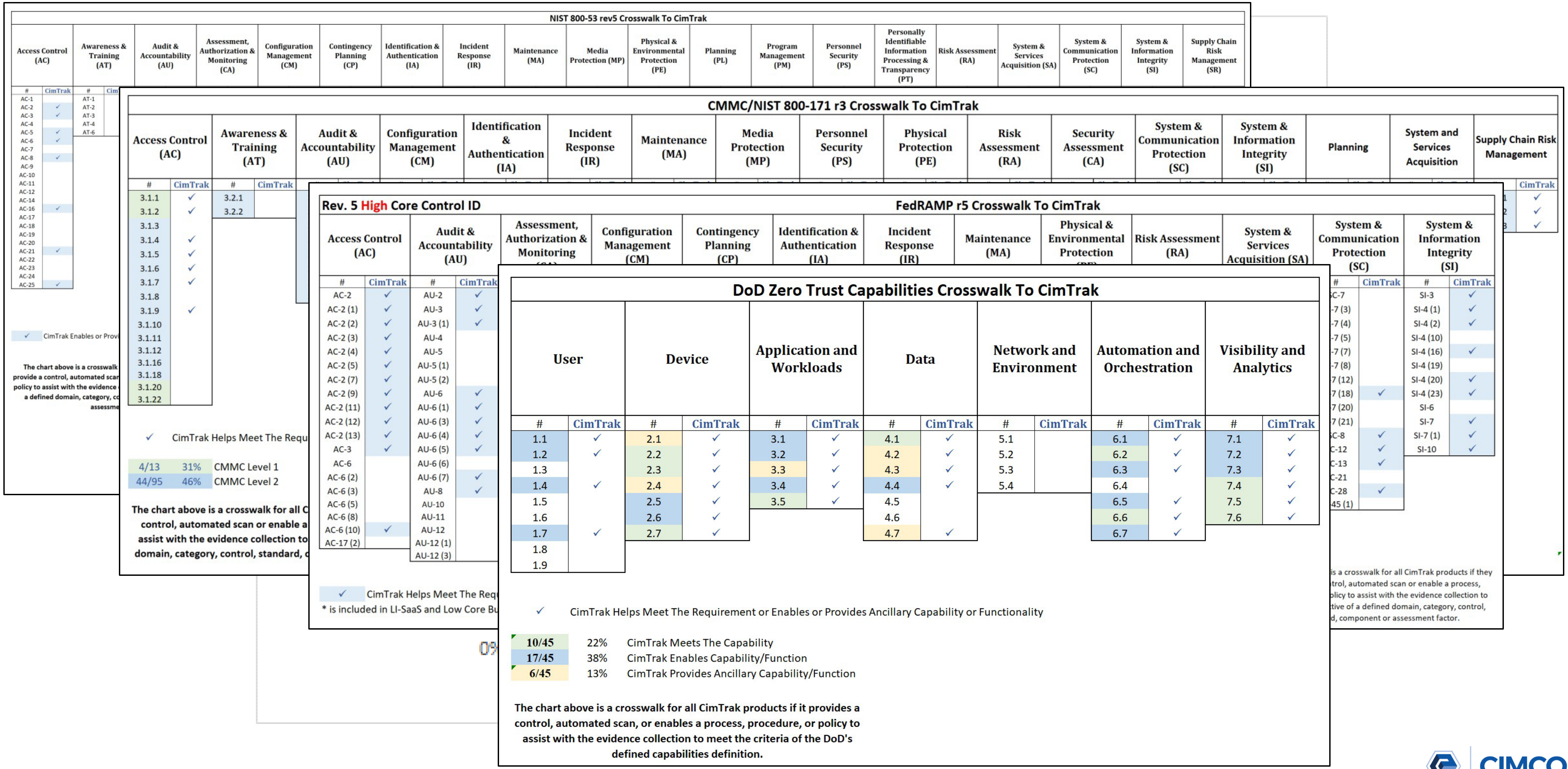
- Critical to achieving a Zero Trust framework.


CIMTRAK INTEGRITY, TRUST & RESILIENCY
Recovery
08
Unwanted & Unexpected Changes are Highlighted for Review and/or Remediation
01
Configuration Management
Hardening/ Trusted/Baseline/ Benchmark
02
Change/ Classification Request
03
Change Advisory Board/Team Approval
Release Management
04
Release Plan: Build, Test, Schedule & Deploy
05
Capture Scheduled & Approved Changes
06
Changes are Identified & Stored in Real-Time
07
Changes are Reconciled with the Approved Change Request
Change Reconciliation
8 STEPS
Change Management
Integrity Management & Assurance
CIMTRAK INTEGRITY, TRUST & RESILIENCY
CIS Center for Internet Security
CIMTRAK INTEGRITY, TRUST & RESILIENCY
servicenow
ATLASSIAN
ivanti
bmc
opentext
ca technologies A Broadcom Company

state of being compliant.

CIMCOR

Compliance - Integrity Controls/Crosswalks



NIST 800-53 rev5 Crosswalk To CimTrak

Access Control (AC)	Awareness & Training (AT)	Audit & Accountability (AU)	Assessment, Authorization & Monitoring (CA)	Configuration Management (CM)	Contingency Planning (CP)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Physical & Environmental Protection (PE)	Planning (PL)	Program Management (PM)	Personnel Security (PS)	Personally Identifiable Information Processing & Transparency (PT)	Risk Assessment (RA)	System & Services Acquisition (SA)	System & Communication Protection (SC)	System & Information Integrity (SI)	Supply Chain Risk Management (SR)

#	CimTrak	#	Cim
AC-1		AT-1	
AC-2	✓	AT-2	
AC-3	✓	AT-3	
AC-4		AT-4	
AC-5	✓	AT-6	
AC-6	✓		
AC-7			
AC-8	✓		
AC-9			
AC-10			
AC-11			
AC-12			
AC-14			
AC-16	✓		
AC-17			
AC-18			
AC-19			
AC-20			
AC-21	✓		
AC-22			
AC-23			
AC-24			
AC-25	✓		

✓ CimTrak Enables or Provi

The chart above is a crosswalk provide a control, automated scan policy to assist with the evidence a defined domain, category, co assessme

CMMC/NIST 800-171 r3 Crosswalk To CimTrak

Access Control (AC)	Awareness & Training (AT)	Audit & Accountability (AU)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Risk Assessment (RA)	Security Assessment (CA)	System & Communication Protection (SC)	System & Information Integrity (SI)	Planning	System and Services Acquisition	Supply Chain Risk Management

#	CimTrak	#	CimTrak
3.1.1	✓	3.2.1	
3.1.2	✓	3.2.2	
3.1.3			
3.1.4	✓		
3.1.5	✓		
3.1.6	✓		
3.1.7	✓		
3.1.8			
3.1.9	✓		
3.1.10			
3.1.11			
3.1.12			
3.1.16			
3.1.18			
3.1.20			
3.1.22			

✓ CimTrak Helps Meet The Requ

4/13	31%	CMMC Level 1
44/95	46%	CMMC Level 2

The chart above is a crosswalk for all C control, automated scan or enable a assist with the evidence collection to domain, category, control, standard, c

Rev. 5 High Core Control ID

FedRAMP r5 Crosswalk To CimTrak

Access Control (AC)	Audit & Accountability (AU)	Assessment, Authorization & Monitoring (CA)	Configuration Management (CM)	Contingency Planning (CP)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Physical & Environmental Protection (PE)	Risk Assessment (RA)	System & Services Acquisition (SA)	System & Communication Protection (SC)	System & Information Integrity (SI)

#	CimTrak	#	CimTrak
AC-2	✓	AU-2	✓
AC-2 (1)	✓	AU-3	✓
AC-2 (2)	✓	AU-3 (1)	✓
AC-2 (3)	✓	AU-4	
AC-2 (4)	✓	AU-5	
AC-2 (5)	✓	AU-5 (1)	
AC-2 (7)	✓	AU-5 (2)	
AC-2 (9)	✓	AU-6	✓
AC-2 (11)	✓	AU-6 (1)	✓
AC-2 (12)	✓	AU-6 (3)	✓
AC-2 (13)	✓	AU-6 (4)	✓
AC-3	✓	AU-6 (5)	✓
AC-6		AU-6 (6)	
AC-6 (2)		AU-6 (7)	✓
AC-6 (3)		AU-8	✓
AC-6 (5)		AU-10	
AC-6 (8)		AU-11	
AC-6 (10)	✓	AU-12	
AC-17 (2)		AU-12 (1)	
		AU-12 (3)	

#	CimTrak	#	CimTrak
C-7		SI-3	✓
-7 (3)		SI-4 (1)	✓
-7 (4)		SI-4 (2)	✓
-7 (5)		SI-4 (10)	
-7 (7)		SI-4 (16)	✓
-7 (8)		SI-4 (19)	
7 (12)		SI-4 (20)	✓
7 (18)	✓	SI-4 (23)	✓
7 (20)		SI-6	
7 (21)		SI-7	✓
C-8	✓	SI-7 (1)	✓
C-12	✓	SI-10	✓
C-13	✓		
C-21			
C-28	✓		
45 (1)			

✓ CimTrak Helps Meet The Req

* is included in LI-SaaS and Low Core Bu

is a crosswalk for all CimTrak products if they trol, automated scan or enable a process, licy to assist with the evidence collection to tive of a defined domain, category, control, d, component or assessment factor.

DoD Zero Trust Capabilities Crosswalk To CimTrak

User		Device		Application and Workloads		Data		Network and Environment		Automation and Orchestration		Visibility and Analytics	
#	CimTrak	#	CimTrak	#	CimTrak	#	CimTrak	#	CimTrak	#	CimTrak	#	CimTrak
1.1	✓	2.1	✓	3.1	✓	4.1	✓	5.1		6.1	✓	7.1	✓
1.2	✓	2.2	✓	3.2	✓	4.2	✓	5.2		6.2	✓	7.2	✓
1.3		2.3	✓	3.3	✓	4.3	✓	5.3		6.3	✓	7.3	✓
1.4	✓	2.4	✓	3.4	✓	4.4	✓	5.4		6.4		7.4	✓
1.5		2.5	✓	3.5	✓	4.5				6.5	✓	7.5	✓
1.6		2.6	✓			4.6				6.6	✓	7.6	✓
1.7	✓	2.7	✓			4.7	✓			6.7	✓		
1.8													
1.9													

✓ CimTrak Helps Meet The Requirement or Enables or Provides Ancillary Capability or Functionality

10/45	22%	CimTrak Meets The Capability
17/45	38%	CimTrak Enables Capability/Function
6/45	13%	CimTrak Provides Ancillary Capability/Function

The chart above is a crosswalk for all CimTrak products if it provides a control, automated scan, or enables a process, procedure, or policy to assist with the evidence collection to meet the criteria of the DoD's defined capabilities definition.

CIMCOR

amazon web services

Google Cloud

Microsoft Azure

General Governance & Definition

1. All data sources and computing services are considered resources.

Encryption

2. All communication is secured regardless of network location.

3. Access to individual enterprise resources is granted on a per-session basis.

4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.

paloalto NETWORKS

cisco

appgate

netskope

iboss

CIMCOR

tripwire

5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.

okta

Centrify

Microsoft

onelogin by ONE IDENTITY

6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

splunk>

IBM Radar

SECURONIX

Microsoft

CROWDSTRIKE

7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture (M-21-31 & M-22-09)

servicenow

CIMCOR

bmc

Workflow Management

Demos

Integrity Coupled With Authorization

- CimTrak/Zscaler- Continuous ATO of Systems - Benchmark/Audit Score Triggers
- CimTrak/Zscaler - Continuous ATO of Systems - Integrity Triggers
- CimTrak Monitoring ZIA Configuration Changes
- CimTrak Monitoring ZPA Configuration Changes

Q&A

Mark Allers
VP of Business Development – Cimcor
Allers.Mark@cimcor.com