CIMCOR

IEC 62443 OVERVIEW

COMPANY INFORMATION

CIMCOR, INC.
Founded – 1997
Corporate Headquarters
8488 Georgia St Suite A
Merrillville, IN 46410
Phone: 219-736-4400
Fax: 219-736-4401
Website: www.cimcor.com
Email: sales@cimcor.com

DUNS Number: 013258426
Unique Entity ID: ELA7MJUVJ6Z5
Cage Code: 1K2L8
Status: Minority Owned Small Business
NAICS 511210

CIMTRAK CONTRACT VEHICLES

GSA Schedule 70
NASA SEWP V
CDM
DHS FirstSource II
Others

CIMTRAK CERTIFICATIONS

CDM Approved Products List
Common Criteria EAL 4 w/FLR
NIST FIPS 140-2 Level 2
Army Information Assurance (APL)
Section 508 of the Rehabilitation Act
IPv6 Compatible – Tested Ft. Huachuca

CIMTRAK COMPLIANCE

FISMA, NIST 800-53 and 800-137
Continuous Diagnostics and Mitigation (CDM)
Cybersecurity Maturity Model Certification (CMMC)
PCI-DSS
ISO 27001 and 27002
COBIT
HIPAA/HITECH
GLBA
Dozens of others

CIMTRAK

The CimTrak Integrity Suite is a comprehensive solution that directly facilitates compliance with IEC 62443 and a wide range of other industry standards, such as CIS Controls Framework, NIST CSF, NERC CIP, FISMA (800-53), and many others.

The IEC 62443 4-2 standard defines foundational requirements for each security level, with increasing criticality and expectations as the level rises. In particular, CimTrak directly impacts the following foundational requirements:

FR1 Identification and Authentication Control (IAC)
FR3 System Integrity (SI)
FR6 Timely Response to Events (TRE)
FR7 Resource Availability (RA)

CimTrak alignment to IEC62443 security levels SL1 to SL4 enables functionality for organizations with no attack skills to the most sophisticated nation-state activity.

The CimTrak Integrity Suite provides unique cybersecurity capabilities that are well-aligned with the requirements of IEC 62443 and other relevant industry standards. This enables robust and tailored cybersecurity solutions specific to the needs of critical infrastructure sectors.

CIMTRAK DOES THIS BY IMPLEMENTING IEC FOUNDATIONAL SECURITY CONTROLS THAT:

1. Facilitate configuration management and integrity checks
2. Identify changes by authorized and unauthorized personnel
3. Enable continuous monitoring requirements
4. Provide incident response and remediation capabilities
5. Deliver continuous compliance and audit reports

SECURITY CONTROLS IMPLEMENTATION CimTrak implements the necessary security controls that adhere to the requirements outlined in IEC 62443 4-2. These controls cover aspects such as access control, change management, incident response, and network security, ensuring that critical infrastructure systems are adequately protected against cyber threats.

CONFIGURATION & CHANGE MANAGEMENT CimTrak facilitates configuration management best practices recommended by IEC 62443 by providing features for identifying, tracking and managing unauthorized changes to critical systems.

AUTHORIZED CHANGE(S) CimTrak provides the capability of not only identifying who or what is making changes, but can also provide the necessary controls and integrity to ensure your authentication and access tools are not compromised.

CONTINUOUS MONITORING CimTrak offers continuous monitoring capabilities that are essential for maintaining the security and integrity of industrial control systems (ICS) as mandated by IEC 62443. CimTrak continuously monitors for unauthorized changes and security incidents, helping organizations detect and respond to cyber threats in real-time. This includes monitoring changes to software, firmware, and hardware configurations to prevent unauthorized modifications that could compromise system security and integrity posture.

INCIDENT RESPONSE CimTrak supports incident response procedures outlined in IEC 62443 by providing detailed insights into security incidents and unauthorized changes. In the event of a security incident or breach, CimTrak can recover and reconstitute to a previously known and secure state after disruption or failure. By enabling rapid incident detection and response, CimTrak helps you and your organization minimize the impact of cyber-attacks and maintain operational resilience.

AUDIT AND COMPLIANCE REPORTING CimTrak generates comprehensive reports and assessments that can be used to demonstrate compliance with IEC 62443 and dozens of other industry standards. These reports provide evidence of security controls implementation, continuous monitoring, and incident response activities, enabling a trusted, secure, and resilient infrastructure.

IEC 62443

Identification & Authentication Control (IAC)		Use control (UC)		System integrity (SI)		Data confidentiality (DC)		Restricted data flow (RDF)		Timely response to events (TRE)		Resource availability (RA)	
#	CimTrak	#	CimTrak	#	CimTrak	#	CimTrak	#	CimTrak	#	CimTrak	#	CimTrak
CR 1.1	✓	CR 2.1	✓	CR 3.1		CR 4.1	✓	CR 5.1		CR 6.1	✓	CR 7.1	
CR 1.2	✓	CR 2.2		CR 3.2	✓	CR 4.2		CR 5.2		CR 6.2	✓	CR 7.2	
CR 1.3	✓	CR 2.3		CR 3.3	✓	CR 4.3	✓	CR 5.3				CR 7.3	✓
CR 1.4	✓	CR 2.4		CR 3.4	✓			CR 5.4				CR 7.4	✓
CR 1.5	✓	CR 2.5		CR 3.5								CR 7.5	
CR 1.6		CR 2.6		CR 3.6	✓							CR 7.6	✓
CR 1.7	✓	CR 2.7		CR 3.7	✓							CR 7.7	✓
CR 1.8	✓	CR 2.8	✓	CR 3.8								CR 7.8	✓
CR 1.9		CR 2.9		CR 3.9	✓								
CR 1.10		CR 2.10	✓	CR 3.10	✓								
CR 1.11		CR 2.11	✓	CR 3.11									
CR 1.12	✓	CR 2.12		CR 3.12	✓								
CR 1.13		CR 2.13		CR 3.13	✓								
CR 1.14				CR 3.14	✓								

✓ CimTrak Helps Meet The Requirement or Enables or Provides Ancillary Capability or Functionality
31/58 | **53%** CimTrak meets the capability

The chart above is a crosswalk for all CimTrak products if they provide a control, automated scan or enable a process, procedure or policy to assist with the evidence collection to meet the objective of a defined domain, category, control, standard, component or assessment factor.

SUPPORTED PLATFORMS

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS XP, Vista, 7, 8, 10, 11, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise, Windows 11 IoT Enterprise
WINDOWS SERVER 2003, 2008, 2012, 2016, 2019, 2022
LINUX Alma, Amazon, ARM, CentOS, ClearOS, Debian, Fedora, Oracle, Red Hat, Rocky, SUSE, Ubuntu, others
FreeBSD 12, 13
SUN SOLARIS x86/SPARC
MacOS 5, 6, 7, 8, 9, 10, 11
HP-UX Itanium, PA-RISC
AIX 6.1, 7.1, 7.2, 7.3

Windows Parameters Monitored

FILE ADDITIONS, DELETIONS, MODIFICATIONS, AND READS
ATTRIBUTES Compressed, hidden, offline, read-only, archive, reparse point, Creation time, DACL information, Drivers, File opened/read, File Size, File type, Group security information, Installed software, Local groups, Local security policy, Modify time, Registry (keys and values), Services, User groups

UNIX Parameters Monitored

FILE ADDITIONS, DELETIONS, AND MODIFICATIONS
Access Control List, Attributes: read-only, archive, Creation time, File Size, File type, Modify time, User and Group ID

Supported Platforms CimTrak For Network Devices

Arista, Aruba, Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Palo Alto, Sophos, others

Supported Platforms CimTrak For Databases

IBM DB2, Microsoft SQL Server, MySQL, Oracle
PARAMETERS MONITORED Default Rules, Full-text indexes, Functions, Groups, Index definitions, Roles, Stored Procedures, Table definitions, Triggers, User defined data types, Users, Views

Supported Hypervisors

Microsoft Hyper-V, VMware ESXi 3x, 4x, 5x, 6x, 7x

Supported Cloud Platforms

Amazon AWS, Google Cloud, Microsoft Azure

Supported Container & Orchestration Integrations

Amazon Elastic Kubernetes Service (EKS), Docker, Docker Enterprise, Google Kubernetes Engine (GKE), Kubernetes, Podman

Supported Ticketing Integrations

Atlassian Jira, BMC Remedy, CA ServiceDesk, ServiceNow

Supported SIEM Integrations

IBM QRadar, LogRhythm, McAfee Event Security Manager, Microfocus Arcsight, Splunk, others

Supported Under CimTrak's Trusted File Registry™

CentOS 7, Microsoft Windows 7, 8, 8.1, 10, 11, XP, 2003, 2008, 2012, 2016, 2019, 2022, Oracle Linux 7, Redhat Enterprise Linux 7

SUPPORTED BENCHMARKS

ALIBABA
ALMA
AMAZON ELASTIC KUBERNETES
AMAZON LINUX
APACHE
APPLE MAC OS
AZURE
CENTOS
CISCO Firewall, IOS
DEBIAN
DISTRIBUTION INDEPENDENT
FEDORA
GOOGLE Chrome, Container, Kubernetes
IBM
KUBERNETES
MICROSOFT Access, Edge, Excel, IIS, Intune, Office, PowerPoint, SharePoint, SQL, Windows, Windows Server, Word
MONGODB
NGINX
ORACLE Cloud, Database, Linux, MySQL
PALO ALTO
POSTGRESQL
RED HAT
RHEL8
ROCKY
ROS
SUSE
UBUNTU LXD, Linux
VMWARE

CIMCOR

Cimcor develops innovative, next-generation, file integrity monitoring software. The CimTrak Integrity Suite monitors and protects a wide range of physical, network, cloud, and virtual IT assets in real-time, while providing detailed forensic information about all changes. Securing your infrastructure with CimTrak helps you get compliant and stay that way.

REQUEST A DEMO

CIMTRAK