CIMCOR

Capability Statement/Executive Summary

COMPANY INFORMATION

CIMCOR, INC.
Founded – 1997
Corporate Headquarters
8252 Virginia Street, Suite C
Merrillville, IN 46410
Phone: 219-736-4400
Fax: 219-736-4401
Website: www.cimcor.com
Email: sales@cimcor.com

DUNS Number: 013258426
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
Pv6 Compatible – Tested Ft. Huachuca

CIMTRAK CERTIFICATIONS

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

CIMCOR Overview

Cimcor is the leading provider of System Integrity Assurance with our award winning CimTrak Integrity Suite that protects a wide range of physical, network, cloud, and virtual IT assets in real-time. CimTrak provides detailed analysis, evidence and automated workflow that enforces an unprecedented security posture, ensures operational availability, stops zero-day attacks, detects unwanted/unexpected/unauthorized changes, and achieves and maintains continuous compliance in a simple and cost-effective manner.

This is all achieved through the establishment and implementation of foundational controls of configuration management, hardening, change control, whitelisting, and integrity assurance both on-premise and cloud environments. When unwanted, unauthorized, or malicious activity is detected, CimTrak can also enable a resilient infrastructure through its manual or automatic roll-back and remediation capabilities. For those files, directories and configurations that should never change, CimTrak can prevent changes regardless of one's admin privileges.

CimTrak Product Summary

Detecting change doesn't give you integrity...it's all the collective functionality that surrounds the trigger or identification of change that enables you to introduce the concept of System Integrity Assurance and ensure the accuracy and consistency of data throughout its entire life-cycle of operation.

AT A GLANCE

Delivering Integrity, Trust and Resiliency

Foundational Security Controls

» The Only Self-Contained System Integrity Assurance Platform and Workflow Solution in the Market

» Real-Time Detection, Analysis and Response of Change and Configuration Mgmt.

» Roll-Back and Remediation

» MTTI and MTTC Measured in Seconds

» Broad Range of Integrations

» Aligns w/ All Major Best Practice Frameworks

Compliance & Audit

» Continuous Compliance with a Proven Workflow and Repeatable Process

» Large Compliance Library

» CIS Benchmarks/DISA STIGs mappings

» Remediation Guidelines for Failed Systems

» Comprehensive Audit Reports

» Mitigate and Eliminate Cost of Capital Resources

Operational Excellence

» Enforce Standard Configurations

» Change Audit and Reconciliation

» Improved MTTD, MTTR & MTBF

» RTO/RPO Enablement

» Change and Configuration Workflow Platform

» Software Supply Chain Risk Mitigation

» Broad Range of Integrations

Problems CimTrak Is Solving for Customers

» Ability to identify unauthorized changes on critical systems within my environment

» Ability to roll-back and remediate unwanted changes to critical systems

» Ability to stop or prevent unauthorized changes to critical systems

» Ability to comply with regulatory requirements regarding file integrity monitoring (FIM)

» Ability to drastically reduce auditing cost of preparation, inspection, assessment, and reporting

» Ability to reconcile and curate authorized changes on critical systems

» Ability to manage the change control process across my entire enterprise

» Ability to set up security policies & procedures and enforce them for critical system files

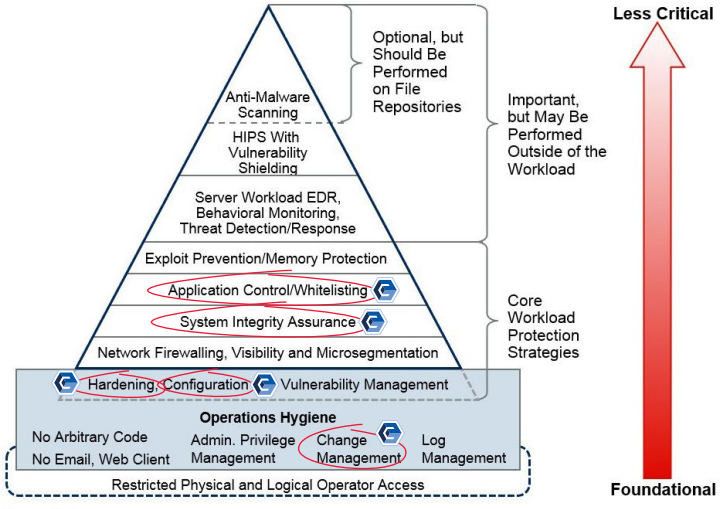
» Ability to digest and analyze real-time threat intelligence feeds (STIX and TAXII)

» Ability to whitelist files for risk assessment and mitigation

» Ability to leverage CIS Benchmarks and DISA STIGs to create a root of trust

Gartner Perspective – Cloud Workload Protection Platform (CWPP)

CWPP Controls Hierarchy



Source: Gartner

= CimTrak

Return on Investment

CimTrak and its ROI can be summarized through cost avoidance/ reduction and risk mitigation while effectively delivering a more robust, secure, and manageable System Integrity Assurance solution.

Security Risk

Reduce the overall security risk – CimTrak's core value proposition is to suppress good change and only highlight unknow, unauthorized or unexpected changes to your infrastructure. This 1) reduces the total number of incidents/alerts 2) provides a prescriptive guidance as how to resolve problematic changes or configurations driving the mean time to resolve down to seconds and 3) reduces the number of analysts needed to operate and manage a fully encompassing system integrity assurance solution.

Security Cost

Reduce the Mean Time to Resolve – CimTrak's core value proposition is to suppress good change and only highlight unknow, unauthorized or unexpected changes to your infrastructure. This reduces 1) the total number of incidents/alerts 2) a prescriptive guidance as how to resolve problematic changes or configurations driving the mean time to resolve down to seconds and 3) the number of analysts to needed to operate and manage a fully encompassing system integrity assurance solution.

Audit & Compliance Cost

Decrease the average time to assess or complete an audit – CimTrak can accomplish this through its innovative technology where compliance scans can be scheduled daily. Where previously, IT professionals and auditors would go through a rigorous process of acquiring, analyzing, and reporting data, only to be outdated the following day. If a particular compliance requirement failed, CimTrak will provide prescriptive guidance how to immediately fix and resolve.

Why Should You Use CimTrak?

- Provides real-time system integrity assurance for your entire infrastructure
- Easy to install, configure and operate
- Suppresses +95% of traditional change noise
- Mean-Time-To-Identify (MTTI) and Mean-Time-To-Contain (MTTC) is measured in seconds
- Integrated ticketing system to enable a comprehensive change management and compliance workflow process
- Manually or automatically roll-back and remediate changes to previous state(s)
- Prevent file changes completely
- Integrated benchmarks from CIS and DISA STIGs for baseline configurations and system hardening
- Compliance scoring and policy groupings allowing compliance requirements to be illustrated as a single test with remediation instructions
- Most cost-effective integrity platform in the market

Supported Platforms

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS: XP, Vista, 7, 8, 10, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise
WINDOWS SERVER: 2003, 2008, 2012, 2016, 2019
LINUX: Amazon, CentOS, ClearOS, Debian, Fedora, Oracle
SUN SOLARIS: x86, SPARC Red Hat, SUSE, Ubuntu, others
MAC: Intel, Power PC
HP-UX: Itanium, PA-RISC
AIX

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

Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Netgear, NetScreen, Palo Alto, Others

Supported Platforms CimTrak For Databases

Oracle, IBM DB2, Microsoft SQL Server
MySQL 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

Google Cloud, Amazon AWS, Microsoft Azure

Supported Container & Orchestration Integrations

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

Supported Ticketing Integrations

CA ServiceDesk, Atlassian Jira, ServiceNow, BMC Remedy

Supported SIEM Integrations

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

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.