CIMCOR

SOLUTION BRIEF

Securing, Meeting, and Maintaining NERC Critical Infrastructure Compliance (CIP)

AT A GLANCE

CHANGE AND CONFIGURATION CONTROL

Instantly detect all changes to your critical systems and know who is making them, how they are being made, and where they originate.

PREVENT INTERNAL AND EXTERNAL THREATS

From unsignatured malware to fat-finger errors, CimTrak has you covered. CimTrak can even protect custom applications or unpatchable systems.

COMPLETE REPORTING FOR AUDITS

CimTrak provides a wide variety of reports and seamlessly integrates with all major SIEM and alarm systems.

CIMTRAK By CIMCOR

NERC is one of the most critical entities that is responsible for reducing overall risk and threat to the Bulk Electrical System (BES) in eight provinces of Canada, one state in Mexico and every state in the United States. Its mission is to create and enforce standards that drive reliability, resiliency, and security to one of the most critical yet fragile and antiquated IT infrastructures. As hacking continues to increase and the bullseye shifts towards the energy sector, security best practices and compliance requirements are becoming paramount as IT infrastructure plays a key role in ensuring that electric power is delivered reliably.

The North American Electric Reliability Corporation (NERC) has developed a set of standards designed to ensure that “Critical Cyber Assets” are secure and functioning properly. Ensuring compliance with these standards is critical in order to minimize the overall security and operational risk as well as avoid costly penalties for non-compliance.

CimTrak System Integrity Assurance platform provides the detective controls that help you meet several key NERC-CIP requirements and covers a broad range of critical servers, SCADA systems, workstations, and network devices found within the energy production environment. CimTrak keeps your IT environment secure and in a known and trusted state of integrity through a process of continuously managing the configuration and changes from a trusted baseline from either CIS Benchmarks or DISA STIGs. If unknown, unwanted or unexpected change causes drift from a trusted baseline (either malicious or accidental), CimTrak has the ability to automatically or manually restore those changes. Furthermore, CimTrak can also completely deny and prevent changes from happening. CimTrak has assembled these detective controls into a simple workflow process that enforces a closed-loop change control best practices.

CIMTRAK'S SYSTEM INTEGRITY ASSURANCE PLATFORM INCLUDES:

- CIS or a DISA STIG benchmark support and integration.
- Real-Time change monitoring and detection to identify all changes within the environment.
- Collection and storage of forensic evidence and detail for every change, including the source IP, user, time, and process.
- Reconciliation and curation between observed changes against authorized/approved changes.
- Categorization (i.e. whitelist/allowlist and blacklist/deny list) of changes as good, bad, or unknown.
- Alerting for unknown changes that require human intervention.
- Prevention of disallowed changes to critical assets.
- Roll back and remediation (A.K.A. 'self-healing' or resiliency) of disallowed changes to other asset groups.
- Baseline updates to include new file hashes and configurations categorized as good.
- Embedded ticketing functionality to enable workflow automation and control or integration with traditional ITSM tools
- Integrates with a wide variety of Security Information Event Management (SIEM) technologies

CIMTRAK CIP CROSSWALK

The chart below 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.

NATIONAL ELECTRIC RELIABILITY COUNCIL (NERC) CIP CROSSWALK TO CIMTRAK

	CIP-005	CIP-007	CIP-008	CIP-009	CIP-010
TITLE	ELECTRONIC SECURITY PERIMETER(S)	SYSTEMS SECURITY MANAGEMENT	INCIDENT REPORTING & RESPONSE PLANNING	RECOVERY PLANS FOR BES CYBER ASSETS	CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENTS
Description	• Electronic /Security Perimeter • Interactive Remote Access	• Ports and Services • Security Patch Management • Malicious Code Prevention • Security Event Monitoring • System Access Control	• Cyber Security Incident Response Plan Specifications • Cyber Security Incident Response Plan Implementation and Testing	• Recovery Plan Specifications • Recovery Plan Implementation and Testing • Recovery Plan Review, Update and Communication	• Configuration Change Management • Configuration Monitoring • Vulnerability Assessment • Transient Cyber Assets and Removable Media
CIP ID	# CimTrak CIP-005-5-R1 ✓ CIP-005-5-R2	# CimTrak CIP-007-6-R1 ✓ CIP-007-6-R2 ✓ CIP-007-6-R3 ✓ CIP-007-6-R4 ✓ CIP-007-6-R5 ✓	# CimTrak CIP-008-5-R1 ✓ CIP-008-5-R2 ✓ CIP-008-5-R3	# CimTrak CIP-009-6-R1 ✓ CIP-009-6-R2 CIP-009-6-R3	# CimTrak CIP-010-2-R1 ✓ CIP-010-2-R2 ✓ CIP-010-2-R3 ✓ CIP-010-2-R4

✓ CimTrak Provides a Solution

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.

SAVINGS AT A GLANCE

An example of a current customer with a before and after calculation of man hours to produce the exact same compliance report(s) as they pertain to CIP-005, CIP-007, CIP-008, CIP-009, and CIP-010 has a 98.2% savings on working capital when using CimTrak.

OLD METHOD	WITH CIMTRAK
2 engineers once a month	1 engineer once a month
24 hours per engineer (48 hours of man-time per month)	1 hour per engineer (1 hour of man-time per month)
48 x 12 = 675 man hours per year	1 x 12 = 12 man hours per year
675 x $65/hr/engineer = $43,875	12 x $65/hr/engineer = $780

CIP ID	REQUIREMENTS	HOW CIMTRAK HELPS
CIP-005 **ELECTRONIC/ SECURITY PERIMETER**	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].	CimTrak can monitor a wide variety of network devices, including firewalls and routers for changes that can compromise critical IT environments. This allows instant notification of changes that can allow unauthorized access past the security perimeter.
	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	
CIP-007 **SYSTEM SECURITY MANAGEMENT** **PORTS AND SERVICES/ MALICIOUS CODE PREVENTION/ SECURITY EVENT MONITORING**	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]	CimTrak can monitor both ports and services and identifies any changes to these. Changes that open ports or enable services can allow unauthorized access or malicious activity to occur within an otherwise secure IT environment. IT personnel can be immediately notified of any changes so immediate action can be taken. CimTrak can be 100% effective at detecting malware because it does not rely on signatures. Malware can slip by existing network defenses for a number of reasons. As a last line of defense, CimTrak detects and notifies you of any changes instantly! Further, with its ability to prevent changes or restore them in real-time, malware can be effectively prevented.
	Where technically feasible, enable only logical network-accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	
	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	
	Deploy method(s) to deter, detect, or prevent malicious code.	
	Mitigate the threat of detected malicious code.	
	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	

CIP ID	REQUIREMENTS	HOW CIMTRAK HELPS
CIP-007 **SYSTEM SECURITY MANAGEMENT** **PORTS AND SERVICES/ MALICIOUS CODE PREVENTION/ SECURITY EVENT MONITORING**	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]	CimTrak can monitor both ports and services and identifies any changes to these. Changes that open ports or enable services can allow unauthorized access or malicious activity to occur within an otherwise secure IT environment. IT personnel can be immediately notified to any changes so immediate action can be taken. CimTrak can be 100% effective at detecting malware because it does not rely on signatures. Malware can slip by existing network defenses for a number of reasons. As a last line of defense, CimTrak detects and notifies you of any changes instantly! Further, with its' ability to prevent changes or restore them in real-time, malware can be effectively prevented.
	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	
	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging	
CIP-008 **INCIDENT REPORTING AND RESPONSE PLANNING** **CYBER SECURITY INCIDENT RESPONSE PLAN SPECS**	Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].	CimTrak has the capability to dynamically baseline and restore configurations when it detects changes (unauthorized) to the baseline. This helps address issues that affect deployed assets such as workstations, servers, network devices, applications, databases, services and the Windows registry when integrity drift occurs. Any unauthorized modifications of any of these resources are tracked and can be used to roll-back or leveraged to alert on security incidents affecting integrity events. Events can also be sent to a SIEM or event monitoring system through Syslogs or SNMP traps. The depth and breadth of forensic data and information in the CimTrak repository provides immediate ability to analyze and respond with immediate action(s). CimTrak has a built-in ticketing system (which is also the integration mechanism to traditional ITSM products if deployed) to manage the process of classifying and approving change. This process provides the unique ability to capture the expected changes and reconcile/curate those changes with observed changes to then highlight everything that is unauthorized change on critical systems within your environment.
	One or more processes to identify, classify, and respond to Cyber Security Incidents.	

CIP ID	REQUIREMENTS	HOW CIMTRAK HELPS
CIP-008 **INCIDENT REPORTING AND RESPONSE PLANNING** **CYBER SECURITY INCIDENT RESPONSE PLAN SPECS**	One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident.	CimTrak has the capability to dynamically baseline and restore configurations when it detects changes (unauthorized) to the baseline. This helps address issues that affect deployed assets such as workstations, servers, network devices, applications, databases, services and the windows registry when integrity drift occurs. Any unauthorized modifications of any of these resources are tracked and can be used to roll-back or leveraged to alert on security incidents affecting integrity events. Events can also be sent to a SIEM or event monitoring system through Syslogs or SNMP traps. The depth and breadth of forensic data and information in the CimTrak repository provides immediate ability to analyze and respond with immediate action(s). CimTrak has a built-in ticketing system (which is also the integration mechanism to traditional ITSM products if deployed) to manage the process of classifying and approving change. This process provides the unique ability to capture the expected changes and reconcile/curate those changes with observed changes to then highlight everything that is unauthorized change on critical systems within your environment.
	The roles and responsibilities of Cyber Security Incident response groups or individuals	
	Incident handling procedures for Cyber Security Incidents.	
	Retain records related to Reportable Cyber Security Incidents.	
CIP-009 **RECOVERY PLANS FOR BES CYBER SYSTEMS** **RECOVERY PLAN SPECS**	Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].	CimTrak's unique ability to restore and recover from unwanted change is measured in seconds which differs from traditional ITSM back-up and restoration functionality of reprovisioning. CimTrak can discreetly identify and restore the necessary files from any number of previously trusted baselines and avoid the costly time and effort of reprovisioning an entire system. CimTrak can roll-back and remediate changes if and when necessary (manually or automatically), to any previous trusted state(s) as it securely stores the previous files associated with that state of operation in a compressed and encrypted format.
	Conditions for activation of the recovery plan(s).	
	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	
	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	
	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	

CIP ID	REQUIREMENTS	HOW CIMTRAK HELPS
CIP-010 **CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENTS** **CONFIGURATION MONITORING/ VULNERABILITY ASSESSMENT**	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	CimTrak's core competency is to keep data secure by establishing, maintaining, and monitoring system baselines. Baselines can be created at any point throughout a system's lifecycle. System baselines are securely stored within the CimTrak Master Repository, where they are monitored for changes. Changes to a system's baseline can be tracked over time, and alerts issued should an unexpected change occur, indicating a possible compromise. CimTrak leverages the best practices of both CIS benchmarks as well as DISA STIGs to establish a referenceable configuration baseline of trust. Deviations to this baseline are detected in real-time to ensure there is no integrity drift from a known and trusted reference point. This includes the addition, modification, and deletion of software applications. CimTrak provides a historical configuration setting to establish a chain of evidence and root of trust. CimTrak's patented real-time change detection and response technology provides a closed-loop change control system that covers everything from servers and desktops to cloud configurations, hypervisors, container orchestration, databases and more. CimTrak has a built-in ticketing system that can be used standalone or in unison with leading ITSM vendors to capture authorized work orders to reconcile expected changes with observed leaving unwanted and unexpected changes highlighted for review and/ or remediation. CimTrak provides manual or automated roll-back capability as well as change prevention for those files, directories or configurations that should never change. CimTrak also provides both black and whitelisting correlation, STIX/TAXII feeds and file reputation services to provide more contextual information to help identify what should and should not be running in your environment.
	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied.	
	Authorize and document changes that deviate from the existing baseline configuration.	
	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	
	For a change that deviates from the existing baseline configuration: 1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change; 1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and 1.4.3. Document the results of the verification	
	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	
	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	

CIP ID	REQUIREMENTS	HOW CIMTRAK HELPS
CIP-010 **CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENTS** **CONFIGURATION MONITORING/ VULNERABILITY ASSESSMENT**	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R3– Vulnerability Assessments. [Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]	CimTrak's core competency is to keep data secure by establishing, maintaining, and monitoring system baselines. Baselines can be created at any point throughout a system's lifecycle. System baselines are securely stored within the CimTrak Master Repository, where they are monitored for changes. Changes to a system's baseline can be tracked over time, and alerts issued should an unexpected change occur, indicating a possible compromise. CimTrak leverages the best practices of both CIS benchmarks as well as DISA STIGs to establish a referenceable configuration baseline of trust. Deviations to this baseline are detected in real-time to ensure there is no integrity drift from a known and trusted reference point. This includes the addition, modification, and deletion of software applications. CimTrak provides a historical configuration setting to establish a chain of evidence and root of trust. CimTrak's patented real-time change detection and response technology provides a closed-loop change control system that covers everything from servers and desktops to cloud configurations, hypervisors, container orchestration, databases, and more. CimTrak has a built-in ticketing system that can be used standalone or in unison with leading ITSM vendors to capture authorized work orders to reconcile expected changes with observed leaving unwanted and unexpected changes highlighted for review and/ or remediation. CimTrak provides manual or automated roll-back capability as well as change prevention for those files, directories or configurations that should never change. CimTrak also provides both black and allowlisting correlation, STIX/TAXII feeds, and file reputation services to provide more contextual information to help identify what should and should not be running in your environment.
	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	
	Where technically feasible, at least once every 36 calendar months: 3.2.1 Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and 3.2.2 Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	

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

CIMCOR.COM | FOLLOW US @CIMTRAK