Meeting and Maintaining NERC Critical Infrastructure Compliance (CIP)

Maintaining the reliability of critical electric infrastructure has never been more crucial. Ever increasing demand means that outages and other problems cost utilities greater amounts of income, not to mention the time needed to investigate and remediate problems. 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 function properly. Ensuring compliance with these standards is critical in order to avoid significant penalties.

CimTrak, a highly innovative security and compliance tool, helps you by meeting 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 state of integrity. Additionally, CimTrak has the ability to automatically prevent changes, whether malicious or accidental, which can interrupt the supply of electrical power.

**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.

**Complete Perimeter Protection**
Monitor devices such as routers and firewalls to ensure that changes don't expose your critical cyber assets.

**Continuity of Operations**
CimTrak offers the option to instantly restore changes, keeping your critical systems running.

**Stop Internal and External Threats**
From unsigned malware to fat-finger errors, CimTrak has you covered! CimTrak can even protect custom applications or unpatchable systems.

**Complete Logging/Reporting**
CimTrak provides a wide variety of reports on watched systems and seamlessly integrates with all major SIEM and alarm systems.
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.

### Ports and Services

**1.1** 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.

**1.2** Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.

### Malicious Code Prevention

**3.1** Deploy method(s) to deter, detect, or prevent malicious code.

**3.2** Mitigate the threat of detected malicious code.

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.

### Preventative activities can lower the number of incidents, but not all incidents can be prevented. A preplanned recovery capability is, therefore, necessary for rapidly recovering from incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services so that planned and consistent recovery action to restore BES Cyber System functionality occurs.

CimTrak can function as a point backup solution by storing incremental baselines of files and configurations as they change. CimTrak allows you the ability to re-deploy any previous baseline at any time to recover from malicious or accidental changes. With the ability to also restore changes in real-time, CimTrak can prevent service disruptions by ensuring that critical systems stay running.

### As a last line of defense in your network, CimTrak can detect malware that may bypass other network defenses.
CIP-010

1.1 The configuration change management processes are intended to prevent unauthorized modifications to BES Cyber Systems.

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.

CimTrak baselines critical IT systems and then monitors them for any changes. It can monitor all of the items detailed in Requirement 1.1.

1.2 Authorize and document changes that deviate from the existing baseline configuration.

CimTrak's advanced integrated ticketing functionality allows changes to be planned and documented simply and easily. This allows any unplanned, and therefore potentially malicious change, to rise to the surface for quick response.

1.3 For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.

CimTrak's dynamic baselining capability gives users simple, granular control over baselines and allows for easy baseline comparison to track deviations.

2.1 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.

CimTrak monitors for baseline configuration changes in real-time, thus alerting personnel to changes in an extremely timely manner before they potentially mushroom into a large problem affecting power generation and/or transmission.

CimTrak ensures that configuration changes don’t take your critical systems down by detecting and alerting you to changes in real-time.

CimTrak logs all changes to your critical IT infrastructure and applications as well as provides complete reporting as well as simple integration with log management tools such as SIEM’s.