FORTRA

EXECUTIVE BRIEF (TRIPWIRE)

NERC CIP Best Practices: The Tripwire Approach

Smarter Compliance for Critical Infrastructure

Tripwire's NERC CIP Track Record

Tripwire has helped registered entities achieve and maintain NERC CIP compliance since 2008, learning from and collaborating with customers to solve their biggest challenges. This collaboration allowed Tripwire to develop a team of consultants well-versed in NERC CIP and the product extensions and CIP-specific content now embedded in Tripwire solutions.

As a recognized leader in solutions for IT and OT security and compliance, Tripwire has extensive experience helping customers automate compliance for numerous standards across almost any device, platform, and system. The following strategies are time-tested and will help you optimize NERC CIP compliance.

Industrial operators subject to the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standard know that achieving compliance is no minor feat, and serious strategic consideration is required to ensure efficient resource use in the compliance process. By meeting NERC CIP compliance, these companies take important steps towards securing their IT/OT systems against inadvertent misuse and intentional, malicious cyberattacks. In turn, securing these systems helps organizations ensure the reliability of North America's bulk electric system.

The Four-Phase Maturity Model

Achieving compliance is a rigorous process, not a short-term project. That's why the best approach is to use a maturity model. Maturity models allow you to assess where you currently are in your compliance journey and take incremental, prioritized steps to get to the optimum level of NERC CIP maturity.

Fortra's Tripwire offers solutions that help with nearly every element of NERC CIP that involves technical controls. However, your keys to success are the people and processes that work with these technical components. These take longer to develop and adjust.

The best course of action is to implement a bit of technology at a time and then let your people and processes adapt before moving on. This will allow you to ultimately scale your implementation across your entire organization.

Tripwire's compliance experts created a maturity model specifically for NERC CIP that breaks the process down into four basic phases:

1. **Establish the Ability to Monitor Assets**
   With robust security configuration management (SCM) and file integrity monitoring (FIM), Tripwire® Enterprise is the core tool for addressing NERC CIP compliance. Therefore, implementing it should be your first course of action. It monitors the system state of assets and notes any changes to their configurations. You can also set it up to evaluate the configuration against a certain standard (in this case NERC CIP). Tripwire Enterprise also has powerful reporting capabilities that will provide you with evidence reporting and help create holistic visibility. This step establishes the comprehensive capability to monitor and report on just about any configuration detail of in-scope assets.
2. **Implement the Most Essential Controls First**
   Start implementing the easy-to-solve controls that are critically important. The next core tool for addressing these controls is Tripwire State Analyzer. This tool

allows you to add automation for seven of the controls in the NERC CIP compliance framework. This turns a lot of work and difficult requirements into simple red and green reports. It also defines records in a centralized database and automates the validation of detected system configurations against those database records.

3. **Achieve Instrumentation for the Other Required CIP Controls**
   Your next milestone in the maturity model is addressing the few remaining explicitly required controls that are outside of what is covered by the Tripwire State Analyzer. They are fairly easy to implement, such as rules about password length and complexity and OS/firmware versions. Implementing this will not change your processes and which views and reports you utilize—it builds on what you have already established.
4. **Automate Data Collection for Deeper Insights**
   From here, you will be getting more comfortable with using Tripwire solutions and knowing you have a grasp on NERC CIP compliance for some of the toughest technical controls. However, a question that you'll want to ask yourself—before an auditor does—is, "How do I know that my technology is doing what it says it's doing?" If you have an area of concern, you can leverage Tripwire Enterprise to monitor those configuration details in question. You can visualize the correct configuration of details with the same red and green charts for what you are already monitoring.

Operationalizing the CIP Baseline

Following the four-phase maturity model takes the guesswork out of becoming NERC CIP compliant. But there is another best practice that will save your organization's resources and improve efficiency: effectively operationalizing the CIP baselines. It's crucial to be deliberate and clear on your strategy for operationalizing the CIP baselines.

CIP baseline requirements call for comparing your current state against trusted configurations. You can take several different approaches to define how the trusted configuration is represented. You could compare the current observed state to a past observed state. This approach of "chasing the change" requires substantial manual effort, however. Utility companies have used this approach for successfully meeting audit requirements, but also regularly voice that the amount of human labor required is high.

But a more sophisticated approach is to compare the current state to a reference standard, also known as an allowlist in Tripwire State Analyzer. Essentially, freshly observed configurations are compared to the allowlist reference using an automatic evaluation, rather than a human comparing to previous observed configuration. This automation-focused approach saves considerable time and effort.

An Emerging Approach for CIP-007 Patch Management

CIP-007 requires monthly investigation for security enhancements that must be implemented with patch updates. This aspect of NERC CIP is particularly challenging, but one emerging practice that is helping organizations meet patch management requirements is taking an automated, security-forward approach which leverages Tripwire's research into available security patches.

Tripwire IP360 helps automate CIP-007 compliance by delivering reports that delineate which patching actions must be taken to address vulnerabilities. Implementing this security-forward approach to patching helps teams see vulnerabilities from a holistic perspective and saves them time when patch reports show that no actions are needed at particular points in time.

Summary

With Tripwire, electric utilities have a comprehensive solution—from products to customized extensions and content and expert consulting—to help them automate and simplify NERC CIP compliance.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.