NERC CIP Compliance with Tripwire and RedSeal

The NERC Critical Infrastructure Protection standards are designed to enhance reliability of the electrical supply by securing the connected assets on which that supply relies. When building a program for NERC CIP compliance, registered entities must balance the need to be audit ready with the resources required to achieve and maintain compliance.

NERC CIP version 6 increases the amount of work required to achieve and maintain compliance, effectively raising the bar on registered entities. While many tools can help, Tripwire and RedSeal offer a unique combination of capabilities that automate difficult parts of the NERC CIP standards.

RedSeal and NERC CIP Compliance

RedSeal supports controls within four of the NERC CIP Version 5 Requirements. RedSeal provides strong organization/visualization for CIP-002-5 and CIP-005-5 regarding continuous monitoring and management of the Electronic Access Control or Monitoring systems (EACMS) and the Electronic Security Perimeters (ESP). Additional coverage is provided for CIP-007-5 and CIP-010-1 regarding continuous monitoring of configuration standards and vulnerability assessments/prioritizations.

Tripwire and NERC CIP Compliance

Tripwire has been assisting with NERC CIP compliance since the standard emerged, and applying our products and our deep domain expertise in compliance as well as security has helped hundreds of electric utilities achieve, maintain and produce evidence of compliance for their NERC audits. The Tripwire NERC CIP Solution Suite is built on our award-winning and patented technology, dramatically reducing the time and effort for power and utility companies to pass their audits. Tripwire's products provide capabilities for 20 of the 32 NERC CIP requirements.

The Value of Partnership

With Tripwire's extensive endpoint data and vulnerability information, and RedSeal's unique network access intelligence, Tripwire and RedSeal provide deeply complementary perspectives on the environment. Together, the two product portfolios provide a multi-level view into critical cyber assets and their environment.

Benefits:

- RedSeal's robust analytics of network architecture identify unknown devices and systems which, when combined with Tripwire® Enterprise, ensures complete visibility of the network and all connected systems.
- RedSeal's "what-if" analysis can be used to validate changes before they are implemented, while Tripwire

Enterprise can detect the specific changes that occur.

» Tripwire IP360™'s vulnerability scanning results are combined with RedSeal's network access context to provide comprehensive risk metrics per host, including downstream (multi-hop) exposure.

» Tripwire Enterprise can identify malicious code on in-scope assets, while RedSeal can prevent spread of malicious code by identifying direct and downstream accessible systems which can be quarantined or otherwise isolated.

COVERAGE OF NERC CIPv5 REQUIREMENTS

10 Standards | 32 Requirements | Tripwire with RedSeal supports 22

CIP-002 BES CYBER SYSTEM IDENTIFICATION AND CATEGORIZATION	CIP-003 SECURITY MANAGEMENT CONTROLS	CIP-004 TRAINING AND PERSONNEL SECURITY	CIP-005 ELECTRONIC SECURITY PERIMETER	CIP-006 PHYSICAL SECURITY OF BES CYBER SYSTEMS	CIP-007 SYSTEMS SECURITY MANAGEMENT	CIP-008 INCIDENT REPORTING AND RESPONSE PLANNING	CIP-009 RECOVERY PLANS FOR BES CYBER SYSTEMS	CIP-010 CONFIGURATION CHANGE MANAGEMENT AND VULNERABILITY ASSESSMENTS	CIP-011 INFORMATION PROTECTION
1. BES CYBER SYSTEM IDENTIFICATION	1. CYBER SECURITY POLICY FOR HIGH/MEDIUM SYSTEMS	1. AWARENESS	1. ELECTRONIC SECURITY PERIMETER	1. PHYSICAL SECURITY PLAN	1. PORTS AND SERVICES	1. CYBER SECURITY INCIDENT RESPONSE PLAN	1. RECOVERY PLAN SPECIFICATIONS	1. CONFIGURATION CHANGE MANAGEMENT	1. INFORMATION PROTECTION
2. REGULAR APPROVAL	2. CYBER SECURITY POLICY FOR LOW SYSTEMS	2. TRAINING	2. INTERACTIVE REMOTE ACCESS MANAGEMENT	2. VISITOR CONTROL PROGRAM	2. SECURITY PATCH MANAGEMENT	2. CYBER SECURITY INCIDENT RESPONSE PLAN IMPLEMENTATION AND TESTING	2. RECOVERY PLAN IMPLEMENTATION AND TESTING	2. CONFIGURATION MONITORING	2. BES CYBER ASSET REUSE AND DISPOSAL
	3. IDENTIFICATION OF SENIOR MANAGER	3. PERSONNEL RISK ASSESSMENT PROGRAM		3. MAINTENANCE AND TESTING PROGRAM	3. MALICIOUS CODE PREVENTION	3. CYBER SECURITY INCIDENT RESPONSE PLAN REVIEW, UPDATE, COMMUNICATION	3. RECOVERY PLAN REVIEW, UPDATE AND COMMUNICATION	3. VULNERABILITY ASSESSMENTS	
	4. DELEGATION OF AUTHORITY	4. ACCESS MANAGEMENT PROGRAM			4. SECURITY EVENT MONITORING				
		5. ACCESS REVOCATION PROGRAM			5. SYSTEM ACCESS CONTROLS				

TRIPWIRE ALONE
TRIPWIRE and REDSEAL

Fig. 1 Tripwire with RedSeal helps electric utility companies meet 22 of the 32 requirements contained in the 10 standards.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook

TAPRS1j 1510