DATASHEET

NERC CIP Compliance with Tripwire and SigmaFlow

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 compliance, especially when approached using manual methods, is complex, time-consuming and prone to human error. Further, NERC CIP requirements often infer security skill sets beyond those of many workers in the power and electric utility sector.

The coming deadline for NERC CIP version 5 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 SigmaFlow offer a unique combination of capabilities that automate difficult parts of the NERC CIP standards.

SigmaFlow and NERC CIP Compliance

SigmaFlow Compliance Manager (CM) is a real-time, evidentiary NERC compliance management software solution solving the challenges of CIP unmet by traditional GRC approaches. The CM solution manages all documents, data, and work activities while automatically collecting and building the evidence for NERC compliance in a real-time repository. The NERC CIP solution collects and manages compliance evidence through data management, document management, tasks, and procedures for NERC CIP-002 through CIP-009.

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, built on our award-winning and patented technology, dramatically reduces 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

Tripwire and SigmaFlow are uniquely positioned to deliver combined benefits to utility customers who must comply with NERC CIP standards. Tripwire excels at data collection and compliance mapping, while SigmaFlow provides powerful workflow tools to automate documentation and evidence collection. Together, the solutions provide unparalleled benefits:

- Integrated Tripwire baseline and change detection with SigmaFlow change workflow and evidentiary reporting
- SigmaFlow Access rights management integrated with Tripwire's asset rights validation

» Tripwire baselines and whitelists integrated with SigmaFlow workflow and evidentiary reporting

Very simply Tripwire provides the data that makes SigmaFlow valuable, and SigmaFlow provides the workflow that drives value from the data collection.

Workflow

1. Scheduler/Workflow invokes SigmaFlow integration
2. SigmaFlow calls Tripwire API
3. Tripwire API collects data
4. Tripwire API returns data to SigmaFlow API
5. SigmaFlow feeds data to database

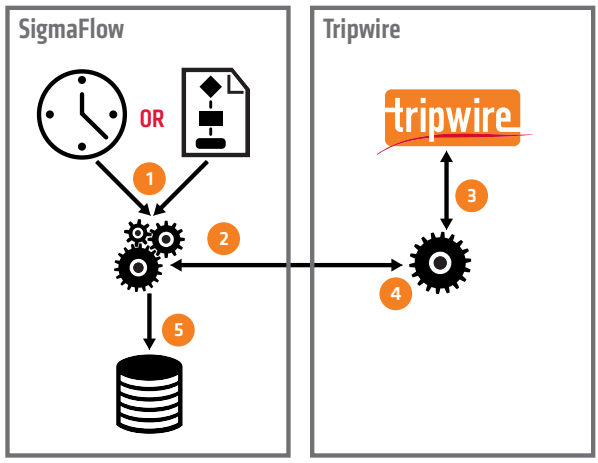

Fig. 1 Collecting data from Tripwire is performed through integrations supplied by SigmaFlow.

COVERAGE OF NERC CIPv5 REQUIREMENTS

10 Standards | 32 Requirements | Tripwire with SigmaFlow supports 28

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				

SIGMAFLOW ALONE
TRIPWIRE ALONE
TRIPWIRE and SIGMAFLOW

Fig. 2 The Tripwire NERC Solution Suite helps electric utility companies meet 20 of the 32 requirements contained in the 10 standards.

tripwire

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

TAPSF1j 1510