Integrated Compliance Automation

AN AUTOMATED APPROACH TO VALIDATING WHAT'S APPROVED WITH WHAT'S OBSERVED.

SigmaFlow is the industry-leading solution for orchestrating NERC CIP compliance to achieve an ongoing state of Audit Readiness. Tripwire, Inc. is a leading global provider of advanced threat, security and compliance management solutions. Integrating these solutions offers an automated way to drastically reduce the time and resources required to manage NERC compliance and collect comprehensive audit evidence.
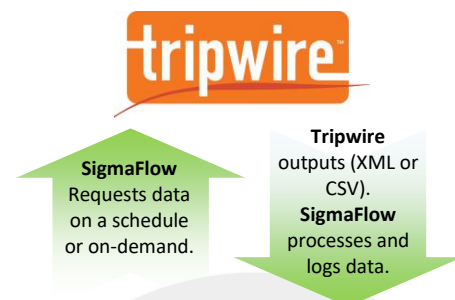
Integration Summary

Energy organizations are required to gather, analyze, validate and document an overwhelming amount of vulnerability and network data to protect their most critical assets and meet compliance requirements. SigmaFlow uses process-driven compliance and closed-loop controls allowing customer to manage and enforce internal compliance controls, streamline work, and build the "stack" of evidence to meet all aspects of each NERC Requirements. While some aspects of NERC compliance are validated wholly within the SigmaFlow solution, other controls can only be validated with data collected directly from cyber assets.

The integration between the Tripwire NERC Solution Suite and SigmaFlow provides customers with an automated and consistent approach to the management and maintenance of secure configurations across a wide range of devices, including ICS, SCADA, Microsoft Windows and Windows servers. SigmaFlow's Closed-Loop Controls Framework™ collects data from the Tripwire® Enterprise solution and then verifies actual practices against policy. Evidence is automatically produced and associated to various NERC compliance standards to ensure an audit-ready state. This drastically reduces the time and resources required to collect comprehensive audit evidence and manage the mandated compliance activities.

### Common Compliance Integrated Controls

- **Logical and Physical Access Rights**
  EX: Local and named accounts
- **Security Controls**
  EX: Password rules, Malware status, Antivirus status, Log forwarding settings, SNMP community strings
- **Baselines**
  EX: Ports and services, Security patches, Software, OS/Firmware

SigmaFlow Requests data on a schedule or on-demand.

Tripwire outputs (XML or CSV). **SigmaFlow** processes and logs data.

- Automatically **produce evidence** from provisioned data.
- Automatically **tag evidence** to Standards.
- Automatically **validate** what's provisioned against what's approved.
- Automatically **trigger remedial actions/notifications**.

Benefits of an Integrated Solution

SigmaFlow's focus on comprehensive evidence management for all CIP Standards in addition to the work management platform for all CIP Requirements makes it the most comprehensive NERC CIP Compliance solution available today. The capabilities of Tripwire to access and report on provisioned data from the cyber assets themselves fill an important gap that is often overlooked in compliance approaches. SigmaFlow's integration to Tripwire maximizes the value and leverages automation to ensure that all provisioned data is properly collected, stored and validated. The resulting solution solves complex and time-consuming NERC CIP compliance challenges that utilities face.

Centralized Compliance Management, Evidence, & Analytics Solution
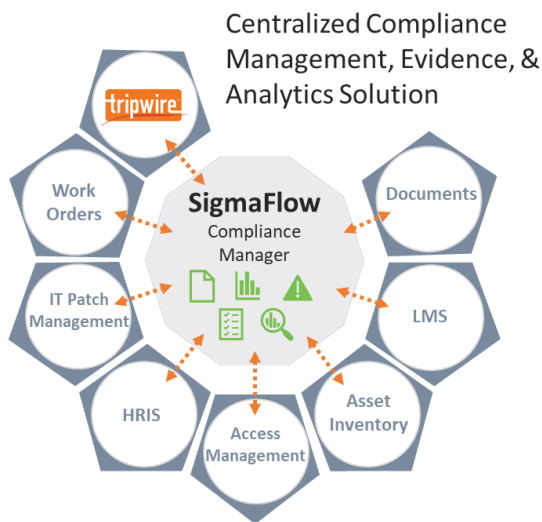
Internal Controls Validation Steps

1. **Collect/Manage Approved Lists** — Leverage SigmaFlow process controls, scheduling, and automation to build and manage your approved lists in a centralized evidence repository.
2. **Collect Provisioned Evidence** — Using SigmaFlow's pre-built Tripwire integration connector, retrieve scan data for use as evidence and monitoring.
3. **Validate Approved vs Provisioned** — Monitored by SigmaFlow, a mismatch between approved and provisioned data can be viewed in discrepancy reports, automatically generate notifications and initiate remediation processes.
4. **Report on Your Compliance Health** — SigmaFlow's solution provides critical compliance information through real-time dashboards and extensive reporting to help utilities maintain a continuous state of audit readiness. SigmaFlow is designed to provide easy access to historical data, giving utilities the ability to report on baselines and access rights for any given date or date range in the past. This is particularly important during an audit when the compliance evidence being reviewed covers multiple years.
5. **Generate Audit/RSAW Packages** — A centralized evidence repository allows for one-click automated RSAW and Audit Package generation, where the solution automatically produces and packages the RSAW form, pre-populated with your data, and the supporting evidence files.

About SigmaFlow

The SigmaFlow Compliance Manager (CM) is a real-time, evidentiary software solution designed specifically for NERC Compliance. The CM solution manages all documents, data, work activities and schedules while automatically collecting and building the evidence for NERC compliance in a real-time repository; thus streamlining, automating, and optimizing the process of collecting and managing compliance evidence.

Solution Benefits:

- **Internal Controls & Policy Enforcement** Enforces prerequisites for granting approval, gathers formal approval, and assigns work.
- **Compliance Transparency & Validation** Collect information to compare "as-is" state against policies.
- **Audit Readiness** Generates and associates evidence with the proper requirements for 1-click RSAW generation.
- **Productivity Enhancement** Automation and simplification improve productivity and drive consistency.

SIGMAFLOW®
Delivering Business Excellence