SigmaFlow and Tripwire
Solving NERC CIP Compliance

SigmaFlow provides a NERC CIP solution designed to collect and manage all evidence for NERC CIP compliance reporting, including the generation of RSAWs and Audit Packages. The SigmaFlow solution also provides a comprehensive NERC CIP work management platform with compliance workflows for all CIP standards and scheduling that is used to automatically invoke workflows when they are required to be performed.

Tripwire provides a solution that connects to and manages Cyber Assets, including the ability to report on baselines, validate Security Controls, and extract events from Cyber Asset logs in order to demonstrate compliance.

The solutions are synergistic with very little overlap, if any. The SigmaFlow solution does not have the functionality required to connect to Cyber Assets and collect data. In turn, the Tripwire solution does not have the ability to manage all NERC CIP evidence or the workflows needed to demonstrate compliance for the NERC CIP standards. While the Tripwire solution is certainly a valuable and important part of NERC CIP compliance for many utilities, it is in effect an "evidence feed" into the SigmaFlow solution.

In addition to the general role of each solution in respect to NERC CIP there are several other areas where the use of these two solutions provides the utility customer with additional value.

Evidence and Evidence Sources

For a given audit, there will often be several thousand evidence documents or more that a utility must provide in order to prove compliance. SigmaFlow manages the generation, collection, and oversight for all needed evidence. This includes workflow reports that are required evidence for many Requirements. The data and reports that Tripwire is capable of generating covers the majority of what is commonly referred to as provisioned data. Provisioned data is drawn directly from the Cyber Assets themselves. While provisioned data represents a very small percentage of the evidence required for RSAWs and Audit Packages, this data can be difficult to access. Tripwire's primary value is the collection of this data.

Approved Versus Provisioned

People are often confused by the terms Approved and Provisioned, yet this is an extremely important part of NERC CIP Compliance. Approved and Provisioned data primarily apply to cyber asset baselines, logical access rights, and physical access rights.

The NERC CIP Standards require that utilities maintain approved evidence in three specific areas:

- Baselines for cyber assets
- Logical access rights for people
- Physical access rights for people

In order to qualify as evidence, approved baselines and access rights must go through a compliance process prior to actual implementation. Each change to these approved areas requires additional supporting evidence demonstrating that the utility's process was followed prior to making the change. A workflow report is the best evidence to demonstrate this.

For example, any change to a cyber asset must go through the utility's change management process. This is one of the workflow templates included in the SigmaFlow solution. It doesn't matter if the change adds something or takes something away – the change management process is required for all cyber asset changes. The same goes for any change (grant and revoke) to logical and physical access rights.

Provisioned data demonstrates what has actually been configured on the cyber assets themselves. Everything that is provisioned must have corresponding process evidence to demonstrate that the change was made in the appropriate manner. Provisioned data must come from the assets themselves. It is the record of what has actually been implemented. Where SigmaFlow manages and demonstrates compliance for approvals, Tripwire collects and reports on what has actually been implemented.

Approved and Provisioned Data Validation

Once the challenge of collecting both approved and provisioned evidence has been met, the next challenge is validation. A mismatch between approved and provisioned data is a compliance concern that can easily qualify as compliance non-conformance. This requires that the approved and provisioned evidence not only be collected, but validated as well.

SigmaFlow provides API integration to Tripwire so that the provisioned data that Tripwire collects can be pulled by the SigmaFlow solution as actual data, not just a report. This facilitates the validation of approved versus provisioned evidence in SigmaFlow, and the solution is designed to do so automatically. The result is that the utility customer always knows if they are in compliance or if there are mismatches between approved and provisioned data that need further attention.

The other advantage of this approach comes from the retention and access to history. The Tripwire solution is primarily focused on what is happening now - not what happened the week, month or year prior. SigmaFlow is designed to provide easy access to all history, 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.

Conclusion

When the SigmaFlow and Tripwire solutions are used together, they offer a uniquely compelling solution for NERC CIP Compliance. The solutions serve specific purposes that are synergistic with little to no overlap.

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 the vast majority of the NERC CIP compliance challenges that utilities face, as evidenced by the following matrix.