Tripwire Integration Use Cases

March 4, 2014 / Revision 1
Table of Contents

INTRODUCTION .............................................................................................................................................2
Integration Solution Components ...................................................................................................................2
USE CASES ..................................................................................................................................................3
Closed-Loop Controls: .................................................................................................................................3
   Use Case 1 – Track System Changes .......................................................................................................4
   Use Case 2 – Change Management Testing ............................................................................................5
Initial Data Load: .......................................................................................................................................6
   Use Case 3 – Cyber Assets: .......................................................................................................................6
Introduction

Tripwire monitors and collects data from various systems that can potentially be used as evidence and/or to provide existing/historical data in the SigmaFlow solution. This document describes these integration opportunities.

Integration Solution Components

The SigmaFlow integration solution will be comprised of two primary components:

- **Integration Service** — a SigmaFlow Integration Service will act as the middleware to manage integration requests. For example, the Integration Service will determine when the integration will occur (ex. schedule or on-demand) and what connector will be used to handle the request.

- **Connectors** — custom connectors will support specific integrations to external systems and may support one or more functions. For example, a Tripwire Connector will be designed to use specific Tripwire API(s) that support the defined use cases.

The following diagram illustrates the interactions between the SigmaFlow Compliance Solution, The SigmaFlow Integration Service and Tripwire to support integration.
Use Cases

The following use cases represent common Compliance activity that would benefit from integration.

Closed-Loop Controls:

NERC requires operators to understand, monitor and track changes to current systems. To support this, current system data can be imported into the SigmaFlow solution where users can monitor changes and validate actual changes against the changes approved in SigmaFlow.

An integration with Tripwire can be used to retrieve the following system information:

- Ports & Services (Port 80: HTTP, Port 25: SMTP, etc.)
- Software and versions (Anti-virus, Anti-malware etc.)
- OS Version and Patches
- Accounts, Roles and Permissions
- Password Policies
Use Case 1 – Track System Changes

SigmaFlow allows operators to review current system data and verify actual changes against approved changes. In this use case, system data is imported into SigmaFlow on a periodic basis (ex. daily).

The following diagram illustrates the interactions between the SigmaFlow Compliance Solution, The SigmaFlow Integration Service and Tripwire to support the described use case.

Closed Loop Controls: Track System Changes
Use Case 2 – Change Management Testing

Before implementing changes that will affect critical assets (ex. installing patches and software, etc.) NERC requires that the changes are first applied to test servers. This allows operators to identify and address any resulting system changes. In this use case, a SigmaFlow user would retrieve, on-demand, the current system data, both before and after changes are applied. The user would then compare the results to identify any changes.

The following diagram illustrates the interactions between the SigmaFlow Compliance Solution, The SigmaFlow Integration Service and Tripwire to support patch application.
**Initial Data Load:**

During implementation, it's common to bulk upload existing/historical data into the SigmaFlow solution. This activity could be automated by integrating with Tripwire, Active Directory and other systems.

**Use Case 3 – Cyber Assets:**

Ideally, assets information would be extracted from Tripwire and then data related to selected assets added to the SigmaFlow solution.

The following diagram illustrates the interactions between the SigmaFlow Compliance Solution, The SigmaFlow Integration Service and Tripwire to support the described use case.