tripwire®
ENTERPRISE

# TRIPWIRE ENTERPRISE INTEGRATION WITH HP ARCSIGHT ESM

## A "SUPER CONNECTOR" FOR FILE CHANGE AND CONFIGURATION STATE DETAILS

### TRIPWIRE ENTERPRISE ACHIEVES COMMON EVENT FORMAT (CEF) CERTIFICATION

Tripwire Enterprise is now certified as an ArcSight Common Event Format (CEF) solution. In fact, it's the only CEF-certified solution to provide "system state intelligence"—the stateful combination of critical change and security configuration data—to ArcSight ESM deployments.

SIEMs are the incident detection tool of choice, but as organizations broadly deploy them throughout large distributed networks, IT security teams face a growing challenge: isolating the real threats from the volumes of noise generated by the IT infrastructure. Industry research and practitioners say the best way to reduce that noise is by comparing security events to other trusted sources of security data—specifically, change and configuration data. This added context quickly knocks away volumes of false positives, and helps security teams focus on the events that matter the most.

Tripwire® Enterprise, an industry-leading security configuration management solution, provides end-to-end configuration assessment and file integrity monitoring. It's also widely used as the "definitive source of truth" for highly detailed file change and configuration state data. We're talking about changes to key items like configuration files, ports, servers, binaries and executables—the types of changes that tell you if a system can be trusted.

Now that Tripwire Enterprise is an ArcSight CEF-certified solution, you can combine its highly detailed change and configuration data with security event information in ArcSight ESM using a standard communication format. The payoff? Reduced noise and false positives and greatly improved incident detection.

### PRE-PROCESSED DATA TO MAXIMIZE ARCSIGHT ESM CAPABILITIES

Tripwire Enterprise pre-processes its change and configuration data with internal rules and data correlation. This pre-processing allows Tripwire Enterprise to include leading indicators and key metadata in the security data it sends to ArcSight—for example, severities, asset- and test-based risk scoring, and alert information. Plus, you can link back to Tripwire Enterprise from the ArcSight ESM and perform detailed, side-by-side analysis of changes to files and configuration items. This added context lets you maximize the capabilities of ArcSight ESM, giving you a jumpstart on distinguishing between data noise and serious threats.

The Tripwire® VIA™ Event Integration Framework (EIF), a workflow component of Tripwire VIA, serves as an ArcSight connector between Tripwire Enterprise and ArcSight ESM. It lets you:

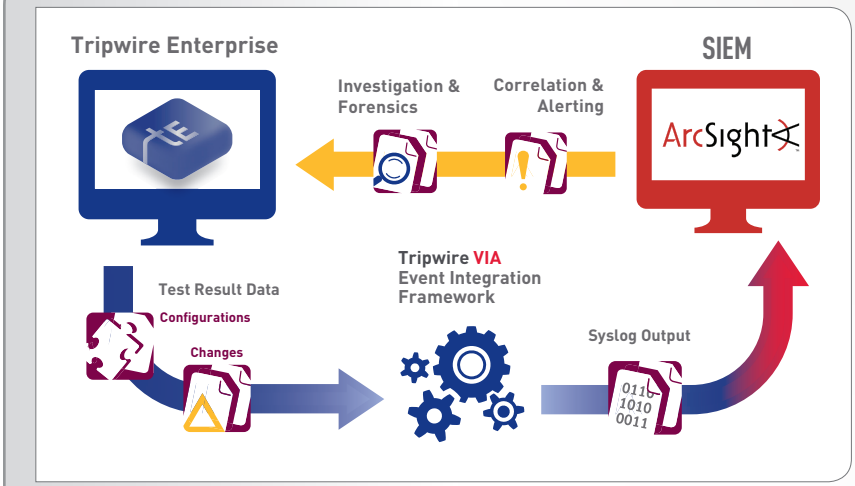
- Leverage Tripwire Enterprise's trusted agent, system state visibility, and configuration policy analysis capabilities

- Provide critical state change information as a new, defining variable in ArcSight's SIEM correlation rules
- Augment security events with context from change and configuration data, like new services opened, new users added, suspiciously elevated privileges, and even attribution information on "who" altered these critical system elements

Adding this detailed change and configuration data from Tripwire Enterprise to ArcSight ESM events shows you not just that "something happened," but exactly what happened. The cross-linking capability between the two systems even shows users detailed, side-by-side comparisons of detected changes and configuration alterations, allowing them to determine root cause or risk.

## HOW THE INTEGRATION WORKS

- Tripwire Enterprise detects a file state change, or identifies a test failure or score change related to a configuration policy.
- Tripwire Enterprise processes that data using the Tripwire VIA Event Integration Framework.
- Tripwire VIA EIF compiles the data and generates a richly detailed security event message—a "super-event"—to send to ArcSight ESM via Syslog.
- ArcSight ESM normalizes the message and then applies correlation rules to determine the next course of action.
- If the results indicate the need for investigation by the Tripwire Enterprise administrator, details can be incorporated back into Tripwire Enterprise reports and homepages.




.: **FIG. 1** As an ArcSight CEF-certified solution, Tripwire Enterprise can use the Tripwire VIA EIF to pass file change and configuration state data to ArcSight ESM.

| File Change Data | Configuration State Data |
|---|---|
| File changes from baseline | current CI state |
| Severities | Configuration test details |
| Type of changes (content, DACLs, etc.) | Current # and % of pass vs. fail |
| "Who" made the change | Score improvements/declines |
| Deviation from "Known Good" | Change in passes/failures |
| Previous vs. Current deltas | Details of node being tested |
| Number of changes discovered | Numerical change in score |

.: **FIG. 2** Examples of File Change and Configuration State Data Provided by Tripwire Enterprise

## A POWERFUL PAIRING FOR INCIDENT DETECTION

ArcSight ESM is the premier SIEM solution in an increasingly threatening world. Tripwire Enterprise is the authority on achieving and maintaining the "known and trusted" state for information security systems, across all platforms and physical and virtual infrastructures.

The integration of the two, using the ArcSight CEF and the Tripwire VIA Event Integration Framework, creates the best of both worlds: an intelligent, scalable, and manageable solution for enterprise-wide information security.

tripwire®
TAKE CONTROL.

.: Tripwire is a leading global provider of IT security and compliance solutions for enterprises, government agencies and service providers who need to protect their sensitive data on critical infrastructure from breaches, vulnerabilities, and threats. Thousands of customers rely on Tripwire's critical security controls like security configuration management, file integrity monitoring, log and event management. The Tripwire® VIA™ platform of integrated controls provides unprecedented visibility and intelligence into business risk while automating complex and manual tasks, enabling organizations to better achieve continuous compliance, mitigate business risk and help ensure operational control. :.

LEARN MORE AT WWW.TRIPWIRE.COM OR FOLLOW US @TRIPWIREINC ON TWITTER.

©2012 Tripwire, Inc. Tripwire, Log Center, VIA and ChangeIQ are trademarks of Tripwire, Inc. All other product and company names are property of their respective owners. All rights reserved.
TEASI1n 201204