Tripwire Log Center

Centralized Log Management Made Simple

Given today's environment of sophisticated security threats, security analytics solutions and regulatory compliance demands, the need for a more intelligent log solution has become clear.

As the volume and sophistication of cyberthreats increase, organizations must sift through mountains of data to identify real threats. The traditional approach of relying on inadequate log collection tools to deliver ever-increasing log and event data to expensive, large-scale SIEM deployments is no longer sufficient.

Tripwire® Log Center™ provides secure, reliable centralized log collection, analysis and delivery. Tripwire Log Center integrates with your existing infrastructure and includes a large library of available correlation rules, empowering your team to monitor, detect and quickly respond to threats in your environment.

Whether you collect logs strictly for regulatory compliance or to increase awareness of credible cyber threats, Tripwire Log Center ensures the process is secure and reliable.

What Distinguishes Tripwire Log Center?

Tripwire Log Center offers an alternative to traditional approaches to meeting organizational needs for early breach detection, compliance, and secure, reliable log collection.

Centralized Forensics Data

Tripwire Log Center integrates data from Tripwire Enterprise and Tripwire IP360, providing organizations with insight into the relationships between suspicious events, system changes, weak configurations and current vulnerabilities. This rich combination of information enables you to identify risk and prioritize your security efforts more effectively. For those using the 20 Critical Security Controls as a security framework, Tripwire protects your critical infrastructure by correlating data and providing context from the first four controls.

Enabling Local Expertise

Deploying Tripwire Log Center at the departmental or agency level allows for faster response and investigation of incidents by putting the data in the hands of the individuals who know it best, the local engineers and operators. A centralized SIEM or analytics tool can provide great value across a wide set of data, but investigating an incident requires detailed data your fingertips. Tripwire Log Center can support a centralized analytics function while simultaneously enabling local visibility.

Efficient Analytics

Most SIEMs and security analytics tools are licensed based on consumption, either data indexed or events per second, which is a model that suffers from high cost, difficult budget planning, and a poor signal to noise ratio. Tripwire Log Center can be used to collect and store all log events, while only forwarding those that are relevant to centralized analytics tools. This reduces the cost of analytics tools, and improves the signal to noise ratio.

Cost Effective Compliance

Most compliance standards require collection and storage of log events, but meeting these requirements with a centralized SIEM can be expensive. It can also be difficult to ensure that geographic compliance requirements are met for log storage. Tripwire Log Center can be used as the comprehensive log storage tool for compliance, at a lower cost than traditional SIEMs. Tripwire Log Center can also support keeping log data local to a geography, while providing centralized access for analysis. Customers use Tripwire Log Center to meet the requirements of, and demonstrate compliance with, the PCI DSS, NERC CIP, NIST-800-53, HIPAA and other standards.

Faster Time-to-Value: Mitigate Risks Out of the Box

Tripwire Log Center has a drag-and-drop interface that allows you to quickly define and customize correlation rules. When a correlation rule is triggered, you choose the action: store for reporting, proactively alert or launch a scripted action. The Tripwire Log Center rule builder reduces the need for specialized expertise and resources to create complex rules. Tripwire Log Center comes with the solution packs listed below. Consisting of correlation rules, dashboards and other tools for security and compliance, your team can employ them to quickly get up to speed.

Threat & Security Solution Packs

- Insider Threat
- User Audit and Authentication
- Denial of Service Detection
- Breach and Intrusion Detection
- Network and System Audit
- Vulnerability and Cybercrime Control Integration
- Database Audit

Compliance Solution Packs

- NERC
- PCI
- NIST 800-53

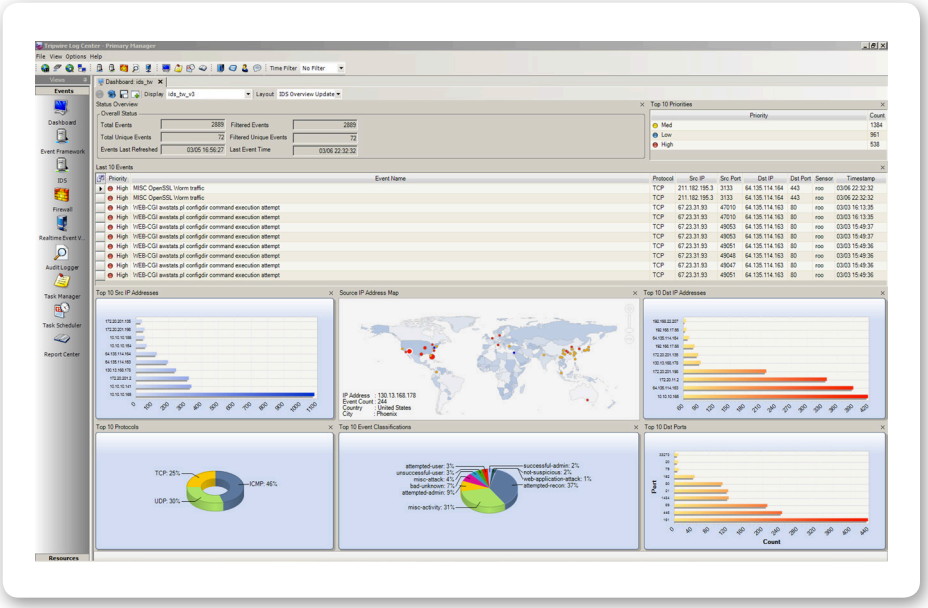

Fig. 1 Security dashboards and trending analysis views help you manage your security risks and dynamically drill down on areas requiring greater scrutiny.

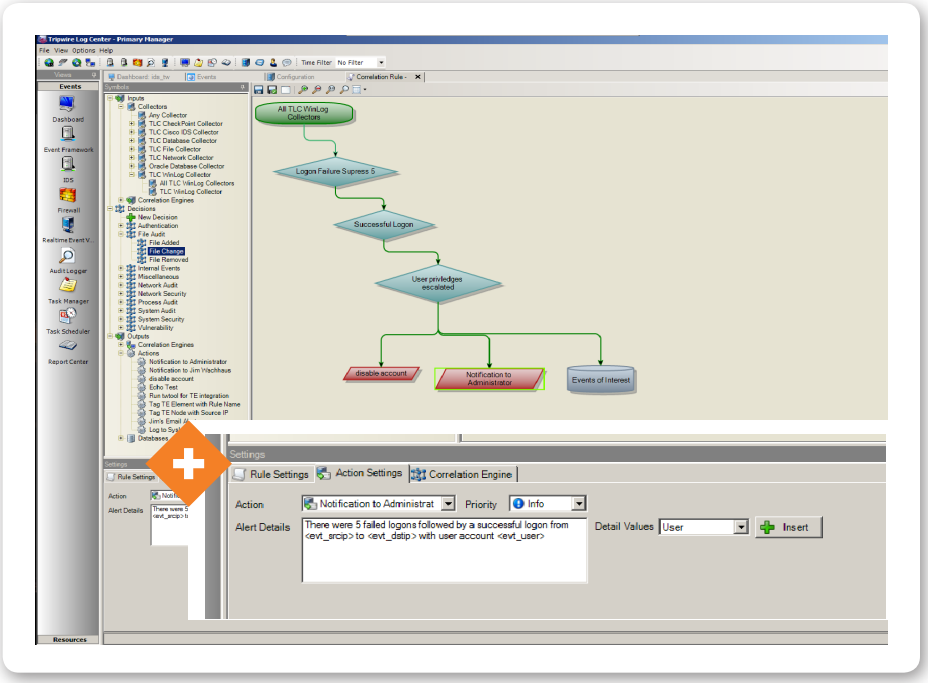

Fig. 2 Tripwire Log Center lets you define complex combinations of events by easily creating correlation rules with a graphical drag and drop rule creator.

Tripwire Integrations

- Tripwire Enterprise
- Tripwire IP360™

You also get a high-level view of your state of security with the solution's advanced event correlation, dashboards and trending analysis capabilities, and you can easily access historical data for forensic investigations.

Tripwire Log Center makes it easy to gather and share security data. The standards-based classification of log and event activity supports searches across platforms and devices, which yields comprehensive and accurate results for security investigations or in compliance reports.

Business and User Context

Asset View in Tripwire Enterprise can be used to tag and categorize your assets by business context. Tripwire Log Center can automatically use the context from Tripwire Enterprise through dynamic correlation lists. In addition, Tripwire Log Center integrates with Active Directory, which enables you to monitor specific users and user groups based on user attributes such as entitlements, groups and roles.

Combining business and user context lets you easily monitor assets and users that together may warrant a closer watch—for example, your highest value assets to which contractors have access. You can further prioritize risk by correlating suspicious events from Tripwire Log Center with suspicious changes detected by Tripwire Enterprise and vulnerabilities identified by Tripwire IP360.

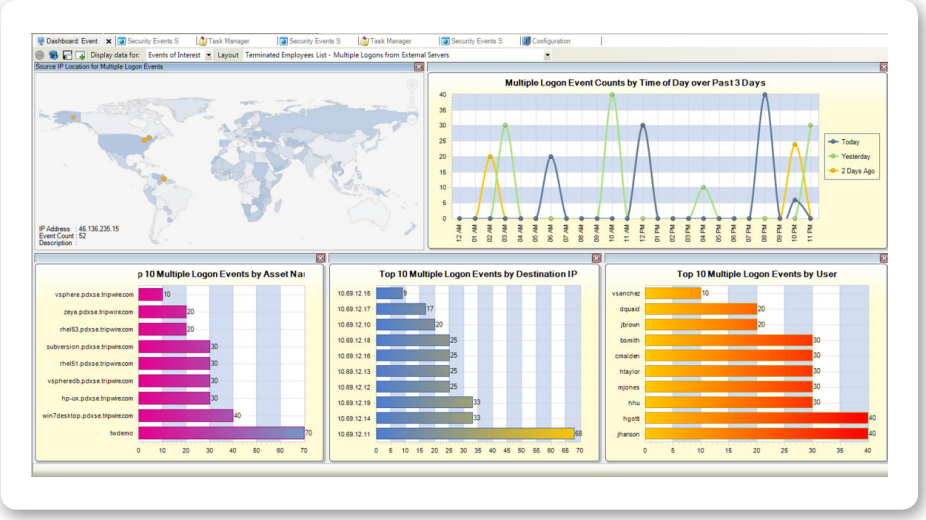

Fig. 3 Obtain leading indicators of breach activity by adding business and user context to your incident detection efforts.

Tripwire Log Center Features

Secure, Reliable Log Collection

Tripwire Log Center's complete, secure and reliable log collection ensures that organizations can meet regulatory requirements for logging and have the data they need for security analytics and incident response. The Tripwire Axon agent, used to collect log data, ensures that if a system, device or other asset fails, you have certainty your log data is safe. Tripwire Log Center supports agentless log collection for platforms where agents cannot be installed. And Tripwire provides high levels of compression to reduce storage demands, while simultaneously protecting logs from alteration.

Log Storage, Indexing and Search

Collected logs are stored and indexed for efficient searching, allowing for the examination of every collected detail during an incident investigation. Tripwire Log Center can store logs centrally or distribute them via secondary managers to retain local storage while facilitating centralized access.

Event Correlation

While Tripwire Log Center comprehensively collects log events, it can also extract the signal from the noise through the use of its correlation engine. Prebuilt correlation rules are included for a number of platforms and purposes, including compliance standards and security use cases. Customers can create custom correlation rules using the simple 'drag and drop' user interface in Tripwire Log Center.

Filtering and Forwarding

Security analytics tools require data from a variety of sources to achieve accurate results, and log data is a key source. Tripwire Log Center can provide the collection infrastructure to securely, reliably deliver log data to centralized analytics tools, like a SIEM. Tripwire Log Center can filter the events it sends, reducing the noise generated by sending every event to a SIEM, and reducing the cost of analytics tools that license by data indexed or events per second.

Asset Discovery

Tripwire Log Center can mine the collected log data to discover previously unknown assets through their activity and interaction with monitored assets. This passive method of asset discovery doesn't rely on network scans or monitoring captured traffic. Users can add discovered assets to Tripwire Log Center for log collection.

Integration With Tripwire Products

Tripwire's products are designed to deliver best-in-class capabilities alone, but also to deliver additional value by working together. Tripwire Log Center can use the vulnerability data from Tripwire IP360 and the business context data from Tripwire Enterprise to deliver more accurate, complete correlation results. Tripwire Enterprise can display log events directly from Tripwire Log Center in its user interface, resulting in less time spent switching context and tools.

Tripwire paired with Tofino's Xenon malicious traffic detector provides deep visibility and configuration management insight not previously possible

- The only industrial security appliance that is 100% undiscoverable and undetectable
- Integration with Tripwire Log Center provides real-time visibilty to assets communicating through the Xenon and which packets are being blocked
- Complies with NERC CIP, ISA/IEC-62443, IEC 60870-5-104, ATEX, ISA-12.12.01 Class 1 Div.2, EN 50121-4, Germanischer Lloyd

Learn more at tripwire.com

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*: Security news, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook