Tripwire LogCenter

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® LogCenter® provides secure and reliable centralized log collection, analysis, and delivery. It readily integrates with your existing infrastructure, and with a large library of available correlation rules it empowers 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 LogCenter ensures the process is secure and reliable.

What Distinguishes Tripwire LogCenter?

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

Centralized Forensics Data

Tripwire LogCenter integrates data from Tripwire Enterprise and Tripwire IP360™ to provide organizations 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 CIS Controls as a security framework, Tripwire protects your critical infrastructure by correlating data and providing context from the critical first six.

Enabling Local Expertise

Deploying Tripwire LogCenter 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 at your fingertips. Tripwire LogCenter can support a centralized analytics function while simultaneously enabling local visibility.

Efficient Analytics and Filtering

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 LogCenter 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 those tools while improving 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 for log storage are met. Tripwire LogCenter can be used as the comprehensive log storage tool for compliance, at a lower cost than traditional SIEMs. It can also support keeping log data local to a geography, while providing centralized access for analysis.

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

Tripwire LogCenter allows you to quickly define and customize correlation rules. When a correlation rule is triggered, you choose the response: store for reporting, proactively alert, or launch a scripted action. Its rule builder reduces the need for specialized expertise and resources to create complex rules.

To get your team quickly up to speed, Tripwire LogCenter includes the following solution packs:

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
- HIPAA

Business and User Context

Tripwire LogCenter makes it easy to gather and share security data. Its 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.

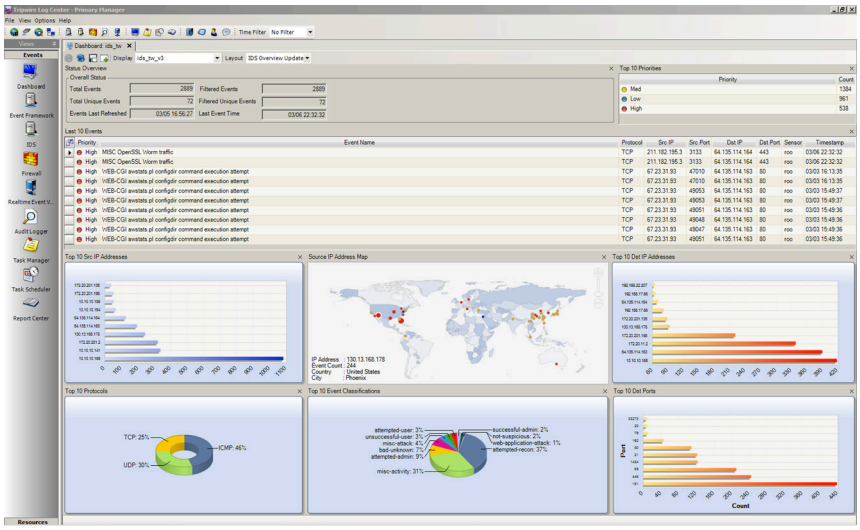

Fig. 1 Security dashboards and trending analysis views help you manage your security risks and dynamically drill down on areas requiring greater scrutiny.

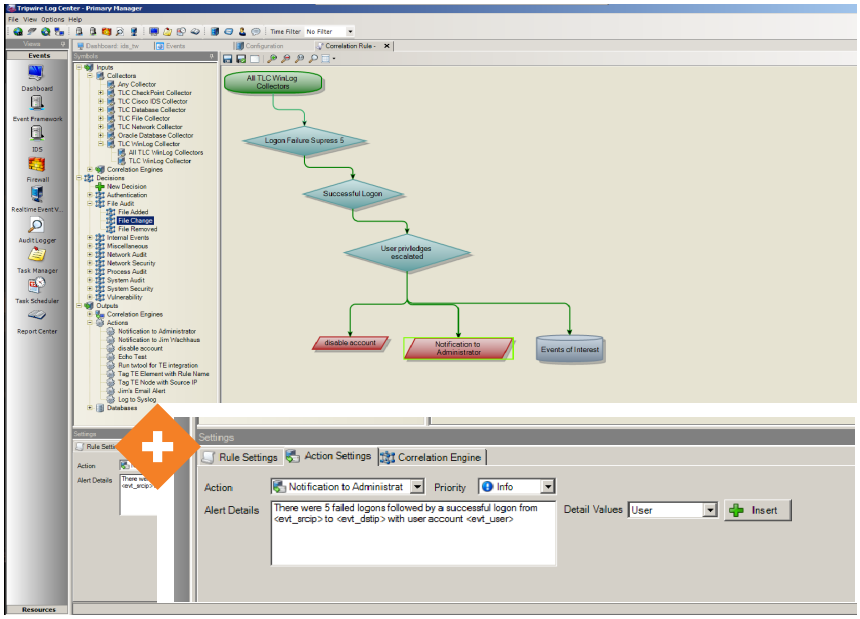

Fig. 2 Tripwire LogCenter lets you define complex combinations of events by easily creating correlation rules with a graphical drag and drop rule creator.

Tripwire LogCenter can automatically use the context from its integration with the other Tripwire solutions through dynamic correlation lists. In addition, you can 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 LogCenter with suspicious changes detected by Tripwire Enterprise and Tripwire Industrial Visibility, as well as vulnerabilities identified by Tripwire IP360.

Secure, Reliable Log Collection

Tripwire LogCenter's comprehensive 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, your log data is still safe. And Tripwire LogCenter supports agentless log collection on platforms where agents cannot be installed.

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 LogCenter can store logs centrally or distribute them via secondary managers to retain local storage while facilitating centralized access.

Event Correlation

While Tripwire LogCenter 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. Users can easily create custom correlation rules using a simple drag and drop user interface.

Asset Discovery

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

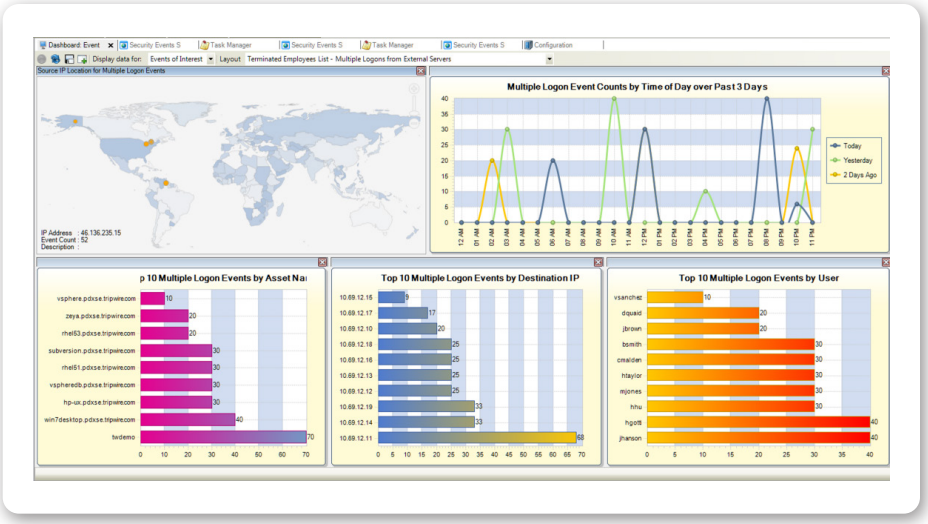

Fig. 3 Obtain leading indicators of breach activity by adding business and user context to your incident detection efforts.

High Availability

To ensure seamless logging, Tripwire LogCenter's Failover Manager provides high availability in the event that the Primary Manager goes offline. In the event that the Active Manager remains unresponsive for a certain amount of time, the Failover Manager will automatically takes over the workload.

Integration With Tripwire Products

While Tripwire's products are designed to deliver best-in-class capabilities alone, they deliver additional value by working together. Tripwire LogCenter can use the vulnerability data from Tripwire IP360 and the business context data from Tripwire Enterprise to deliver more accurate, complete correlation results. These integrations increase your visibility and reduce time spent on switching tools, improving efficiency to protect your system.

Ready for a Demo?

Let us take you through a demo of Tripwire LogCenter and answer any questions you have.
Visit **tripwire.me/demo**

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 LogCenter 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

As a Belden company, Tripwire is uniquely positioned to bridge the cybersecurity gap between your IT and OT environments. Tripwire solutions integrate seamlessly with the industrial products you already have in play, like Tofino firewalls and Hirschmann switches.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

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

TLCDS743c 2107