Tripwire and LinkShadow

LinkShadow integrates with Tripwire solutions to complete the full cycle of behavioral analytics and threat hunting, providing the combined benefits of Tripwire's file integrity monitoring (FIM) technology and proactive threat detection.

Key Features

- » Detects if an insider modifies critical files
- » Gets intelligence into both commodity and targeted attacks
- » Gains visibility on the remote workers
- » Provides insights on the endpoint file tampering or malicious activities

Next-Generation Cybersecurity Analytics

LinkShadow® Cyber Security Analytics Platform is designed to manage threats in real time. It utilizes AI-based machine learning to analyze events and perform UEBA. Cutting-edge threat hunting provides state-of-the-art cyber event anticipation.

Integration Use Cases

Suspicious File Access & Tripwire Enterprise

Using the Tripwire® Enterprise/ LinkShadow integration, customers can receive the following benefits:

- » Compliance audit reports showing how business compliance goals are or are not being met on individual systems, with details to correct
- » Faster resolution and investigation by combining LinkShadow anomalies with data from Tripwire Enterprise: what changes were made, who made the them, and when.
- » Prioritized criticality of a given change that enables more rapid response by combining LinkShadow anomalies with Tripwire Enterprise results.

Tripwire Enterprise feeds LinkShadow with enriched detection of file events to hunt for any suspicious file access by anomalous users. With Shadow360 Dashboard, the analyst gains full visibility on all user activities before and after the suspicious file access behavior.

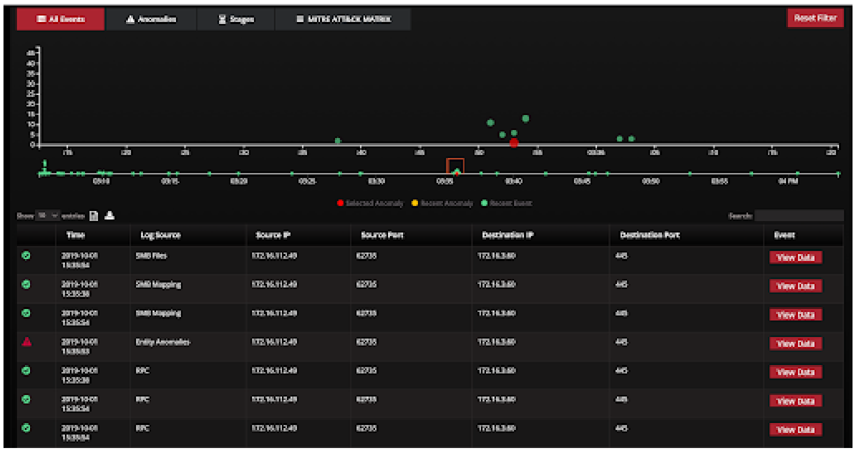
Anomalous File Tampering

LinkShadow gains full visibility of file tampering activities on endpoints from Tripwire Enterprise. LinkShadow injects this intelligence into the machine learning algorithms to identify suspicious and anomalous activities based on the behavioral analysis. File tampering can indicate the early stages of an attack.

Suspicious File Access & Tripwire IP360

The Tripwire IP360™ and LinkShadow integration provides following benefits:

- » Asset inventory list provided to LinkShadow
- » Detailed software inventory on individual systems
- » Vulnerabilities of the OS and the software installed on the system
- » Accurate CVE records related to the vulnerability, including Tripwire risk score
- » Prioritized systems by combining LinkShadow anomalies, Tripwire-identified vulnerabilities, and the criticality of the systems



	Time	Log Source	Source IP	Source Port	Destination IP	Destination Port	Event
✓	2019-10-01 15:35:54	SMB Files	172.16.112.49	62735	172.16.3.60	445	View Data
✓	2019-10-01 15:35:38	SMB Mapping	172.16.112.49	62735	172.16.3.60	445	View Data
✓	2019-10-01 15:35:54	SMB Mapping	172.16.112.49	62735	172.16.3.60	445	View Data
▲	2019-10-01 15:35:53	Entity Anomalies	172.16.112.49	62735	172.16.3.60	445	View Data
✓	2019-10-01 15:35:38	RPC	172.16.112.49	62735	172.16.3.60	445	View Data
✓	2019-10-01 15:35:54	RPC	172.16.112.49	62735	172.16.3.60	445	View Data
✓	2019-10-01 15:35:54	RPC	172.16.112.49	62735	172.16.3.60	445	View Data

Fig. 1 With LinkShadow's Shadow360 Dashboard, analysts gain full visibility on all user activities before and after the suspicious file access behavior.

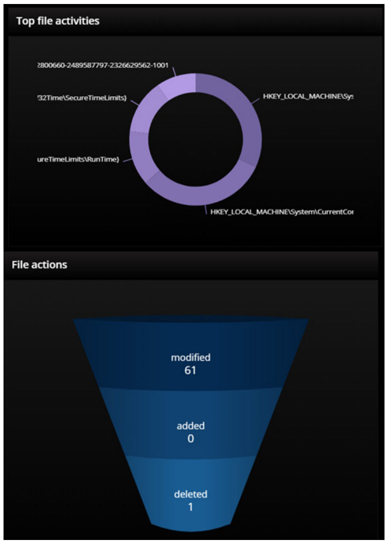


Fig. 2 LinkShadow gains full visibility of file tampering activities on endpoints from Tripwire Enterprise.

LINKSHADOW®
Combat the Dark

LinkShadow was created by a team of highly skilled experts, solution architects, product specialists and programmers to formulate a next-generation cybersecurity solution that provides unparalleled detection of even the most sophisticated threats.

LinkShadow was built with the vision of enhancing organizations' defenses against advanced cyber-attacks, zero-day malware and ransomware, while simultaneously gaining rapid insight into the effectiveness of their existing security investments.

tripwire®

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