ziften
PARTNER

Ziften + ReversingLabs™
Actionable Threat Intelligence

ReversingLabs™ and Ziften Integration Solution for Advanced Malware Detection and Analysis

Integrated for Day One Value

The ReversingLabs Malware Protection (MWP) feed and A1000 Malware Analysis Platform each deliver game-changing solutions for detection, reputation assessment and analysis of advanced cyber threats in files. Ziften's continuous endpoint visibility solution uses critical data to provide a unique capability that further extends unprecedented insights. With this integration, organizations are enabled to efficiently prevent security exposures and respond to advanced threats.

Ziften solutions are purposely architected for day one value with three key components:

View | Continuously monitor every endpoint on and off the network, along with the contextual behavior of users

Inspect | Rapidly analyze the level of risk using behavioral context, input from existing tools and threat intelligence

Respond | Accelerate remediation and response in order to contain threats before they spread using automated workflows to eliminate both alert fatigue and manual processes in order to deliver only pertinent intelligence for immediate response

ReversingLabs
TitaniumCloud™ Threat Intelligence

The ReversingLabs TitaniumCloud™ File Reputation Service provides the industry's most comprehensive source for threat intelligence and reputation data on over 2.5B goodware and malware files. ReversingLabs acquires over 2 million files daily and processes them with unique "deep content inspection" technology. Threat information is then made available as a file reputation feed to Ziften customers through easy integration into their endpoint solutions.

To select relevant content for its daily feed, ReversingLabs leverages its Deep Content Inspection technology that includes automated static analysis to expose internal threat indicators, functional similarity comparison to known malware and continual rescanning providing historical detection information. TitaniumCloud identifies threats in files by examining internal characteristics and capabilities rather than observing behavioral symptoms. Results of these analyses are then published in its feeds.

Drill-Down Visibility for Immediate Response

In this integration, Ziften and ReversingLabs are providing a limited time offer to Ziften customers wherein ‘interesting’ files identified by Ziften solutions can be automatically checked against the ReversingLabs reputation database, returning real-time file threat intelligence based on hourly updates against the most current and actionable information. Additionally, the Ziften solution will provide a link to the ReversingLabs A1000 Malware Analysis Platform for deeper inspection, unpacking and advanced analysis of files identified as ‘suspicious’ or ‘malicious’ by the customer at no charge during this offer. Links will remain in place and the customer will be able to continue the A1000 analysis option offer subsequent to the expiration of this offer by subscribing directly with ReversingLabs.

About Ziften

Ziften solutions take the complexity, time, and cost out of threat detection with a solution that deploys and can be utilized in minutes, not days. Ziften’s continuous monitoring solution helps organizations quickly detect and stop threats, monitor for vulnerabilities and exposures, and identify abnormalities utilizing context-rich historical data. Ziften’s ZFlow technology extends network telemetry down to the endpoint, providing critical “last mile” network visibility with rich endpoint context. By pairing end-to-end visibility with actionable intelligence, Ziften customers secure their environment and protect their reputation.

https://ziften.com

About ReversingLabs

ReversingLabs solutions provide enterprises and security vendors a foundation for protecting digital assets. These solutions enable security professionals to detect and analyze the latest and most advanced cyber threats on computers, mobile devices and embedded systems. The ReversingLabs Malware Protection (MWP) feed and A1000 Malware Analysis Platform each deliver game-changing solutions for detection, reputation assessment and analysis of advanced cyber threats in files. The platform classifies files by binary content as well as their complexity and sophistication enabling classification based on whether the files contain embedded executable content, obfuscated JavaScript or implement a known exploit.

www.reversinglabs.com