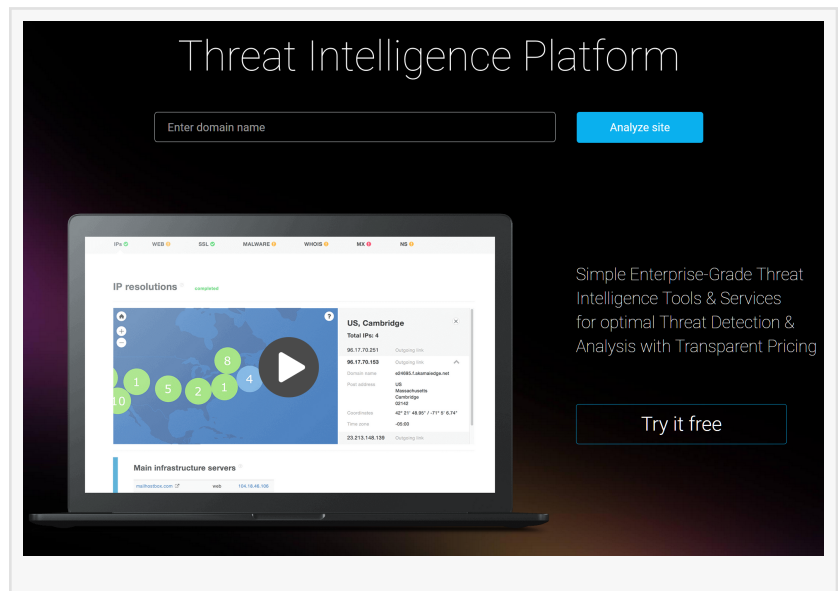


How Threat Intelligence Platform is Utilizing a Unique Approach than other Cyber Security Companies

Threat Intelligence Platform Utilizing Unique Context-Based Cybersecurity Approach for Monitoring Third-Party Reliability and Efficient Resource Allocation

SAN FRANCISCO, CALIFORNIA, USA, February 19, 2019 /EINPresswire.com/ -- Threat Intelligence Platform, a California-based data, tool, and API provider specializing in automated threat detection, security analysis and threat intelligence solutions for Fortune 1000 and cybersecurity entities, has pushed to the front of the cybersecurity pack by utilizing a unique content-based approach for monitoring third-party reliability/safety and efficient resource allocation.



“Businesses today vary in their approach to operating data and information systems and, as such, evaluating IT infrastructure according to standardized auditing routines for cybersecurity just isn’t enough,” states Jonathan Zhang, founder, and CEO of Threat Intelligence Platform. “Many aspects must be taken into consideration, including industry, size and system-specific configurations. This is where our deployment of a context-based cybersecurity system comes into play; rather than taking a one-size-fits-all stance, our engineers are able to explore risks proactively while future-proofing systems from attacks and accidents.

“

At the end of the day, threat intelligence provides a framework to stop cybercriminals from finding new ways to exploit countless online assets and deceive users into committing errors”

Jonathan Zhang

“This is accomplished by checking the computing infrastructure in a risk-based method across various parameters and recommending what needs to be done,

making the overall process cost-effective while investigating all conceivable situations within a given context and confirming or negating assumptions regarding threats and risks with precision.”

With regard to monitoring third-party reliability and safety, Threat Intelligence Platform representatives point to the way businesses – as they grow and become more successful – rely more on third-party tools and services, and how this is providing cybercriminals the opportunity to gain access to these businesses via partners and suppliers with more lenient security practices. Threat Intelligence Platform, in response, examines the connections to third parties

with which sensitive information is frequently shared, an investigation that ultimately assesses the reliability and safety of third-party providers' systems – both prior to their selection and throughout a contract's implementation.

Threat Intelligence Platform analysts also help clients optimize the allocation of their security budgets, establishing more secure systems, upgrading security protocols and correcting system anomalies. Meanwhile, management and users involved are advised on what they can do to protect their data and systems, reduce human errors and, at times, even change their cybersecurity roadmap.

“At the end of the day, threat intelligence provides a framework to stop cybercriminals from finding new ways to exploit countless online assets and deceive users into committing errors,” concludes Zhang.

The unique draw of Threat Intelligence Platform remains its provision of fundamental building blocks for constructing cybersecurity, threat hunting/defense, and cyber threat intelligence applications and platforms. The company's system offers easy-to-use threat intelligence tools, services and APIs to obtain detailed information about hosts and the infrastructure behind them, gathering data from various providers, utilizing substantial internal databases – compiled for more than 10 years – and real-time host configuration analysis.

Threat Intelligence Platform is part of the Whois API Inc. Family, an intelligence vendor trusted by over 50,000 clients. For more information visit <https://threatintelligenceplatform.com> or email support@ThreatIntelligencePlatform.com.

Zed Augustine
Threat Intelligence Platform
+1 800-207-0885
[email us here](#)

This press release can be viewed online at: <http://www.einpresswire.com>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases. © 1995-2019 IPD Group, Inc. All Right Reserved.