Trellix

Trellix Advanced Threat Landscape Analysis System

Gain a unique and global insight into malicious threats.

The Advanced Threat Landscape Analysis System (ATLAS) is a cutting-edge data analysis tool provided by Trellix. ATLAS gives customers a unique, global insight into malicious file, domain, and IP detections, leveraging data gathered worldwide by billions of Trellix sensors. With its geospatially enabled situational awareness and powerful analytics, customers better understand the evolving threat landscape and can react promptly and effectively to secure their assets

Solving Customer Problems

ATLAS is designed to address critical customer problems in the cybersecurity domain. Organizations have top-priority, highly sensitive data that are under constant threat from evolving global cyberthreats. ATLAS provides situational awareness based on the types of threats targeting the organization, allowing for focused and efficient internal analysis.

Key Benefits

- Unique global insight into the malicious threat detections seen worldwide by Trellix.

- Geospatially enabled situational awareness.

- Utilize the Trellix telemetry data collected worldwide.

- View current and emerging threats by highlighting those of particular interest by type, industry sector, geolocation, most seen, etc.

- Correlate Trellix telemetry with the latest contextual threat intelligence containing campaign data provided by Trellix as well as open-source data.

- Access to a dedicated view for campaigns consisting of events, dates, threat actors, IOCs, threat tools, threat categories, MITRE ATT&CK patterns, countries, and more.

- Includes dashboards for threat intelligence created by ARC, including vulnerability intelligence consisting of the latest high impact vulnerabilities.

- Flexible and dynamic. Users can craft queries and filter results in any view, using any combination of fields present in ATLAS.

Harnessing the strength of both enterprise resources and the cloud, Trellix provides a hybrid environment that significantly enhances threat intelligence. Through our private cloud and single-tenant-dedicated environment, organizations can securely tap into our threat intelligence solutions, enabling the efficient sharing of critical information across the enterprise. Trellix offers both on-premises and off-premises cloud services, empowering your organization to deploy global or regional cloud services as needed, aligning to your specific requirements.

In this digital age, the integration of various data sources is crucial in building an effective threat intelligence system. Our ATLAS platform collects and aggregates data from diverse Trellix sources. The data is further enriched with crucial details like industry sector and geolocation, offering an up-to-date, global view of emerging threats.

Data Aggregation and Enrichment & Threat Correlation

ATLAS employs a sophisticated approach to threat correlation, providing a comprehensive view of cyber campaigns. By correlating aggregated threat data with campaign details, ATLAS delivers a detailed perspective on events, dates, threat actors, indicators of compromise (IOCs), and more enriching the investigation and analysis with meaningful context.

Real-Time Threat Detection & Contextual Threat Intelligence

ATLAS provides real-time visibility into current and emerging threats, highlighting those of specific interest based on type, source/destination, and geolocation. Utilizing the extensive telemetry data collected by Trellix, ATLAS offers a real-time global view of malicious threat detections and their severity.

The platform also enhances Trellix telemetry with the latest contextual threat intelligence, including campaign data, threat actor and tool profiles, and vulnerability intelligence. This intelligence is enriched with open-source data, empowering customers to understand and counter threats effectively.

Vulnerability Intelligence & Dashboards

ATLAS offers a dedicated view of the latest high-impact vulnerabilities, analyzed by industry experts. This feature ensures timely and informed responses to these threats, aiding in the mitigation and prevention of potential breaches.

Furthermore, ATLAS includes several standard dashboards for IOCs, threat actors, and campaigns, each providing unique visualizations and
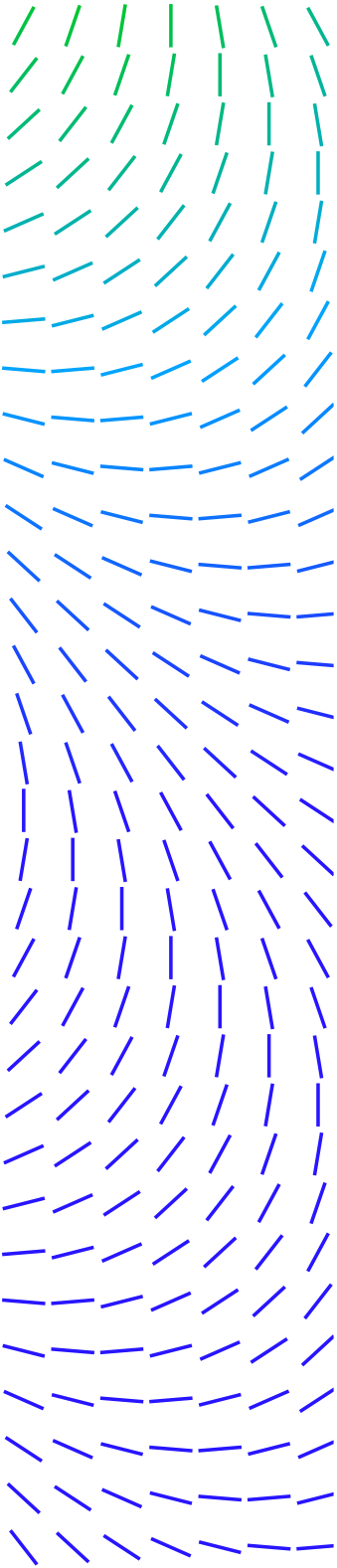
workflows. These dashboards offer insights into the prevalence of malicious IP addresses, files, and URLs, equipping customers with comprehensive situational awareness of the global threat landscape. ATLAS also allows users to craft queries and filter results, offering a custom approach to data analysis.

Trellix's hybrid threat intelligence solutions offer an advanced, multi-faceted approach to threat intelligence, providing your organization with the tools to navigate the cybersecurity landscape confidently and proactively.

Don't wait for the next attack to happen. Prevent it.

At Trellix, we give our customers the most comprehensive picture possible. Our cybersecurity experts track threat actors as well as campaigns, techniques, and tools the attackers use so we can better equip you to prevent future attacks and enhance your situational awareness giving you a more actionable view of threat exposures.

Want to learn more about Trellix Threat Intelligence and speak to an expert or schedule a demo? Visit https://www.trellix.com/en-us/platform/threat-intelligence.html. And to learn more about Trellix's other products and services, visit trellix.com.

062023-01

Trellix