



POWERED BY
Business Integra






*Driving Enhancements in
Cyber Threat Intelligence*

As the cyber threat intelligence data landscape continues to evolve every day, and the world becomes more saturated with data, the goal is to shift the focus toward taking action on insights – and away from laborious data engineering cycles to make sense of all the data.

Power and Precision – The perfect combination for supporting cyber situational awareness.

To ensure cyber situational awareness, at all times, Business Integra (BI)'s **Threatelligence** solution was built to support cyber leaders who need to be the first to know. Cyber situational awareness is a complex objective, so we built our solution to use a multi-dimensional approach that pulls together experience, expertise, and powerful components (*Table 1*) to offer a total end-to-end solution.

Table 1: Components of BI's **Threatelligence** Solution

<p>Trellix's ATLAS serves as the base for the solution</p> 	<p>Active AI/ML deep learning capabilities, backed by current R&D</p>	<p>Use of CMMI Level 5 appraised processes to support project management</p>  	<p>Access to specialized, industry experts and the latest threat research</p>
<p>Data Scouts</p>	<p>Secure Portal</p>	<p>Customizable Views</p>	<p>Computing Power</p>

Using the team's understanding of CTI, BI's solution is focused on providing the richest, most useful CTI and threat data, bringing it for consideration, consumption, and use. Thus, the environment itself is viewed as a living solution. that continuously matures its integrations and refines its development to provide high-value threat intelligence and reporting – on a scheduled and ad-hoc basis. Additionally, the **Threatelligence** solution relies on human and machine-based

interactions with threat data to maintain a thorough understanding of malicious cyber actors' characteristics, methods, and objectives – ultimately providing a comprehensive level of understanding to support situational awareness. While the CTI data provided is initially based on the Trellix ATLAS framework, **Threatelligence** is an extendable platform, allowing CTI data sources to be added.

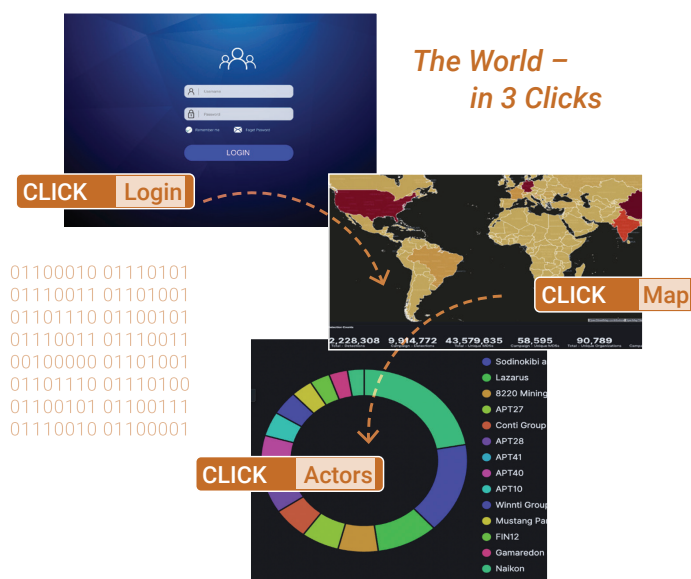
ATLAS – It's all in the details.

The standard ATLAS Dashboard includes default views for the prevalence of malicious IP addresses, files, and URLs that empower comprehensive situational awareness of the global threat landscape. Each of these views provides the following data at a glance in *Table 2*.

Table 2: ATLAS Dashboard Default Views

- Global Heat Map of Malicious Detections
- Malicious File/URL/IP Detection Counts
- Top Industry Sectors Affected
- Top File Hashes/URL Domains/IPs detected
- Top Organizations Affected
- Top Categories (URL)
- Top Client Country Codes Affected
- Top Destination Country Codes (IP)
- Top Products Providing Detections
- Product Type
- Threat Timeline
- Client Timeline
- Top MITRE ATT&CK Patterns

Data scientists no longer need to spend hours cleansing and rearranging data sets to decipher them and build patterns.



SOLUTION HIGHLIGHTS

- Use of Trellix's Advanced Threat Landscape Analysis System (ATLAS), providing global reach that is tuned and correlated to what is happening in networks
- Ability to leverage existing Machine Learning (ML) products that already support the IC
- ML models that enable correlation and predictions between global (outside) and internal activity views
- CTI – ability to provide a threat activity view
- Proven capabilities and tools that provide the ability to stay in front of the threat

- Ability to access credible and actionable data ahead of other sources, on both the high and low side
- “The World in 3 Clicks” – zoom in to any location, simply and quickly
- Ready Day 1 – Simple, quick and easy web access installation

Schedule a demo today!

growth@businessintegra.com



BusinessIntegra.com