Use Case: Insider Threat Detection

Monitor for insider threats and vulnerabilities

The situation

Insider threats do not discriminate, permeating all industries and corporations of all sizes. According to the Ponemon Institute, as of 2022 insider threat incidents have risen 44% over the previous two years,[1] and the recent paradigm shift to a virtual workforce has created an even more vulnerable environment. The majority of threats result from employee negligence, with workers sharing confidential information over insecure infrastructure. Malicious insider threats, while fewer in number, are the most financially damaging to any organization.

Regardless whether the insider threat is malicious or accidental, either type of threat can cripple a company's infrastructure and cause significant monetary and reputational loss. Depending on the type of incident, scope of problem, and location, there may also be productivity loss and/or compliance implications.

Our PAI solution

Babel Street enables organizations to keep watch around the world 24/7/365 to uncover any potential insider risks – whether it is from compromised technology, malicious sabotage, or unintentional carelessness.

Are there risks within your organization?

Babel Street empowers teams with actionable insights to monitor for threats and vulnerabilities and minimize harm to the organization.

Babel Street's analytics platform offers an AI-enabled cross-lingual, persistent search of thousands of global and regional publicly available information (PAI) sources in over 200 languages to rapidly discover and decipher insights on potential indicators of malicious behavior or insider threats. Machine learning algorithms constantly monitor social media, the deep and dark web, and message boards for the likelihood of any threat. These insights are automatically translated into your native language and presented on a single pane of glass for analysis, and response.

Business impact

Constant vigilance acts as an early warning system to identify suspicious activity and allows for the best security countermeasures to guard against future insider threats.

PAI DATA SOURCES	DATA STREAMS	FILTERS	KNOWLEDGE
• 50,000+ hyper local & global news sites • Billions of blogs & message boards • 50+ social media/ consumer review sites • Dark web	• Entity and brand name variants • Products • Domains • Geolocation • Relevant user handles • Phones • Addresses • Emails	• Temporal • Keywords • Exclusions • Intent • Geo vernacular • Language • Regular expressions	• Insider threats • POIs & GOIs • Linkages • Consumer sentiment • Loss prevention • Brand reputation impact • Images of interest • Disgruntled employees/ customers • Compromised IP

1 Ponemon Institute, "2022 Cost of Insider Threats Global Report," 2022. https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats