BABELSTREET

USE CASE

Using Babel Street to Detect and Mitigate Insider Threats

Employee mistakes, negligence, and malice all threaten businesses and government agencies. According to the Ponemon Institute, simple errors and negligence account for 55 percent of all insider threats.[1] These threats typically include exposure of sensitive or proprietary data caused by phishing or social engineering attacks, the use of weak passwords, or employees unthinkingly exposing confidential information in their social media posts.

Of course, some workers also deliberately engage in malicious or criminal acts against their employers. These acts may include theft of intellectual property, corporate espionage, or corporate sabotage. These willful actions account for the remaining 45 percent of insider threats.[2]

Mitigating insider threats with OSINT

Whether an insider threat is accidental or malicious, it can cause significant monetary loss and reputational damage. To combat these threats, organizations need holistic risk management programs. These typically consist of risk and impact assessments, and mitigation activities. Perhaps most important is the overall threat awareness that open-source intelligence (OSINT) technologies can provide. Through social media monitoring and other capabilities, Babel Street solutions can help organizations better identify and mitigate the damage from insider threats.

Using Babel Street to find insider threats

Here are the steps analysts can take to spot insider threats using Babel Street Insights.

Proactively search for suspicious behavior

Investigators can structure a search query focused on a specific individual, company, or key words/phrases around a product or brand. Babel Street Insights allows users to monitor specific social media sites and the dark web for irregular activity. Insights can also persistently monitor specific URLs with a web-crawling capability that scrapes data three levels down. Instant or daily alerts can be established to notify investigators if any search criteria are triggered.

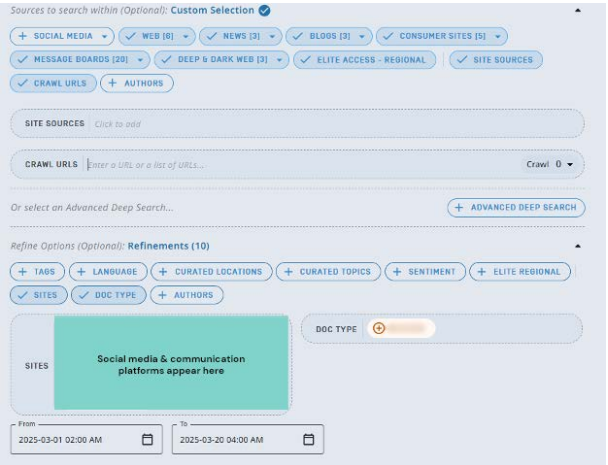

Figure 1: An Insights search targeting types of sites and specific sites

Investigate suspicious activity

Once an individual has been identified as a potential insider threat, or displays characteristics of insider threat activity, investigators can look for other compromising indicators, such as lifestyle changes, legal problems, debt, etc. For extra protection during investigations, Babel Street Secure Access allows users to analyze publicly available information in a secure, isolated environment.

Map social networks

Investigators can employ Babel Street Synthesis to map the social networks of suspected insider threats. Synthesis can identify relationships that would otherwise go undetected and assist in characterizing those connections.

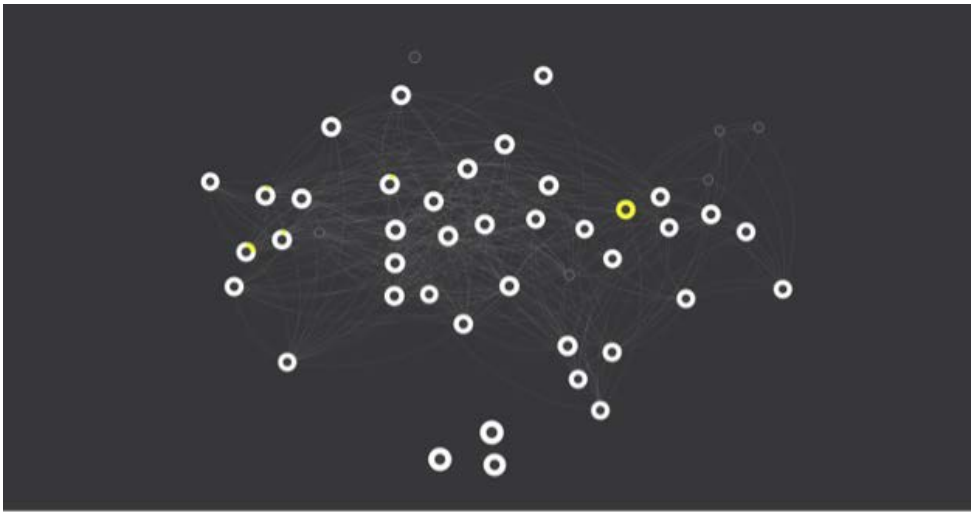

Figure 2: Anonymized output from Babel Street Synthesis shows connections within a social network

Endnotes

[1] Ponemon Institute, "2022 Cost of Insider Threats Global Report," accessed February 2025, https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats

[2] Ibid

Babel Street is the trusted technology partner for the world's most advanced identity intelligence and risk operations. The Babel Street Insights platform delivers advanced AI and data analytics solutions to close the Risk-Confidence Gap.

Babel Street provides unmatched, analysis-ready data regardless of language, proactive risk identification, 360-degree insights, high-speed automation, and seamless integration into existing systems. We empower government and commercial organizations to transform high-stakes identity and risk operations into a strategic advantage.

Learn more at **babelstreet.com.**

BABELSTREET