BABELSTREET

USE CASE

Babel Streetによる内部脅威の検知と抑制

従業員のミス、過失、悪意はすべて、企業や政府機関にとり脅威となります。Ponemon Instituteによると、単純なミスや過失が内部脅威全体の55%を占めています[1]。これらの脅威には通常、フィッシングやソーシャルエンジニアリング攻撃による機密データや専有データの漏洩、脆弱なパスワードの使用、従業員がSNSへの投稿で機密情報を不用意に暴露することなどが含まれます。

もちろん、意図的に雇用主に対して悪意ある行為や犯罪行為を行う労働者もいます。このような行為には、知的財産の窃盗、企業スパイ、企業破壊行為などが含まれます。このような故意の行為が、内部脅威の残り45%を占めています[2]。

OSINTで内部脅威を軽減

内部脅威は、偶発的なものであれ悪意あるものであれ、多大な金銭的損失と風評被害をもたらす可能性があります。このような脅威と闘うために、組織には総合的なリスク管理プログラムが求められます。こうしたプログラムは通常、リスクと影響の評価、および抑制活動で構成されます。おそらく最も重要なのは、オープンソースインテリジェンス（OSINT）テクノロジーの活用によりもたらされる全体的な脅威認識でしょう。Babel Streetのソリューションは、SNSモニタリングやその他の機能を通じて、内部脅威の特定と被害の軽減を支援します。

Babel Streetを利用して内部脅威を発見する

Babel Street Insightsを使用してアナリストが内部脅威を発見するための手順を紹介します。

不審な行動を積極的に検索

調査員は、特定の個人、企業、または製品やブランドに関するキーワード/フレーズに焦点を当てた検索クエリを構成することができます。Babel Street Insightsは、特定のSNSサイトやダークウェブでの不自然な活動を監視することができます。Insightsはまた、3階層下のデータをスクレイピングするウェブクローリング機能により、特定のURLを持続的に監視することができます。インスタントアラートまたはデイリーアラートを設定すれば、検索条件にヒットした場合に調査担当者に通知することができます。

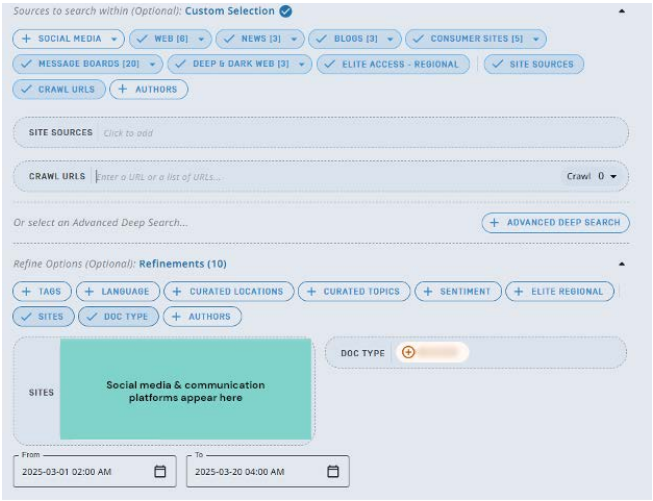

図 *1:* サイトの種類や特定のサイトを対象とした*Insights*検索

不審な活動を調査

ある個人を潜在的な内部脅威として特定できた、または個人が内部脅威活動の特徴を示した場合、調査者は対象者に関して、ライフスタイルの変化、法的問題、負債など、内部脅威活動につながりかねない危険な指標が他にないかを探します。調査中に調査官や調査機関を危険にさらすことがないよう、Babel Street Secure Accessを活用することで、ユーザーは安全で隔離された環境で公開情報を分析することができます。

SNS上でのつながりをマッピング

調査官は、Babel Street Synthesisを利用して、内部脅威の疑いのある人物のSNS上のつながりをマッピングすることができます。Synthesisは、通常なら見逃してしまう関係を特定し、それらのつながりの特性を示す手伝いをします。

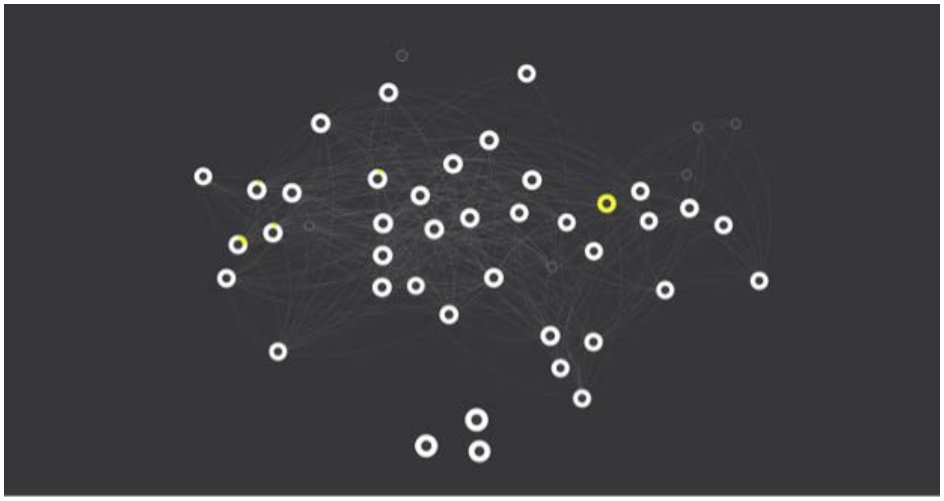

図 2：*SNS*内のつながりを示す*Babel Street Synthesis*の出力（掲載にあたって匿名化されています）

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 は、世界で最も高度なアイデンティティ・インテリジェンスとリスク管理を可能にする、信頼、実績のあるテクノロジーパートナーです。 Babel Street Insights プラットフォームは、リスクと信頼のギャップを埋める高度な AI およびデータ分析ソリューションを提供します。

Babel Street は、言語を問わず他に類を見ない分析対応データ、能動的なリスク識別、360 度のインサイト、高速自動化、既存システムへのシームレスな統合を提供します。 当社は、政府機関や企業組織が、重要なアイデンティティおよびリスク管理を戦略的な優位性に変換できるように支援します。

詳細については、babelstreet.jp をご覧ください。

BABELSTREET