



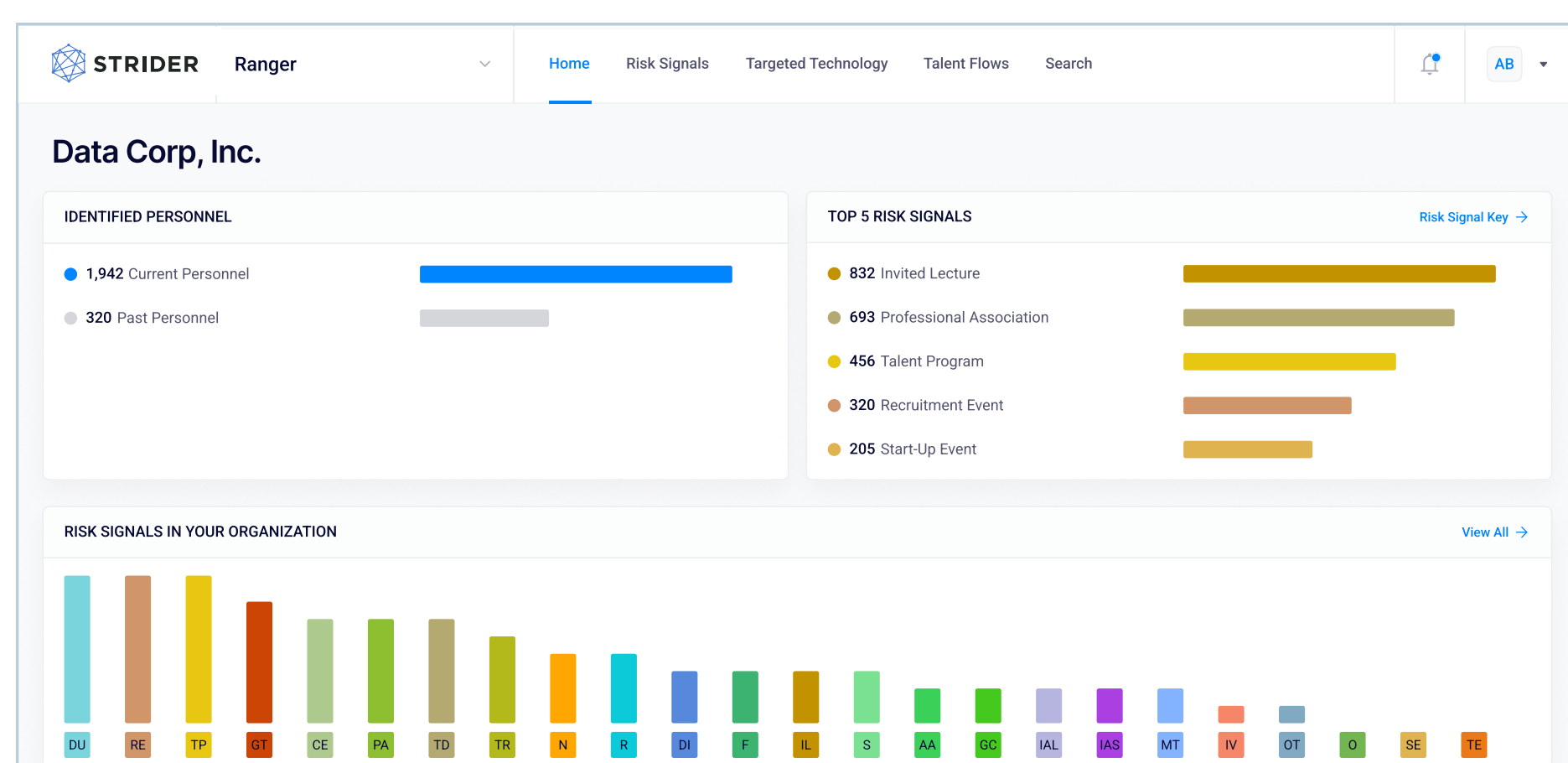
STRIDER

RANGER

貴組織内のテクノロジーと人材を標的とする経済安全保障リスクを特定し、対応します。

世界中の国家支援型脅威アクターは、国家の目標を進めるために、官民両セクターをますます標的にしています。これらのアクターは政府、企業、研究機関から技術と人材を抽出するために、融合型の洗練されたアプローチを取っています。

Rangerは、史上初の、組織内に存在する国家支援型の経済安全保障リスクを特定および可視化して対応できるようにした「サービスとしてのデータ」（DaaS）製品です。Strider独自のオープンソース手法を活用したRangerは、国家支援型脅威アクターによって頻繁に標的とされている技術や人材を貴組織が特定し、事前に防御を確立するのに役立ちます。



Rangerは、以下を通じて戦略的インテリジェンスを提供します。

Targeted Technology (ターゲットテクノロジー)

組織の主要技術と、国家支援型脅威アクターが標的とする技術の共通部分を理解しましょう。ターゲットテクノロジーは、産業界、政府、政策文書、その他の公的情報源を使用して、貴組織の技術のうち、国家支援型脅威アクターが求めている部分を明らかにします。

Risk Signals (リスクシグナル)

国家支援型脅威アクターが貴組織の人材に近づくために活用する可能性があるつながり/人脈に光を当てます。リスクシグナルは、貴組織の人材と国家支援型脅威アクター間の高リスクのつながり/人脈を20種類以上特定します。

Talent Flows (人材フロー)

社員の入退社の流れを追跡し、人材を確保しましょう。人材フローは、貴組織と業界全体にわたる人材の移動状況を示します。これには、離職する社員の上位40の職位と、同様の人材を引き付ける上位40の競合他社が含まれます。

ゼロタッチアーキテクチャ:

内部クライアントのデータを必要としません。

データ来歴:

フラグが付けられたリスクはすべて、法的に利用可能な情報源から入手しています。



サプライチェーン・ネットワークの安全性とコンプライアンスを確信を持って保証する方法をご覧ください。詳細については、以下からデモをご依頼ください。

striderintel.com/request-demo

