石油・ガス産業を支援するStrider

知的財産、事業運営、グローバル・サプライチェーンを国家主体の脅威から守ります

概要

石油・ガス産業は国家主体の脅威に絶えずさらされています。探査の革新的発見、精製プロセス、材料化学の副生成物に関する知的財産は頻繁に標的にされています。グローバル規模の事業やパートナーシップでは、企業はサプライチェーン、合弁事業、人材に潜むリスクにさらされます。同時に攻撃者は、事業を妨害して戦略的優位を得るために、活発にデジタル・アクセス・ポイントを探し回っています。

Striderは業界最高水準の戦略的インテリジェンス・プラットフォームを提供し、そのようなリスクの軽減を支援します。オープンソースのデータとStrider独自のリスク評価方法を組み合わせることで、イノベーション・パイプライン、事業活動、評判を損なう可能性のある隠れた脅威を明らかにします。

石油・ガス企業はStriderで次のことが可能になります。

- 探査、精製、材料化学の副生成物に関する重要な知的財産を保護します。
- 従業員、請負業者、経営層の来訪者をスクリーニングして、リスクの高い関係性や虚偽の経歴がないかを確認します。
- グローバル・サプライチェーン、合弁事業、事業提携における隠れたつながりを明らかにします。
- 既知の国家アクターに関連付けられる攻撃者の通信をブロックしてサイバー防御を強化します。

Striderを使用して知的財産の保護、サプライチェーンの透明性、人材の審査を一つのプラットフォームで統合することで、石油・ガス業界のリーダーは、資産と事業活動の安全性を確保しながら、競争力と優位性を維持できます。

危険にさらされているもの

石油・ガス産業は、高まる地政学的リスク、サイバー・リスク、内部リスクに直面しています。最近のインシデントから、侵害されたデータ、サプライチェーン・パートナー、あるいは物理的インフラストラクチャによって、いかにして世界中に影響を与えるような脆弱性がもたらされるのかがわかります。

- **Halliburtonへのサイバー攻撃（2024年）**– ランサムウェア攻撃によってHalliburtonはシステムを停止せざるを得なくなりました。[1]
- **Oiltanking GmbHとMabanaftへの攻撃（2022年）**– サイバー攻撃によってドイツ国内の燃料供給に混乱が生じ、Shellは石油供給ルートの変更を余儀なくされました。[1]
- **石油・ガス分野の研究開発における知的財産窃盗（2022年）**– 独自の探査データや化学的副生成物に関する研究成果が、事業提携や合弁事業を介して盗まれるケースが発生していますが、専門家は、石油・ガス分野の知的財産がスパイ活動の標的になっていることへの認識が十分ではないと警告しています。[2]
- **タンカーによる破壊工作 – イーグルS（2025年）**– 石油タンカーが海底でアンカーを引きずり送電ケーブルと複数の海底通信ケーブルを損傷させ、6,000万～7,000万ユーロの損害を引き起こしたとして、フィンランド当局は石油タンカーの乗組員を重大な破壊工作の疑いで起訴しました。[3]

身元を偽装した請負業者であれ、隠れたつながりを持つ合弁事業パートナーであれ、危険な海域を通るタンカーであれ、たった一つ弱点があるだけで、外国勢力が悪用できる状態に企業全体が陥れられてしまう可能性があるのです。

[1] https://www.juvare.com/the-halliburton-cyberattack-a-wake-up-call-for-critical-infrastructure-cybersecurity/?
https://www.mcgriff.com/resources/articles/cyberattack-forces-oil-and-gas-services-provider-Halliburton-to-take-systems-offline/
[2] https://www.iqpc.com/media/8657/15220.pdf
[3] https://www.theguardian.com/world/2025/aug/11/finland-accuses-tanker-crew-sabotage-undersea-cables-anchor

対応を怠った場合には次のことが起こる可能性があります。

- **知的財産および研究開発の窃取** – 精製や材料化学における革新的開発が窃取されることで、何億ドルもの投資の損失につながります。
- **供給の停止** – サイバー攻撃や損傷したインフラにより操業が停止します。
- **規制当局による監視および罰金** – OFAC、CFIUS、国際的な制裁の枠組みの対象となるリスクがあります。
- **社会的信用の低下** – 国家の支援を受けたアクターと関連付けられることで評判が損なわれます。

エネルギー企業を支援するためのStriderの機能

機能	どのように役立つか	Strider製品の活用例
知的財産および研究開発パイプラインの保護	国家アクターが接触する可能性が高い技術や専門人材を特定し、化学的副生成物のイノベーションと材料化学の進歩を保護します。	**Insights** リスクの高い技術と専門人材を正確に特定します。 **People Search** 採用者、請負業者、訪問代表団を審査して、国家とのつながりや身元の偽装がないかを確認します。
グローバル・サプライチェーンとパートナーシップの安全性の確保	隠れた所有関係、事業を介した結びつき、処理提携業者をマッピングして、重要な投入資源、合弁事業、原料供給業者において国家が関与する影響力を明らかにします。	**Organizations Search** 多層的なサプライヤー、顧客、株主のつながりを明らかにします。 **Insights** 新たな地政学的リスクや提携リスクについて経営層向けの報告書を作成します。
サイバーとフィジカルのレジリエンスの強化	既知の攻撃者につながる高リスクの通信に警告を出してブロックし、厳選されたセレクターをフォレンジック調査で活用します。	**Shield** 攻撃活動に関連付けられた悪意のあるドメイン、メール、多言語キーワードをフィルタリングします。 **People Search** 警告が出された個人に対して行われる内部調査を支援します。

事業運営と知的財産を守る準備はできましたか？

ぜひデモをご予約ください。Striderの**戦略的インテリジェンス・プラットフォーム**が、研究開発投資の保護、グローバル・パートナーシップの安全性の確保、変化する規制へのコンプライアンス維持などを通じて、どのように最前線での防御を強化するのかをご紹介します。

デモを申し込む →