STRIDER FOR THE OIL & GAS SECTOR

Safeguarding IP, Operations, and Global Supply Chains From Nation-State Threats.

Overview

The oil & gas sector faces persistent nation-state threats. Intellectual property from exploration breakthroughs, refining processes, and material-science byproducts are frequent targets. Global operations and partnerships expose companies to hidden risks in supply chains, joint ventures, and personnel. Meanwhile, adversaries actively seek digital access points to disrupt operations and gain strategic advantage.

Strider provides the leading Strategic Intelligence Platform to identify and mitigate these risks. By combining open-source data with our proprietary risk methodology, we surface hidden threats that could compromise innovation pipelines, operations, and reputation.

Oil & Gas companies use Strider to:

- Protect valuable intellectual property in exploration, refining, and material-science byproducts.
- Screen employees, contractors, and executive visitors for risky affiliations or falsified credentials.
- Uncover hidden ties in global supply chains, joint ventures, and venture partnerships.
- Strengthen cyber defenses by blocking adversary communications tied to known state actors.

By uniting IP protection, supply chain transparency, and personnel vetting in one platform, Strider enables oil & gas leaders to secure their assets and operations while staying compliant and competitive.

What's at Stake

The Oil & Gas industry faces increasing geopolitical, cyber, and insider risks. Recent incidents highlight how compromised data, supply chain partners, or physical infrastructure can introduce vulnerabilities with global consequences:

- **Halliburton Cyberattack (2024)** – A ransomware attack forced Halliburton to take systems offline.[1]
- **Oiltanking GmbH and Mabanaft Attack (2022)** – A cyberattack disrupted fuel distribution in Germany, forcing Shell to reroute oil supplies.[1]
- **IP Theft in Oil & Gas R&D (2022)** – Proprietary exploration data and chemical byproduct research have been stolen via partnerships and joint ventures, with experts warning that Oil & Gas intellectual property is an under-recognized target for espionage.[2]
- **Tanker Sabotage – Eagle S (2025)** – Finnish authorities charged the crew of an oil tanker with aggravated sabotage after dragging its anchor across the seabed and damaging multiple undersea cables and a power link, causing €60–70M in damages.[3]

Even a single weak link—whether a contractor with falsified credentials, a joint venture partner with hidden ties, or a tanker in hostile waters—can expose the entire enterprise to foreign exploitation.

[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

Failure to Act Can Lead to:

- **IP & R&D Theft** – Hundreds of millions in lost investment from stolen refining or materials-science breakthroughs.
- **Supply Disruptions** – Operations halted by cyberattacks or damaged infrastructure.
- **Regulatory Scrutiny & Fines** – Exposure under OFAC, CFIUS, and international sanctions regimes.
- **Loss of Public Trust** – Reputation damage from association with state-sponsored actors.

What Strider Does for Energy Companies

CAPABILITY	HOW IT HELPS	STRIDER PRODUCTS IN ACTION
Protect Intellectual Property and R&D Pipelines	Identify targeted technologies and subject-matter experts most likely to be approached by state actors; safeguard chemical byproduct innovation and material-science advances.	**Insights** Pinpoint at-risk technologies and experts. **People Search** Vet hires, contractors, and visiting delegations for state ties or falsified credentials.
Secure Global Supply Chains & Partnerships	Map hidden ownership, venture ties, and processing partners to uncover state-sponsored influence in critical inputs, joint ventures, and feedstock suppliers.	**Organizations Search** Expose multi-tier supplier, customer, and shareholder ties. **Insights** Generate reports for leadership on emerging geopolitical and partner risks.
Strengthen Cyber & Facility Resilience	Flag and block high-risk communications tied to known adversaries; leverage curated selectors in forensic investigations.	**Shield** Filter malicious domains, emails, and multilingual keywords tied to adversary campaigns. **People Search** Support internal investigations of flagged individuals.

Ready to Secure Your Operations & IP?

Schedule a demo to see how Strider's **Strategic Intelligence Platform** can strengthen your frontline defenses—protecting R&D investments, securing global partnerships, and ensuring compliance with evolving regulations.

REQUEST A DEMO →