Cyber Security in the Oil and Gas Industry

Security by challenge, not testing.

There are many facilities that supply diesel oil, gasoline, petrochemicals, natural gas and more to the many aspects of our daily lives. Even the smallest supply chain or information system infiltration can affect every aspect of our lives.

**OIL AND GAS POWER OUR LIVES**

Many of the largest industries in America are considered critical infrastructure sectors. In the last 12 months, 38% of cyberattacks on the oil and gas industry are from a virus or worm while 37% of cyberattacks on the oil and gas industry are ransomware.

**THE CURRENT STATE**

$1.87 billion will be spent on cyber security by the oil and gas industry in 2019.

46% of cyberattacks on the oil and gas industry are automated.

87% of oil and gas companies feel underappreciated. 30% feel underappreciated by customers.

**FIGHTING THIS TREND**

Traditional classroom training can get expensive. Project Ares enables your team to train against real-world scenarios and threats, anytime, anywhere, for a much lower cost.

**Project Ares**

- **Modular and Transform Oil and Gas Cybersecurity Readiness**
- **Low Cost Training**
- **Better Retention**

Project Ares, equipped with powerful AI, aggregates best practices from player behavior which you can then teach to your entire team. Team performance is elevated as best practices are collected and taught.

- **Lower Training Cost**
- **Better Retention**
- **Better Retention**

To increase cyber team performance in IT and OT for oil and gas sectors, organizations can adopt continual learning opportunities for teams to grow in cyber skill and competency to stop threats before they hit a network.

- The information security sector has been dealing with traditional security for decades.
- Enterprises can engage with Project Ares to improve security response and threat hunting.
- The problem allows your team to practice these skills against the latest threats.

Get the Project Ares Demonstration.