IQUILA
SOFTWARE DEFINED NETWORKS

CYBERSECURITY FOR THE OIL AND GAS INDUSTRY

Like critical industries everywhere, Oil and Gas operations make prime targets for cyber threats of all kinds. Unlike many of the less specialised industries however, Oil and Gas utilises a wide array of proprietary communication protocols, as well as standard protocols that are more commonplace, making it harder to balance access/control with security, thus creating a broader field for intrusion.

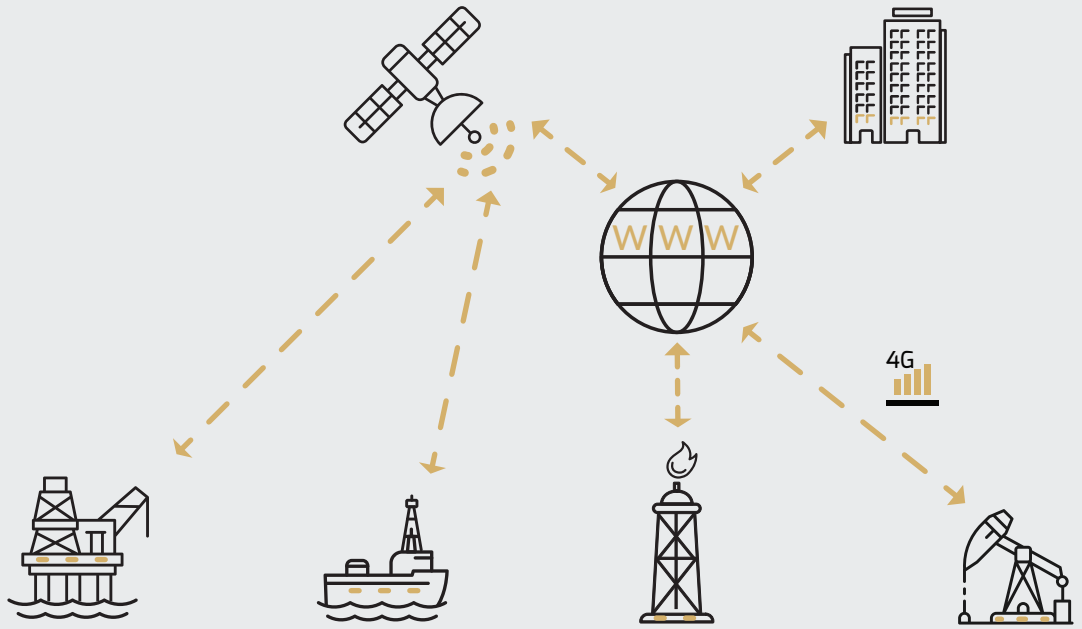
On April 29 2021, hackers gained entry into the networks of Colonial Pipeline Co.[1] According Charles Carmakal, senior vice president at cybersecurity firm Mandiant, the attackers gained access through a virtual private network (VPN) account, which allowed employees to remotely access the company's computer network. The account was no longer in use at the time of the attack but could still be used to access Colonial's network, he said.

Late in 2019, hackers reportedly perpetrated a ransomware attack on Pemex, Mexico's state oil company, forcing it to shut down numerous computers across the country.[2] According to the company, only 5 percent were affected, while fuel production, supply and inventory were not disrupted.[3] Nonetheless, the episode was disruptive and demonstrated the ability of hackers to penetrate the cyber defences of one of the world's largest oil and gas companies.

> IN FACT, ACCORDING TO THE PONEMON INSTITUTE,[4] THE AVERAGE TIME U.S. COMPANIES TOOK TO DETECT AND CONTAIN A DATA BREACH IS WITH AN AVERAGE COST OF $8.2 MILLION

If there is one fundamental problem facing the sector as it transforms to support ever evolving digitisation and the demand greater speeds and access, it is how to bring a wide range of legacy systems and applications, of various vintages, into a common, resilient, high security communications framework. This framework needs to be able to cater for legacy systems communications vagaries and yet also support future security systems communication requirements, ideally using the existing communications infrastructures wherever possible and progressively migrating to new infrastructures that will cater for future security monitoring and control requirements.

iQuila is a proven technology that solves these and many other problems, by encapsulating the full extent of the WAN, within the controllable confides of a Software Defined LAN. iQuila will utilise any existing communications infrastructure (4G, 5G, Satellite) and does not require a costly hardware modernisation programme to be deployed.



Encrypted Layer2 Data Via Any Available Connection Source

Unlike traditional connectivity solutions, iQuila is constructed around the VEN protocol, a proprietary Layer 2 communications medium that utilizes AI and a unique construct to provide the speed, resilience, security, and control of a direct connection, to any device regardless of location.

iQuila is cloud-native, so can be deployed and scaled at pace without requiring a large overhaul and most significantly, no downtime which means that field-based assets, running cutting edge or even legacy applications can be secured without any operational or commercial disruptions.

Please visit www.iquila.com or contact us for more details.

1 Hackers gained entry into the networks of Colonial Pipeline Co. through a virtual private network accounthttps://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

2 Adriana Barrera and Raphael Satter. Hackers demand $5 million from Mexico's Pemex in cyberattack. Reuters. November 12, 2019. https://www.reuters.com/article/usmexico-pemex/hackers-demand-5-million-from-mexicospemex-in-cyberattack-idUSKBN1XN03A

3 Pemex Is Operating Normally. Pemex. November 11, 2019. https://www.pemex.com/en/press_room/press_releases/Paginas/2019-048_national.aspx

4 2019 Cost of a Data Breach Study. Ponemon Institute.

iQUILA

United Kingdom

Unit 5, Excelsior Business Park,
Cardiff, CF14 3AY, UK

Tel: +44 (0)29 20602170
hello@iquila.com
www.iquila.com

United States

2010 El Camino Real #2069
Santa Clara, CA 95050

Tel: + 1 (408) 7094530
hello@iquila.com
www.iquila.com