Hi Jonathan,

Thank you for the post, it was great to see the oil industry highlighted as a prime target for a range of threat actors. This highlights the crucial nature of cyber security for industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems.

To elaborate, Industrial automation processes make use of ICS/SCADA systems to monitor, collect, and analyse real-time data and to operate industrial operations locally or remotely. As interconnectivity among systems continues to grow at tremendous speeds, ICS and SCADA systems have become accessible over the internet and are becoming high–priority targets for hackers. Cyber criminals have already developed malware threats capable of wreaking havoc on industrial operations. Given how an attack might jeopardise the physical safety of communities, workers, or consumers, ICS/SCADA security has now become a greater priority.

Given the neglect in the past, research indicate that 449 vulnerabilities were published in the second half of 2020. During the first half of 2021, around 600 vulnerabilities in industrial control systems were revealed, affecting 76 suppliers.

The majority of identified vulnerabilities posed a substantial danger to industrial control systems, with 71% vulnerabilities rated as high or critical.

Almost three-quarters of vulnerabilities did not need privileges, i.e., allowing them to be exploited by an adversary who without the need of authentication or authorization.

Given these figures and the simplicity with which they may be exploited, it is reasonable to assume that the OT industry demands a strong emphasis on cyber security.

**References**

* Coble, S. (2021). ICS Vulnerabilities Increase 41%. Infosecurity Magazine. Available from: https://www.infosecurity-magazine.com/news/ics-vulnerabilities-increase-41/ [Accessed 20 Mar. 2022].