Cybeta

CASE STUDY

# Manufacturing Sector

**Contact us today** to learn how Cybeta can augment your existing security program.

A major petroleum company was considering transferring some of its terrorism and cyber risk through a specialty insurance program for limits in excess of **hundreds of millions of dollars.** Although the company was confident in the security of both its IT and OT systems and believed they presented low risk, they contacted Cybeta to better understand how **proactive threat intelligence** could further secure their operations and potentially help them land reasonable coverage.

## SOLUTION / ACTION

Within hours, Cybeta retrieved, decrypted, and analyzed archived chat transcripts from the dark web involving members of a global hacking collective that had been sharing a reconnaissance report of the company's network and discussing the ease with which the group could disrupt the company's SCADA systems. Although the chat transcripts were historical in nature and did not appear to be active, it nonetheless revealed the oil company to be a confirmed target to global hacktivists and highlighted their vulnerable industrial operations.

Cybeta discovered exposed telecom and SCADA room diagrams in full detail, as well as account passwords of employees responsible for sensitive SCADA equipment installation. To a determined adversary, such vulnerabilities serve as an intelligence windfall that greatly accelerates attack planning. These gaps were made even more serious when it was discovered that online photos of critical hardware currently deployed in one of the company's SCADA rooms existed, detailing unique identifiers such as make and model information and, in some cases, their serial numbers.

Lastly, open-source intelligence collected from the company's supply chain allowed Cybeta to learn the degree to which suppliers were revealing sensitive information about the company via online performance reviews and other media. These same partners were also found by us to have significant network vulnerabilities including a series of exposed hosts and applications that were introducing serious risk both upstream and downstream in the supply chain.

## BENEFITS / IMPACT

Using Cybeta threat intelligence, the petroleum company immediately took corrective action through employee education and awareness programs focusing on the threats posed to the oil industry and their company. The company instituted additional technical and administrative controls, including on their suppliers. And through Cybeta Overwatch monitoring, enhanced their ability to lower their threat profile moving forward and the opportunity to obtain favorable insurance coverage by demonstrating a proactive and preventative approach to monitoring evolving threats.