USE CASE: NATIONAL OIL COMPANY

Middle East

SITUATION ANALYSIS

The oil and gas industry is a valuable target for malicious actors seeking to exploit industry control system (ICS) environments, a leading industry report warned.[1] Due to the political and economic impact, and direct effect on civilian lives and infrastructure, the oil and gas industry has a high risk for ICS-targeted destruction campaigns originating from a cyber-attack.

Cyber security visibility in oil and gas operational environments remain severely vulnerable, the report continued, allowing intrusion to dwell longer and root cause analysis to remain elusive, long after an incident.[2]

Cyber security attacks are not only targeting the oil and gas industry but telecommunication providers in the greater Middle East, Central Asia and Africa. These attacks are potentially a stepping stone to network-focused man in the middle (MitM) attacks where the hacker secretly relays, and possibly alters, communications between two parties who believe they are directly communicating with each other.

And, as automation continues to evolve and become more important worldwide, the use of ICS/SCADA systems are going to become even more frequent.

INDUSTRIAL CONTROL SYSTEMS (ICS)

ICS are devices, systems networks and controls used to operate and/or automate industrial processes. These devices are often found in nearly any industry from vehicle manufacturing and transportation to the energy and water treatment segment.

SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)

SCADA networks are systems and/or networks that communicate with ICS to provide data to operators for supervisory purposes as well as control capabilities for process management.

THE CUSTOMER

A National Oil company in the Middle East ("customer") wanted visibility of their data as it traversed across the network with minimal, if any blind spots. Network blind spots due to problems, outages and even cyber-criminals using encryption to conceal malware, increase network security risk and are potential regulatory compliance issues. According to a recent survey from Vanson Bourne, roughly two-thirds, or 67 percent, of organizations say that network blinds spots are one of the biggest challenges they face when trying to protect their data.[2,3]

The customer also wanted to transmit and exchange information in real-time via their HQ Data Center and their remote network sites. However, the security and IT teams had no secure key management system to automate easy key rotation nor the ability to define and deploy policies, all resulting in very little control of their security posture. Moreover, monitoring tools were limited and did not work once a policy was deployed.

CHALLENGE

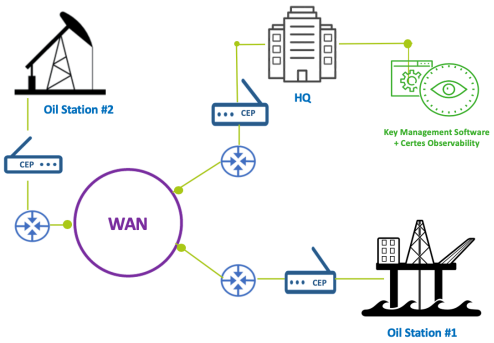
The customer was unwilling to rearchitect their routing around IPSEC tunnels in order to accommodate new encryption solutions to safeguard their data. However, they still wanted a secure key management system that would segment specific data flows, with the ability to control the key generated with each policy in order to prevent unauthorized use and enforce policy access.

Current generation of policies, keys and distribution were manually rotated with each policy and the monitoring of policy data flows was not visible within the customer's current network infrastructure. With limited control of their security posture, the company was extremely vulnerable to potential threats and malicious cyber-attacks.

SOLUTION REQUIREMENTS

The ability to define, segment and deploy policies in order to gain a deeper understanding of every application and user that tries to communicate across the network was crucial in order to thwart potential threats and take full control of their security posture.

All Certes Encryption Point (CEP) appliances needed to be owned, staged and monitored by a multinational telecommunications service provider with read only access, while the customer fully maintained control of the encryption policies, keys, configuration, deployment and analysis of data flows between CEPs. This solution was to be sold as part of a Security Connectivity Managed Service from the telecommunications service provider, a Certes partner of over three years.



THE SOLUTION

With the implementation of the Certes Layer 4 solution, the customer was able to preserve their entire network infrastructure and functionalities. And, by providing access to L2 and L3 headers, as well as the TCP/UDP protocols (Transmission Control Protocol and User Datagram Protocol) the customer was enabled with the monitoring tools they required.

In addition, the Certes CryptoFlow® Net Creator (CFNC) key management platform provided the customer with control of their security posture with the ability to define and generate policies and data flows, as well as segment each policy with different keys, to ensure data is transmitted to only those who need to see it.

OBSERVABILITY

However, with the new Certes Observability feature, it would be simple to provide this valuable add-on tool to assist in strengthening the customer's security posture. This feature is used to analyze and gain deeper understanding of network policy deployment ***and policy enforcement*** to analyze every application that tries to communicate across the network. And, all the while monitoring pathways for potential threats now that each policy is observable in real-time.

RESULT

The Customer was able to secure the communication between the remote sites (Opco) and HQ with the Certes Layer 4 patented technology, preserving all the network functionalities.

In addition, segmentation will be a key factor as each of the sensitive data flows will be contained by unique policies that will use different keys and automatic key rotation for further security.

And, with the Certes Layer 4 solution, the customer could continue to use any of the Layer 3 technologies that were already deployed at some of their remote sites.

REFERENCES

1. Dragos Oil and Gas Threat Perspective Summary, Assessing the Threats, Risks, and Activity Groups Affecting the Global Oil and Gas Industry, August 2018.
2. Industrial control system cyber security risk high, report warns, ComputerWeekly.com, August 1, 2019
3. Hide and Seek – Cybersecurity & the Cloud, Vanson Bourne, Aug 2017

CERTES NETWORKS

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1(888)833-1142
Fax: 1(412)262-2574

info@certesnetworks.com
sales@certesnetorks.com

We offer an encryption solution that is simple, scalable and uncomplicated.