CN one pager solution - TSA SD02D – July 27th 2023

THE CHALLENGE

- May 7 2021 – US 'Colonial Pipeline' hit with Ransomware attack causing fuel availability panic across the US Eastern Seaboard. This wakeup call to the impact of an attack on national infrastructure led to CISA and the TSA collecting 25 major pipeline and industrial control systems partners to formulate Security Directives to prevent this from happening again.
- One aspect the TSA identified was to ensure CEO's and board of directors embrace cyber risk as a matter of good governance , a strategic imperative and a business enabler.
- "Cyber-attacks are a reality for the foreseeable future" – CISA Director Jen Easterly
- TSA SD02D Mandate – Applies to all owner/operators of TSA designated hazardous liquid and natural gas pipelines or liquified natural gas facilities. This includes Airport and aircraft operators as well as passenger and freight railroad carriers
- IPSec tunnels could be an option but can be complex, have a performance impact on low bandwidth links, have scalability limits and can only be configured/managed by the IT network team.
- IPSec tunnels blind all monitoring and analytics systems, do not prevent data exfiltration and are not granular in nature.

THE SOLUTION

- Certes Crypto-segmentation ensures true separation of data flows across any IP network. This ensures that IT activities and traffic cannot see or interrupt any OT traffic running over the same network and vice versa.
- The ability to control data sovereignty for individual application flows means only the intended recipient can access the data. This prevents any lateral movement incidents in the same physical network.
- Highly granular data encryption of traffic in transit controlled by policy and 100% under the control of the customer and not the network vendor for True Zero Trust.
- Anti-exfiltration and Data sovereignty measures protect data should the network be breached no matter where it goes ensuring it can only be read by the intended recipient

Mandated requirements under TSA SD02D

Section III-B
- Network Segmentation between IT/OT systems
- Logical zones of the network based on criticality, consequence and operational needs
- Prevent unauthorised comms between zones unless contents is encrypted
- Encryption of Data whilst in transit

Section III-D
- Ensure industrial control systems can be isolated from an IT systems cybersecurity incident
- Ensure Safety and reliability of OT Systems

Section III-E
- Control and secure patch management on Critical Cyber Systems

Contact Certes Networks

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

www.certesnetworks.com

CERTES NETWORKS

Tel: 1 (888) 833-1142
Fax: 1 (412) 262-2574
sales@certesnetworks.com
info@certesnetworks.com