CYBERSECURITY A BUSINESS IMPERATIVE:

Certes and the TSA SD02D Mandate

The recent ransomware attack on the Colonial Pipeline sent shockwaves across the United States, serving as a stark reminder of our national infrastructure's vulnerability to cyber threats. The fallout of this attack resulted in widespread panic and fuel shortages along the US Eastern Seaboard.

In response to this crisis and to prevent it from happening again, the Cybersecurity and Infrastructure Security Agency (CISA) and the Transportation Security Administration (TSA) gathered 25 major pipeline and industrial control systems partners to formulate the Security Directives, known as TSA SD02D. Established with one goal in mind – to safeguard the critical infrastructure from future cyber threats.

A key aspect of these directives is the need for CEOs and the C-Suite to view cyber risk as a matter of good governance, a strategic necessity, and a driver for business growth.

> **Cyber-attacks are a reality for the foreseeable future.**
>
> *Jen Easterly – CISA Director*

The TSA SD02D Mandate casts a wide net, encompassing owner/operators of TSA-designated hazardous liquid and natural gas pipelines, liquified natural gas facilities, and even airport and aircraft operators, passenger and freight railroad carriers. While the mandate is extensive, the solution need not be complex.

What the TSA Mandate means to you

The TSA has introduced sensible changes, such as testing cybersecurity policies in real-world scenarios to ensure their effectiveness. This Directive underscores the TSA's commitment to safeguarding our critical oil and gas pipelines from cyber threats. If you are responsible for one of these pipelines, it's advisable to compare your current practices with the new rules in the Directive and seek assistance if needed.

Certes DPRM delivers Crypto-Segmentation: The Shield for Critical Infrastructure and Data Protection Risk Management

Now, considering the landscape of cybersecurity, it's worth acknowledging that while IPSec tunnels could be an option, they can be complex, have a performance impact on low bandwidth links, and have scalability limits. Furthermore, these tunnels can only be configured and managed by the IT network team.

It's also crucial to note that IPSec tunnels can blind all monitoring and analytics systems, do not effectively prevent data exfiltration, and lack granularity in their approach. This is where Certes Crypto-Segmentation comes into play as an advanced and robust solution

With Certes Crypto-Segmentation, there's guaranteed true separation of individual data flows across any IP network. This robust technology ensures that IT activities and traffic cannot see or interrupt any Operational Technology (OT) traffic running over the same network, and vice versa. This separation is fundamental in preventing the cross-contamination of these two domains.

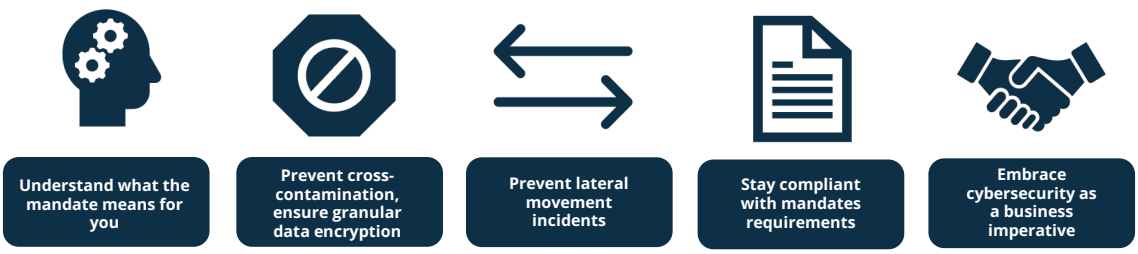
It allows for highly granular data protection of traffic in transit, and this protection is controlled by policy and is 100% under the control of the customer, not the network vendor. This level of control ensures a state of 'True Zero Trust,' which is vital for comprehensive security and effective data protection risk management.

For more on what True Zero Trust really means, watch a short clip from the Certes team here: [What is True Zero Trust? | Certes Network]

Certes DPRM Preventing Lateral Movement Incidents and Protecting Data Sovereignty

One of the most significant features of Certes DPRM is the ability to control data sovereignty for individual application flows, ensuring that only the intended recipient can access the data. By focusing on applying security to the data itself we can be certain that the data is the sovereign item and not the physical network – wherever the data goes it remains sovereign. This security measure prevents any lateral movement incidents within the same physical network by making it impossible for one flow to be able to identify any other flow even when on the same physical network segment. In case of a network breach, anti-exfiltration and data sovereignty measures in Certes DPRM have already protected the data, any extracted data is unreadable and valueless to the attacker, Certes DPRM makes sure the data can only be read by the intended recipient.

The Certes DPRM & TSA Mandate



Mandated Requirements under TSA SD02D: Certes Delivers

The mandate outlines critical requirements to secure infrastructure, including robust data protection risk management:

- **Network Segmentation:** Certes DPRM Crypto-Segmentation provides robust network segmentation between IT and OT systems, a crucial element to prevent unauthorised communication between zones, unless contents are encrypted.
- **Logical Zones:** Certes DPRM through customer defined policy supports the establishment of logical zones based on criticality, consequence, and operational needs, aligning perfectly with the mandate's vision.
- **Data Encryption in Transit:** Certes DPRM ensure the protection of data while in transit, a key requirement for safeguarding critical essential systems and effective data protection risk management.
- **Isolation of Industrial Control Systems:** The ability to isolate industrial control systems from IT systems during a cybersecurity incident is paramount for safety and reliability, a task Certes DPRM fulfils seamlessly.
- **Patch Management:** Certes assists in controlling and securing patch management on critical cyber systems, ensuring that vulnerabilities are promptly addressed without compromising security. Certes DPRM policies can be defined to control who can perform a patch / upgrade preventing malicious insertion of code by bad actors.

Conclusion

Embracing cybersecurity as a fundamental business requirement is no longer a choice but an imperative. Cutting-edge DPRM Crypto-Segmentation technology stands at the forefront of safeguarding essential systems, surpassing regulatory mandates. The overarching mission is to empower organisations to securely navigate our interconnected world.

It's time to prioritise data protection risk management, regardless of its journey, through the data centric functions of Certes DPRM. Utilising solutions like DPRM can help segregate IT and OT networks on the same physical infrastructure, ensuring that sensitive information remains accessible only to authorised personnel and protecting critical national infrastructure.