illumio

SOLUTION BRIEF

Meeting TSA Security Directive Pipeline 2021-02C Requirements

Globally we are seeing the major impact of challenges in energy supply. Increasing prices are creating energy poverty, even in G7 countries. Energy is becoming a weapon in global physical and cyber conflicts. Increasingly, the energy sector is becoming a target for threat actors, criminal groups, terrorists, and other nations.

Energy must be transported via a physical medium, and that network needs to be managed and monitored. This requires a combination of Information Technology (IT) and Operational Technology (OT). The attack surface for this hybrid model is substantial and the potential for an attack to cross the boundaries is very real. Traditionally, the two worlds were separate, but now they are becoming more integrated.

To address the cybersecurity of pipelines, the U.S. Transportation Security Administration has issued a directive to reduce the impact of malicious cyber intrusions. The directive addresses multiple areas of cybersecurity, and in this document, we will show how Illumio with its partners addresses the highest-profile issues.

Key measures to be implemented

1. Implement network segmentation policies and controls designed to prevent operation disruption to the Operation Technology system if the Information Technology system is compromised or vice versa.
2. If the operator cannot apply patches, the strategy must include a description of additional mitigations.
3. Operators must have a current Cybersecurity Incident Response Plan that must include measures to:
    - Segregate infected network or devices
4. Until the operator's plan is approved, the following requirements must be applied:
    - Identify IT & OT interdependencies
    - Implement network segmentation

Section III - Cybersecurity Measures		
	Directive	**Illumio Solution**
A	Identify the owner's critical cyber systems as defined in section VII of the directive	Illumio with their asset management partners can gather detailed data on all IT and OT devices connected to the network either physically or in the cloud.
B	Implement network segmentation policies and controls designed to prevent operation disruption to the Operation Technology system if the Information Technology system is compromised or vice versa.	Illumio can build very granular controls to implement a least-privilege approach to segmentation. This means that only verified systems can communicate using only allowed protocols. This prevents the propagation of malware between systems.
B.1	Included should be a list and description of: a. IT & OT interdependencies b. External connections to the OT system c. Zone boundaries including IT & OT logical zones	Illumio can build a map of all the interdependencies between IT & OT devices, including connections to external environments and the cloud. A search function means that any connection can be isolated and firewall mis-configurations can be found.
B.2	Identification and description of measures for securing and defending zone boundaries	Zones can be created and enforced by applying rules to block all unauthorized connections. The zones can be created by using simple labels based on a variety of parameters.
E.3	If the operator cannot apply patches on specific OT systems, the strategy must include a description of mitigations	Illumio can use data from our vulnerability scanning partners to populate the map with information that shows the exposure of any system. This data can be used to apply rules to mitigate any patching issues.
F.1	The operator must have an up-to-date incident response plan to ensure the following objectives. a. Prompt containment of infected server or device b. Segregation of infected network or devices	Illumio can simply apply a stringent lock down of key resources in the event of an incident. This can either lockdown an infected network or apply enterprise-wide controls to protect resources. Working with our SOAR partners, these processes can be automated.

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.