SECURE NETWORK MONITORING SOLUTIONS

Cybersecurity for Critical Infrastructures

ST Engineering

Contents

Every day, we turn on the taps, expecting clean water. We get ourselves to the train stations, expecting regular train services. When we reach our offices, we turn on our workstations, expecting our networks to be connected without disruptions.

These unassuming activities are often taken for granted, and most people would not give them a second thought. The ground reality is that any disruption of these services can cause massive disruptions to our everyday routines, affecting thousands or even millions of lives. With more cities and corporations adopting “smart” initiatives, the growing risks of cyber attacks has become even more evident.

Cyber Threats Are Escalating!

Cyber warfare is gradually becoming the strategy used by cyber criminals and hostile states. Remember Stuxnet? Or when the Ukraine power grid was attacked multiple times? Even the most recent event, such as the Colonial Pipeline ransomware attack in the United States, shows us how critical, yet delicate our critical infrastructures are.

Targeting public utility infrastructures (energy plant, oil & gas facility, metro system, etc.) has become attractive to cyber attackers due to the large scale of destruction when these infrastructures are brought down. Furthermore, these attacks can be performed without stepping out of one's house and it is generally very difficult for authorities to trace their source. Simply put, the world is not yet competent to defend or react proficiently against cyber attacks.

The Fourth Industrial Revolution (Industry 4.0) and Smart City initiatives are driving the convergence and integration of computer networks, to move massive amount of operational data. Traditionally, however, most of the critical public utility infrastructures are built and operated as physically isolated networks.

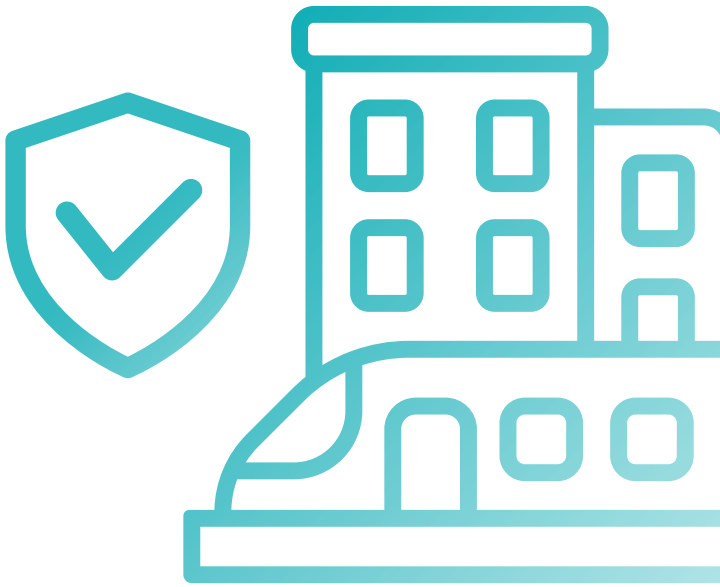
As a result, moving data in and out of these isolated networks is cumbersome. While directly connecting these isolated networks seemed the most convenient, it would also mean the removal of any security that isolation provides, exposing them directly to the cyber threats that come with the internet.

On the other hand, using removable media devices, such as USB flash drives, would bring about their inherent set of risks and perils, such as embedded malwares, advanced persistent threats in firmware, loss of data and more. Inevitably, cyber risks are increasing, and thus, we are witnessing increasing cyber attacks (massive data leakages, power supply stoppage, disrupted logistical supply chains, etc.) in the recent years.

Unifying Convenience and Cybersecurity

for Critical Infrastructures

ST Engineering Data Diode is designed specifically for data transfer while maintaining the air-gap between the separated networks, i.e. allowing whitelisted network connections to transfer data across the air-gap networks. Any data leakage (or back flow of data) is prevented due to its hardware enforced unidirectional data transfer. ST Engineering Data Diode is both CC EAL 4+ and NITES certified by Cyber Security Agency of Singapore.



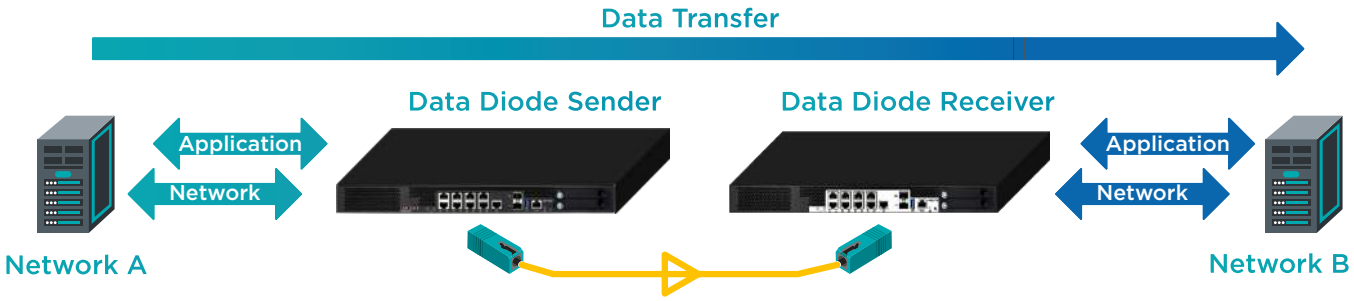


Figure 1 - ST Engineering Data Diode

ST Engineering Data Diode is designed specifically for data transfer while maintaining the air-gap between the separated networks.

Deployment of data diodes in critical infrastructure networks is becoming an essential cybersecurity instrumentation. By securely connecting the OT networks to the enterprise IT networks with a data diode, operational status of individual utility plants can continually be sent securely, and monitored centrally at the Corporate HQ, while the individual plant operation remains isolated from cyber threats.

However, system integration challenges remain in OT systems where outdated/unpatched Windows OS, legacy SCADA/ICS applications and different databases, etc. are used. To meet the desired outcomes of Fourth Industrial Revolution, the operational data need to be standardized and aggregated before data analytic engines can ingest them for operational insights.

Therefore, we highly recommend that OT operators make use of modern operational data aggregators such as Open Platform Communications Unified Architecture (OPC UA) to harmonize the data across the myriad of sub-systems, and ease the works of system integration.

ST Engineering Data Diode has modules within that replicate OPC UA data across the Plant and HQ networks seamlessly and reliably. ST Engineering Data Diode can also be integrated with IT/OT network monitoring tools such as Industrial Threat Detection system.

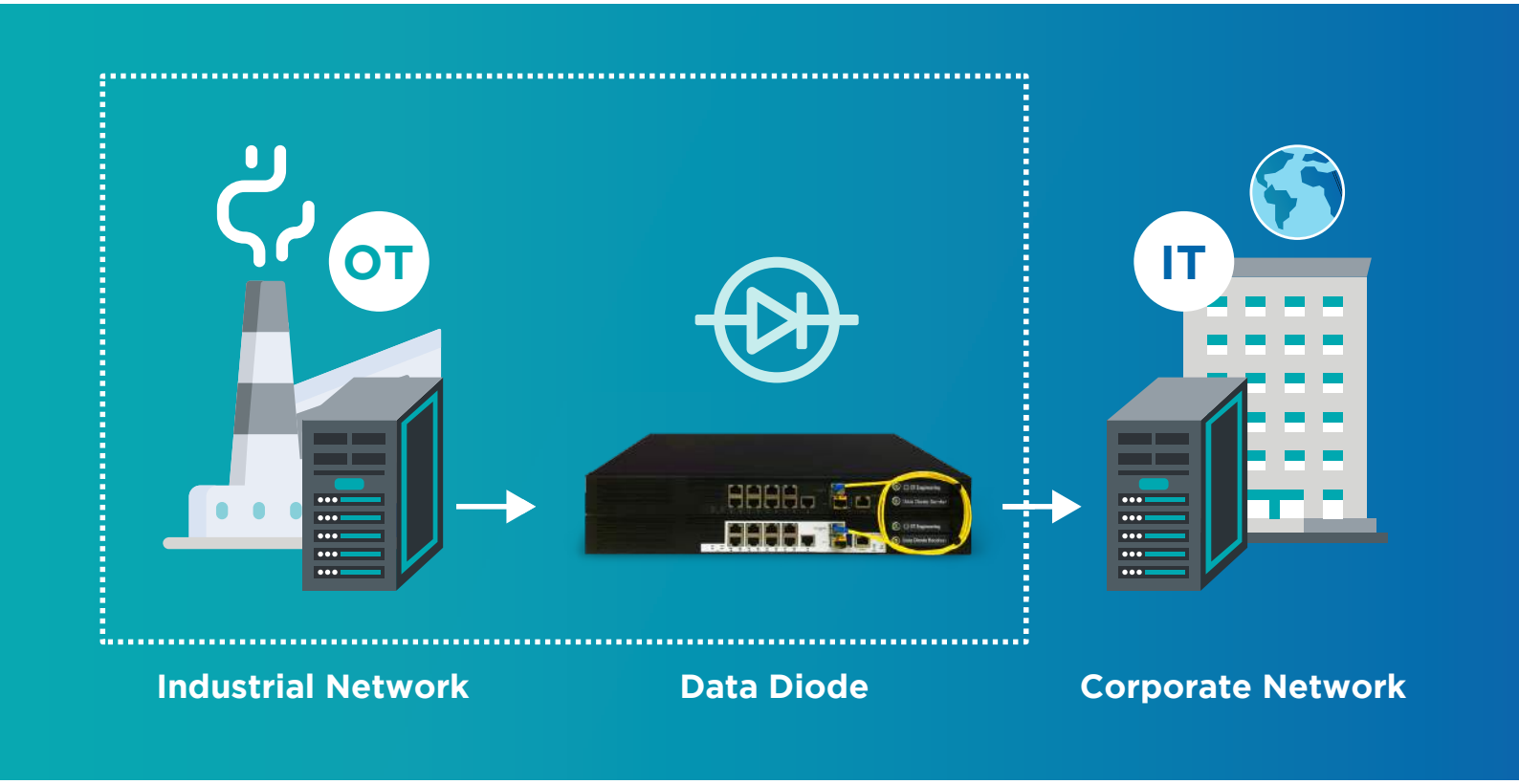


Figure 2 - Securing Critical Information Infrastructure

MITRE ATT&CK

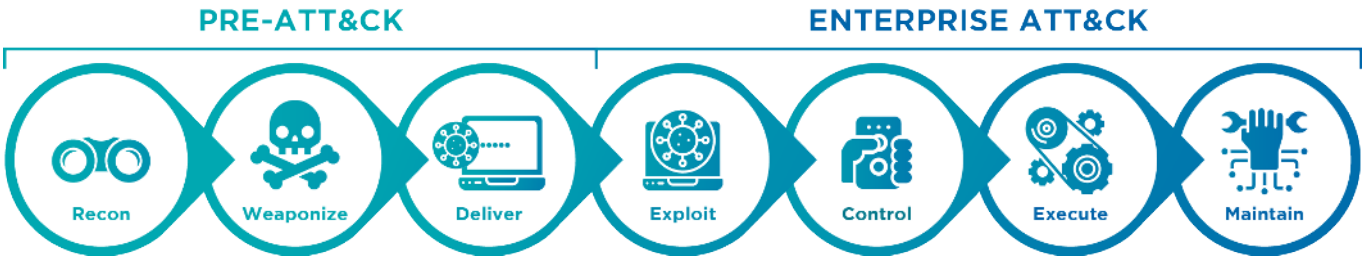


Figure 3 - MITRE ATT&CK Framework

We can follow a hacker tactical activities using the MITRE ATT&CK[1] framework (Figure 3), and analyse how the Secure Files Transfer Gateway can defeat the cyberattacks (Figure 4).

S/No	MITRE ATT&CK	Tactical Activities	Mitigation by Data Diode & Content Checker Module
1	**Recon**	Researching and gathering information about the target bank, e.g. IP addresses, domain names, email addresses, system vulnerabilities, etc.	Data Diode breaks both network (IP, Ports, SSL, etc) and application (SMB, SFTP, etc) layers communication protocols. Hence, hackers can only scan those internet-facing ports and services.
2	**Weaponize & Deliver**	Infiltrating further into the network by acquiring access privileges and upgrading access to penetrate back-office and operational networks	Only whitelisted end-points, and file types can be transferred across the Secure File Transfer Gateway. Any malicious content will be removed by the FCS or CXC.
3	**Exploit & Control**	Infiltrating the network (lateral movement), establishing C&C links back to Mothership, and injecting malware into critical systems.	In the event that the Intranet or Classified Network has been compromised, the hacker will not be able to establish C2 linkages back to the "*mothership*" through Data Diode.
4	**Execute & Maintain**	Exfiltration of data, or detonate ransomware.	Without any access or control, hackers would not be able to execute their objectives, such as detonating ransomware. The CXC conducts deep inspection on all outbound traffic so as prevent any leakage of data.

Figure 4 - Defeating the Cyber Attacks

[1] *https://attack.mitre.org/*

ST Engineering Cybersecurity Solutions

As more cities and corporations around the world continue to leverage on improving technologies to better operate and manage services, the amount of data generated will only continue to increase. ST Engineering Data Diode not only allows real time movement of data, it does so while eliminating cyber threats and maintaining the segregation between these networks. ST Engineering Data Diode complements the suite of cybersecurity solutions offered by ST Engineering.

ST Engineering's cybersecurity arm is a pioneering and leading provider of cybersecurity solutions with almost two decades of comprehensive future-ready cybersecurity solutions, forming trust with their customers in national, government, critical information infrastructures, and commercial enterprises. Backed by indigenous capabilities and deep domain expertise in cybersecurity, we offer robust cyber-secure products and services in cryptography, cybersecurity engineering, cross domain solutions, SCADA protection, audit and compliance.

Our team of cybersecurity expertise have designed, built, operated and maintained up to 18 cybersecurity operations centres globally. We also provide cybersecurity professional and managed security services to empower organisations with cyber resilience and increase operational efficiency. To-date, our cybersecurity academy have certified and trained cybersecurity professionals in more than 150 organisations.

References

The MITRE Corporation (2015-2020).
ATT&CK Matrix for Enterprise.
Retrieved from MITRE Web Site:
https://attack.mitre.org

100 Jurong East Street 21
Singapore 609602

(65) 6914 5959

cybersecurity@stengg.com

ST Engineering Info-Security Pte. Ltd.
www.stengg.com/cybersecurity
cybersecurity@stengg.com

V0620