txOne networks | Keep the Operation Running

Achieving Compliance with Saudi NCA Regulations (OTCC-1:2022)

A Guide to Saudi Arabia's New OT Cybersecurity Controls:

Protecting Critical Infrastructure from Cyber Threats

February 2024 **TXOne Networks**

Table of Contents

1. INTRODUCTION 03
   1.1. Overview of OTCC in Saudi Arabia 03
   1.2. Overview of TXOne Solutions 03
2. OTCC-1:2022 MAIN DOMAINS AND SUBDOMAINS 04
   2.1. Objectives 04
   2.2 OTCC Main Domains and Subdomains 05
   2.3 OTCC Structure 06
3. TXONE NETWORKS SOLUTIONS 07
4. MAPPING TXONE NETWORKS SOLUTIONS TO OTCC 09

1. Introduction

This document aims to provide valuable insights into how TXOne Networks solutions can assist customers in achieving compliance with the OTCC-1-2022 regulations in Saudi Arabia. This document will explore the key features, benefits, and capabilities of TXOne solutions that enable organizations to enhance their cybersecurity posture and meet regulatory requirements effectively.

1.1. Overview of OTCC in Saudi Arabia

In 2022, the Saudi National Cybersecurity Authority (NCA) conducted a comprehensive study of multiple national and international cybersecurity frameworks and standards, leveraging OT/ICS guidance, standards and controls to create regulations designed to protect critical infrastructure and ensure the resilience of organizations operating within Saudi Arabia. These regulations were released as the Operational Technology Cybersecurity Controls (OTCC), a framework that would enhance the security of Operational Technology (OT).

The OTCC framework includes a range of controls and guidelines that organizations must comply with in order to mitigate cyber threats and vulnerabilities in their OT environments. These controls are specifically designed for Industrial Control Systems (ICS) situated in facilities deemed critical, whether owned and/or operated by government entities (such as ministries, authorities, establishments, etc.) or private sector organizations responsible for Critical National Infrastructures (CNIs), be they domestic or international. Therefore, compliance with OTCC regulations is essential for organizations operating within critical infrastructure sectors, as it not only fortifies defenses against cyber threats but also ensures alignment with national cybersecurity initiatives.

1.2. Overview of TXOne Solutions

TXOne Networks offers cybersecurity solutions that ensure the reliability and safety of ICS and OT environments through adherence to the OT zero trust methodology. At TXOne, we work together with both leading manufacturers and critical infrastructure operators to develop practical, operations-friendly approaches to cyber defense.

The OT zero trust-based technologies we've developed go beyond the limits of traditional cyber defense to streamline management, reduce security overhead, and quickly resolve challenges. We offer both network- and endpoint-based solutions that integrate with the layered arrangements and varied assets common to work sites, providing real-time, defense-in-depth cybersecurity to both mission-critical devices and the OT network as a whole.

2. OTCC-1:2022 Main Domains and Subdomains

The Operational Technology Cybersecurity Controls (OTCC) document contains the following:

- 4 Main Domains
- 23 Subdomains
- 47 Main Controls
- 122 Subcontrols

2.1. Objectives

These controls were developed as an extension to the Essential Cybersecurity Controls (ECC) in order to achieve higher levels of national cybersecurity goals by focusing on Industrial Control Systems (ICS) and defining its cybersecurity requirements. This enables national organizations to fulfill mandated cybersecurity requirements to increase the protection of its critical infrastructure and its readiness level regarding cybersecurity risks.

The OTCC document addresses the four main cybersecurity pillars below

- Strategy
- People
- Process
- Technology

2.2. OTCC Main Domains and Subdomains

The table below shows OTCC Main Domains and Subdomains

1. Cybersecurity Governance	1-1	Cybersecurity Policies and Procedures	1-2	Cybersecurity Roles and Responsibilities
	1-3	Cybersecurity Risk Management	1-4	Cybersecurity in Industrial Control System Project Management
	1-5	Cybersecurity in Change Management	1-6	Periodical Cybersecurity Review and Audit
	1-7	Cybersecurity in Human Resources	1-8	Cybersecurity Awareness and Training Program
2. Cybersecurity Defense	2-1	Asset Management	2-2	Identity and Access Management
	2-3	System and Processing Facility Protection	2-4	Network Security Management
	2-5	Mobile Device Security	2-6	Data and Information Protection
	2-7	Cryptography	2-8	Backup and Recovery Management
	2-9	Vulnerability Management	2-10	Penetration Testing
	2-11	Cybersecurity Event Logs and Monitoring Management	2-12	Cybersecurity Incident and Threat Management
	2-13	Physical Security		
3. Cybersecurity Resilience	3-1	Cyber Resilience Aspects of Business Continuity Management (BCM)		
4. Third-Party Cybersecurity	4-1	Third-Party Cybersecurity		

Figure 1: Exploring OTCC - Detailed Overview of Main Domains and Subdomains

2.3. OTCC Structure

The NCA has introduced a pioneering supplemental resource—the Operational Technology Cybersecurity Controls (OTCC) Methodology and Mapping Table. This addition to the existing OTCC document presents a strategic approach to fortifying the defenses of critical infrastructure.

At the heart of this methodology lies a set of design principles that elucidate both the structure and the philosophy underpinning the OTCC. These principles guide the development of main domains and subdomains, ensuring a comprehensive and robust cybersecurity posture.

The methodology extends to the granular level, defining controls and subcontrols. This meticulous process categorizes various cybersecurity measures into actionable and auditable levels. Such detail ensures that each control is not merely a theoretical concept but a practical step towards cybersecurity.

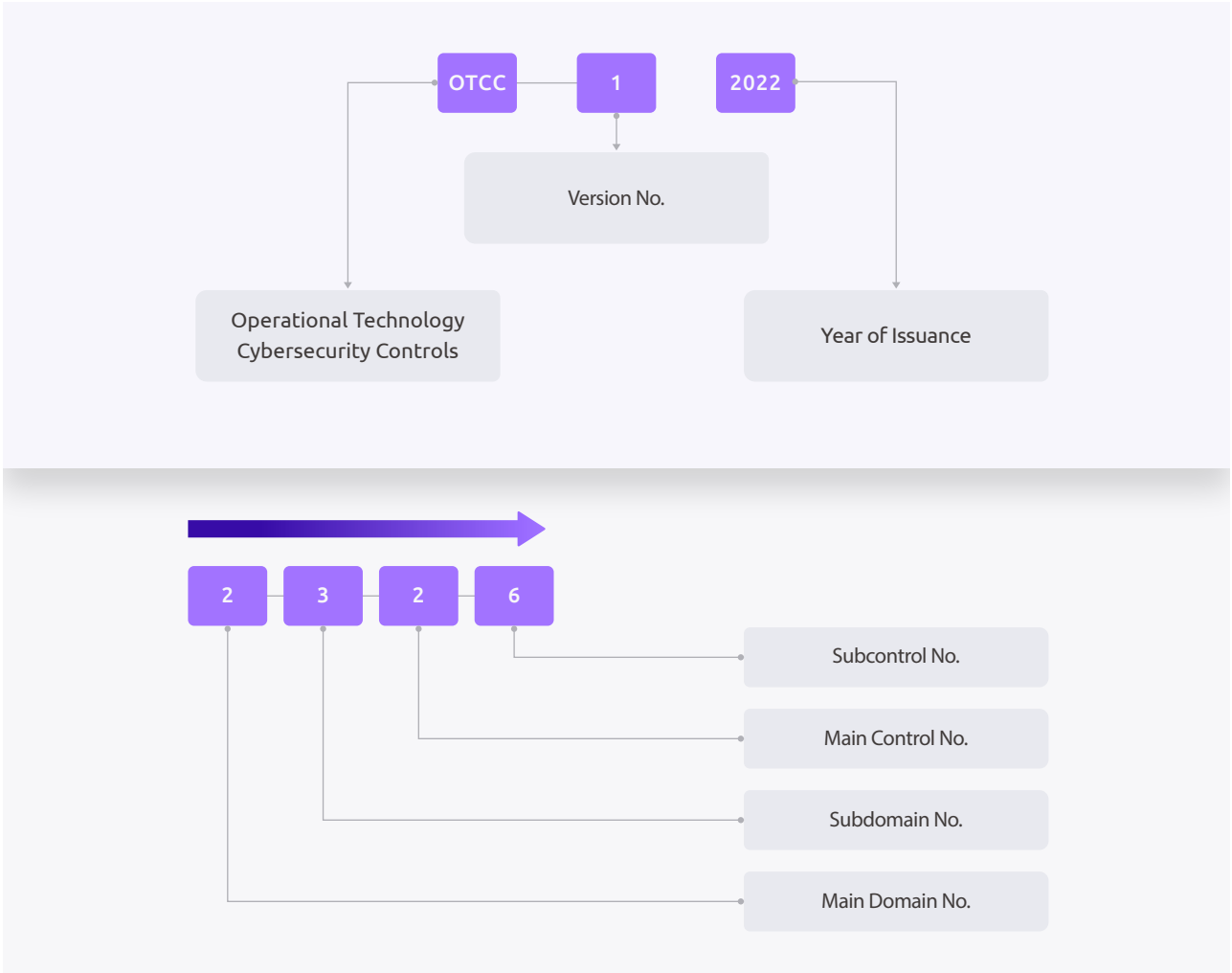


Figure 2: Understanding Control Codes in OTCC

3. TXOne Networks Solutions

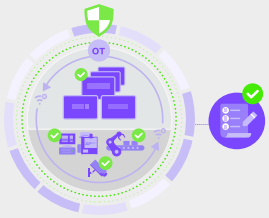
The following are the technology solutions offered by TXOne Networks that can be included in the compliance matrix provided to customers to boost compliance as measured against the OTCC controls:

- TXOne Stellar (Endpoint Protection)
- TXOne EdgeIPS (OT Intrusion Prevention System)
- TXOne EdgeFire (OT Firewall)
- TXOne EdgeOne (Centralized Management)
- TXOne Portable Inspector (Portable Anti-malware Scanning and Secure File Transfer)
- ElementOne (Centralized Management)

By implementing these technology solutions in their OT environment, organizations can enhance their compliance measurement against the OTCC controls and better secure their OT infrastructure.
TXOne Stellar provides a pure software endpoint protection solution rooted in industrial control systems. We break down the barriers between old and new equipment, using operational field normative baselines as references. Without disrupting operations, we proactively block unauthorized system changes and malicious activities.

Bringing Operational Focus to OT Security

Stellar circumvents the risk of unauthorized changes by focusing on comprehension of the operation and its devices and contextualizing them with security outcomes.



Uniquely Built for OT

Stellar protects assets without interfering with the operation. It mitigates environmental barriers to maintain cyber hygiene in OT.

OT Security Without Compromise

The different objectives and priorities between security and operations teams cause friction and frustration. Stellar removes the need for compromise by meeting the needs of each team concurrently.

Figure 3: TXOne's All-Terrain Endpoint Protection

TXOne Edge product line brings enhanced stability and resilience to industrial control network environments. Adhering to a zero-trust principle centered on packet detection, all data exchanges and command transmissions between devices are subject to precise management control. The mining technology developed for industrial control communication protocols plays a vital role in disaster prevention, detection, and repair, contributing to improved overall operational stability.

EdgeFire is the ideal firewall designed purely for OT with VPN support.

EdgeIPS features a series of IPS appliances to suit OT environments of any size.

EdgeOne functions as the information and control center for your OT network security and Edge appliances.

Figure 4: Strengthening OT Network Defense and Protecting Critical Assets with TXOne Edge

TXOne Element product line offers foolproof cybersecurity detection for assets entering and exiting the factory area, as well as for portable storage media. The product's design logic closely aligns with existing operational processes, making it easy for general staff to adopt and effortlessly achieve cybersecurity maintenance and inventory tasks.

Portable Inspector scans critical assets to keep them malware-free.

Safe Port sanitizes portable storage media to maintain cyber hygiene.

ElementOne consolidates scan results to establish a security inventory overview.

Figure 5: Enhancing Asset Integrity and Supply Chain Security Through TXOne Element

4. Mapping TXOne Networks Security Solutions to the OTCC

TXOne's solutions offer valuable assistance to customers in addressing a wide range of controls and subcontrols outlined in the OTCC guidelines. This includes Cyber Defense and various subdomains such as Asset Management, Identity and Access Management, System and Processing Facilities Protection, Network Security Management, and Cybersecurity Event Logs and Monitoring Management.

Control No.	Subcontrol No.	Control Description	TXOne Assistance
Cybersecurity Risk Management			
1-3	**1-3-1-2**	Cybersecurity risk assessment for OT/ICS assets must be conducted periodically and must be sure to include risks associated with signing contracts and agreements with OT/ICS related third-party organizations and/or upon changes in related regulatory requirements as part of the assessment.	**TXOne Portable Inspector** can be used in the risk assessment process. It performs vulnerability assessments on various operating systems, identifying and reporting the criticality of each vulnerability found. In addition, the Portable Inspector (PI) collects asset information to generate an inventory list that grants IT/OT visibility and eliminates shadow IT/OT. Along with providing effective malware scanning and removal for standalone computers and air-gapped systems, PI also automatically collects detailed snapshots of asset data which includes computer information, Windows Update status and application lists, completely unprompted. PI supports legacy systems starting from Windows 2000 SP3, modern systems, and embedded systems as well as Linux. Portable Inspector is easy to implement and helps customers quickly adopt a cybersecurity solution that can keep the operation running.
Asset Management			
2-1-1	**2-1-1-2**	Automated solutions to collect asset inventory information must be utilized.	**TXOne Portable Inspector**: Collects details of asset data, including device information, Windows Update status, and application lists. **EdgeFire**: Enables high asset visibility through passive asset identification and IT/OT traffic communication within OT networks. **Stellar**: Provides an ICS application inventory that is supplied by OT vendors. Supports both legacy and modern systems.

System and Processing Facilities Protection			
2-3-1	**2-3-1-1**	Advanced, up-to-date mechanisms and techniques must be securely managed and utilized to protect systems from malware, Advanced Persistent Threats (APT), malicious files, and activities.	**Stellar** is a next generation antivirus solution specifically created for OT (Operational Technology) environments. It offers a range of cutting-edge features, such as application lockdown. This feature ensures that only authorized operations and executions can take place, effectively preventing any unauthorized activities within the system. Stellar provides enhanced security and protection for industrial settings, safeguarding critical infrastructure from potential threats.
	2-3-1-6	Application whitelisting techniques or other similar techniques must be deployed to limit the applications that are allowed to run in OT/ICS environments.	**Stellar** is specifically designed to address the challenge of unauthorized application execution in OT/ICS (Operational Technology/Industrial Control Systems) environments. Its primary objective is to ensure that only approved applications are allowed to run within the system. Stellar limits the number of executable applications to those present on the approved list. This proactive approach enhances security and reduces the risk of unauthorized software compromising the integrity and stability of the OT/ICS environment.
	2-3-1-7	OT/ICS assets must be managed through dedicated, segmented and hardened Engineering Workstations (EWS) and Human-Machine Interfaces (HMI) for management purposes and maintenance.	**EdgeFire/EdgeIPS** is a comprehensive solution that specializes in OT-aware segmentation, offering enhanced support for secure access control to OT/ICS asset information systems. With EdgeFire/EdgeIPS, organizations can enforce strict measures to restrict access to authorized entities such as EWS (Engineering Workstations) and HMI (Human-Machine Interface) devices. By implementing this level of segmentation, EdgeIPS ensures that only trusted and designated sources can interact with the OT/ICS asset information systems, limiting the risk of unauthorized access or potential vulnerabilities.

2-3-1	**2-3-1-8**	External storage media is scanned and analyzed against malware and APT. The scan must be executed in an isolated and secure environment.	**Portable Inspector** is a solution designed to provide secure storage for data transfer, ensuring protection against any potential malware infections. By utilizing Portable Inspector, organizations can confidently transfer data without the risk of malware infection. **TXOne Stellar** complements this solution by offering support for malware scanning of network drives and removable media. This integrated approach ensures that all data accessed or transferred through network drives and removable media is meticulously scanned for malware, enhancing overall security, and mitigating the risk of infection. With Portable Inspector and TXOne Stellar, organizations can maintain a robust defense against malware threats throughout their data transfer processes. **TXOne Safe Port** assists in sanitizing external storage media within a protected and secure setting. SafePort is capable of inspecting external media, identifying and removing malware, rendering it suitable for use in OT environments.
	2-3-1-9	Usage of external storage media in the production environment must be restricted unless secure mechanisms for data transfer are developed and properly implemented.	**Portable Inspector Pro** is a solution specifically designed to provide a secure storage facility for carrying sensitive data. With Portable Inspector Pro, users can confidently store their sensitive information, ensuring its privacy and protection. This solution offers robust security features to safeguard the stored data from unauthorized access or potential breaches. The Portable Inspector is equipped with AES-256 hardware encryption, allowing owners and operators to carry sensitive data in air-gapped environments while ensuring the operational integrity of the business. Files are scanned when transferred into secure storage, and only clean files can be stored. **TXOne Stellar's** USB Vector Control feature can block the use of external storage media. It can also be used to allow a few selected external storage devices based on device identification like Vendor ID, Product ID or Serial Number. **TXOne Safe Port** assists in sanitizing external storage media within a protected and secure setting. SafePort is capable of inspecting external media, identifying and removing malware, rendering it suitable for use in OT environments.

2-3-1	**2-3-1-10**	Systems' logs and critical files must be protected from unauthorized access, tampering, illegitimate modification and/or deletion.	**Stellar** implements a write protection feature to ensure the security of critical data, configurations, and files by preventing unauthorized overwriting. With Stellar's write protection functionality, organizations can effectively safeguard their valuable information from accidental or intentional modifications that could compromise the integrity or confidentiality of the data. This proactive measure adds an extra layer of protection, ensuring that only authorized individuals or processes have the necessary permissions to make changes.
	2-3-1-11	Unauthorized applications, scripts, tasks, and changes must be detected and analyzed.	**Stellar** is an effective endpoint protection solution designed to prevent the unauthorized execution of applications that are not included in the approved list. By implementing strict controls, Stellar ensures that only authorized applications are allowed to run within the system. This proactive approach significantly reduces the risk of unauthorized software compromising the security and stability of the environment.
	2-3-1-12	New communications sessions and commands must be executed and analyzed.	**Stellar** uses Operations Behavior Anomaly Detection, which enables the identification of any abnormal behavior within system operations. By leveraging advanced algorithms and analytics, Stellar effectively detects deviations from expected patterns or behaviors in real-time. Stellar's Operations Behavior Anomaly Detection enhances the overall security posture by providing early detection and timely alerts, allowing for prompt investigation and mitigation of any suspicious activities within system operations.
	2-3-1-13	Direct communications between the OT/ICS environment and external hosts must be detected and analyzed.	**EdgeFire** is an advanced next generation firewall solution specifically crafted for OT (Operational Technology) environments. This solution facilitates network segmentation and effectively isolates connectivity between facilities and production zones. By implementing EdgeFire, organizations can enhance the security and control of their OT networks. This enables a more secure and efficient operational environment, ensuring that critical systems and assets remain protected from potential threats.

Network Security Management			
2-4-1	**2-4-1-1**	The OT/ICS environment must be segmented logically or physically from other environments or networks.	**EdgeFire/EdgeIPS** is a comprehensive industrial next generation firewall and IPS solution specifically engineered to segment OT networks from other environments or networks, whether it be through logical or physical means. By leveraging EdgeFire/EdgeIPS, organizations can establish boundaries and isolate their OT networks, ensuring enhanced security and control over network traffic.
	2-4-1-2	Different zones within the OT/ICS environment must be segmented logically or physically in accordance with the zone's appropriate level in a manner that isolates data flows and directs traffic to "choke points".	**EdgeFire/EdgeIPS** is a specialized industrial firewall solution and IPS specifically designed to cater to the unique requirements of OT segment networks. This solution provides a range of security features that enable effective segmentation, whether it is achieved logically or physically, based on the appropriate levels defined for each zone. Signature-Based Virtual Patching: Through virtual patching, the network has a powerful, up-to-date first line of defense against known threats. Users have superior control of the patching process, which creates a preemptive defense during incidents, and provides additional protection for legacy systems.
	2-4-1-3	Safety Instrumented Systems (SIS) must be segmented logically or physically from other OT/ICS networks.	**EdgeFire/EdgeIPS** is a next generation firewall and IPS solution crafted specifically for the logical or physical segmentation of Safety Instrumented Systems (SIS) from other OT/ICS networks. By implementing EdgeFire, organizations can establish boundaries to ensure the separation and isolation of SIS, enhancing their security and reliability. Both solutions segment networks and isolates connectivity both to and between facilities as well as production zones.
	2-4-1-5	Wireless technologies must be segmented logically or physically from other OT/ICS networks.	**EdgeFire** is an industrial next generation firewall solution that provides secure connectivity for OT networks that can be used to segment wireless technologies logically or physically from other OT/ICS networks.

2-4-1	**2-4-1-6**	Network communications, services, and connection points between different zones must be limited to the minimum to meet operational, maintenance, and safety requirements.	**EdgeFire** is an industrial next generation firewall designed for segmenting OT networks. It can be used to monitor/secure network communications, services, and connection points between different zones. These can be limited to the minimum to meet operational, maintenance, and safety requirements. It offers network segmentation and isolates connectivity both to and between facilities as well as production zones.
	2-4-1-7	Direct exposure of common remote authentication and access management services on external-facing hosts must be prevented.	**EdgeFire/EdgeIPS** is an advanced next generation firewall/IPS designed specifically for OT environments. It offers comprehensive support for various OT protocols, such as Modbus, Ethernet/IP, CIP, and more. With this capability, both OT and IT security system administrators can seamlessly collaborate. One of the key advantages of EdgeFire is its ability to effortlessly forge the connection to existing network architectures. By enabling OT and IT security teams to work together, it ensures a smooth integration process and enhances the overall security of the network.
	2-4-1-8	Only authorized business-critical services are accessible from the internal OT/ICS networks, and accessibility to services with known vulnerabilities must be limited to the greatest extent possible.	**EdgeFire/EdgeIPS** are next generation firewall/IPS designed specifically for industrial environments. It offers support for a wide range of OT protocols, including Modbus, Ethernet/IP, and more. This comprehensive support allows OT and IT security system administrators to collaborate effectively, facilitating seamless integration with existing network architecture.
	2-4-1-9	Direct communications between corporate zones and OT/ICS zones must be prevented, and all the required connections must be directed through dedicated, secured, and hardened jump hosts/solutions in the DMZ zone.	**EdgeFire** is an industrial next generation firewall designed for segmenting OT networks. It can be used to prevent all non-required connections. EdgeFire detects and intercepts threats with hardware specially created to prevent worms from spreading.

2-4-1	**2-4-1-12**	Dedicated gateways must be used to segment OT/ICS networks from corporate zones.	**EdgeFire** is an industrial next generation firewall/ IPS that provides flexible segmentation and isolation capabilities. It is an ideal solution for segmenting a network into easily managed security zones, offering enhanced security and protection. It can be used to create dedicated gateways to segment OT/ICS networks from corporate zones.
	2-4-1-13	Dedicated DMZ zone must be used to house any system that needs services provided by corporate zones.	**EdgeFire** is an industrial next generation firewall/ IPS designed for segmenting OT networks. EdgeFire segments networks and isolates connectivity both to and between facilities as well as production zones.
	2-4-1-14	Strictly limit the enablement or usage of industrial protocols and ports to the minimum to meet operational, maintenance, and safety requirements.	**EdgeFire** is an industrial next generation firewall/ IPS designed for segmenting OT networks. It can be used to control protocols and ports and limit enabling/usage of industrial protocols and ports to the minimum to meet operational, maintenance, and safety requirements.

Cybersecurity Event Logs and Monitoring Management			
2-11-1	**2-11-1-1**	Cybersecurity event logs and audit trails must be activated for all OT/ICS assets.	**Stellar** diligently records all event incidents generated by its agents, offering an invaluable additional layer of security to your systems. By logging these incidents, Stellar enhances your ability to monitor and analyze potential security threats, enabling proactive measures for protection. **Management Program, or ElementOne,** seamlessly logs all events generated from PI and PI Pro. This comprehensive logging functionality ensures complete visibility of security incidents throughout your network. **EdgeOne** performs a similar function by logging all event incidents generated within your network. This powerful solution adds an additional layer of security by meticulously recording these events, allowing for comprehensive monitoring and analysis.
	2-11-1-7	Malicious events must be detected and analyzed.	**Stellar** diligently records all event incidents generated by its agents. By logging these incidents, Stellar enhances your ability to monitor and analyze potential security threats, enabling proactive measures for protection. **Management Program, or ElementOne,** seamlessly logs all events generated from PI and PI Pro. This comprehensive logging functionality ensures complete visibility of security incidents throughout your network. **EdgeOne** performs a similar function by logging all event incidents generated within your network. This powerful solution adds an additional layer of security by meticulously recording these events, allowing for comprehensive monitoring and analysis. Moreover, all these solutions possess the capability to forward logs to SIEM solutions, further enhancing their integration and overall security effectiveness.

txOne networks