SECTRIO

Comprehensive OT Security Services

www.sectrio.com

TABLE OF CONTENTS

1. Document Objective

This document aims to share information on the full spectrum of OT security services offered by Sectrio.

2. OT and IoT Incident response and detection

The ability of an enterprise to quickly swing into action after detection and breach to contain it constitutes a key element of an Incident response and detection approach. In the Operational Technology world, however, the speed and quality of response to an incident is a function of many factors. Not only is OT incident response a complex process but it is also taxing in terms of resources and operational dependencies.

Therefore, a proven, well-defined, tested, and playbook-based approach to incident response is essential not just from an enterprise security standpoint but also from a SecOps efficiency perspective as well.

- Insufficient actionable threat intelligence and false positives
- Inaccurate incident categorization and prioritization leading to delays or inaccurate response
- Wrong incident diagnosis and response
- Lack of qualified staff limited visibility and capability to handle complex events
- Information overload and alert fatigue impacting the accuracy of threat detection

How Can Sectrio Help?

Sectrio's managed OT and IoT Incident response and detection services are designed to help ease the workload on internal security teams while improving the efficiency and accuracy of post-incident action. These services available to all OT and IoT operators can make a remarkable difference to your overall security posture, improve your ability to comply with global and regional security mandates and enable you to ramp up your security measures in a short period of time.

Our offering

- Helps manage your entire security workload from detection to remediation
- Reduces the burden on your internal SecOps team allowing them to focus on other KPIs
- Comes with continuous threat detection, prioritized incident response and detailed reporting on all KPIs
- Reduce scope for downtime
- Build trust: gives your customers an added level of confidence while enabling businesses to comply with various mandates

- Comes with multi-level forensics to identify and report on various aspects
- Offers flexibility to choose many response options depending on the incident and impact

How Sectrio helped a mid-sized manufacturer with managed incident response

The entity was facing a challenge with limited resources, alert fatigue, and unaddressed threats. With a complex OT environment spanning a multitude of systems and locations, the manufacturer was finding it difficult to manage its incident management needs. Once the OT incident response project was handed over to Sectrio, our team established a custom incident management approach that considered all factors and variables to improve Mean Time to Detection and Mean Time to Respond. Coupled with Continuous Threat Detection, automated response for low-grade incidents and incident analysis help, the manufacturer was able to scale up its SecOps without adding any new resources.

3. ISA/IEC 62443 Conformation Services

The ISA/IEC 62443 series of standards outline the requirements for ensuring secure industrial automation and control systems (IACS). At a bare minimum, these standards define security levels that arise from deploying security and operational visibility and control measures to address the gap between process safety and cybersecurity as well as ICS and OT systems and IT.

IEC 62443 comprises nearly 14 standards with each covering a specific purpose. To move towards IEC 62443 compliance, enterprises need to take measured steps in areas such as vulnerability management, network and operational visibility, network segmentation, network monitoring and threat detection. IEC 62443 presents a way for enterprises to ramp up their security maturity in key areas. In fact, the IEC 62443 journey can be extrapolated to go well past compliance into the proactive security management realm.
Challenges

- Resources skilled in IEC 62443
- Adequate visibility, control and preparedness
- Planning a roadmap and aligning resources and attention
- Deriving the right interpretation of IEC 62443 for a business
- Working at a device and protocol level to achieve IEC 62443 objectives

How Sectrio can help?

Sectrio's IEC62443 offering has been put together by industry experts with a clear consulting, tactical and pragmatic elements. It can take your enterprise to IEC 62443 compliance in 7 clear steps with milestones and KPIs to measure progress.

Our offering

- Offers a clear and comprehensive path to IEC 62443 without any resource or operational strain. Our assessment team will take care of understanding your current SL level and the gaps.
- Helps meet all objectives including visibility, control, patch management and mitigation of cyberattacks
- Gives your enterprise an IACS security program that is unique to your security and operational objectives
- Helps understand the gaps between current SL level and the desired SL level and ways to fix that gap
- Can also help in areas such as policies and procedures, implementation and other lifecycle requirements
- Gives custom consulting guidance for security processes, workflows, security lifecycles, controls, protocols, security acceptance and factory testing and output management

In addition, Sectrio's IEC 62443 consulting team can also work with you to establish a cybersecurity management system.

How Sectrio helped a leading automotive industry leader with IEC 62443 compliance

The company approached Sectrio with a clear requirement around IEC 62443 compliance leading to the adoption of more comprehensive set of proactive measures to curb the possibility of a breach as it was facing a huge volume of cyberattacks each day. Sectrio IEC 62443 consulting team set about the project and defined the 6 stages in association with the customer's security and plant operations teams. These steps were: pre-assessment, risk survey (at device, network, user, plant and enterprise levels) and SL identification, IACS security program design, implementation, testing and feedback analysis and program maintenance and continuous improvement planning and finally institutionalizing of IEC 62443 measures.

In addition to being IEC 62443 compliant, the business also won an award for its security measures recently and is now seen as a model enterprise in terms of its approach to security.

4. OT and ICS Penetration testing

A penetration test, or simply a pen test is a structured security testing activity designed to identify, test and highlight vulnerabilities and gaps in the security posture and approach of enterprises. The test helps identify weaknesses that could be exploited by hackers or malware to breach devices, networks and systems to attack ICS, OT and IoT infrastructure.

Enterprises conduct OT and ICS penetration testing at pre-determined schedules and frequency to ensure their infrastructure is free of any security issues. It is also recommended to conduct penetration testing when there are any major changes to networks or infrastructure, when new devices and/or systems are added or if any security measure has been violated.

Challenges

- Defining RoE and scope
- False positives in ICS and OT environments
- Optimal threat and risk coverage during testing
- Using the right tools to prevent incidents due to heavy scanning
- Scanning systems that may not be available for scanning
- Interpreting results

How Can Sectrio Help?

Sectrio's OT and ICS specific penetration testing services rely on proven tools, team expertise and hardened frameworks for every project. This ensures faster discovery of latent gaps, easy accesses to remedial measures and RoI on every penetration testing program. Sectrio deploys industry specific tools and tactics to pen test infrastructures that result in better outcomes and a more relevant outcome.

Our offering

- Leverages industry specific relevant tools for testing OT and ICS infrastructure
- Uses component and protocol level activity to expose deep gaps
- Is based on proven frameworks and tactics
- Enables validation of test outcomes
- Includes the only testing framework that covers the most sophisticated threats, variants and actors
- Sectrio also offers compensatory controls for key gaps for instant remediation
- Can also include probable attack paths

An oil and gas entity approached Sectrio to conduct two levels of penetration testing. One for identifying gaps and threat surfaces and second for testing their infrastructure against penetration by sophisticated actors with complex breach tools. The entity was satisfied by the results as Sectrio provided a clear view of the gaps and provided actionable insights into gaps by Purdue level, location, device type, system, network access rules and more.

5. OT and IoT Risk Assessment and Gap Analysis

A risk assessment and gap analysis project can help identify and prioritize unaddressed security challenges and vulnerabilities. It can form the foundation for a robust enterprise security program and offer actionable insights in areas such as security KPIs, budgets, resource allocation, operational practices, risk and threat exposure, robustness of governance measures, and overall security posture. It can identify vulnerabilities and gaps concerning technology, processes, people, architectures and supply chains and prioritize them for remedial attention.

The findings of a risk assessment and gap analysis exercise can be deployed to frame an OT, ICS and IoT security roadmap or to act to address immediate security challenges on priority. As systems evolve, the risk and threat assessment practices and methodology should also evolve to cover new threats and gaps. Conducting an OT security assessment without the help of an experienced partner can, however, be a daunting task.

Challenges

- Conducting an assessment with the right tools and frameworks
- Lack of skilled resources for conducting the assessment
- Interpreting the results for actionable interventions
- Lack of adequate visibility into systems and networks
- Covering new and emerging threats and vulnerabilities

How Can Sectrio Help?

Sectrio's OT, ICS and IoT risk assessment and gap analysis services can address such challenges while enabling security teams and leaders to focus on the overall security roadmap. The assessment is followed by the generation of a comprehensive actionable report complete with charts and other visual representations and easy-to-consume threat metric information and risk score. It also offers prioritized recommendations for addressing the gaps.

Our offerings

- Identifies a range of vulnerabilities, risks, and gaps and prioritizes them
- Enables the conduct of multiple assessments or validation of an existing assessment
- Helps comply with mandates such as NIS2, IEC 62443 and more
- Offers a comprehensive actionable report as one of the deliverables
- Detects architecture, network, system and subsystem level risks and gaps

How Sectrio helped a large enterprise meet its security assessment goals

The enterprise had conducted an OT security risk and gap assessment recently but was not satisfied with the results. Sectrio was given the project after it convinced the security team of the enterprise about its capabilities. The team was given capabilities 5 days to complete the exercise across 3 plants in different locations. After Sectrio assessment team conducted the assessment, the team did a readout of the findings in front of the entire security team of the enterprise. 73 major issues and 198 minor ones were uncovered by Sectrio's team. The enterprise used the report to address the gaps. Further, Sectrio was chosen to prepare an OT and IoT security roadmap for the company along with an OT governance policy.

6. On-demand Security Operations Center as a Service (SOCaaS) for cyber resilience

Scaling security operations requires balancing delegating security operations within internal teams and choosing the right SOCaaS (managed security services) partner. Sectrio's SOC-as-a-Service offering gives you instant access to comprehensive security solutions that fit well with your security needs, budgets and resource optimization needs. As part of the SOCaaS subscription, you get a dedicated and experienced security team with real-time threat monitoring, analysis, protection, and incident response capabilities. It is a fully modular and optimized offering that gives you the freedom to choose (or scale) various capabilities based on your OT or IoT security needs, compliance mandates, or even a threat environment requirement.

Industry challenges

- Scalability constraints due to lack of resources or budgets
- Lack of availability of skilled security analysts to run internal SOCs
- Compliance
- Balancing security, workloads and efficiency needs while addressing detection fatigue
- Lack of real-time actionable insights

Sectrio's OT and IoT SOC-as-a-Service/Managed Security Services offering comes with the right mix of capabilities in areas such as continuous threat detection, network monitoring, vulnerability management, asset discovery and intelligence, intrusion detection and prevention, incident response, event forensics and compliance management.

How Sectrio helped a large enterprise rapidly scale its OT security operations

A large global manufacturer with multi-geo operations approached Sectrio with a need to scale its security operations in line with its growing scale of production as it lacked an OT SoC. The entity was finding it difficult to meet its growing security needs due to a lack of in-house OT expertise and time and resource constraints. Sectrio initially augmented the company's own IT SOC by implementing continuous threat detection, network monitoring, secure remote access and vulnerability management capabilities around OT. Within 270 days, Sectrio scaled up the operations to cover threat hunting, decoy and deception, IEC 62443 compliance, and automated incident management.

The company now has a full-fledged OT SoC operated by Sectrio.

7. Zero Trust Enablement Services

Zero Trust is a series of measures to secure an enterprise by removing implicit trust. Simply put, it means that every action, device, operation, and configuration change has to earn trust before it can access network resources or modify the network itself in some way. At its core, Zero Trust involves a framework wherein every action is validated in terms of origin, need and end result to ensure that no unauthorized action is allowed to occur.
Deploying Zero Trust requires a complete revamp of many aspects of network usage. In an ICS environment, where many tasks and workflows are allowed based on pre-approved rules, implementing Zero Trust can present many challenges. Which is why many companies have Migration to a Zero Trust framework can however bring many benefits including better flexibility in deploying more complex security measures and improved ability to meet existing and new compliance mandates.

Challenges

- Lack of adequate visibility into networks, assets and identities, workflows, privileges and operations
- Legacy systems that run unsupported technologies
- Network complexities and integration challenges
- Defining scope and coverage
- Securing remote access
- Timely implementation

How can Sectrio help?

Sectrio's Zero Trust Services offering can equip ICS, OT, and IoT operators with the necessary wherewithal to deploy a complete Zero Trust framework based on trust provisioning across their infrastructure. Unlike vendors that promise Zero Trust in parts, Sectrio's offering ensures the deployment of Zero Trust principles across assets and sites fully customized to an enterprise's security needs. Sectrio's Zero Trust services include infrastructure review, Zero Trust gap and maturity assessment, blueprint preparation, specific analyst inputs for the Zero Trust roadmap and Sectrio's Zero Trust Security consultants will also work with your security teams to deploy the Zero Trust blueprint.

Our offering

- Offers the simplest, most comprehensive, and rapid path to Zero Trust
- Covers all compliance and regulatory requirements
- Spans the entire breadth of Zero Trust deployment from assessment and blueprint to deployment and testing of approach
- Is designed to meet the unique needs of ICS and OT operators around legacy systems, application and network complexities and latency
- Milestone-based approach covers integration of assets, sites and workflows in a streamlined manner
- Is customized to an enterprise's unique needs

How Sectrio helped a leading critical infrastructure operator implement Zero Trust

As part of an ongoing consulting engagement, Sectrio suggested the operator opt for a zero-trust approach for its various sites, assets, and operations. The suggestion was accepted and Sectrio was awarded the project based on a proposal it submitted in response to a formal EOI. Unlike competition which provided an opaque and complex project approach and schedule, Sectrio proposed a simple and easy to implement approach which won the project for it.

Sectrio's Zero Trust Consulting team visited various sites, conducted Zero Trust readiness audits, suggested soft and hard recommendations, and proposed a roadmap for the project. The team then worked with the SecOps, CISO's office, and ICS teams to implement the recommendations. The project is now in its final phase of implementation and the operator has selected Sectrio for the second phase of the project wherein the company plans to go well beyond Zero Trust.

8. Cyber Threat Intelligence Services for OT and IoT systems

The right threat intelligence can mean the difference between detecting and missing a threat. Accurate cyber threat intelligence can also reduce false positives and help you prioritize your security operations to focus on threats that matter. However, because of how it is collected, most threat intelligence service providers often go way off the mark highlighting threats that are often harmless or designed to load SecOps teams.
Thus, having the right cyber threat intelligence is not a matter of choice but a strategic and operational need for businesses.

Challenges

- Getting accurate threat intelligence
- Actionable threat intelligence for OT and ICS systems
- Threat intelligence relevant to your sector, geo, and operations
- Choosing the right cyber threat intelligence partner

How can Sectrio help?

Sectrio's cyber threat intelligence gathering facility across over 80 countries collects CTI focused on IoT and OT. In addition, our CTI is further processed and analyzed by LMMs to weed out the noise and render accurate detection of threats with fewer false positives. The CTI feeds are easy to integrate into your SIEM solutions and exponentially augment your cyber threat detection capabilities.

Our offering

- Delivers curated threat intelligence for OT and IoT systems
- Reduces load on SecOps or managed security teams
- Scale your threat detection capabilities with minimal upfront investment
- Improve cyber threat hunting across OT and IoT environments
- Improve the efficiency of your security operations

How Sectrio is helping a large FMCG business with its threat detection and awareness needs

Sectrio is working with a large manufacturer with operations in 3 continents to meet its cyber threat intelligence needs through CTI feeds. The feeds have led to a reduced workload on the SecOps team and the company has hired a full-time threat analyst to further analyze the threats reported to provide reports on the threat environment and the systems being targeted by bad actors. The company is using this information sensitize employees on the risks the business is facing to improve their behaviors and prevent any unintentional insider activity.

9. NERC CIP Compliance Services

The North American Electric Reliability Corporation Critical Infrastructure Protection or simply NERC CIP are security requirements to regulate, monitor, secure and manage North America's Bulk Electric System (BES). At its core, the NERC CIP standards provide a comprehensive set of controls to secure the functioning of critical power infrastructure by securing critical assets. NERC CIP is applicable to power plants, transmission infrastructure, and control centers.

These standards are a response to the growing threats to power infrastructure from sophisticated actors, hacktivists and other sources that could disrupt the sector and impact the economies of the countries involved as well.

Challenges

- Lack of skilled resources
- Security teams are unable to keep up with the requirements of NERC CIP
- Identifying issues to be remedied
- Complexity of OT environments
- Lack of adequate operational visibility and control

How Can Sectrio Help?

Sectrio's NERC CIP Compliance Services offer a robust path for securing the bulk electric system's critical cyber assets. The service covers identifying and securing critical and non-critical assets, specifying governance principles and training regimens for employees, incident response planning, cyber resilience and recovery and a layered, zero trust-based defense-in-depth approach that promotes resilience, and reliability across the infrastructure.

Our offering

- Covers requirements around CIP-002-5.1a - BES Cyber System Categorization, CIP-003-8 - Security Management Controls, CIP-004-6 - Personnel & Training, CIP-005-7 - Electronic Security Perimeter(s), CIP-007-6 - System Security Management, CIP-008-6 - Incident Reporting and Response Planning
- It also covers CIP-009-6 - Recovery Plans for BES Cyber Systems, CIP-010-4 - Configuration Change Management and Vulnerability Assessments and CIP-012-1 - Communications between Control Centers
- Helps tide over any resource crunch as Sectrio team can manage most of the requirements with very little intervention from your security team
- Meet any internal or external deadlines faster

10. OT and IoT Device Security Lab

ICS and IOT device integrity, data security, and overall firmware protection are important aspects to be tested before a device is integrated into a network. When devices are not tested for cybersecurity before deployment, the risk to the infrastructure grows exponentially as they may contain vulnerabilities, backdoors, and other security issues.

It is therefore important to have devices tested in an OT and IoT security lab that has the right test bed to probe and test their devices. Sectrio hosts one of the largest integrated OT and IoT security lab in the world. This lab also hosts a device testing test bed, a monitored and controlled testing and experimentation platform where solutions can be deployed via testing in real-world conditions. The lab has four parts an experimental subsystem, a probing and integrity verification facility, a monitoring subsystem, and a stimulation subsystem.

Challenges

1. Ascertaining the security level of devices rapidly before deployment
2. Ensuring a higher level of trust in devices and firmware
3. Validating the deployment readiness of devices from a security standpoint
4. Testing devices for compliance
5. Minimizing supply chain risks from devices

How can Sectrio help

Sectrio's security testbed provides the frameworks, testing principles, and platform to evaluate the behavior of devices to meet stringent security standards including those related to IEC 62443, NIST, NIS2, and various critical infrastructure regulations passed by regulators worldwide.

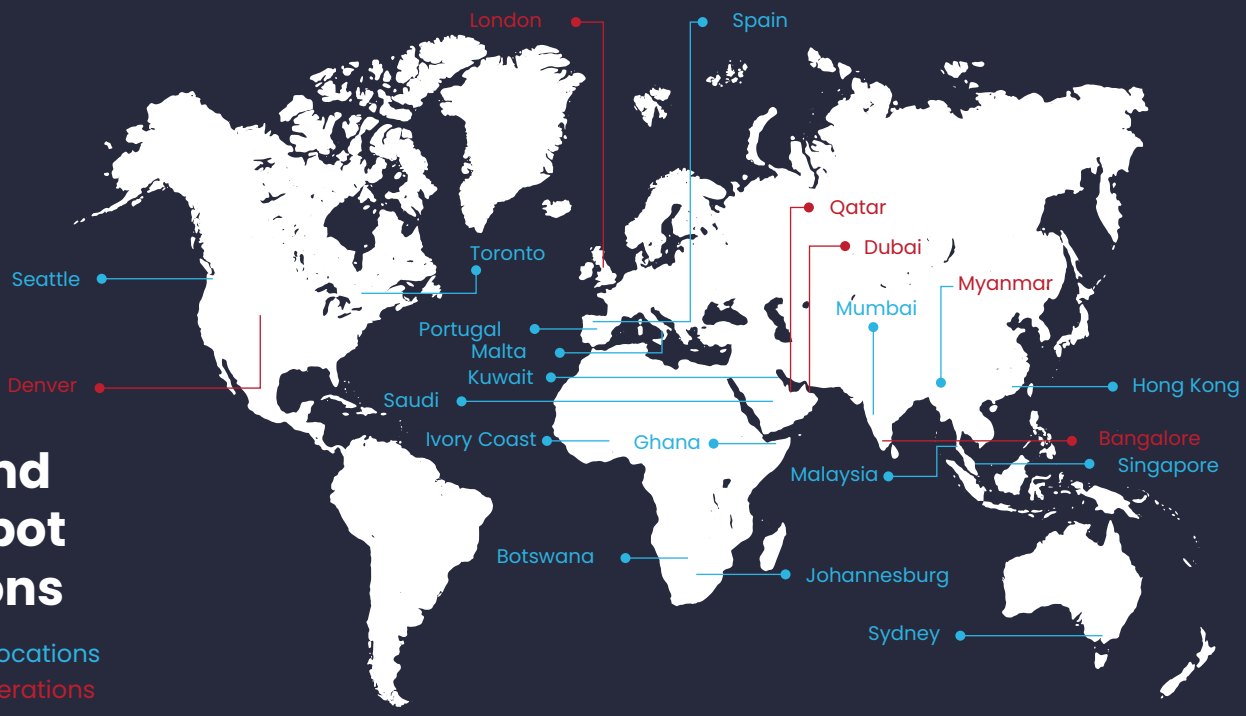
The test bed, within the lab, is backed by proven testing frameworks and methodologies and offers comprehensive security-related quantitative measurements, including risk and vulnerability score, the probability for the device being hacked, and the level of hardening needed to ensure operational integrity. Devices are also subjected to various data loads and malicious traffic in a controlled environment to test their behavior under various operational scenarios.

Our offering

- Provides a platform for rigorous, transparent, and replicable testing of devices at scale
- OEMs and device end-users can get their devices tested at our lab
- The testing covers all aspects of device security
- The testing can be customized for any compliance requirement
- Testing provides a test score with recommendations for hardening

At the end of each test cycle, a report is generated that provides a comprehensive view of the security status of the device including recommendations for improving the security profile.

ABOUT SECTRIO



ISOC and Honeypot Locations

- Honeypot Locations
- Security operations

Sectrio is a division of Subex Digital LLP, a wholly owned subsidiary of Subex Limited. Sectrio is a market and technology leader in the Internet of Things (IoT), Operational Technology (OT) and 5G Cybersecurity segments. We excel in securing the most critical assets, data, networks, supply chains, and device architectures across geographies and scale on a single platform. Sectrio today runs the largest IoT and OT focused threat intelligence gathering facility in the world. To learn more visit: www.sectrio.com

INDIA

Pritech Park-SEZ, Block 9,
4th Floor, B Wing, Survey
No. 51 to 64/4, Outer Ring Road,
Bellandur Village, Varthur Hobli
Bangalore – 560 103

Tel : +91 80 6659 8700
Fax : +91 80 6696 3333

AMERICAS

Westminster:
1499 W. 120th Ave, Ste 210
Westminster, CO 80234

Tel : +1 303 301 6200
Fax : +1 303 301 6201

EUROPE

1st Floor, Rama Apartment,
17 St Ann's Road, Harrow,
Middlesex, HA1, 1JU

Tel : +44 207 8265300
Fax : +44 207 8265352

REGIONAL – MUMBAI

Level 13, R-Tech Park,
Nirlon Knowledge Park,
Goregaon (East),
Mumbai - 400063
India.

Tel : +91-22-4476 4567

MIDDLE EAST & AFRICA

#Office number 722,
Building number 6WA,
Dubai Airport Free Zone
Authority(DAFZA,Dubai
United Arab Emirates

Tel : +9 714 214 6700
Fax : +9 714 214 6714

ASIA PACIFIC

175A Bencoolen Street
#08-03 Burlington Square
Singapore 189650

Tel : +65 6338 1218
Fax: +65 6338 1216