DATA SHEET

Cybersecurity Advisory

Operational Technology Module

Our outcome-driven advisory engagement is intended to identify gaps, as well as areas for improvement in your industrial controls systems or Operational Technology (OT) security program, **including policies, practices, infrastructure, and controls culminating in detailed expert recommendations and an actionable improvement roadmap.**

As industrial controls systems (ICS) continue to migrate towards Internet Protocol (IP) and software driven architectures to power intelligent networks and modern systems, the need to ensure security of these systems is a top priority. Threats continue to evolve rapidly, some of which could be catastrophic for mission critical control systems. Whether the risks are financial or safety, they are real, and the likelihood of a negative event is increasing regularly.

Our industry standards and good practices approach to reviewing your Operational Technology (OT) Cybersecurity program will provide a pragmatic and measurable manner to continuously assess, improve, and ultimately increase confidence in your mission critical operations. A robust security roadmap includes the unified and integrated design, implementation, and operation of security practices across your environment. This will enable you to formulate a plan to manage risks, maintain compliance with external regulations and contractual mandates, and align to industry good practices.

Our Cybersecurity Advisory service is a business-outcome driven consulting engagement with a flexible, modular framework that spans the entire lifecycle of security from developing a strategy and plan aligned to your business needs, optimizing existing security controls, to designing your next-generation OT security architecture, policies and control framework. Insight gained from optional evidence-based assessments allows you to apply your resources and controls in the most effective way to protect your mission.

> The current explosion in the number of vulnerabilities has only served to increase complexity **as organizations strive to keep up with patches and migrating controls on a weekly and daily basis.**
>
> *Source: 2019 Global Threat Intelligence Report*

Business outcome

Business outcome	Benefits
Identification of gaps in your OT security policies, practices, architecture and security controls aligned to NIST SP800-82r2.	Reduction in cybersecurity risk, transparency between business outcomes and technology controls, and achievement of your governance, risk and regulatory compliance requirements supporting an effective and secure Operational Technology environment.
Prioritized and actionable roadmap and implementation recommendations.	Improvement in cybersecurity posture across your Industrial and Operational Technology environment supporting future scale and business opportunities.
Solid cybersecurity architecture supporting future growth in a flexible and scalable manner.	A flexible and properly crafted cybersecurity OT architecture provides a solid foundation to develop and adapt to the fast-changing technology environment in a safe and secure manner.
Gain visibility between cybersecurity spend and business objectives.	Mapping cybersecurity controls to business goals and objectives helps to ensure linkage between business opportunities and business risks allowing you to make more informed and intelligence resource allocation decisions.

How we deliver

The Cybersecurity Advisory is delivered in a flexible way, allowing the engagement to be customized based upon the level of detail required.

Our Operational Technology (OT) module uses workshops and interviews to analyse the capability maturity levels of your organizations OT security policies, standards, processes and controls aligned to NIST SP800-82r2.

Our consultants work with your stakeholders to determine the gaps between your security posture today, where you want to be in the future and how your organization bridges the gap to meet future requirements. We then benchmark the results against other organizations in your industry and region to develop a highly tailored, recommended roadmap, focused on improving the efficacy of your OT cybersecurity program and your overall business resiliency.

The recommended roadmap can be used to build a budget and resource plan, or simply aligned to an existing strategy for confirmation and reassurance.

Key service features:

- Globally consistent methodology, reporting and benchmarking.
- Provides a comprehensive baseline review of the people, process and control aspects of your operational technology environment to identify any gaps.
- Provides a prioritized and actionable security roadmap that is aligned to your business requirments.

Additional Cybersecurity Security Modules for consideration

Digital Infrastructure evaluates your security capabilities for all aspects of physical/virtual networking and computing, so your organization is able to manage risks from the countless entry points into your environment from potentially insecure devices and applications.

Breach Detection evaluates your capabilities, so your organization is able to detect, investigate, control and mitigate security breaches.

Threat Intelligence evaluates your capabilities, so your organization is able to predict and prevent, protect, and respond to cybersecurity attacks.

Identity and Access Management evaluates identity and access management practices so that your organization is able to protect the identity of users and accounts and the associated access across applications, data, devices and cloud services.

Micro Segmentation evaluates your organizations maturity for your infrastructure and network security policies, standards, processes and controls so your organization is prepared for micro segmentation of your physical and virtual network and infrastructure.

Multi-cloud evaluates your security capabilities for all aspects of multi-cloud environment, so your organization is able to manage risks from the virtual machines and applications that process, store and transmit your data.

Why NTT?

Global experience
More than 15,000 security engagements with clients spanning 49 countries across multiple industries.

Track record
Decades of experience in providing professional, support, managed, and fully outsourced security services to over 6,000 clients.

Expert skills
Highly certified security consultants with expertise across various infrastructures, systems, and application technologies.

Proven approach
Client-centric, pragmatic approach using proven assessments, methodologies, frameworks, and best practices to deliver consistent, high-quality engagements.

For more on cybersecurity advisory, click here