Navigator

Industrial Security Consulting and Managed Services 2023

EY

2023
Leader
Industrial Security Consulting
& Managed Services
EY

navigator.westlandsadvisory.com

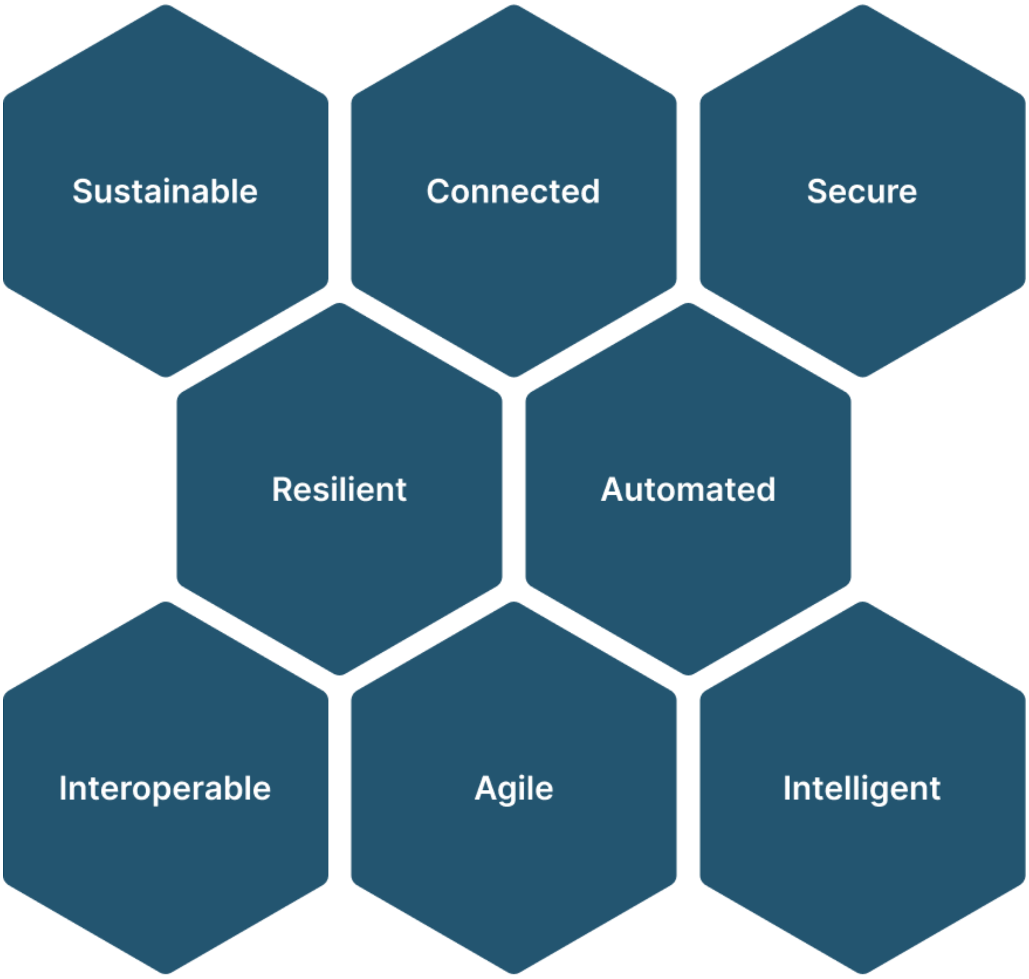
Cybersecurity challenge

Despite lower manufacturing output globally, asset owners continue to invest in digitalising plant operations. The long-term vision for most manufacturers is clear: highly connected, automated, and intelligent plants that optimise operations and create value for the entire supply chain. Yet, digitalisation also brings with it new cybersecurity challenges and risks.

One of the most pertinent issues arises from the convergence of Information Technology (IT) and Operational Technology (OT). While the merger can lead to streamlined operations and real-time data analytics, it also blurs the lines between two distinct domains, each with its own unique characteristics and requirements. This intersection can introduce new vulnerabilities, from malware being inadvertently introduced by supply chain partners to misconfigurations that could result in security incidents.

Cloud-based OT applications introduce another layer of complexity. While cloud environments offer scalability and operational flexibility, they are also susceptible to a wide range of cyber threats, including ransomware and data breaches. Moreover, the cloud's remote accessibility can extend the attack surface, providing new entry points to exploit.

The overarching challenge faced by asset owners is finding the right balance between accelerating digital transformation without incurring additional or unacceptable risks. The transition to intelligent manufacturing hinges on implementing new operations that are secure-by-design, and by moving from a security model that is entirely dependent on protecting the perimeter to blending traditional layered defence with Attack Surface Management and Zero Trust Principles. Future operations will be connected, interoperable and agile, but they also need to be secure and resilient.

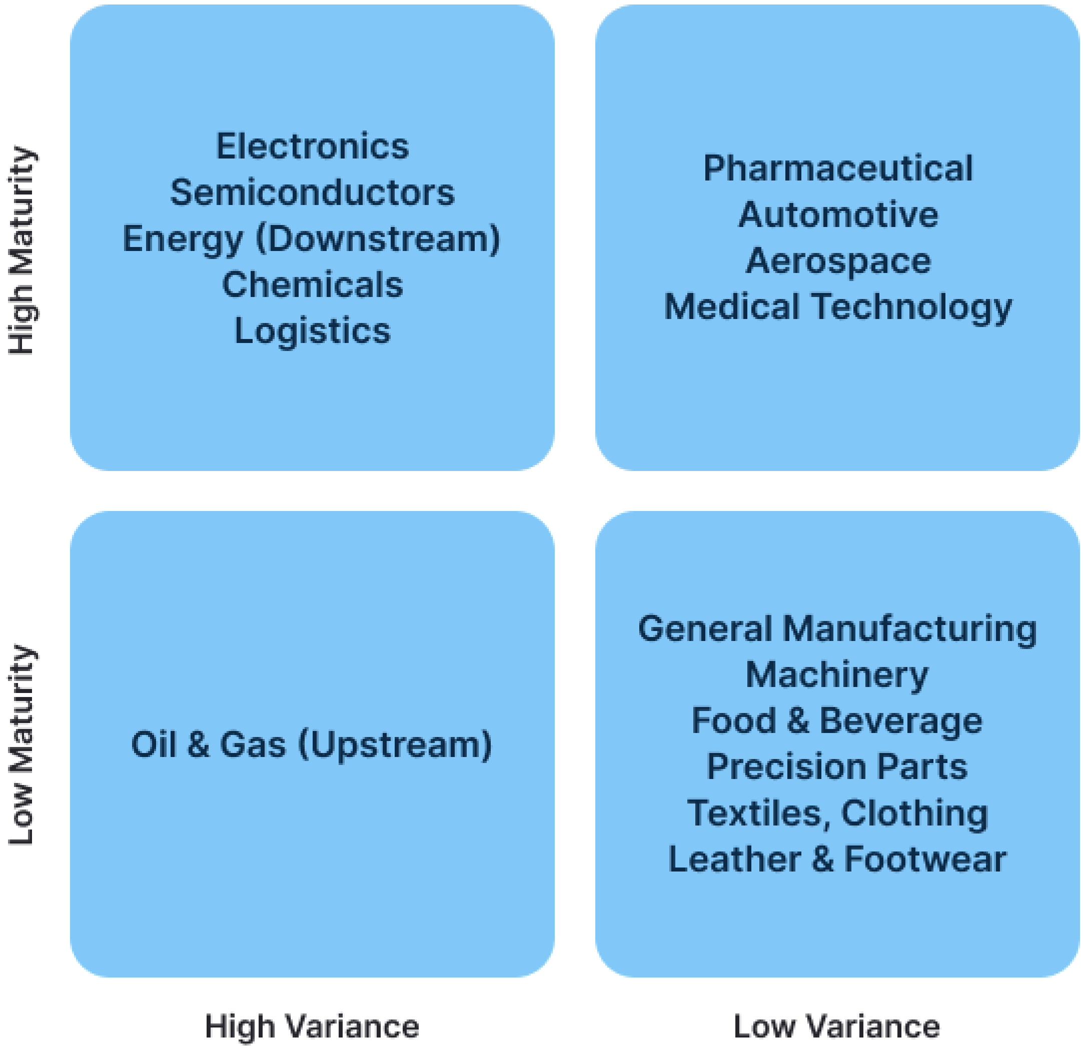


Cybersecurity maturity and target model

Despite the increased investment in OT cybersecurity, there remains a wide gap between the program maturity of the front-runners – those managing Advanced Programs – and the followers who make up most asset owners.

In most countries there is wide variation in the maturity of cybersecurity programs, ranging from no program at all to Advanced OT cybersecurity operations. In the US for example, there are a reported 250,000 manufacturing sites which contribute significantly to economic performance – about 17% of the US economy is dependent on Operational Technology. One of the largest sectors – chemical manufacturing – consists of 9,000 organisations managing around 13,500 plants.

Yet, despite the importance of manufacturing to the economy, OT cybersecurity maturity at many sites remains nascent. This can be largely traced to the maturity of digital programs. Research by the World Economic Forum (WEF) highlights the large variance that exists within industrial sectors, with Energy, Chemicals and Oil & Gas, highlighted as having highly contrasting levels of digital maturity among the operators.



Digital Maturity of Industry Sectors

	High Variance	Low Variance
High Maturity	Electronics Semiconductors Energy (Downstream) Chemicals Logistics	Pharmaceutical Automotive Aerospace Medical Technology
Low Maturity	Oil & Gas (Upstream)	General Manufacturing Machinery Food & Beverage Precision Parts Textiles, Clothing Leather & Footwear

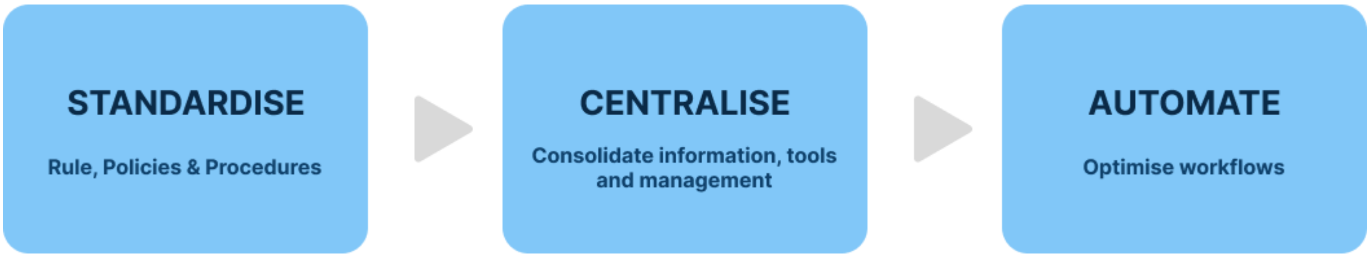
Asset owners without an OT cybersecurity program or with fledgling plans, should start with implementing Foundational security controls. This includes policies and procedures, as well as technical controls such as network segmentation, AV and patch management, and access management.

This may be the destination, or Target Security Operating Model (TSOM) for asset owners with small and less complex operations. There are many consultants and SI’s able to provide these services with high levels of specialisation by region or industry. For asset owners with large, complex operations, this is likely the start of a journey towards a more Advanced program characterised by greater strategic alignment with business operations, continuous improvement, and increasing levels of automation.

Foundational	Intermediate	Advanced
Most consultants and SI’s	Some consultants and SI’s	Few consultants
Access Controls Asset Discovery AV and Patch Management Back-up Incident Response Plans Network Segmentation Policies & Procedures Risk Assessment	Awareness and Training System Hardening Security Monitoring Vulnerability Management	Asset Management Cloud Migration Forensics IT/OT Integration Managed Threat Detection OT Security Operations Center Threat Simulation Zero Trust Architechture

The Pathway to Cybersecurity Maturity: Standardise, Centralise, and then Automate

Managing the transition from Foundational to Advanced OT security programs across sites, business line owners, and regions is challenging, requiring partners with the scale and skills to deliver large security transformation programs. Security Leaders should start the journey with a comprehensive risk assessment to identify vulnerabilities and quantify the potential impact on the availability and safety of operations. This will result in a sequential set of processes to accelerate the program: Standardise, Centralise, and finally Automate. Security Leaders rushing to automation without completing the first two steps are likely to achieve an unsatisfactory outcome.



STANDARDISE

Rule, Policies & Procedures

CENTRALISE

Consolidate information, tools and management

AUTOMATE

Optimise workflows

Standardisation is essential. Given the diversity of technologies, processes, and human practices in OT environments, harmonising rules, policies, and procedures is indispensable and lays the foundation for centralisation. A clear, consistent set of guidelines not only reduces the likelihood of error but also serves as the cornerstone upon which other security measures can be implemented. This includes using standards and frameworks such as NIST Cybersecurity Framework and IEC 62433 and adapting them to the unique exigencies of the asset owners OT environment.

The next logical progression is centralisation. There are advantages to distributed security operations that offer localised agility, but they also introduce systemic vulnerabilities through inconsistencies and siloed data. Centralising security operations in a Security Operations Center (SOC) offers the dual advantage of consolidated oversight and unified control. It simplifies the execution of policy adjustments and enables real-time, data-driven decision-making. Centralisation also allows for more effective allocation of resources, ensuring that the best tools and talents are utilised where they are most needed.

Once standards have been implemented, and the security operating model has been centralised, then asset owners can evaluate where and how automation can add value to the security operation. By adopting this framework Security Leaders are more likely to maximise the return on their investment, building a comprehensive, cohesive, and scalable security operation.

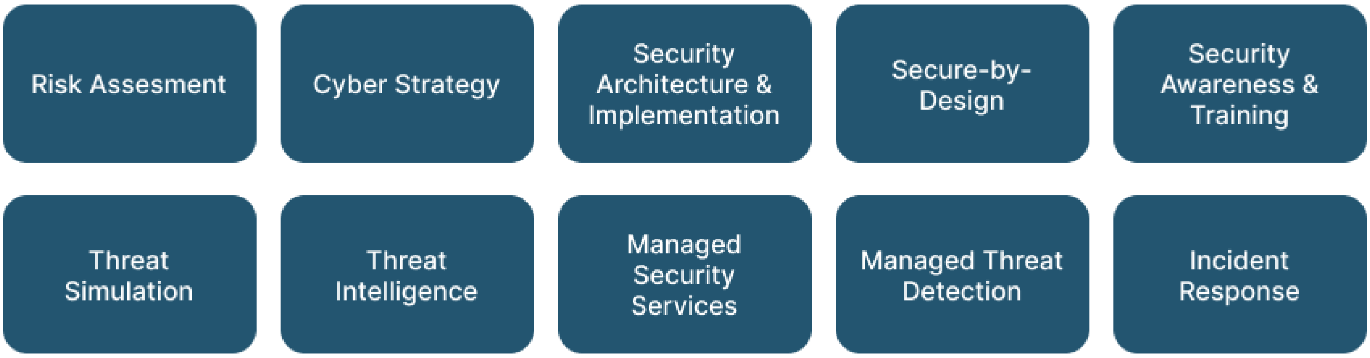
Trusted OT Security Service Providers

The design and implementation of an Advanced OT security program requires specialist skills and resources that few multinational organisations have internally. In most cases asset owners will require support from a strategic partner.

However, sourcing and selecting the right partner can be difficult as the breadth and depth of OT cybersecurity skills provided by cybersecurity services firms isn’t always clear. In addition, asset owners will have different requirements driven by the type of operation, the complexity of the organisation, and the severity of the threats and risk. For example, a small, regional manufacturing firm requiring support to implement ‘Foundational’ security requirements is unlikely to need the services of an international partner that specialises in large-scale transformation projects.

Security Leaders should consider a range of criteria when choosing partners, including the partner’s current capability and strategic direction. Capability is a measure of the security service vendors ability to deliver the required service and includes its technical capability, its experience with OT security product vendors, the quality of its customer operations, adjacent skill sets including change management, and the experience of its personnel.

Technical capability covers a wide range of disciplines. However, whilst areas such as risk assessment and security architecture design are table stakes, potential partners tend to differentiate themselves by providing mastery of a specific discipline such as Incident Response, Awareness & Training, Threat Simulation, and Managed Threat Detection. A leading OT cybersecurity service provider is likely to have dedicated OT SOC’s, OT labs for testing and threat simulation, and training facilities.



Risk Assesment

Cyber Strategy

Security Architecture & Implementation

Secure-by-Design

Security Awareness & Training

Threat Simulation

Threat Intelligence

Managed Security Services

Managed Threat Detection

Incident Response

WA advises Security Leaders to select service providers with in-depth knowledge of OT and a strong record of delivery. The market is attracting many new services firms, some bringing new skills and services, others repackaging IT security services.

2023
Leader
Industrial Security Consulting
& Managed Services
EY

Profile: EY

Summary

EY has been recognised as an industry leader in OT cybersecurity consulting and managed services for the second consecutive year.

The EY cybersecurity practice team is comprised of more than 13,700 risk professionals, augmented by an extended team with expertise spanning regulatory, engineering, change management, and legal fields. The company is present in over 150 markets worldwide. The team expanded by over 40% in 2022 to accommodate the growing demand for EY's cyber operations and OT cybersecurity services, which are among the company's fastest-growing sectors. EY's success in OT can be attributed to the firm's commitment to localising services, extensive and varied functional expertise, and sustained innovation in its cyber platform and services. These efforts have led to impressive customer retention, successful new customer acquisition, and substantial productivity gains for its clients.

The OT security practice at EY traces its roots back to 2007 and was followed by the establishment of competency centres in Warsaw, Poland (2008), Houston, US (2010), Singapore (2013), and Oman (2019). EY's experience and expertise encompass the delivery of more than 500 OT-related projects and a team of approximately 720 dedicated OT security staff, the majority of whom have backgrounds in industrial engineering. EY has a strong presence in industries such as Oil and Gas, Utilities, Chemicals, Manufacturing, Transport, Mining & Metals, and Pharmaceuticals.

EY's cyber ecosystem partner network continues to grow and now features Nozomi Networks as a recent addition. The company frequently receives accolades from its partners, including recognition from Microsoft (Global Security Partner of the Year, 2022) and CrowdStrike (Global SI Partner of the Year, 2022).

Positioning

EY has a strong reputation within government and critical infrastructure sectors, including advisory roles and contributions to regulations and standards. The company fosters a culture of innovation in OT cybersecurity, exemplified by a solutions design studio dedicated to enhancing the delivery of OT service management design and operation, OT cloud services, and the implementation of Zero Trust principles.

As a full security lifecycle service provider, EY possesses robust capabilities in risk assessment, architecture design and implementation, and security operation management. This includes extending IT SOCs to IT/OT or exclusively OT SOCs. Innovative applications developed by EY include tools for risk assessment (EY Assess), testing, training and sandboxing (ASC), threat intelligence (CTI), and cyber metrics and operations (CRD and SMP).

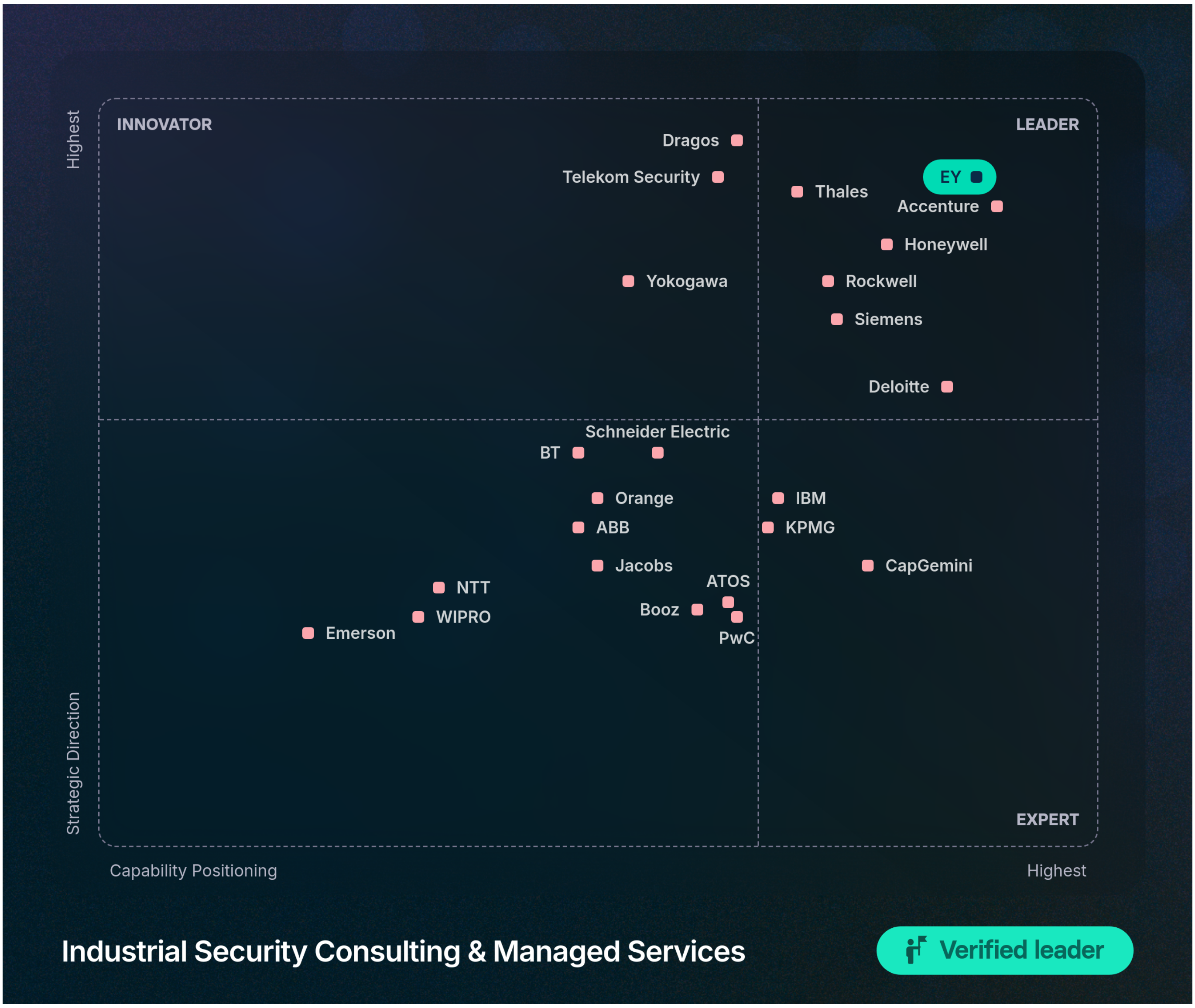
EY continues to evolve its global cybersecurity service and has outlined a long-term investment plan focused on people development, infrastructure enhancement, and service innovation. EY's customers are currently supported by a network of local offices adhering to a hub-and-spoke model. This network comprises 73 cybersecurity operations centres, IoT/OT security-specific centres of excellence, and five global SOCs equipped with OT monitoring capabilities. EY's OT labs concept and flagship facility in Poland utilises over 350 ICS environments covering all sectors and the leading IoT/OT security solutions, enabling asset owners to develop Proof of Concepts as well as testing and deploying next-generation security services.

Known for

- Security service innovation
- World leading OT Lab in Warsaw, Poland
- Complex program management
- OEM agnostic with deep technical expertise in OT systems

Industrial Security Consulting & Managed Services

The following service providers were reviewed and qualified for the 2023 OT Cybersecurity Services Navigator. Each scored highly against the main evaluation criteria and provide an end-to-end OT cybersecurity service from risk assessment to architecture design, network monitoring and incident response. All demonstrated strong technical capability across most of the 10 categories evaluated, providing customers with a global service. Service providers not included in the Navigator includes regional based OT cybersecurity specialists, IT security service providers with low levels of OT expertise, or service providers with highly specialised or niche OT cybersecurity services.



The following service providers were reviewed and qualified for the 2023 OT Cybersecurity Services Navigator. Each scored highly against the main evaluation criteria and provide an end-to-end OT cybersecurity service from risk assessment to architecture design, network monitoring and incident response. All demonstrated strong technical capability across most of the 10 categories evaluated, providing customers with a global service. Service providers not included in the Navigator includes regional based OT cybersecurity specialists, IT security service providers with low levels of OT expertise, or service providers with highly specialised or niche OT cybersecurity services.

Evaluation

The evaluation included a review of capabilities and strategic direction. The following services were reviewed as part of the capability evaluation.

- Risk Assessment

- Cyber Strategy
- Security Architecture & Implementation
- Secure-by-Design
- Security Awareness & Testing
- Threat Simulation
- Threat Intelligence
- Managed Security Services
- Managed Threat Detection
- Incident Response

Further information on WA’s methodology is on the website.

Qualification

Service providers must meet the following criteria to qualify for consideration in the IT/OT Cybersecurity Service Navigator.

- Operational Technology expertise including people, OT specific SOC’s and capability centres that includes cyber ranges.
- A wide range of services to support customers deliver against IEC 62443, NIST CSF and other relevant regulation or standards. This includes the ability to advise, integrate, monitor, and respond to incidents.
- Global capability with strong representation in more than two regions globally (NA, LATAM, Europe, Middle East & Africa, Asia)
- Strong set of customer references

Further insight on the market and industry trends is available in the related WA Insight report, “Industrial Cybersecurity Industry Analysis”

Concluding

It takes time and significant resource to design and implement an Advanced security program. For large multinational asset owners, designing and implementing the TSOM is often a highly complex change program. The large number of stakeholders, variation in technology and processes across sites, local regulatory requirements, and differing attitudes to risk, often results in a web of differing and sometimes conflicting requirements.

Asset owners should seek OT cybersecurity services firms with the requisite knowledge of OT systems and networks, experience of implementing relevant standards, and with the skills to manage change. Equally, OT Security Leaders should also consider the strategic direction of the OT security services firm including investment in new technology, processes and skills, and current and future partnerships. As manufacturing becomes more connected, automated, and intelligent, security services firms must be able to demonstrate that they have the knowledge, skills, and capacity to help customers transform operations securely.