Industrial Cybersecurity Services

BUYER GUIDE 2021

Industrial Cyber

TAKEPOINT RESEARCH

A Little Help Goes a Long Way

It's been said by those in the know that cybersecurity is a journey, rather than a destination, but not one that you need to walk alone. There are many consulting organizations, service providers, vendors and industry experts that can help you along the way.

As companies focus on their core, whether that be pharmaceuticals, manufacturing, energy distribution or chemical refining, the teams that own and run the operational technology (OT) and industrial cybersecurity in those companies will be pressed to deliver more with less.

Irrespective of where you are in the journey or cycle, starting out or well underway, there are a myriad of services offerings available to assist you. Security risk audits and vulnerability assessments are often key to getting a complete picture of the current maturity level and establishing a starting point for aligning the stakeholders in any program (OT, IT, Risk, Management). As always, it is about people, processes and technology.

Determining which standards to adopt and the best strategy for creating an enterprise-wide cybersecurity program that is applicable to all system lifecycle phases is a major task. Whether you need help segmenting your product network, or creating a cybersecurity awareness training program, or running tabletop exercises, these are not necessarily skills that you will have inside your organization.

If you need help getting started, or need to bring in a project expert along the way, or are looking for a complete managed service, the intent of this Industrial Cybersecurity Services Buyers' Guide is to help you find your way. Its aim is to give a clear and concise picture of the many services available and the companies that provide them to help secure your OT/ICS environments. The guide covers the scope of offerings from each service provider across several service categories.

This guide does not endeavor to paint a complete picture or strategy, but is intended to help purchasers, suppliers, and users of OT to better appreciate the gamut of cybersecurity solutions and tactics being addressed by vendors today.

The guide is intended to answer some initial questions to help industrial enterprises make informed decisions on where to begin when it comes to securing OT/ICS environments, and how to integrate OT/ICS cybersecurity into an organization's overall cybersecurity and risk management programs.

Jonathon Gordon
Directing Analyst
Takepoint Research

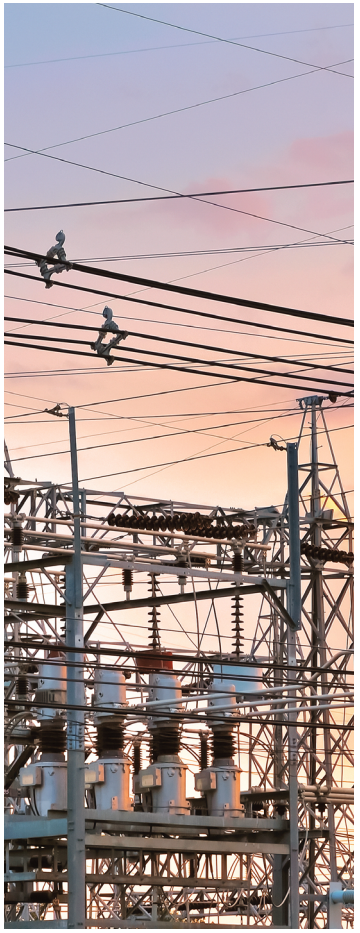
State of Market

Driven by a new wave of digitization, operational technology (OT) continues to evolve, bringing several tantalizing benefits. Operations are pursuing increased efficiency, with production processes becoming more agile and flexible. Additionally, these gains are leading to increased quality and reduced costs.

Digitalization has, however, also introduced significant risks into industrial environments. In the past, production and control systems were traditionally isolated, but the increasingly interconnected nature of these systems has created new challenges.

The integration of the Internet of Things (IoT) technologies with legacy systems and OT/IT convergence has proven especially problematic due to the absence of integrated, standardized cybersecurity mechanisms. OT systems need to be monitored, modified, revised or retrofitted, and companies often lack the required tools, support, risk awareness and expertise to get the job done.

OT and industrial enterprises remain extremely vulnerable. Cyberattacks are impacting industrial environments across multiple industries from energy and manufacturing to transportation and healthcare. Such security attacks have forced organizations to operate under stricter regulatory mandates. The threat surface continues to expand, as industrial cybersecurity is no longer simply about protecting OT networks and devices. Security threats can come from the inside as well as the outside, from the enterprise IT network or from the cloud.



To combat these negative consequences and more quickly adapt to the ever-shifting reality of digitalization, it is vital for organizations to adopt an enterprise-wide, unified industrial cybersecurity strategy. An industrial cybersecurity service firm can play a vital role in this effort, providing a wide range of tools, resources and expertise to ensure organizations are protected.

Key trends

1 COVID-19 pandemic

COVID has left its mark on how organizations maintain and secure their industrial environments. Many websites are simply not accessible, resources have been diverted and plans have been thrown into disarray. Whether the impact will outlast with the pandemic is hard to say.

2 High Demand

The demand for a specialized service player is high and growing due to the increase in attackers looking to compromise critical infrastructure for political and economic gain.

3 IT-Based Attacks

As OT systems are connected to IT networks, they often represent the weakest link in the security chain and adversaries are using IT-based threats to attack OT systems.

4 Skill Shortage

While industrial cybersecurity may no longer be in its infancy, many organizations lack expertise in this area. As a result, they must hire third-party providers to fill the gap.

5 Commercial Solutions

Security teams are shifting from homegrown approaches and defenses to commercial solutions that provide a high level of visibility across the entire OT environment.

6 Evolving Services Market

While this market has seen a flurry of new entrants in the past few years, established industrial cybersecurity vendors are also evolving their product lines to address industrial control system (ICS)-specific use cases.

Challenges

- The transformative waves of **new technologies** make securing the industrial cybersecurity environment **more challenging, and managing risks** internally a daunting task.
- Risk factors, such as an **increased threat landscape,** geopolitical instability, and a global shortage in OT cybersecurity skills have made this the most dangerous period that industrial companies have had to face.
- It is easier and cheaper than ever for malicious actors to initiate attacks. **OT equipment is readily available on eBay** and hackers can set up a home lab to find vulnerabilities. A distributed denial-of-service (DDoS) attack program can be initiated online through the dark web. Ransomware can be re-tweaked and relaunched, if it fails on the first go.
- As systems inevitably converge, OT/IT pathways become **conduits for lateral movement** across perimeters and in both directions. Innovative uses of cloud and SaaS (Software as a service) platforms also create new opportunities for malicious actors.

Technical Concerns

Inadequate network segregation: Segmentation in the OT domain is critical, but inadequate. Non-OT specific firewalls are not up to the task and there are weak boundaries between OT and IT environments.

Lack of system hardening: A lot of device installations implement minimal hardening measures, if any.

Weak access control: Access control in both the physical and digital sense is often poorly managed and can undermine the security controls that have been set in place.

Insufficient levels of identity management and authentication to both physical and logical assets, and authorization and auditing are a problem.

Insufficient logging and monitoring: Systems should be monitored in real-time for anomalous behavior, and system logs can help with forensics post-attack.

Security orchestration, automation, and response (SOAR): There is a lack of integrated holistic view and response across IT, OT, IIoT and cloud systems.

Device-level security has long been put on the 'too hard list,' although, the signals and data coming from devices and sensors can create serious blind spots. The inability to determine if the data itself is reliable is a major concern, as data can be injected and manipulated.

Cloud Security is a major concern for certain verticals such as manufacturing and building management systems (BMS), where data is exported directly into cloud-based analytics platforms.

Business Concerns

Collaboration: There are many stakeholders that need to come together to successfully secure the industrial environment. Industrial cybersecurity should be a company-wide pursuit.

Governance: Overall governance of industrial cybersecurity is still relatively low. Company-wide security policies, regular risk assessments and security planning are notable by their absence.

Staff training and security awareness: Human error and unqualified personnel are still the primary causes of industrial cybersecurity breaches. Employers must provide regular training to help staff change risk-prone behavior.

Business continuity plan: There is a lack of definition of roles and responsibilities among personnel in the event of an incident. Having such definitions in place and communicating them to operational staff can make a real difference in reducing the impact of incidents when they take place.

Third-party management: Many site operations rely on external suppliers of systems to implement and integrate security. But, there are often no formal agreements with these suppliers to ensure that the products are secure by design, posing a potential risk to the industrial cybersecurity of the organization..

Incident response planning: A detailed incident response plan that includes documented processes for isolating the cause of an incident and taking appropriate steps to restore operations is vital, if an organization is going to mitigate the amount of downtime, data loss, and reputation damage from an industrial cybersecurity incident.

Industrial Cybersecurity Services

The categorization framework in this guide has been designed to enable industrial enterprises to identify, evaluate and determine what type of services may be beneficial to their organization. These categories are designed to offer an elementary assessment of services along with an introduction to vendors who deliver those services. It is not an exhaustive checklist. The framework is not sequential, as certain services may be required at different points in the journey. Some services will likely be ad-hoc, while others may be continuous, depending on the starting point and the cyber maturity of the industrial organization at hand.

Industrial Cybersecurity Services Overview

Service categories	Sub-categories
Assess and Audit	• Asset Discovery and Inventory hygiene • Cybersecurity maturity assessment/audit • Governance, policy & procedure review • Vulnerability and risk assessment/audit
Design and Plan	• Contingency and crisis planning • IIoT cybersecurity strategy/plan • Network architecture and design planning • Playbook and response procedures • Regulations and compliance • Risk management • Secure development • Security framework and standards adoption • Social engineering and security awareness program • Supply chain security program
Implement	• Configuration and patching • Network hardening • Network segmentation • Technology deployment
Test	• Penetration testing • Recovery testing • Social engineering and phishing assessments
Protect, Respond and Recover	• Backup and recovery • Breach assessment and threat hunting • Forensics and Incident Response • Managed SOC or SOC-as-a-service • Patch Management • Remote Monitoring and Security • Threat Intelligence
Train and Educate	• Cyber Range — simulation training • Cybersecurity skills development • Industrial Cybersecurity workshops (for IT) • OT/IT alignment Program • Red vs. Blue training • Security Awareness Training

ASSESS AND AUDIT

Many industrial cybersecurity projects start with an assessment and audit phase. The primary objective of this category of services is to estimate the maturity of the industrial cybersecurity of an organization. The evaluation aims to identify flaws at all levels, including physical and network security and vendor-specific vulnerabilities in industrial control system (ICS) components, such as supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), sensors and other devices. These services often identify misconfigurations and equipment degradation, in addition to cybersecurity concerns. Hence, many services in this category will be valuable for industrial cybersecurity managers and engineers alike.

Services under this classification provide customers with information on the consequences of vulnerability exploitation, and evaluate the effectiveness of implemented security measures. It also enables an organization to plan further actions to fix detected flaws and improve industrial cybersecurity.

Services covered in this category include:

- Asset discovery and inventory sanitation
- Cybersecurity maturity assessment
- Maturity assessment
- Security and risk assessments/audit (site or company-wide)
- Supply chain assessment
- Vulnerability assessment and health check

DESIGN AND PLAN

The preparation stage is where an organization selects the areas it wants to strengthen and improve its industrial cybersecurity capabilities. Some areas may be strategic and high level such as addressing the need to demonstrate the financial and reputational impact on the company, or how to retain key staff or tactical and low level, such as identifying and documenting components essential to business-critical processes.

Services covered under this classification include:

- Contingency and crisis planning
- Identifying critical business processes and network/device mapping
- Network architecture and design
- Regulations and compliance
- Risk management
- Security framework and standards
- Supply chain security program

IMPLEMENT

The implementation phase includes installing necessary software/hardware/systems prescribed during the design and planning stage to improve industrial cybersecurity. These services may range from simple to complex, within time frames ranging from hours to weeks and months. Implementation will often require coordination across vendors and internal teams, along with the service provider conducting the work.

The implementation stage is a crucial phase and companies normally look for expedient installation. With this goal in mind, vendors often try to sell commercial off-the-shelf solutions combined with in-house tools and accelerators. However, custom-made solutions are also offered, if required.

Services covered under this category include:

- Configuration and patching
- Network hardening
- Network segmentation implementation
- Technology deployment such as firewalls, data diodes, anomaly detection, inventory and discovery platforms, device-level security, and Identity and access management (IAM)

TEST

These services include ICS penetration testing network perimeters and segmentation, as well as stress and robustness testing. Service providers will examine a wide range of factors such as authentication weaknesses, portable media security, known and unknown vulnerabilities, degradation of networked equipment, software quality and the company's employees. Many of these services will be conducted using a digital twin or another form of industrial environmental reproduction, as it is unlikely that industrial enterprises will allow system penetration testing on a live production environment.

Services covered under this classification include:

- Employee test (assessments and/or phishing/scamming scenarios)
- Penetration testing
- Vulnerability exploitation
- Recovery testing (time and efficacy)

PROTECT, RESPOND AND RECOVER

Industrial cybersecurity services may be delivered as a one-off project, at regular intervals or as part of an ongoing fully managed service. This service category is an amalgamation of multiple services that can be bundled together in line with an organization's requirements and the service providers capabilities.

Services covered under this stage include:

- Backup and recovery
- End-to-end program management
- Incident response
- Managed SOC or SOC-as-a-service
- Patch management
- Remote monitoring/security
- Threat intelligence

TRAIN AND EDUCATE

IIndustrial Cybersecurity training and education can be categorized into basic, advanced, and other training.

The basic industrial cybersecurity training often includes:

- Employees: This training introduces basic industrial cybersecurity concepts and will give employees a better understanding of why industrial cybersecurity is relevant to the organization and industry. It also covers recent cyberattacks, and provides tools and tips for spotting vulnerabilities.
- Managers: This training package includes the topics for employees mentioned above, but with a deeper dive into regulatory matters, best practices, standards, methods and tools to assess and mitigate risks.

Advanced industrial cybersecurity training:

- This training is geared towards IT/OT engineers who are responsible for maintaining the integrity, safety and performance of business operations. It is uniquely tailored for each industry and will use practical examples that are relevant to day-to-day operations.

Other industrial cybersecurity training may include:

- Social Engineering (phishing) defense: Uses simulated attacks to highlight cybersecurity risks and raise general awareness levels
- Incident response training: Assessing, training and verifying that employees are prepared for cyber incidents

Services covered under this phase include:

- Cybersecurity team training and development
- Cyber range that includes simulations, wargames, and tabletop exercises
- Security awareness training
- OT/IT alignment and collaboration program
- Industrial cybersecurity workshops

Mission Secure

CASE STUDY: IMPROVED OT CYBERSECURITY AND SERVICES RESULTS IN INSURANCE PREMIUM SAVINGS

Oil and Gas Midstream Operator | North America

In this case study, you'll learn how a North American oil and gas midstream operator collaborated with Mission Secure to establish cybersecurity best practices and improve their preventative security measures on critical ICS/OT networks that were vulnerable to threats.

Established Cybersecurity Protection Strategy

Improved OT Cybersecurity and Performance

Reduced Cybersecurity Insurance Premiums

About the Customer

The customer is one of the largest and fastest-growing vertically integrated and privately-owned midstream services providers in the USA. The provider manages 4 plants, 1,300 miles of pipelines, 1.3 Bcf/d of processing capacity, and 90,000 barrels of crude storage capacity. They provide the gathering, compression, processing, transportation and water management services required to bring natural gas, natural gas liquids and crude oil to market. Their outputs provide home heating/cooling and they generate electricity to power homes, factories and organizations of all sizes.

> *"Operational safety is the foundation upon which we provide services to our customers. We believe that prioritizing safety is good business, and, through the implementation of first-class systems, controls, policies and practices, we make every effort to create and maintain a culture that puts safety first."*
>
> **— EVP of Operations**

The provider's concerns about cybersecurity rose as their IT and control system infrastructure evolved to support the company's fast-growing operations at multiple refining facilities. Existing protections for their operations included passwords, basic firewalls and endpoint protection, which were less than optimal. Likewise, secure remote access control for third-party vendors who frequently access their control systems network for support and maintenance was also a concern. They wanted an overall cybersecurity strategy that would protect their critical and very volatile production processes.

Crafting a Solution

Mission Secure was brought in to assess the existing infrastructure. Reviews were conducted with key stakeholders to determine the IT and control system requirements and the operational engineering processes necessary to support refinery operations and to identify vulnerabilities that could lead to cyber-related incidents within those processes.

On recommendations from the Mission Secure assessment, the provider implemented new OT cybersecurity control measures including Mission Secure segmentation, protection and signal-integrity monitoring to mitigate vulnerabilities in existing systems. They also built a roadmap to remedy technology gaps, to assure the protection of people and processes as the company continues to grow, and to provide the governance and incident management needed to address security in the long term.

Together with Mission Secure experts, the provider designed a security solution for their overall ICS/OT network. They leveraged Mission Secure's services teams to install all Mission Secure Platform components at each facility. And with the Mission Secure Platform in place and staff trained, the customer turned to Mission Secure's Managed Services team for 24/7 management of their network visibility and monitoring, network segmentation and protection, and signal-integrity monitoring at each facility. With the solution in place, the provider is able to:

- Protect the operational networks from inbound traffic coming from untrusted, connected third-party networks and equipment
- Prevent unauthorized access into the multiple wireless access points around the facilities
- Provide access control and tracking in the main control system communications ring
- Lock down communications to and from engineering workstations and HMI's

Mission Secure seamless deployment was implemented with minimal impact on operations. The provider has also forged a long-term security partnership with Mission Secure to address evolving security needs, to improve security incident management, and to regularly review and update their security strategy as the threat landscape changes.

Big Savings on Cybersecurity Insurance Premiums and other Benefits

With the cybersecurity improvements and 24/7 managed services deployed with Mission Secure to reduce their exposure to potential cyber threats, the customer successfully negotiated cybersecurity insurance premium savings of approximately $50,000 per location per year.

"By taking proactive measures to improve our cybersecurity and establish best practices across our ICS/OT network infrastructure, we were able to take advantage of financial incentives and reduce our cybersecurity insurance premiums."

— EVP of Operations

Better OT Network Security, Visibility, Performance, Control

Working with Mission Secure's services team, the customer now has a custom cybersecurity plan for the people, policies and technologies associated with their production processes. Their custom security roadmap delivers a cost-effective solution and establishes best practices including:

- **Segregation of Third-Party Networks** – Segregating the ICS/OT network improves security and helps control visitor access.
- **Control System Asset Protection** – Reduces exposure across all ICS/OT systems. The customer now has comprehensive protection of the PLC ring, individual PLC's and engineering workstations / HMIs.
- **Comprehensive Network Monitoring** – Continuous OT network monitoring automates network mapping, asset discovery, logging and notification of unauthorized access attempts, and network scans through configuration rules. In this way, the customer was able to detect and block unauthorized use of DHCP and digital media players on their networks.
- **24/7 Managed Services** from Mission Secure support visibility, protection, threat hunting, and incident response functions in the operations control system networks of all facilities to improve cybersecurity resilience.

Mission Secure

As a company, we remain steadfastly focused on the use of technology to ensure operations remain safe and environmentally compliant, and that includes the cybersecurity of our operational control systems. Our work with Mission Secure is part of an on-going effort to maintain operational safety and resilience, including the reduction of cybersecurity risks.

— EVP of Operations

Mission Secure Products Utilized

- **Mission Secure Onsite OT Network Assessment:** This assessment included network monitoring, packet capture and analysis; network penetration testing; documentation of findings and recommendations; executive presentations; and go forward design guidelines.
- **Mission Secure OT Cybersecurity Platform:** This platform was purpose-designed for each processing facilities' needs and its own unique network architecture and was quickly installed with no disruption to operations.
- **Mission Secure 24/7 Managed Services:** The customer leverages Mission Secure for 24/7 Managed Services to manage visibility, protection, threat hunting, and incident response support for their facility's operations control system environments

Robust solutions need to work in the real world, not just exist on the drawing board. 1898 & Co. was born to turbocharge that purpose and is focused on envisioning and enabling the future for clients, making it both practical and progressive.

SERVICES AVAILABLE

Business depends on resilient operations and workforce safety. Clients need a partner that knows critical infrastructure facilities, is familiar with the evolving threats and risks they face, and is a steady hand navigating ever-evolving regulatory challenges.

Risk management and resiliency for critical infrastructure environments are all about safety and reliable operations. 1898 & Co. achieve risk management and resiliency using a three-pronged approach that balances regulatory compliance, system reliability and cyber risk management. The team integrates consultants experienced in all three areas, and is focused on improving the safety, security and reliability of the critical infrastructure. It delivers people, processes and technology that enable risk and resiliency, preparedness and situational awareness.

The team knows that protecting assets is a balancing act, weighing what's right for the business, managing risks and deploying offerings that enable focusing on core business. Its highly experienced consultants help strategize, design, implement and operate a cybersecurity program that balances business goals, budget and risk tolerance. It acts as a force multiplier for the organization, program and workforce, and will help establish a culture of resiliency.

SERVICES INCLUDE:

- **Asset inventory**
- **Business outcome solutions**
- **Diagnostic assessments**
- **Incident response**
- **Strategy and advisory**
- **Secure system design and implementation**
- **Training**

1898andco.burnsmcd.com
+1 816-605-7800
matt.morris@1898andCo.com

Advenica Ab

SERVICES AVAILABLE

Advenica helps operators of critical infrastructure recognize vulnerabilities in current network or hardware components, and take strategic measures for higher information security. Advenica's Data Diode ensures unidirectional information exchange, thereby blocking everything from the outside. Advenica offers infrastructure security related products as well as services.

SERVICES INCLUDE:

- **Risk and security analysis:** helps in surveying the current and future IT security needs of an organization.
- **Customized solutions:** Offers tailor-made application and service development. The company can either help the client create a boutique solution or teach them how to solve it in-house.
- **Advenica academy:** Advenica Academy provides the client's staff with the right skills and knowledge to use its products and maximize the security investmentt.
- **Penetration testing:** Advenica provides penetration testing of embedded systems, mobile applications, operating systems, windows applications, and networks.
- **Managed services include:** Advenica also provides managed security services to its clients.

https://www.advenica.com/
+46 (0)40-60 80 400
sales@advenica.com

Airbus Cybersecurity

SERVICES AVAILABLE

Airbus OT security services help critical infrastructure providers to build and maintain persistent cyber resilience for interconnected industrial systems. The company follows a three-step approach for Operational Technology (OT) cybersecurity - Access, Protect, and Manage. Airbus is an experienced player in this industry, and offers industry-specific know-how for critical and complex infrastructure and production environments.

Airbus OT services solution is modular in nature, and can be integrated into existing security programs and ways of working.

SERVICES INCLUDE:

- **Access:** The service includes OT asset discovery and analysis, OT security maturity check, OT security pen-testing, and risk assessment.
- **Protect:** It includes services like OT policies and framework consulting, OT security design, integration, and training and awareness.
- **Manage:** These services include SOC, managed OT security infrastructure and cyber-on-demand.

https://airbus-cyber-security.com/
+33 (0) 1 61 38 50 00

BAE Systems

SERVICES AVAILABLE

BAE Systems is an Operational Technology (OT) security service provider. Its services include assessing, designing and managing cybersecurity offerings for complex and mission-critical assets. As a global manufacturer and systems-integrator, BAE brings rich experience in this segment, coupled with the latest industrial cybersecurity knowledge and products, and uses its expertise to help customers successfully secure their operational infrastructure.

BAE has a team of dedicated industrial cybersecurity experts with professional engineering pedigree and experience. Its offerings are compliant with CPNI and IEC62443 cybersecurity standards.

SERVICES INCLUDE:

Services include security advisory, security diagnostic, risk assessment, security strategy, security architecture, security framework, network segmentation, network monitoring, security testing, security assurance, security training, and security cases.

https://www.baesystems.com/

Cisco Systems, Inc.

SERVICES AVAILABLE

Being the World leader in both cybersecurity solutions and industrial network equipment, Cisco has built comprehensive services to help industrial organizations secure their OT infrastructure.

SERVICES INCLUDE:

- **Security Assessment:** a simple, high value method for end users to begin or accelerate their cyber security journey. Conducted onsite or remote, it leverages Cisco Cyber Vision to analyse the industrial network. Assessment deliverables includes asset inventory, vulnerabilities, maps of application flows, and actionable roadmap to enhance security posture.
- **Proof of Value (POV):** provides the end user a chance to see live OT security monitoring in action in their facility, combining protocol analysis, intrusion detection and behavioral analysis to detect simulated attacks and vulnerabilities.
- **Industrial Network Primer:** a comprehensive industrial network analysis that documents the customer network architecture and presents a recommendation for improving the architecture to meet the current and future demands.
- **Plan, Design, Implement (PDI):** a full suite of services to help customers from start to finish including architecture planning, high level and low level design, implementation, testing, and long term support.

www.cisco.com
cxpmiot@cisco.com

Booz | Allen | Hamilton

SERVICES AVAILABLE

Booz Allen Hamilton combines industry knowledge and experience with people and technologies to reduce risk, improve safety, and increase business profitability. Its Operational Technology (OT) security offering is called SAF-ICS, which is developed in partnership with Splunk. SAF-ICS is a pragmatic OT risk assessment lifecycle used by Booz Allen Hamilton to prioritize and mitigate risks in industrial cybersecurity environments.

With a unique perspective born from supporting OT offerings across markets, Booz Allen Hamilton provides a hands-on, mission-focused approach to OT security, with cutting-edge approach enabling broad visibility and secure OT.

SERVICES INCLUDE:

- **Cyber Risk:** Its cyber threat-centric approach helps to quickly identify and prioritize cyber vulnerabilities to implement a resilient defense. Managing cyber risk thresholds promotes improved organizational readiness.
- **Cyber Architecture and Engineering:** The company helps clients to deploy the best hardware and software offerings to meet the evolving cyber threat landscape while remaining aligned with their cyber strategy and operations plan.
- **Cyber Defense Operations:** Advanced cyber defense empowers users to become more proactive through threat-informed decision making.
- **Cyber-Enabled Platforms:** Booz Allen Hamilton assesses and hardens system security at the intersection of cyber and physical platforms. It empowers industrial companies to anticipate and respond to today's cyber challenges. From strategy and design, to implementation and operations— the company enables users to keep their energy company secure.

www.boozallen.com

Capgemini

Capgemini offers its clients a range of services designed to protect business-critical systems, such as industrial control systems (ICS), Supervisory Control and Data Acquisition (SCADA), and embedded systems. Its cybersecurity offerings includes industrial system security assessment that helps critical system operators defend themselves against sabotage and blackmail attacks; digital manufacturing securing products and industrial systems; and energy IoT that protects smart and connected assets.

The company's capability for protecting industrial and embedded systems is supported by R&D teams working on offerings adapted to an industrial context. It has been securing industrial systems of major industrial operators and manufacturers for many years,and demands a high level of system security. For example, Capgemini helped a global industry leader in the utilities sector define the security protections and deploy them on all their industrial sites. The plan included raising awareness on security amongst employees.

SERVICES AVAILABLE




SERVICES INCLUDE:

- **Industrial System Security Assessment:** Helps critical system operators defend themselves against sabotage and blackmail attacks.
- **Digital Manufacturing:** Focuses on improving the digital maturity of core manufacturing functions across product and asset lifecycle management, onsite and remote operations management, industrial IoT and big data, system simulation, and industrial cybersecurity.
- **Energy IoT:** Allows businesses to deploy offerings to meet the broadest range of use cases through intelligent edge technologies, open machine-to-machine communications capabilities, and big data analytics.

https://www.capgemini.com/

Deloitte.

To counter the growing industrial cybersecurity risks and threats, Deloitte's cyber threat management for Operational Technology (OT) uses a combination of cybersecurity offerings and services to manage cyber risks in Industrial Control System (ICS) environments. The integrated end-to-end offering leverages Deloitte Cyber Strategy Framework (CSF), technology platforms, Deloitte Cyber Intelligence Center (CIC), and dedicated ICS threat intelligence team.

SERVICES AVAILABLE






SERVICES INCLUDE:

- With the Deloitte CSF based on industry standards such as ISO27001/2, NIST 800-82/53 and IEC 62443, Deloitte sets a standard in helping organizations assess their maturity, and in developing and tracking the implementation of ICS security.
- Deloitte uses a technology platform that helps in managing asset inventory and ICS assessments.
- Deloitte assists with deploying the ICS platform for continuous monitoring.
- Deloitte Secure Operations Center (SOC) as a managed service.
- Deloitte leverages the technology partner's Threat Operation Center for extended ICS knowledge, training and intelligence.

https://www.deloitte.com/de
RA_cyber_marketing@deloitte.de

Dragos

SERVICES AVAILABLE

Dragos is a cybersecurity company with an ecosystem tailored for industrial environments, including industrial control systems (ICS), Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS), and Operational Technology (OT) environments.

SERVICES INCLUDE:

- **Threat Intelligence:** Backed by a team of ICS cybersecurity practitioners, Dragos Threat Intelligence provides organizations with in-depth visibility of threats targeting industrial cybersecurity environments, and tried-and-true defense recommendations to combat them.
- **Neighborhood Watch:** The ICS security team can be boosted by leveraging Dragos technology and expert analysts using managed ICS/OT network visibility and threat hunting.
- **Professional Services:** Help build an ICS industrial cybersecurity strategy for the organization that provides proactive and responsive offerings for understanding the ICS environment, mitigating risks, and responding to threats.
- **Training:** Strengthen the team's ICS cybersecurity skills with training and improve their ability to prevent, detect, and respond to cyber attacks in OT environments.

https://www.dragos.com/
(855)-372-4670

ElevenPaths (Telefonica)

SERVICES AVAILABLE

ElevenPaths, Telefónica Group's global cybersecurity company, guarantees peace of mind to customers knowing that their Operational Technology (OT) and IoT (Internet of Things) offerings include best practices in security matters, with appropriate defence mechanisms.

SERVICES INCLUDE:

- OT & IoT Security Professional Services: Cybersecurity consultancy and audit (GDPR, ISO, ENS, ISA 62443, NIST 8082, IoT security framework and security checklist, ETSI)
- Perimeter protection with network segmentation and from P-LTE/P-5G networks
- OT & IoT security monitoring providing assets visibility and risk mitigation
- Remote access providing the best fit for the client's remote access needs
- USB protection as a portable security or as an advance USB sanitization
- Secure credentials automates process of providing an identity to IoT devices for accessing public cloud IoT services and establishes a secure end-to-end IoT communication
- Automated Telecom Network Audit tailored solution for the use cases 4 and 5 of industrial IoT networks based on private LTE or 5G
- MSSP services from SOCs with global footprint

https://www.elevenpaths.com/

DXC Technology

SERVICES AVAILABLE

DXC Technology's Operational Technology (OT) Diagnostic provides consulting services and specialized tools to help organizations gain insights into their enterprise's OT cyber maturity. It combines skills and experience, partner technologies, and DXC's Cyber Reference Architecture (CRA) to elevate industrial cybersecurity in client's OT environments.

The company has more than 3,500 security advisors and a global network of security operations centers.

SERVICES INCLUDE:

- **Cyber Defense:** Consists of tailored offerings to support the digital enterprise, enabling them to monitor and respond to evolving threat landscapes.
- **Secured Infrastructure:** Helps meet the unique security requirements of clients through design, installation, and integration of perimeter, network, endpoint, and advanced threat protection offerings.
- **Digital Identity:** Includes provisioning and access governance to deliver strong authentication and Public Key Infrastructure (PKI) that protects the enterprise.
- **Data Protection:** Helps with protecting critical data and assists enterprises understand the use of critical content.

https://www.dxc.technology/
+1 (877) 889-9009

Emerson

SERVICES AVAILABLE

Emerson manufactures products and provides engineering services across industrial, commercial, and consumer markets. As part of its OT services, the firm combines its power and water cybersecurity suite with a portfolio of industrial cybersecurity services to deliver platform-independent offerings. Its solution also helps in securing all assets, and strengthening the OT security posture.

Emerson's OT security services include project services, lifecycle services, educational services, and cybersecurity services.

SERVICES INCLUDE:

- **Project Services:** This includes systems projects, instrumentation projects, valve projects, conceptual design and feasibility studies, and data management services.
- **Lifecycle services:** This covers a set of flexible services to support the specific needs of the control system and cybersecurity suite.
- **Educational services:** Includes ongoing training programs for operators, engineers, technicians, and maintenance personnel.
- **Cybersecurity services:** This involves services for critical infrastructure protection, such as assessment services, custom cybersecurity services, and fleet cybersecurity services.

www.emerson.com
+1 888 889 9170

GE Digital offers industrial managed security services for OpShield, designed for operational technology (OT) environments. GE Managed security services allow organizations to support and protect their critical processes and control strategy, while providing visibility and insight for broad situational awareness.

With OpShield deployed in Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and other OT environments, features such as network segmentation, deep protocol inspection, and network whitelisting capabilities inform GE Digital security analysts, either with alerts or block commands.

SERVICES AVAILABLE

SERVICES INCLUDE:

- **Advisory Services:** GE helps organizations plan and start their industrial IoT journey to align with specific business outcomes.
- **Managed Services:** This includes maintenance of critical machines from remote locations around the world using model-based predictive analytic technology.
- **Implementation Services:** GE's automation partners can implement a collaborative, multi-generational program that marries (integrates) the existing investments to the right enhancements and technology.
- **Education Services:** GE specializes in education services to ensure that the customers are leveraging GE's offerings to the fullest extent with training and certificate programs.
- **GlobalCare Support Services:** This enables users by ensuring that their business continues to operate at its highest efficiency.
- **Cyber Security Services:** GE provides industrial-grade security for a variety of OT network and application topologies.

www.ge.com
+1 855 968 7143

HCL's Managed Services provide the ability to monitor, identify, investigate, respond, report, evaluate, and recommend, to help maintain a responsive industrial cybersecurity ecosystem. The managed services also complete the 'Dynamic Cybersecurity Framework' by ensuring that the posture is continuously monitored and reviewed for 360-degree protection, around the clock and across the globe.

SERVICES AVAILABLE

SERVICES INCLUDE:

HCL offers three services as part of its 'Dynamic Cybersecurity Framework':

- **Strategy and Architecture (Plant OT-IT):** This includes risk assessment, asset definition and inventory management, cybersecurity assessment consulting, security controls, and convergence consulting services.
- **Transformation and Integration (Controls Validation and Integration):** This includes operations protection, network design security, network segregation, systems and connected device security configuration, implementation of Industrial Control Systems (ICS) vulnerability management tools, and plant IT/OT security monitoring services.
- **Managed Services (Continuous Security Lifecycle Improvement):** This includes business-aligned security service management, track and monitor cyber incidence, threat and vulnerability management, continuous review and predictive maintenance, and triage management and service.

www.hcltech.com

Honeywell

Industrial companies no longer have to choose between security and the benefits of a connected enterprise. Honeywell provides over 30 specialized industrial cybersecurity offerings and custom consulting to help process control industries safely operate and accelerate their digital transformation — regardless of their cybersecurity maturity.

WHERE INNOVATION MEETS IMPLEMENTATION TO DRIVE INDUSTRIAL CYBERSECURITY EXCELLENCE

Honeywell

SERVICES AVAILABLE

Honeywell Forge Cybersecurity solutions strengthen and protect the availability, reliability and safety of critical Industrial Control System (ICS) and Operational Technology (OT) assets in manufacturing, refinery and critical infrastructure sectors. These solutions are designed for process control environments found in Oil & Gas, Chemicals, Refining & Petrochemicals, Energy & Power, Minerals, Mining & Metals, and Pulp & Paper.

Honeywell Forge Managed Security Services (MSS): Honeywell MSS utilizes Honeywell's Security Service Centers in the USA, Europe and Asia to provide 24x7 "follow-the-sun" service, staffed by cybersecurity experts who know how to protect complex OT infrastructure. Honeywell Forge MSS includes:

- **Secure Remote Access and Support** is for customers who want a single, industrial grade secure solution for all remote connectivity.
- **Advanced Monitoring and Incident Response (AMIR)** accelerates cyber threat detection through proactive, 24x7 monitoring, threat detection, deeper analysis, and incident response. The result is broader visibility of cybersecurity threats, while minimizing the risk of severe operational, financial and reputational damage.
- **Automated Patch and Anti-Virus Delivery** uses an industrial-grade, remote connection to automate the encrypted delivery of all patches and anti-virus files. Honeywell software updates undergo extensive application testing and qualification in an emulated customer environment before implementing onsite.

Honeywell Security Consulting Services: Honeywell consultants provide cybersecurity expertise, knowledge and training so OT organizations can focus their valuable resources to drive business results while ensuring security, compliance and avoiding production losses.

www.honeywellprocess.com
1 215 641 3610
hfs-tac-support@honeywell.com

IBM Security

SERVICES AVAILABLE

IBM Security offers end-to-end threat management for OT, IoT, and Internet-of-Medical-Things (IoMT) environments. It offers a portfolio of Operational Technology (OT) security offerings that help industrial, asset-intensive environments monitor and secure networks, protect endpoints and deliver industrial cybersecurity services.

SERVICES INCLUDE:

- **Assessment:** IBM can help clients understand risks, gaps and vulnerabilities using a phased approach. It includes engaging in strategy and planning, OT security risk, compliance and vulnerability assessments, and developing governance policies and requirements.
- **Protection:** IBM's partner ecosystem can help clients with data discovery, classification and analysis, network and endpoint security design and implementation, and designing, building and deploying identity and access management (IAM) offerings. It can also help plan and deploy an OT SOC protection for client's operations.
- **OT Managed Security Services:** IBM can also help clients manage alerts and reduce false positives with OT Managed Security Services, develop OT security incident response plan and playbooks, and leverage security analytics.

https://www.ibm.com/

SOPHIC
powered by ISRAEL ELECTRIC

IECyber is a cyber entrepreneurship and business development unit in the Israel Electric Corporation (IEC) that provides a portfolio of cyber offerings and services. The company's experience, insights, practices, and tools have been packed into its cyber defense and resilience suite and service offering – SOPHIC.

SERVICES AVAILABLE

The SOPHIC Suite provides cyber services and offerings that leverage assets, and integrate human skills and behaviors with advanced technologies. It includes cyber defense and cyber resilience offerings and services based on experiences, gained in challenging geopolitical environments.

SERVICES INCLUDE:

- **SOPHIC PRO:** Services are precisely adapted to customer needs, culture, regulations, and procedures. It unites a range of professional and consultancy services, covering the whole range of cyber management in an organization, in order to provide users with tools and practical recommendations for both routine and crisis times.
- **SOPHIC OT:** Sophic Info: It allows secure file sanitation and transfer for global SCADA critical infrastructure operators.
- **Sophic Access:** It allows remote users, including employees and third party vendors, to securely support critical parts of the OT networks, efficiently and timely.
- **Sophic Zone:** It emulates, simulates and validates actual cyber-attacks on ICS/SCADA, in a near real-world environment, outside operational boundaries. Users will be able to upload or set any architecture based on virtual and physical devices.
- **SOPHIC PICTURE:** An integrative cyber security platform that provides detailed, accurate, continuous and updated holistic cyber picture of the organization. SOPHIC PICTURE aims on becoming the "customer cyber compass".

www.iecyber.co.il
+972-72-3434588
sophic@iecyber.co.il

Kaspersky

SERVICES AVAILABLE

Kaspersky Industrial Cybersecurity (KICS) solution includes a portfolio of products and services designed to provide holistic protection for every industrial layer, including Supervisory Control and Data Acquisition (SCADA) servers, Human-Machine Interface (HMI), engineering workstations, programmable logic controllers (PLCs), network connections, and people.

SERVICES INCLUDE:

- **Training and awareness services:** On-site and online professional education in incident response and investigation in Operational Technology (OT) and basic training for OT specialists.
- **Incident Response:** Remote and on-site investigation and remediation plans, handbook preparation and simulations.
- **Threat Intelligence:** Includes Industrial Control System (ICS) vulnerability research, threat intelligence data feeds, advanced persistent threat (APT) reports, and customized reporting.
- **Cybersecurity Assessment and other services:** Includes Penetration testing, cybersecurity assessments, cybersecurity maturity model, SOC and CERT consultancy.

www.kaspersky.com/ics
ics@kaspersky.com

KPMG International

SERVICES AVAILABLE

KPMG's cybersecurity team works with organizations to prevent, detect, and respond to cyber threats. The company provides users with its expertise in Operational Technology (OT) using capabilities in strategy and governance, security transformation, cyber defense, and digital response services.

SERVICES INCLUDE:

- **Assessing risks and capabilities:** Adopt established methodologies, international standards, and experience.
- **Improving Governance:** Helps bridge the gap between OT and IT teams, and reduce uncertainty over responsibilities.
- **Building Assurance:** From point-in-time Industrial Control Systems (ICS)-specialized security testing to creating ICS-inclusive internal audit programs, and governance, risk and controls (GRC) integration.
- **Delivering Transformation:** KPMG brings specialized knowledge, sound program, and project management practices.

https://home.kpmg/

MARSH

SERVICES AVAILABLE

Marsh is an insurance broking and risk management firm that works with clients to define, design, and deliver offerings to better quantify and manage risk. The company offers risk consulting, insurance broking, alternative risk financing, and insurance program management services to businesses, government entities, organizations, and individuals. It has a presence spread across 130 countries.

Marsh cyber risk offerings are primarily centered around consulting services that address the essential elements of cybersecurity, from strategy, governance, and enterprise risk management to control architecture, implementation, and management.

SERVICES INCLUDE:

- **Enterprise-wide cybersecurity program review and road mapping:** Includes risk assessment, testing, performance validation, and joint roadmapping.
- **Cybersecurity risk quantification:** Includes enterprise risk management and modeling the cyber operating environment, and generating a dashboard view of the «cyber value-at-risk.»
- **Security technical controls review:** Includes review of cybersecurity technical controls environment, assessment of the enterprise cybersecurity architecture and technical controls, and evaluation of operational effectiveness.
- **Third-party cybersecurity risk management review:** Helps in identifying likelihood of cyber risk based on third-party relationships.
- **Scenario-based cyber exercises:** Includes executive-level tabletop exercises, test assumptions, operational processes, validating external resources, and points-of-contacts (POCs).

https://www.marsh.com/
Phone: 1 (617) 385 0200

Mission Secure

SERVICES AVAILABLE

Mission Secure is an industrial control system (ICS) cybersecurity company providing patented Mission Secure Platform and cyber advisory services to help its clients spread across the energy, defense, maritime, and critical infrastructure sectors. The company follows a technology-based Operational Technology (OT) cyber assessment that helps its clients understand the industrial cybersecurity risk for their critical control system.

The Mission Secure Platform offers an end-to-end ICS industrial cybersecurity solution delivering visibility and protection down to Purdue Levels 0 and 1.

SERVICES INCLUDE:

- **Managed Services:** a 24x7 OT security team for monitoring, protection, and incident response. Mission Secure has two Threat Management Centers that help in monitoring operational network health, device protection and maintenance, anomalies detection, and incident response support.

www.missionsecure.com
info@missionsecure.com

PricewaterhouseCoopers

SERVICES AVAILABLE

PwC provides industrial cybersecurity services to increase the security posture of ICS/OT systems. PwC can help an industrial organization in various ways, such as through strategy and governance, security architecture, security implementation, threat and vulnerability management, risk and compliance, incident management, managed services, and identity and access management (IAM) security.

SERVICES INCLUDE:

- **ICS risk assessments:** The assessment covers system records and activities to determine the adequacy of system controls. The activities include a review of network architecture and network security systems configuration to assess operating efficiency of technical controls.
- **ICS vulnerability assessment /penetration testing:** This evaluation provides a three-step approach to examine the ICS security posture. It includes capabilities to test ICS network from the internet, test ICS network from IT, and test selected offline ICS systems for vulnerabilities.
- **Compliance assistance:** PwC can help industries in adapting to international and country-specific security standards.
- **Security operations center (SOC):** PwC also provides services SOCs to set up a combined ICS-IT environment.

www.pwc.com

NTT

NTT works with global organizations to achieve business outcomes through technology offerings. Its Intelligent Cybersecurity services help clients create a digital business, which is secure by design. With its threat intelligence, NTT helps users to predict, detect, and respond to cyberthreats, while supporting business innovation and managing risk.

NTT believes in securing both IT and Operational Technology (OT) at the same time, as the two environments are converging. Using a 'Secured by Design' methodology, NTT's offerings help clients secure the OT network every step of the digital journey with intelligence-driven security – from planning and design, to implementation, to live operations and monitoring, and lifecycle maintenance.

SERVICES AVAILABLE

SERVICES INCLUDE:

- **OT Cybersecurity Advisory:** Delivered by OT cybersecurity consultants, NTT bridges the client's IT-OT gap, performs rapid and detailed OT cybersecurity assessments, and delivers an IT-OT converged assessment.
- **IT-OT Threat Monitoring:** SOC-based service that monitors threats in both IT and OT networks. This service is technology agnostic and focuses on outcomes. Client uses this service to obtain state-of-the-art monitoring.
- **IT-OT Managed Security Services:** SOC-delivered service that covers a client's end-to-end cybersecurity operation to help manage technology lifecycle such as configuration, and patching.
- **Global Technology Services:** Delivered by technical experts, NTT provides best of breed technology, carries out in-depth design workshops, and manages deployment. Its footprint supports a variety of procurement and deployment models – globally, locally, or both.

https://hello.global.ntt/en-us/solutions/intelligent-cybersecurity/secure-ot

radiflow

Secure your Assets

Radiflow develops industrial cybersecurity solutions for critical business operations that empower users to maintain visibility and control of their operational Technology (OT) networks; detect, prevent and monitor cyber threats; and manage and reduce network risk.

iSID, Radiflow's industrial threat detection system provides non-intrusive network visualization and threat detection using multiple security engines. iSID is compatible with MSSP-SOC operation through a central management utility, and is a recognized compliance enabler.

CIARA, Radiflow's industrial risk analysis platform, enables users to optimize their network security expenditure with business-driven risk-mitigation recommendations that maximize overall network risk reduction. CIARA is fully IEC62443 compliant, and is ideal for managed security service provider (MSSP) operations. For more information visit:

www.radiflow.com

SERVICES AVAILABLE

Industrial Cybersecurity Solutions for Critical Business Operations

- Scaleable detection & prevention tools
- Business-driven OT risk scoring
- Enabler for IEC62443, NERC CIP & NIS-D
- Over 4,500 protected sites worldwide

Request a personalized demo at
radiflow.com/demo

radiflow

www.radiflow.com | info@radiflow.com

Rockwell Automation

SERVICES AVAILABLE

Rockwell provides industrial cybersecurity offerings with a comprehensive approach beyond just network security, protecting the integrity and availability of complex automation offerings. The industrial security services will help assess, implement, and maintain Industrial Control System (ICS) security within operations, while enabling transformational technologies that rely on enterprise connectivity.

SERVICES INCLUDE:

- **Security Assessments:** The first step clients need to take to manage their security posture is to assess the current state of their environment. It is impossible to become completely risk free, but Rockwell will help establish a tolerable level of risk for operating environments. This includes understanding security posture within clients' software, networks, control system, policies and procedures, and employee behaviors.
- **Protect Against Threats:** After evaluating current security state and identifying risks, it is time to safeguard operations against a vast landscape of threats. The company's industrial security services team can help develop and implement an industrial cybersecurity offering to help protect ICS using a defense in depth (DiD) security approach.
- **Continuous Threat detection:** Rockwell's threat detection services can help monitor and detect these increasingly complex industrial threats.
- **Develop a Response Action Plan and Get Back to Production:** If a security event occurs, it is critical to immediately respond and address the threat(s). Building on the expertise of its industrial security services team in networks and security, Rockwell will help develop an action plan that uses proven methods to contain the incident and minimize damage.

www.rockwellautomation.com
1 440 646 3434

SCADAfence

SERVICES AVAILABLE

SCADAfence provides extended services to help asset owners deal with the digitalization of their OT networks and the shortage of in-house OT security experts.

SERVICES INCLUDE:

- **Onsite Workshops:** Customized workshops will help Operational Technology (OT) decision makers identify what level of exposure of their OT network is due to the convergence of OT networks with corporate IT networks.
- **OT Network Assessment and Gap Analysis:** Security assessments provide clients with detailed findings reports and recommendations to mitigate the issues found.
- **Incident Response and Forensics:** The company's response teams offer OT experience and security understanding, are globally distributed, and willing to offer their support at any given moment, 24/7.
- **IT/OT Alignment:** IT SecOps practices are in most cases more mature than their OT counterparts. Services include creating OT playbooks and response procedures, gap analysis, constructing an adaptive framework, and tooling.
- **OT Network Monitoring and Response as a Managed Service:** Coupling the company's capabilities with the expertise needed to respond in real-time is critical to cybersecurity incidents in OT environments.

https://www.scadafence.com/
+1-646-475-2173
info@scadafence.com

Schneider Electric

SERVICES AVAILABLE

Schneider Electric provides offerings that support the need for industrial cybersecurity protection across various business types and industries. It offers an end to end solution that includes cybersecurity consulting, design and implementation, security-specific maintenance, and cybersecurity training.

SERVICES INCLUDE:

- **Cybersecurity Consulting:** Schneider's assessment and analysis services help an organization identify the gaps between where they are now and worry-free protection.
- **Design and Implementation:** Offers multiple security layers to safeguard Schneider Electric control, safety, and Supervisory Control and Data Acquisition (SCADA) systems, which helps enable defense-in-depth (DiD) for both legacy and new systems.
- **Security-specific Maintenance:** An annual maintenance service that ensures that the client's cybersecurity protection is always current and updated.
- **Cybersecurity training:** Provides comprehensive industrial cybersecurity training.

www.se.com

SIEMENS energy

Siemens Energy helps users confront growing cyber threats with its monitoring, detection and protection offerings for critical infrastructure. The company assists customers navigate through the challenges and opportunities of strengthening industrial cyber defenses, as attackers increasingly seek to exploit complex relationships between the IT and Operational Technology (OT) environments that run energy assets in digital ecosystems.

The company places cybersecurity at the core of its clients' business by providing executives and cyber professionals with the visibility, context and control needed to identify threats to their operating environment – stopping them before execution.

SERVICES AVAILABLE

SERVICES INCLUDE:

- **AI-based technologies:** Siemens' AI-based monitoring, detection and response offerings provide energy companies and critical infrastructure operators with the visibility and context to stop attacks before they execute. With enterprise-scale offerings for small and mid-sized companies, Siemens' MRD platform comes powered by Eos.ii, which leverages artificial intelligence (AI) and machine learning methodologies to gather and model real-time energy asset intelligence.
- **Professional services:** The power of Siemens Energy's industrial cybersecurity expertise is based on human intelligence – experts who can seamlessly transition from analyzing intelligence in the digital world to acting in the physical world to stop an attack. The company's OT-trained cyber experts work with customers from the time a potential threat is detected to the time it is neutralized.
- **Industrial Cyber Integrator:** Siemens Energy's OT-native industrial cybersecurity competence provides critical technologies and offerings for industrial operating environments.

www.siemens-energy.com

ST Engineering

SERVICES AVAILABLE

ST Engineering's future-ready offering has been optimized by significant R&D investments, active engagement with research institutes, academic partners, and industry leaders.

ST's ICS security is branded as 90 percent, 9 percent, and 1 percent cybersecurity architecture. The technology is used to eliminate 90% of the known threats to reduce the noise threshold; processes are then applied to counter another 9% of the sophisticated threats and malware; and then, ST's deep expertise is utilized to eliminate the last 1% of sophisticated and unknown threats.

SERVICES INCLUDE:

- **Identification:** Develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect:** Evolve appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect:** Develop and adopt appropriate activities to identify occurrences of a cyber attack.
- **Respond:** Offer appropriate responses to a detected cyber attack.
- **Recover:** Develop and use appropriate activities to maintain plans for resilience and restore any impaired capabilities or services due to a cyber attack.

www.stengg.com
(65) 6722 1818
infosec.mktg@stengg.com

ThreatGen

SERVICES AVAILABLE

ThreatGEN services are delivered worldwide by OT cybersecurity professionals using chosen partnerships to create a holistic service offering. ThreatGEN's signature 'Red vs. Blue' training provides OT cybersecurity skills gap centers around cutting edge gamification, allowing clients to train cybersecurity skills and cybersecurity awareness, making it both practical and cost effective.

The company works with the client's team in many ways to improve their network resiliency and OT cybersecurity capabilities through a modernized approach to ThreatGEN's OT Security Services. It helps organizations identify, assess, and manage industrial cyber risk in a way that is safe, resource-effective, and makes sense to engineers, IT, and business leaders alike.

SERVICES INCLUDE:

- ICS/OT Security Manager as a Service
- ICS/OT security program and governance (advisory, creation, and maintenance)
- ICS/OT cyber risk assessment and "cyber HAZOP"
- ICS/OT standards, regulatory and compliance assessments
- ICS/OT architecture and security engineering
- IT/ICS/OT threat monitoring
- ICS/OT cyber incident response
- Cybersecurity training and awareness

https://threatgen.com

THALES

SERVICES AVAILABLE

Thales offers a comprehensive, long-term approach that helps operators implement the security policies they need to protect critical information systems. The company's Managed Security Services deliver high levels of protective outsourced offerings to defend information systems over its lifecycle.

SERVICES INCLUDE:

- **CERT:** To anticipate detection of cyberthreats, Thales offers tailored intelligence on vulnerabilities, threats and attacks of common hardware and software components in information, communications and operational systems infrastructures. Vulnerability data is graded by cross-checking and analysis from different sources. They are classified using a risk score based on the standard CVSS (Common Vulnerability Scoring System) and European Information Security Promotion Programme (EISPP) metrics, and supplemented with recommended offerings, including known patches or fixes.
- **Cybersecurity Consulting:** Thales provide cyber consulting to critical infrastructures in order to address the challenges of regulatory compliance, implementation of security from design, risk assessment and penetration testing.
- **Rapid Response Team:** Thales has a rapid response team with on-site intervention capacity, made up of multi-disciplinary specialists that aim to help private companies and public agencies respond to cyber incidents and develop their plan, in case of an attack.
- **SOC (Security Operation Center):** Thales' security experts ensure security information and event management flow in real-time from its CSOCs located around the world. The company also has the ability to provide a full range of SOC deployment and implementation models capable of adapting to the specific needs and expectations of each customer.

www.thalesgroup.com
+33 (0) 1 57 77 80 00

txOne networks

SERVICES AVAILABLE

TXOne Networks, formed out of a joint venture by Trend Micro and Moxa, offers cybersecurity offerings that protect Industrial Control Systems (ICS), and ensure reliability and safety from cyberattacks. Some of these ICS systems include legacy devices that were designed before cybersecurity became a serious concern, leaving them vulnerable to modern digital threats. In many cases, it is inconvenient to install patches and updates to treat vulnerabilities.

TXOne's work environment is made up of multiple layers that need in-depth defense, but the responsibility for the security of these combined layers is traditionally unclear. The company is seeing more and more breaches and incidents occurring in the Industrial sector, leading to significant business disruption and human lives put at risk.

SERVICES INCLUDE:

- TXOne provides offerings for tackling security weaknesses prevalent across industrial environments. The company listens to needs of both manufacturers and critical infrastructure operators to develop actionable approaches within partnering companies. This results in customized technology that goes beyond traditional security tools to help mitigate complex challenges.
- Given the ICS environments are layered and composed of a variety of equipment in different operating systems, TXOne offers both network-based and endpoint-based products to secure the OT network and mission critical devices in real-time, defense-in-depth (DiD) manner. Both IT and OT can have comprehensive visibility regarding the ICS assets, protocols, control commands, risks, and threats. The goal is to maximize ICS protection, and keep the business and operations running even when security is being breached in some way.

https://www.txone-networks.com

Verve Industrial

SERVICES AVAILABLE

Verve helps industrial cybersecurity clients ensure reliability of their ICS/OT environments. Security risks are increasing daily, as attackers leverage newly found zero-day and other vulnerabilities. The company's VIP Security services support clients through their security maturity journey.

Verve's experience in industrial controls engineering can assist in bridging the IT-OT gap that often exists in industrial security. The company's engineers translate the critical IT security needs into sensitive and unique Operational Technology (OT) environments. Its team understands what can be done safely and efficiently, instead of what cannot be done in industrial control security.

SERVICES INCLUDE:

- **Assess:** Tech-enabled vulnerability and risk assessment, Network design review, Policy and procedure review
- **Plan:** Cyber security roadmap, Strategic advisory services
- **Secure:** Network segmentation, System hardening, Backup and restore, Application whitelisting
- **Defend:** Managed compliance, Managed defense

https://www.verveindustrial.com
+1 (888) 756-3251
info@verveindustrial.com

Wipro

SERVICES AVAILABLE

Wipro's OT security is part of its Cyber Security and Risk Services (CRS) and falls under industrial IoT cybersecurity services. Clients in the oil and gas, water and power utilities, and mining and manufacturing industries use Wipro's services to manage their Operational Technology (OT) cyber risk, implement more efficient technology service operating models, and lay the foundations for accelerated and resilient industrial IoT and Industry 4.0 innovation initiatives.

Wipro conducts a gap analysis against industrial cyber standards such as NIST CSF, 800.82, CPNI, and NERC CIP. It also provides risk assessment to operations, strategic roadmaps for OT and IoT risk management, apart from developing and operationalizing critical initiatives.

SERVICES INCLUDE:

- Visibility
- Protection and security of OT environments
- OT and IoT risk assessment
- IT-OT-IOT integration
- Design, architect, and build IT-OT cyber defense centers
- Threat intelligence services
- Cyber physical offerings and services
- Industry 4.0 and IIoT initiatives
- Business continuity and disaster recovery

www.wipro.com
global.consulting@wipro.com
Phone: +91 80 2844 0011

YOKOGAWA

Yokogawa provides a centralized and standardized cybersecurity management solution to clients. The offering reduces cost by simplified, standardized, and more integrated security management, and is also compliant with international industry standards such as IEC 62443.

Yokogawa Industrial Control System (ICS) security is part of its Plant Security Services. Yokogawa ICS security services ensure plant safety and security by providing a comprehensive program which focuses on cybersecurity lifecycle management. The cybersecurity services are based on a defense-in-depth approach and best practice from global industrial cybersecurity standards.

Yokogawa supports customers in addressing cyber risk challenges through a Cybersecurity Lifecycle Management program focused on continuous improvement and a sustainable ICS security risk management framework.

SERVICES AVAILABLE

SERVICES INCLUDE:

- Cybersecurity Awareness Training: Provides a suite of cybersecurity training designed to address the different functional levels and responsibilities within the organization. The suite offers structured or tailored training programs with appropriate levels of awareness for management, experts, engineers, and users.
- Industrial Cyber Security Risk Assessment: Includes technical, operational, and business risk assessments.
- Cyber Security Policies and Procedures: Have a ready set of 36 policy and procedures templates following the best practices and the IEC-62443 standard.
- Cyber Security Business Case: Yokogawa has developed a calculation methodology as part of its business case model, which helps draft the appropriate resources and budgets plan.
- Operational Technology Architecture Design
- Plant Security Managed Services: Include asset inventory and monitoring, remote operation and engineering, small security update, help desk for incident response, and compliance and threat monitoring.

www.yokogawa.com/cybersecurity

About Takepoint

We empower our clients with actionable, incisive research to make even the toughest decisions a little easier. Collaboration is at the heart of our model and our mission is simply to deliver expert insight that has tangible value for your company.

About Industrial Cyber

Industrial Cyber is a publication dedicated to providing news and features on everything happening in Industrial Cybersecurity. It is a valuable meeting place for Industrial Cybersecurity professionals and cybersecurity experts, cybersecurity vendors and industry influencers, who learn from one another and shape the future of this dynamic and critically important market.

For more information on vendors and services providers, check out our Vendor Directory