



BUYER'S GUIDE 2024

Industrial Cybersecurity Technology, Solutions & Services

State of the Industrial Cybersecurity Market in 2024

Welcome to the sixth annual edition of the Industrial Cybersecurity Technology, Solutions, and Services Buyers' Guide. As we celebrate another year, our goal remains to clarify the complex cybersecurity landscape for industrial organizations, aiding them in enhancing their operational safety and security.

The dedication of industrial cybersecurity professionals, with their passion for safeguarding operational environments, continues to inspire. This guide offers a thorough overview of cybersecurity solutions, showcasing tools and vendors that address the unique challenges industrial entities face, and providing guidance on solution selection and priority setting.

This year, our exploration covers the dynamic nature of the market, encompassing trends in consolidation, the array of technology and solutions available, emerging market drivers, regulatory changes, and market activity. Emphasizing the

need for solutions that align with operational priorities like safety and efficiency, we highlight the industry's growth and the critical nature of cybersecurity in operational technology (OT).

This guide is aimed at bolstering the security and resilience of industrial operations, designed to strengthen the security and resilience of industrial operations. It serves as your comprehensive guide for navigating cybersecurity choices in a constantly changing industrial environment.

Despite the many challenges, a positive and prepared outlook for the future of industrial cybersecurity is achievable. By implementing effective security measures, fostering collaboration, and learning from past experiences, secure and resilient industrial systems capable of facing current and future threats can be developed and maintained. Moving forward, let's use the insights from the past as a foundation for a secure industrial future.



Jonathon Gordon

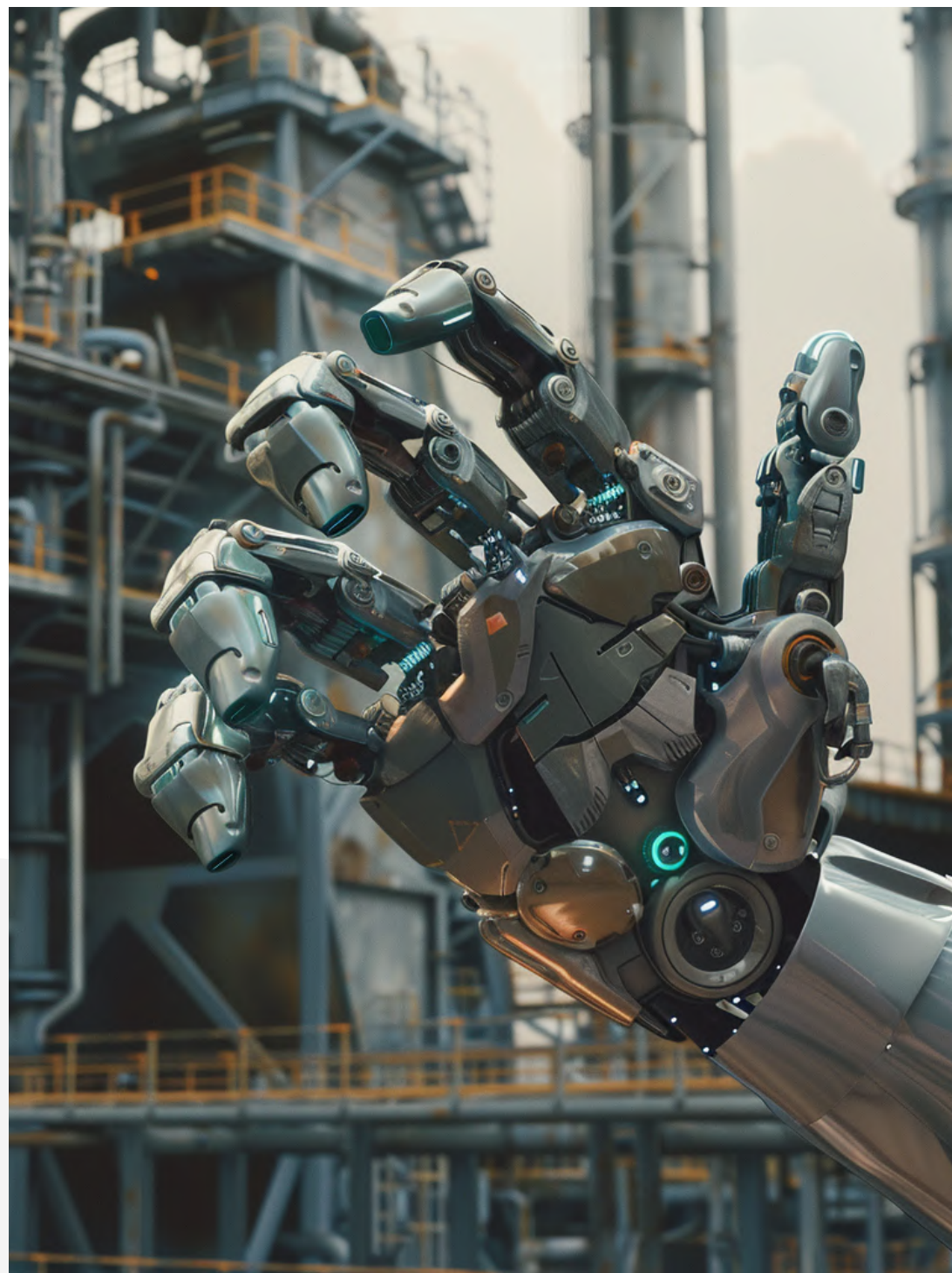
Directing Analyst
Takepoint Research



Adapting to the Evolving Threat Landscape

The landscape of industrial cybersecurity is dynamic, and constantly reshaped by emerging threats and sophisticated attacks. These range from indirect threats that compromise a company's capacity for production and service delivery to direct assaults on operational technology. Recent analyses indicate that threats, such as ransomware, are continually evolving, posing a challenge for static defense strategies.

To remain resilient, organizations must be proactive in their approach to cybersecurity, regularly updating their awareness of potential threats and refining their defensive strategies. This proactive stance involves the adoption of updated security tools, the reconfiguration of network infrastructures, and the implementation of new protocols with This proactive stance involves adopting updated security tools, techniques, and paradigms, implementing what makes sense to further reduce risk to your business.



Geopolitical tensions continue to affect industrial cybersecurity

The industrial cybersecurity sector continued to be significantly impacted by geopolitics in 2023, as global tensions and conflicts shaped cybersecurity threats and regulations. Cyberattacks targeting OT and ICS environments exploited the increasing interconnectedness with IT networks, exposing vulnerabilities for exploitation. Advanced techniques like supply chain compromises and zero-day exploits bypassed traditional security measures, prompting a shift towards resilient infrastructures, stringent protocols, and international cooperation to combat cyber threats.

Globally, cybercrime has become a major concern, as electric grids, water systems, hospitals, local governments, and critical infrastructure installations are being targeted by criminal groups and hostile nations, such as China, Russia, Iran, and North Korea.

As geopolitics increasingly influences cyber operations, the convergence of geopolitics and industrial cybersecurity underscores the importance of adopting a proactive and flexible approach to managing cybersecurity risks within a dynamic and evolving threat environment shaped by global political forces.

The escalating need for robust cybersecurity strategies and collaborative efforts to safeguard critical infrastructure is evident. Heightened geopolitical tensions between major powers have fueled increased cyber threats against critical infrastructure, manufacturing facilities, and supply chains. Geopolitical dynamics also influence regulatory frameworks and compliance requirements in the industrial cybersecurity sector.



Combating the Ransomware Scourge in Industrial Sectors

Ransomware has emerged as a prominent threat to industrial cybersecurity, with a notable increase in attacks targeting or inadvertently affecting manufacturing operations. The risk of physical repercussions resulting from indiscriminate cyber-attacks is also on the rise. Geopolitical tensions have further fueled threat activities, with regional and global kinetic events intersecting with OT cybersecurity threats.

The relentless nature of these ransomware campaigns, coupled with their continuous adaptation, emphasizes the need for enhanced protective measures within ICS/OT environments. Implementing rigorous network

segmentation and adopting persistent monitoring practices are essential for preventing malware proliferation, quarantining affected systems, and ensuring continuous operation despite attempts at disruption.

The fallout from ransomware reaches beyond operational disruptions, affecting economic stability and societal trust. Criminals targeting critical infrastructure and key sectors demand large ransoms, with incidents like the Colonial Pipeline highlighting the risk to national infrastructure.

To combat these risks, adopting cybersecurity best practices, such as incident response, employee training, and advanced threat detection, is crucial. Strengthening ICS/OT security helps safeguard critical supply chains and supports economic and public well-being.

The Living off the Land (LotL)

LotL refers to a cybersecurity attack strategy where actors exploit built-in, legitimate tools and features within an organization's network to carry out malicious activities. This approach allows attackers to blend in with normal network activity, making detection significantly more challenging. By leveraging tools such as system administration commands, scripts, and software that are already present on the system for legitimate purposes, attackers can avoid triggering alarms that are typically set off by foreign malware.

These LotL techniques represent a sophisticated threat vector that requires a multifaceted defense strategy. By prioritizing data integrity, adopting comprehensive security frameworks, carefully selecting technology partners, and maintaining vigilant monitoring and change control processes, industrial organizations can defend against these stealthy attacks. As the landscape evolves, so too must the defenses, ensuring the continued safety and reliability of critical infrastructure.

Integrating a Collaborative Security Culture Organization-Wide

Bridging the Gap: Enhancing Talent Diversity and Collaboration

The industrial cybersecurity field lacks diversity, underscoring the need for broader recruitment strategies. To ensure the future resilience and innovation of the domain, it's essential to engage people from diverse backgrounds. By adopting more inclusive hiring and development practices, organizations can bridge the skills gap while bringing varied perspectives and expertise vital for crafting effective security solutions.

Transparency and collaboration are pivotal; for example, explaining to a control room operator or plant engineer how minor procedural changes can significantly mitigate production risks can lead to greater buy-in. Understanding that engineers are adept at creating workarounds emphasizes the need for engaging them in the cybersecurity dialogue, especially when discussing cyber-physical risks.

Involving engineers who understand the operational aspects can highlight how continuous cyber risk management not only enhances security but also boosts productivity and reliability. This cooperative approach is vital for addressing the cybersecurity talent and skills gap effectively, underscoring the importance of diversity and inclusion in strengthening cybersecurity efforts across the organization.



Embracing Continuous Risk Management

The shift towards continuous cyber-physical risk management is crucial as adversaries exploit advanced technologies. Traditional one-off or annual risk assessments are outdated and ineffective. Cybersecurity strategies are shifting towards a continuous model for monitoring, vulnerability management, and risk management, including ongoing risk assessment, prioritization, breach attack simulation, and attack path analysis.

To adapt to the evolving threat landscape, continuous risk management processes must be strategic and consequence-driven, prioritizing risks based on potential impact on critical operations and assets. This strategic focus enhances the efficacy of continuous risk management, making it a powerful ally in the real-time battle against rapidly evolving cyber threats.

Adopting a cyclical process of continuous assessment and adaptation, with a feedback loop from security incidents and drills, allows organizations to evolve their security measures dynamically, ensuring effective cybersecurity practices.

Balancing Act:

Generative AI in Industrial Cybersecurity

Generative AI in industrial cybersecurity offers a blend of advantages and challenges that cannot be ignored. AI-powered systems enhance threat detection and prevention by learning from past incidents, allowing for real-time identification of suspicious activities. This proactive approach gives manufacturers the upper hand against evolving cyber threats, promising a more secure operational environment.

However, generative AI's ability to produce content rather than just analyze data brings its own set of risks. While it can optimize processes and increase efficiency within organizations, it also enables attackers to launch sophisticated and automated cyberattacks. Generative AI can streamline the stages of the cyber kill chain, making attacks faster and more covert. This accessibility to advanced tools increases the threat level, especially for industries still leaning on manual defenses.

As generative AI technologies become more accessible, the potential for AI-powered threats escalates. Industrial sectors must adopt a cautious yet proactive stance, leveraging AI's potential to improve security while being aware of its ability to empower adversaries. This nuanced approach is essential for navigating the complex landscape of generative AI in industrial cybersecurity.

The Rise of the Industrial Chief Information Security Officer (CISO)

The CISO within industrial sectors is emerging as a pivotal figure in managing cyber risk from end to end. This trend, observed through client interactions and advisory calls, highlights the expanding scope of the CISO's responsibilities. As the primary liaison for cybersecurity matters, including the integration of cyber-physical systems, the role of the Industrial CISO is undergoing a significant transformation.

Today's Industrial CISO transcends traditional boundaries, acting as a conduit between executive management's strategic objectives and their operational execution. This role demands the translation of high-level cybersecurity frameworks into tangible practices and protocols, bridging the gap between IT and OT teams.

Soft skills, such as the ability to garner executive buy-in and foster cross-departmental collaboration, are increasingly vital. The Industrial CISO's challenge lies in articulating and harmonizing the organization's risk appetite with its technological initiatives, ensuring a unified approach to risk that enhances overall resilience. This shift marks a departure from isolated departmental efforts, encouraging a holistic strategy for cybersecurity.

At its core, the Industrial CISO's mission is to facilitate business objectives—fostering innovation and productivity while ensuring these advancements are secure and sustainable. This role is not just about safeguarding assets but enabling the organization to operate more efficiently and reliably within a secure framework. Thus, the evolution

of the Industrial CISO epitomizes OT cyber transformation as a catalyst for business growth, emphasizing safety and reliability in the digital age.

Regulations, Standards and Compliance Update

The industrial cybersecurity landscape is rapidly evolving, driven by the increasing complexity and connectivity of industrial control systems, along with the rising threat of cyberattacks on critical infrastructure. Regulatory bodies worldwide are responding by developing and updating standards and regulations aimed at enhancing the security and resilience of these vital systems. What follows is a concise overview of the principal regulations, frameworks industry standards, and compliance mandates currently influencing the industrial cybersecurity domain – however, the summary below serves as a sample and is not intended to be exhaustive.

Regulations Developing Across Industries and Regions

- 01 NERC CIP** focuses on protecting North America's bulk power system, requiring cybersecurity protections for critical cyber assets.
- 02 The U.S. HHS FDA** has introduced cybersecurity requirements for medical devices, emphasizing the need for a software bill of materials (SBOM) and vulnerability disclosure.
- 03 CMMC** by the U.S. Department of Defense aims to standardize cybersecurity preparedness across the defense industrial base.
- 04 CFATS** targets high-risk chemical facilities, mandating risk assessments and the implementation of security measures. Though, as of July 28, 2023, Congress has allowed the statutory authority for the CFATS program to expire.
- 05 FISMA** applies to U.S. federal agencies, requiring the development of information security programs.
- 06 TSA Security Directives** for pipelines and rail enhance the security protocols for these critical infrastructures.
- 07 The NIS2 Directive** updates EU critical infrastructure regulation, broadening its scope and introducing comprehensive cybersecurity requirements.
- 08 The Cyber Resilience Act (CRA)** sets EU-wide cybersecurity standards for digital products, with provisions for third-party assessments.
- 09 Machinery Regulation (EU) 2023/1230** incorporates cybersecurity into machinery design and construction requirements.
- 10 Singapore's CCoP 2.0** updates the standards for Critical Information Infrastructure regulation.
- 11 Australia's Security of Critical Infrastructure (SOCI) Act** addresses threats to critical infrastructure, emphasizing protection measures.





Industry Standards and Frameworks

- 01** IEC 62443 is becoming the global benchmark for securing industrial control systems (ICS) across various sectors.
- 02** MITRE ATT&CK ICS Framework serves as a knowledge base for understanding tactics and techniques used by cyber threat actors.
- 03** CIS Critical Security Controls provide actionable guidance for protecting against cyber threats.
- 04** NIST SP 800-171 Revision 3 impacts businesses working with the federal government, emphasizing cybersecurity controls.
- 05** NISTIR 8374 (Draft) guides on managing ransomware attack risks.
- 06** NIST 800-53 defines security controls for U.S. federal information systems, supporting critical infrastructure protection.
- 07** NIST 800-82 offers a roadmap for securing industrial control systems.
- 08** API Pipeline Standards focus on managing cyber risks in industrial automation and control environments.
- 09** Guidelines by the International Maritime Organization aim at enhancing maritime cyber risk management.
- 10** The Australian ASD Essential Eight Maturity Model provides strategies for mitigating cybersecurity incidents, relevant to industrial control systems.
- 11** The Canadian Cyber Security Framework offers cybersecurity best practices for critical infrastructure sectors.



Europe 2024 Spotlight: Analyzing the NIS2 Directive and Cyber Resilience Act

The NIS2 Directive

The NIS2 Directive marks a significant evolution in European Union cybersecurity policy, introducing extensive changes that could have profound implications across various industries and regions. Here's a summary of its key points and potential impacts:

Key Features of the NIS2 Directive



Expanded Scope

The directive broadens its applicability beyond critical infrastructure to include a wider array of digital service providers and SMEs, acknowledging the interconnectedness of cybersecurity across all sectors in a digital ecosystem.



Harmonization and Clarity

It seeks to standardize cybersecurity requirements across the EU, aiming to eliminate the fragmentation seen previously and provide clear, predictable standards for cross-border operations.



Proactive Risk Management

A shift towards anticipatory risk management is at the heart of the NIS2 Directive, compelling organizations to implement risk management measures and report incidents promptly, promoting a culture of constant vigilance and improvement in cybersecurity practices.



Dynamic Response to Threats

The directive is adaptable and designed to evolve with the changing cyber threat landscape, ensuring that regulatory frameworks remain relevant and effective.



Collaborative Effort

It emphasizes the importance of information sharing and cooperation among national authorities, regulatory bodies, and the private sector, aiming to foster a united and effective approach to tackling cyber threats.

Implications for the ICS/OT Sectors

For sectors involving Industrial Control Systems (ICS) and Operational Technology (OT), such as energy, transportation, and manufacturing, the NIS2 Directive is particularly consequential. These sectors are crucial for societal and economic functions, and the Directive recognizes the unique vulnerabilities and the potentially

catastrophic consequences of cybersecurity incidents within these environments. By establishing rigorous cybersecurity standards and promoting best practices, the NIS2 Directive aims to strengthen the defenses of these critical sectors against a wide range of cyber threats.

Potential Impact and Why It Matters



Strategic Importance

The NIS2 Directive represents a crucial step in enhancing the cybersecurity defenses of the European Union, setting a precedent that could influence global cybersecurity standards.



Investment in Cybersecurity

Entities affected by the directive will need to allocate significant resources towards upgrading their cybersecurity infrastructure, developing a skilled workforce, and ensuring compliance with the new regulations.



Enhanced Cyber Resilience

The directive's focus on risk management and proactive cybersecurity measures is expected to significantly enhance the cyber resilience of entities across the EU, reducing the risk of major cyber incidents and their potential impacts.



Global Benchmark

By setting a high standard for cybersecurity, the NIS2 Directive could serve as a benchmark for other regions, encouraging a worldwide uplift in cybersecurity practices, particularly in sectors that are integral to the global economy and infrastructure.

The Cyber Resilience Act (CRA)

The Cyber Resilience Act (CRA) introduces a pivotal shift in EU cybersecurity standards by integrating security requirements into the CE marking process for products. The CE marking signifies that products with digital components comply with the CRA, allowing them to circulate freely within the internal market. It indicates that the manufacturer assumes responsibility for ensuring the product meets all relevant European health, safety, performance, and environmental standards. This development marks a significant step towards harmonizing cybersecurity regulations across the EU, making security a fundamental component of product certification.

Underpinning the CRA is the adoption of harmonized European Norms (hENs), developed by standardization bodies like CEN, Cenelec, and ETSI. These norms are essential because they will outline the specific cybersecurity criteria that products must meet to earn the CE mark, indicating compliance with EU directives. This streamlined approach aims to eliminate regulatory fragmentation, facilitating easier access to the EU market for product manufacturers.

The CRA reflects a balanced approach to regulation, emphasizing the need for essential, risk-based security measures while allowing manufacturers the freedom to choose how to meet these requirements. This strategy builds on the EU's extensive regulatory experience, aiming to enhance product security without stifling innovation.

The implications of the CRA are significant, not only for unifying cybersecurity standards across the EU but also

for potentially influencing global regulatory practices. By embedding cybersecurity into the CE marking, the CRA sets a new standard for product safety and security, aiming to create a more secure digital environment in the EU and beyond.



Supply Chain Security in Industrial Settings

The evolving focus on supply chain security for industrial and OT cybersecurity highlights the need for a comprehensive, proactive approach. By prioritizing vendor risk management, software integrity, and secure-by-design principles, organizations can enhance their resilience against the complex array of cyber threats facing critical infrastructure today.

The importance of elements like Software Bill of Materials (SBOMs), Hardware Bill of Materials (HBOMs), Vulnerability Exploitability eXchange (VEX), and Cybersecurity Advisory Framework (CSAF) is growing. These tools aid in transparently managing and communicating the components and vulnerabilities within software and hardware, enhancing the security posture of OT environments.



Secure by Design/Default

The industry is shifting towards integrating cybersecurity into product design and development processes, reducing the security burden on end-users and transferring responsibility to manufacturers. This involves creating a security decision base, modeling systems with cybersecurity in mind, and making informed security decisions throughout the design process. Transparency and accountability are also essential, requiring an executive-level commitment.

Organizations can build resilience by leveraging a controls framework and applying it consistently across IT and OT. Achieving secure-by-design and secure-by-default

products requires a reevaluation of legacy systems, budget allocation for security improvements, and a collaborative approach between vendors and operators.

Developing effect of CIE and CCE approaches

Both cyber-informed engineering (CIE) and consequence-driven cyber-informed engineering (CCE) are essential in today's interconnected and digital world to ensure the security and resilience of critical systems and infrastructure against evolving cyber threats. By embedding cybersecurity principles into the engineering process and aligning security measures with potential consequences, organizations can build robust and secure systems that can withstand cyber attacks and protect sensitive information effectively.

These principles are universally applicable across various engineering domains and serve as foundational pillars that demonstrate consistent effectiveness across critical infrastructure sectors. Moreover, the practical implementation of these methodologies goes beyond theoretical limitations, offering comprehensive guidance for identifying and mitigating vulnerabilities within critical infrastructure systems.

The Emerging Role of Zero Trust for OT

Zero Trust for OT represents a paradigm shift in security strategies, essential for safeguarding critical infrastructure.

Implementing Zero Trust in OT involves key strategies like enforcing least privilege access, and prioritizing security and safety without compromising productivity.

The drive towards Zero Trust in OT is largely motivated by the need for modernization and regulatory compliance, with a notable emphasis on managing the risks introduced by merging OT and IT infrastructures through digital transformation. The model is increasingly viewed as a vital approach to mitigate emerging risks, though the urgency and specific motivations vary across sectors.

The industrial cybersecurity community is focusing on identifying optimal use cases for zero trust to enhance security while maintaining productivity. Notably, remote access for employees and third-party contractors has emerged as a prime application, offering clear benefits in security and operational effectiveness.

Current views on Zero Trust for OT and its deployment can vary widely, highlighting the importance of a cohesive and cooperative strategy to integrate zero trust principles with cyber-physical risk management. This collaborative effort is crucial to ensure that every stakeholder plays a part in achieving the collective aims of safeguarding productivity, reliability, and security securely.

Resilience: Respond, Recover and Learn

There's an increasing emphasis on enhancing system resilience, highlighting the importance of systems withstanding and recovering swiftly from disruptions. Key initiatives include developing comprehensive

disaster recovery and business continuity strategies, complemented by routine data backups. These efforts are critical, not only for the immediate response to incidents but also for the swift recovery that preserves business integrity and customer trust.

In the industry, there's a notable focus on the 'Identify, Detect, and Protect' components of the NIST Cybersecurity Framework, yet the 'Respond and Recover' aspects often receive less attention and investment. This oversight underscores the need for a more balanced approach to cybersecurity, one that equally emphasizes all facets of resilience.

The 2023 cybersecurity outlook underscores a shift towards proactive protection of ICS. Core tactics involve thorough infrastructure assessment, effective network segmentation, diligent communication monitoring, and continuous enhancements to safeguard against critical infrastructure threats. This proactive stance extends beyond merely defending against threats to effectively responding to and recovering from them when they occur.

As we advance, transitioning from reactive to proactive cybersecurity practices, cultivating security awareness, and boosting collaborative efforts are crucial. A comprehensive approach to cybersecurity includes robust response and recovery plans, significantly strengthens defenses against cyber threats.

Facing challenges head-on, a proactive, well-prepared stance on ICS/OT cybersecurity is within reach. By implementing stringent security measures, investing in response and recovery capabilities, and drawing on past learnings, it's possible to develop resilient industrial

systems ready for future challenges. This journey towards enhanced cybersecurity requires persistent effort and cooperation, emphasizing the need for a balanced focus across all elements of the NIST Framework. Using past experiences as a solid foundation, we can build a more secure and resilient industrial future.

Focus on Resilience and Operational Continuity

Increasing threats and attacks against OT/ICS environments have led to a shift towards focusing on resilience over operational continuity is crucial. Resilience emphasizes the ability to adapt and recover quickly from disruptions, rather than just maintaining operations. This approach acknowledges the increasing complexity and frequency of cyber threats in critical infrastructure systems. By prioritizing resilience, organizations can proactively identify vulnerabilities, implement robust security measures, and develop response plans to mitigate risks effectively.

Highlighting resilience promotes a mindset of readiness and ongoing enhancement and guarantees the enduring viability and safeguarding of critical assets amidst challenging threats and attacks across OT/ICS environments.

Operational resilience is now a vital requirement rather than a choice in today's swiftly changing operational landscape. This crucial element dictates the ability of organizations to recover from disturbances while upholding essential operations. Operational resilience aids companies in mitigating risks and maintaining operations seamlessly even in unexpected situations. It acts as a foundation that sustains operational efficiency regardless of the obstacles encountered.

Increasing Vertical Specialization

The movement towards vertical specialization marks a pivotal transition in tailoring operational environments to meet the distinct demands of each industrial sector. From defense manufacturing to healthcare, and energy to transportation and logistics, each field presents unique challenges and requirements that

necessitate customized solutions. This trend is fueled by the necessity for asset owners and operators to judiciously manage their limited resources, such as equipment, workforce, or finances, amidst the constantly shifting terrain of cybersecurity threats.

Particularly in sectors that are vital to national security and the fabric of daily life, the drive toward specialization is becoming increasingly visible:

01

In Defense Manufacturing,

the implications of cyber vulnerabilities reach into the realms of national security.

03

The Health and Medical

sector emphasizes the utmost importance of patient safety and the protection of sensitive data.

02

Power and Energy

sector acts as the backbone for the functionality of a broad spectrum of other sectors.

04

Transportation and Logistics,

with its extensive sub-categories like automotive, aviation, maritime, and rail, each brings its own operational intricacies and security predicaments.

As vendors and service providers increasingly tailor their offerings to meet the unique requirements of critical industries, the field of industrial cybersecurity is advancing toward a more refined landscape. This evolution is marked by solutions that are not only highly effective but also precisely aligned with the specific operational nuances of each sector. This move towards vertical specialization not only strengthens the security defenses of these essential industries but also drives innovation and enhances the effectiveness of cybersecurity strategies.



Business Considerations

Roles, Responsibilities, and Industrial Incident Handling

In the face of evolving cybersecurity threats, it's imperative for companies to integrate robust industrial cybersecurity practices within their operational framework. A collaborative, multi-faceted approach involving all stakeholders is essential for safeguarding industrial ecosystems. Precise definitions of roles and responsibilities, especially during incidents, significantly mitigate the impact. Tools like the RACI (Responsible, Accountable, Consulted, and Informed) model enhance clarity and ensure effective stakeholder engagement in incident management, which should blend proactive strategies with reactive measures for comprehensive risk mitigation.

Governance, Compliance, and Information Exchange

Adherence to governance and compliance standards, such as those set by NIST, IEC, and MITRE, is crucial despite the traditionally low priority given to industrial cybersecurity governance. Aligning chosen frameworks with company policies and conducting thorough risk assessments prepare organizations better for potential incidents. Furthermore, the importance of cross-organizational and cross-border information sharing in strengthening cybersecurity defenses cannot be overstated.

OT Cybersecurity Incident Response

Crafting a detailed incident response plan is critical for quickly pinpointing issues and efficiently restoring operations. Such plans must integrate proactive measures, including planning and prevention, with reactive solutions for fast incident detection and resolution. A rapid and efficient response to security breaches is crucial to mitigate downtime, data loss, and reputational impact. With the growing frequency and severity of

cyberattacks, the urgency to establish robust incident response protocols and embrace secure access and monitoring technologies has never been higher. Every incident presents a unique challenge, but also an opportunity to enhance future preparedness.

The Incident Command System for Industrial Control Systems (ICS4ICS) represents a developing approach designed to enhance the handling of cybersecurity incidents within industrial environments. It incorporates protocols from FEMA's Incident Command System to ensure standardized responses. With a track record of successful application in a wide array of emergencies, from natural disasters to industrial accidents, across both the public and private sectors for over thirty years, the reliability of the ICS is well-established. The adoption of the ICS4ICS framework into OT cyber incident management markedly bolsters cybersecurity measures and operational resilience.

Rethinking Risk Management Strategies

As the landscape of industrial cyber risk evolves, there's a pressing need for organizations to adopt a more nuanced approach to risk management. This entails a combined strategy that leverages both a strategic, top-down view of business value and a detailed, bottom-up analysis of assets, vulnerabilities, and exposures. Such a comprehensive methodology is essential to pinpoint the "value at risk" effectively, providing robust protection against cyber threats.

Moreover, the shift towards continuous risk management marks a critical change, moving from sporadic risk evaluations to an ongoing, adaptive process. This continuous vigilance allows for real-time adjustments in response to emerging threats, vulnerabilities, and shifts in the business landscape, ensuring that cybersecurity efforts are consistently aligned with business

objectives, thereby enhancing resilience and protecting business value. Additionally, the hesitancy, reluctance, and apparent immaturity of industrial cyber insurance underwriters highlight the importance of organizations strengthening their internal risk management capabilities.

Technology Concerns

Enhancing Network Segmentation

Effective network segmentation is paramount in OT/ ICS for securing business-critical processes. Despite its importance, many industrial enterprises fall short of adequately segmenting their networks, often relying on IT-specific firewalls that do little to strengthen the OT security posture. A targeted approach, such as consequence-based analysis and identifying 'crown jewels,' is crucial for effective segmentation and prioritizing asset protection.

Strengthening System Hardening

System hardening is essential for enhancing operational resilience and cybersecurity. This involves securing interfaces that link control systems to external networks, connections within the ICS network, and wireless access points. Despite the necessity, many IT/OT systems lack sufficient hardening and inadequate access management often leads to compromised security controls.

Improving Industrial Identity Management

A significant gap in many industrial setups is the absence of robust authentication and auditing mechanisms, especially for remote and third-party access. Real-time monitoring to catch abnormal activities and stronger log management are needed for better threat detection and response. Adopting a zero-trust

framework, which requires strict verification for every access attempt, can significantly improve security for both internal and external users, driving a proactive stance in cybersecurity practices.

Addressing Vulnerabilities in Product Security and Supply Chain

The launch of industrial products with unaddressed critical vulnerabilities underscores the need for a security-by-design approach, incorporating Software Bill of Materials (SBOMs) and Vulnerability Exploitability Exchange (VEX). Although options exist, aligning these practices with industry standards requires further effort.

Securing the Industrial Cloud

Cloud security is increasingly critical, especially for sectors like manufacturing and building management systems, where data is frequently moved to cloud-based analytics. Ensuring robust cloud security measures is fundamental to protecting sensitive data.

Applying Zero-Trust Principles

Implementing a zero-trust model in industrial environments, which entails no inherent trust and demands verification for every access request, offers a promising route to enhance cybersecurity. This model advocates for continuous verification, stringent access control, and risk-aware decision-making. However, given the model's relative novelty in industrial contexts, a thorough evaluation is necessary before implementation.

Industrial Cybersecurity Technology & Solutions

The categorization framework in this guide is designed to enable Industrial Enterprises to identify, evaluate and determine what type of technology and solution may be beneficial to their organization. The categories are designed to provide an elementary assessment of solutions, it is not an exhaustive checklist. Furthermore, the framework is not sequential. Certain solutions may be required at different points in the journey, depending on the starting point and the cyber maturity of the organization.



Asset - Discovery and Vulnerability Management

- Automated Network Inventory
- Asset Intelligence - IT/OT/IloT
- Network Asset Discovery and Mapping



Cyber-Physical Security and Operational Systems Health

- Data Manipulation and Data Injection
- OT/ICS Asset-Signal Integrity and OT Anomaly Detection
- Predictive Maintenance



Identity and Access Management (IAM)

- Identity Governance Across Assets and Users
- MFA, Passwordless, and SSO
- Policy and Role Management
- Privileged Access Management (PAM)



Industrial IoT (IIoT) Device Security

- Continuous Vulnerability Management
- Embedded IoT Agent-IIoT Inventory
- Hardware/Software
- Secure and Validate Device Updates



Network Security Monitoring and Anomaly detection

- Monitor, Alert, and Report
- Network Anomaly and Threat Detection
- Attack Path Management and Breach Attack Simulation (BAS)



Operational IT/OT Endpoint Security and Patch Management

- Industrial IT Endpoint Protection, EDR/xDR/EPP
- Device-level Zero-Trust
- Firmware, Configuration, and Patch Management
- OT Endpoint



Perimeter Security, Segmentation, and Zone Enforcement

- Data Diode/Unidirectional Gateways
- Industrial Firewalls
- Soft/Virtual/Micro-Segmentation
- USB/Removable Media Sanitization



Product, Software, and Supply Chain Security

- Monitoring and Remediation
- Product Security and SDLC
- SBOM/HBOM Analysis, VEX, File Integrity
- Third-party Risk Management
- Vulnerability Management



Risk Management, Governance, and Compliance

- Exposure Reduction and Vulnerability Prioritization
- Industrial Threat Intelligence
- Risk Exposure Analysis and Reporting
- Risk Management and Mitigation




Secure Remote Access

- Access Control: ABAC/DAC/MAC/BAC
- Audit and Compliance: Session Logging/Recording/Termination
- Jump box, VPN Access, Converged SRA platform Privileged SRA, Zero-Trust, and Identity



Social Engineering and Phishing Prevention

- Inbox Cyber Security and Phishing Deterrence
- Training Platforms, Behavioral Modification/Interactive Training, CBT/Video
- Network Prevention/Enforcement
- Secure Email Gateways



Asset – Discovery and Vulnerability Management

Asset discovery and vulnerability management play a crucial role in industrial cybersecurity by enhancing visibility into the components of industrial control systems (ICS). This process involves cataloging all devices within an ICS, including their specifications and operational data, which is essential for identifying vulnerabilities and improving operational reliability. A detailed and accurate asset inventory is critical for enabling targeted security measures, efficient incident response, and minimizing disruptions during cybersecurity incidents.

Given the dynamic nature of industrial environments, the integration of automated discovery and management tools is vital for keeping asset registries current, thereby supporting both operational management and cybersecurity. These tools and platforms, which focus on refining asset registers for various purposes, must balance the need for detail and accuracy with cost-efficiency to effectively protect critical assets and maintain the security and efficiency of industrial operations.

Automated Network Inventory

Automated network inventory helps to automatically discover, identify, and catalog all network-connected assets and associated attributes. It involves using specialized tools or software to scan the OT network and collect relevant information about devices, systems, and configurations. By implementing automated network inventory processes, organizations can improve their understanding of the OT network infrastructure, enhance


security management practices, and streamline asset-related activities.

Asset Intelligence – IT/OT/IloT

Asset Intelligence covers the process of gathering, analyzing, and leveraging information about assets in various domains, including IT, OT, and IloT. It involves understanding and managing the characteristics, performance, dependencies, and vulnerabilities of assets to make informed decisions and optimize use.

Network Asset Discovery and Mapping

Network Asset Discovery and Mapping work on gaining visibility and maintaining an accurate inventory of all the assets present in the OT environment. This information is critical for effective network management, security, maintenance, and compliance purposes.



Cyber-Physical Security and Operational Systems Health

Cyber-physical security involves safeguarding the convergence of the physical and digital worlds, where physical systems are increasingly connected to digital networks. This integration of the physical and digital worlds makes them more vulnerable to cyber attacks, which can lead to significant consequences, such as disruption of services, equipment damage, and safety risks. To ensure cyber-physical security, organizations need to implement robust cybersecurity measures, such as implementing firewalls, intrusion detection and prevention systems, encryption, access controls, and incident response plans.

Operational systems health works on ensuring the optimal performance and reliability of ICS and other operational infrastructure. It involves monitoring the health of these systems, early problem detection, and taking corrective action before they cause disruptions or failures.

Organizations need to implement automated monitoring and reporting systems that can continuously monitor the performance of critical infrastructure to ensure operational systems' health. These systems can help alert operators of problems in real-time, enabling them to take corrective action before they cause significant damage or disruption.

Overall, cyber-physical security and operational systems health are critical aspects of protecting critical infrastructure and ensuring safe and reliable operations. By implementing robust cybersecurity measures and continuously monitoring and maintaining the health of operational systems, organizations can maintain the integrity of systems, mitigate risks, and ensure safe and reliable operations.

Data Manipulation and Data Injection

OT data manipulation and data injection attacks are becoming more common as more industrial facilities and critical infrastructure become connected to the internet and other digital networks. These attacks can cause significant damage and disruption, leading to safety hazards, equipment damage, and environmental harm. To mitigate these risks, organizations need to implement robust cybersecurity measures, to protect OT systems from cyber threats.

OT/ICS Asset-Signal Integrity and OT Anomaly Detection

Effective OT/ICS asset signal integrity and anomaly

detection are critical components of modern industrial cybersecurity measures, helping to protect against attacks like ransomware, malware, and other malicious activities that could disrupt critical infrastructure and cause widespread damage. By leveraging advanced technologies like machine learning and artificial intelligence, organizations can more effectively identify potential threats and take proactive steps to mitigate risks before they result in significant damage or operational disruptions.

Predictive Maintenance

OT predictive maintenance helps organizations prioritize and schedule maintenance by providing real-time monitoring and alerting businesses to impending failures. However, one of the biggest obstacles preventing plant operators from implementing a successful predictive maintenance program is the integration of current OT infrastructure into contemporary IT systems. Most manufacturers frequently use third-party vendors because integrating systems costs money and is difficult to manage. As the data lacks the necessary context to generate insights and prompt action for OT systems, many people are unable to understand it.



Identity and Access Management (IAM)

OT IAM covers managing identities and access to critical ICS and other OT infrastructure, providing necessary access and privileges to carry out roles while ensuring that unauthorized individuals are prevented from accessing critical systems. It is used to ensure that only authorized

users have access to critical systems and data, alongside assisting in mitigating the risk of malicious insiders or cybercriminals accessing critical systems and data, which could negatively impact operations.

OT IAM involves various processes and technologies, including identity authentication that verifies the identity of users attempting to gain access to critical systems; role-based access control that assigns access permissions and privileges based on user roles and responsibilities; and credential management that manages users' digital identities and credentials to ensure validity and prevent unauthorized access.

Identity Governance Across Assets and Users

Identity Governance lies at the center of organizational operations, as it enables and secures digital identities across systems and infrastructure and for all users, applications, and data. It allows businesses to provide automated access to an ever-growing number of technology assets while managing potential security and compliance risks. With identity as a foundation and making appropriate access decisions, organizations adopt the benefits of hyper-connectivity while ensuring that only the right people have access at the right times.

MFA, Passwordless, and SSO

These solutions are vital tools used for securing access to operational environments, which can be implemented through a host of technologies, such as smart cards, tokens, mobile devices, and biometric sensors. They can also be integrated with existing authentication systems to provide an additional layer of security. Overall, these solutions help to minimize the risk of unauthorized access and security breaches and ensure the safety and reliability of industrial

operations.

Policy and Role Management

Policy management involves developing, documenting, communicating, and enforcing these policies to ensure they are followed consistently, while role management involves assigning specific responsibilities or duties to individuals or groups based on job functions, skills, and access privileges. By implementing and enforcing well-defined policies and roles, organizations can reduce the risks of cyber threats, data breaches, and non-compliance with industry regulations.

Privileged Access Management (PAM)

PAM in industrial environments refers to the practice of managing and controlling access rights for privileged users who have administrative access to critical systems, applications, and data. The approach is crucial in industrial environments to protect OT assets, prevent unauthorized access, and reduce the risk of cyber-attacks and industrial espionage. It also protects against insider threats and external cyber-attacks, prevents data loss or theft, and ensures compliance with industry standards and regulations.



Industrial IoT (IIoT) Device Security

Continuous Vulnerability Management

Continuous vulnerability management is a critical component of maintaining the security and resilience of OT environments, as it helps ensure that any vulnerabilities are identified and remediated before being exploited by

attackers. Constant assessment of the risk posture of the OT environment enables organizations to remain vigilant and resilient to potential threats across organizational devices, systems, and applications. It also focuses on what must work together seamlessly to bring about safe and reliable operations. However, this complexity also creates security vulnerabilities that can be exploited by cyber attackers.

Embedded IoT Agent-IIoT Inventory

EmbeddedIoTagent-IIoTInventoryacrossOTenvironments covers software integrated into IIoT (Industrial Internet of Things) systems that manage inventory and supply chain processes within OT environments. These elements play a crucial role in collecting and transmitting data to a centralized platform for real-time tracking and analysis of inventory and supply chain processes. They also enable businesses to stay ahead of the competition by optimizing inventory and supply chain processes, reducing costs, and improving productivity.

Hardware/Software

OT hardware and software detect or cause a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise. Periodic hardware and software scans must be executed to detect any unauthorized hardware or software changes and identify any unauthorized hardware and non-essential software applications installed within the infrastructure.

Secure and Validate Device Updates

Secure and validated updates reduce the risk of unauthorized access, system vulnerabilities, and potential disruptions, safeguarding critical infrastructure and ICS

environments. It works on securely deploying and verifying updates or patches to these OT devices, to maintain the reliability, availability, and security of OT infrastructure. It calls for appropriate authentication and authorization; updates must be delivered using secure channels; integrity verification; and appropriate monitoring and anomaly detection.



Network Security Monitoring and Anomaly detection

Essential for safeguarding industrial systems, effective network monitoring, and threat detection enable the early spotting of potential threats, ensure regulatory compliance, and streamline network management. This requires a blend of automated tools and human expertise to address the unique challenges of segmented networks.

Continuous monitoring of network traffic and activities helps maintain system availability and identify performance issues or anomalies. Meanwhile, threat detection focuses on monitoring for indicators of compromise, suspicious behaviors, or anomalies that could signal security incidents or unauthorized access, ensuring the security and reliability of OT environments.

Monitor, Alert, and Report

Continuous surveillance of critical systems, generation of alerts for potential issues, and creation of reports provide insights into operational status and security posture in OT environments. Effective monitoring, alerting, and reporting enable proactive identification, timely response to incidents, and data-driven decisions. Key features of network security monitoring include compliance

monitoring, behavior analysis, and network flow security analysis. Advanced threat detection and the integration of automated tools and human expertise enhance response to security incidents, maintaining industrial operations' integrity and safety.

Network Anomaly and Threat Detection

Network Anomaly and Threat Detection play a crucial role in safeguarding OT systems by identifying and addressing potential threats, such as cyberattacks and operational errors. This involves monitoring for unusual activities and analyzing behavior to spot deviations from the norm, thereby identifying potential risks. Key to this process is exception reporting, which notifies administrators of policy breaches or odd behaviors, and the differentiation between routine changes and potential sabotage through operational monitoring.

Additionally, correlating IT and OT system events, with tools like SIEM, is essential for detecting unauthorized access or unexpected shifts in operations. This cohesive strategy improves the management of security risks, fortifying defenses against cyber threats.

Attack Path Management and Breach Attack Simulation (BAS)

In OT environments, attack path management works on identifying, analyzing, and managing potential attack paths that malicious actors could exploit to compromise critical systems or infrastructure. It involves understanding the interconnectedness of various components within the OT network, assessing vulnerabilities, and implementing measures to mitigate the risks associated with these attack paths.



Operational IT/OT Endpoint Security and Patch Management

Operational IT/OT endpoint security and patch management is crucial for maintaining the security of critical infrastructure and industrial processes. It involves regular monitoring, assessment, and adaptation to address emerging threats and vulnerabilities. Measures include access controls, antivirus and anti-malware solutions, application whitelisting, and network segmentation.

Regular assessments help identify vulnerabilities in endpoint devices, and appropriate patches and updates are applied promptly. Organizations must review and manage endpoint device configurations to align with security policies and industry best practices, and implement endpoint security and patch management practices that align with applicable regulations and standards.

Industrial IT Endpoint Protection, EDR/xDR/EPP

Industrial IT Endpoint Protection is vital for safeguarding critical infrastructure, ensuring the availability and integrity of industrial processes, and mitigating the risks associated with cyber threats in industrial environments. By implementing comprehensive security measures and regularly updating endpoint protections, organizations can enhance the resilience of industrial IT infrastructure.

Device-level Zero-Trust

Implementing device-level zero-trust across OT endpoints requires a combination of technology, processes, and security controls tailored to the unique characteristics of OT environments. It helps organizations enhance security,

protect critical infrastructure, and ensure the integrity and availability of operational processes. Device-level zero-trust will have a bearing on authentication and authorization, continuous authentication, least privilege access, micro-segmentation, device integrity and health monitoring, device behavior analytics, and secure remote access.

Firmware, Configuration, and Patch Management

Firmware, configuration, and patch management are critical for maintaining security, reliability, and accessibility across operational IT/OT endpoints, as they manage and maintain the firmware, configurations, and software patches of endpoint devices. These practices focus on ensuring that endpoints have up-to-date firmware, secure configurations, and the latest patches to address vulnerabilities.

OT Endpoint

Securing and managing OT endpoints is critical to offering the availability, reliability, and safety of industrial processes. Effective measures must be implemented to protect OT endpoints from cyber threats while maintaining the integrity of critical infrastructure.



Perimeter Security, Segmentation, and Zone Enforcement

Perimeter security, segmentation, and zone enforcement are crucial for protecting critical infrastructure and preventing unauthorized access. These measures establish secure boundaries, control access, and limit the impact of security incidents within OT networks. Firewalls,

IDS/IPS solutions, and VPNs are essential for enforcing security boundaries.

Segmentation involves dividing the OT network into logical segments or VLANs based on operational needs and security requirements. Physical isolation of sensitive or critical systems from less vulnerable ones is also possible. Zones, such as DMZs, separate external-facing systems from internal OT networks. Perimeter Access Control uses strict access controls to regulate and monitor access to OT environments from external networks. Access Control Lists can be used to define and enforce access policies and restrictions at the network level.

Data Diode/Unidirectional Gateways

Data diodes provide an additional layer of protection for sensitive networks, enabling controlled and secure data transfer in environments where data leakage or unauthorized access is a significant concern. They enable data to flow in one direction only, typically from a high-security network (source) to a lower-security network (destination), while preventing any data or information from flowing back to the source network.

Industrial Firewalls

Industrial firewalls help secure OT networks, safeguard critical infrastructure, and protect ICS from cyber threats and attacks. Advanced capabilities and specialized features help defend against network-based attacks, enable secure remote access, and enforce strict access controls, ensuring the secure operation of industrial processes.

Soft/Virtual/Micro-Segmentation

This technique improves network security and mitigates

the risks associated with lateral movement of threats in modern complex IT environments. By implementing this practice, organizations can achieve enhanced network visibility, fine-grained access control, and isolation of critical assets, bolstering overall security posture.

USB/Removable Media Sanitization

USB/removable media sanitization protects sensitive information and prevents data breaches. By securely erasing data from USB drives and other removable media devices, organizations can mitigate the risk of data exposure, maintain compliance with data protection regulations, and safeguard confidential information.



Product, Software, and Supply Chain Security

Implementation of robust security measures throughout the product lifecycle, supply chain, and operational processes enables organizations to reduce the risk of vulnerabilities, unauthorized access, and disruption to OT systems, safeguarding operations and protecting against potential cyber threats. It further also covers specific measures and practices employed to ensure the security and integrity of products, software applications, and the entire supply chain within OT systems and infrastructures.

Product security in OT involves designing and manufacturing devices that are resistant to cyber-attacks and other forms of tampering. It covers measures taken to protect the security and integrity of physical products, such as devices or equipment. It can also include implementing secure boot processes to ensure only trusted firmware can run on the device and hardening firmware to protect

against exploitation of vulnerabilities.

Supply chain security in OT involves ensuring that components and devices used in OT systems are authentic and free from tampering. This can include verifying the authenticity of devices and components before they are installed and implementing secure supply chain processes to prevent unauthorized access to devices and components.

Monitoring and Remediation

By proactively monitoring for vulnerabilities, intrusions, and suspicious activities, organizations can swiftly identify and respond to security incidents, minimizing potential damages and protecting systems from threats. They also help in immediate remediation ahead of adversarial attacks.

Product Security and SDLC

Blending product security, software security, and supply chain security considerations into the SDLC (software development lifecycle) establishes that organizations can effectively mitigate risks, identify vulnerabilities, and respond to security incidents. The holistic approach ensures that security is addressed at every stage of the development and deployment process, helping to safeguard products, software, and supply chains against potential threats.

SBOM/HBOM Analysis, VEX, File Integrity

These methods assist organizations to monitor and contribute towards the identification and remediation of vulnerabilities, prioritization of security efforts, and maintenance of the integrity and trustworthiness of critical files and components.

Third-party Risk Management

Organizations can minimize the potential security risks associated with external dependencies by implementing third-party risk management practices. It helps ensure that third-party products, software, or components meet the required security standards, protecting against vulnerabilities, breaches, or disruptions that may arise from the involvement of external entities.

Vulnerability Management

Vulnerability management helps organizations minimize the risk of exploitation, protect against potential breaches or compromises, and ensure the security and integrity of products, software, and supply chains.



Risk Management, Governance, and Compliance

By implementing effective risk management practices, establishing governance frameworks, and adhering to regulatory requirements, organizations can enhance the security and resilience of OT systems.

Risk management conducts comprehensive assessments to identify and understand potential threats, vulnerabilities, and the potential impact on OT systems and operations. With a good risk management blueprint in hand, organizations get a broad perspective on identifying the industrial risks that could cause a company to fail to meet its strategies and objectives. Given the volatility that exists in the landscape, the risk management process should be audited periodically to make sure weaknesses are identified and addressed, enabling continual improvement.

When it comes to governance, organizations work on establishing policies, procedures, and frameworks to guide decision-making, risk management, and operational practices. Creating policies and guidelines that define security objectives, roles and responsibilities, and acceptable use of OT systems and resources. -

Compliance primarily covers adhering to specific regulations and standards applicable to OT environments, such as NERC CIP, IEC 62443, or sector-specific regulations for critical infrastructure. Organizations must conduct regular audits to assess compliance with established security controls and regulatory requirements. They must also establish incident response procedures to handle security incidents, including reporting requirements to regulatory bodies, law enforcement, or relevant authorities.

Exposure Reduction and Vulnerability Prioritization

Organizations can reduce the attack surface, strengthen the security posture of OT environments, and mitigate risks to critical infrastructure, operations, and personnel safety by focusing on reducing exposure, and effectively prioritizing vulnerabilities. Exposure reduction focuses on minimizing the potential attack surface and vulnerabilities, using appropriate measures to reduce exposure risk. Vulnerability prioritization largely focuses on resources and efforts to address critical vulnerabilities effectively.

Industrial Threat Intelligence

Leveraging industrial threat intelligence enables organizations to proactively identify and respond to emerging threats, enhance security practices, and maintain compliance with regulations and standards specific to OT environments. These sources include both open-source intelligence (OSINT) and commercial

intelligence providers that specialize in monitoring and analyzing threats specifically targeting industrial environments.

Risk Exposure Analysis and Reporting

Risk exposure analysis involves evaluating and quantifying the potential impact and likelihood of risks to OT systems and operations so that organizations understand the magnitude of risks and prioritize mitigation efforts. Effective risk reporting enables informed decision-making, drives risk awareness, and supports compliance efforts.

Risk Management and Mitigation

Risk management uses processes, methods, and tools that help organizations identify what could go wrong, evaluate which risks should be dealt with, and implement strategies to deal with those risks. Risk Mitigation implements various measures to reduce or mitigate identified risks, such as applying security controls, implementing redundancy, or introducing intrusion detection and prevention systems.



Secure Remote Access

In industrial frameworks, secure remote access strikes a balance between operational efficiency and maintaining a robust security posture. By implementing appropriate security measures and adhering to best practices, organizations can enable remote access while safeguarding critical OT systems and infrastructure from unauthorized access and potential cyber threats. The approach allows authorized personnel to remotely access

and monitor OT systems, reducing the need for physical presence at the facility or site, enabling faster response times, efficient troubleshooting, and improved operational efficiency.

Secure remote access typically involves the use of virtual private networks (VPNs) or other secure remote access technologies, which can encrypt the data being transmitted between the remote user and the OT system. This helps to protect against interception and unauthorized access to OT systems. Alongside using secure technologies, secure remote access often involves implementing strict access control measures, – and limiting access to only those users who require it for the job.

Another important aspect of secure remote access is monitoring and logging of remote access sessions. This can include keeping a record of which users accessed the system when they accessed it, and what actions they took while connected.

Access Control: ABAC/DAC/MAC/BAC

Effective access control measures for secure remote access in OT environments can include the use of strong authentication methods, implementing user role-based access control, using firewalls to restrict access to specific IP addresses and/or ports, limiting the ability to remotely modify system configurations, and settings, and restricting the duration of remote access sessions to minimize exposure. Some commonly used access control models include Attribute-Based Access Control (ABAC), Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC).

Audit and Compliance: Session Logging/Recording/Termination

Roping in robust audit and compliance measures, including session logging, recording, and termination, enables organizations to maintain visibility, accountability, and traceability of remote access activities in OT environments. Helping organizations maintain accountability, traceability, and compliance with regulatory requirements, these mechanisms contribute to security monitoring, incident response, compliance management, and overall risk reduction.

Jump box, VPN Access, Converged SRA platform

Technologies like jump boxes, VPN access, and converged SRA platforms enable organizations to establish secure remote access in OT environments. These allow authorized personnel to remotely manage and monitor OT systems while maintaining the necessary security controls. The specific choice of technology depends on factors such as the organization's security requirements, infrastructure complexity, and regulatory compliance obligations.

Privileged SRA, Zero-Trust, and Identity

These mechanisms contribute to enhancing security, reducing the risk of unauthorized access, and improving accountability across OT systems. They play crucial roles in enhancing security and minimizing risks.

Social Engineering and Phishing Prevention

Social engineering is the art of manipulating individuals to divulge sensitive information or perform actions

that may be harmful to an organization's security. In OT environments, social engineering can be particularly damaging, as it can lead to the compromise of critical infrastructure systems.

Phishing is a specific type of social engineering that involves the use of fraudulent emails, text messages, or websites to trick individuals into divulging sensitive information such as usernames, passwords, or financial information. In an OT environment, phishing attacks can be particularly dangerous, as they can be used to gain access to critical systems and cause damage or disruption.

Phishing prevention in OT environments involves a combination of technical controls and user education. Organizations must implement email security measures to prevent fraudulent emails from reaching users and conduct regular phishing awareness training for employees to educate them on the dangers of phishing and how to identify and report suspicious emails. They must also adopt multi-factor authentication (MFA) for access to critical systems, to prevent unauthorized access even if a user's credentials are compromised.

Additionally, organizations need to update system software and patch vulnerabilities to prevent attackers from exploiting known vulnerabilities. They must also conduct regular security assessments and audits to identify and address potential vulnerabilities in the OT environment.

Inbox Cyber Security and Phishing Deterrence

Organizations must work to protect users' inboxes from malicious emails and actively discourage phishing attempts. The adoption of robust inbox cybersecurity measures enables organizations to significantly reduce the risk of successful phishing attacks in OT environments.

These measures, combined with user education and awareness, help create a more secure email environment and enhance the overall resilience against social engineering threats.

Training Platforms, Behavioral Modification/Interactive Training, CBT/Video

Organizations must utilize training platforms, behavioral modification/interactive training techniques, CBT (computer-based training) modules, and videos to effectively educate employees on social engineering and phishing prevention in OT environments. These approaches enhance awareness, promote responsible behavior, and equip employees with the skills and knowledge to recognize and respond appropriately to potential security threats. They largely work on driving behavioral changes regarding social engineering and phishing prevention.

Network Prevention/Enforcement

Organizations can significantly improve defense against social engineering and phishing attacks in OT environments by implementing strong network prevention and enforcement measures. These controls offer proactive security, reveal suspicious activity, and aid in preventing malicious actors from breaching the network and gaining unauthorized access to vital systems.

Secure Email Gateways

By using a secure email gateway, organizations can scan incoming and outgoing emails for malicious content. It can also be configured to block or quarantine suspicious emails from known malicious sources, quarantine suspicious emails, and protect OT systems. Additionally, secure email gateways can also be used to help prevent data leakage and unauthorized access to sensitive information.



Industrial Cyber Guide Services Categories

The categorization framework in this guide has been designed to identify, evaluate and determine those services that will add value and benefit the cybersecurity posture of the operational environment. These categories are designed to offer a preliminary assessment of services and introduce vendors who deliver those services. Therefore, it is not an exhaustive checklist. Furthermore, the framework is not sequential, as organizations may require certain services across different points within 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. Moreover, it also depends on the risk appetite of the organization.



Assessments and Testing

- Asset Discovery, Inventory Hygiene, and Diagnostic Assessments
- Conduct Gap, Vulnerability, and Risk Assessment/Audit Governance, Policy, and Procedure Review
- Governance, Policy, and Procedure Review
- Network Architecture Evaluation
- Penetration Testing
- Readiness Assessment
- Social Engineering and Phishing Testing/Assessments
- Technology Efficacy and Efficiency Evaluation



Deployment, Implementation, and Managed Services

- Acceptance Testing: Backup and Recovery
- Configuration and Patch Management
- Managed SOC and Monitoring
- Network Design and Segmentation
- Network Hardening
- Platform Integration
- SIEM/SOAR, EDR/XDR, Network, Identity, Asset, Cloud
- Systems Hardening
- Endpoint, Appliance, and Device



Incident Planning, Response, and Recovery

- Contingency and crisis planning
- Manage and remediate cybersecurity incidents
- Playbooks and Response Procedures
- Post-incident Forensics
- Threat Hunting and Investigation
- Threat Modeling and Visualization



Program Development

- Cyber Risk Management
- IIoT cybersecurity strategy/plan
- Network Architecture and Design Planning
- Program Development, Review, and Management
- Regulatory Compliance
- Security Framework and Standards Adoption
- Social Engineering and Security Awareness Program



Supply Chain and Product Security

- Continuous Monitoring
- File and Patch Integrity Service
- Product Assessment
- SBOM/HBOM Analysis
- Secure System Design, Implementation, and Development
- Third-party Risk Management
- Vulnerability Management



Train and Educate

- Cyber Range: Simulation Training
- Cybersecurity Skills Development
- OT/IT Alignment Program
- Red vs. Blue training
- Security Awareness Training
- Tabletop exercises



Assessments and Testing

Organizations conduct assessments and testing across OT environments to proactively identify and address vulnerabilities, evaluate security controls, and enhance security and resilience across these systems. The technique evaluates the current level of knowledge and skills of OT personnel, identifying any gaps that may exist, and then developing and delivering structured training programs to address those gaps.

Asset Discovery, Inventory Hygiene, and Diagnostic Assessments

Assessments in asset discovery, inventory hygiene, and diagnostics provide visibility into the assets present, maintain accurate inventory records, and evaluate the security of OT systems. They help organizations understand the scope of OT infrastructure and identify potential vulnerabilities or issues while supporting effective asset management, vulnerability management, patch management, and configuration management.

Conduct Gap, Vulnerability, and Risk Assessment/Audit

Executing a gap and vulnerability assessment involves evaluating the current state of the OT system, identifying any potential risks and vulnerabilities, and developing a plan to mitigate or eliminate those risks. Risk assessment/audit reviews of system architecture, network topology, security protocols, access control measures, and other critical components of the system.

Governance, Policy, and Procedure Review

The review aims to ensure that proper governance

structures are in place, policies are comprehensive and aligned with industry standards, and procedures are well-defined and followed consistently.

Network Architecture Evaluation

This evaluation throws light on the effectiveness of the network design, identifies vulnerabilities or weaknesses, and makes recommendations to improve the security, reliability, and performance of the network. It works on ensuring that the network design meets the operational and security requirements of the OT environment, including considerations for availability, scalability, and fault tolerance.

Penetration Testing

Penetration testing simulates real-world attack scenarios, enabling organizations to evaluate the effectiveness of security controls, enhance incident response capabilities, and improve the overall resilience of OT systems and infrastructure. It helps to proactively identify weaknesses and potential entry points that could be exploited by malicious actors.

Readiness Assessment

Readiness Assessment provides organizations with insights into the current state of preparedness and identifies areas that require improvement in terms of security, operational readiness, and compliance. Based on these findings, targeted action plans work on addressing any gaps and enhance overall readiness to handle the unique challenges of OT systems and infrastructure.

Social Engineering and Phishing Testing/Assessments

Conducting social engineering and phishing testing/assessments enables organizations to identify

vulnerabilities in human factor security controls and raise awareness among employees about the risks associated with social engineering attacks and phishing attempts. It helps strengthen the organization's security posture and reduces the likelihood of successful attacks targeting the OT environment.

Technology Efficacy and Efficiency Evaluation

Technology efficacy and efficiency evaluation helps organizations identify weaknesses, vulnerabilities, or performance bottlenecks that require proactive measures to improve technology infrastructure and enhance the overall effectiveness and efficiency of OT systems.



Deployment, Implementation, and Managed Services

Deployment, implementation, and managed services are used within OT environments to ensure improved efficiency, reduce the risk of downtime, and enhance the overall safety and security of operations across industries. With the intent of delivering smooth operation, security, and optimization of OT environments, these services help organizations maximize the benefits of OT investments, optimize system performance, ensure security and compliance, and provide the necessary support for efficient and reliable OT operations.

Acceptance Testing: Backup and Recovery

Acceptance testing for backup and recovery verifies that the procedures are functioning as intended. It also tests the backup process to ensure that all relevant data is backed up and that backups can be restored successfully.

Configuration and Patch Management

By implementing robust configuration management practices and staying proactive with patch management, organizations can enhance the security and resilience of OT assets, reducing the likelihood of successful cyberattacks and minimizing operational disruptions.

Managed SOC and Monitoring

Managed SOC and monitoring services give organizations the expertise, resources, and continuous monitoring capabilities necessary to protect critical OT systems and assets from emerging cyber threats. By leveraging specialized security technologies, threat intelligence, and skilled analysts, managed SOC services enhance the organization's security posture, improve incident response capabilities, and enable efficient detection and mitigation of security incidents in the OT environment.

Network Design and Segmentation

By implementing robust network design and segmentation practices in OT environments, organizations can achieve improved security, reduced attack surface, better network performance, and increased resilience. These measures help protect critical assets, prevent unauthorized access, contain security incidents, and ensure the uninterrupted operation of OT systems.

Network Hardening

When it comes to network hardening, organizations must work on securing network device configuration, network segmentation, perimeter security, network access control, network monitoring and logging, and secure network protocols.

Platform Integration

Effective platform integration enables organizations to collect and analyze data from a wide range of sources, and to use this data to drive operational efficiencies, optimize performance, and improve organizational decision-making.

SIEM/SOAR, EDR/XDR, Network, Identity, Asset, Cloud

These components work together to provide a comprehensive security posture for OT environments, enabling organizations to detect and respond to security threats in real-time. They also proactively identify and address potential vulnerabilities before they can be exploited by attackers.

Systems Hardening

Effective systems hardening is critical to reducing the risk of cyber attacks against OT systems. By reducing the attack surface, organizations can make it more difficult for attackers to gain access to critical systems and data and can minimize the impact of any successful attacks.

Endpoint, Appliance, and Device

Securing endpoints, appliances, and devices in OT environments will ensure the integrity, availability, and safety of industrial processes. It will also drive regular maintenance, updates, monitoring, and compliance with security best practices.



Incident Planning, Response, and Recovery

When it comes to OT environments, incident planning, response, and recovery require a proactive and well-coordinated approach. It involves a combination of technical controls, skilled personnel, effective processes, and continuous improvement to mitigate the impact of incidents, minimize downtime, and ensure the operational resilience of OT systems and processes.

These activities are crucial for minimizing the impact of incidents, restoring operations, and ensuring the resilience of the OT environment. The mechanism used primarily focuses on preparing for, responding to, and recovering from security incidents and disruptions that may impact the OT systems and industrial processes.

The game plan involves a combination of technical controls, skilled personnel, effective processes, and continuous improvement to mitigate the impact of incidents, minimize downtime, and ensure the operational resilience of OT systems and processes.

Contingency and crisis planning

Contingency and crisis planning deliver a proactive and comprehensive approach to managing and mitigating the impact of disruptions or crises. By anticipating potential risks, organizations can work on developing appropriate strategies and maintaining preparedness, thus enhancing the resilience of OT systems and minimizing downtime during critical incidents.

Manage and remediate cybersecurity incidents

A clear communication channel, well-defined incident response roles and responsibilities, and collaboration between different teams are necessary for managing and remediating cybersecurity incidents in OT environments. By implementing robust incident response processes, organizations can manage and remediate cybersecurity incidents, protect critical industrial processes, and maintain the security and resilience of OT environments.

Playbooks and Response Procedures

Playbooks and response procedures provide a structured and standardized approach to incident response, enabling organizations to respond efficiently, reduce incident resolution time, minimize the impact of incidents, and maintain the security and resilience of OT systems and processes.

Post-incident Forensics

Following a cybersecurity incident, organizations must adopt a streamlined process that investigates and analyzes the cyber breach. It involves gathering and examining digital evidence, conducting forensic analysis, and reconstructing the events that led to the incident. This will help throw light on the root cause of the incident, identify the extent of the compromise, and gather information that can be used for remediation, legal purposes, and future incident prevention.

Threat Hunting and Investigation

A proactive process of searching for and identifying potential threats and malicious activities within the OT network, threat hunting, and investigation involves collecting and analyzing data from various sources

to uncover indicators of compromise (IoCs), signs of unauthorized access, or suspicious behaviors that may indicate a security breach. The key objective is to detect and respond to threats before they can cause significant damage or disruption to critical industrial processes.

Threat Modeling and Visualization

Threat modeling and visualization provide a structured approach for identifying and addressing security concerns, enabling organizations to make informed decisions about security controls and risk mitigation strategies.



Program Development

Program development designs and implements a comprehensive cybersecurity program addressing the unique security challenges and requirements of OT systems. It involves establishing the necessary policies, procedures, and controls to protect critical infrastructure, industrial control systems, and other OT assets from cybersecurity threats. The goal of program development in OT environments is to build a structured and proactive approach to managing cybersecurity risks and ensuring the resilience of OT operations.

Cyber Risk Management

A critical aspect of program development in OT environments, cyber risk management involves a systematic approach to identifying, assessing, and mitigating cybersecurity risks, ensuring the protection and resilience of OT systems against evolving threats. By incorporating risk management practices into program development, organizations can effectively address the

unique security challenges posed by OT environments and establish a robust cybersecurity posture.

IloT cybersecurity strategy/plan

As OT systems increasingly leverage IloT technologies for improved connectivity and operational efficiency, it becomes crucial to establish a comprehensive cybersecurity strategy to address the unique challenges and risks associated with IloT deployments. The plan must include identifying the IloT assets, assessing the risks associated with each asset, charting a risk management plan, defining policies and procedures, implementing appropriate security controls, and monitoring and continuous maintenance of the IloT cybersecurity strategy/plan.

Network Architecture and Design Planning

Network architecture and design planning within the broader program development in OT environments involve implementing secure and resilient network infrastructures to support the communication needs of OT devices and systems. These approaches set the structure for how data flows to, from, and between resources within the organizational framework.

Program Development, Review, and Management

Program development, review, and management encompass systematic and ongoing processes involved in designing, evaluating, and maintaining a robust OT security program. By defining clear objectives, establishing governance structures, conducting regular assessments, and managing resources, organizations can enhance the security posture of OT environments and better mitigate cyber threats.

Regulatory Compliance

By incorporating regulatory compliance into program development, organizations can establish a strong foundation for maintaining a secure and compliant OT environment. Compliance with regulations helps organizations minimize legal and operational risks, protect critical infrastructure, and demonstrate commitment to maintaining a secure OT environment.

Security Framework and Standards Adoption

Adoption of appropriate security frameworks and standards can help organizations benefit from established guidelines and best practices to enhance the security posture of OT environments. These frameworks and standards help organizations establish a comprehensive and consistent security program while aligning with industry best practices and regulatory requirements.

Social Engineering and Security Awareness Program

Implementation of a comprehensive social engineering and security awareness program can reduce the risk of successful social engineering attacks in OT environments. Increased awareness and vigilance among employees can serve as a powerful defense against social engineering threats, enhancing the overall security posture of the organization's OT systems and operations.



Supply Chain and Product Security

Supply chain and product security include various measures and practices implemented to ensure the integrity, confidentiality, and availability of components,

systems, and software throughout the supply chain lifecycle. It involves managing the security risks associated with procuring, developing, deploying, and maintaining OT products and solutions, in addition to ensuring that all products and components used in the OT environment are secure and free from potential vulnerabilities.

Continuous Monitoring

Continuous monitoring provides organizations with real-time visibility into the security posture of the supply chain and OT products. By actively monitoring and assessing the ecosystem, organizations can proactively detect and respond to security threats, vulnerabilities, and incidents, minimizing potential risks and ensuring the integrity, confidentiality, and availability of OT environments.

File and Patch Integrity Service

Monitoring and verifying file integrity and patch management allows organizations to ensure the trustworthiness and integrity of software and firmware components throughout the supply chain and product lifecycle. The approach helps organizations maintain the trustworthiness and integrity of software and firmware components, reducing the risk of security breaches, operational disruptions, and compromised systems.

Product Assessment

Executing product assessment is carrying out due diligence and determining the security of products and components before they are integrated into the OT environment to ensure that they are free from potential vulnerabilities. Organizations must identify products and components, conduct security assessments, test for vulnerabilities, analyze security controls, develop risk management plans,

and monitor and maintain the security of products and components on an ongoing basis.

SBOM/ HBOM Analysis

SBOM analysis involves creating a list of software components used in a product or system, while HBOM analysis covers all hardware components used across the product or system. SBOM/ HBOM analysis will identify any potential security risks associated with the use of specific software or hardware components, and detect anomalies in the organizational framework.

Secure System Design, Implementation, and Development

Organizations must execute secure system design, implementation, and development plans that adopt a proactive and holistic approach to security, continually assessing and updating security measures to adapt to evolving threats. These concepts help establish security practices to protect against threats such as unauthorized access, tampering, data breaches, and malicious activities.

Third-party Risk Management

Third-party risk management deals with the interconnected business landscape that organizations must account for, as they rely on third-party vendors, suppliers, and service providers to support operations. However, these external entities can introduce potential security risks if not properly managed.

Vulnerability Management

Vulnerability management involves identifying, assessing, and mitigating vulnerabilities in products and components used in the OT environment. Organizations can bolster the resilience and security of OT environments, protect critical

infrastructure, and mitigate the risks associated with potential vulnerabilities by implementing a comprehensive vulnerability management program across the supply chain and product security.



Train and Educate

Train and -educate services involve establishing a security culture that works on training and educating employees and stakeholders on the unique needs and challenges of the OT environment. With this outlook, organizations can better manage risks, respond to incidents, and proactively handle security challenges in OT infrastructure by improving the knowledge, abilities, and awareness of staff. The goal is to ensure that everyone involved in managing and maintaining these systems has the knowledge and skills necessary to minimize the risk of cyber-attacks and other security incidents.

Cyber Range: Simulation Training

Cyber Range uses simulation training to create realistic virtual environments that simulate cyber attacks, vulnerabilities, and incidents specific to OT systems. It provides a controlled and safe environment for training personnel on how to detect, respond to, and mitigate cyber threats in OT infrastructure. It delivers practical experience, enhances incident response capabilities, and develops a proactive and resilient security posture in the face of evolving cyber threats.

Cybersecurity Skills Development

Cybersecurity skills development works on improving the technical expertise and knowledge of employees

and stakeholders who are responsible for managing and maintaining industrial control systems and other critical infrastructure. This may include training on the latest cybersecurity threats and best practices, as well as hands-on experience with security tools and technologies. The goal is to ensure that everyone involved in OT environments has the skills and knowledge necessary to detect, prevent, and respond to cyber-attacks and other security incidents.

OT/IT Alignment Program

An OT/IT alignment program works on aligning technology roadmaps, defining common standards and protocols, and establishing clear lines of communication and accountability. It may also involve developing joint training and development programs to ensure that both teams have the skills and knowledge necessary to work together effectively. The benefits of an OT/IT alignment program include improved operational efficiency, reduced downtime, and enhanced security and compliance.





Red vs. Blue training

Red vs. Blue training provides a realistic and practical approach enabling organizations can identify vulnerabilities, strengthen defenses, and prepare personnel to respond to cyber threats. It helps improve incident response capabilities and enhances security across critical environments.

Security Awareness Training

Security Awareness Training works on educating employees and stakeholders on the importance of cybersecurity and how to identify and respond to security threats. It allows organizations to create a security-conscious workforce that actively contributes to the protection of critical infrastructure.

Tabletop exercises

Tabletop exercises prepare OT environments for potential cybersecurity incidents or operational disruptions, delivering a safe environment for testing response strategies, enhancing communication and coordination, and identifying areas for improvement. The conduct of these exercises aims to assess, validate, and improve the effectiveness of incident response plans and procedures across OT systems.

Case Study#1

Enforcing Policy and Incident Response

Darktrace/OT monitors connections in and out of an organization's OT environment using a Secure Remote Access Solution (SRAS). It alerts the security team to a suspicious remote access attempt, revealing a compromised user's account. Darktrace DETECT blocks the connection by updating firewall rules, while Darktrace RESPOND blocks the connection autonomously.

Even without the integration, Darktrace can respond by taking a native response against the jump host, such as blocking matching internal connections to prevent the attacker from reaching further OT devices.

Additionally, the victim organization leverages Darktrace to enforce incident management policies.

While Darktrace autonomously responds to the compromised remote access, the security team is prompted with additional human-confirmable response actions:

- Block all incoming connections to the ICS via Darktrace pushing preset rules to the firewall at the security perimeter.
- Isolate the endpoint device of the user with the compromised endpoint device via Darktrace/Endpoint.
- Force logout or lock the remote access account of the end user via integration with the remote access solution.

Case Study#2

Protecting Industrial IoT

The widespread adoption of IIoT devices has increased the complexity and vulnerability of industrial environments. Recently, a manufacturing firm in the EMEA region was alerted by Darktrace to a series of pre-existing infections in IIoT devices.

Darktrace's self-learning AI identified a device exploiting the SMBv1 protocol for lateral movement and using default vendor credentials for device enumeration. Unusual connections, including those to internal endpoints previously unknown to the company, were detected. Darktrace illuminated the spread of this unusual activity across the infrastructure.

A total of 13 infected production devices were identified by Darktrace. This 'unknown known' threat was uncovered without prior knowledge of the devices, their supplier, or patch history, and without relying on malware signatures or IoCs.

By uncovering this previously unknown threat, Darktrace empowered the customer to conduct a comprehensive incident response and threat investigation, preventing serious damage to the company from the attack.

Case Study#3

Protecting Industrial IoT

Darktrace/OT detected a subtle deviation from normal behavior when a reprogram command was sent by an engineering workstation to a PLC controlling a pump, an action an insider threat with legitimized access to OT systems would take to alter the physical process without any malware involved.

In this instance, AI Analyst, Darktrace's investigation tool that triages events to reveal the full security incident, detected the event as unusual based on multiple metrics including the source of the command, the destination device, the time of the activity, and the command itself.

As a result, AI Analyst created a complete security incident, with a natural language summary, the technical details of the activity, and an investigation process explaining how it came to its conclusion. By leveraging Explainable AI, a security team can quickly triage and escalate Darktrace incidents in real-time before they become disruptive, even when performed by a trusted insider.

DARKTRACE

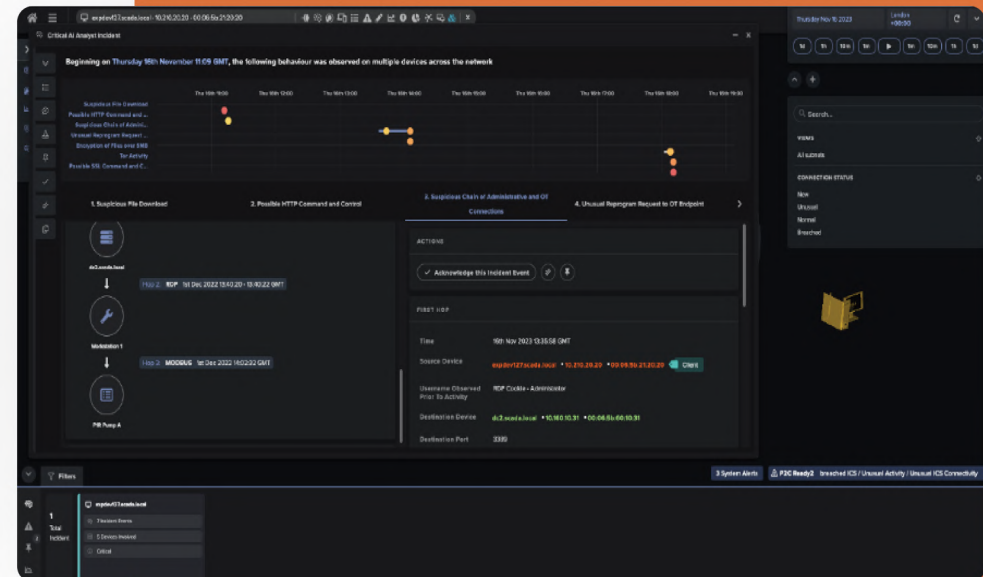
The increase in OT cybersecurity solutions underscores the dedication of critical infrastructure and industrial sectors to mitigate risks associated with digitalizing and networking operations while addressing disruptive threats. This shift towards more connected and digital systems necessitates robust cybersecurity measures, with technologies such as AI and blockchain being key to defending against sophisticated cyber threats.

As industrial systems grow more complex, there's a heightened need for comprehensive cybersecurity solutions. Darktrace exemplifies innovation in this area, providing extensive monitoring and analysis of network traffic and activities, ensuring continuous detection, visibility, and, if needed, autonomous response in complex

ICS environments. Its Self-Learning AI adapts to identify deviations from 'normal' behavior, potentially signaling cyber attacks.

Darktrace/OT secures infrastructure down to the Purdue Model's lowest levels, covering all aspects from operational devices to corporate networks and cloud services, and enhances security around the DMZ. This approach not only protects but also offers insights into potential vulnerabilities and threats, representing a significant advancement in cybersecurity for industrial enterprises.







Here are three practical case studies that illustrate the unique requirements of industrial enterprises and how Darktrace is assisting customers in meeting these challenges.



Industrial Cybersecurity Technology & Solutions

-  Asset - Discovery and Vulnerability Management
-  Cyber-Physical Security and Operational Systems Health
-  Identity and Access Management (IAM)
-  Industrial IoT (IIoT) Device Security
-  Network Security Monitoring and Anomaly detection
-  Operational IT/OT Endpoint Security and Patch Management
-  Perimeter Security, Segmentation, and Zone Enforcement
-  Product, Software, and Supply Chain Security
-  Risk Management, Governance, and Compliance
-  Secure Remote Access
-  Social Engineering and Phishing Prevention

Industrial Cyber Guide Services Categories

-  Asset - Discovery and Vulnerability Management
-  Cyber-Physical Security and Operational Systems Health
-  Identity and Access Management (IAM)
-  Industrial IoT (IIoT) Device Security
-  Network Security Monitoring and Anomaly detection
-  Operational IT/OT Endpoint Security and Patch Management

Industrial
Cyber

Research

VENDORS



Airbus Cybersecurity

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

OFFERINGS:

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.

airbus-cyber-security.com ↗



Armexa

Armexa is a team of dedicated operational technology (OT) and industrial cybersecurity experts that provide practical and scalable industrial cybersecurity services and solutions. The company's team has decades of hands-on experience working in critical infrastructure facilities to help those operations run safely, reliably, and securely.

SERVICES INCLUDE:

Governance: Foundational support in establishing OT governance models, frameworks, and documentation.

Assess and Plan: Services focus on helping companies assess their baseline cybersecurity posture, prioritize risks, and establish remediation plans.

Design and Build: Hands-on design and implementation of secure control systems.

Run and Maintain: White-glove technical and staffing support.

www.armexa.com ↗

marketing@armexa.com ↗



Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages cyber risk exposure in real-time. Deployed at thousands of sites worldwide, Armis ensures that organizations, including critical infrastructure, industrial manufacturing, and national, state, and local governments, continuously see, protect, and manage - critical assets.

Armis Centrix for OT/IoT Security offers - insights into - connected assets, wired and wireless, within and surrounding converged OT networks. It discovers, classifies, and profiles, offering rich contextual insights into every asset including SCADA, PLCs, DCS, IIoT, IoT, IoMT, and IT, and the interconnected support devices that keep facilities operational. Armis Centrix interoperates seamlessly with the existing technology toolset to focus attention on critical events and prevent their expansion, mitigate their effects, and resolve them quickly. By monitoring all assets and their transactions and dependencies, Armis Centrix delivers true insights into the cyber asset attack surface of the entire enterprise.

Paired with Armis Centrix for Vulnerability Prioritization and Remediation, Armis Centrix for OT/IoT Security goes beyond simple vulnerability scanning and addresses the full cyber risk management lifecycle of OT assets, including mapping risk to business criticality, prioritizing assets needing immediate attention, orchestrating remediation, and tracking processes and workflows through to remediation. Armis is FedRAMP and U.S. DoD Defense Level 4 certified and aligns with industry standards: ISO 27001, ISO 28018 Best Practices, and SOC 2 Type II certifications.

The security policies provided with the platform were designed based on NIST 800-53 and are updated every year. Armis is a privately held company headquartered in California.

OFFERINGS

- OT/IoT Security
- Vulnerability Prioritization and Remediation
- Asset Management and Security
- Medical Device Security
- Actionable Threat Intelligence
- Managed Threat Services

www.armis.com ↗



BAE Systems

BAE Systems is an 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.

OFFERINGS:

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.

www.baesystems.com ↗



Beacon Security

Beacon Security is an OT security-focused services company that helps industrial organizations with their cybersecurity needs through every phase - from assessment, to design and implementation to operations. The company safeguards industrial environments against evolving cyber threats, ensuring enhanced security, resilience, and operational continuity.

IT'S COMPREHENSIVE SERVICES INCLUDE:

- **OT Cybersecurity Assessment:** Evaluating vulnerabilities and risks in OT infrastructure.
- **Risk Management and Compliance:** Developing robust strategies and ensuring compliance with industry standards.
- **ICS Security:** Implementing secure controls for critical infrastructure protection.
- **Incident Response and Recovery:** Creating effective plans to mitigate cybersecurity incidents.
- **Employee Awareness and Training:** Educating the workforce on best practices for OT cybersecurity.

www.beaconsecurity.io ↗

kunal@beaconsecurity.io ↗



Booz | Allen | Hamilton

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 ↗



BELDEN



For more than 120 years, Belden has been a trusted provider of network infrastructure, laying the foundation for operations in global organizations. Today, Belden is building the future for the digital world, empowering organizations to operate more efficiently, safely, and reliably.

In response to the evolving cyber-risk landscape, Belden cybersecurity solutions deliver less complex, more automated protection. We guard against inadvertent and malicious behavior from the IO block to the edge, helping customers embark on their Industry 4.0 journey.

OFFERINGS:

- Identify cyber-risk gaps through risk and vulnerability assessments.
- Manage end-to-end network architecture and hardware and software inventory with solutions including TXCare, PROVIZE, macmon NAC, and Industrial HiVision.
- Protect organizations with network segmentation and isolation via the industry's strongest industrial firewalls, EAGLE and Tofino, and the Hirschmann Rail Data Diode.
- Master logical access control and secure remote access with macmon NAC and macmon SDP, while managing remote connectivity and edge orchestration with Belden Horizon.
- Detect malicious code with Tofino industrial protocol deep packet inspection, and identify unexpected network events with PROVIZE Explorer, TXCare, Industrial HiVision, Belden Horizon Network Insights, and macmon NAC.
- Respond by taking automated action with macmon NAC, Hirschmann, OTN Systems, NetModule, and the EAGLE and Tofino firewalls.

Belden's industrial cybersecurity solutions offer visibility into and protection from events that threaten the safety, quality, and productivity of the control systems. From hardware devices with embedded security features to cyber-resilient software, Belden helps organizations transform raw system data into actionable insights for a powerful defense against cyber disruption. It also protects operational infrastructure, enhances the resilience of converged networks, and takes proactive measures to maximize uptime with Belden.

www.belden.com ↗

belden.com/support/contact-us ↗

Identify risk. Protect operations. Detect events. Respond immediately.

Belden industrial cybersecurity solutions reduce complexity, automate protection, safeguard operations and enable the Industry 4.0 journey. Move beyond just visibility and provide protection today with Belden.

belden.com/cybersecurity

BELDEN

CYBERSECURITY FROM THE GROUND UP.

From assessments to managed services, we help our clients design, develop, and run their cyber programs to stay ahead of the game and protect the critical infrastructure we have over 100 years of experience helping build.

Because who better to build that home-field advantage than those who helped build the field?

One partner, end-to-end solutions.



 **BLACK & VEATCH**



Black & Veatch is a global engineering, procurement, construction (EPC), and consulting leader with over 100 years' experience in innovation, operational risk management, and safety.

Our industrial cybersecurity practice is built on the belief that cybersecurity is better built-in rather than bolted-on, and begins with integrating cyber into the engineering, design, and construction of assets. Post-delivery, we design, build, and run cybersecurity programs that keep assets up and running safely throughout their lifetime.

Our "security-by-design" methodology establishes operational safety and security in critical infrastructure projects throughout the project lifecycle, from building of assets to running your programs. Our comprehensive range of services include Technical Consulting (Assessments, Network Design Review, Supply Risk Management, Policy Reviews, Asset Inventory, Vulnerability Assessment, Incident Response Plan Development), Implementation (Cyber Acceptance Testing, Program Stand-up, Technology Implementation, Hardening, Segmentation, Asset Management, Vulnerability Management) and Ongoing Services (Managed Services, Monitoring, Predictive Intelligence).

Black & Veatch's experience in building the very sites and assets that need protection makes us the go-to industry partner to help design, develop, and run these industrial cyber programs.

With cyberattacks infiltrating equipment, networks, and devices that run operations, it's vital to have a strong cyber program in place as a home-field advantage to mitigate those risks. Who better to help our clients build a home-field advantage than the people who built the field?

One partner, end-to-end solutions.

www.bv.com ↗

cybersecurity@bv.com ↗



Byos

The Byos micro-segmentation platform provides Edge networking protection, asset invisibility and isolation, and granular secure access to resources without data leakage or device exposure. Byos was built for zero-trust networking and is inherently compatible with all sorts of existing devices and network environments. This brings dramatic risk reduction – as well as unlocks new opportunities for greater efficiencies, productivity, and data aggregation for optimal performance and savings.

Byos serves customers across the fields of critical infrastructure, manufacturing, defense and government, healthcare, energy, and financial services – securing everything from plant floor machinery to EV charging stations, to individual employee laptops.

www.byos.io

engage@byos.io



Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial, healthcare, and commercial environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide comprehensive controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by investment firms and industrial automation.

www.claroty.com

info@claroty.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 include 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 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.

www.capgemini.com



The bridge to possible

Cisco's comprehensive cybersecurity solutions, industrial networking portfolio, and expertise with OT requirements are a rare combination in the OT/ICS security market.

OFFERINGS:

Cisco Cyber Vision: Get comprehensive visibility into connected assets and your OT security posture. Embedded into industrial network equipment, Cyber Vision enables the deployment of OT security at scale without additional hardware or SPAN collection networks.

Cisco Secure Firewall: Build the industrial demilitarized zone (IDMZ) to protect OT and IT networks from cyber threats.

Cisco Identify Service Engine (ISE): Shrink the zones of trust with a dynamic and automated approach to policy enforcement that simplifies implementing ISA/IEC62443 zones and conduits.

Cisco Secure Equipment Access: Secure remote access to your OT/ICS assets with a zero-trust network access (ZTNA) solution which is simple to deploy at scale without additional hardware.

Cisco Extended Detection and Response (XDR): Augment OT security events with intelligence from other sources and orchestrate remediation across IT and OT domains.

Cisco Talos: Keep all security tools up to date with threat intelligence from one of the world's largest cybersecurity research teams and the official developer of Snort intrusion detection rules.

Talos Incident Response: Get OT security experts to deliver proactive services on-site to strengthen your security posture, test your capabilities, or help respond and recover from a breach.

www.cisco.com/go/IoTsecurity

AskIoT@cisco.com



The bridge to possible

If it's connected,
it's protected

Simplify your OT security architecture. See more, protect more, and scale simply with OT visibility, microsegmentation, zero-trust remote access, and threat detection embedded in your industrial network, as only Cisco can.



www.cisco.com/go/iotsecurity



IoT Security
Innovation of the Year





Cybersplice

A privately held South African Company based in Cape Town. Cybersplice prevents destructive cyber-physical attacks, by evolving the Purdue model principles into a specialized ICS Secure Access Edge to shield vulnerable equipment inside an encrypted overlay network.

OFFERINGS:

- **SPLICECLOUD** provides rapid OT security visibility by profiling communications between OT nodes and alerting on outliers and anomalous activity. Get up and running in an hour.
- **SPLICE IN-PATH** actively shields vulnerable OT equipment inside an encrypted overlay network, disrupting the kill chain for would-be attackers. Extend visibility with logical isolation, secure identity management, deception techniques and secure remote access.
- **SPLICE-NET** Industrial Connectivity Cloud extends OT network reach across hostile carriers and corporate IT networks.

www.cybersplice.com ↗

splice@cybersplice.com ↗



Cynalytica

Cynalytica develops sensor and software machine learning analytics platforms that provide fully passive, fail-safe monitoring and analysis of physical communications in industrial control systems (ICS/SCADA). Giving control system operators the ability to securely provide visibility and unique situational awareness to high-risk, high-impact cyber-physical assets, such as energy systems, water/wastewater treatment facilities, manufacturing, nuclear power, defense systems, and building facilities.

www.cynalytica.com ↗

info@cynalytica.com ↗



Cylus

Cylus provides rail operators with a specialized cybersecurity solution for operational rail technology systems, ensuring service availability and safety. Combining deep expertise in rail and cybersecurity, Cylus has pioneered a comprehensive rail tech security platform that delivers real-time asset visibility and threat detection and response capabilities across heterogeneous operational rail technology environments.

Delivering deep rail context and rail framework compliance to customers across the globe, Cylus is leading the way with a cybersecurity solution that reduces risks and ensures compliance in the face of escalating cyber threats.

www.cylus.com ↗

info@cylus.com ↗



Cyolo

Cyolo enables privileged remote operations, connecting verified identities directly to applications with continuous authorization throughout the connection. Purpose-built for deployment in every type of environment, the company's hybrid secure access solution combines multiple security functions required to mitigate high-risk access, including zero-trust access for users and devices, MFA for the last mile, IdP, password vault, secure file transfer, supervised access, session recording, and much more into a single, cost-effective, easy to deploy, and user-friendly platform.

The company also helps to consolidate the security stack and experience the power of seamless and secure operations across any application in any environment, from critical infrastructure to the cloud.

www.cyolo.io ↗

info@cyolo.com ↗



DeNexus

DeNexus empowers CISOs to optimize their cybersecurity program and budget by quantifying cyber risks in monetary terms and prioritizing risk mitigation based on impact and ROI. Using DeNexus and its AI-powered DeRISK platform, security teams can identify cyber risks with the highest potential financial loss and simulate the positive impact of risk mitigation projects. CISOs and CFOs can collaborate to justify cybersecurity investments, including cyber insurance.

DeNexus is dedicated to industrial sectors with OT/ICS environments or cyber-physical systems such as energy, manufacturing, hyperscale data center operations and transportation. Global 1000 companies in North America and Europe trust DeNexus to optimize their cyber risk management strategy.

www.denexus.io

info@denexus.io



Keeping you updated

It's our mission to keep you informed of the rapidly changing industrial cybersecurity landscape. Benefit from minimized risk, maximized productivity, and optimized decision-making with our valuable insights.

Our market research has earned a global reputation for its precision, quality, and practicality.

Discover why today

We're excited to share this exclusive offer with all Industrial Cyber readers. Secure a special discount on any of our Decision Point Reports or Vendor Research today.

coupon code

INDCYBG24

checkout to take advantage of this offer.



DARKTRACE

Cybersecurity AI company Darktrace delivers complete AI-powered solutions in its mission to free the world of cyber disruption. The company protects more than 9,000 customers from the world's most complex threats, including ransomware and cloud and SaaS attacks.

The Darktrace AI Research Centre based in Cambridge, UK, has conducted research establishing new thresholds in cyber security, with technology innovations backed by more than 165 patents and pending applications. The company's second, European R&D center is located in The Hague, Netherlands.

Industry-first Cyber AI platform

Darktrace's Cyber AI platform is an industry-first set of cyber capabilities that will not just prevent, detect, respond, and heal from cyber-attacks, but do it all at once. An always-on, feedback system with a deep, interconnected understanding of the enterprise creates a virtuous cycle in which each capability strengthens and hardens the entire security ecosystem. With its - Self-Learning AI, Darktrace empowers bespoke solutions unique to each customer based on continuous visibility into an organization's entire digital ecosystem.

Trusted Across the World

Customers include public sector agencies, education institutions, media, organizations supplying critical infrastructure, and businesses of all sizes across all industries. Headquartered in Cambridge, UK, Darktrace has more than 2,300 employees.

www.darktrace.com

sales@darktrace.com

The logo for Darktrace, featuring the word "DARKTRACE" in a bold, white, sans-serif font. The letter "D" is stylized with a red and orange gradient. The background of the entire image is a dark industrial facility at night, with various pipes, tanks, and structures illuminated by blue and white lights. A prominent orange and yellow glowing line curves across the bottom of the image.

DARKTRACE

Revolutionizing OT Risk Management

New innovations to Darktrace/OT makes it the industry's first OT cybersecurity solution to move beyond CVE scores and redefine vulnerability management for critical infrastructure, tackling the full breadth of risks not limited by traditional controls.

[Learn more](#)



Dispel

Dispel provides secure remote access designed for OT (operational technology) networks. Built on Moving Target Defense architecture, Dispel helps organizations enable OT remote access while staying aligned to regulatory frameworks and compliance standards.

OFFERINGS:

Dispel Remote Access is explicitly built for OT teams and prioritizes network uptime, availability and safety. That means a 30-second connection time, a straightforward user experience for operators and vendors, and complete control for the OT network admin. It also ensures that the team maintains invisible compliance with modern security frameworks.

www.dispel.io ↗

hello@dispel.io ↗

[+1 \(917\) 268-4029](tel:+19172684029) ↗



DriveLock

DriveLock SE is an international specialist for cloud-based endpoint and data security with offices and representations in Germany, Australia, Singapore, the Middle East, and the USA. In the digital transformation era, the success of businesses depends on how reliably people, businesses, and services are protected against cyberattacks and the loss of valuable data.

Founded in Munich, Germany in 1999, DriveLock's mission is to protect company data, devices, and systems. To achieve this, DriveLock utilizes the latest technologies, experienced security experts, and solutions based on the zero trust model. In today's security architectures, zero trust means a paradigm shift according to the maxim "Never trust, always verify". This way, data can even be reliably protected in modern business models.

www.drivelock.com ↗

briantuck@drivelock.com ↗



Dragos

The Dragos Platform delivers unmatched visibility of an organization's ICS/OT assets and communications. It rapidly pinpoints threats through intelligence-driven analytics, identifies and prioritizes vulnerabilities, and provides practitioner focused response playbooks. Codified with the expertise of the largest, most experienced team of ICS/OT security practitioners, Dragos ensures its customers are armed with the most up-to-date technology and intelligence to combat the most sophisticated industrial adversaries. In addition to the Dragos Platform, Dragos solutions include OT Watch, a managed threat hunting service, Dragos Worldview, an OT-specific threat intelligence service, and Neighborhood Keeper, a free, opt-in collective defense solution for Dragos Platform customers.

OFFERINGS:

In addition to the Dragos Platform, Dragos solutions include OT Watch, a managed threat hunting service; Dragos Worldview, an OT-specific threat intelligence service; and Neighborhood Keeper, a free, opt-in collective defense solution for Dragos Platform customers.

www.dragos.com ↗

info@dragos.com ↗

DXC Technology

DXC Technology's 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.

OFFERINGS:

- **Cyber Defense:** Consists of tailored offerings to support the digital enterprise.
- **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 PKI that protects the enterprise.
- **Data Protection:** Helps with protecting critical data and assists enterprises understand the use of critical content.

www.dxc.technology ↗



Emerson

As part of its OT services, Emerson combines its power and water cybersecurity suite with a portfolio of industrial cybersecurity services to deliver platform-independent offerings.

OFFERINGS:

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 ↗



EXALENS

Exalens Industrial AI Analyst unifies device and process monitoring, autonomously learning every detail of your operational system and its processes. Like a seasoned analyst, it integrates seamlessly with your existing monitoring solutions, such as SCADA, DCS, HMI, to broaden the scope of their isolated visibility. It gains a deep understanding of normal activity across your connected cyber-physical systems, adapting as they evolve. Exalens swiftly identifies and investigates the root causes of abnormal activity at machine speed, providing real-time, early warnings to your operational teams. This enables them to respond in minutes and seconds, rather than hours and days.

www.exalens.com ↗
team@exalens.com ↗



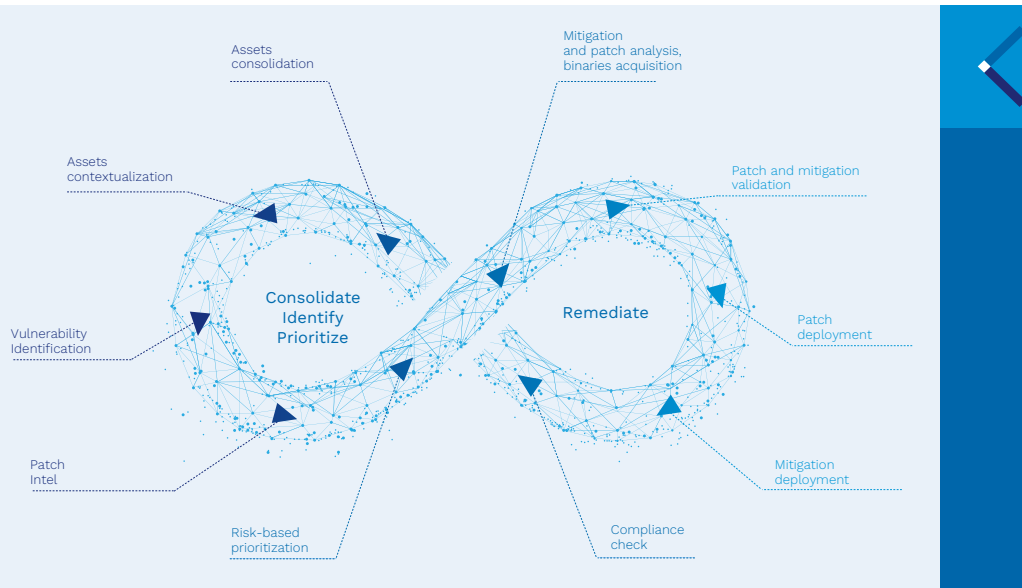
FORTINET®

Fortinet is a driving force in the evolution of OT cybersecurity and the convergence of networking and security, with a mission to secure people, devices, and data everywhere. It provides cybersecurity everywhere needed with the largest integrated portfolio of over 20 industrial cybersecurity products.

SERVICES:

- FortiOS, Fortinet’s security operating system, expands the Fortinet OT Security Platform’s ability to consolidate multiple security point products across an ever-expanding attack surface, helping customers reduce and manage the attack surface, prevent advanced threats, and reduce complexity.
- FortiGate Next-Generation Firewalls are powered by purpose-built security processing units (SPUs). They enable security-driven networking and are ideal network firewalls for hybrid and hyper-scale data centers. Options include Industrially hardened appliances providing network connectivity and securing critical industrial and control networks.
- Secure Remote Access: Remote access with multi-factor authentication (MFA) traffic inspection, and application control to protect the organization’s remotely accessed digital assets.
- Network and Security Operations: Fortinet Security Operations solutions deliver advanced OT threat intelligence to detect, prevent, and respond to sophisticated malware. It also helps achieve compliance and improve overall security awareness.
- The OT Security Service provides the capability to detect and protect against cyber threats by leveraging over 70 industrial protocols while enabling extensive visibility into industrial applications used in ICS environments.
- Fortinet Training Institute is dedicated to making cybersecurity training and new career opportunities available to everyone.
- FortiGuard Labs, Fortinet’s threat intelligence and research organization, develops and utilizes machine learning and AI technologies to provide customers with timely protection and actionable OT threat intelligence.

www.fortinet.com/OT ↗
OT@fortinet.com ↗



A Comprehensive Program for Securing OT

Keeping up with cybersecurity threats and exploitable vulnerabilities in your OT systems can be challenging, especially with constrained resources. Unlike IT assets, OT assets cannot be interrupted at will and are critical to safety processes and continuous operations.

Securing your OT systems amid constant cybersecurity threats, revised regulatory requirements, and evolving vulnerabilities can be daunting.

Our extensive experience in critical industrial environments ensures your cybersecurity needs are met. We offer end-to-end solutions, drawing from industry-leading data sources and best practices.

Whether you need help with conducting an asset inventory, prioritizing vulnerabilities to address, implementing a remediation plan, or support with cybersecurity services, we're here for you.

Count on it.



© 2023 Framatome. All rights reserved.



Check out our cybersecurity solutions
Contact us: cyber-services@framatome.com

Framatome Cybersecurity, a solutions line of Framatome, offers solutions to protect IT and OT systems in critical sectors like energy, defense, transportation, and public administration. Framatome leverages its experience as a global leader in the nuclear industry to develop solutions to protect IT and OT technologies for critical industries and assets.

With over 800 global customers using Framatome Cybersecurity, its commitment is to strengthening resilience against cyber risks while meeting sovereignty requirements with the following products and services:

- **Asset and Vulnerability Management:** a simple and complete platform to consolidate IT and OT asset inventory, manage vulnerabilities, and enhance cybersecurity posture.
- **Patch Analysis and Acquisition:** a single source for patch data to lower patch management, operational expense, improve cybersecurity posture, and simplify compliance programs.
- **Secure Patch Delivery:** securely receive signed and verified patches through secure delivery channels when needed and where it is needed.

The company's experts are also available to provide patch validation before installation apart from delivering deployment assistance.

- **Cybersecurity services:** Its portfolio of services covers security (review, design, and implementation consulting), vulnerability and patch management (advisory service and program buildouts) hardening (system, infrastructure, and asset) risk assessment, compliance to standards and norms (NERC CIP, NEI/NRC, NIST, TSA).
- **TAG4TRUST:** detects and manages physical intrusions on I&C systems, ensuring the integrity of I&C equipment helping plant operators detect unauthorized access attempts and maintain secure operations.

With 30 years of experience in OT security, Framatome Cybersecurity has a pragmatic approach to help customers improve their cybersecurity posture and grow in maturity, with an approach called the 'Virtuous loop.' This comprehensive program includes consolidating, identifying, prioritizing, and remediating, for securing operational technology (OT). This continuous cycle ensures the resilience of OT systems against cyber risks.

www.framatome.com

cyber-services@framatome.com





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 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



Honeywell

Honeywell provides IT/OT cybersecurity solutions that help protect critical infrastructure and IIoT technologies worldwide. Solutions are vendor-neutral, supporting

both Honeywell and non-Honeywell assets and deliver an integrated solution to operational technology (OT) cybersecurity.

OFFERINGS:

- **Honeywell Forge Cybersecurity Suite** helps to simplify, scale, and strengthen OT cybersecurity at a single site or across an enterprise. It comes with passive and active methods built for industrial operations.
- Honeywell's highly skilled OT cybersecurity consultants can provide **services** to support the cybersecurity lifecycle from start to finish, from risk assessments to remediation to incident response. The company's portfolio includes cybersecurity software, managed security services, industrial security consulting, and integrated security solutions.

www.honeywellforge.ai/us/en/solutions/ot-cybersecurity



KPMG International

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.

OFFERINGS:

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.

www.home.kpmg

Securing OT: Identify, evaluate and prioritize risk

PAS Cyber Integrity® delivers the risk-based data and insight needed to make your operations safer and more resilient.

hexagon.com/ICScybersecurity



Hexagon's PAS OT Integrity™ platform is a proven asset and vulnerability management security solution designed to address the unique needs of critical infrastructure systems. It supports ICS automation engineers and security professionals in identifying, evaluating, and prioritizing cybersecurity risk that exists within the industrial facility. The risk scoring methodology provides enhanced risk and operational context by determining the criticality of assets. This additional context is determined through Hexagon's deep inventory and ICS/OT system knowledge.

The platform also enables the rapid recovery and restoration of the industrial control system by providing a known good, trusted restore point in the event of unplanned downtime because of an operational or cybersecurity incident.

OFFERINGS:

PAS Cyber Integrity® – Inventory: Provides unmatched industrial control systems discovery and topology mapping down to Level 0 devices without passive network detection limitations and active network polling risks. Cyber Integrity creates a comprehensive inventory of all hardware, software and firmware components used in the OT environment and provides asset characteristics about each asset, such as make, model, version, serial number, location, and function.

PAS Cyber Integrity® – Vulnerability Management: Identifies and assesses vulnerabilities hidden in industrial infrastructure and determines where risk resides. The solution determines the severity of vulnerabilities, including enhanced context specific to your environment and provides remediation recommendations on how to resolve issues.

PAS Automation Integrity™ – Configuration Management: Baselines and tracks ICS configurations enabling automated change management. With Automation Integrity, you can visualize complex configurations and interdependencies between disparate systems and establish consistency across assets while benchmarking, replicating, and scaling control schemes enterprisewide.

Consulting Services: Policy Review and Development; Security Maturity Assessments; OT Cybersecurity Threat, Evasion, Response and Tactical Training; Governance, Risk, and Compliance Assessments; Security Strategy, Roadmap, and OT/IT Convergence support services.



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.

OFFERINGS:

OT security strategy, risk and compliance: Clients can evaluate existing security governance against business requirements, including PCI, security, identity and IT regulatory compliance.

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.

IBM QRadar: This helps clients gain actionable insights, identify the top threats and reduce the total alert volume. The IBM QRadar Security Intelligence Platform offers automated analytics for detection and investigation and search-based threat hunting tools designed to analyze and sort through a range of logs, events, and network flows.

X-Force Red ICS testing: Clients can build and test industrial control system attack scenarios to disrupt the attack chain.

IBM X-Force Exchange is a cloud-based threat intelligence sharing platform enabling users to rapidly research the latest security threats, aggregate actionable intelligence, and collaborate with peers.

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.

www.ibm.com

info@ibm.com

+1 (800) 426-4968



Mandiant

Mandiant works on making every organization secure from cyber threats and confident in its readiness. It delivers dynamic cyber defense solutions by combining services and products powered by the company's expertise, intelligence, and technology.

OFFERINGS:

- A variety of services focused on ICS and OT with three key areas – consultation and assessment, intelligence, and managed detection and response. The company's experts have worked in almost every industry utilizing ICS and understand the nuances and context each different field requires.
- Mandiant leverages the company's intelligence to inform its services of the latest attacker methods and techniques, and uses its experience in ICS/OT incident response to further enrich the intelligence.

www.mandiant.com

pshaver@google.com



Mocana

The Mocana TrustCenter operations platform provides a tamper-resistant and scalable workflow for transferring ownership and lifecycle management.

Mocana TrustEdge is a comprehensive software solution for IoT device protection.

The Mocana TrustCore development platform empowers application developers with a simple set of APIs to leverage data privacy and protection controls for safety, security, and compliance.

www.mocana.com

sales@mocana.com

+1 (415) 617-0055



Trustworthy OT Asset Data is the Bedrock of OT Security and Compliance

Achieve deeper-level asset data and vital endpoint information, along with historical context and change detection with **Industrial Defender**.



OT Asset Management

Inventory and manage all OT hardware and software details



Configuration & Change Management

Ensure secure configuration; detect changes from known good baselines



Vulnerability Management

Assess vulnerabilities and manage patching and mitigation efforts



Policy Compliance

Automated reporting for assessing against frameworks (e.g. NIST, NERC-CIP, IEC 62443, etc.)

Our integrated data collection approach is proven to be operationally safe and effective for managing even your hard-to-reach and/or offline assets.

[Manual Ingestion](#)[Passive Monitoring](#)[Native Polling](#)[Agentless](#)[Agent](#)[Direct Database](#)[INDUSTRIALDEFENDER.COM](https://www.industrialdefender.com)

Industrial Defender delivers the OT asset data needed to protect industrial operations.

The Massachusetts, USA-headquartered company, established in 2006, is trusted by industrial organizations and critical infrastructure operators around the world.

Industrial Defender provides deeper-level asset data, vital endpoint information, historical context, and change detection for addressing cyber risks across the OT environment. Industrial organizations leverage Industrial Defender's platform as a single source of truth for all operational asset information, enabling them to achieve key goals in OT asset management, change and configuration management, vulnerability management, and policy compliance.

Industrial Defender serves customers globally across all OT-intensive sectors, including manufacturers, power utilities, oil and gas, and other critical infrastructure operators. Building upon a strong heritage of NERC CIP compliance solutions, Industrial Defender's expanded set of OT data capabilities supports the safety, availability, and security of critical operations.

PLATFORM CAPABILITIES:

- OT Asset Management: Inventory and manage all OT hardware and software details
- Configuration Management: Ensure secure configuration; detect changes from known good baselines
- Risk-Based Vulnerability Management: Assess vulnerabilities and intelligently prioritize patching and mitigation efforts based on risk
- Compliance Management: Automated reporting for assessing against frameworks and auditing

Industrial Defender has been safely deploying active methods since 2006, as part of an integrated approach for gathering the most comprehensive data. Combining active and passive methodologies, operators can manage even the most hard-to-reach assets.

- Manual Data Ingestion
- Passive
- Active
- Agent-Based
- Agentless Monitoring
- Native Polling
- Direct Database Integration

www.industrialdefender.cominfo@industrialdefender.com



Keeping you updated

It's our mission to keep you informed of the rapidly changing industrial cybersecurity landscape. Benefit from minimized risk, maximized productivity, and optimized decision-making with our valuable insights.

Our market research has earned a global reputation for its precision, quality, and practicality.

Discover why today

We're excited to share this exclusive offer with all Industrial Cyber readers. Secure a special discount on any of our Decision Point Reports or Vendor Research today.

coupon code

INDCYBG24

checkout to take
advantage
of this offer.



Nozomi Networks is the leader in OT and IoT cybersecurity, delivering exceptional network and asset visibility, threat detection, and AI-powered insights. Critical infrastructure, organizations worldwide rely on Nozomi to minimize risk while maximizing resilience.

OFFERINGS:

The Nozomi platform is designed for scalability and centralized management. It uses AI to streamline tasks and provides deep insights and root cause analysis to quickly detect and prioritize vulnerabilities, threats and anomalies.

Vantage & Vantage IQ

Vantage scales security monitoring and visibility for large multi-site enterprises, with the cost benefits and flexibility of a cloud-hosted solution. It unifies visibility, threat detection and security monitoring for an unlimited number of nodes and systems. Vantage IQ provides AI-assisted data analysis, helping security teams reduce cyber risk and speed response.

Guardian

Guardian sensors collect and analyze operational data on-premises, including visibility for OT and IoT networks and assets. They detect cyber threats and vulnerabilities, providing situational awareness that is critical for ensuring security, compliance and continuity.

Arc

The Arc endpoint sensor is an EDR solution that provides detailed asset visibility and continuously monitors individual host attack surfaces and activity. Arc can easily identify compromised hosts, rogue applications, unauthorized USB devices and suspicious activity.

Guardian Air

Guardian Air is the industry's first wireless security sensor for OT and IoT. It monitors activities from all prominent wireless frequencies, providing visibility to connected assets and attack surfaces.

Threat Intelligence

Available for use with the Nozomi platform and other third party cybersecurity platforms, Nozomi's Threat Intelligence offers up-to-date information on malicious IP addresses or URLs, IOC signatures, threat sources, malware hashes, and methods and tactics to gain system access.

www.nozominetworks.com ↗

info@nozominetworks.com ↗



NanoLock Security

NanoLock Security protects manufacturing companies and utilities against external and insider cyber attacks impacting OT and production, as well as against human errors, and supply chain threats. Empowering industrial leaders with device-level, zero-trust OT cybersecurity solutions, NanoLock Security minimizes production downtime and eliminates operational risks.

Trusted by global industrial customers, NanoLock OT Defender protects Programmable Logic Controllers (PLCs) of all ages, both new and legacy from all vendors. It authenticates and authorizes every access or change request, offering the complete device, user, and group policy management, centralized audit trails, and compliance with international standards.

www.nanolocksecurity.com

info@nanolocksecurity.com



Network Perception

Network Perception's NP-View is a lightweight, non-invasive OT network visualization platform. The platform efficiently parses network device configuration files to deliver comprehensive insights, including network topology maps, data flow diagrams, and access rule analysis. These reports provide organizations with clear visualization and understanding of their network to swiftly pinpoint high-risk configurations and ensure compliance with policy, thereby reducing critical asset exposure and eliminating misconfigurations.

Designed for on-premise use, NP-View operates offline requiring no changes to the network, ensuring zero risk to operations. Its ease of deployment and user-friendly functionality make it the fastest path to comprehensive OT network visibility and verification.

<https://network-perception.com>

marketing@network-perception.com



NTT

NTT's Intelligent Cybersecurity services help clients create a digital business that is "Secured by Design." With enhanced threat intelligence, NTT can predict, detect and respond to cyber threats while supporting business innovation and managing risk.

OFFERINGS:

Cybersecurity Advisory Services: NTT has a dedicated team of OT cybersecurity consultants globally.

IT-OT Threat Monitoring & Response: This is a 24x7 SOC-delivered service that monitors and responds to IT and OT network threats.

IT-OT Managed Security Services: 24x7 SOC-delivered service that covers a client's end-to-end cybersecurity operation.

Global Technology Services: Delivered by NTT's technical experts, the services deliver in-depth design workshops, supply industry best-of-breed technology, and deploy solutions globally.

www.services.global.ntt

sales@global.ntt



Opswright

Opswright is passionate about injecting security into the engineering domain to achieve secure by design and by default for critical infrastructure. By leveraging Opswright Impact software platform, the company embeds the principles of Cyber Informed Engineering into the engineering process, empowering any engineer to design safe and secure systems for critical infrastructure.

Opswright's software supports the needs of engineering firms and asset owners. It is also aligned with industry guidance, such as the Security Engineering Maturity Matrix, IEC 62443, and others. Founded in Space Coast

Florida, all development is U.S.-based and aligned to NIST 800-218 practices for secure development.

www.opswright.com

sales@opswright.com



OPSWAT.

Protecting the World's
Critical Infrastructure

OPSWAT offers IT and OT/ICS critical infrastructure protection cybersecurity solutions and deep content disarm and reconstruction (CDR), protecting organizations from malware and zero-day attacks. Its solutions safeguard public and private sector organizations with the latest technology, processes, and hardware scanning to secure the transfer of data, files, and device access across critical networks; ensure compliance with policies and regulations; and protect their reputation, finances, employees, and customers from cyber-driven disruption.

Built on the company's 'trust no file, trust no device' philosophy, and integrated by design, OPSWAT works to solve customers' challenges with critical lines of defense across every level of their infrastructure. Its comprehensive platform is underpinned by patented, foundational technologies that are trusted worldwide to secure critical environments. These purpose-built technologies provide advanced cyberthreat prevention against known and unknown threats, zero-day attacks, traditional and AI-based malware, and more.

OPSWAT's MetaDefender Platform offers a comprehensive threat prevention solution that allows for the seamless integration of advanced malware prevention and detection features into current IT/OT solutions and infrastructure. This integration enhances the ability to address common attack vectors both in the cloud and on-premises, safeguarding web portals from malicious file uploads, securing email communications, protecting against threats from peripheral media, ensuring supply chain security, and more.

With this one-platform approach, OPSWAT simplifies defense-in-depth cybersecurity challenges, reducing time, effort, cost, and most importantly, risk.

The patented technologies and modules that power MetaDefender Platform include deep content disarm and reconstruction (Deep CDR), multi-scanning with 30+ AV engines, Software Bill of Materials (SBOM), country of origin detection, proactive data loss prevention (proactive DLP), next-generation sandbox, file-based vulnerability, threat intelligence, usability designed for OT, deep endpoint compliance, vulnerability management, patch management, advanced endpoint protection, and secure access.

www.opswat.com

sales-inquiry@opswat.com



Perygee Inc.

Perygee offers a cyber-physical security platform that enhances operational efficiency by consolidating data, safeguarding assets, and automating critical workflows. The company addresses the challenges of securing IoT/OT environments, recognizing the limitations of traditional security practices in these settings.

Founded by a former NSA mathematician, Perygee provides a no-code/low-code automation platform tailored for industrial organizations. It focuses on automating security and IT tasks related to OT and IoT devices, enabling cyber and IT leaders to enhance system security and streamline operations. It also helps solve various use cases, including IAM, asset management, device security, and onboarding/offboarding of people and organizations.

www.perygee.com

hello@perygee.com



PwC

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 IAM security.

OFFERINGS:

ICS risk assessments: The assessment covers system records and activities to determine the adequacy of system controls.

ICS vulnerability assessment /penetration testing: This evaluation 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



Radiflow

Radiflow is a global provider of security solutions and services that protect cyber-physical systems in critical infrastructure and industrial automation. With broad and deep OT cyber experience, the company enables OT operators to safeguard their processes while managing risk, optimizing the security budget, and complying with regulations and best practices.

Radiflow security solutions are deployed at more than 8000 sites worldwide in more than a dozen major industries and include:

- iSID threat detection
- iCEN centralized cybersecurity management
- CIARA data-driven, continuous risk management

Employing its - solutions, Radiflow also offers Managed Detection and Response (MDR) and risk management services.

www.radiflow.com ↗

Daniela_s@radiflow.com ↗



Rhebo

Rhebo delivers offerings that help with the cybersecurity and operational stability of the ICS and IoT infrastructure in energy, industrial, and water companies. Using its industrial network monitoring solution with anomaly detection and its services, the Leipzig, Germany-based company, can monitor all communication within the ICS and reliably report any attacks, vulnerabilities, and technical error states.

Rhebo directly supports operators of ICS to increase cybersecurity, productivity, and availability of their systems.

www.rhebo.com ↗

info@rhebo.com ↗



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](tel:+14406463434) ↗

RMC provides industrial cybersecurity solutions, safeguarding the essential services that power our tomorrow



Industrial Cybersecurity Solutions for Critical Infrastructure and Critical Missions

— rmcglobal.com —



RMC provides risk management and industrial cybersecurity solutions and services for critical infrastructure and critical missions. RMC believes that resilience depends on minimizing and managing the increasing risks facing the critical infrastructure and industrial systems that support the country, companies, and civilization.

RMC was purpose-built for mission assurance and ICS/OT cybersecurity, dedicated to strengthening and protecting government and commercial assets. Its expertise is in critical infrastructure environments, especially in high-value government facilities and private-sector industries, such as electrical utilities, other energy providers, and manufacturing.

RMC combines its decade of full-lifecycle mission assurance and risk management solutions with expertise in industrial cybersecurity to protect the country's most vital assets. Operating worldwide, RMC provides its clients with the analysis, assessments, strategy, and remediation required to protect personnel, facilities, networks, and critical infrastructure.

OFFERINGS:

Risk & Vulnerability Assessments to inform security investment decisions and increase cyber resilience

Penetration Testing of networks, devices, and applications to ensure that security controls can withstand the most advanced cyber adversaries

Governance, Risk & Compliance to provide organizations the guidance needed to achieve, maintain, and prove compliance, irrespective of the framework (IEC 62443, NIST 800-82, NERC CIP, and more)

Cyber Engineering, Design & Remediation to build cybersecurity into the environment from the outset and to help mitigate vulnerabilities while keeping industrial processes up and running throughout

www.rmccglobal.com ↗

sales@rmccglobal.com ↗



Schneider Electric

SE 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.

OFFERINGS:

Cybersecurity Consulting: SE'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 SE control, safety, and 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 ↗



Seckiot

SECKIOT's mission is to enhance the safety and availability of cyber-physical systems. The company provides a European solution to secure industrial and IoT systems.

- OT Cybersecurity Map: providing 100 percent visibility to eliminate grey areas that are conducive to cyber-attacks (equipment inventory, network architectures, real flow matrix, segmentation control, weakness detection, event logging).
- OT Threats and Anomalies Detection: detecting cyber-attacks so that we can stop them before they materialize (IoCs, signatures, risky behavior, behavioral analysis based on machine learning).

The company helps strengthen the immunity of industrial and XIoT networks and safeguard critical infrastructures.

www.seckiot.fr ↗
contact@seckiot.fr ↗



Secret Double Octopus

Secret Double Octopus offers a passwordless MFA solution designed to meet enterprise authentication requirements. This solution covers a wide range of needs, including workstations, SSOs, on-premises infrastructure, and legacy applications.

By eliminating the need for employees to manage passwords and providing a secure yet user-friendly interface, the Octopus passwordless MFA enhances security. It removes vulnerable passwords from user logins, employs a phishing-resistant MFA workflow, and reduces the attack surface by preventing attackers from exploiting passwords and phishing users.

Additionally, the Octopus passwordless MFA integrates with existing password directories, delivering the benefits of passwordless MFA without the added costs, risks, or delays associated with recoding apps or rearchitecting the identity infrastructure.

www.doubleoctopus.com ↗

sales@doubleoctopus.com ↗



Tempered Network

Tempered offers secure connectivity for vital infrastructure, industrial control systems, and the industrial Internet of Things (IIoT). Tempered Networks' solutions are used by a range of sectors, including water, energy, petroleum, manufacturing, and other industries

OFFERINGS:

The **Airwall** solution delivers network segmentation and secure remote access. Airwall is a zero-trust software-defined perimeter that provides multi-factor authentication, comes micro-segmented, encrypted end-to-end, and is impervious to lateral movement.

Airwall Teams allows users to build truly private system-to-system networks that span public, private, cloud, and mobile networks, with just a few clicks using an intuitive graphical interface.

www.tempered.io ↗

info@tempered.io ↗

[+1 \(206\) 452-5500](tel:+12064525500) ↗



SecurityRisk ADVISORS

Security Risk Advisors (SRA) is a computer and network security company providing cybersecurity consulting and managed security services.

Its cyber-physical systems security practice provides advisory architecture, engineering, and operations support throughout OT/IoT/IoMT/IIoT/robotics security programs. The company works to collaboratively execute cyber-physical systems security programs and initiatives using its industry experience, cross-vertical best practices, and technical subject matter expertise.

Its team of specialized practitioners brings strategy, assessment, enablement of trusted technology solutions, and 24x7 managed security service provider (MSSP) capabilities.

SRA offers purple teams, cloud security, penetration testing, cyber-physical systems security, and 24x7x365 cybersecurity operations. Based in Philadelphia, SRA operates across the USA, Ireland and Australia.

OFFERINGS:

- **Testing and Purple Teams:** Penetration testing, hardware assessments, and a collaborative, programmatic approach to measuring and increasing security visibility in alignment with MITRE ATT&CK for ICS
- **Risk Assessment:** ISA/IEC 62243 and NIST-based security risk assessments for sites and global entities
- **Strategy and Framework:** Defense-in-depth strategy and architecture to address the unique security risks of cyber-physical systems assets and environments with ISA/IEC 62443 and NIST inputs
- **Controls and Solution Enablement:** Development of vendor-agnostic security controls and deployment of visibility, secure remote access, network isolation, access management, removable media protection, and Software Bill of Materials (SBOM) solutions
- **24x7 OT/IoT Security Monitoring and Response:** Monitoring and response with a turnkey analytics ecosystem that can intake OT/IoT security solution data.

www.sra.io ↗

info@sra.io ↗



SIEMENS

Siemens Critical Infrastructure Defense Center (CIDC) is a customer-facing cybersecurity competency established to assist critical infrastructure industries to improve and mature their cybersecurity program and resiliency to cyber-attacks. Its team of cyber experts will support Canada's cyber and physical security needs and projects in the US, Europe, and the Middle East while delivering a holistic approach to cybersecurity and covering the entire security lifecycle.

OFFERINGS:

- **Cybersecurity Assessments:** A variety of cybersecurity assessments to help organizations understand their cybersecurity programs relative to baselines and different frameworks such as ISA/IEC 62443, NIST CSF, and NIST SP 800-82.
- **Security Strategy and Roadmap Development:** Develop a future-proof multi-year security strategy and an implementation roadmap as the output of cybersecurity assessments.
- **Program Management:** Provide comprehensive, integrated program management of security strategy, project and risk management, and security services planning.
- **Critical Infrastructure Security Operations Center (SOC):** The Critical infrastructure SOC monitors and protects the OT network and infrastructure of critical infrastructure and large manufacturing. It delivers automated real-time monitoring of core OT and related IT security events, along with automated detection of security outliers by observing deviations from known good baseline. The SOC also provides 24 /7 security monitoring, security event triage, analysis, alerting, and incident response support.
- The company's **services** range from advisory, managed security, and research services, with the singular mission to secure customers' OT infrastructure. Its managed security services consist of services that enable customers to detect, prevent, respond and recover from cybersecurity threats.

www.siemens.ca/cidc ↗

cidc.ca@siemens.com ↗



Thales Group

Thales offers a comprehensive, long-term approach that helps operators implement the security policies they need to protect critical information systems.

OFFERINGS:

CERT: To anticipate detection of cyberthreats, Thales offers tailored intelligence on vulnerabilities, threats and attacks of common hardware and software components.

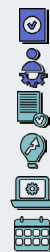
Consulting: Thales provide cyber consulting to critical infrastructures in order to address the challenges of regulatory compliance, implementation of security from design, risk assessment and penetration testing.

Rapid Response Team: Thales has a rapid response team with on-site intervention capacity, made up of multi-disciplinary specialists.

SOC: Thales' security experts ensure security information and event management flow in real-time from its CSOCs located around the world.

www.thalesgroup.com ↗

[+33 \(0\) 1-57-77-8000](tel:+330157778000) ↗



ThreatGEN

ThreatGen is a game-based cybersecurity simulation platform that combines the power of an actual computer gaming engine and active adversary simulation AI to provide the most practical and effective way for anyone to learn cybersecurity, from beginners to experts, and even leadership. The ThreatGEN Red vs. Blue portal is web browser delivered and provides access to the cybersecurity simulation platform, on-demand courses, labs, and scenarios.

www.threatgen.com ↗

sales@threatgen.com ↗



Veracity Industrial Networks

Veracity Industrial Networks provides a robust and secure approach to OT network management. Their SDN solution, tailored for the OT environment, centrally manages the network based on specific rules to enhance visibility and security for all communicating endpoints, streamlining network management processes.

OFFERINGS:

The Veracity OT Network Controller uses automated network segmentation with self-healing capabilities to manage cyber risk.

Veracity leverages SDN functionality to protect east/west and north/south traffic, while delivering enhanced resiliency by eliminating firewall configuration issues, loopbacks, and manual IP address updates.

The Veracity OT Network Management Platform is a secure-by-default network that moves beyond the detection and alerting of cyber events into a resilient network that reduces the attack surface by design.

www.veracity.io ↗

jason.weber@veracity.io ↗



Keeping you updated

It's our mission to keep you informed of the rapidly changing industrial cybersecurity landscape. Benefit from minimized risk, maximized productivity, and optimized decision-making with our valuable insights.

Our market research has earned a global reputation for its precision, quality, and practicality.

Discover why today

We're excited to share this exclusive offer with all Industrial Cyber readers. Secure a special discount on any of our Decision Point Reports or Vendor Research today.

coupon code

INDCYBG24

checkout to take advantage of this offer.





Keep the Operation
Running

OT Cybersecurity. Simplified.



txone.com



TXOne Networks aims to protect cyber-physical systems (CPS), the essential components for OT environments. By integrating with existing business processes, TXOne delivers practical security without interrupting operations. TXOne advocates the OT Zero Trust framework by protecting assets in their entire lifecycle.

The latest asset-centric Detection and Response (CPSDR) innovations create a unique value for the entire OT space and bring security level and visibility to a new height. With OT priorities in mind, TXOne Networks is a valuable partner in optimizing OT business processes.

OFFERINGS:

Security Inspection:

The Element product family enables installation-free security capability that both ops and security teams can use. Integrating with existing procedures, this product line aims to inspect new equipment before moving it to production, as well as all removable storage media. It performs regular audit and inventory management functions and provides advanced security for out-of-band and isolated devices.

Endpoint Protection:

The Stellar product line integrates with individual devices, becoming a native extension to their base functionalities. It defends modern and legacy devices by actively preventing unauthorized changes to baseline operations at an application and process level without interrupting normal operations.

Network Defense:

The Edge product family introduces stability and resilience across OT networks. It regulates traffic and operational commands between devices. Industry-informed protocol analysis techniques apply prevention, detection, and remediation functions to reduce the impacts of incidents and promote operational stability.

CPS Protection Platform:

SageOne aggregates security intelligence from the entire TXOne portfolio. It's also a cross-product mission control center with the capability to discover potential unknown risks with AI-driven security insights from multiple security control points of different angles.

www.txone.com

info@txone.com



Velta Technology is a leading cyber solution provider in the industrial space. They help integrate digital safety solutions, expertise, and tools, with the current environment and existing technologies. They understand the differences between industrial and IT infrastructures, and the toolsets required to secure them.

Velta Technology bridges the gap in expertise and understanding from industrial assets from the plant floor to the enterprise. They provide mitigating and compensating controls for digital safety and support organizations with industrial IoT and OT/IT convergence. They help protect the industrial environment with multi-disciplinary industrial manufacturing and critical infrastructure experts.

OFFERINGS:

Tabletop Exercise – They help facilitate important OT / IT discussions to strengthen internal communication and security ownership across industrial assets and operations.

Visibility Study Program – A three-week program to identify the top vulnerabilities unique to one's industrial environment.

CDV Index – Measure real-time risks and vulnerabilities of all connected devices within an industrial facility over time to accurately gauge risk and potentially defend insurance rates or claims.

OT Monitoring Optimization – Optimize the value and benefits of your cybersecurity platform with our OT security platform optimization. Velta Technology serves as an extension of the in-house team offering hands-on expertise, knowledge and best practices.

Secure Remote Access (with Audit Trail) For Industrial Environments – Minimize risk of remote users and the industrial environment.

Industrial Endpoint Protection – Secure existing industrial networks with an impenetrable barrier.

SenseR Ready Panel Program – Build and install industrial panels Digital Safety Ready with the latest cybersecurity technology. Eliminate expensive retrofit costs down the road.

www.veltatech.com

asktheexperts@veltatech.com



Wallix

WALLIX specializes in digital identity, access, and governance security solutions, assisting over 3000 organizations in securing their digital transformation. Their technologies address data protection challenges, ensuring detection and resilience against cyberattacks for business continuity. Additionally, they facilitate compliance with regulatory requirements for accessing OT and IT infrastructures.

With a global network of over 300 resellers and integrators, WALLIX provides OT Security solutions under the brand OT.security. The brand focuses on secure remote access to cyber-physical systems (CPS) security.

OT.security by WALLIX offers purpose-built solutions for ICS, leveraging expertise and software certified by the French National Cybersecurity Agency to deliver optimal security while accommodating production constraints. OT.security solutions safeguard vulnerable OT environments without disrupting industrial and business operations.

www.ot.security

marketing@wallix.com



Wipro

Wipro recognizes that OT security is the key enabler to enterprise adoption of Industry 4.0. The company's approach is to blend its technical engineering heritage with a new business-focused consulting approach to deliver successful transformation and business continuity.

The recent attacks on the OT networks have alerted business stakeholders to the potential impact of cybersecurity incidents on reputation and revenue. Governments are enforcing regulatory compliances making it mandatory for companies to report breaches to the authorities. As a result, OT cybersecurity is transitioning away from siloed engineering supervision to management by IT and OT teams' collaboration.

www.wipro.com



Xage is on a mission to protect the world's critical operations. It provides a unified identity and access management solution with secure enforcement for any user, device, or data across IT, OT, and cloud. The Xage solution can be deployed across any type of asset – from modern data centers and cloud workloads to legacy devices and applications – all without installing a single agent. Xage is hyper-resilient and has been tested and validated in some of the most complex, distributed, brittle environments.

Xage delivers access and protection that's easy to deploy, easy to manage, and easy to use, while preventing attacks at every stage of the MITRE ATT&CK framework. –With Xage, critical operations can eliminate disjointed solutions that make the enterprise more complex and less secure. It also protects the entire environment without compromising on agility, usability, or security.

OFFERINGS:

- **Zero Trust Access & Protection:** Xage Zero Trust Access & Protection is available either wholly on-site or via the cloud with additional on-site enforcement. It can be deployed across any type of asset to provide user-to-machine/app as well as machine-to-machine access control and policy enforcement with no agents.
- **Zero Trust Remote Access:** Xage Zero Trust Remote Access enables granular secure access to modern and legacy assets across OT, IT, and the cloud. Enable secure and privileged access to any device or application from anywhere with an easy-to-use browser-based solution. Eliminate workforce burden by equipping employees and third parties to collaborate in real-time via a virtual operation center.
- **Zero Trust Data Exchange:** Xage Zero Trust Data Exchange enables end-to-end security across the entire data ecosystem, from physical machines through edge analytics to shared cloud-based data lakes. Share data securely across multiple parties and domains with complete assurance of data authenticity, integrity, privacy, and access control.

www.xage.com ↗

hello@xage.com ↗



Shield your Enterprise. Seize your Mission.

Zero Trust Access and Protection for Critical Environments

www.xage.com



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 ICS security services ensure plant safety and security by providing a comprehensive program which focuses on cybersecurity lifecycle management.

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.

OFFERINGS:

- Cybersecurity Awareness Training
- Industrial Cyber Security Risk Assessment
- Cyber Security Policies and Procedures
- Operational Technology Architecture Design
- Plant Security Managed Services

www.yokogawa.com/cybersecurity ↗



ABOUT TAKEPOINT

Takepoint Research (TPR) is a boutique industry analyst firm that provides focused research and actionable insight for industrial enterprises and those tasked with protecting them from cyber threats. TPR resources and analysis help them make informed decisions about evolving their industrial cybersecurity programs to meet the changing threat landscape. 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.