# **Cyber and IT Security Investment Opportunities for Spectrum Safety Solutions**

Spectrum Safety Solutions, established in July 2024 through the consolidation of prominent brands Autronica, Det-Tronics, Fireye, and Marioff, stands as a global leader in providing specialized safety solutions. Operating within the critical infrastructure, energy, and marine sectors, Spectrum caters to clients in high-hazard and mission-critical environments worldwide 1. The unification of these established entities under a single banner signifies a strategic move to leverage their collective expertise and market presence, offering a comprehensive suite of advanced lifecycle solutions and services 2. This consolidation phase presents a unique juncture to analyze and address the evolving cybersecurity landscape, particularly concerning the integration and standardization of their IT and operational technology (OT) infrastructure.

### **1. Strategic Initiatives Requiring OT and IT Security**

While Spectrum Safety Solutions' website at spectrum-safety.com does not explicitly detail ongoing digital transformation initiatives, an examination of broader industry trends and related information suggests several potential programs that would necessitate enhanced security measures. Given Spectrum's focus on critical infrastructure and hazardous environments, the implementation of remote asset monitoring is a highly probable strategic direction 6. Such initiatives, common in industries managing geographically dispersed assets, allow for real-time oversight and proactive maintenance of fire detection and suppression systems. However, the integration of remote monitoring capabilities introduces significant OT security considerations, demanding secure communication protocols, robust data encryption to safeguard sensitive operational information, and stringent access controls to prevent unauthorized intrusion [Insight 1.2]. The interconnected nature of these systems means any vulnerability could be exploited, potentially leading to the manipulation or disruption of critical safety functions.

Furthermore, Spectrum may be exploring the integration of Artificial Intelligence (AI) and Machine Learning (ML) into their operational workflows 6. These technologies hold the potential to enhance predictive maintenance capabilities for their systems, allowing for early detection of potential failures and optimized performance. AI and ML could also be leveraged for advanced threat detection within their own IT and OT environments, identifying anomalies and potential cyber threats more effectively. Nevertheless, the incorporation of AI/ML into safety-critical systems mandates careful validation and robust security protocols [Insight 1.3]. The integrity of the algorithms and the security of the data they rely upon are paramount to ensure the reliability of these systems and to prevent malicious actors from manipulating them for nefarious purposes.

The trend of Cloud-OT integration is also gaining traction across industrial sectors, and Spectrum Safety Solutions may be considering leveraging cloud platforms for data analytics, remote management, and the delivery of enhanced services 6. Connecting OT systems to the cloud offers benefits such as scalability and accessibility but simultaneously expands the attack surface [Insight 1.4]. A comprehensive cloud security strategy tailored specifically for industrial environments is essential to address the unique challenges associated with this integration, including secure data transfer, robust access management, and protection against cloud-specific threats.

Enhancing the digital customer experience is another area where Spectrum might be focusing its efforts 9. This could involve the development of more sophisticated customer portals, the provision of online technical support, and the offering of digital services related to their safety solutions. Securing these customer-facing digital platforms is of utmost importance to protect sensitive customer data and to maintain the trust that is paramount in the safety industry [Insight 1.5]. Data breaches in these systems can lead to significant reputational damage and potential regulatory penalties, underscoring the need for robust authentication mechanisms, data encryption, and ongoing security monitoring.

Moreover, the adoption of Industry 4.0 principles is transforming manufacturing processes globally, and Spectrum's Det-Tronics brand is explicitly engaged in "Factory Digital transformation / Factory 4.0 projects" 10. This modernization likely involves increased automation, the integration of Industrial Internet of Things (IIoT) devices, and the utilization of advanced data analytics to optimize production. The ongoing digital transformation within Det-Tronics' manufacturing operations presents a direct and immediate requirement for securing industrial control systems (ICS) and operational technology (OT) environments [Insight 1.6]. Interconnected systems on the factory floor are increasingly vulnerable to cyberattacks that could disrupt production, compromise intellectual property, or even impact the integrity of the safety products themselves.

Given the mission-critical nature of Spectrum's business in high-hazard environments, strong operational resilience programs are undoubtedly a priority. These programs likely encompass investments in redundant systems, comprehensive disaster recovery plans, and robust business continuity strategies. Cybersecurity must be an integral component of these operational resilience efforts [Insight 1.7]. Ensuring that systems can withstand and effectively recover from cyber incidents without compromising the safety and availability of their critical services is paramount. A cyberattack that cripples Spectrum's ability to deliver essential safety solutions could have severe and far-reaching consequences.

Furthermore, Spectrum Safety Solutions is likely aware of the overarching need for security enhancement programs 16. Snippet20's mention of Cybersecurity Maturity Model Certification (CMMC) suggests that Spectrum may be involved in contracts with the US Department of Defense, particularly given their presence in the marine and infrastructure sectors. This indicates a proactive approach towards meeting specific security standards. The general organizational awareness of cybersecurity needs further suggests that Spectrum is receptive to implementing more specialized OT and IT security measures tailored to their unique operational context and regulatory obligations [Insight 1.8].

The implementation timelines for these initiatives will vary depending on their scope and complexity. ICS modernization and large-scale digital transformation projects can span several months to years, requiring careful planning and execution. The scale of these initiatives will also depend on the specific brand and operational area within Spectrum. Crucially, these initiatives often involve critical infrastructure, including ICS/SCADA systems that are integral to the functionality of their products and potentially control their manufacturing processes 21. The long lifecycles and critical nature of these systems necessitate a phased and meticulously planned approach to security implementation, ensuring minimal disruption to ongoing operations [Insight 1.9]. Downtime in critical safety systems is simply not an option.

Among these potential initiatives, control systems upgrades, ICS modernization, cloud-OT integration, and any programs involving remote access to operational environments carry the highest security implications [Insight 1.10]. The "Factory Digital transformation / Factory 4.0 projects" at Det-Tronics also represent a high-risk area from a cybersecurity perspective. These initiatives represent the most immediate and critical areas where enhanced OT and IT security measures are essential, creating key opportunities for specialized vendors like NCC Group, Dragos, and Adelard to offer their expertise and solutions.

### **2. Current Security Vendor Assessment**

Based on the publicly available information, there is no direct evidence in the provided snippets regarding Spectrum Safety Solutions' current security vendor relationships. While Spectrum Enterprise, a separate entity, utilizes vendors like Cisco and Fortinet for its security offerings 16, it is unclear whether Spectrum Safety Solutions has similar arrangements. It is plausible that Spectrum Safety Solutions employs standard IT security vendors for general network and endpoint protection. However, given their recent formation in July 2024, it is unlikely that they have established publicly known or extensive relationships with dedicated OT security vendors such as Dragos, Nozomi, or Claroty [Analysis 2.1].

If Spectrum Safety Solutions primarily relies on traditional IT security vendors, this could present both advantages and potential vulnerabilities. An advantage might be existing relationships and a degree of familiarity with their IT infrastructure. However, a significant vulnerability likely exists in the security of their OT environments [Insight 2.2]. Traditional IT security solutions often lack the specialized capabilities required for the unique characteristics of OT systems. These include a deep understanding of industrial protocols, access to ICS-specific threat intelligence, and the ability to perform passive monitoring without disrupting sensitive operational processes 22. This gap in dedicated OT security expertise and tooling creates a clear opportunity for specialized vendors like Dragos, whose platform is built specifically for industrial cybersecurity, and for consulting services from NCC Group, which has a strong focus on OT security assessments and strategy. No public information about specific security partnerships or technology implementations by Spectrum Safety Solutions was identified within the provided snippets. Therefore, any further assessment of their current security posture at this stage relies heavily on competitive intelligence analysis and inferences based on industry best practices and the inherent security needs of organizations operating in critical infrastructure sectors.

### **3. Active Procurement Opportunities**

A review of the provided research material did not yield any specific publicly advertised Requests for Proposals (RFPs), Requests for Information (RFIs), or tenders related to OT security or cybersecurity for Spectrum Safety Solutions 26. Therefore, at this time, direct, publicly verifiable procurement opportunities are not evident [Analysis 3.1].

Information regarding Spectrum Safety Solutions' specific budget cycles and capital expenditure plans is not publicly accessible within these snippets. However, a broader analysis of industry trends reveals a significant and growing pattern of security investments within the infrastructure, energy, and marine sectors 28. This surge in investment is driven by an increasing awareness of the escalating cyber threat landscape targeting these critical industries, coupled with mounting regulatory pressures to enhance security postures. The recent formation of Spectrum Safety Solutions itself may act as a catalyst, prompting a comprehensive review and potential upgrade of their existing security infrastructure across the newly consolidated brands [Insight 3.2]. New organizations often prioritize establishing a robust and secure foundation for their operations.

While specific details on upcoming project phases and associated security investment budgets are not publicly available for all of Spectrum's brands, the identified "Factory Digital transformation / Factory 4.0 projects" within Det-Tronics represent a confirmed upcoming phase that will undoubtedly require security considerations and corresponding financial allocations 15. Furthermore, any future initiatives related to remote monitoring, cloud-OT integration, or the modernization of ICS will inherently necessitate security assessments, the implementation of protective measures, and thus, dedicated security investments. These digital transformation projects, particularly within Det-Tronics' manufacturing environment, constitute a tangible and near-term procurement opportunity for specialized OT security solutions and expert consulting services [Insight 3.3]. Security is not merely an add-on but a fundamental component of any successful digital modernization effort in industrial settings. This section primarily relies on market intelligence and the inference of opportunities based on identified needs and prevailing industry trends, as no verified procurement activities were found within the scope of the provided research.

### **4. Specific OT Security Challenges**

Spectrum Safety Solutions and their clientele operating within the infrastructure, energy, and marine sectors face a complex and evolving array of OT security challenges. Ransomware stands out as a significant and pervasive threat, increasingly targeting industrial control systems with the potential to cause severe operational disruptions and substantial financial losses 30. The energy sector, in particular, has emerged as a prime target for ransomware attacks 37. Given the critical nature of Spectrum's operations and the essential infrastructure their products protect, both Spectrum and their customers face a high risk of ransomware incidents that could compromise safety and business continuity [Insight 4.1]. Dragos' specialized expertise in defending against industrial ransomware is therefore highly relevant to addressing this critical challenge.

Nation-state actors also pose a significant threat to critical infrastructure, including the energy and marine sectors, with their sophisticated capabilities for espionage, sabotage, and disruptive cyber operations 30. Considering the vital role of Spectrum's products in safeguarding critical infrastructure, the organization and its clients are potential targets for these advanced persistent threats [Insight 4.2]. Disrupting fire detection and suppression systems could have far-reaching national security implications, making robust defenses against nation-state attacks paramount.

Supply chain attacks represent another growing concern, particularly within the interconnected energy sector 38. As a provider of critical safety solutions, ensuring the security and integrity of Spectrum's own supply chain is vital [Insight 4.3]. Compromised components or vulnerabilities introduced through the supply chain could have catastrophic consequences for the reliability and effectiveness of their safety systems.

Phishing and social engineering attacks remain prevalent and effective methods employed by cyber adversaries across all industries 31. These attacks often target employees to gain initial access to networks, highlighting the critical need for comprehensive employee training and awareness programs within both Spectrum and their client organizations to mitigate the risk of human error leading to security breaches [Insight 4.4].

In addition to these broad threat categories, Spectrum and their clients must also navigate a complex landscape of regulatory compliance requirements. In the marine sector, the US Coast Guard has recently issued a final rule establishing minimum cybersecurity requirements for the marine transportation system 47. This regulation mandates specific cybersecurity practices for US-flagged vessels, Outer Continental Shelf (OCS) facilities, and facilities subject to the Maritime Transportation Security Act (MTSA). Key requirements include the development and maintenance of a Cybersecurity Plan, the designation of a Cybersecurity Officer, and the implementation of various technical and organizational security measures. This regulatory development creates a direct and immediate need for Spectrum's marine clients to enhance their cybersecurity posture, presenting significant opportunities for NCC Group and Adelard's consulting services in areas such as compliance assessment and risk management, as well as for Dragos' OT security platform to secure operational technology on marine vessels [Insight 4.5].

Similarly, in the energy sector, Spectrum's clients in the North American electric utility industry are subject to the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards 21. These mandatory standards require specific cybersecurity measures to protect the bulk electric system. Compliance with NERC CIP is a critical driver for security investments among Spectrum's energy clients, creating a demand for specialized OT security solutions and compliance expertise that vendors like Dragos and NCC Group can provide [Insight 4.6].

Depending on Spectrum's global operations and client base, other regulatory frameworks such as the General Data Protection Regulation (GDPR) or various regional cybersecurity regulations may also be relevant. Snippet20's mention of CMMC suggests potential compliance requirements related to US Department of Defense contracts. Therefore, a thorough understanding of the applicable regulatory landscape is essential for tailoring security solutions that meet the specific obligations of Spectrum and their diverse clientele [Insight 4.7].

As Spectrum Safety Solutions embraces digital transformation initiatives, they will likely encounter several operational challenges from a cybersecurity perspective [Insight 4.8]. The increasing connectivity of systems and devices will inevitably lead to an expanded attack surface, creating more potential entry points for cyber adversaries. The convergence of IT and OT systems, while offering operational efficiencies, can also introduce new vulnerabilities if not managed with a security-first approach 23. Furthermore, the presence of legacy OT systems, which may lack modern security features and can be difficult to patch, poses a significant challenge 23. The shortage of cybersecurity professionals with specialized OT expertise is another hurdle that Spectrum and many industrial organizations face 41. Securing remote access for employees and third-party vendors, which is often necessary for maintenance and support, is also a critical area of concern 33. Ensuring the security and privacy of sensitive operational data and customer information is paramount, and all security measures must be implemented in a way that minimizes disruption to critical safety operations. These multifaceted operational challenges underscore the significant need for expert guidance and specialized OT security solutions that NCC Group and Dragos are well-equipped to provide, with Adelard's safety focus ensuring that security enhancements do not inadvertently compromise operational safety.

### **5. NCC Group Consulting and Dragos Solution Alignment**

NCC Group offers a comprehensive suite of consulting services that can be strategically aligned with the potential cybersecurity needs of Spectrum Safety Solutions 23. Their Facility Due Diligence services 23 are particularly well-suited for assessing the current OT security posture of the newly formed Spectrum Safety Solutions and its constituent brands. This would provide Spectrum with a comprehensive initial assessment to identify immediate security risks and prioritize future security investments across the entire organization [Insight 5.1]. Understanding the current security landscape is a fundamental first step towards developing and implementing an effective security program. NCC Group's Technical Architecture Assessments 23 are essential for designing and verifying secure OT and IT network architectures, which is crucial for Spectrum's ongoing digital transformation initiatives and ICS modernization efforts [Insight 5.2]. Building security into the infrastructure from the outset is a more effective and sustainable approach than attempting to retrofit security measures later.

Adelard, part of the NCC Group, brings specialized expertise in cyber safety and reliability for industrial companies 23. This unique focus on the intersection of cybersecurity and operational safety is particularly valuable for Spectrum's high-hazard environments, ensuring that implemented security measures enhance safety rather than inadvertently compromising it [Insight 5.3]. NCC Group also offers expertise in navigating the complex landscape of regulatory compliance 23. They can assist both Spectrum and their clients in meeting relevant regulations, such as the US Coast Guard's maritime cybersecurity rules and NERC CIP standards, providing valuable guidance in interpreting and implementing these requirements, thereby reducing the burden of compliance [Insight 5.4]. Furthermore, NCC Group's Incident Response Readiness services 60 can help prepare Spectrum to effectively respond to and recover from cyber incidents in both their OT and IT environments, enhancing their overall resilience and minimizing potential downtime and safety impacts [Insight 5.5].

Dragos' OT security platform offers a suite of capabilities that directly address Spectrum's potential needs. The platform provides comprehensive OT asset visibility 25, enabling Spectrum to gain a clear understanding of their OT attack surface, which is fundamental for effective security monitoring and vulnerability management [Insight 5.6]. Dragos' platform also offers specialized threat detection capabilities for industrial control systems 25, identifying malicious activities that traditional IT security solutions might overlook. This provides an early warning system for potential cyberattacks targeting Spectrum's OT environment and the safety systems they provide [Insight 5.7]. Moreover, Dragos provides OT-specific vulnerability intelligence 25, helping Spectrum prioritize and address security weaknesses in their industrial systems, thereby reducing the risk of exploitation [Insight 5.8]. Given the increasing prevalence of ransomware attacks targeting industrial organizations, Dragos' platform includes features and threat intelligence specifically designed to detect and respond to these threats 33, offering specialized protection against a significant and growing risk to Spectrum's operations and customer base [Insight 5.9].

A joint approach leveraging NCC Group's consulting expertise, including Adelard's safety focus, and Dragos' specialized OT security platform can provide a robust solution for Spectrum Safety Solutions. For Spectrum's energy sector clients, securing turbine control systems is paramount. NCC Group's deep expertise in ICS/SCADA security, combined with Dragos' platform's granular visibility and threat detection within these environments, offers a comprehensive security posture. Adelard's safety analysis ensures that any security measures implemented do not compromise the safe operation of these critical assets [Insight 5.10]. Regarding the increasing threat of AI-powered ransomware, Dragos' behavioral analytics and threat intelligence are specifically designed to detect sophisticated attacks, potentially including those leveraging AI. NCC Group can provide strategic guidance on implementing best practices for ransomware prevention and response, while Adelard can assess the safety implications if operational systems are targeted [Insight 5.11]. This multi-layered defense, combining advanced detection, strategic planning, and safety considerations, is essential to counter evolving ransomware threats effectively.

Specific Dragos platform components most relevant to Spectrum's environment include: Asset Visibility & Inventory for a complete understanding of their OT landscape; Threat Detection to identify and alert on malicious activity; Vulnerability Management to prioritize and address security weaknesses; Investigation & Response for efficient incident handling; Dragos Threat Intelligence to stay informed about the latest threats and adversary tactics; and Neighborhood Keeper for collaborative defense and shared threat intelligence.

**Table 1: Alignment of Spectrum Safety Solutions' Potential Needs with NCC Group, Dragos, and Adelard's Offerings**

| **Potential Spectrum Need** | **NCC Group Solution** | **Dragos Solution** | **Adelard Contribution** |
| --- | --- | --- | --- |
| Initial OT Security Assessment | Facility Due Diligence | Dragos Platform - Asset Visibility & Inventory | Cyber Safety & Reliability considerations for assessment scope |
| Continuous ICS Threat Monitoring | Managed Security Services, Threat Intelligence | Dragos Platform - Threat Detection, Dragos Threat Intelligence, Neighborhood Keeper | Cyber Safety & Reliability analysis of detected threats and potential impacts |
| Maritime Cybersecurity Compliance | Regulatory Compliance Consulting | Dragos Platform - Asset Visibility for maritime OT | Cyber Safety & Reliability guidance on implementing compliant security measures |
| Energy Sector (NERC CIP) Compliance | Regulatory Compliance Consulting, NERC CIP Expertise | Dragos Platform - NERC CIP Compliance Mapping | Cyber Safety & Reliability review of NERC CIP controls in the context of operations |
| Securing "Factory Digital transformation" at Det-Tronics | Technical Architecture Assessments, OT Security Strategy Consulting | Dragos Platform - Asset Visibility, Threat Detection, Vulnerability Management | Cyber Safety & Reliability assessment of security controls in the manufacturing OT |
| Ransomware Protection for Industrial Environments | Incident Response Readiness, Security Awareness Training | Dragos Platform - Ransomware Detection & Response Capabilities, Threat Intelligence | Cyber Safety & Reliability analysis of ransomware impact on safety systems |
| Turbine Control Security | ICS/SCADA Security Expertise, Technical Architecture Assessments | Dragos Platform - ICS Protocol Analysis, Threat Detection for ICS | Cyber Safety & Reliability focus on turbine safety implications of security measures |

**Table 2: Key Regulatory Compliance Requirements for Spectrum's Target Sectors**

| **Sector** | **Relevant Regulation** | **Key Requirements** | **Implications for Spectrum and its Clients** |
| --- | --- | --- | --- |
| Marine | US Coast Guard Cybersecurity Final Rule (Effective July 16, 2025) 47 | Develop and maintain a Cybersecurity Plan; Designate a Cybersecurity Officer; Implement account security, device security, and data security measures; Network segmentation; Incident reporting. | Spectrum's marine clients (vessels, OCS facilities, MTSA facilities) must comply. Spectrum may need to offer solutions and services that align with these requirements. |
| Energy | NERC CIP Standards 21 | Mandatory cybersecurity standards for the North American bulk electric system; Covers areas like security management controls, physical security, cyber security perimeter, incident response, and recovery plans. | Spectrum's energy clients (electric utilities) must comply. Spectrum's solutions for fire and gas safety in power generation facilities must align with these standards. |

## **Conclusion**

The analysis indicates a significant and timely opportunity for cybersecurity investments within Spectrum Safety Solutions. The company's recent consolidation, coupled with its focus on critical infrastructure, energy, and marine sectors, positions it at the forefront of industries facing increasing cyber threats and regulatory scrutiny. Spectrum's likely pursuit of digital transformation initiatives, particularly within manufacturing and remote asset management, further underscores the urgent need for robust OT and IT security measures.

While Spectrum may have existing relationships with traditional IT security vendors, a potential vulnerability lies in the specialized security requirements of their OT environments. This gap presents a clear avenue for Dragos, with its purpose-built industrial cybersecurity platform, to offer significant value in asset visibility, threat detection, vulnerability management, and ransomware protection tailored for ICS/SCADA systems.

NCC Group, including Adelard's safety expertise, is well-positioned to provide crucial consulting services. Facility Due Diligence can offer an immediate understanding of Spectrum's current security posture, while technical architecture assessments can guide the development of secure infrastructure for future initiatives. Adelard's unique focus on cyber safety and reliability is particularly relevant for Spectrum's high-hazard operating environment, ensuring that security enhancements align with and support overall safety objectives. Furthermore, NCC Group's expertise in regulatory compliance can assist both Spectrum and their clients in navigating the complex requirements of the marine and energy sectors.

The identified digital transformation projects within Det-Tronics represent a near-term procurement opportunity. The increasing regulatory pressures, especially the new US Coast Guard maritime cybersecurity rule and the ongoing NERC CIP requirements, will continue to drive security investments within Spectrum's client base. By strategically aligning their offerings to address these specific needs and challenges, NCC Group, Dragos, and Adelard can establish themselves as key partners in enhancing the cyber and operational resilience of Spectrum Safety Solutions and the critical industries they serve.

#### Works cited

1. Spectrum Safety Solutions 2025 Company Profile: Valuation, Funding & Investors, accessed March 23, 2025, <https://pitchbook.com/profiles/company/663942-61>
2. Spectrum Safety Solutions, accessed March 23, 2025, <https://www.spectrum-safety.com/>
3. Sentinel Capital Partners Carves Out Industrial Fire Business from Carrier, accessed March 23, 2025, <https://www.autronicafire.com/en/press-and-marketing/news/news-article/sentinel-capital-partners-carves-out-industrial-fire-business-from-carrier.html>
4. Sentinel Capital Partners Carves Out Industrial Fire Business from Carrier | My Site - Marioff, accessed March 23, 2025, <https://www.marioff.com/en/news/news-articles/sentinel-capital-partners-carves-out-industrial-fire-business-from-carrier.html>
5. Sentinel Capital Partners Carves Out Industrial Fire Business from Carrier - Det-Tronics, accessed March 23, 2025, <https://www.det-tronics.com/newsitem/BRAND_PRESS_RELEASE>
6. Digital transformation | Spectrum.Life, accessed March 23, 2025, <https://www.spectrum.life/digital-transformation/>
7. Three ways state IT leaders can foster digital transformation | Spectrum Enterprise, accessed March 23, 2025, <https://enterprise.spectrum.com/insights/blog/state-it-leaders-digital-transformation.html>
8. Spectrum Labs Presents Safety Matters Summit to Examine Corporate Trust in the Metaverse Era - Business Wire, accessed March 23, 2025, <https://www.businesswire.com/news/home/20220420005319/en/Spectrum-Labs-Presents-Safety-Matters-Summit-to-Examine-Corporate-Trust-in-the-Metaverse-Era>
9. How network modernization improves digital customer experience - Spectrum Enterprise, accessed March 23, 2025, <https://enterprise.spectrum.com/insights/blog/digital-customer-experience-network-modernization.html>
10. National Spectrum Research and Development Plan - NITRD, accessed March 23, 2025, <https://www.nitrd.gov/pubs/National-Spectrum-RD-Plan-2024.pdf>
11. Private 4G and 5G networks: Driving Industry 4.0 and industrial ecosystem growth | Communications Today, accessed March 23, 2025, <https://www.communicationstoday.co.in/private-4g-and-5g-networks-driving-industry-4-0-and-industrial-ecosystem-growth/>
12. Manufacturing technology solutions - Spectrum Enterprise, accessed March 23, 2025, <https://enterprise.spectrum.com/solutions/industries/manufacturing.html>
13. 10 Core Components of Industry 4.0 - Oracle, accessed March 23, 2025, <https://www.oracle.com/industrial-manufacturing/industry-4-components/>
14. A primer for Industry 4.0 insight - Ericsson, accessed March 23, 2025, <https://www.ericsson.com/en/blog/north-america/2024/primer-for-industry-40>
15. Detector Electronics Factory It Supervisor Job Minneapolis - ZipRecruiter, accessed March 23, 2025, <https://www.ziprecruiter.com/c/Detector-Electronics-LLC/Job/Factory-IT-Supervisor/-in-Minneapolis,MN?jid=00a84691ecc56c7c>
16. Internet & WiFi Network Security - Spectrum, accessed March 23, 2025, <https://www.spectrum.com/internet/wifi-service/spectrum-advanced-wifi/security>
17. Security products and services - Spectrum Enterprise, accessed March 23, 2025, <https://enterprise.spectrum.com/products/security.html>
18. Managed security solutions | Spectrum Enterprise, accessed March 23, 2025, <https://enterprise.spectrum.com/solutions/security.html>
19. Spectrum is Committed to Safety, accessed March 23, 2025, <https://www.spectrumplastics.com/about/technical-resources/spectrum-is-committed-to-safety/>
20. Project Spectrum, accessed March 23, 2025, <https://www.projectspectrum.io/>
21. OT Security: Your Guide to Protecting Critical Infrastructure - Verve Industrial, accessed March 23, 2025, <https://verveindustrial.com/resources/blog/the-ultimate-guide-to-understanding-ot-security/>
22. ICS410: ICS/SCADA Security Essentials - SANS Institute, accessed March 23, 2025, <https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/>
23. Cyber Security for Operational Technology (OT) - NCC Group, accessed March 23, 2025, <https://www.nccgroup.com/us/consulting-implementation/operational-technology/>
24. Safety First! Secure OT To Protect Your People & Productivity | NCC Group, accessed March 23, 2025, <https://www.nccgroup.com/us/securing-ot-against-cyber-attacks-to-protect-your-people-and-productivity/>
25. AWS Marketplace: Dragos Platform - Industrial Cybersecurity for OT Environments, accessed March 23, 2025, <https://aws.amazon.com/marketplace/pp/prodview-qyydwbbsdieom>
26. Contracts For Dec. 10, 2024 - Department of Defense, accessed March 23, 2025, <https://www.defense.gov/News/Contracts/Contract/Article/3993982/>
27. Cyber Security Specialist - Fiji Islands - Tender Impulse, accessed March 23, 2025, <https://tenderimpulse.com/government-tenders/fiji-islands;vanuatu/cyber-security-specialist-4802524>
28. DNV report highlights increased OT cybersecurity investment in energy sector due to escalating threats - Industrial Cyber, accessed March 23, 2025, <https://industrialcyber.co/utilities-energy-power-water-waste/dnv-report-highlights-increased-ot-cybersecurity-investment-in-energy-sector-due-to-escalating-threats/>
29. Cybersecurity Moving Up Priority Lists for Energy Firms, DNV Finds - Marine Link, accessed March 23, 2025, <https://www.marinelink.com/news/cybersecurity-moving-priority-lists-521415>
30. Critical infrastructure faces 30 percent surge in cyber attacks, KnowBe4 report highlights, accessed March 23, 2025, <https://industrialcyber.co/critical-infrastructure/critical-infrastructure-faces-30-percent-surge-in-cyber-attacks-knowbe4-report-highlights/>
31. 5 Cyber Attacks that Threaten Critical Infrastructure and How to Protect Against Them, accessed March 23, 2025, <https://learn.assetlifecycle.trimble.com/blog/5-cyber-attacks-that-threaten-critical-infrastructure-and-how-to-protect-against-them>
32. NEW: House Homeland Releases “Cyber Threat Snapshot” Highlighting Rising Threats to US Networks, Critical Infrastructure, accessed March 23, 2025, <https://homeland.house.gov/2024/11/12/new-house-homeland-releases-cyber-threat-snapshot-highlighting-rising-threats-to-us-networks-critical-infrastructure/>
33. Dragos reports evolving ransomware threat landscape with increased operational disruptions as attacks target ICS - Industrial Cyber, accessed March 23, 2025, <https://industrialcyber.co/industrial-cyber-attacks/dragos-reports-evolving-ransomware-threat-landscape-with-increased-operational-disruptions-as-attacks-target-ics/>
34. Dragos finds ransomware attacks on industrial sector surge 87%, manufacturing hit hardest as OT targeting rises, accessed March 23, 2025, <https://industrialcyber.co/reports/dragos-finds-ransomware-attacks-on-industrial-sector-surge-87-manufacturing-hit-hardest-as-ot-targeting-rises/>
35. Dragos Industrial Ransomware Analysis: Q4 2024, accessed March 23, 2025, <https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2024/>
36. Industrial Cyber Risk Management Solutions - Dragos, accessed March 23, 2025, <https://www.dragos.com/cybersecurity-solutions/industrial-cyber-risk-management/>
37. Top 10 Security Threats for the Energy Sector - Kaseware, accessed March 23, 2025, <https://www.kaseware.com/post/top-10-security-threats-for-the-energy-sector>
38. Cyberattacks on Energy Infrastructure | GE Vernova, accessed March 23, 2025, <https://www.gevernova.com/gas-power/resources/articles/2021/energy-cyber-attack>
39. 67% of Energy Sector Breaches Linked to Software and IT Vendors, SecurityScorecard Reports, accessed March 23, 2025, <https://securityscorecard.com/company/press/67-of-energy-sector-breaches-linked-to-software-and-it-vendors-securityscorecard-reports/>
40. Growing Cyber Threats to the Energy Sector - CyberSaint, accessed March 23, 2025, <https://www.cybersaint.io/blog/growing-cyber-threats-to-the-energy-sector>
41. Protecting the power grid: Cybersecurity in the energy sector, accessed March 23, 2025, <https://cybersecurityguide.org/industries/energy/>
42. Cyber Threats and Advisories | Cybersecurity and Infrastructure Security Agency CISA, accessed March 23, 2025, <https://www.cisa.gov/topics/cyber-threats-and-advisories>
43. Cybersecurity Threats in Maritime for 2025 - Dryad Global, accessed March 23, 2025, <https://channel16.dryadglobal.com/cybersecurity-threats-in-maritime-for-2025>
44. Cybersecurity for Maritime: Definition & Examples - Darktrace, accessed March 23, 2025, <https://darktrace.com/cyber-ai-glossary/cybersecurity-in-maritime>
45. The Digital Threat: Why Cybersecurity Can't Be an Afterthought - The Global Treasurer, accessed March 23, 2025, <https://www.theglobaltreasurer.com/2025/03/18/the-digital-threat-why-cybersecurity-cant-be-an-afterthought/>
46. CERT-UA Warns of Cyber Scams Using Fake AnyDesk Requests for Fraudulent Security Audits - The Hacker News, accessed March 23, 2025, <https://thehackernews.com/2025/01/cert-ua-warns-of-cyber-scams-using-fake.html>
47. Cybersecurity in the Marine Transportation System - Federal Register, accessed March 23, 2025, <https://www.federalregister.gov/documents/2025/01/17/2025-00708/cybersecurity-in-the-marine-transportation-system>
48. US Coast Guard releases final rule on maritime security and cybersecurity standards, accessed March 23, 2025, <https://industrialcyber.co/transport/us-coast-guard-releases-final-rule-on-maritime-security-and-cybersecurity-standards/>
49. Coast Guard Issues Final Maritime Cybersecurity Rule: Key Requirements and Implementation Timeline - The National Law Review, accessed March 23, 2025, <https://natlawreview.com/article/coast-guard-issues-final-maritime-cybersecurity-rule-key-requirements-and>
50. Coast Guard Maritime Industry Cybersecurity Resource Website, accessed March 23, 2025, <https://www.uscg.mil/MaritimeCyber/>
51. Top 5 OT Security Standards and How to Implement Them Effectively - SimSpace, accessed March 23, 2025, <https://simspace.com/blog/top-5-ot-security-standards-and-how-to-implement-them-effectively/>
52. Regulatory Compliance and OT Cybersecurity: What You Need to Know, accessed March 23, 2025, <https://www.micromindercs.com/blog/regulatory-compliance-and-ot-cybersecurity>
53. OT Security Compliance Regulations: Standards in Critical Industries, accessed March 23, 2025, <https://www.micromindercs.com/blog/ot-security-compliance-regulations-standards-in-critical-industries>
54. NERC CIP: A Complete Guide to OT Security for Critical Infrastructure - OTORIO, accessed March 23, 2025, <https://www.otorio.com/resources/what-is-nerc-cip/>
55. Ensure ICS Compliance with Cybersecurity Controls - Dragos, accessed March 23, 2025, <https://www.dragos.com/cybersecurity-solutions/industrial-cybersecurity-compliance/>
56. The Importance of Governance, Risk, and Compliance with Practical Exposure in OT Security - Industrial Cyber, accessed March 23, 2025, <https://industrialcyber.co/analysis/the-importance-of-governance-risk-and-compliance-with-practical-exposure-in-ot-security/>
57. Energy & Utilities Sector | Cyber Security - NCC Group, accessed March 23, 2025, <https://www.nccgroup.com/uk/energy-utilities-services/>
58. Acquisition of Adelard LLP - NCC Group, accessed March 23, 2025, <https://www.nccgroup.com/uk/adelard/>
59. Consulting & Implementation | NCC Group, accessed March 23, 2025, <https://www.nccgroup.com/sg/consulting-implementation/>
60. Facility Due Diligence & OT Risk Assessment Services | NCC Group, accessed March 23, 2025, <https://www.nccgroup.com/us/consulting-implementation/operational-technology/facility-due-diligence/>
61. NCC Group | Leading Cyber Security & Managed Services, accessed March 23, 2025, <https://www.nccgroup.com/>
62. The Operational Technology Cyber Incident Response Checklist - NCC Group, accessed March 23, 2025, <https://www.nccgroup.com/uk/the-operational-technology-cyber-incident-response-checklist/>
63. Capabilities | Adelard, accessed March 23, 2025, <https://www.adelard.com/capabilities/>
64. Security-informed safety - Adelard, accessed March 23, 2025, <https://www.adelard.com/capabilities/security/security-informed-safety/>
65. Downloadable Resources - CAE FRAMEWORK, accessed March 23, 2025, <https://claimsargumentsevidence.org/resources/downloadable-resources/>
66. (PDF) Safety and Assurance Cases: Past, Present and Possible Future – an Adelard Perspective - ResearchGate, accessed March 23, 2025, <https://www.researchgate.net/publication/225907154_Safety_and_Assurance_Cases_Past_Present_and_Possible_Future_-_an_Adelard_Perspective>
67. Adelard, accessed March 23, 2025, <https://www.adelard.com/>
68. NCC Group - Wikipedia, accessed March 23, 2025, <https://en.wikipedia.org/wiki/NCC_Group>
69. Adelard 2025 Company Profile: Valuation, Investors, Acquisition | PitchBook, accessed March 23, 2025, <https://pitchbook.com/profiles/company/144750-34>
70. Our Office Locations | NCC Group PLC, accessed March 23, 2025, <https://www.nccgroupplc.com/our-office-locations/>
71. The Dragos Platform - Cybersecurity Excellence Awards, accessed March 23, 2025, <https://cybersecurity-excellence-awards.com/candidates/the-dragos-platform-2024-2/>
72. Our Cybersecurity Platform Protects OT Environments - Dragos, accessed March 23, 2025, <https://www.dragos.com/cybersecurity-platform/>
73. OT Vulnerability Management - Dragos, accessed March 23, 2025, <https://www.dragos.com/cybersecurity-platform/ot-vulnerability-management/>
74. Dragos Platform with Vulnerability Management, accessed March 23, 2025, <https://www.dragos.com/resources/video/dragos-platform-with-vulnerability-management/>