# **Strategic Sales Approach & Battle Card for KAMO Energy**

**1. Executive Summary**

This report outlines a strategic approach for NCC Group's sales team to engage KAMO Energy, a Generation and Transmission (G&T) cooperative providing power to 17 member distribution cooperatives in northeast Oklahoma and southwest Missouri 1. The analysis suggests a high priority level for engagement, given KAMO Energy's critical infrastructure role, ongoing digital transformation and network expansion initiatives, and the regulatory landscape of the energy sector. The expected engagement timeline is considered mid-term, allowing for thorough discovery, relationship building, and solution implementation. Key stakeholders to target within KAMO Energy include the CISO, CIO, VP of Operations, and Head of Regulatory Compliance. The core value proposition for KAMO Energy centers on enhancing the security and resilience of their operational technology (OT) environment, ensuring compliance with North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards, and mitigating the risks associated with an evolving cyber threat landscape. Anticipated challenges include potential budget constraints, the complexity of integrating with legacy OT systems, and competition from incumbent vendors. Mitigation strategies involve demonstrating a clear return on investment, offering a phased implementation approach, and highlighting NCC-Dragos' specialized expertise in OT cybersecurity within the energy sector.

**2. Business Initiative Analysis**

**2.1 Active and Planned Business Initiatives:**

KAMO Energy is actively involved in digital transformation projects, as evidenced by their deployment of Infinera's XTM Series to upgrade their rural broadband network 2. This initiative supports high-capacity 100G transport services and allows for future scalability to 400G, indicating a significant investment in modernizing their network infrastructure to meet increasing bandwidth demands and potentially offer new digital services to their members. This network upgrade signifies a strategic move towards enhancing KAMO's digital capabilities and the underlying infrastructure that supports them. The scale of this investment suggests a forward-looking approach to their technological landscape.

Business expansion efforts are also underway, with KAMO Power, through its subsidiary K-Powernet, requesting American Rescue Plan Act (ARPA) funding for a Green Country Rural Broadband Backhaul Network expansion 4. This project aims to significantly increase internet capacity and reliability in rural Oklahoma, demonstrating a strategic focus on expanding their service footprint to underserved areas and addressing the growing demand for broadband connectivity. This expansion into broadband services represents a diversification of KAMO's offerings beyond traditional power transmission.

In terms of operational efficiency programs, the rate increase implemented by Ozark Electric was partly attributed to KAMO's rising costs associated with new generation and transmission projects 5. These capital investments are aimed at bolstering the reliability and overall efficiency of KAMO's power delivery infrastructure. While not explicitly labeled an efficiency program, these substantial investments in infrastructure upgrades and new facilities are likely intended to optimize their operational performance.

Innovation initiatives at KAMO Energy include offering green power options to their cooperative members 7. This indicates an engagement with renewable energy sources, providing members with the choice to meet some of their energy needs through more sustainable options. While perhaps not a central strategic pillar at present, this offering suggests an awareness of the evolving energy landscape and a potential openness to further exploration of renewable energy solutions in the future.

KAMO Energy's core product and service launch revolves around providing safe, low-cost, and reliable power to its member cooperatives 1. The expansion of broadband services through K-Powernet represents a notable service diversification, moving beyond their traditional role as a power transmission provider to also meet the growing demand for internet connectivity in their service area 4.

**2.2 Current Security and Compliance Projects:**

Specific active Requests for Proposals (RFPs) related to security were not identified in the provided information. Further investigation through procurement channels or direct contact would be needed to ascertain any current security-related procurement activities.

However, there are announced security improvement initiatives within the electric cooperative sector that likely involve KAMO Energy. These include industry-wide efforts to strengthen the cyber workforce and enhance overall cybersecurity posture through training and personnel development 8. Additionally, KAMO Power participates in safety initiatives, including those focused on nighttime crews 9. While primarily focused on physical safety, these initiatives indicate a broader organizational commitment to safety, which can extend to cybersecurity considerations, especially given the increasing convergence of IT and OT systems.

Compliance deadlines and related projects are significant for KAMO Energy, as they are subject to NERC reliability standards as a G&T cooperative 10. Their past NERC violation related to operational procedures 11 highlights the critical and ongoing importance of compliance and suggests that KAMO Energy likely has projects and processes in place aimed at addressing past deficiencies and ensuring continued adherence to these mandatory standards.

Information regarding KAMO Energy's specific cyber insurance requirements was not found in the provided snippets. Understanding their insurance coverage could offer insights into their risk management strategies and potential areas of security focus.

The past NERC violation 11 implies that KAMO Energy has undertaken post-incident remediation efforts to address the identified non-compliance. The nature and extent of these efforts would provide further understanding of their incident response capabilities.

**2.3 Budget Cycles and Financial Planning:**

Specific details regarding KAMO Energy's fiscal year schedule were not available in the provided information. Determining this would be beneficial for aligning sales efforts with their financial planning timelines.

Similarly, the exact budget approval timelines for KAMO Energy are not detailed in the snippets. Understanding when they typically review and approve budgets for capital and operational expenditures would aid in forecasting sales cycles.

However, the capital expenditure patterns of KAMO Energy can be inferred. The rate increase for Ozark Electric due to KAMO's investments 5 indicates ongoing capital spending in generation and transmission infrastructure. Furthermore, their broadband expansion initiatives 2 also signify capital investment in network infrastructure. These patterns suggest a willingness to make significant capital investments in key areas of their operations.

Information regarding KAMO Energy's specific financial planning cadence and quarterly financial priorities was not found within the provided research material.

**2.4 Industry-Specific Priorities:**

Several sector trends are likely influencing KAMO Energy's priorities. The electric cooperative industry is facing increasing demand for power, coupled with growing concerns about grid reliability and the imperative to integrate renewable energy sources into their generation mix 13. Cybersecurity is also a paramount concern within the energy sector due to the critical nature of the infrastructure and the escalating sophistication of cyber threats 8. These trends collectively shape the strategic direction and operational focus of electric cooperatives like KAMO Energy.

Specific peer benchmarking data for KAMO Energy's initiatives was not available in the provided snippets. Understanding how KAMO compares to similar G&T cooperatives in their adoption of new technologies, security measures, and sustainability efforts could provide valuable context for their strategic outlook.

KAMO Power is a member of the Association of Missouri Electric Cooperatives (AMEC) 1 and operates within a three-tiered structure that includes Associated Electric Cooperative, Inc. (AECI) 1. These industry associations play a role in shaping the priorities of their members by offering guidance, resources, and advocating for common interests within the electric cooperative community. The Oklahoma Association of Electric Cooperatives (OAEC) 30 also serves electric cooperatives in Oklahoma and may have relevant initiatives influencing KAMO.

Regulatory-driven priorities are significant for KAMO Energy. Compliance with NERC CIP standards is a major driver for security initiatives within the electric power industry 1. KAMO's past violation 11 underscores the critical importance of adhering to these regulations and the potential for related security projects. The Federal Energy Regulatory Commission (FERC) also provides regulatory oversight for the energy sector 38.

**3. OT Environment Analysis**

**3.1 Industrial Systems Landscape:**

While specific manufacturing facilities operated by KAMO Energy are not detailed in the snippets, it is likely they possess operational facilities for the maintenance, control, and administration of their extensive transmission network. The core of KAMO Energy's operational technology (OT) environment is their high voltage transmission network 1, which spans a significant geographical area across northeast Oklahoma and southwest Missouri. Critical operational systems within this landscape likely include SCADA (Supervisory Control and Data Acquisition) and other industrial control systems (ICS) 48 that are essential for the real-time monitoring and control of power flow and overall network operations, ensuring grid stability and reliability.

KAMO Energy's supply chain connectivity involves a critical upstream relationship with Associated Electric Cooperative, Inc. (AECI), their power supplier 1. Downstream, they serve 17 member distribution cooperatives 1. Their recent expansion into broadband services through K-Powernet 4 potentially introduces connectivity with other internet service providers and telecommunications carriers, adding another layer to their supply chain considerations.

The deployment of a rural broadband network 2 indicates the presence of numerous remote sites and likely unmanned infrastructure. The safety initiatives aimed at nighttime crews 9 further suggest significant field operations and a need to ensure the security of remote assets and the safety of personnel working in these dispersed locations.

**3.2 OT Security Maturity:**

Specific details regarding KAMO Energy's current OT security controls are not available in the provided snippets, although their participation in industry-wide cybersecurity efforts 8 suggests a general awareness of security needs. KAMO Energy's utilization of cloud services 53 for various functions indicates that they have likely implemented some level of IT/OT convergence to enhance operational efficiency and facilitate data sharing, though the specifics of this integration are unclear. Given the typical longevity of equipment in the energy sector, it is highly probable that KAMO Energy operates legacy OT systems 54, which often present unique security challenges. Information regarding specific security measures for industrial protocols and the extent of their OT monitoring capabilities was not found in the research material.

**3.3 OT Threat Exposure:**

The energy sector is a high-profile target for various threat actors, including nation-states, terrorist organizations, and cybercriminals motivated by financial gain 59. KAMO Energy faces potential exposure to sophisticated threat groups such as VOLTZITE, known for targeting critical infrastructure with a focus on stealing OT data 65. While primarily focused on Ukraine, KAMACITE and ELECTRUM have demonstrated capabilities that could be adapted to target energy infrastructure elsewhere, with ELECTRUM having a history of using disruptive wiper malware.

Given KAMO Energy's reliance on AECI and its network of member cooperatives, they are also susceptible to supply chain vulnerabilities 63. Compromises at upstream or downstream partners could potentially impact KAMO's operations. Their expansion into broadband services may further extend their supply chain and associated risks. The likely use of remote access for managing their transmission network and supporting broadband services 74 also introduces security risks if not adequately secured, as the energy sector has seen an increase in attacks targeting remote access vulnerabilities. Finally, the potential use of vulnerable industrial protocols like Modbus and DNP3 55 could represent another avenue of threat exposure.

**3.4 OT Security Initiatives:**

Specific OT security projects publicly announced by KAMO Energy were not identified in the provided snippets, although industry-wide efforts to enhance cybersecurity within electric cooperatives are underway 8. No executive statements from KAMO Energy specifically addressing OT security were found. However, KAMO Energy's ongoing efforts to comply with NERC CIP standards 10, particularly in light of their past violation, represent a significant OT security initiative driven by regulatory requirements. While network upgrades are in progress 2, the extent to which these include specific ICS/SCADA security enhancements is unclear. Similarly, no specific information regarding OT network segmentation projects at KAMO Energy was found in the research material.

**4. Value Proposition Matrix**

**4.1 Business Impact Mapping:**

NCC-Dragos capabilities, including Foundational Security Testing (FDD), the Dragos Platform, OT Watch, and the Incident Response (IR) Retainer, directly align with KAMO Energy's business objectives of providing reliable, low-cost power and expanding broadband services. The Dragos Platform can provide comprehensive visibility into KAMO's OT environment, identifying vulnerabilities and potential threats that could disrupt their critical transmission network, directly impacting power reliability. By proactively detecting and mitigating these risks, NCC-Dragos can help KAMO Energy avoid costly downtime and maintain the trust of their member cooperatives. Furthermore, enhanced security can contribute to operational efficiency by minimizing disruptions and ensuring the smooth operation of their expanding broadband infrastructure. NCC Group's expertise in NERC CIP compliance, coupled with the Dragos Platform's capabilities for asset inventory and vulnerability management, can significantly reduce the risk of non-compliance and associated financial penalties, contributing to cost savings. The IR Retainer provides KAMO Energy with access to specialized OT cybersecurity expertise in the event of an incident, ensuring rapid and effective remediation, minimizing potential financial and reputational damage.

**4.2 "Now/Next/Never" Prioritization:**

Immediate protection requirements for KAMO Energy ("Now") include gaining comprehensive visibility into their OT environment to identify and address critical vulnerabilities that could be exploited by threat actors like VOLTZITE, KAMACITE, or ELECTRUM. Addressing immediate NERC CIP compliance gaps to avoid potential penalties based on their past violation is also a priority. Securing their expanding broadband network from emerging threats should also be considered an immediate need as they extend their digital footprint.

Strategic security improvement opportunities ("Next") for KAMO Energy involve implementing advanced threat detection and intelligence capabilities tailored to the energy sector, such as Dragos OT Watch, to proactively identify and respond to sophisticated attacks. Establishing robust OT network segmentation to isolate critical assets and limit the lateral movement of attackers is another strategic improvement. Enhancing their incident response plan with NCC Group's IR Retainer and conducting regular exercises will further strengthen their resilience.

Areas where risk can be accepted by KAMO Energy ("Never") would require a thorough understanding of their risk appetite and a collaborative discussion. However, given the critical nature of their services and the regulatory environment, accepting significant risk in core areas like transmission network security or NERC CIP compliance is likely not advisable. Risk acceptance might be considered in less critical supporting systems after a thorough risk assessment.

A phased implementation approach would be most suitable for KAMO Energy. The initial phase ("Now") could focus on deploying the Dragos Platform to achieve immediate asset visibility and vulnerability assessment across their critical OT network segments. The next phase ("Next") could involve implementing advanced threat detection and integrating the Dragos Platform with their existing security infrastructure. Subsequent phases could address strategic improvements like network segmentation and the establishment of a comprehensive incident response plan with NCC Group's support.

Quick wins for KAMO Energy include the rapid deployment of the Dragos Platform, which can provide immediate visibility into their OT assets and identify potential vulnerabilities. This can be followed by the implementation of basic threat detection rules. Long-term improvements involve building a mature OT security program that includes proactive threat hunting, robust incident response capabilities, and continuous compliance with evolving regulations.

**4.3 Competitive Differentiation:**

NCC-Dragos offers a distinct advantage over general IT security vendors or those with less specialized OT capabilities. Dragos's deep expertise in OT cybersecurity, specifically within the energy sector, is a key differentiator. The Dragos Platform is purpose-built for industrial control systems, providing granular visibility and threat intelligence that generic IT security tools lack. NCC Group's broader cybersecurity capabilities, including incident response and managed services, complement Dragos's OT focus, offering a comprehensive security solution. Unlike competitors with a more generic approach, NCC-Dragos provides threat intelligence derived from real-world OT incidents, ensuring that KAMO Energy is protected against the latest and most relevant threats. The combination of NCC Group's consulting expertise in areas like NERC CIP compliance with Dragos's technical capabilities provides a unique value proposition that addresses both regulatory and security requirements.

**4.4 Success Metrics:**

Key Risk Reduction KPIs for KAMO Energy include a measurable reduction in the number of identified vulnerabilities within their OT environment over time, a decrease in the average time to detect and respond to security incidents affecting their OT systems, and the prevention of successful cyberattacks that could lead to disruptions in power transmission or broadband services.

Time-to-value metrics will focus on the speed at which KAMO Energy can realize tangible benefits from the NCC-Dragos solution. This includes the time taken to deploy the Dragos Platform and achieve initial visibility into their OT assets, as well as the time required to identify and mitigate high-priority vulnerabilities after the platform's deployment.

Operational impact measurements will assess how the security improvements contribute to KAMO Energy's core business objectives. This includes maintaining a high level of uptime and availability for their critical transmission network, minimizing disruptions to their expanding broadband services due to security incidents, and improving the overall performance and reliability of their OT systems through enhanced security and reduced risk.

Compliance achievement timelines will track KAMO Energy's progress in meeting specific milestones for NERC CIP compliance with the assistance of NCC-Dragos' solutions and expertise. Success will be measured by their ability to successfully navigate NERC audits and demonstrate continuous compliance with evolving regulatory requirements.

The ROI calculation framework for KAMO Energy will involve a comprehensive analysis of the costs associated with potential cyber incidents (based on industry averages and their specific infrastructure), the operational efficiency gains achieved through reduced downtime and improved visibility, the avoidance of potential fines for NERC CIP non-compliance, and the optimization of their security resource allocation, all compared to the investment in NCC-Dragos' solutions.

**5. Engagement Strategy**

**5.1 Initial Contact Approach:**

Primary contact targets at KAMO Energy should include the Chief Information Security Officer (CISO), who is ultimately responsible for the organization's overall security posture. Secondary targets include the Chief Information Officer (CIO), who oversees the IT and potentially OT infrastructure, the Vice President of Operations, who is concerned with the reliability and efficiency of the power transmission network, and the Head of Regulatory Compliance, who is responsible for ensuring adherence to NERC CIP standards.

Outreach messaging should be tailored to each role. For the CISO, the message should focus on the increasing cyber threats to the energy sector, the specific vulnerabilities of OT environments, and how NCC-Dragos can provide enhanced visibility, threat detection, and incident response capabilities to protect KAMO's critical infrastructure and ensure NERC CIP compliance. For the CIO, the messaging should highlight the importance of a unified security strategy across IT and OT, the challenges of IT/OT convergence, and how NCC-Dragos can provide a comprehensive solution that integrates with their existing IT security investments while addressing the unique needs of their OT environment. The VP of Operations should receive messaging that emphasizes how NCC-Dragos can help maintain and improve the reliability and safety of their power transmission network by preventing cyber incidents that could lead to costly downtime and disruptions. For the Head of Regulatory Compliance, the outreach should focus on NCC Group's deep expertise in NERC CIP compliance, how the Dragos Platform can aid in meeting specific requirements, and how the joint solution can reduce the risk of future violations.

Custom value propositions should be developed for each stakeholder. For the CISO, the value proposition is enhanced security posture and reduced risk. For the CIO, it's a comprehensive IT/OT security solution. For the VP of Operations, it's improved reliability and safety. For the Head of Regulatory Compliance, it's simplified and strengthened NERC CIP compliance.

The engagement sequencing should ideally start with the CISO or a senior executive responsible for OT security, as they are likely to be most receptive to the core value proposition. Once initial interest is established, engagement should be expanded to other relevant stakeholders like the CIO, VP of Operations, and Head of Regulatory Compliance to build broader support for the initiative.

A multi-threading strategy should be employed by engaging multiple stakeholders across different departments and levels within KAMO Energy simultaneously. This can help to build a more comprehensive understanding of their needs and priorities, identify potential champions within the organization, and accelerate the sales process.

**5.2 Discovery Process:**

Key discovery questions for KAMO Energy should aim to understand their current OT environment in detail, including the types of industrial control systems in use, network architecture, and communication protocols. Questions should also focus on their existing security controls, policies, and procedures for protecting their OT environment. Understanding their key pain points related to the reliability and efficiency of their operations, as well as any challenges they face in meeting NERC CIP compliance requirements, is crucial. Finally, exploring their future strategic initiatives, particularly any plans for further digital transformation or integration of renewable energy, will help identify opportunities for alignment.

The technical assessment approach should involve proposing a non-intrusive assessment of KAMO Energy's OT environment using the Dragos Platform. This assessment can provide valuable insights into their asset inventory, identify existing vulnerabilities, and detect any potential threats without causing any disruption to their operations.

Business impact discovery should focus on exploring the potential financial, operational, and reputational consequences that KAMO Energy could face in the event of a successful cyberattack on their critical infrastructure. The discussion should highlight how NCC-Dragos' solutions can help mitigate these risks and protect their core business objectives.

The need verification process should involve confirming the identified pain points and security gaps with multiple stakeholders across different departments within KAMO Energy. This will ensure a clear and consistent understanding of their requirements and priorities and validate the assumptions made during the initial outreach and discovery phases.

The current state analysis methodology will involve analyzing the information gathered during the discovery process, including the technical assessment results and insights from stakeholder interviews, to develop a comprehensive understanding of KAMO Energy's OT security posture, identify key areas of risk, and tailor a solution and value proposition that directly addresses their specific needs.

**5.3 Sales Process Flow:**

The expected sales cycle length for an engagement of this nature with a critical infrastructure provider like KAMO Energy is likely to be in the mid-to-long term, potentially ranging from six to twelve months or longer, due to the complexity of their environment and the critical nature of their operations, which often necessitates thorough evaluation and multiple levels of approval.

Decision stages and milestones at KAMO Energy will likely include an initial evaluation phase where they assess different security solutions and vendors, followed by a technical validation phase involving a proof of concept or pilot deployment. The business case approval stage will involve internal review and justification of the investment, potentially requiring sign-off from multiple departments and executive leadership. The final stage is contract negotiation and execution, leading to procurement. Key milestones to track progress could include securing an initial meeting, completing a successful proof of concept, receiving budget approval, and finalizing the contract.

Approval requirements at KAMO Energy will likely involve multiple stakeholders and levels of management. Technical approval may be required from the IT and OT security teams, while budget approval may need sign-off from the finance department and executive leadership. Understanding the specific approval hierarchy and identifying the key decision-makers and influencers will be crucial for navigating the sales process effectively.

The contract process for KAMO Energy will likely involve a thorough review by their legal and procurement teams. Familiarity with standard contract terms in the energy sector and a willingness to be flexible in negotiations will be important.

Procurement procedures at KAMO Energy may involve formal RFPs, especially for significant investments. However, direct negotiations may also be possible, particularly if NCC-Dragos can establish a strong relationship and demonstrate unique value. Understanding their preferred procurement methods will help tailor the sales approach accordingly.

**5.4 Objection Handling:**

Anticipated objections from stakeholders at KAMO Energy may include concerns about the cost of the NCC-Dragos solution, especially in comparison to existing IT security investments or perceived budget limitations. There might also be objections related to the potential disruption to their critical OT operations during the implementation process. Internal resource constraints, with concerns about their team's capacity to manage a new security platform, are also possible. Skepticism about the actual value proposition and the return on investment in OT-specific security solutions could arise. A preference for their existing security vendors, with established relationships and familiarity, might also be an objection. Finally, the timing of the investment might be questioned if it doesn't align with their current budget cycle or strategic priorities.

To address competitor displacement, NCC-Dragos should emphasize their deep and specialized expertise in OT cybersecurity, particularly within the energy sector, which differentiates them from more general IT security vendors. Highlighting the purpose-built nature of the Dragos Platform and its superior capabilities in OT asset visibility, threat intelligence, and incident response, which are often lacking in competitor offerings, will be key. Focusing on specific areas where incumbent vendors may be weak, such as limited OT threat intelligence or insufficient support for NERC CIP compliance, can also be effective.

Responses to timing and budget objections should emphasize the potential costs of inaction, highlighting the significant financial and operational impact of cyber incidents in the energy sector and the strong ROI that proactive OT security measures can provide. Offering flexible payment options, a phased implementation approach that aligns with their budget constraints, or demonstrating the potential for cost savings through improved operational efficiency and reduced compliance risks can also help overcome these objections.

To address technical feasibility concerns, NCC-Dragos should provide comprehensive technical documentation detailing the solution's architecture, integration capabilities, and minimal impact on OT network performance. Offering a proof-of-concept deployment in a representative environment can also effectively demonstrate the solution's compatibility and effectiveness. Being prepared to address any specific technical requirements or concerns raised by KAMO's technical teams is essential.

Change management objections can be addressed by outlining a clear and well-supported implementation plan that minimizes disruption to operations. Providing comprehensive training and user-friendly documentation for the Dragos Platform, highlighting its ease of use, and emphasizing the long-term benefits of improved security and reduced risk can help alleviate concerns about the impact on their internal teams and processes.

**6. Implementation Roadmap**

**6.1 Implementation Methodology for KAMO Energy:**

A phased deployment approach is recommended for KAMO Energy. Phase 1 should focus on rapidly deploying the Dragos Platform to achieve comprehensive asset visibility across their critical OT network segments. This initial phase will provide a foundational understanding of their environment and identify immediate vulnerabilities. Phase 2 will involve implementing threat detection and alerting rules tailored to the specific threats targeting the energy sector and KAMO's unique infrastructure. This will enable proactive monitoring and early detection of malicious activity. Phase 3 could involve engaging NCC Group's expertise for a thorough NERC CIP compliance assessment and the development of remediation strategies to address any identified gaps. Phase 4 would focus on establishing a comprehensive incident response plan, potentially including an IR Retainer with NCC Group, to ensure they are prepared to effectively handle any future security incidents.

Resource requirements for the implementation will include deployment engineers and security analysts from NCC-Dragos to manage the technical aspects of the deployment and configuration of the Dragos Platform. KAMO Energy will need to provide access to their IT and OT network infrastructure, as well as allocate personnel from their IT, OT, and security teams to collaborate with the NCC-Dragos team and provide subject matter expertise. A dedicated project manager from both organizations will be essential for coordinating the implementation process.

A realistic timeline with clearly defined milestones should be developed collaboratively with KAMO Energy. Key milestones could include the project kickoff meeting, completion of the initial asset discovery and vulnerability assessment, configuration of threat detection rules, completion of the NERC CIP compliance assessment, finalization of the incident response plan, and the go-live date for the full solution.

Success criteria for the implementation should be specific and measurable. This could include achieving a defined percentage of asset visibility within a specific timeframe, successful integration of the Dragos Platform with key OT systems, completion of initial training for KAMO's security team, and a positive assessment of their NERC CIP compliance posture following the implementation.

A proactive change management approach will be crucial for a smooth implementation. This will involve clear and consistent communication with all stakeholders at KAMO Energy about the project's progress and any potential impacts on their operations. Engaging key stakeholders early in the process, providing comprehensive training on the new platform and processes, and addressing any concerns or resistance to change will be essential for successful adoption.

**6.2 Strategic Expansion Opportunities at KAMO Energy:**

The initial engagement with KAMO Energy should aim for a focused deployment that addresses their most pressing immediate needs, such as gaining visibility into their critical OT assets and improving their NERC CIP compliance posture. Once this initial value is demonstrated and a strong relationship is established, opportunities for strategic expansion can be explored.

Cross-sell opportunities include leveraging NCC Group's broader portfolio of cybersecurity services. This could involve offering managed security services to augment KAMO's internal team, providing regular penetration testing of their IT and OT environments, and establishing a comprehensive incident response retainer to ensure they have expert support available in case of a security incident.

Solution expansion paths within the Dragos Platform can also be pursued. As KAMO's security maturity evolves, they may be interested in deploying additional modules and features, such as OT Watch for proactive threat hunting and deeper integration capabilities with their existing security information and event management (SIEM) or other security tools.

Developing a long-term relationship based on trust and mutual success is paramount. NCC-Dragos should aim to become a trusted advisor to KAMO Energy, providing ongoing support, proactively identifying future security needs and challenges, and collaborating on strategic security initiatives.

Ultimately, the goal should be to help KAMO Energy enhance their overall security maturity across both their IT and OT environments. This could potentially lead to expanding the engagement beyond the initial OT focus to address broader cybersecurity challenges within their organization.

**6.3 Proof of Concept Strategy for KAMO Energy:**

A focused Proof of Concept (POC) is highly recommended for KAMO Energy. The POC scope should be carefully defined to address a specific pain point or compliance requirement. For instance, it could focus on gaining comprehensive visibility into a critical segment of their high-voltage transmission network or demonstrating the Dragos Platform's ability to detect specific types of threats known to target the energy sector, such as those associated with VOLTZITE or ELECTRUM.

Success metrics for the POC should be clearly defined and measurable. This could include achieving a predetermined level of asset visibility within the defined network segment, successfully detecting simulated threat activity, or demonstrating the platform's ease of use and the value of its threat intelligence capabilities.

A clear plan for transitioning from a successful POC to a full production deployment should be outlined. This plan should detail the steps involved in scaling the deployment across their entire OT environment, integrating the platform with their existing systems, and ensuring a smooth and efficient transition process.

The POC timeline should be realistic and agreed upon with KAMO Energy, taking into account the complexity of their environment and the availability of resources from both teams. The resource needs from NCC-Dragos would include personnel for platform deployment, configuration, and support during the POC. KAMO Energy would need to allocate personnel from their IT, OT, and security teams to participate in the POC, provide necessary access, and evaluate the results.

Effective stakeholder management during the POC is crucial. Identifying and engaging the key stakeholders from KAMO Energy who will be involved in the POC, including technical personnel and decision-makers, ensuring their buy-in and active participation, and regularly communicating the POC's progress and results will be essential for its success.

**6.4 Long-Term Success Measurement at KAMO Energy:**

Demonstrating ongoing value will be crucial for long-term success. NCC-Dragos should provide regular reports to KAMO Energy detailing the value delivered by their solution, such as the number of threats detected and mitigated, the improvement in their OT security posture, and their progress towards achieving and maintaining NERC CIP compliance.

Key security improvement metrics should be tracked over time. These could include a reduction in the number of identified vulnerabilities in their OT environment, an improvement in the average time to detect and respond to security incidents, and an overall strengthening of their security controls as a result of the NCC-Dragos engagement.

Business impact reporting should clearly demonstrate how the security improvements are contributing to KAMO Energy's core business objectives. This includes highlighting the role of enhanced security in maintaining the reliability and availability of their power transmission network, minimizing disruptions to their broadband services, and protecting their reputation as a trusted energy provider.

Recommendations for an executive dashboard should be provided to KAMO Energy's leadership. This dashboard should include key metrics and visualizations that offer a clear and concise overview of their OT security posture, the value being delivered by the NCC-Dragos solution, and their progress towards achieving strategic security goals.

A client success timeline should be established, outlining key milestones for achieving long-term success and demonstrating the ongoing value of the partnership. Regular communication, proactive support, and a focus on continuous improvement will be essential for maintaining a strong and mutually beneficial long-term relationship with KAMO Energy.

**7. Battle Card**

**7.1 Company Profile Snapshot of KAMO Energy:**

KAMO Electric Cooperative, Inc. (KAMO Power) is a Generation and Transmission (G&T) cooperative headquartered in Vinita, Oklahoma 1. Key company statistics include an estimated annual revenue in the range of $10 million to $50 million 84 and approximately 147 employees 84. KAMO Power serves 17 member distribution cooperatives across northeast Oklahoma and southwest Missouri 1. Key decision-makers likely include the CEO, CTO Walt Kenyon 53, Chief Operations Officer T. G., and Chief Financial Officer A. H84. (further research is needed to identify specific individuals). Their current security posture likely involves a significant focus on NERC CIP compliance, potentially with ongoing efforts to address past violations 11. They likely have a mix of modern and legacy OT systems, some level of IT/OT convergence through cloud usage 53, and face exposure to sophisticated threat actors, supply chain risks, and remote access vulnerabilities.

**7.2 Primary Pain Points of KAMO Energy:**

Top business challenges for KAMO Energy include the constant need to maintain a reliable and low-cost power supply for their members 1. They are also focused on expanding their broadband services in rural areas through their subsidiary K-Powernet 4. Adapting to evolving energy trends, including the potential integration of more renewable energy sources, presents another key challenge 7.

Critical security gaps likely exist within their OT environment, potentially including a lack of comprehensive visibility, challenges in managing and securing legacy systems 54-58, risks associated with remote access 74-78, and ensuring robust monitoring capabilities. Potential vulnerabilities in industrial protocols 79-83 and weaknesses highlighted by their past NERC violation 11 are also critical areas of concern.

Specific OT security vulnerabilities likely include those inherent in legacy systems, risks associated with potentially unsecure remote access connections, and potential weaknesses in the security of their industrial control protocols. Their reliance on a complex supply chain also introduces vulnerabilities 70-73.

KAMO Energy faces significant compliance pressures, primarily driven by the mandatory NERC CIP standards 10 and the need to avoid penalties for non-compliance 47.

**7.3 Decision-Maker Matrix for KAMO Energy:**

| **Role** | **Name** | **Pain Points** | **Value Proposition** | **Likely Objections** | **Contact Strategy** |
| --- | --- | --- | --- | --- | --- |
| CISO |  | OT security concerns, NERC CIP compliance, critical infrastructure protection, managing cyber threats, securing IT/OT convergence, lack of OT visibility | Enhanced OT security visibility and threat detection, improved NERC CIP compliance, reduced risk of downtime, better protection for transmission and broadband infrastructure | Cost, integration with existing tools, resource constraints, complexity of OT security | Focus on OT security criticality, KAMO's challenges, offer assessment |
| CIO |  | Secure digital transformation, managing IT/OT convergence, securing cloud, supporting broadband expansion | Comprehensive IT/OT security coverage, secure remote access, cloud security expertise, security integrated into expansion | Budget, impact on network performance, existing IT security investments | Highlight unified IT/OT security, benefits of NCC-Dragos joint solution |
| VP of Operations |  | Maintaining reliable power, minimizing disruptions, ensuring field safety, improving efficiency | Enhanced OT security and resilience, preventing cyber-related downtime, improved operational visibility, safe remote operations | Disruption to OT systems during deployment, complexity of OT security, impact on performance | Focus on reliability and safety improvements through cyber security |
| Head of Regulatory Compliance |  | Ensuring NERC CIP adherence, managing audits, addressing past violations, staying updated on regulations | Expertise in NERC CIP, Dragos Platform for compliance, audit support, proactive identification of gaps | Cost of compliance solutions, perceived burden of new controls, skepticism about effectiveness | Emphasize NERC Group's CIP expertise, streamlined compliance efforts, reduced violation risk |

**7.4 Solution Configuration for KAMO Energy:**

The recommended NCC-Dragos solution stack for KAMO Energy includes the Dragos Platform for comprehensive OT asset visibility, advanced threat detection, and efficient incident response. Complementing this, NCC Group's expertise should be leveraged for NERC CIP compliance consulting to ensure regulatory adherence and mitigate the risk of penalties. An Incident Response Retainer with NCC Group will provide KAMO Energy with access to specialized OT cybersecurity expertise and support in the event of a security incident.

A phased implementation approach is advised. Phase 1 should focus on the rapid deployment of the Dragos Platform to establish a complete inventory of OT assets and gain immediate visibility into their security posture. Phase 2 will involve configuring and tuning threat detection and alerting rules specifically tailored to the energy sector and the threats most relevant to KAMO Energy's environment. Phase 3 will engage NCC Group's consultants to conduct a thorough assessment of KAMO's current NERC CIP compliance posture and develop a roadmap for addressing any identified gaps and ensuring ongoing compliance. Phase 4 will establish a formal incident response plan and an IR Retainer with NCC Group to provide expert support and guidance in the event of a security incident.

The initial focus area should be achieving comprehensive visibility into KAMO Energy's critical OT environment, particularly the segments of their transmission network that are most vital for maintaining grid reliability. This will provide immediate security benefits and lay the foundation for subsequent phases of the implementation.

Quick wins for KAMO Energy include the rapid deployment and initial configuration of the Dragos Platform, which will provide immediate visibility into their OT assets and identify potential vulnerabilities. Strategic improvements will involve the implementation of OT network segmentation to isolate critical assets, the enhancement of their incident response capabilities through NCC Group's expertise, and the achievement and maintenance of full NERC CIP compliance.

**7.5 Competitive Displacement Strategy for KAMO Energy:**

Analysis of KAMO Energy's current vendors (to be researched) likely reveals a reliance on general IT security vendors and potentially some basic OT security tools that lack the depth and specialization required for a robust defense. Key competitive differentiators for NCC-Dragos include Dragos's purpose-built OT cybersecurity platform and deep expertise in the energy sector, combined with NCC Group's comprehensive security consulting and services, including strong NERC CIP knowledge.

Win themes against general IT security vendors should emphasize NCC-Dragos's specialized focus on OT security, highlighting that OT environments have unique requirements that generic IT tools cannot adequately address. Against less comprehensive OT security vendors, the win theme should focus on the Dragos Platform's superior visibility, more accurate and actionable threat intelligence derived from real-world OT incidents, and comprehensive incident response capabilities specifically tailored for industrial control systems.

Potential weaknesses of incumbent vendors (to be researched) could include a lack of deep OT-specific expertise, limited threat intelligence relevant to industrial control systems, insufficient support for navigating the complexities of NERC CIP compliance, or a lack of integrated incident response capabilities for OT environments.

**7.6 Objection Handling Guide for KAMO Energy:**

| **Objection** | **Response** | **Supporting Evidence** | **Relevant Case Study** |
| --- | --- | --- | --- |
| "OT security is too expensive." | "The cost of a cyber incident in the energy sector can be substantial, averaging millions of dollars 85. Our solution helps prevent these costly incidents and provides a strong ROI, often exceeding 300% 89." | Industry reports on cyberattack costs in energy, ROI studies for OT security solutions. | Case study of an energy company preventing a multi-million dollar incident with Dragos. |
| "We don't have the internal resources to manage another security tool." | "The Dragos Platform is designed for ease of use, and we provide comprehensive training and ongoing support. NCC Group also offers managed services to augment your team and handle the day-to-day management." | Information on Dragos Platform's user-friendliness, details of NCC Group's managed security services. | Case study of a utility with limited resources successfully utilizing the Dragos Platform with NCC Group's support. |
| "Our current IT security measures should be sufficient for OT." | "OT environments have unique protocols and security requirements that differ significantly from IT. Standard IT security tools lack the necessary visibility and threat intelligence for OT 51." | White papers on IT vs. OT security differences, reports on attacks bypassing IT security to impact OT. | Case study of an energy company experiencing an OT incident despite robust IT security measures. |
| "We are already compliant with NERC CIP." | "While you may have achieved compliance, our solution helps maintain and improve your security posture beyond the basic requirements, reducing your overall risk and ensuring continuous compliance with evolving standards 43." | Information on benefits of exceeding basic NERC CIP compliance, details on Dragos Platform's compliance-aiding features. | Case study of a utility using NCC Group and Dragos to significantly enhance their NERC CIP compliance and overall security. |

**7.7 ROI Model for KAMO Energy:**

The cost of a cyber breach in the energy sector can average between $4.65 million and $5.24 million 85. Implementing NCC-Dragos solutions can help prevent such incidents, leading to significant cost avoidance. Operational efficiency gains can be realized through reduced downtime of their transmission network, estimated conservatively at a potential savings of $100,000 per incident avoided. Avoiding NERC CIP violations, which can result in substantial fines, could save KAMO Energy upwards of $1 million per violation. Security resource optimization can be achieved by automating threat detection and response, potentially freeing up 10% of a security analyst's time, valued at approximately $15,000 annually per analyst. Conservatively projecting the prevention of just one major cyber incident and one significant NERC CIP violation over three years, coupled with operational efficiency gains and resource optimization, the total value projection for KAMO Energy from investing in NCC-Dragos solutions could exceed $6 million over the three-year period, demonstrating a strong return on their investment.

**8. About NCC Group and Dragos**

NCC Group is a global cybersecurity firm with extensive capabilities in consulting, managed services, and incident response, including a specialized IR Retainer service. Their Foundational Security Testing (FDD) can provide a comprehensive assessment of KAMO Energy's current security posture. Dragos is the leading provider of OT cybersecurity solutions, offering the purpose-built Dragos Platform that delivers unparalleled asset visibility, advanced threat detection, and efficient incident response capabilities for industrial control systems. Their OT Watch service provides proactive threat intelligence tailored to the energy sector. The joint solution offered by NCC Group and Dragos provides comprehensive security coverage across both IT and OT environments, combining deep expertise in both domains. This partnership offers proactive threat detection and response capabilities specifically designed for the unique challenges of the energy sector, leading to improved NERC CIP compliance and enhanced operational resilience for organizations like KAMO Energy. NCC Group and Dragos have a proven track record of successful engagements with other clients in the energy sector, demonstrating their ability to deliver significant value and improve the security posture of critical infrastructure providers.

**9. References and Citations**

1

**Conclusions and Recommendations:**

The analysis of KAMO Energy's business initiatives, OT environment, and industry context indicates a significant opportunity for NCC Group and Dragos to provide substantial value. KAMO Energy is actively investing in modernizing and expanding its infrastructure, which necessitates a robust and specialized approach to cybersecurity, particularly for their critical OT environment. The regulatory landscape, especially NERC CIP compliance, further underscores the importance of a strong security posture.

It is recommended that the NCC Group sales team prioritize engaging with KAMO Energy, focusing on the immediate need for enhanced OT visibility and threat detection, as well as support for NERC CIP compliance. The initial outreach should target key decision-makers with tailored messaging that addresses their specific pain points and highlights the unique benefits of the NCC-Dragos joint solution. A non-intrusive technical assessment using the Dragos Platform should be proposed early in the engagement process to demonstrate the value and capabilities of the solution in KAMO's specific environment.

A phased implementation approach, starting with quick wins like asset visibility and progressing to more strategic improvements such as network segmentation and enhanced incident response, will likely resonate well with KAMO Energy. Demonstrating a clear return on investment, particularly in terms of preventing costly cyber incidents and avoiding NERC CIP penalties, will be crucial for securing the engagement. By positioning NCC Group and Dragos as trusted advisors with deep expertise in OT cybersecurity for the energy sector, the sales team can establish a strong and long-lasting partnership with KAMO Energy, contributing to the security and resilience of critical energy infrastructure.

#### Works cited

1. KAMO Power: Home, accessed March 21, 2025, <https://kamopower.com/>
2. KAMO Power Promotes Digital Inclusion with 400G-ready Optical Network, accessed March 21, 2025, <https://www.infinera.com/case-study/kamo-power>
3. KAMO Power Deploys Infinera's XTM Series to Upgrade Its Rural Broadband Network, accessed March 21, 2025, <https://www.infinera.com/press-release/kamo-power-deploys-infinera-xtm-series-to-upgrade-its-rural-broadband-network/>
4. KAMO Electric Cooperative, Inc. (KAMO Power) / K-Powernet LLC - Oklahoma Watch, accessed March 21, 2025, <https://oklahomawatch.opalstacked.com/arpa/10389>
5. 2025 Rate Increase Information - Ozark Electric Cooperative, accessed March 21, 2025, <https://www.ozarkelectric.com/my-post>
6. Southwest Missouri - Ozark Electric Cooperative, accessed March 21, 2025, <https://www.ozarkelectric.com/2025-rate-increase-information>
7. Green Power, accessed March 21, 2025, <https://kamopower.com/green-power>
8. Cybersecurity and Grid Resilience - America's Electric Cooperatives - NRECA, accessed March 21, 2025, <https://www.electric.coop/issues-and-policy/cybersecurity-and-grid-resilience>
9. Oklahoma G&T Takes Extra Steps to Protect Nighttime Crews - Cooperative.com, accessed March 21, 2025, <https://www.cooperative.com/news/Pages/KAMO-Power-Takes-Extra-Steps-to-Protect-Nighttime-Crews.aspx>
10. September 18, 2019 The Honorable Kimberly D. Bose Secretary Federal Energy Regulatory Commission 888 First Street NE Washington - Southwest Power Pool, accessed March 21, 2025, <https://www.spp.org/documents/60647/20190918_2987r1%20aeci%20and%20pso%20and%20kamo%20interconnection%20agreement_er19-2827.pdf>
11. NERC Case Notes: Reliability Standard TOP-004-2, accessed March 21, 2025, <https://www.whitecase.com/insight-alert/nerc-case-notes-reliability-standard-top-004-2>
12. RELIABILITY | RESILIENCE | SECURITY - NERC, accessed March 21, 2025, <https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_FinalFiled_NOP_NOC-2681.pdf>
13. KAMO Power - Products, Competitors, Financials, Employees, Headquarters Locations, accessed March 21, 2025, <https://www.cbinsights.com/company/kamo-power>
14. Top Trends Affecting Electric Cooperatives in 2025 - Capp/USA, accessed March 21, 2025, <https://cappusa.com/top-trends-affecting-electric-cooperatives-in-2025>
15. U.S. Not-For-Profit Public Power, Electric Cooperative, And Gas Utilities 2025 Outlook: Climate Change, Energy Transition, And Load Growth Underlie Negative Trends | S&P Global Ratings, accessed March 21, 2025, <https://www.spglobal.com/ratings/en/research/articles/250114-u-s-not-for-profit-public-power-electric-cooperative-and-gas-utilities-2025-outlook-climate-change-energy-13377866>
16. Electric Co-op Facts & Figures - America's Electric Cooperatives, accessed March 21, 2025, <https://www.electric.coop/electric-cooperative-fact-sheet>
17. Electric Co-op Technology Trends for the Next 25 Years - Cooperative.com, accessed March 21, 2025, <https://www.cooperative.com/remagazine/articles/pages/technology-tends-how-electric-co-ops-will-change-next-25-years.aspx>
18. U.S. Public Power And Electric Cooperative Utilities 2024 Outlook: Mandates, Rising Costs, And Diminishing Affordability | S&P Global Ratings, accessed March 21, 2025, <https://www.spglobal.com/ratings/en/research/articles/240123-u-s-public-power-and-electric-cooperative-utilities-2024-outlook-mandates-rising-costs-and-diminishing-aff-12968567>
19. Enhancing Cybersecurity - Oklahoma Association of Electric Cooperatives, accessed March 21, 2025, <https://oaec.coop/2022/03/enhancing-cybersecurity/>
20. Industry Links | KAMO Power, accessed March 21, 2025, <https://www.kamopower.com/industry-links>
21. KAMO Power - Association of Missouri Electric Cooperatives, accessed March 21, 2025, <https://www.moelectriccoops.com/facilities/kamo-power/>
22. Cooperative Principles | Association of Missouri Electric Cooperatives, accessed March 21, 2025, <https://amec.org/cooperative-principles>
23. Associations That Matter: Association of Missouri Electric Cooperatives, accessed March 21, 2025, <https://themissouritimes.com/associations-that-matter-association-of-missouri-electric-cooperatives/>
24. Association of Missouri Electric Cooperatives, accessed March 21, 2025, <https://www.moelectriccoops.com/>
25. Association of Missouri Electric Cooperatives: Home, accessed March 21, 2025, <https://amec.org/>
26. Preventing electrical emergencies - Cuivre River Electric Cooperative, accessed March 21, 2025, <https://www.cuivre.com/knowingwhattodo>
27. 2023 annual report - Associated Electric Cooperative Inc., accessed March 21, 2025, <https://aeci.org/media/7082/2023-annual-report-associated-electric-cooperative-spreads.pdf>
28. Structure | KAMO Power, accessed March 21, 2025, <https://www.kamopower.com/structure>
29. Three-tiered System & Service Area | Associated Electric Cooperative Inc., accessed March 21, 2025, <https://www.aeci.org/three-tiered-system-service-area>
30. Oklahoma Assn of Electric Cooperatives, accessed March 21, 2025, <https://oaec.coop/>
31. Industry Partners | East Central Electric Cooperative, accessed March 21, 2025, <https://www.ecoec.com/industry-partners>
32. Oklahoma's Electric Cooperatives - Powerful Web Design for Utilities, accessed March 21, 2025, <https://www.powerfulweb.com/case-study/oklahoma-association-of-electric-cooperatives/>
33. From the Top — Mar. 2025 | OEC News - Oklahoma Electric Cooperative, accessed March 21, 2025, <https://okcoop.org/ceo-mar-2025-oec-news/>
34. Oklahoma Electric Cooperative News March 2025 - Issuu, accessed March 21, 2025, <https://issuu.com/oklaelec/docs/oklahoma_electric_cooperative_news_march_2025>
35. Compliance | Federal Energy Regulatory Commission, accessed March 21, 2025, <https://www.ferc.gov/enforcement-legal/enforcement/compliance>
36. Regulatory Compliance | Department of Energy, accessed March 21, 2025, <https://www.energy.gov/em/regulatory-compliance>
37. COMPLIANCE HANDBOOK - Federal Energy Regulatory Commission, accessed March 21, 2025, <https://www.ferc.gov/sites/default/files/2020-04/ComplianceHandbook.pdf>
38. Federal Energy Regulatory Commission rules in favor of clean energy growth, accessed March 21, 2025, <https://www.selc.org/news/federal-energy-regulatory-commission-rules-in-favor-of-clean-energy-growth/>
39. What FERC Does | Federal Energy Regulatory Commission, accessed March 21, 2025, <https://www.ferc.gov/what-ferc-does>
40. Federal Energy Regulatory Commission: Home Page, accessed March 21, 2025, <https://ferc.gov/>
41. Co-op utility group joins fight against FERC's transmission planning rule - Factor This™, accessed March 21, 2025, <https://www.renewableenergyworld.com/power-grid/transmission/co-op-utility-group-joins-fight-against-fercs-transmission-planning-rule/>
42. Co-ops to FERC: Diverse Portfolio Key to Reliable, Affordable Power - NRECA, accessed March 21, 2025, <https://www.electric.coop/co-ops-to-ferc-diverse-portfolio-key-to-reliable-affordable-power>
43. What Is NERC CIP and Why Is It Important? - Kiteworks, accessed March 21, 2025, <https://www.kiteworks.com/risk-compliance-glossary/nerc-cip/>
44. NERC CIP: A Complete Guide to OT Security for Critical Infrastructure - OTORIO, accessed March 21, 2025, <https://www.otorio.com/resources/what-is-nerc-cip/>
45. NERC CIP Compliance: Ensuring Security with LastPass, accessed March 21, 2025, <https://blog.lastpass.com/posts/nerc-cip-compliance>
46. Why NERC CIP Compliance Matters: 10 Key Reasons - AssurX, accessed March 21, 2025, <https://www.assurx.com/why-nerc-cip-compliance-matters-10-key-reasons/>
47. NERC CIP Compliance: What It Is and Why You Need to Know About It - Carbide Security, accessed March 21, 2025, <https://carbidesecure.com/resources/what-is-nerc-cip/>
48. Protecting Energy Sector Industrial Control System: The Role of PrivX PAM Solution, accessed March 21, 2025, <https://www.ssh.com/academy/pam/protecting-energy-sector-industrial-control-system-role-of-privx-pam-solution>
49. Industrial Control Systems (Energy & Power) Market Size and Trends 2029, accessed March 21, 2025, <https://www.techsciresearch.com/report/industrial-control-systems-energy-power-market/23011.html>
50. What Are Industrial Control Systems?, accessed March 21, 2025, <https://blog.ivesequipment.com/2018/01/what-are-industrial-control-systems.html>
51. A brief introduction to Industrial Control Systems and Security - BitSight Technologies, accessed March 21, 2025, <https://www.bitsight.com/blog/brief-introduction-industrial-control-systems-and-security>
52. Electrical Control Systems for Power Transmission - MAC Products, accessed March 21, 2025, <https://www.macproducts.net/blog/how-electrical-control-systems-support-electrical-power-transmission>
53. TechSurveillance - Cooperative.com, accessed March 21, 2025, <https://www.cooperative.com/programs-services/bts/Documents/TechSurveillance/ts_demystifying_the_cloud_sept_2015.pdf>
54. Overcoming OT Security Challenges and Complexities - Supply Chain Digital, accessed March 21, 2025, <https://supplychaindigital.com/articles/overcoming-ot-security-challenges-and-complexities>
55. Securing Legacy OT Systems: Challenges & Strategies | 2023 - Sectrio, accessed March 21, 2025, <https://sectrio.com/blog/securing-legacy-ot-systems-challenges-and-strategies/>
56. The cybersecurity challenges of legacy OT and how to manage them - Control Engineering, accessed March 21, 2025, <https://www.controleng.com/the-cybersecurity-challenges-of-legacy-ot-and-how-to-manage-them/>
57. OT Security Challenges and How to Solve Them - Verve Industrial, accessed March 21, 2025, <https://verveindustrial.com/resources/blog/ot-security-challenges/>
58. Legacy OT risks: The hinderances of aging systems – and how to move forward, accessed March 21, 2025, <https://blog.se.com/digital-transformation/cybersecurity/2024/07/11/legacy-ot-risks-and-how-to-move-forward/>
59. sepiocyber.com, accessed March 21, 2025, <https://sepiocyber.com/resources/whitepapers/cyber-attacks-against-energy-sector/#:~:text=Energy%20Sector%20Cyber%20Security%3A%20Actors,by%20geopolitical%20or%20ideological%20goals.>
60. Cybersecurity in Energy Sector - Sepio Cyber, accessed March 21, 2025, <https://sepiocyber.com/resources/whitepapers/cyber-attacks-against-energy-sector/>
61. Top 6 Industries Targeted By Threat Actors In 2024 - Cyble, accessed March 21, 2025, <https://cyble.com/knowledge-hub/top-6-industries-targeted-by-threat-actors-in-2024/>
62. Energy Sector Cyber Threat Intelligence | Cybersixgill, accessed March 21, 2025, <https://cybersixgill.com/use-cases/industries/energy-sector>
63. The Top 5 Cyber Threats in the Energy Sector - Avertium, accessed March 21, 2025, <https://www.avertium.com/resources/threat-reports/top-5-cyber-threats-in-energy-sector>
64. Power for the People | Cyber Threats in the Energy Sector and How To Defend Against Them - SentinelOne, accessed March 21, 2025, <https://www.sentinelone.com/blog/power-for-the-people-cyber-threats-in-the-energy-sector-and-how-to-defend-against-them/>
65. Hybrid Warfare - Marinelink, accessed March 21, 2025, <https://www.marinelink.com/news/hybrid-warfare-523502>
66. Connecting the Dots: State Actors, Hacktivists, and Critical Infrastructure Attacks in 2024, accessed March 21, 2025, <https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2025/february/State-Actors-Hacktivists-Critical-Infrastructure-Attacks/>
67. Ransomware, state actors, hacktivists exploited geopolitical tensions to target critical infrastructure in 2024 - Industrial Cyber, accessed March 21, 2025, <https://industrialcyber.co/reports/ransomware-state-actors-hacktivists-exploited-geopolitical-tensions-to-target-critical-infrastructure-in-2024/>
68. Dragos Reports OT/ICS Cyber Threats Escalate Amid Geopolitical Conflicts and Increasing Ransomware Attacks, accessed March 21, 2025, <https://www.dragos.com/resources/press-release/dragos-reports-ot-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks/>
69. Dragos says 2024 lowered the barrier for OT/ICS attacks - - Enterprise Times, accessed March 21, 2025, <https://www.enterprisetimes.co.uk/2025/02/26/dragos-says-2024-lowered-the-barrier-for-ot-ics-attacks/>
70. DNV report highlights increased OT cybersecurity investment in energy sector due to escalating threats - Industrial Cyber, accessed March 21, 2025, <https://industrialcyber.co/utilities-energy-power-water-waste/dnv-report-highlights-increased-ot-cybersecurity-investment-in-energy-sector-due-to-escalating-threats/>
71. Addressing the Growing Supply Chain Cyber Threats Facing the UKs Critical Energy Infrastructure - Risk Ledger, accessed March 21, 2025, <https://riskledger.com/resources/supply-chain-cyber-threats-energy>
72. 8 Key Insights for Managing OT Threats in the Energy Sector | NCC Group, accessed March 21, 2025, <https://www.nccgroup.com/us/8-key-insights-for-managing-ot-threats-in-the-energy-sector/>
73. Why US Energy Sector is at High Risk of Supply Chain Attacks, accessed March 21, 2025, <https://supplychaindigital.com/supply-chain-risk-management/us-energy-sector-high-risk-supply-chain-attacks>
74. Study Finds Excessive Use of Remote Access Tools in OT Environments - SecurityWeek, accessed March 21, 2025, <https://www.securityweek.com/study-finds-excessive-use-of-remote-access-tools-in-ot-environments/>
75. Best Practices for Secure Remote OT Access - SSH Communications Security, accessed March 21, 2025, <https://www.ssh.com/academy/operational-technology/best-practices-for-secure-remote-ot-access>
76. Remote Access Tool Sprawl Increases OT Risks - BankInfoSecurity, accessed March 21, 2025, <https://www.bankinfosecurity.com/remote-access-tool-sprawl-increases-ot-risks-a-26288>
77. 55% of OT Environments Contain Four or More Remote Access Tools, Greatly Expanding Attack Surface and Operational Complexity | Claroty, accessed March 21, 2025, <https://claroty.com/press-releases/55-percent-of-ot-environments-contain-four-or-more-remote-access-tools-greatly-expanding-attack-surface-and-operational-complexity>
78. Identifying Risks in Third-Party OT Remote Access - Claroty, accessed March 21, 2025, <https://claroty.com/blog/third-party-remote-access-in-ot-security-operational-risks>
79. Cyber security Threats in Industrial Networks and How to Mitigate Them - Omnitron Systems, accessed March 21, 2025, <https://www.omnitron-systems.com/blog/cybersecurity-threats-in-industrial-networks-and-how-to-mitigate-them>
80. Unveiling the Dark Side: Common Attacks and Vulnerabilities in Industrial Control Systems, accessed March 21, 2025, <https://www.aon.com/en/insights/cyber-labs/unveiling-the-dark-side-common-attacks-and-vulnerabilities-in-industrial-control-systems?collection=5b76135e-4196-415b-ab1d-f42b6f0abb10&parentUrl=null>
81. Manufacturing Security Vulnerabilities: Combating the Risks - Nuspire, accessed March 21, 2025, <https://www.nuspire.com/blog/manufacturing-security-vulnerabilities-combating-the-risks/>
82. Why OT environments are vulnerable – and what to do about it | SC Media, accessed March 21, 2025, <https://www.scworld.com/perspective/why-ot-environments-are-vulnerable-and-what-to-do-about-it>
83. Top Vulnerabilities In Industrial Control Systems - Antaira Technologies, accessed March 21, 2025, <https://www.antaira.com/Top-Vulnerabilities-in-Industrial-Control-Systems>
84. KAMO Power Company Overview, Contact Details & Competitors | LeadIQ, accessed March 21, 2025, <https://leadiq.com/c/kamo-power/5a1d85e32400002400604412>
85. The Downside of Digital Transformation for Utilities: Data Privacy and Cybersecurity Risks, accessed March 21, 2025, <https://www.sustainalytics.com/esg-research/resource/investors-esg-blog/the-downside-of-digital-transformation-for-utilities--data-privacy-and-cybersecurity-risks>
86. Report: Cost of a Data Breach in Energy and Utilities - Security Intelligence, accessed March 21, 2025, <https://securityintelligence.com/articles/cost-data-breach-energy-utilities/>
87. Data breach costs for critical infrastructure sector exceed $5 million, as time 'new currency' in cybersecurity - Industrial Cyber, accessed March 21, 2025, <https://industrialcyber.co/reports/data-breach-costs-for-critical-infrastructure-sector-exceed-5-million-as-time-new-currency-in-cybersecuritydata-breach-costs-for-critical-infrastructure-sector-exceed-5-million-as-time-new/>
88. Must-know cyber attack statistics and trends 2025 - Embroker, accessed March 21, 2025, <https://www.embroker.com/blog/cyber-attack-statistics/>
89. Are OT Security Investments Worth It?, accessed March 21, 2025, <https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/are-ot-security-investments-worth-it/>
90. Zero Trust OT Security: Protection for Industrial Operations - Palo Alto Networks, accessed March 21, 2025, <https://www.paloaltonetworks.com/network-security/zero-trust-ot-security>
91. The ROI of OT Security: Quantifying the Value of Protection - Cybervizer Newsletter, accessed March 21, 2025, <https://www.cybervizer.com/p/the-roi-of-ot-security-quantifying-the-value-of-protection>
92. OT Security - Securing Industrial & Manufacturing Environments in 2025 with Armis and Microsegmentation - Elisity, accessed March 21, 2025, <https://www.elisity.com/blog/ot-security-securing-industrial-manufacturing-environments-in-2025-with-armis-and-microsegmentation>
93. The Convergence of OT and IT: A Transformation in the Electric Business | Energy Central, accessed March 21, 2025, <https://energycentral.com/c/gr/convergence-ot-and-it-transformation-electric-business>
94. Five Best Practices For Industrial Cybersecurity: Closing The Gap Between IT And OT, accessed March 21, 2025, <https://www.forbes.com/councils/forbestechcouncil/2023/01/26/five-best-practices-for-industrial-cybersecurity-closing-the-gap-between-it-and-ot/>