## **Executive Brief: Securing Energy's Digital Future**

**Navigating OT Cybersecurity Challenges in the Era of Transformation with NCC Group & Dragos**

**Introduction**

The energy sector is undergoing a rapid digital transformation, integrating IT and Operational Technology (OT) to enhance efficiency, reliability, and sustainability. However, this convergence dramatically expands the cyber attack surface. As highlighted in the Dragos 2025 OT/ICS Cybersecurity Report and the DHS 2025 Homeland Threat Assessment, adversaries ranging from state-sponsored groups to ransomware operators and hacktivists are increasingly targeting energy infrastructure. Successfully navigating this complex landscape requires a specialized, integrated approach to cybersecurity that protects critical operations while enabling innovation. NCC Group and Dragos provide this essential partnership.

**The Challenge: Escalating Threats to Energy OT**

Energy companies face a unique and intensifying set of cyber threats with potentially devastating consequences for safety, operations, and national security:

1. **Sophisticated State-Sponsored Attacks:** Groups like VOLTZITE (China-linked) and KAMACITE/ELECTRUM (Russia-linked) actively target energy infrastructure, pre-positioning for disruption (as seen with VOLTZITE's focus on electric, oil & gas) and conducting espionage. Their use of "living-off-the-land" techniques and compromised infrastructure makes detection difficult. (Source: Dragos Report, DHS Assessment)
2. **Ransomware's Crippling Impact:** Ransomware attacks against industrial organizations surged 87% in 2024. While manufacturing is the top target, the energy sector remains highly vulnerable due to its low tolerance for downtime. Adversaries exploit VPNs, remote access, and credential weaknesses, with 25% of incidents leading to full OT shutdowns. (Source: Dragos Report)
3. **ICS-Specific Malware:** The emergence of malware like Fuxnet and FrostyGoop demonstrates adversaries' growing capability and intent to directly manipulate or disrupt OT processes (e.g., impacting heating systems, industrial sensors). (Source: Dragos Report)
4. **Exploitable Vulnerabilities:** Many vulnerabilities reside deep within OT networks (70%), often in legacy or third-party components. Exploits targeting perimeter devices (VPNs, firewalls) are increasing, providing initial access for broader attacks. DLL hijacking and insecure IoT devices present further risks. (Source: Dragos Report)
5. **Hacktivism & Geopolitical Spillover:** Groups like BAUXITE (Iran-linked) and various pro-Russia hacktivists exploit internet-exposed devices and leverage geopolitical conflicts to disrupt critical services, sometimes achieving Stage 2 ICS Kill Chain impacts (direct OT manipulation). (Source: Dragos Report, DHS Assessment)

**Impact on Energy Leaders:**

* **CISOs:** Struggle with visibility gaps between IT and OT, managing complex vulnerabilities, quantifying OT risk, ensuring compliance, and responding effectively to sophisticated threats.
* **COOs:** Face risks of operational disruption, safety incidents, environmental damage, significant financial losses, and reputational harm. Digital transformation initiatives can stall without adequate security.
* **OT Operations:** Need to maintain system availability and safety amidst increasing cyber threats, securely integrate new digital technologies, and manage vulnerabilities without disrupting critical processes.

**The Solution: Integrated IT/OT Security with NCC Group & Dragos**

NCC Group and Dragos offer a powerful combination of deep OT expertise and comprehensive cybersecurity services tailored for the energy sector's digital transformation journey:

* **Dragos - The OT Cybersecurity Leader:**
  + **Unmatched OT Visibility:** The Dragos Platform provides asset identification, threat detection, and vulnerability management specifically designed for ICS/OT environments, understanding unique industrial protocols and behaviors.
  + **Actionable Threat Intelligence:** World-class intelligence on OT-specific threat groups (tracking 23 groups), malware, and TTPs enables proactive defense.
  + **Expert OT Incident Response:** Specialized IR teams rapidly contain and remediate OT incidents, minimizing operational impact.
  + **OT Vulnerability Management:** Contextualized "Now, Next, Never" prioritization helps focus resources on the highest-risk vulnerabilities impacting operations.
* **NCC Group - Comprehensive Cyber Resilience Partner:**
  + **Strategic Guidance:** Consulting services help align security with digital transformation goals, manage risk (Strategy, Risk & Compliance), and build secure architectures for converged IT/OT environments.
  + **Specialized OT Security Services:** Leveraging the Dragos partnership, NCC Group provides OT-specific assessments, secure architecture design, converged IT/OT security operations, and facility due diligence.
  + **Technical Assurance:** Rigorous testing (penetration testing, attack simulation) identifies weaknesses across applications, networks (IT & OT), cloud, and hardware.
  + **Managed Security Services:** 24/7 Managed Extended Detection & Response (MXDR) monitors complex hybrid environments, integrating IT and OT data streams for unified threat detection.
  + **Holistic Incident Response:** Comprehensive IR capabilities cover readiness, management, and recovery across both IT and OT domains.
  + **Supply Chain & Third-Party Risk:** Services assess and mitigate risks introduced by vendors and software components.

**Key Benefits for Energy Sector Leaders:**

* **For the CISO:** Gain unified visibility across IT and OT; leverage expert OT threat intelligence; improve detection and response times; quantify and manage OT cyber risk effectively; achieve and maintain regulatory compliance.
* **For the COO:** Reduce risk of operational disruptions and safety incidents; enhance system reliability and resilience; enable secure and confident digital transformation; ensure business continuity.
* **For OT Operations:** Receive timely, OT-specific threat alerts; implement effective, context-aware vulnerability management; securely adopt new technologies; benefit from expert support during incidents.

**Take the Next Step**

The convergence of digital transformation and escalating OT cyber threats demands a proactive, integrated security strategy. NCC Group and Dragos provide the technology, intelligence, and expertise energy companies need to secure their operations and confidently embrace the future.

Contact us today to schedule a joint workshop or assessment and learn how we can help secure your digital transformation journey.