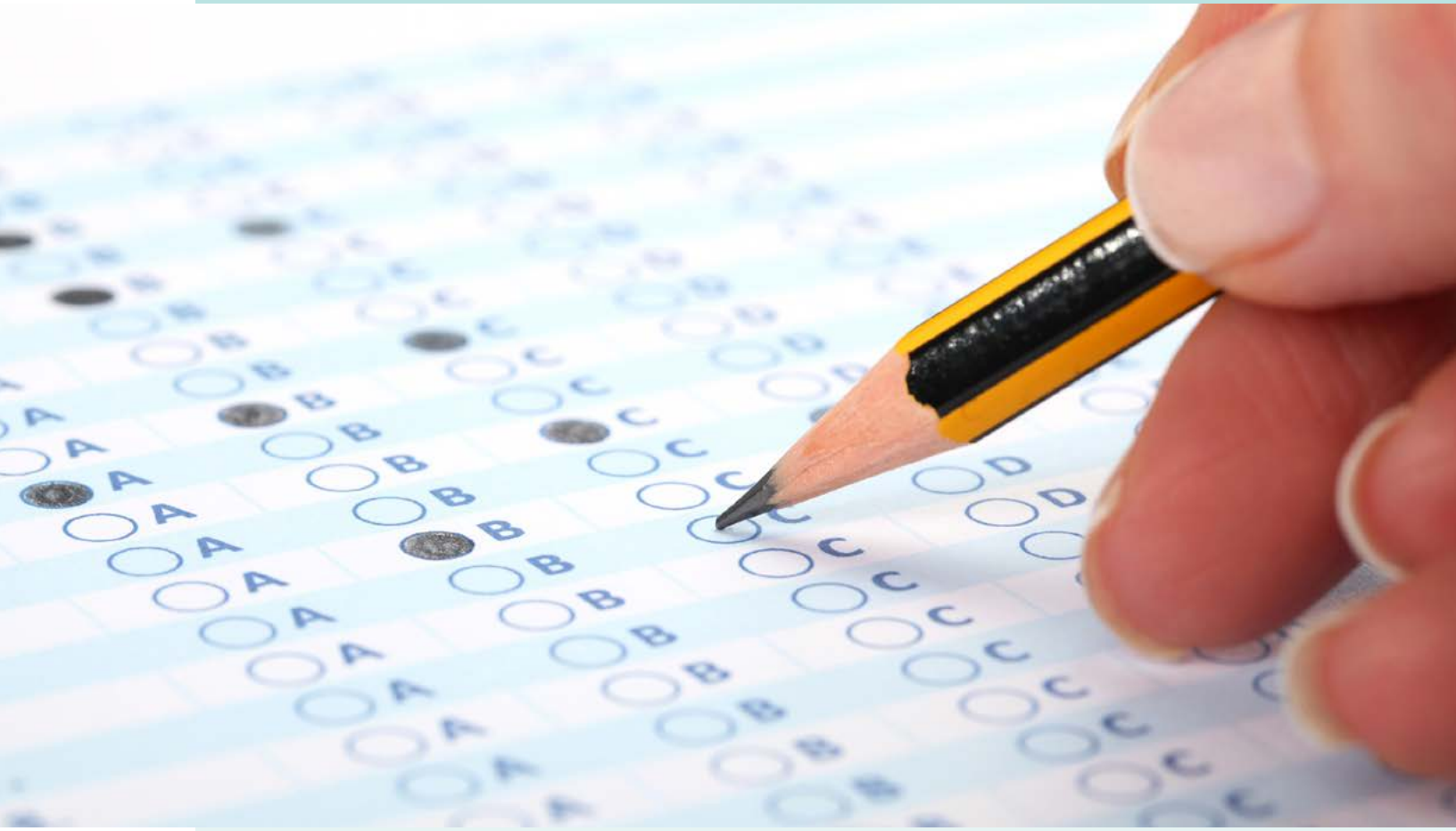
DRAGOS
SAFEGUARDING CIVILIZATION

Vendor Evaluation Checklist



From Transactions to Trust: Building Strong Cybersecurity Partnerships

A Checklist for Evaluating Your Cybersecurity Vendors

Selecting the right vendor for your cybersecurity needs is crucial for building a robust, scalable, and tailored security infrastructure. The right vendor brings specialized expertise, advanced tools, and comprehensive support, which are essential for effectively segmenting your network, enforcing security policies, and maintaining visibility and control over your OT environment. A well-chosen vendor ensures that your security measures are not only effective but also aligned with your specific operational needs, regulatory requirements, and budget constraints. This partnership is vital for minimizing risks, enhancing resilience against cyber threats, and ensuring the protection of critical assets.

Vendor Evaluation Checklist

When evaluating potential vendors, consider the following capabilities to ensure they meet your organization's needs:

PROVEN TRACK RECORD

- ☐ Does the vendor have a history of successful implementations in ICS/OT environments?
- ☐ Do they have team members with specific OT expertise and experience in your industry?

CUSTOMIZATION

- ☐ Can the vendor tailor their solutions to your specific industry and operational needs?
- ☐ Do they offer realistic and relevant scenarios that reflect potential threats to your organization?

INTEGRATION

- ☐ Does the vendor's solution integrate seamlessly with your existing systems and tools?
- ☐ Can the platform scale with your organization's growth and evolving needs?

USER-FRIENDLY INTERFACE AND SUPPORT

- ☐ Is the solution easy to use and manage for your security team?
- ☐ Does the vendor offer comprehensive training and ongoing support for their tools and technologies?

COST-EFFECTIVENESS AND ACCURATE SCOPING

- ☐ Are the vendor's solutions cost-effective and within your budget?
- ☐ Is the scope of your investment clear, and does it cover your needs?

COMPLIANCE

- ☐ Does the solution help you meet regulatory compliance requirements and provide necessary reporting capabilities?

REAL-TIME MONITORING AND DETECTION

- ☐ Does the vendor discover and maintain an inventory of OT assets?
- ☐ Does the vendor provide real-time monitoring capabilities that reflect potential threats to your organization?
- ☐ Do they offer tools for continuous monitoring of OT environments to detect new vulnerabilities and changes in risk?
- ☐ Does the solution enable OT network visibility from level 1 – level 3 of the Purdue model and at the IT/OT network boundary with multiple methods of data capture?
- ☐ Will your operators be able to see rich technical context about related threats and detection timelines?

INCIDENT RESPONSE SUPPORT

- ☐ Does the vendor offer robust incident response capabilities, including forensic analysis and case management tools?
- ☐ Does the solution offer OT expert-authored Playbooks to streamline investigation and response?

COMPREHENSIVE VULNERABILITY MANAGEMENT

- ☐ Does the vendor integrate threat intelligence into its vulnerability prioritization methodology?
- ☐ Does the vendor map vulnerabilities to assets and offer analysis?
- ☐ Does the solution provide practical mitigation steps?

MUST-HAVE QUALITIES AND QUALIFICATIONS

To ensure the vendor can meet your cybersecurity needs effectively, they should possess the following qualities and qualifications:

- ☐ Experience and expertise, with a proven track record in ICS cybersecurity
- ☐ Team members with specific OT expertise and experience in your industry
- ☐ Comprehensive, ongoing training and support for their tools and technologies
- ☐ Dedicated technical resources to help deploy, maintain, and troubleshoot the technology
- ☐ Robust security measures, such as real-time monitoring and detailed reporting
- ☐ Solutions that show historical disposition through continuous, automated collection and analysis
- ☐ Integration of threat intelligence into vulnerability prioritization, and provision of rich technical context about related threats and detection timelines
- ☐ Full logging capabilities to help meet regulatory compliance requirements
- ☐ Comprehensive reporting capabilities for audits and demonstrating your security posture

By focusing on these considerations and leveraging the recommended tools and technologies, organizations can build a robust cybersecurity program that enhances resilience against cyber threats and ensures the protection of critical assets.

Select a Partner Who Truly Understands Your Environment

Dragos, Inc. is a US-owned OT cybersecurity company based in the Washington, DC area, dedicated to safeguarding civilization from cyber threats targeting critical infrastructure. With a focus on industrial control systems (ICS) and operational technology (OT), Dragos serves a wide range of industries, including manufacturing, electric utilities, oil and gas, and government agencies. Our mission is to protect enterprises from the ever-evolving threat landscape, ensuring the safety, productivity, and reputation our end users.

What makes Dragos different?

- **Specialized Expertise:** Dragos boasts a team of ICS/OT experts with deep knowledge of manufacturing security, making them uniquely qualified to address the specific needs of OT environments.
- **Proactive Threat Research:** Dragos is committed to staying ahead of adversaries, with research showing a significant increase in ransomware attacks against industrial organizations.
- **Comprehensive Solutions:** Dragos offers a full suite of hardware, intelligence, and services tailored to the unique challenges of OT cybersecurity.

The Dragos Platform

The Dragos Platform is the industry's most advanced cybersecurity platform designed to monitor and secure OT environments. Key features include:

- **Visibility:** Real-time inventory of OT assets and ICS network monitoring.
- **Detection:** High-fidelity, low-noise threat detection tailored to OT environments.
- **Vulnerability Management:** Identify and manage vulnerabilities to maintain continuous operations offering practical risk mitigation.
- **Response:** Provides forensics and prescriptive playbooks for efficient investigations and response.

The Dragos Platform Delivers Value Across the SANS 5 Critical Controls

ICS Incident Response Plan

- Detect & contextualize threats
- Forensic data & timelines for investigations
- Response playbooks

Defensible Architecture

- View asset groups & communications
- Validate security controls
- Audit & compliance

ICS Network Visibility and Monitoring

- Asset discovery
- Protocol analysis
- Activity logging
- Threat detection
- Response playbooks
- Vulnerability management

Secure Remote Access

- Monitor third-party remote access sessions
- Validate SRA controls for internal and third party

Risk-Based Vulnerability Management

- Match vulnerabilities to asset inventory
- Now, next, never priorities & alternate mitigation
- Track status to completion

DRAGOS PLATFORM

> The Dragos Platform technology has provided continuous monitoring and detection of potential cyber threats, allowing the ports to take proactive measures to mitigate the risk of cyber attacks.
>
> **Maritime Terminal Operator Case Study**

> Dragos' cutting-edge technology and unparalleled expertise in OT cybersecurity have played a pivotal role in ensuring the resilience and security of our critical infrastructure.
>
> **Water Utility Case Study**

> Dragos' expertise has been instrumental in enabling our critical projects and ensuring the resilience of our operations.
>
> **Creative Energy Case Study**

> I want our company to be in the best position to stay in business, increase revenue, and prevent or mitigate attacks. Dragos makes that possible.
>
> **Brandon Catalan, Boston Beer CISO, Boston Beer Case Study**

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo | Contact Us