Blue Ridge Networks Cybersecurity Assessment

Overview

Digital transformation continues to drive the convergence of IT and OT data, systems, and services. The result is an increase in attack surface, threat vectors, and potential asset exposure. To combat these challenges and evolving threats, there needs to be an understanding of operational structure, technology processes, data flows and security controls. Blue Ridge's OT cybersecurity assessments provide a comprehensive evaluation of existing systems, procedures, and guidelines according to industry standards.

Assessment Methodology

Blue Ridge's methodology involves a structured approach to evaluating an organization's operational technology (OT) cybersecurity posture based on guidelines outlined in frameworks such as NIST SP 800-82 Rev 3, IEC 62443, or NERC CIP.

Key Components of the assessment include:

- **System Characterization**
  - Mapping out the OT network topology, including critical assets, devices, communication protocols, and operational dependencies.
  - Identifying unique characteristics of OT systems like legacy equipment, custom software, and specialized protocols.
- **Threat Analysis**
  - Identifying potential threat actors that could target OT systems (e.g., insider threats, cybercriminals, nation-states).
  - Analyzing the potential impacts of cyberattacks on operational processes and safety.
- **Vulnerability Assessment**
  - Conducting vulnerability scans to identify weaknesses in OT devices, software, and network configurations.
  - Prioritizing vulnerabilities based on their potential impact on operational continuity.
- **Risk Evaluation**
  - Assessing the likelihood of a threat exploiting a vulnerability based on factors like system complexity, access controls, and security practices.
  - Determining the potential consequences of a cyber incident on operational processes and safety.

Assessment Process

1. **Initial Consultation**

   Define assessment scope, objectives, and gather relevant documentation.
2. **Data Collection & Analysis**
   a. Review of existing policies, plans, procedures.
   b. Review of personnel, systems, assets, processes and physical/logical access control.
   c. Assessor and client Q&A sessions to conduct discovery and analysis through inspection and or interviews. Can be done onsite or virtual.
3. **Risk Identification**

   Analyze findings to identify critical risks and potential attack vectors.
4. **Reporting & Recommendations**

   Deliver a comprehensive report with clear, prioritized recommendations.
5. **Follow-Up Support**

   Optional support for remediation planning and implementation.

Achieve Operational Resilience

Digital transformation, siloed IT/OT teams, legacy systems, and limited resources all present challenges on the road to safeguarding your critical infrastructure.

How is your team ready to respond when production, safety, and physical operations are on the line?

Blue Ridge Networks can help you on the path to cyber resilience and operational readiness.

Contact us today at sales@blueridgenetworks.com to accelerate your compliance journey!

About Us

Blue Ridge Networks is a proven and trusted provider of highly secure cybersecurity solutions. Our mission is to deliver resilient, seamless, and efficient preemptive zero trust protection for critical assets, data, and operations. Our CyberCloak solutions utilize unique Data Privacy Facility (DPF) technologies with your OT/IT infrastructure and tools to reliably segment and control access for critical network operations. Government and commercial industry organizations have trusted Blue Ridge Networks for over 20 years to prevent exploits and receive continuous returns on their investments while achieving uninterrupted operational efficiency.

BLUERIDGE NETWORKS

1-800-704-5234
sales@blueridgenetworks.com
BlueRidgeNetworks.com