Threat IQ
Committed to keeping you secure, always.

OT Remote Access Risk Review

Secure Your Operational Technology with Confidence

The Business Challenge

Without a secure remote access framework, organizations risk operational disruptions, data breaches, and non-compliance.

Supporting OT infrastructure often requires OEM's and 3rd parties to access your OT environment to perform maintenance and support industrial automation and control systems, which means granting remote access to third-party vendors and remote employees.

Adversaries have successfully exploited vulnerable remote access configurations and backdoors to infiltrate OT environments, leading to outages and significant financial losses. Increased remote access to Operational Technology (OT) environments has introduced significant risks, including:

01 Remote Access via Unsecured Networks

Unsecured networks enabling unauthorized access, malware, and data exfiltration.

02 Third-Party Risks

Vendors and contractors needing remote access, introduces new risks and potential vulnerabilities.

03 Limited Monitoring

Lack of visibility into remote access sessions can leave breaches undetected.

Business Benefits

- ✓ **Reduced Security Risks**
- ✓ **Enhanced 3rd Party Security**
- ✓ **Best Practices Alignment**
- ✓ **Increased Visibility**

Take the First Step

Is your OT remote access truly secure?

Contact us to schedule an OT Remote Access Risk Review and protect your critical operations from evolving cyber threats.

Our Assessment Methodology

Our OT Remote Access Risk Review evaluates the security and efficiency of your current remote access setup, focusing on risk identification and mitigation.

Network and Protocol Review

- Evaluate the security of VPNs, jump servers, and other access mechanisms.
- Analyze encryption protocols and session isolation techniques.

Access Control Assesssment

- Review policies and procedures for granting, monitoring, and revoking remote access.
- Evaluate the use of technologies like multi-factor authentication (MFA).

Monitoring and Logging

- Examine how remote access sessions are monitored and logged for accountability.
- Identify gaps in real-time alerting and forensic capabilities.

Third-Party Access Review

- Assess access provided to contrators, vendors, and third-party partners.
- Identify risks stemming from unmanaged or excessive permissions.

Best Practices Benchmarking

- Compare your current practices with industry standards like IEC 62443 and NIST 800-82.

What You'll Receive

Risk Assessment Report

- Identification of vulnerabilities in your remote access framework.
- Detailed findings on third-party risks, access controls, and monitoring gaps.

Actionable Recommendations

- Prioritized steps to mitigate risks and improve remote access security.
- Suggestions for adopting technologies and practices that enhance security.

Best Practice Guidance

Insights on how to align with relevant industry standards.

Business Benefits

Reduced Security Risks

Protect your OT environment from unsecured networks risks unauthorized access, malware, and data exfiltration.

Enhanced Third-Party Security

Minimize risks from vendor and contractor access with robust controls.

Best Practices Alignment

Ensure your remote access practices align with industry standards.

Increased Visibility

Gain insights into remote access activities with improved monitoring and logging.