Threat IQ
Committed to keeping you secure, always.

Operational Technology Cybersecurity Risk Assessment

A Preliminary Security Assessment Offering

Unlock the Power of Operational Technology Security

Discover and Protect Your OT Environment

Today's interconnected and digitized world, the security of Operational Technology (OT) is paramount.

Protecting a production plant requires a deep understanding of your OT assets and the vulnerabilities associated with them. Our comprehensive cursory OT risk assessment service empowers you to uncover, evaluate, and address cyber risk associated to your OT environment. Enabling your journey towards cyber resilience.

Understanding cybersecurity risk associated to your Operational Technology environment are of utmost importance in today's digital landscape. Cyber breach statistics further reinforce the significance of proactive measures in securing OT Systems.

01 Silver | Understand Your OT Cyber Deficiencies

Our Silver-level OT Cybersecurity Health Check assessment includes an automated OT asset discovery and vulnerability identification process. This is followed by a thorough analysis of cybersecurity gaps and areas for improvement, utilizing ThreatIQ's OT Cybersecurity best practices that adhere to industry guidelines.

Upon completion, you will receive a comprehensive OT Cybersecurity Health Check report, providing valuable recommendations to strengthen your OT Cyber resilience.

02 Gold | Prioritize your Remediation Roadmap

Elevate your cybersecurity strategy with our cutting-edge "Gold-tier" service, surpassing our OT Cybersecurity Risk Assessment. This comprehensive assessment includes advanced OT asset discovery, combining automated and manual techniques, as well as precise vulnerability identification. Additionally, let us evaluate your network segmentation and defense in depth capabilities.

Upon completion, you will receive a prioritized set of actionable security recommendations, meticulously tailored to fortify your OT Cybersecurity resilience, and enhance your overall protection.

Business Benefits

Enable Revenue Growth through Trust

Demonstrating a strong commitment to cybersecurity and protecting your OT infrastructure fosters trust among your customers and partners leading to increased customer loyalty, repeat business, and revenue growth.

Achieve Competitive Advantage & Business Growth

Investing in OT security showcases your dedication to cybersecurity, differentiating you from competitors in the marketplace. This advantage can attract new customers and business opportunities, resulting in revenue growth.

OT Cybersecurity Risk Assessment

First step towards achieving OT cybersecurity resilience

OT Asset Discovery

Plays a crucial role in establihshing an accurate inventory of OT assets, which is a fundamental step in OT cybersecurity and risk management. Our approach to asset discovery:

- *Automated dicovery of network connected devices*
- *Manual site walk for non-IP connected devices*

Vulnerability Assessment

Identifies vulnerabilities, potential impact associated to your OT assets. Holistic review of identified vulnerabilities associated to:

- *Control devices & Firmware vulnerabilities*
- *Device configuration*
- *Communication protocols*

Gap Analysis

A comprehensive look at assets, vulnerabilities & impact in order to establish security gaps associated to the OT assets. A subjective assessment involving:

- *Review of the identified assets, associated vulnerabilities, and impact to business in the event of a cyber-attack against the assets*
- *Review of existing safeguards & safeguard effectiveness*
- *Identification of security gaps*

Recommendations & Remediation Plan

Development of actionable recommendation to mitigate identified gaps along with implementation priority. Focuses on providing clients with:

- *Meaningful recommendations based on identified security gaps*
- *Recommended priority for remediation along with roadmap*

Assessment Scope & Options

Service Options	Siver	Gold
Number of Site(s) for Assessment	1	1
OT asset discovery of IP connected devices	✓	✓
Number of Asset	Up to <500	Up to <1,000
End of Life Devices Reporting	✓	✓
Protocol Analysis (OT/ICS)	✓	✓
OT Device Configuration Review	✓	✓
Asset Vulnerability Assessment	✓	✓
OT Cyber Health Check based on identified assets and associated vulnerabilities	✓	✓
Gap analysis and recommendations	✓	✓
OT Cyber Health Check report containing OT asset inventory and associated vulnerabilities along with identified gaps and recommendation to improve the overall security posture	✓	
Manual Discovery of non-IP connected OT devices (1 day Site Walk)		✓
Current State High-level Network Topology Diagram Development (Layer 2)		✓
Network Segmentation Review and Risk Assessment		✓
Remote Access Service and Risk Assessment		✓
OT cybersecurity assessment report with asset inventory and associated vulnerabilities, high-level current state network topology diagrams along with associated risks, actionable recommendation and remediation options with implementation roadmap		✓