MANUFACTURING OT CYBERSECURITY ASSESSMENT

Get Expert Insight and Recommendations

Manufacturing is #1 most attacked industry two years in a row[1]

61% of successful breaches are occurring in operational environments[2]

With manufacturing becoming the #1 most attacked industry and 61% of all successful breaches occurring in operational technology (OT) environments, it's vital that manufacturers have complete asset visibility, real-time operational insight, and the ability to prioritize actions that will significantly mitigate risks and improve overall security posture. Our Manufacturing OT Cybersecurity Assessment lets our experts examine your operational environments to discern a complete asset inventory, vulnerabilities, and associated risk factors, to bring transparency and visibility to your greatest threat vectors.

Achieve Full Asset Visibility and Operational Insight

Our passive approach to scanning allows our experts to identify IT, OT, and ICS assets, the relationship of those assets to network infrastructure, communication paths to the Internet, unauthorized remote access, and a complete listing of vulnerabilities. Our assessment identifies various assets, including building controls, computers, gateways, industrial control systems (ICS), industrial networking, servers, sensors, and third-party equipment. The process also provides operational insights into industrial logs, process variables, controller software, and access associated with outside resources—allowing our experts to assess risks and prioritize recommendations to remediate and improve your overall cybersecurity posture.

How It Works

Connection's Manufacturing Practice, Engineering, and Services teams will work with you to understand your business objectives, concerns, and OT environment. Additionally, we will conduct an onsite assessment and deliver a comprehensive report.

53% of industrial customers have already been attacked[3]

55% don't think they know their OT network well enough and communication patterns are largely unknown[4]

1. **Pre-planning:** First, we go through a virtual briefing to review corporate objectives, assessment goals, and logistics associated with the assessment process. We will also define boundaries for the engagement and review deliverables. The level of comprehensiveness will depend upon our access to the facility, line of business process experts, and tours of the targeted process areas.

2. **On-site Visit:** Next, our team conducts an in-person, on-site session to install equipment, conduct targeted facility tours, and meet with pre-determined business and IT stakeholders. This approach allows our experts to better understand the physical environments, infrastructure, and processes associated with the business value stream and correlate them with the cybersecurity data collected. Our non-invasive assessment leverages deep packet inspection (DPI) that is capable of decoding both IT and OT protocols to gain visibility of industrial components and detect anomalies, allowing us to execute the assessment without impact to production.

3. **Out Brief and Recommendations:** Following the on-site assessment, our experts will review the information collected and produce a comprehensive report that takes into consideration benchmarking, business goals and challenges, asset inventory, data flows, and vulnerabilities. We will also provide detailed insight into your security posture, risks, and prioritized recommendations. Lastly, our team will meet with key stakeholders virtually to review the most salient risks and recommendations.

Throughout the assessment, your dedicated sales team will be accompanied by a member of our manufacturing practice, network and security practice, and a field solution architect.

Assessment and Out Brief Outcomes

- 100% Visibility and Insight into the Industrial Environment
- Detailed Asset Discovery and Inventory
- Vulnerability Detection and Risk Scoring
- Map of Industrial Zones and Conduits
- Identify Traffic Flows and Remote Access
- Report with Prioritization of Risks and Mitigation Recommendations

For more information about Connection's Manufacturing OT Cybersecurity assessment, contact one of our manufacturing experts today!
www.connection.com/manufacturing

Connection®
we solve IT®

Contact a Connection expert today for more information.

Business Solutions
1.800.800.0014

Enterprise Solutions
1.800.369.1047

www.connection.com/manufacturing

1 IBM, 2023, X-Force Threat Intelligence Index 2023
2 IBM, 2022, 2022 X-Force Threat Intelligence Index
3, 4 IBM report 2017