



DISCOVERY & ASSESSMENT

The Discovery and Assessment engagement is designed to provide an effective cybersecurity assessment across an organisation's Operational Technology (OT) environment to address key challenges in OT environments.

Why 2TWENTY

2Twenty Solutions is a cyber security company that provides leading technology solutions and services to its customers. It is managed by, and partners with, technology experts who are focused on providing the most effective and efficient solutions and services to its customers. 2Twenty proactively stays ahead of technology trends to identify innovative solutions, understand and master complexities, enabling its customers to concentrate on their core competencies.

CYBERSECURITY THROUGH EMPOWERMENT AND VISION

Business drivers & challenges



Asset Visibility and Inventory

Many organisations lack a full inventory of OT assets, including legacy and shadow systems. This complicates risk assessments, patching, and incident response.



Cybersecurity risks and threats

OT systems are often outdated and lack security features. Critical environments like power grids, processing plants and manufacturing cannot afford downtime for updates. Operational technology networks are not isolated (air gapped) as many are now integrated with Information Technology networks or connected to the Internet.



Regulatory and Compliance

OT environments must comply with industry regulations and standards (e.g., IEC 62443, NIST 800-82, SOCI Act, Essential Eight). Balancing compliance and security with operational demands can be challenging.



Convergence of IT and OT

Increased integration brings productivity benefits but can expose OT systems to IT-level threats. There are conflicting objectives between IT and OT systems as IT focuses on confidentiality and OT focuses on availability and safety.

Outcomes & benefits



Visibility

Provides the foundation for security by giving your organisation the ability to see and identify connected devices and communication flows.



Security Posture Improvement

Enhances your organisation's defense mechanisms, policies, and response capabilities, while promoting best practices such as segmentation, zero trust and least privilege.



Risk Reduction

Provides a risk-based view of security threats and helps prioritise remediation efforts based on likelihood and impact.



Business Impact Assessment

Creates a risk profile that accounts for OT assets and uncovers the risk of potential cybersecurity incidents.

Approach

Stage 1: Discovery

During this phase of the assessment all devices and assets connected to the target network segments are discovered, identified and catalogued. Asset information will include:

- Asset role, risk rating and vendor details
- Asset type and version
- Asset classification based on Purdue model
- Asset communication protocol patterns

Stage 2: Assessment

This stage identifies assets that are exposed to threats in your organisation which, if exploited could, potentially cause damage or loss to your organisation. The assessment will report on the following:

- Assets with known exploitable vulnerabilities (by severity)
- Critical alerts grouped by categories
- Risky communications between network segments
- Next steps and recommendations



info@2twenty.io



2twenty.io