GTE

Greater Engineering™

Cybersecurity in OT Networks:
A Safer, More Reliable Approach

Client: Industrial and critical infrastructure operators
Date: Ongoing service offering
Location: Western Australia

Operational Technology (OT) networks are the backbone of mining, manufacturing, and energy industries. They control critical infrastructure that must remain operational at all times. While cybersecurity is a priority for all businesses, traditional Information technology (IT) security methods often fall short when applied to OT environments. Unlike IT systems, which can tolerate minor disruptions, OT networks require constant uptime, prioritised safety, and a resilience-first approach to security.

Applying standard IT penetration testing (pen testing) techniques to OT networks can lead to unintended operational failures, jeopardising productivity, safety, and financial stability. Organisations need a tailored security strategy to protect OT environments effectively that detects vulnerabilities without disrupting essential operations.

Challenges

Relying on IT-based cybersecurity strategies in OT environments presents significant risks:

- **Operational Disruptions**
  Traditional IT pen testing involves simulating cyberattacks, which often cause system downtime. In OT environments, these disruptions can halt automated production lines, disrupt industrial control systems (ICS), and result in extensive financial losses.

- **Safety Hazards**
  Unlike IT failures, an OT system failure can lead to serious physical consequences, such as machine malfunctions, loss of process control, or compromised worker safety.

- **Regulatory and Compliance Risks**
  Many critical infrastructure sectors require cybersecurity frameworks designed explicitly for OT, meaning a lack of tailored security measures could result in regulatory penalties.

- **Legacy System Vulnerabilities**
  Older OT systems weren't built with cybersecurity in mind, making them particularly susceptible to cyber threats if not appropriately secured.

Organisations risk compromising safety, compliance, and operational efficiency without a dedicated OT security strategy.

Approach and Solution

OT-Specific Vulnerability Testing

Instead of applying traditional IT pen testing methods, OT networks require a more refined approach—one that ensures security without operational disruption.

OT vulnerability testing is a safer alternative that detects security gaps while keeping systems fully operational. Much like assessing a bridge's structural integrity without stopping traffic, OT vulnerability testing strengthens security without compromising uptime.

What Makes OT-Specific Vulnerability Testing Effective?

- Identifies weaknesses in ICS, Supervisory Control and Data Acquisition (SCADA) networks, and field devices while maintaining continuous operations.
- Protects legacy infrastructure without causing compatibility issues or system malfunctions.
- Maintains operational efficiency by implementing security controls without introducing downtime.

By adopting an OT-first approach, organisations can enhance security without sacrificing productivity, ensuring that critical infrastructure remains resilient against cyber threats.

Results and Impact

OT-specific security solutions have led to measurable improvements for businesses, including:

Zero Operational Downtime

OT vulnerability testing ensures security measures do not interfere with live operations, avoiding costly disruptions.

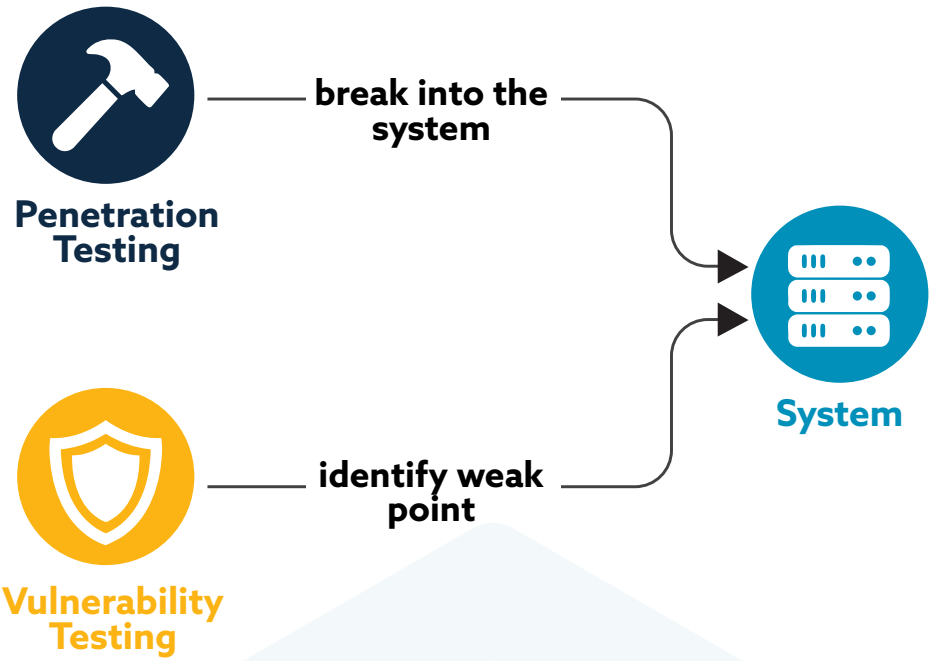
Stronger Compliance & Regulatory Adherence

OT cybersecurity frameworks are aligned with industry-specific compliance requirements, ensuring organisations meet all necessary security standards.

Enhanced Risk Management

Proactively identifying vulnerabilities reduces the likelihood of cyber incidents, strengthening overall security posture. Team Lead Network Engineer at GTE Group.

Business Priority	Confidentiality	Availability
Major Focus	Data integrity is key	Control processes cannot tolerate downtime
Protection Targets	Windows computers, servers	Industrial legacy devices: PLC, HMI, meters
Environmental Conditions	Air-conditioned	Harsh environments: extreme temperatures, vibrations & shocks



Conclusion and Future Impact

As industrial environments become increasingly connected, cyber threats targeting OT networks will continue to rise. A failure to address OT-specific vulnerabilities puts systems at risk and compromises safety, compliance, and operational continuity.

Organisations can fortify their infrastructure without operational compromise by moving beyond IT-based cybersecurity approaches and implementing OT-specific security solutions. GTE Group is committed to helping industries develop resilient, tailored OT cybersecurity strategies that protect assets, ensure compliance, and maintain uptime.