OnDefend

Operational Technology Security

Uncover Hidden Threats Across Your Critical OT Environment

OnDefend OT security testing evaluates industrial systems, networks, hardware, and workflows as integrated ecosystems to identify risks to safety and operations without disrupting production.

Testing Capabilities

Adversary-Driven OT Testing

Simulates real adversaries to identify how attackers access industrial systems and create operational risk.

Industrial Network & Segmentation

Identifies IT/OT segmentation weaknesses and insecure trust relationships enabling unauthorized access.

Control System & Protocol Assessment

Tests control systems and protocols for misconfigurations enabling manipulation or operational disruption.

Hardware, Firmware & Embedded Devices

Tests PLCs, RTUs, controllers, and sensors for firmware weaknesses and unauthorized communications.

Remote Access & Vendor Connectivity

Evaluates remote access pathways and vendor connections for unauthorized OT entry points.

Human & Operational Workflow Testing

Assesses how human processes can be exploited to bypass technical controls or delay response.

Outcomes

- OT attack paths identified across industrial networks, control systems, hardware, and remote access
- Findings mapped to NIST 800-82, IEC 62443, ISA/IEC standards, and MITRE ATT&CK for ICS with operational impact context
- Validated OT security posture across IT/OT boundaries, control systems, and embedded devices
- Improved detection, response, and recovery readiness across industrial environments

Protect operational safety, system availability, and the critical processes your organization depends on.

OnDefend.com