Privia SECURITY

# OT/SCADA Penetration Test Service

## Professional Offensive Security Services

"Uncover Hidden Threats in Industrial Systems!"

The information contained in this document is related to the Professional Offensive Services provided by Privia Security Information and Consulting Services and is of a general nature. All information presented in this document is publicly available.

Queen Elizabeth Olympic Park, 14 East Bay Lane, Plexal, London, England, UK, E20 3BS

info@priviasecurity.co.uk

www.priviasecurity.co.uk

*“Identifying invisible cyber threats within your industrial infrastructure ensures preparedness against potential future attacks.”*

The OT (Operational Technology) Security Testing Service is a comprehensive assessment process designed to protect industrial control systems (ICS/SCADA) and related infrastructures against cyber threats. Hardware components used in industrial facilities are increasingly exposed to cyber attacks, which poses significant risks to uninterrupted production operations. Our OT Security Testing Service aims to enhance the security of critical infrastructure and improve cyber resilience.

The tests we conduct include a range of assessments and methodologies aimed at identifying vulnerabilities within OT (ICS/SCADA) systems. Techniques such as attack simulations, vulnerability scanning, gap analysis and configuration testing are utilized to thoroughly evaluate and report on the current security posture of the systems. Adherence to national and international cybersecurity standards during the testing process enhances the quality and reliability of the results.

Our OT Security Testing Service goes beyond identifying existing threats; it also provides additional solutions to help you prepare for future risks. Based on the information, documentation and findings obtained during the tests, strategic recommendations are offered to help mature the security posture of your hardware and systems. As a result, the operational security of industrial facilities is strengthened and potential cyber-related disruptions are prevented.

The OT Security Testing Service supports the goal of preserving business continuity by enhancing the cybersecurity of industrial control systems. The detailed reports generated at the end of the testing process include all necessary steps and guidance for identifying and mitigating vulnerabilities. With organization-specific action plans, the service ensures that systems remain secure and up to date at all times.

# Service Components

### Security Assessment

During the testing process, both hardware and software components of OT systems are examined in detail. Potential security vulnerabilities are identified and the security posture of each component is analyzed. The collected information, documents and findings serve as the basis for strategic recommendations on how to remediate weaknesses. These assessments help strengthen the overall security of the system and elevate the maturity level of the infrastructure against cyber attacks.

### Network Security Testing

Potential vulnerabilities within OT (ICS/SCADA) systems are thoroughly investigated. The identified security weaknesses are assessed in collaboration with the organization’s security team to determine their risk levels. This approach supports effective prioritization of vulnerabilities and ensures that critical issues are addressed first.

### Vulnerability Analysis

As part of the vulnerability testing phase, security tests are conducted on the organization's industrial control systems and associated peripheral devices such as PLCs, SCADA units, RTUs and DSS components, as well as IT assets that receive sensor data from these devices. Physical access control systems, security cameras and other physical security measures in the facilities are also evaluated. Identifying physical security vulnerabilities is essential to prevent unauthorized access. Physical security inspections are conducted alongside the technical vulnerability assessments.

### Physical Security

Physical security of OT systems is a critical audit phase. The assessments focus on inspecting facility access control systems, surveillance cameras and other protective measures. Detecting physical security vulnerabilities is one of the most crucial steps in preventing unauthorized entry. These inspections help ensure the integrity of all systems and support the uninterrupted continuation of operations.

### Cyber Threat Simulations

Cyber threat simulations are used to identify security weaknesses in OT systems and to enhance cybersecurity maturity through real-world attack scenarios. These simulations involve customized techniques, tactics and procedures (TTPs) that a potential attacker might use, tailored specifically for the organization. During testing, the network architecture, hardware and software components are subjected to simulated attacks to expose hidden vulnerabilities.

# FAQ

### What is an OT Penetration Test?

An OT (SCADA) penetration test is a security assessment that examines the cybersecurity posture of industrial control systems (ICS), including PLCs, SCADA systems and peripheral devices. These tests aim to identify vulnerabilities in critical infrastructures and develop countermeasures against cyber threats. During the tests, techniques similar to those used by real attackers are applied to uncover weaknesses. Periodic security assessments of SCADA environments are crucial for ensuring business continuity and operational resilience. The collected data, documents and findings are used to enhance the security maturity of critical infrastructure.

### Why is an OT Penetration Test Necessary?

Since OT (SCADA) systems often operate in closed-loop environments, they tend to lack adequate cybersecurity measures. ICS/SCADA penetration tests help identify and remediate vulnerabilities in critical infrastructure. The main goal is to secure operational processes, prevent business disruptions and mitigate data breaches. Cyberattacks targeting production facilities can lead to major financial losses, production delays and decreased output. Regular SCADA security assessments increase protection levels and prepare the organization against future cyber threats.

### Why is an OT Penetration Test Necessary?

Since OT (SCADA) systems often operate in closed-loop environments, they tend to lack adequate cybersecurity measures. ICS/SCADA penetration tests help identify and remediate vulnerabilities in critical infrastructure. The main goal is to secure operational processes, prevent business disruptions and mitigate data breaches. Cyberattacks targeting production facilities can lead to major financial losses, production delays and decreased output. Regular SCADA security assessments increase protection levels and prepare the organization against future cyber threats.

### Which Systems and Devices are Included in an OT Penetration Test?

OT penetration tests cover industrial control systems and critical devices such as PLCs, SCADA, RTUs, HMIs, DSS, MES and Engineering Workstations. Sensors and peripheral devices connected to these systems are also included. The tests also assess network firewalls and access control systems to ensure a comprehensive evaluation. Vulnerabilities across both hardware and software layers are identified and addressed.

## How Long Does an OT Penetration Test Take?

The duration of a SCADA penetration test depends on the size and complexity of the system. While smaller infrastructures can be assessed in a few days, larger and more complex environments may require several weeks or even months. The tests are planned in a way that ensures no disruption to operations. Alternative workflows are considered during the assessment of critical processes to maintain business continuity.

## What is Included in an OT Penetration Test Report?

The final report includes detailed findings on identified vulnerabilities and their associated risk levels. Each vulnerability is accompanied by remediation recommendations and actionable mitigation plans. The report is structured to include both technical details for IT teams and an executive summary for management. These results serve as a vital reference for system improvements and long-term cybersecurity strategy development.

## Will There Be Any System Downtime During the OT Penetration Test?

The goal of ICS penetration tests is to identify vulnerabilities without disrupting operational processes. Test activities are scheduled in coordination with project management teams to minimize impact. In some cases, tests are conducted during night shifts or low-activity periods. Proper planning ensures that critical systems are tested without compromising operations. All assessments are carried out with full consideration of the organization’s operational requirements.

## How Do OT Penetration Tests Contribute to Risk Management?

OT penetration tests are an integral part of the risk management process. Prioritizing the identified vulnerabilities helps organizations address the most critical risks first. The risk reports generated from the tests support the development of strategic plans to mitigate weaknesses and enhance overall cybersecurity posture.

## How Often Should OT Penetration Tests Be Performed?

It is recommended that OT penetration tests be conducted at least twice a year. Additionally, tests should be repeated after new system deployments or major updates. Regular testing ensures that systems remain protected against evolving cyber threats. Frequent assessments enable early detection and mitigation of newly emerging vulnerabilities, improving the organization’s cybersecurity maturity over time.

## Which Standards Do OT Penetration Tests Comply With?

OT penetration tests are conducted in compliance with national and international standards such as ISO 27001, IEC 62443 and regulations set by authorities like the Energy Market Regulatory Authority (EPDK). These standards define the scope of testing and help improve cybersecurity processes. Compliance with regulatory frameworks is essential for meeting legal obligations and enhancing the organization’s reputation.

**Your Trusted Partner in Cybersecurity**

Founded in 2018 with a vision for the future of cybersecurity, Privia Security has been committed to delivering high-quality services to its clients from day one. With a strong and capable team, we provide the most reliable and comprehensive solutions across all areas of cybersecurity, ensuring our clients are well-protected in today's digital landscape.

As cyber threats continue to evolve rapidly and grow in complexity, combating them becomes increasingly challenging. At Privia Security, we offer both defensive and offensive cybersecurity strategies powered by cutting-edge technology to meet our clients' evolving needs. Through our innovative R&D products and strategic consultancy, we aim to enhance organizations' cybersecurity maturity and deliver proactive, tailored solutions. We are proud to be safeguarding the digital assets of more than 300 major organizations.

**Global and Local Cybersecurity Solutions**

Privia Security delivers cybersecurity services across a broad geographical scope, including Europe, Asia, the Middle East and the Americas. Our specialized teams in Offensive, Defensive and Forensic operations develop bespoke solutions for organizations operating in diverse sectors such as critical infrastructure, avionics systems, corporate networks and the military.

In addition, our innovative cyber warfare simulation platform, PriviaHub, offers comprehensive solutions for nations seeking to strengthen their cyber defense capabilities. PriviaHub enables the testing of cyber warfare strategies, execution of simulations and assessment of expert competencies. Designed to meet the exercise needs of private sector entities, academic institutions and military organizations, it bridges the gap between training and real-world readiness.

**A Secure Future Through Advanced Technology**

With R&D centers located in Istanbul, Ankara, London and at Cumhuriyet Technopark, we are continuously developing value-driven projects for our clients. From penetration tests and red team operations to cybersecurity training and custom enterprise solutions, we are redefining the standards in our industry. Through our slogan "Privacy For You," we bring a fresh, innovative perspective to security and privacy—ensuring that our clients' digital futures are secure.

Privia
SECURITY