Privia SECURITY

IoT Penetration Testing Service

Professional Offensive Security Services

"Secure Future for Smart Devices!"

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

info@priviasecurity.co.uk

www.priviasecurity.co.uk

“Protect your IoT devices against cyber threats with our IoT security testing service.”

IoT Security Testing Service is a comprehensive testing process to ensure the security of devices in the Internet of Things (IoT) ecosystem. The tests focus on detecting potential cyber security vulnerabilities, ranging from smart home devices to industrial control systems. IoT devices constitute an important attack surface at both individual and corporate level due to their widespread use.

The IoT Security Testing Service examines the hardware and software components of devices, identifying potential threats and recommending the necessary measures to mature security levels. Threats such as encryption deficiencies, outdated firmware, weak network configurations and configuration errors are analyzed in detail. The testing processes are conducted in accordance with international standards such as OSSTMM and NIST and are reinforced with attack simulations.

The findings obtained during the tests are presented to the security team of the organization in comprehensive reports and organization-specific action plans are created. With continuous improvement suggestions, IoT systems are made ready not only for today's threats but also for the threats of the future.

Service Components

Device Security Tests

The hardware and software components of IoT devices are analyzed to identify authentication and encryption vulnerabilities. Firmware security is examined and recommendations are provided for software updates. Through the conducted tests, the devices are made resilient against the latest threats.

Network Security Tests

Network configurations to which IoT devices are connected are tested and critical connections such as firewalls and VPN accesses are examined. Intrusion detection systems, if any, are tested to identify security vulnerabilities in the network before an attack.

Data Security and Encryption Testing

Data traffic flowing between IoT devices is analyzed and tests for compliance with encryption standards are performed. Necessary improvement suggestions are provided to ensure the protection of sensitive information.

Firmware Tests

The firmware of IoT devices are examined for security and the presence of malicious codes (backdoors, etc.) are detected. Firmware updates are regularly checked and security levels are increased.

Physical Hardware Tests

Physical access risks of IoT devices are tested. Hardware protection solutions are examined and reported to prevent unauthorized interventions.

Action Plan

An action plan is prepared by presenting improvement suggestions for the vulnerabilities identified. The report presented at the end of the process includes the steps to be taken to increase the security level.

FAQ

What is IoT Security Testing?

IoT security testing is a comprehensive testing process to identify vulnerabilities and security weaknesses of internet-connected devices. The tests evaluate the hardware and software components of the devices to protect them against attacks. It aims to protect business continuity and data security by identifying potential threats in advance.

Why IoT Security is Important?

IoT devices offer a large attack surface for cyber attackers. Weak encryption and insecure network connections increase the risk of access to personal and corporate data. IoT Security tests increase the security of IoT devices, protecting both the privacy of individual users and the integrity of corporate systems. Strong security measures enable you to use the opportunities offered by IoT with confidence.

How Long Do IoT Security Tests Take?

Testing time varies depending on the number of devices, the size of the infrastructure and the scope of testing. Tests that take a few days in small projects can take up to several weeks in large systems. During the testing process, tests are completed without interrupting the operational performance of the devices. Each step is customized according to the needs of the organization.

Why Firmware Updates are Necessary?

Firmware updates optimize the performance of devices while also closing security vulnerabilities. Devices that are not updated become easy targets for attackers. Therefore, regular firmware updates not only improve the performance of devices but also increase their security status.

IoT Cihazlarında Hangi Güvenlik Riskleri Bulunur?

IoT devices have many security vulnerabilities such as weak encryption, outdated software, lack of network segmentation. These vulnerabilities can be exploited by malicious actors and lead to data leaks. It is recommended to support devices with protection methods such as firewall, VPN and IPSec. With a strong security policy, identified risks can be minimized.

Which Devices Does IoT Security Testing Cover?

Smart home devices, industrial control systems, healthcare equipment and all other internet-connected devices fall within the scope of IoT security testing. The tests address both the physical and digital security of the devices. Devices that are not compatible or have weak protection are analyzed in detail.

How to Report IoT Security Test Results?

After the tests are completed, a detailed report is prepared in the light of the information, documents and findings obtained. The report includes the security vulnerabilities identified and recommendations for improvement. In addition, strategic predictions are presented about the security level of the devices. These reports guide the development of security strategies and long-term planning.

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—

Privia
SECURITY