Privia SECURITY

Infrastructure Security Testing Service

Professional Offensive Security Services

"Secure Infrastructure, Reliable Security!"

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

"A strong infrastructure prepares you not only for today's risks but also for the challenges of the future."

Our Infrastructure Security Testing Service focuses on comprehensively analyzing all layers of assets within an organization's IT, OT and IoT networks to identify security vulnerabilities. Covering a broad spectrum—from critical network devices and servers to data centers and control systems—these tests are designed to maintain operational continuity and proactively detect weak points. Our service is conducted in accordance with leading security standards such as OSSTMM, NIST and ISO 27001 to effectively counter modern cyber threats.

Our expert team works from an attacker's perspective to uncover all possible vulnerabilities within your infrastructure. Through real-world scenario simulations, we perform detailed analyses of both internal and external networks. Every aspect, from network device configurations to access control policies, is meticulously examined. All collected data, documentation and findings are delivered alongside customized solutions aimed at enhancing your security posture.

Additionally, the service evaluates the effectiveness of your organization's security policies. The comprehensive reports and action plans provided at the conclusion of the process enable continuous system improvements. The stronger your infrastructure, the lower your risk exposure. With the philosophy of "Robust Infrastructure, Reliable Security," we help organizations minimize their security risks effectively.

Service Components

Network Architecture and Configuration Testing

Analyzes the active behavior of network devices such as routers, switches and firewalls to identify vulnerabilities. Detailed assessments are conducted to minimize risks from misconfigurations and evaluate the effectiveness of security policies.

Access Control Testing

Reviews critical system and data access to test who can access what and how. Security weaknesses like weak password policies and unnecessary permissions are identified.

Firewall and VPN Testing

Evaluates firewall and VPN configurations from an attacker's perspective. Tests the security of external connections to minimize the organization's cyber attack surface.

Patch Management

Software, hardware and operating systems are checked for updates to identify any missing patches. The potential exploitation of vulnerabilities caused by missing patches in cyber attacks and their possible impacts are analyzed.

Network Segmentation and Isolation Testing

Network segmentation is tested to separate critical systems and direct traffic in a controlled manner. Security risks of non-isolated systems and the potential spread of attacks are identified. Recommendations are provided to narrow the attack surface through secure segmentation.

Log Management

It is evaluated whether critical logs are properly kept and stored and their usability in incident response processes. Strong log management provides guidance for early detection of attacks and rapid response.

Action Plan and Closure

Solution recommendations and action plans are prepared for the identified vulnerabilities. After the tests, improvement steps are suggested to enhance the organization's security level. The detailed reports prepared serve as a reference for reviewing security strategies and implementing new measures.

FAQ

What is infrastructure security testing?

Infrastructure security testing is a comprehensive process conducted to identify weaknesses in networks and systems and to remediate security vulnerabilities. The test covers servers, network devices and data communication protocols. Infrastructure security testing is critically important to identify potential threats early and prevent operational disruptions.

What is the purpose of this test?

The purpose is to discover vulnerabilities that cyber attackers could exploit in advance and to take preventive measures. Increasing system reliability and preventing data leaks are also key objectives.

Which standards are used?

Internationally recognized standards such as ISO 27001, NIST SP 800-115 and OSSTMM are used. These standards define the scope and methodology of the tests and provide the best solutions for addressing identified vulnerabilities.

How long does the test take?

The duration of the test varies depending on the size and scope of the infrastructure. For small systems, it may take a few days while for large and complex networks, it can take several weeks or months. Each step of the process is carried out through mutual planning with the organization’s team.

Will there be system downtime during testing?

Tests are generally performed without operational interruptions. When testing critical systems, security measures are taken to minimize the risk of downtime. Throughout the testing, business continuity is maintained while enhancing system security.

Which components are tested?

Network devices, servers, firewalls, VPN infrastructure and access control systems are tested. The configurations of these components are checked for correctness and vulnerabilities are identified. The tests help implement preventive measures against both internal and external threats.

How are the results reported?

At the end of the test, a detailed report including all identified vulnerabilities and recommended solutions is presented to the organization's security team. The report outlines the necessary steps for system improvements and contributes to the development of long-term security strategies.

How often should tests be conducted?

It is recommended that tests be performed at least twice a year or after significant system changes. Regular testing ensures that systems remain secure against continuously evolving threats. These tests also help in meeting compliance requirements.

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.