Privia SECURITY

Professional Offensive Service (OaaS)

Professional Offensive Security Services

"All Offensive Security Services in One Place!"

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

“With our Professional Offensive Services, we offer a comprehensive approach to your cybersecurity operations. Consolidate all your offensive service needs under one umbrella — and pay only for what you use..”

Our Offensive-as-a-Service (OaaS) offering is designed to help organizations enhance their cybersecurity maturity and proactively prepare for emerging threats. By leveraging the tactics and techniques used in real-world cyberattacks, we test the security of your systems, networks, hardware and applications. Our mission is to help you build a more secure infrastructure in today’s threat landscape.

Backed by the expertise of our cybersecurity team, our OaaS platform conducts thorough security assessments of your networks, applications, hardware and systems — all from an attacker’s perspective. These offensive tests uncover vulnerabilities and support the implementation of corrective and preventive measures aligned with compliance requirements.

Our professional offensive services help you stay up to date with the ever-evolving threat environment and manage your security strategies dynamically. With detailed reports and actionable recommendations included in every engagement, you can strengthen your security posture and minimize your risks effectively.

Service Components

Penetration Testing

Penetration testing involves comprehensive assessments of your systems and networks using attacker-like techniques to evaluate their security posture. During these tests, our cybersecurity experts use a variety of tools and techniques to identify potential vulnerabilities. Penetration testing includes both external testing (simulating attacks from outside the network) and internal testing (simulating threats from within the organization). The identified vulnerabilities are analyzed and prioritized based on their potential impact on your organization.

Social Engineering Testing

Social engineering testing is designed to measure the impact of the human factor on security. It evaluates how well your employees adhere to security policies and procedures. Techniques may include phishing emails, vishing (voice phishing) calls and physical intrusion attempts. The results help determine which areas require additional employee training. These tests are essential for improving your security culture and reducing risks stemming from human behavior.

Source Code Analysis

Source code analysis is a critical test to ensure the security of your applications and software. Static code analysis checks your code against security standards and best practices, while dynamic analysis evaluates runtime behavior. These analyses help detect security flaws caused by coding errors, including SQL injection, cross-site scripting (XSS) and insecure data handling. Source code analysis enables the integration of security into the software development lifecycle.

Cyber Threat Intelligence

Cyber threat intelligence services help you proactively detect potential threats targeting your organization. Our experts monitor the dark web, deep web and open sources for threat indicators relevant to your environment. We gather intelligence on possible attack plans, leaked data and targeted campaigns. This information is then used to update your security strategies and implement preventive measures accordingly.

Cybersecurity Consulting & Training

With our Professional Cybersecurity Consulting and Training Services, we aim to enhance your organization’s cybersecurity maturity. Our cybersecurity experts guide you in developing and refining your security policies and procedures. Through comprehensive risk assessments, we help you plan your security investments in the most effective way. We also design customized training programs to raise cybersecurity awareness across your teams, ensuring they are better prepared to recognize and respond to evolving threats.

FAQ

What is continuous vulnerability scanning and why is it important?

Continuous vulnerability scanning refers to regularly scheduled scans aimed at identifying and reporting security vulnerabilities within an organization's IT infrastructure. In today's landscape, where cyber threats constantly evolve, one-time scans are no longer sufficient. Regular scans help detect newly emerging vulnerabilities and threats promptly — allowing organizations to address them before attackers can exploit them.

What is the difference between vulnerability scanning and penetration testing?

Vulnerability scanning uses automated tools to detect known weaknesses in systems and is typically broader in scope. Penetration testing, on the other hand, involves manual simulation of real-world attacks from an adversary's perspective to determine whether vulnerabilities can actually be exploited. While scans can be performed frequently and quickly, penetration tests are more in-depth and less frequent. When used together, they provide both surface-level and deep security insights.

How often should vulnerability scans be performed?

The frequency of scans depends on your organization's size, industry and risk profile. Generally, monthly or weekly scans are recommended. For organizations with critical systems, more frequent scanning may be necessary. It's also important to conduct scans after deploying new systems, making major updates, or experiencing a security incident. Regular scanning helps you stay current in a rapidly changing threat landscape.

Which systems and applications are included in the vulnerability scanning service?

The service can include network devices, servers, desktop and laptop systems, mobile devices, web applications, databases and cloud services. Specialized systems like IoT devices and Industrial Control Systems (ICS) can also be included. In particular, OT/ICS/SCADA networks should be scanned with dedicated policies. The scanning scope is tailored to your organization's needs and security objectives.

Will vulnerability scans impact system performance?

Scans are planned and conducted to minimize any impact on system performance. The tools used are configured to avoid excessive consumption of system or network resources (excluding DDoS or load testing). Scanning schedules can be set during non-peak business hours to further reduce potential disruptions.

How are scan results reported and utilized?

Scan results are presented in detailed and easy-to-understand reports. These reports include vulnerability descriptions, risk levels, affected assets and recommended remediation steps. Technical teams use them to prioritize and remediate issues, while executive summaries support decision-making at the management level.

What is the cost of the continuous vulnerability scanning service?

Pricing depends on factors such as the number of assets, infrastructure complexity, scan frequency and additional services required. A tailored proposal is prepared after a needs assessment. In the long run, this service helps you avoid costly cyber incidents and data breaches, making it a cost-effective investment.

How does the service support regulatory compliance?

Regular vulnerability scanning helps fulfill periodic security control requirements for standards such as KVKK, ISO 27001 and PCI DSS. It assists with meeting legal obligations and performing well in audits, while also enhancing trust among customers and partners by safeguarding sensitive data.

Does continuous vulnerability scanning eliminate all cyber risks?

While it significantly reduces risks, it does not eliminate them entirely. Cybersecurity requires a multi-layered defense strategy and vulnerability scanning is just one part of it. When combined with other controls like firewalls, antivirus software, penetration testing and user training, it delivers the best results. Continuous monitoring and improvement are key to minimizing cyber risk over time.

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