Privia SECURITY

Continuous Vulnerability Scanning Service

Professional Offensive Security Services

"Discover, Prevent, Stay Safe!"

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

“Discover security vulnerabilities by regularly scanning your systems. Quickly remediate identified vulnerabilities and protect against cyber threats.”

The Regular Vulnerability Scanning Service is designed to continuously monitor and detect security weaknesses in organizations' Information Technology (IT) and Operational Technology (OT) infrastructures. In today's rapidly evolving landscape of cyber threats and attacks, one-time security scans conducted annually are insufficient. This service regularly scans your organization’s networks, servers, applications, and other critical components to instantly identify newly emerging vulnerabilities.

Promptly identifying security vulnerabilities and mitigating risks within your organization’s systems is a crucial action against cyber attacks. The Regular Vulnerability Scanning Service continuously matures your security posture by utilizing up-to-date threat databases and advanced scanning tools. It also helps ensure compliance with legal regulations and industry standards.

While reducing the workload of your cybersecurity team, the Regular Vulnerability Scanning Service prevents critical vulnerabilities from being overlooked. Based on the collected information, documentation, and findings, the reports and action plans provided enable you to continuously update and enhance your organization's security policies.

Service Components

Automated Vulnerability Scanning

Using advanced scanning tools, all assets, networks, and applications within your environment are regularly scanned. Automated scans quickly detect new vulnerabilities without the need for manual intervention. Scan results are classified and prioritized according to their risk levels.

Real-Time Updates

Scanning tools and vulnerability databases are continuously updated to provide protection against the latest threats. Due to the dynamic nature of cyber threats, new vulnerabilities can emerge at any moment. Real-time updates enable you to respond instantly to new threats.

Reporting and Analysis

Scan results are presented in detailed reports. Identified vulnerabilities, their impact areas, and recommended solutions are included in the reports. While the reports provide detailed information for technical teams, they also offer summaries and strategic insights for management. These reports enable the creation of effective action plans against security weaknesses.

Compliance and Regulation

Our Regular Vulnerability Scanning Service helps ensure compliance with KVKK, ISO 27001, and other national and international standards. Regular vulnerability scans assist you in meeting legal requirements.

Expert Support and Consulting

Our Cybersecurity Experts analyze the scan results and provide the most appropriate solution recommendations for your organization. They offer consulting services to help improve your security strategies and update your policies.

FAQ

What is Regular Vulnerability Scanning Service and Why Is It Important?

Regular vulnerability scanning service consists of periodic scans aimed at continuously detecting and reporting security vulnerabilities within an organization's information technology (IT) infrastructure. As cyber threats and attack methods constantly evolve, one-time scans are insufficient. Regular scans help instantly identify newly emerging vulnerabilities and threats. With periodic scans, security weaknesses are detected and remedied before cyber attackers can exploit them.

What is the Difference Between Regular Vulnerability Scanning and Penetration Testing?

Regular vulnerability scanning focuses on detecting known security vulnerabilities in systems using automated tools and is usually broad in scope. Penetration testing, on the other hand, manually attempts to breach systems from an attacker’s perspective to verify whether vulnerabilities can actually be exploited. Vulnerability scans can be performed quickly and frequently, whereas penetration tests are deeper and performed less often. When used together, they provide both surface-level and in-depth security assessments.

How Often Should Regular Vulnerability Scans Be Conducted?

The frequency of scans depends on your organization's size, industry, and risk profile. Generally, monthly or weekly scans are recommended. However, organizations with critical systems may require more frequent scans. It is also important to perform scans after adding new systems, major updates, or security incidents. Regular scans help you stay updated against an ever-changing threat landscape.

Which Systems and Applications Are Included in Regular Vulnerability Scanning?

The service can cover all IT assets such as network devices, servers, desktops and laptops, mobile devices, web applications, databases, and cloud services. Special systems like IoT devices and industrial control systems (ICS) can also be included. Regular vulnerability scanning for OT/ICS/SCADA networks should be conducted with specially tailored policies. The scanning scope can be customized according to the organization’s needs and security objectives.

Does Scanning Affect System Performance?

Scanning activities are planned and executed to minimize the impact on system performance. Scanning tools are configured not to overconsume network and system resources (except for DDoS and Load Testing). Scan scheduling can be arranged during off-peak hours for the organization to further reduce any disruptions.

How Are Scan Results Reported and How Are These Reports Used?

Scan results are presented in detailed and easy-to-understand reports. These reports include descriptions of detected vulnerabilities, their risk levels, affected assets, and recommended remediation steps. Technical teams use these reports to prioritize vulnerabilities and initiate mitigation processes. Summary reports prepared for managers support strategic decision-making processes.

What Is the Cost of Regular Vulnerability Scanning Service?

The cost of the service varies depending on the number and complexity of systems to be scanned, scan frequency, and any additional services. A customized quote requires a detailed assessment of your needs. In the long run, regular vulnerability scanning helps save costs by preventing potential cyberattacks and data breaches.

How Does Regular Vulnerability Scanning Contribute to Legal Compliance?

Regular vulnerability scans meet the periodic security control requirements mandated by legal regulations and standards such as KVKK, ISO 27001, and PCI DSS. The service helps you fulfill legal obligations and succeed in audit processes. It also enhances your credibility by protecting the data of your customers and business partners.

Does Regular Vulnerability Scanning Completely Eliminate Cyber Risks?

Regular vulnerability scanning significantly reduces cyber risks but cannot eliminate them entirely. Cybersecurity requires a multi-layered defense approach, and vulnerability scanning is one part of this strategy. It is most effective when combined with other security measures such as firewalls, antivirus software, penetration testing, and user training. Continuous monitoring and improvement minimize cybersecurity risks to the lowest possible level.

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