SECRAGON

OFFENSIVE SECURITY SERVICES

Every Bit, Every Byte, WHERE VULNERABILITIES EXIST, ATTACKS HAPPEN! Act Today, Secure Tomorrow!

Secragon is a cybersecurity firm dedicated 100% to penetration testing services, security audits, attack simulations, and specialized cybersecurity solutions. We are certified ethical hackers, penetration testers, innovative engineers, and experienced managers, but first and foremost – professionals, WHO LIVE AND BREATHE OFFENSIVE SECURITY. Our expertise isn't just a list of qualifications; it's a culture of genuine “thinking outside of the box” mindset and we constantly strive to learn, explore, and push forward to master complex concepts and deliver unparalleled services and results. Secragon stands out as the go-to partner for business leaders who are committed to achieving top-tier security and seek to collaborate with best-in-class providers.

Our mission is clear: to leave your digital landscape more secure than we found it. We're here to offer invaluable advice, dissect and reconstruct for enhanced security, educate and consult, enhance quality and reduce costs, and maximize your ROI in cybersecurity.

Why Secragon?

20 Years of Expertise

Tracing our ethical hacking roots back to the early 2000s, we’ve built a solid foundation of knowledge and experience. We understand the technologies, but we also know how to delve on a deeper level!

Offensive Security Passion, Not A Job

At Secragon, hacking is a way of life. Our team is consistently in the top 1% in global CTF hacking competitions.

Flexibility and Adaptation

We approach each project with a hacker's mindset, going beyond standard methodologies. Malicious hackers are not interested in standards and methodologies but in a specific goal. So are we!

Custom Tools and Exploits

Tracing our ethical hacking roots back to the early 2000s, we’ve built a solid foundation of knowledge and experience. We understand the technologies, but we also know how to delve on a deeper level!

Cybersecurity Community and Events

Tracing our ethical hacking roots back to the early 2000s, we’ve built a solid foundation of knowledge and experience. We understand the technologies, but we also know how to delve on a deeper level!

APPLICATION SECURITY

Web Application Penetration Testing

Web Application Penetration Testing is a type of ethical hacking engagement aimed at identifying cybersecurity flaws in web applications. Due to their complexity and ubiquity, custom-designed, proprietary, and increasingly intricate web applications introduce complex and diverse security challenges to the security posture of any organization. Modern web applications handle increasingly sensitive data, so it is important to ensure that they do not introduce significant risks.

Mobile Application Penetration Testing

Mobile application penetration testing is a type of ethical hacking engagement aimed at detecting and identifying loopholes or vulnerabilities before they are exploited for malicious gain and analyzing the severity posed by them. Due to their complexity and ubiquity, custom-designed, proprietary, and increasingly intricate mobile applications introduce complex and diverse security challenges. With the sophistication of cyber-attacks increasing and the million-dollar bug bounty programs offered, organizations are beginning to prioritize penetration testing investments.

API Penetration Testing

API penetration testing is a type of ethical hacking assessment aimed at detecting and identifying loopholes and vulnerabilities before they are exploited for malicious gain. It involves simulating attacks on APIs to uncover potential vulnerabilities, and ensuring that the communication between different software systems is safe and protected from unauthorized access, data breaches, and other security incidents. With the sophistication of cyber-attacks and the million-dollar bug bounty programs, organizations are beginning to prioritize API penetration testing investments.

Thick Client Penetration Testing

Thick client application testing is generally more complicated and customized, involves both local and server-side processing, and often uses proprietary protocols for communication aimed at detecting and identifying loopholes and vulnerabilities before they are exploited for malicious gain. Simple automated scanning is not sufficient and testing thick client applications requires a lot of patience and a methodical approach.

Secure Source Code Review

A secure code review is a strategic 'White Box' testing activity aimed at detecting and identifying loopholes and vulnerabilities before they are exploited for malicious gain. A Secure Source Code Review is always customized and requires a deep understanding of the application's features and business rules. Our approach leverages industry-standard methodologies to ensure a thorough security assessment is conducted under safe and controlled conditions and utilizes an advanced mix of scanning tools and manual inspection. Beyond mere detection, Secragon stands out for discovering complex vulnerabilities not yet published and often not yet discovered.

NETWORK SECURITY

External Network Penetration Testing

The network edge is the last barrier to the open internet. With increased data breaches and attacks on businesses of all sizes, customers, regulators, and insurers require external penetration testing to ensure the perimeter is a reliable stronghold against attackers. At Secragon, we specialize in penetration tests that are 95% manual, designed to replicate real-world hacking, and conducted by experienced ethical hackers. Along with leveraging industry standard methodologies to ensure a thorough security assessment is conducted under safe and controlled conditions, our expert team utilizes an advanced mix of public and in-house developed exploits and in-depth analysis to discover vulnerabilities not yet published and often not yet discovered. The objective is to penetrate target systems and evaluate the robustness of the external network's security so that the organization can implement protective measures to mitigate risk.

Internal Network Penetration Testing

The perimeter cannot be relied upon exclusively to protect internal systems. An attacker needs only one path to gain access. Once inside, an insecure internal network can be exploited to rapidly escalate privileges. Internal attacks have severe results and often go undetected for longer periods.Performing an internal pen test identifies vulnerabilities in critical internal assets, demonstrates the impact if exploited, and provides clear direction on improvements that can be implemented to mitigate that risk. With our Internal Infrastructure Penetration Testing service, we assess the security of your internal systems and infrastructure, including your Active Directory (AD) and Azure environments. By conducting targeted evaluations from an internal perspective, we identify vulnerabilities and weaknesses that could be exploited by insider threats or compromised accounts. This assessment assists you in strengthening your internal security measures, ensuring the integrity and confidentiality of your infrastructure.

Wireless Network Penetration Testing

Our Wi-Fi Security Assessment focuses on evaluating the security of your wireless network infrastructure. We examine the deployment, configuration, encryption protocols, access controls, and authentication mechanisms of your Wi-Fi network. By identifying vulnerabilities and weaknesses, we help you strengthen the security of your wireless infrastructure, ensuring that unauthorized access or data breaches are mitigated.

Mainframe Penetration Testing

Mainframe penetration testing is an assessment that identifies vulnerabilities within mainframe systems, using the same techniques as hackers to breach your infrastructure. According to most mainframe manufacturers' terms and conditions of warranty, including IBM, it is each user's responsibility to detect and mitigate any vulnerabilities, whether at the software or hardware level. In addition, industry standards require that penetration testing needs to be performed regularly.Secragon's mainframe testing services offer valuable insight into your LPAR security, providing actionable guidance on how to improve your in-scope mainframes and systems security and help meet compliance requirements.

OT/ICS/SCADA Penetration Testing

OT/ICS/SCADA Penetration Testing is a specialized form of security testing focused on Operational Technology (OT), Industrial Control Systems (ICS), and Supervisory Control and Data Acquisition (SCADA) systems. These systems are integral to managing industrial and critical infrastructure processes. The testing involves simulating cyberattacks to identify vulnerabilities in these systems, which are often crucial for the functioning of vital sectors like energy, water, and manufacturing. This testing is essential to ensure these systems are resilient against potential security breaches, safeguarding them from disruptions that could have widespread consequences.

CLOUD SECURITY

Our Cloud Security Assessment focuses on evaluating the security of your cloud infrastructure, specifically targeting leading cloud service providers such as AWS, GCP, Azure and others. We assess the configuration, access controls, data storage mechanisms, and communication channels within your cloud environment. By identifying potential vulnerabilities and misconfigurations, we help you enhance the security posture of your cloud deployments, protecting your critical assets and data.

OTHER SERVICES

Vulnerability Assessment

Vulnerability assessment in cybersecurity refers to the process of identifying risks and known vulnerabilities across computer networks, systems, hardware, applications, and other parts of your IT ecosystem, on-prem and cloud. Vulnerability assessments provide security teams and other stakeholders with the information they need to analyze and prioritize risks for potential remediation in the proper context. These assessments are an important component of the vulnerability management and IT risk management lifecycles, helping prioritize time and resources, increase ROI on cybersecurity investments, and protect systems and data from unauthorized access and breaches.

IoT Penetration Testing

At its core, the Internet of Things (IoT) refers to a vast array of physical devices — from smart home appliances and security systems to industrial sensors and healthcare monitors — all interconnected via the Internet, along with their associated software, hardware, and networks. The extensive connectivity of IoT devices to the internet inherently raises significant security concerns. Companies are expected to have concerns over their IoT security as the ever-increasing number of smart devices used for business operations in today opens up a much broader attack surface for cyber-attacks. In other words, the number of entry points available for hackers nowadays is massive. Such security breaches may lead to exceptional financial losses, data and identity theft, compliance issues, unauthorized use of IoT devices, and costly downtime.

Social Engineering Assessment

Social Engineering Penetration Testing encompasses a diverse range of simulated attacks and assessments designed to exploit human vulnerabilities within an organization's security infrastructure. This practice is fundamental for uncovering hidden business risks and enhancing protocols that mitigate the threat of various attacks, including phishing, vishing, smishing, pretexting, impersonation, dumpster diving, USB drops, and tailgating.Among social engineering methods, phishing stands out as the most prevalent, contributing to over 90% of all data breaches. One in 99 emails contains a phishing attempt, and the remediation cost for phishing attacks averages a substantial $4.65 million. Ensure the resilience of your organization by prioritizing Social Engineering testing and comprehensive training programs. Empower your team to recognize and effectively thwart social engineering threats!

Cybersecurity Consulting

Every business is as unique as the threats it faces. As an experienced and established provider of cybersecurity services, we focus our efforts on the threats that can impact your specific industry, technology, and challenges – providing a unique, bespoke, and cutting-edge perspective of offensive security. We ensure our approach is flexible and adaptable to your evolving requirements, fostering a security-aware culture where organizational needs and objectives are balanced with a clear understanding and appreciation of applicable and emerging cyber threats. We don’t just point out security holes; we help you solve them and comply with standards and regulations.

The 3 Types of Penetration Testing

White Box

Involves full disclosure of network and system details, including maps and credentials, streamlining the process and cutting costs. Ideal for simulating attacks using multiple vectors.

Black Box

No prior information, mimicking an unprivileged attacker's approach. This offers a realistic scenario of an external attack but is often the most expensive due to its complexity.

Grey Box

Limited information is provided, typically user credentials. Assesses the damage a privileged user might cause, offering a balance between thoroughness and efficiency. This method is preferred for its realism without extensive reconnaissance.

Deliverables and Insights

At the end of the engagement, your final report will provide a customized course of action for both leadership and technical audiences.

The Executive Summary

is a high-level overview targeted at nontechnical stakeholders— senior management, auditors, boards of directors, and other concerned parties.

The Detailed Technical Report

is primarily for IT professionals, security teams, system administrators, and technical management.

Executive Summary

Key findings, risks, impacts, and critical recommendations.

Methodology

Overview of methodologies, standards, tactics, and techniques used.

Technical Report

Detailed vulnerability analysis, reproduction steps, PoC, evidence.

Recommendations

Strategic and tactical walkthrough on how to fix vulnerabilities.

Expert Guidance

Comprehensive advice on cybersecurity enhancement strategies.

Complimentary Retest

Offered once vulnerabilities are fixed.