Securin

Penetration Testing as Service
Test Your Defenses Before an Attacker Exploits Them

Organizations today need to test their digital environment continuously to know the gaps in their security and to learn how an attacker could exploit them in real time.

Securin's Penetration Testing helps you understand how exploitable your vulnerabilities are and how best you can defend yourself against them. Learn how adversaries can exploit your vulnerabilities and weaknesses to breach your critical systems and sensitive data.

Our penetration testing simulates a real-world attack on your digital assets. We adopt a hacker's perspective to detect and exploit vulnerabilities in your environment to determine if we can move laterally and compromise your entire IT infrastructure and applications.

Securin Penetration Testers are an elite bunch of ethical hackers who use the same tactics, techniques, and procedures (TTP) that attackers use to exploit vulnerabilities and gain a foothold into your environment and disrupt business operations. Securin's Penetration testers use MITRE ATT&CK framework and NIST 800-115 methodology to stress test your defenses.

Detect, Prioritize, Remediate

100+
Penetration Testers & Threat Hunters

54+
Zero-Days Discovered

CVE™

Why Customers Trust Us

We became a CVE Numbering Authority to help the U.S. Department of Homeland Security and MITRE validate newly discovered vulnerabilities and expedite their entry into the National Vulnerability Database.

Securin

Why Should You Penetration Test Your Assets?

Test Your Resilience
Discover and identify vulnerabilities in your digital environment that could be exploited by attackers.

Gain Compliance
Test your compliance with industry standards ISO 27001, ISC2, HIPAA, GRC, PCI-DSS, PCI-QSA, and SOC 2.

Protect Intellectual Property
Validate your security controls, and know how vulnerable your assets are.

Remediate Exploitable Vulnerabilities
Get a penetration testers's perspective about vulnerabilities that could be easily exploited by attackers.

Understand an Attacker's Perspective
Organizations need to continuously penetration test their environment to understand an attacker's perspective and attack chaining capabilities.

Preemptively Remediate
Red flag vulnerabilities that could be exploited by hackers and preemptively remediate weaknesses that could lead to a breach.

OSCP

CISSP® Certified Information Systems Security Professional

PCI DSS COMPLIANT

PCI Security Standards Council

CISA Certified Information Systems Auditor. An ISACA® Certification

CISCO CERTIFIED CCNA

OWASP

Securin

Here's How We Do It!

Our methodology follows the MITRE ATT&CK framework and NIST 800-115 along with the latest Techniques, Tactics, and Procedures (TTPs) used by attackers.
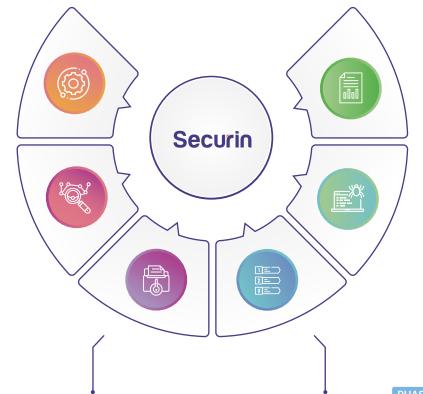
PHASE 1

RECONNAISSANCE

We gather information about ports, protocols, and services by scanning assets and discovering your attack surface.

PHASE 2

VULNERABILITY VALIDATION & EXPOSURE ANALYSIS

We identify vulnerabilities and flag false positives, and analyze all vulnerabilities based on their potential to be exploited and used maliciously against the organization.

PHASE 3

PENETRATION TESTING

We perform automated and manual penetration tests to exploit vulnerabilities by attempting to bypass existing security controls. We follow the MITRE ATT&CK framework and NIST 800-115, along with the latest Tactics, Techniques and Procedures (TTPs) to mimic a hacker's stealth attack methods to gain an initial foothold, escalate privileges, and perform lateral movements without being detected.

Securin

PHASE 6

STRATEGIC REPORTS & DELIVERY

Our results are delivered through a Risk-based Vulnerability Management (RBVM) platform that can be easily integrated with your existing security tools and ticketing systems.

PHASE 5

ATTACK LIKELIHOOD

We warn organizations about vulnerabilities that have a higher probability of weaponization in the future, using our Threat Intelligence Platform (TIP), to ensure your attack surface is patched before an attack is even planned.

PHASE 4

PRIORITIZATION OF VULNERABILITIES

We prioritize vulnerabilities based on weaponization and exploitability and tell you what to fix first.

Securin

Key Benefits

Reduce your Attack Surface

Proactively identify vulnerabilities that could be exploited by attackers and remediate them on priority. Improve your security posture by understanding advanced tactics used by hackers to exploit vulnerabilities.

Know your Security Gaps

Understand your security gaps and your exposures as we adopt a hacker's perspective to target misconfigurations, blindspots, missing patches, coding errors and critical weaknesses.

Remediate Immediately

Remediate the prioritized list of vulnerabilities to achieve fast remediation and to increase your security posture. Knowing what you fix first reduces the burden on security teams.

Synchronized Results

Synchronized delivery of results allows our customers to view identified vulnerabilities within hours of commencing the assessment, thus enabling rapid remediation.

About Securin

For over a decade, Securin, formerly known as Cyber Security Works (CSW), has been helping hundreds of customers worldwide gain resilience against evolving and emerging threats. Powered by accurate vulnerability intelligence, human expertise, and automation, our products and services have enabled organizations to make critical security decisions to manage their attack surface.

Follow us On

Securin

info@securin.io
securin.io

Reduce your risk and exposure. | Email us to schedule a consultation at **info@securin.io**