DATA SHEET

Securin

Penetration Testing

The Need for Penetration Testing

Most organizations – mid to large enterprises, SLED, and government – have holes in their defenses and compliance:

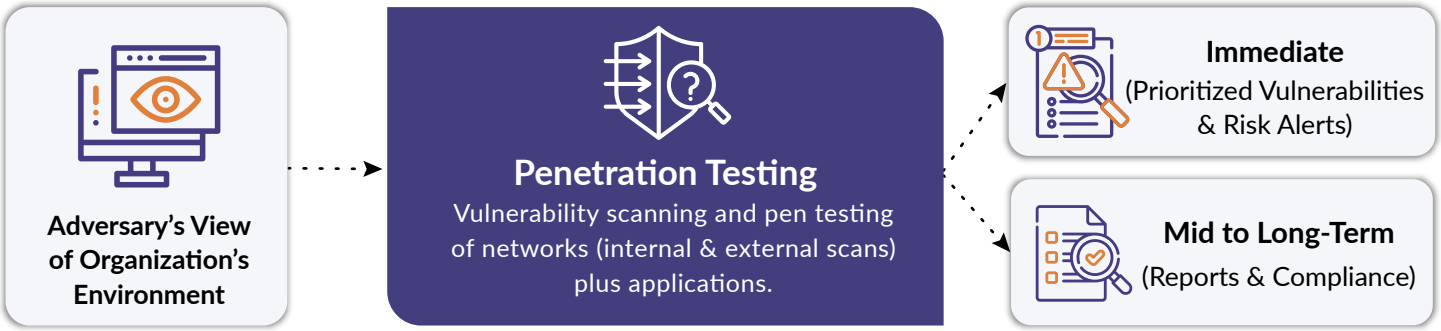
- **Breaches and Exfiltrations:** Incidents are typically discovered long after the damage was done. By then, tracing the adversary's attack path becomes challenging, making it difficult to prevent future attacks.
- **Unknown Attack Surface:** Organizations frequently overlook potential attack surfaces. For instance, a high-profile data breach at a casino began with an attack on the online monitoring system for their aquarium.
- **Compliance Standards:** Documenting compliance with industry standards can be challenging, as the effort required to understand and implement these standards is often burdensome.

Security teams need expert, unbiased testing to uncover immediate vulnerabilities, highlight strategic holes in their organization's defenses, and ensure compliance.

Introducing Securin Penetration Testing

Securin penetration testing (pen testing) replicates a real-world cyberattack on the organization's digital assets. Our expert team approaches the IT environment from an adversary's perspective, identifying and exploiting vulnerabilities to assess whether lateral movement and a full system compromise are possible. Securin penetration testers are an elite group of ethical hackers that use the same tactics, techniques, and procedures (TTP) as malicious attackers to exploit vulnerabilities and gain a foothold in the organization's environment and disrupt business operations.

Service Overview



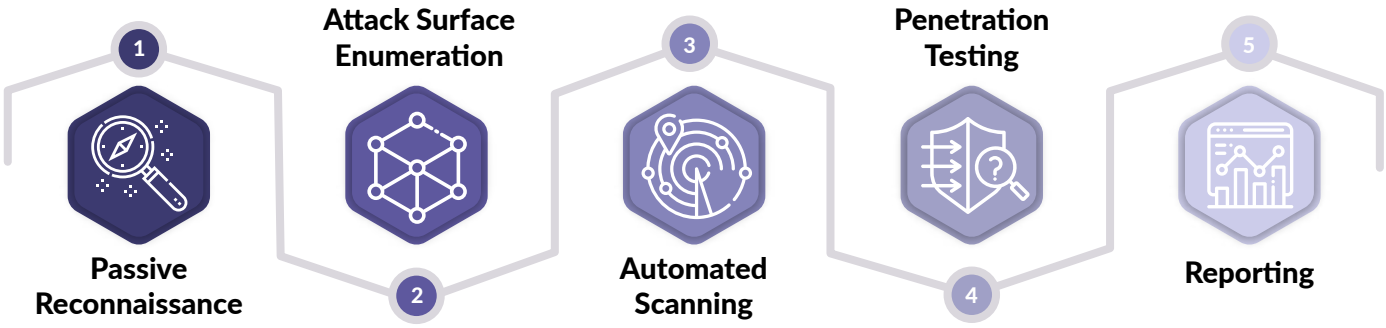
Adversaries move fast, so time is precious. To minimize reaction times, output of pen testing is in two categories:

- **Immediate:** Securin provides a prioritized list of high impact vulnerabilities for immediate action with other high impact risks flagged for attention.
- **Mid to Long-Term:** We provide strategic reports and compliance information, helping organizations implement long-term initiatives to protect their environment. Additionally, organizations can use Securin's data for any required compliance reporting.

Securin provides the full attack chain and kill chain so that the organization's security team can fully address all vulnerabilities and risks discovered by our pen testing team.

Methodology

Securin pen testing leverages a proven methodology in phases to minimize time to implement defenses.



PHASE 1: Passive Reconnaissance

Techniques such as information gathering, documentation review, Dark Web mining, and web service enumeration are employed to collect data on publicly accessible systems and services. This helps establish a baseline understanding of the organization's environment and potential vulnerabilities.

PHASE 2: Attack Surface Enumeration

Testers identify and map out all the potential entry points into the organization's system. This includes discovering IP addresses, operating systems, open ports, and protocols. The process also involves service fingerprinting, analyzing the web application user interface, and reviewing access controls. URL crawling and spidering are used to explore web applications, while business logic identification and recognizing input and reflection vectors help in pinpointing areas vulnerable to attack.

PHASE 3: Automated Scanning

Automated tools are utilized to conduct comprehensive vulnerability scans. These scans aim to identify vulnerabilities, misconfigurations, missing patches, and coding errors, with a focus on known issues such as those listed in the OWASP Top 10 and the CWE/SANS Top 25 Most Dangerous Software Errors. This quickly identifies any potential weaknesses that need to be addressed.

PHASE 4: Penetration Testing

Our pen testers actively exploit identified vulnerabilities to evaluate the organization's security posture. Techniques include exploit development, vulnerability exploitation, and testing various attack vectors. It also involves data injection and manipulation, data exfiltration, chaining multiple vulnerabilities to amplify the impact, and demonstrating the real-world impact of successful attacks.

PHASE 5: Reporting

All collected data is aggregated and mapped to the MITRE ATT&CK framework to provide a comprehensive overview of the findings. The report includes detailed documentation of the exploits used, a prioritized list of vulnerabilities based on their potential impact, cyber risk quantifications, and documentation to reproduce attacks. Additionally, it offers remediation recommendations to help the organization strengthen their security posture.

Features

Securin's core capabilities enable security teams to get ahead of hostile adversaries.

Strategic Security Guidance	Securin provides insights into the advanced, hacker-led tactics most likely to be effective in the organization's unique environment, enabling more strategic efforts to protect against these particular attacks.
Adversary Tactics	Securin penetration testers conduct a real-world attack on the organization's existing security controls to test their efficacy and identify exploitable vulnerabilities. We follow the MITRE ATT&CK framework, NIST 800-115, and the latest TTPs to mimic a hacker's attack methods to gain an initial foothold, escalate privileges, and perform lateral movements to stress test defenses.
Contextual Vulnerability Combinations	Securin identifies combinations of low-scoring vulnerabilities in the Common Vulnerability Scoring System (CVSS) that, when combined, pose significant risks in a specific environment. Hackers often exploit these combinations to evade detection, as each individual vulnerability usually falls below the critical or high threshold.
Full Attack Methodology Reporting	Securin provides comprehensive attack methodology reporting—from initial entry through lateral movement to the final objective, such as undetected data exfiltration or code injection. These reports enable organizations to understand how an adversary could infiltrate their systems and learn how to avoid such an attack.
Kill Chain Reporting	Securin's kill chain reporting offers clear guidance on disrupting the attack chain. The report details the compromised systems or controls and outlines the necessary steps to resolve the issue.
Full Posture Assessment	Securin provides a comprehensive understanding of an organization's vulnerabilities and exposures by identifying misconfigurations, blind spots, missing patches, coding errors, and critical weaknesses.
Phased Result Delivery	Securin makes it a priority to deliver results in a phased manner. By synchronizing the delivery of identified vulnerabilities, organizations can begin remediation efforts as soon as possible.
Actionable, Prioritized Findings	Rather than highlight potentially millions of vulnerabilities, we prioritize findings in an organization's unique environment so security teams can make an immediate impact on strengthening their security posture.
Verify Compliance with Industry Standards	We test compliance with industry standards such as ISO 27001, HIPAA, GRC, PCI-DSS, and SOC 2. Organization's can leverage our expertise to achieve compliance with mandated industry-specific regulations related to healthcare, finance, and technical industries.

Securin pen testing can cover any or all aspects of complex environments.

Environments

With decades of expertise in infrastructure, web, mobile, cloud, and internet of things (IoT) pen testing, Securin is every organization's one-stop shop for all their pen testing needs. We offer both standard and customized testing options.

Network Penetration Testing

Internal Network Penetration Testing

Securin's internal network pen testing focuses on testing infrastructures commonly deployed in data centers and office networks—for example, Windows domains, network configuration interfaces, and printers. Testing simulates scenarios where attackers have gained a foothold on a network through phishing, browser compromise, and virtual private network (VPN) compromise.

External Network Penetration Testing

Securin's external pen testing gives organizations an accurate picture of the risk associated with their externally facing assets. Our pen testers identify all externally facing assets in scope and test their security controls to help determine how vulnerable they are to attackers.

Application Security Services

Web Application Penetration Testing

Securin's web application pen testing evaluates web applications using OWASP Top 10 Web Vulnerabilities and the SANS/MITRE Top 25 Programming Error lists. We use our proprietary framework to discover attack vectors by passing or inputting data to places where inputs are processed. As part of dynamic testing, our team will determine the areas of the code that are critical to application security.

SaaS Penetration Testing

Securin's software as a service (SaaS) pen testing evaluates the platform's web application components, infrastructure, application programming interfaces (APIs), and source code. Securin uses a distinct and customized approach based on the target SaaS platform's development components, features, and business functionality.

Mobile Application Penetration Testing

A mobile application pen test is a point-in-time security control review of a mobile application or its components. This assessment's two key testing sections are static analysis and dynamic analysis. This allows Securin to conduct a detailed security examination of the target mobile application components while gathering information to rank and prioritize threats.

API Penetration Testing

Securin's API pen test validates the security of an organization's methods and corresponding data. Our testing methodology uses standardized processes to ensure consistency and that the organization's API workflow is secure. We evaluate all applications using OWASP API Top 10 and CWE Top 25 programming errors.

Why Securin

Securin leverages a unique set of capabilities in penetration testing.

- **Provide Full Attack Methodology:** Provides full attack methodology (attack chain) covering everything from initial entry and lateral movement to the end goal, such as data exfiltration or undetected code injection.
- **Leverage Data on Compromised Credentials:** Securin pen testers leverage compromised credentials and other information from the Dark Web, obtained from the patented Securin Vulnerability Intelligence (VI) and Securin External Attack Surface Management (EASM) products. Securin's credential intelligence provides 40x more detection of compromised accounts and passwords than open-source (OSINT) frameworks.
- **Break the Attack Chain:** The Securin kill chain report offers guidance on disrupting the attack chain and includes details on the compromised systems or controls, along with the steps needed to address and resolve the issues.
- **Find Contextual Vulnerabilities:** Securin identifies combinations of low CVSS score vulnerabilities that, when combined, can be highly dangerous in a specific environment. Hackers often exploit these combinations to evade detection.
- **Utilize our CNA Thought Leadership:** As a CVE Numbering Authority (CNA), Securin identifies new vulnerabilities, conducts thorough research on both new and existing vulnerabilities from detection through remediation, and publishes formal threat research papers. We use this expertise to help organizations identify, understand, and address issues with their cybersecurity defenses.

Benefits

Penetration testing provides both one-time and ongoing benefits.

Prevent Breaches & Exfiltrations

Prevent breaches and data exfiltrations due to ransomware triggering, Remote Code Execution, and other attack vectors by proactively resolving weaknesses in security.

Span Entire Attack Surface

Cover the organization's entire attack surface in depth – network, applications, SaaS, APIs, mobile, and more – to ensure consistent and full protection.

Compliance with Industry Standards

Prove compliance with industry standards by having certified industry experts test environments with the latest techniques and tactics used by hostile adversaries.

About Securin

At Securin, we empower teams and organizations to minimize their business risk with our comprehensive range of offensive cybersecurity solutions. These solutions are carefully crafted to be intuitive, adaptable, and scalable, catering to organizations of all sizes in today's ever-changing digital landscape. Securin's human-augmented intelligence approach to cybersecurity empowers organizations to thrive by proactively addressing emerging threats and uncertainties, ensuring their security.

Securin
securin.io

Follow Us On