Securitybeat Advisors

(252) 248-9010

Penetration Testing Services

Concern

In today's rapidly evolving cybersecurity landscape, organizations face concerns that jeopardize their valuable assets and sensitive data. Without the necessary expertise and tools to evaluate the business environment from a **hacker's perspective**, companies struggle to proactively identify and manage vulnerabilities, leaving them exposed to potential breaches and their detrimental impacts. Impacts not only impair operations, but breaches also often result in penalties and legal settlements. There is also significant pressure from stakeholders to annually demonstrate robust system security even in the absence of material development.

Our Solution

Securitybeat Advisors utilizes Cobalt's **Penetration Testing as a Service** (PTaaS) platform to deliver a cost-effective, comprehensive, expert evaluation of applications, cloud infrastructure, AI large language models, and Internet of Things (IoT) infrastructure. Clients get the initial test and unlimited retests. Securitybeat Advisors adds value by delivering baselines for Application Security, Cloud Security, AI Security, and IoT Security

Penetration Test Options	Value Proposition
Application Penetration Test - **Web Application** - **Mobile Application** - **API**	1. Establish Trusted Advisor in Application Security. 2. Document software assurances and issues within sensitive applications. 3. Validate underlining technical controls and business logic. 4. Errors and omissions during application development. 5. Identify systemic application development process or training issues.
Cloud Penetration Test	1. Establish Trusted Advisor in Cloud Security. 2. Identify means to exploit and penetrate environment from the outside. 3. Identify rogue and unmanaged cloud assets. 4. Identify unmanaged technical vulnerability. 5. Identify weakness in the security of the cloud network fabric.
LLM/AI Penetration Test	1. Establish Trusted Advisor in AI Security. 2. Identify vulnerabilities to prompt injection, adversarial manipulation, or retrieval-layer attacks across your AI systems. 3. Choose the right level of coverage for your architecture — from a focused prompt injection sprint to a full RAG pipeline assessment. 4. Protect the integrity and confidentiality of your AI system or LLM, preventing unauthorized access or misuse
IoT Penetration Test	1. Establish Trusted Advisor in IoT Security. 2. Gain a holistic view of your IoT ecosystem's security posture. 3. Hedge against supply-chain attacks with firmware testing. 4. Ensure that your device isn't the cause of a wider network compromise

Securitybeat Advisors follows a comprehensive four-step process to prioritize remediation effectively by:

1. Leveraging Cobalt's expertise to defend findings and rate the severity of discovered vulnerabilities.
2. Working with the development team to address findings with minimum impact.
3. Aligning remediation efforts with business needs, considering goals, risk tolerance, and regulatory requirements.
4. Developing a risk-based plan, addressing high-risk vulnerabilities first and tailoring it to the organization's unique context.

As a result of the test, the client knows what was tested, how it was tested, what the specialist identified as vulnerable, remediation recommendations from the specialist, and the agreed upon remediation plan developed in partnership with Securitybeat Advisors.