守阙安全团队服务介绍

守阙安全团队

2026年4月

2026

CONTENT

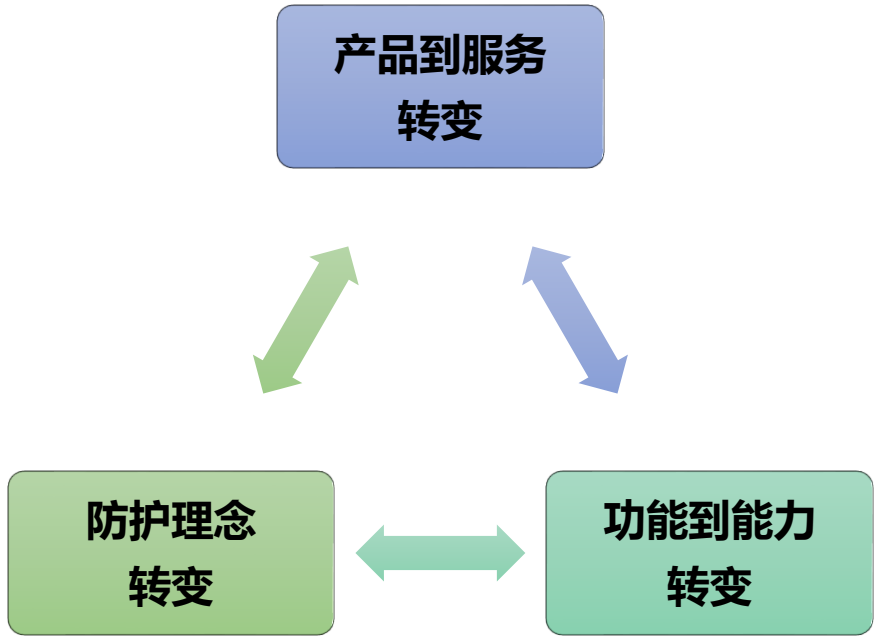
目录

01

安全服务发展趋势

安全服务驱动防护体系转变

根据IDC统计数据，2021年我国网络安全市场规模为122.0亿美元，其中硬件产品为47.0亿美元，占比为38%；软件产品42.4亿美元，占比35%；服务产品32.4亿美元，占比为27%。整体来看，市场呈“三足鼎立”态势。



安全的本质是人与人的对抗，安全服务从以前注重防护，转变为以攻验防，以攻促防。

从安全合规到实战需求跃迁

威胁升级，风险深化

全球网络攻击复杂度与频度持续攀升，深埋的 业务逻辑缺陷与 供应链风险 成为新焦点。

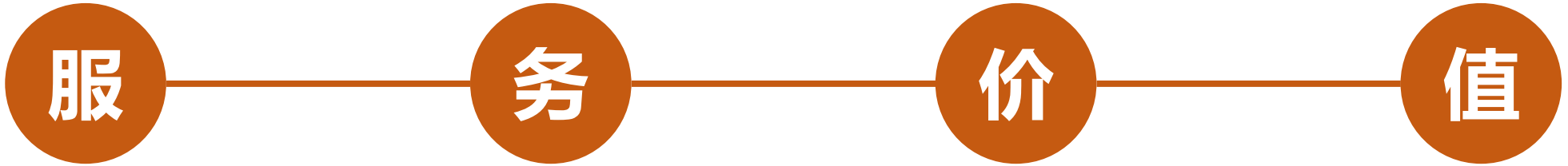
政策驱动，市场扩张

关基条例、数安法等法规叠加，要求关键行业定期开展 深度测试并闭环整改 ，催生第三方安全服务市场高速扩张。

重心转向，实战验证

企业预算重心转向“实战化验证”，通过 模拟真实入侵路径提前暴露隐患，降低重大损失与品牌危机。

安全服务的价值



动态防御	安全合规	能力提升	安全保障
安全产品是静态被动式防御，突破安全产品的防御只是时间问题。 安全服务变被动为主动，防患于未然。	安全服务满足网络安全相关法律法规和政策导向的刚性需求； 助力通过监管单位和上级单位的合规检查。	网络安全的本质是人与人的对抗，服务是攻击者视角。 人员能力参差不齐，安全服务提升安全能力。	有效发现网络安全薄弱点，提供针对性的安全整改建议， 验证网络安全防御能力，护航业务稳定运行。

02

守阙安全团队简介

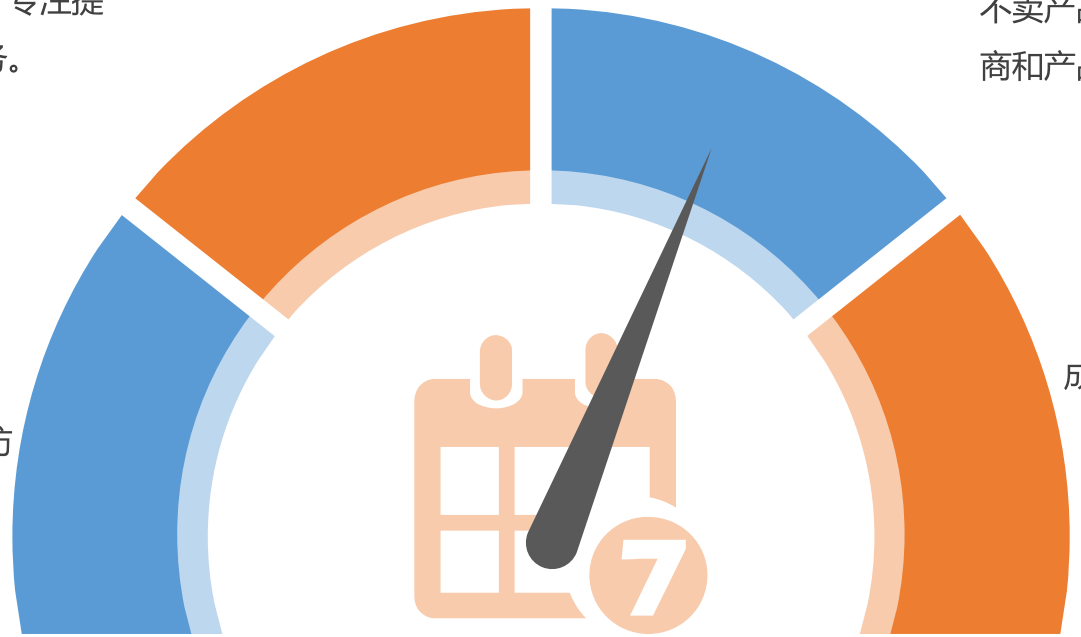
守阙安全团队简介

行动准则

守业务之固，察系统之阙，专注提供高端网络与信息安全服务。

团队实力

具备扎实的安全技术研究、产品实践、服务交付、攻防实战及HW重保能力。



服务理念

不卖产品、只做服务，不与任何厂商和产品产生利益关联，确保服务公开、公平、公正

服务范围

成立于2024年，位于四川省成都市，服务范围全国

三大核心服务

模拟黑客攻击手法，对业务系统进行授权攻击测试，通过模拟攻击查找系统潜在的安全漏洞，并提供修复建议。

运用动态分析和静态检测技术，对APP应用进行安全评估，查找安全漏洞和安全风险，提供针对性的修复建议。

结合工具审计和人工核查，对源代码进行逐条检查，分析源代码中的安全缺陷和不规范编码，分析潜在的安全风险。

服务优势

工具结合人工交叉测试

采用工具与人工交叉测试，先以专业工具探测常见漏洞，再由工程师人工挖掘隐性风险，相互验证补充，提升评估的全面性和精准度。

人工测试占比70%以上

测试中人工挖掘占比超过70%，工程师凭实战经验模拟攻击，捕捉工具难以探测的高危漏洞和逻辑性 漏洞，提供贴合实际的安全保障。

安全漏洞风险整改复测

客户对漏洞和风险进行整改修复后，对修复情况进行复测，若整改未达标则再次给出整改建议，确保漏洞有效清零，无残留安全隐患。

报价模式

守阙安全团队服务报价模式				
服务名称	**序号**	**服务类型**	**区分标准**	**报价模式**
安全渗透测试	1	安全渗透测试-远程	目标可以通过互联网访问，或通过VPN方式访问。	按系统数量报价
	2	安全渗透测试-现场	目标在用户内网，不能通过互联网访问，服务人员需要到用户现场测试。	
服务名称	**序号**	**服务类型**	**区分标准**	**备注**
APP安全评估	1	APP安全评估-标准型	人工评估为主，工具扫描为辅。包括1个APP服务端、1个Andriod客户端、1个IOS客户端。	按APP数量报价
	2	APP安全评估-精简型	工具扫描为主，人工评估为辅。包括1个APP服务端、1个Andriod客户端、1个IOS客户端。	
服务名称	**序号**	**服务类型**	**服务内容（区分标准）**	**备注**
源代码审计	1	源代码审计-标准型	按业务系统的逻辑行代码量报价，工具预审计+人工验证审计+详细报告。	按代码逻辑行报价，精确到万行
	2	源代码审计-精简型	按业务系统的数量报价，工具审计+简单报告。	按系统数量报价

03

三大核心服务内容

安全渗透测试

在用户的授权和监督下，模拟黑客攻击手法，对目标系统进行非破坏性的安全测试，查找存在的漏洞并进行利用，完成后给出详细的漏洞修复建议。

B/S系统、APP

服务价值：

- 主动发现、验证业务系统中的安全漏洞和隐患，并提出针对性的修复建议。
- 变被动为主动，降低系统被攻击的可能性。

服务优势：

- 人工渗透占比80%以上，所有漏洞均手工验证。
- 渗透测试报告人工编写，非工具导出，无误报。

交付成果：

- 渗透测试报告（含漏洞修复建议）
- 渗透测试复测报告（漏洞修复后）

APP安全评估

通过人工和工具结合的方式，运用动态分析和静态检测技术，对APP应用（客户端、服务端）进行安全评估，查找存在的安全漏洞和安全风险，并提供针对性的修复建议，确保APP应用的安全。

Android客户端

程序开发、应用发布、应用安装、应用卸载、应用合规、完整性、机密性、数据输入、数据存储、数据传输、数据输出

IOS客户端

程序保护、安全策略、敏感信息、数据通信、密码软键盘、业务功能

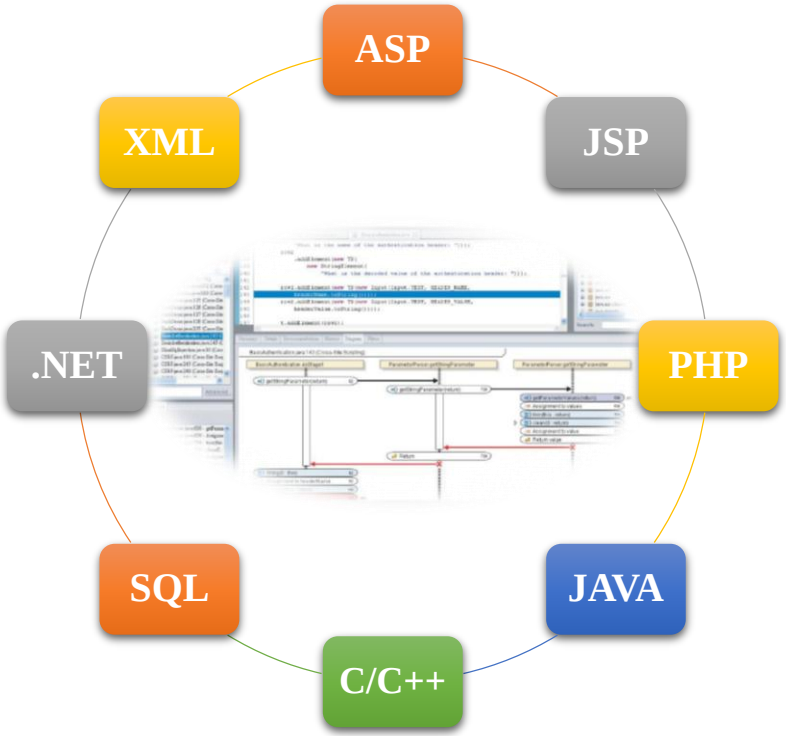
服务端

渗透测试（信息泄露、越权、口令、注入、上传、跨站、逻辑、数据库。。。）

交付成果： Android 客户端安全评估报告、IOS 客户端安全评估报告、服务端渗透测试报告

源代码审计

检查源代码中的安全漏洞、安全隐患、安全缺点、错误信息，分析并验证这些问题可能导致的安全风险，并提供对应的代码修复建议，从而确保系统代码层面的安全。



服务价值：

- 充分挖掘代码中存在的安全缺陷以及规范性缺陷；
- 让开发人员了解应用系统面临的安全威胁，指导其对程序缺陷进行修复，提升系统的安全性。

服务优势：

- 预审计使用业界领先的Fortify SCA，误报率相对较低。
- 人工分析、验证、确认，人工审计超过70%，确保准确。

交付成果：

- 源代码审计报告（含修复建议）
- 回归测试报告（漏洞修复后）

感谢观看，期待合作！

网站：www.nisse.com.cn
电话：181 9085 7504
微信：右侧扫码添加
邮箱：nisse_team@163.com