解决方案手册

SOPHOS

Sophos 咨询服务

Penetration Testing 渗透测试

通过模拟真实攻击手段验证您的安全防御能力

借助独立的专业知识与经验，结合量身定制的策略，来识别漏洞并验证安全防御机制，从而增强您的整体安全状态，降低风险，满足合规要求，并提升运营效率。

主动强化防御与安全状态

对企业资源的未授权访问、利用已知与新出现的漏洞、配置错误及安全策略薄弱等，都是严重的安全隐患。验证应用程序、网络及系统是否不受安全风险的影响，是在攻击者利用漏洞之前采取应对措施的关键。相比仅进行漏洞扫描与评估来识别您网络中的缺口和漏洞的“轻量作法”，需要深入的测试和验证来展示攻击者如何入侵您的环境，并以此为跳板对内部网络发起更深层次的攻击。

Sophos Penetration Testing 渗透测试服务

渗透测试（简称 Pentest）可识别并揭示网络安全漏洞，并解答一个核心问题：“攻击者是否能成功入侵我的网络？”渗透测试通过模拟真实网络攻击，来发现系统、网络与应用中的安全漏洞。经验丰富的测试人员（道德黑客）将尝试利用这些弱点，展示攻击者可能造成的实际影响。

渗透测试的主要类型包括：

- **外部渗透测试：**针对可通过互联网访问的系统，如网站、VPN 和面向公众的服务，模拟攻击者从外部试图突破防线。
- **内部渗透测试：**模拟内部威胁或已成功入侵外部边界的攻击者，重点测试内部网络中的系统、应用程序和数据。

Sophos 将每次渗透测试视为每个客户专属的独特任务。由业内顶尖安全专家执行，采用基于目标的测试方法论，并结合我们的专利战术及 Sophos X-Ops 威胁情报团队的情报。该团队包括对抗威胁小组 CTU，以高级持续性威胁 APT 和国家级攻击者的情报和研究而闻名。

优势

- 通过测试内部与外部安全控制措施，包括对高价值系统和资源的保护，增强安全保障信心。
- 基于符合您独特环境的威胁模型与情景，满足特定测试目标。
- 提供可执行的修补行动方案。
- 支持符合法规要求，包括 PCI DSS、HIPAA、GDPR、NIS、ISO 27001、SOC 2 等。
- 基于 Sophos X-Ops 威胁情报团队的最新情报得出的深度洞察。
- 评估您在真实世界中面临的遭入侵的风险。

模拟高级攻击，测试您的防御能力

组织开展定期渗透测试的目的不仅在于满足行业合规要求，更是为了主动应对日益复杂且不断演变的网络安全威胁态势。定期进行渗透测试，组织能够领先攻击者一步，防范他们不断调整利用新漏洞所采取的手法与技术。此外，渗透测试还可识别因基础设施变动、应用更新或第三方集成而产生的安全薄弱环节。更重要的是，渗透测试为组织提供了对真实风险暴露的清晰认知、可执行的修复策略，以及可量化追踪安全改进成效的方法。

渗透测试的优点包含：

- **主动降低风险：**定期进行渗透测试的组织，其安全事件发生率减少 50%，安全事件处理总成本降低 30%。[1]
- **合规支持：**许多法规框架（如 PCI DSS、HIPAA、ISO 27001）要求开展渗透测试。73% 的组织将合规视为推动渗透测试的主要原因之一。[2]
- **节约成本：**数据泄露平均代价高达 445 万美元，[3] 但透过渗透测试，可以在成本远低于此的情况下应对这些漏洞。
- **提升客户信任：**65% 的消费者表示更倾向信任展现强大网络安全措施的企业。[4]

测试员工的反应能力

人工智能已令钓鱼攻击的风险更为严峻，其能够生成高度复杂而极具说服力的假讯息，让人难以辨识。与传统的钓鱼邮件相比，AI 生成的信息不再充斥拼写错误和通用模板，而是能根据目标生成高度个性化、具有情景关联的内容，精准针对特定个人或组织。这使得安全团队和终端用户在识别和防范钓鱼攻击方面面临前所未有的挑战，也进一步凸显持续安全培训的重要性。

Sophos 渗透测试计划可结合模拟钓鱼攻击，全面评估员工识别、响应钓鱼行为的能力。

服务特点

- 可定制的测试专案规则，包括对目标系统中关键业务数据的检视。
- 提供包含详细发现结果与管理摘要的最终报告。
- 支持现场与远程测试选项。
- 可选择外部渗透测试、内部渗透测试及钓鱼攻击模拟训练，依据您的实际需求建构混合式威胁情境。
- 测试人员主导、人工操作的测试流程，采用真实攻击者使用的战术。
- 以目标为导向的方法，确保测试过程考虑到系统在整体环境中的作用与背景。

报告内容概览

管理摘要：面向高层管理、审计人员、董事会等非技术相关方。

详细发现：为技术人员提供深入的测试结果与修复建议。

测试方法说明：明确测试范围及所执行的测试活动。

过程叙述：描述测试人员为达成目标所采取的行动顺序，帮助理解多阶段及混合型威胁和 / 或相关攻击阶段。

建议措施：详列发现结果、延伸阅读链接，以及修复建议或风险缓解措施。测试人员在适用情况下附上发现的左证资料，并尽可能提供足够信息，让使用公开工具的情况下能重现问题。

钓鱼攻击结果（如适用）：详细说明钓鱼攻击方式及成功率。

更多网络安全测试服务

没有任何单一的评估方或技术可以全面反映组织的安全状态。每种对抗测试方式均有其目标及可接受风险水平。Sophos 可和您协作，来判定合适的评估和技术组合，来评估您的安全现况与控制，从而找出您的漏洞。

了解更多:
sophos.com/advisory-services

[1]Ponemon Institute [2]SANS Institute [3]IBM [4]PwC

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

2025-06-05 BRZHCN (MP)

SOPHOS