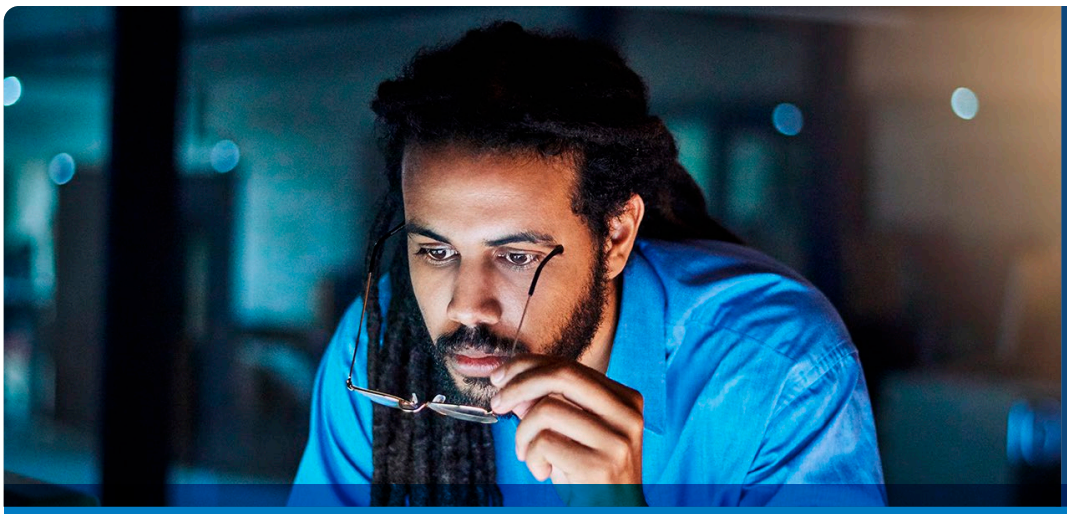
DELL Technologies

验证安全控制措施和策略以拦截攻击载体



模拟攻击者在初始访问、发送恶意文件、窃取数据等方面的技巧

渗透测试和攻击模拟管理

戴尔会验证您在整个杀伤链中的安全控制措施和策略

组织推行数百种安全控制措施，覆盖从端点到 Web 和电子邮件网关的方方面面。这些控制措施通常复杂且难于管理，如果配置有误，则可能给组织带来风险。攻击者会想方设法利用损坏或过时的控制措施。

为考验和证明贵组织安全控制措施的有效性，戴尔渗透测试和攻击模拟管理方案会逼真模仿现实生活中的攻击行为。

本服务具备以下特性：

- 每月进行自动化泄露和攻击模拟 (BAS)，以确定您的控制措施正常运行
- 每年进行渗透测试，让有经验的专家去尝试突破关键资产和数据防护

攻击模拟测试安全控制措施

戴尔安全专业人员会运用先进的 BAS 技术来测试不同的攻击载体，比如说，尝试将恶意软件植入端点，或者是从 Web 服务器获取未经授权的信息。戴尔测试员在整个杀伤链[1]期间运用 BAS 模拟攻击，以应对威胁，包括最近的攻击者 TTPs[2]。

BAS 技术对于生产环境是安全的，并且还能够不断接收新信息、攻击和行为。

渗透测试评估通向高价值目标的路径

尽管我们采用了攻击模拟技术，但也不能保证万无一失 — 有些攻击者仍能够渗入环境，避开障碍，进而窃取宝贵数据。这时，渗透测试可以助您一臂之力。

主要优势：

- 通过全面的泄露和攻击模拟技术，检测配置有误的安全控制措施，避免其被利用
- 进行月度模拟，以检测最近新出现的问题和漏洞
- 进行年度渗透测试，以密切检查针对高价值资产或数据的攻击
- 报告测试结果、季度趋势和值得注意的活动，以帮助您改善安全态势
- 通过特定测试快速了解新出现的高风险威胁

渗透测试能够完善 BAS — 不同于测试单个或成套的控制措施，渗透测试将关注点放在了环境中脆弱或风险较高的方面。戴尔渗透测试员可以针对特定目标（比如捕获高价值系统，或者窃取或禁用特定文件组），模仿攻击者的各种技巧，甚至是模拟不同的有效负载，开展攻击。经验丰富的渗透测试员能够像真正的攻击者一样，改变、调整并应用技巧，以达到目标。

应用测试信息，以改善安全态势

根据运行 BAS 序列得到的结果，Dell Technologies Services 每月都会提供报告，说明哪些安全控制措施问题需要得到纠正。戴尔每季度都会检视根据不同的攻击模拟总结出的趋势，汇报从贵组织的 IT 环境中观察出的值得注意的活动，以及讨论并推荐能够提升贵组织安全态势的措施。

主要特性	
泄露和攻击模拟 (BAS) • 根据客户的环境每月进行一次自动化泄露和攻击模拟 • 在外围和内部基础架构组件（包括 Web 网关、电子邮件网关和端点）上验证安全控制措施 • 持续使用新威胁信息、攻击和行为更新 BAS 工具 • 根据以前的模拟和安全环境因素对模拟工作流进行更改 • 根据威胁情报和戴尔的评估，针对新发现的安全问题运行临时模拟	**渗透测试** • 针对明确的 Web 网关、API、移动设备、外部 IP 地址、内部 IP 地址和云配置进行年度渗透测试 • 根据首轮测试结果进行修复后，重新进行渗透测试（可选）
报告和检视 • 针对进行的泄露和攻击模拟提供月度报告 • 提供季度报告并检视客户 IT 环境中观察到的趋势和值得注意的活动 • 提出改善整体安全态势的建议	**入门** • 召开服务启动会议 • 检视客户完成的合作前注意事项检查清单 • 检视客户 IT 环境 • 为客户激活 BAS 应用程序 • 提供代理程序部署协助

立即联系您的销售代表。

[1] “整个杀伤链” — 包括外部威胁（如网络钓鱼、Web 网关等等）、被侵害端点、在获取凭据或发生攻击传播时行动迟滞、数据泄露等等
[2] “TTPs” — 策略、技术和流程