2025 防御者指南

守护未来，共筑防御之盾

抢先一步应对新出现的攻击媒介，有效防范攻击者利用新手段来攻击旧目标。敬请阅读《防御者指南》文集中的以下重点内容，了解该从何处着手。

利用“安全纵深防御”框架，组织您的安全防护工作

需要考虑的三个关键因素

风险管理。根据特定威胁发生的可能性以及各种应对措施在降低企业风险方面的潜力，确定应优先采取的应对策略

网络架构。通过防火墙、分段和访问控制等技术实施分层安全保护，从而抵御攻击并限制其影响

主机安全。通过系统更新、防病毒软件、防火墙和访问控制等技术，保护各个设备免受恶意软件及未经授权访问的侵扰

恶意软件可能藏在哪里？

2024 年开放端口事件中最常见的协议

58.0%
服务器消息块 (SMB)

14.5%
远程桌面协议 (RDP)

12.9%
安全 Shell (SSH)

攻击者一旦侵入 VPN，他们可以执行哪些恶意活动？

- 使用远程身份验证服务器验证用户身份
- 滥用合法身份验证
- 使用恶意身份验证服务器
- 提取并解密配置文件中的敏感信息

防范 XSS 漏洞

- 对所有用户控制参数增加输出编码
- 通过代码审查和 Web 应用程序防火墙进行防御
- 阻止攻击者实际利用的攻击手段，如 Cookie 窃取、网站篡改和会话劫持/跨网站请求伪造

容器为何会成为攻击者的目标？

Akamai 研究人员发现 Kubernetes 中存在多个漏洞和可被利用的攻击手段，一旦被利用，则可能导致：

- 数据渗漏
- 特权提升
- 远程代码执行

主动防御与应急准备相结合

采取这四个基本原则：

- 全方位实施网络安全策略
- 始终将您的环境置于安全平台之后
- 专注于业务关键型服务
- 确保有可信赖的事件响应团队或合作伙伴随时待命以应对紧急情况

下载《2025 防御者指南》