CIS 2019
网络安全创新大会
Cyber Security Innovation Summit

网络攻防演练的现实思考

孙维伯　斗象科技 北京技术中心 技术总监

CIS 2019
网络安全创新大会
Cyber Security Innovation Summit

甲方80%的安全产品并未发挥有效作用

15%的漏洞是由配置错误造成的

54%的邮件社工、勒索等病毒无法通过技术防御

60%的情况下，攻击者可在数分钟攻破目标企业

现有的安全防御手段到底如何 ？

我的被黑客入侵了吗 ？

防御 还是 攻击 ？

甲方视觉下的攻防演练

理想的攻击队攻击过程（killchian/att&ck）

理想的演练收益

实际场景下乙方攻击队的故事

A队（模拟外部攻击者，主要以社工和技术直接突破为主）：






B队（模拟内部攻击者，主要以发现内网系统漏洞为主）：

OA系统漏洞、堡垒机漏洞、VPN漏洞、内网CRM漏洞、会议系统漏洞……

结论：

门禁管控系统产品和运营策略失效

监控系统产品安全策略失效

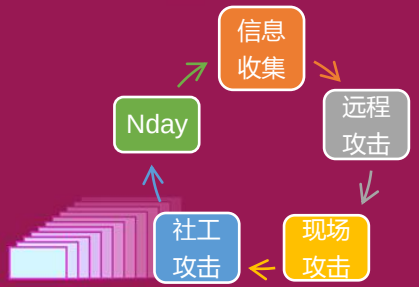
内网无线安全隔离策略失效

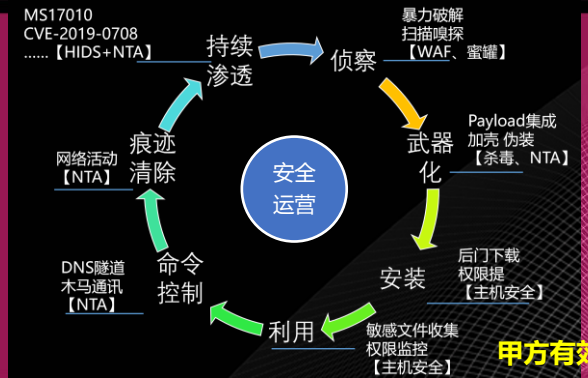
人员安全意识执行策略失效

渗透测试解决的是黑客从哪里进来的问题

攻防演练解决的是企业安全产品、运营策略是否持续有效的问题

真实的红军（red team）攻击过程





甲方有效防守体系

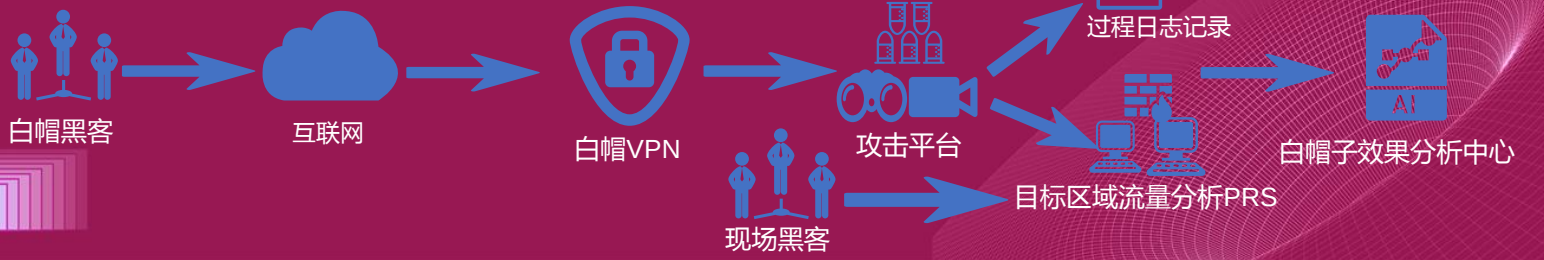
CIS 网络安全创新大会
Cyber Security Innovation Summit

新一代攻防演练技术发展

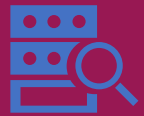
- 从单一的渗透测试变成持续性的攻击模拟
- 从传统的攻击工具变成攻击方式、人员能力的持续扩展平台
- 不断校正攻击手法，持续分析攻击目标，验证更多业务

- 从单一攻击模拟到持续攻击分析
- 从固定团队成员到白帽扩展平台
- 从固定攻击手法到动态的持续攻击分析

结合众测平台的攻防演练方案

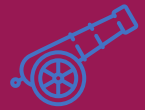


白帽攻击平台



资产探测

情报收集



攻击工具集

目标控制

钓鱼平台

日志回溯

加密流量自动解密

白帽子攻击手段画像

POC过程还原

效能统计

数据泄露预警

全程记录

网络安全创新大会
Cyber Security Innovation Summit

THANKS