锤炼新形势下实网攻防的“剑与盾”

张锦章 360攻防产品事业部总经理

CONTENTS / 目录

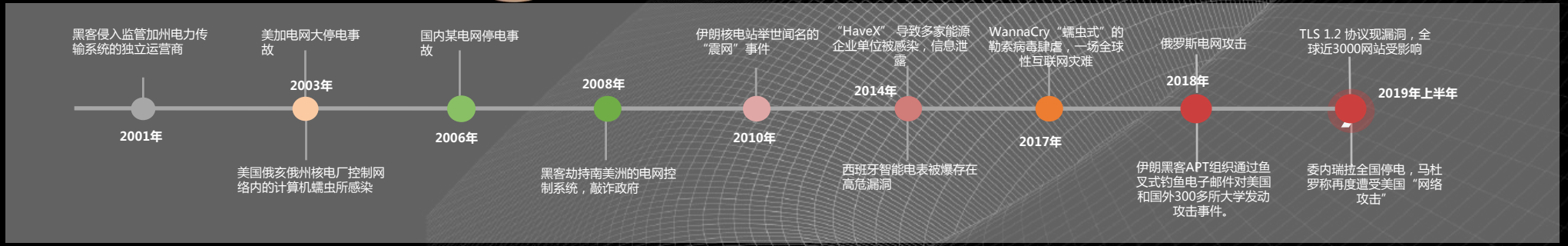
国内外当前安全态势与企业信息安全建设的思考

国内外网络安全发展态势

针对关键信息基础设施网络恶意攻击频发

各国在网络空间对抗态势进一步加剧

- 相关国家网络空间政策的调整以及网络军事力量建设加速，网络空间争夺将掀起新高潮。
- 各国将更加重视数据安全治理
- 我国信息技术产品自主可控生态亟待建立
- 我国关键信息基础设施的网络安全保障体系仍不完善

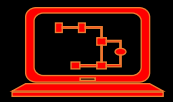


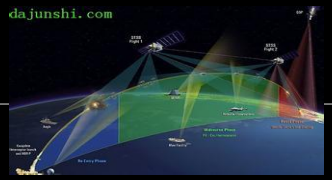
唯一不变的，是一切都在“变”

白开心

纯小偷

大玩家





威胁的演变与进化
需要关注对手与动机

环境、业务、组织架构的
演变？

技术不断的迭代？

四个方面看威胁的不断进化

更加有组织、有目的

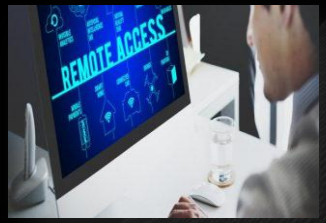
- 国家之间的网络战时时处处都在发生
- 针对中国的境外APT组织超过**38个**

破坏广度和深度加大

- WannaCry攻击全球**150多个**国家
- 国内**3万**多个机构**30万**台电脑被感染

业务环境发生剧变

- 业务云化导致边界模糊
- 移动应用兴起已全面代替传统办公终端



行为隐蔽、难以追踪

- 攻击手段无所不用其极
- **硬盘、芯片、IoT**设备等均可被植入恶意软件

思变：“危”则变，变则通，通则久

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

合规驱动

停留在使用安全设备应对外在威胁的思维模式、单纯的软硬件产品堆砌，面对高度人力化、无行为模式可寻的APT攻击，现阶段只有靠同等水平的人力才能实现抗衡。

渗透测试

依赖网络安全专业人员独立完成，测试对象多为孤立的应用系统，无法从企业整体角度评价安全水平。过程无监管，存在极大的不确定性。

能力提升

通过网络攻防靶场进行演练可以积累经验、锤炼队伍、培养人才、磨炼技术，才是企业应对未知安全威胁的长久之计！

如何践行与落实？

合规驱动安全需求

等保2.0、ISO27000、GB/T20984

BS25999、ITIL、ISO20000等

行业标准、规范及安全要求

企业一贯信息安全实践都是以合规先行，是正向思维，依赖安全标准、信息安全管理体系的建设。

正向思维

构建企业级网络靶场

日常运营模式：通过预置的训练场景实现企业内在安全软实力的全面提升。

事前，通过各种控制技术实现安全可控的渗透通道

事中，建立交火的前沿阵地，降低损失的同时充分了解对手，积累知识经验

事后，使用靶场统筹调度实施应急响应、捕获攻击行为并回溯

战时模式：

可迅速切换成仿真蜜罐，抵御分析，分析溯源

。

逆向思维

网络攻防是逆向思维，注重验证结果，从结论逆推方案，从发现问题切入，研究分析问题，给出解决方案，持续能力提升，在此过程中持续提高企业安全建设能力。

训、打、评、防、控

+

=

实网攻防靶场

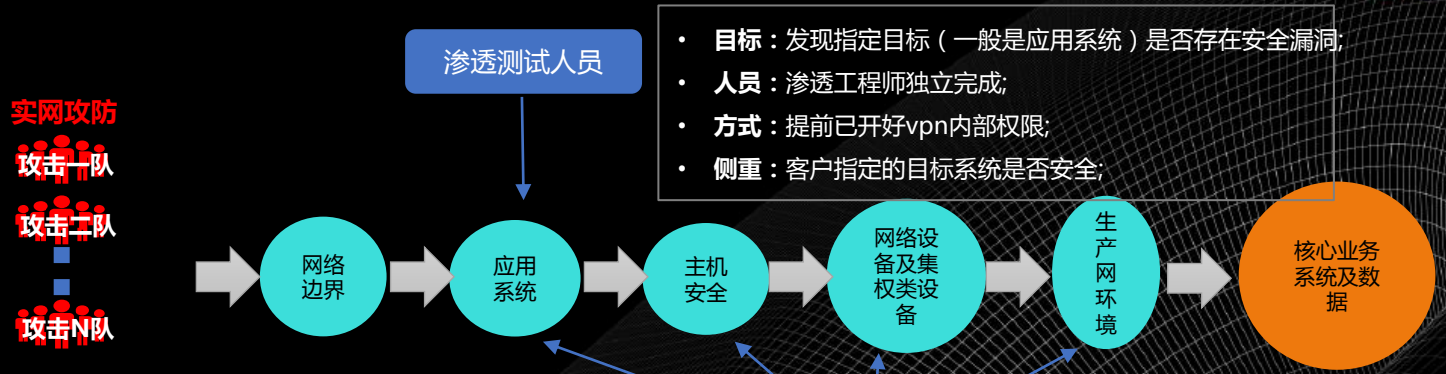
虚拟仿真靶场

最佳的靶场解决方案

“实网攻防”的意义

1. 实网攻防对抗能精准挖掘潜在的脆弱性及威胁
2. 实网攻防对抗能有效验证安全防护是否健壮
3. 实网攻防对抗能促进安全体系的敏捷改进
4. 实网攻防对抗能快速提升人员的安全能力

实网攻防与渗透测试、风险评估的区别

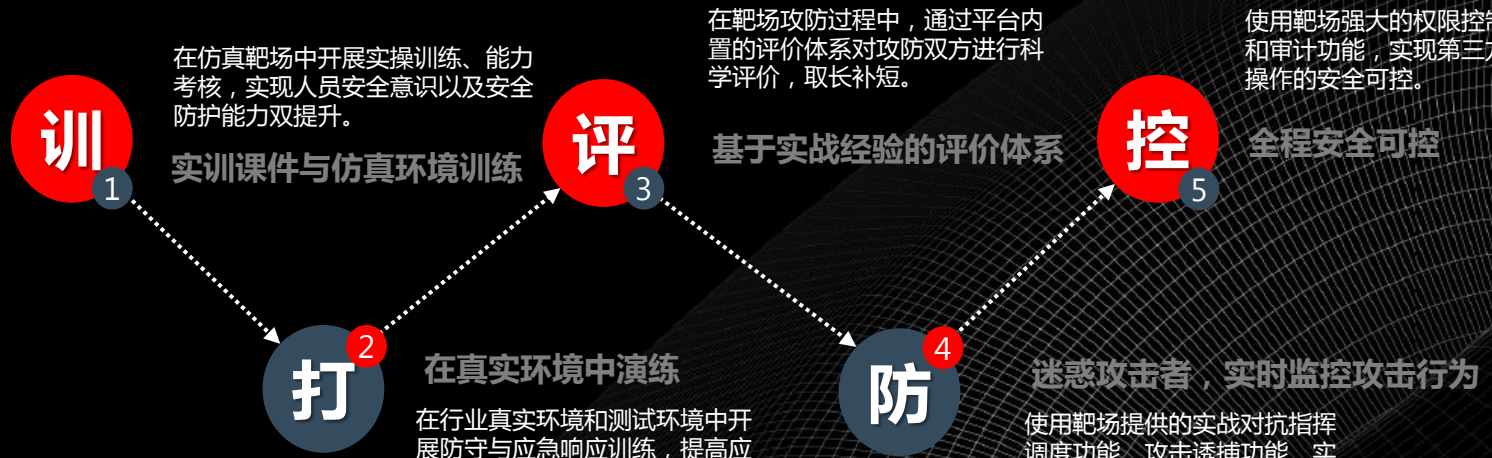


- **目标**：发现指定目标（一般是应用系统）是否存在安全漏洞;
- **人员**：渗透工程师独立完成;
- **方式**：提前已开好vpn内部权限;
- **侧重**：客户指定的目标系统是否安全;

- **目标**：不限制攻击路径、攻击手法，以提权、控制业务、获取数据为最终目的;
- **人员**：团队合作，各有所长;
- **方式**：没有内部权限，不限手段;
- **侧重**：防守单位整体的防护能力、应急响应能力等;

- **目标**：对业务系统安全风险评估;
- **人员**：监管测评机构进行风险评估;
- **方式**：按照一定规则检查;
- **侧重**：客户业务系统安全性评估;

从实践中提炼


训
1
在仿真靶场中开展实操训练、能力考核，实现人员安全意识以及安全防护能力双提升。
实训课件与仿真环境训练
打
2
在真实环境中演练
在行业真实环境和测试环境中开展防守与应急响应训练，提高应对真实威胁的能力+真实环境演练。
评
3
在靶场攻防过程中，通过平台内置的评价体系对攻防双方进行科学评价，取长补短。
基于实战经验的评价体系
防
4
迷惑攻击者，实时监控攻击行为
使用靶场提供的实战对抗指挥调度功能、攻击诱捕功能，实现攻击预警、行为分析以及攻击溯源。
控
5
使用靶场强大的权限控制和审计功能，实现第三方操作的安全可控。
全程安全可控


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