



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

PART / 01

现状与思考

PART / 02

靶场最佳实践

国内外当前安全态势与企业信息安全建设的思考

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

黑客侵入监管加州电力传输系统的独立运营商

美加电网大停电事故

国内某电网停电事故

伊朗核电站举世闻名的“震网”事件

“HaveX”导致多家能源企业单位被感染，信息泄露

WannaCry“蠕虫式”的勒索病毒肆虐，一场全球性互联网灾难

俄罗斯电网攻击

TLS 1.2 协议现漏洞，全球近3000网站受影响

2001年

2003年

2006年

2008年

2010年

2014年

2017年

2018年

2019年上半年

美国俄亥俄州核电厂控制网络内的计算机蠕虫所感染

黑客劫持南美洲的电网控制系统，敲诈政府

西班牙智能电表被曝存在高危漏洞

伊朗黑客APT组织通过鱼叉式钓鱼电子邮件对美国和中国300多所大学发动攻击事件。

委内瑞拉全国停电，马杜罗称再度遭受美国“网络攻击”

+ + + }_ 唯一不变的，是一切都在“变”

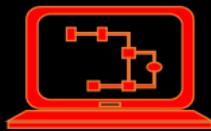
自开心



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**

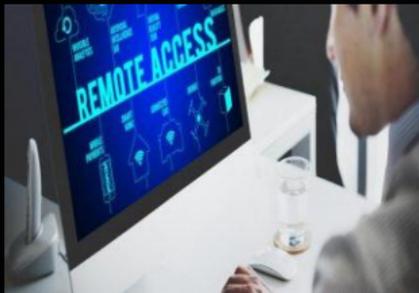


破坏广度和深度加大

- 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

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。

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。

渗透测试

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

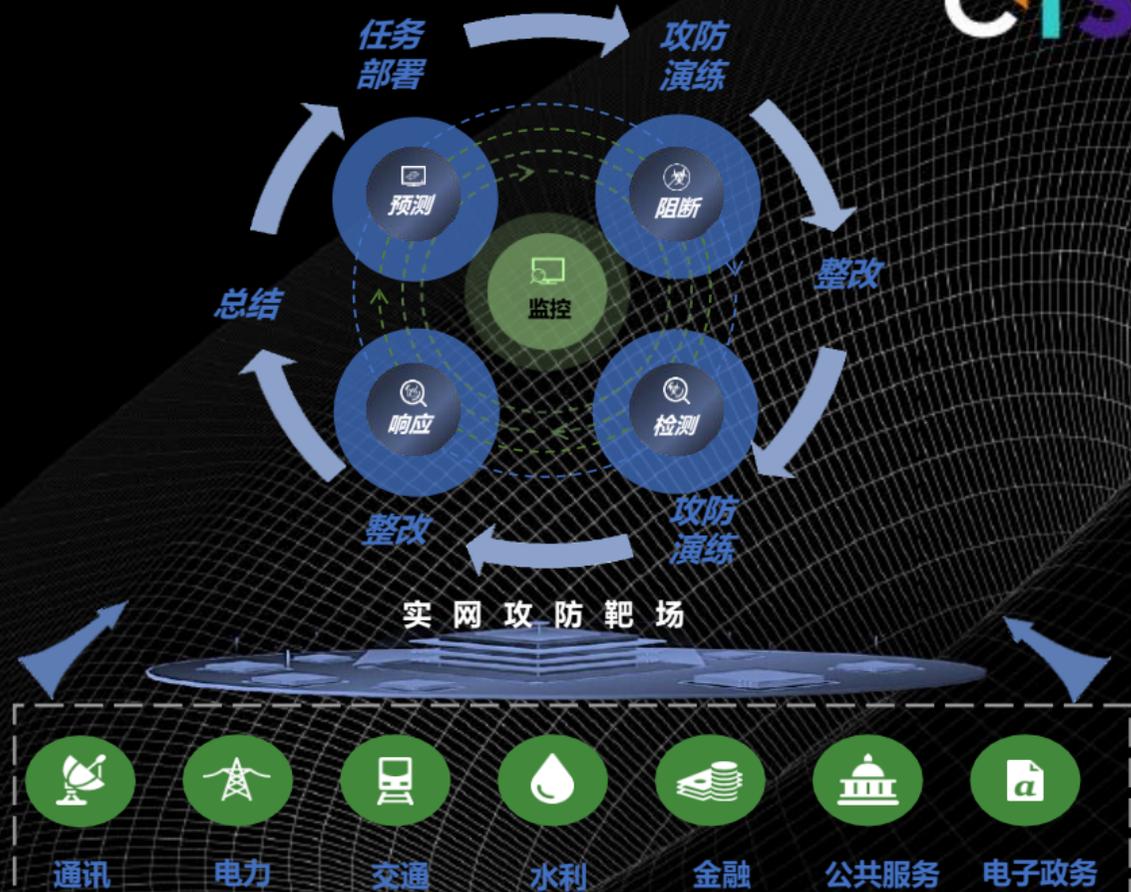
实网攻防对抗能**有效验证**安全防护是否健壮

3

实网攻防对抗能**促进**安全体系的**敏捷改进**

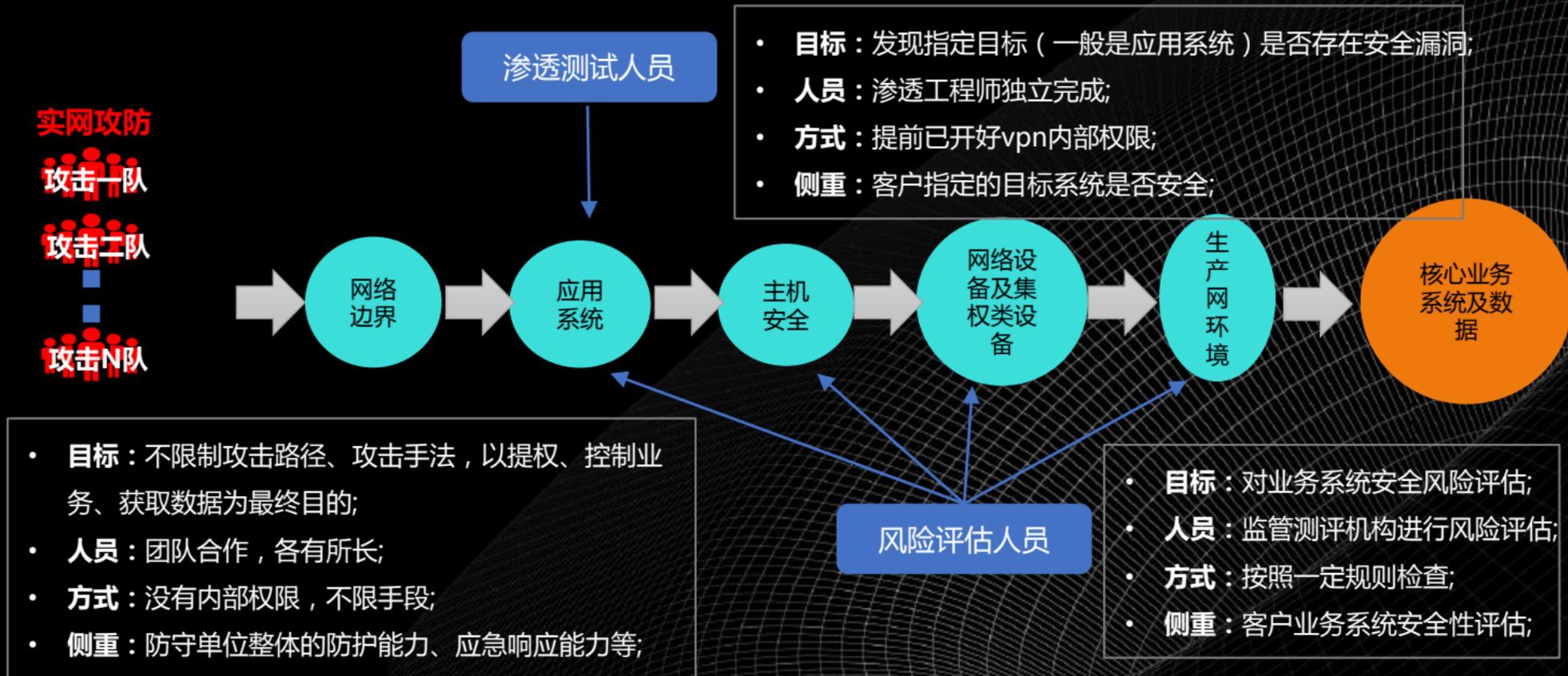
4

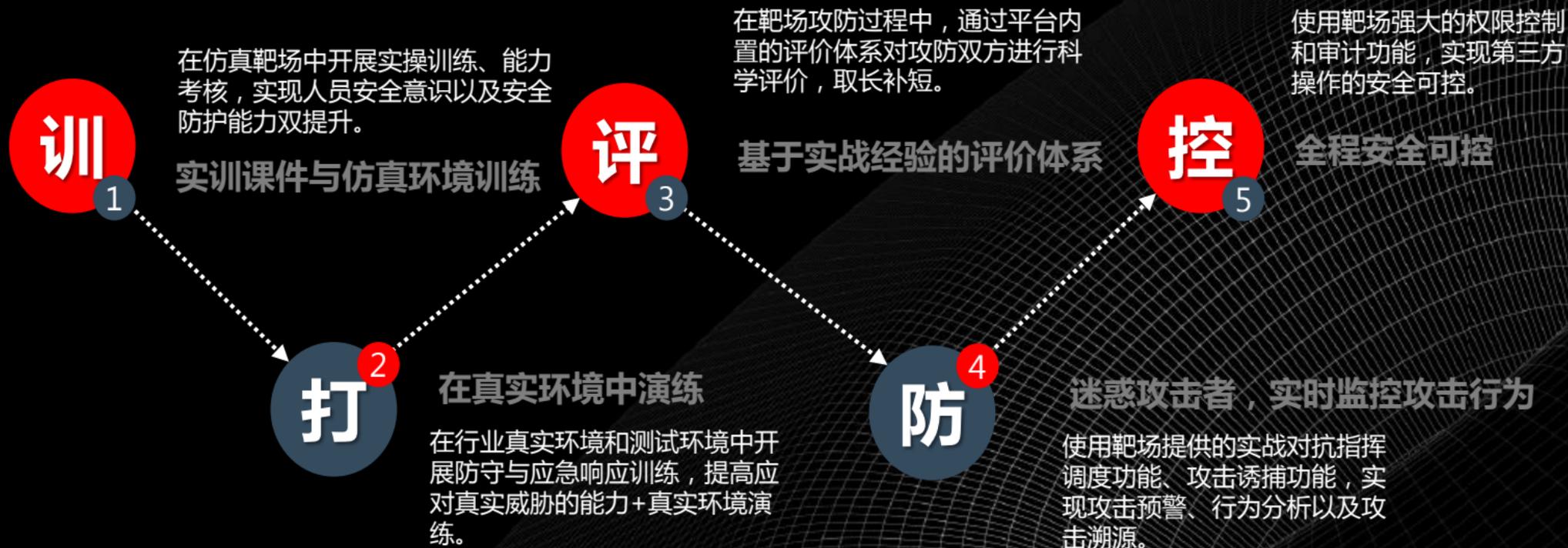
实网攻防对抗能**快速提升**人员的**安全能力**





实网攻防与渗透测试、风险评估的区别







网络安全创新大会
Cyber Security Innovation Summit

HANKS