ansion
安 | 信 | 与 | 诚

蓝队的自我修养

安信与诚 杨 亮

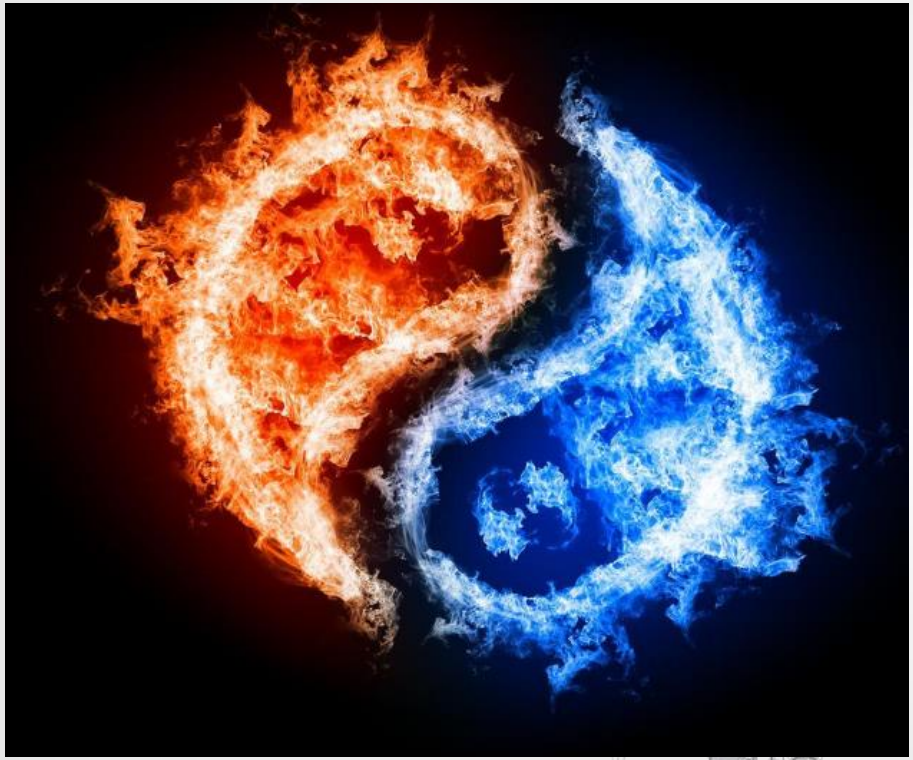
目录
Contents

ansion
安 | 信 | 与 | 诚

了解蓝队

ansion
安 | 信 | 与 | 诚 |

网络实战攻防演练



网络实战的攻防演练，通常是以实际生产中运行的重要信息系统作为保护目标，在有监督的情况下，进行攻防对抗，以不影响业务为前提，最大限度地模拟真实的网络攻击，以此来检验信息系统在实际安全保障工作的有效性。

ansion
安 | 信 | 与 | 诚

攻防演练的角色

红队：一般为攻击方

蓝队：一般为防守方

指挥部：一般为组织者

其他支撑机构

蓝队的组成

蓝队的攻防演练活动

做好全面监测
有效分析研判
提高处置效率

备战

查找自身不足
提高防范意识
建立有效机制

迎战

战后

战后总结分析
重点人才培养
完善安全策略

备战阶段中的蓝队

重要的活动

- 资产梳理
- 安全加固
- 缩小攻击面
- 安全意识宣贯
- 安全运营工作的规划

资产梳理

“过去银行一直是最受欢迎的目标，而现在资产管理者却面临更严峻的攻击威胁”

梳理范围：

- 内部资产（互联网资产、内网资产、人员）
- 分支机构资产
- 下属单位（或子公司）资产
- 外联单位
- 公有云资产
- 第三方厂商（开发商、外包商、服务商等等）

关键的资产属性：

域名、IP、端口、开源软件或框架、接口、管理后台、高危功能、远程接入点（接入方式及终端）、特权帐号

安全加固

安全设备加固

补丁更新

策略优化

数据库加固

网络设备加固

操作系统加固

应用服务加固

配置优化

安全检测手段：

漏洞检测、渗透测试、弱口令检测、配置检测、安全专家分析

安全加固目的：防止被撕口子

高度重视的关键项：

弱口令、远程代码执行、上传下载任意文件、权限问题、欺骗伪造等

可参考标准：

CVE、CNNVD、OWASP、行业安全基线要求等

缩小攻击面

关键资源：网络拓扑

了解攻击路径：

互联网-DMZ-内网

互联网、外设（U盘）-办公终端-内网

下属单位（或子公司）、分支机构-内网

外联单位-内网

业务终端-内网

无线-办公终端-内网

机房-内网

缩小攻击面：

关闭服务

关闭功能

访问和权限控制

管理限制

确定每条攻击路径都有防控手段

安全意识宣贯

培训范围：

内部、分支、子单位、第三方厂家

培训内容：

办公行为安全

防病毒

电子邮件安全

密码安全

违规外联

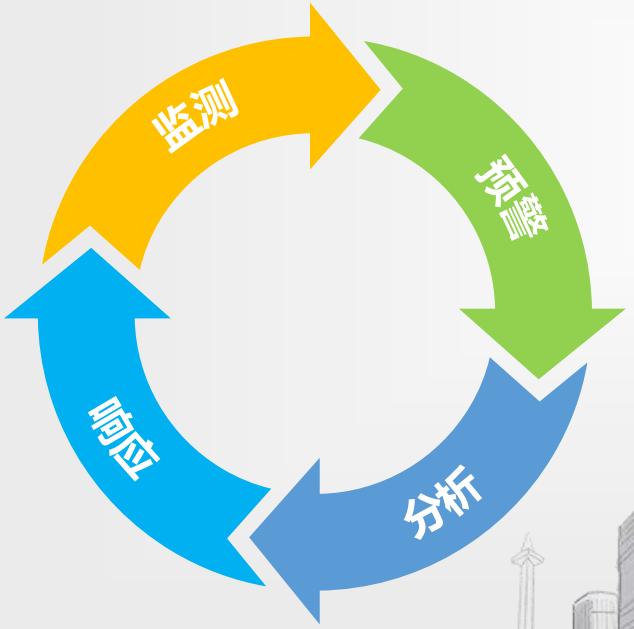
移动存储介质安全

第三方人员安全

移动通讯设备安全

安全运营的规划

人通过工具(平台、设备)来发现安全问题、验证问题、分析问题、响应处置、解决问题并持续迭代优化的过程。



关键的动作：

确认监测手段是否覆盖全资产

确认检测工具的有效性

确认防护手段的有效性

确认响应流程的有效性

明确各个成员职责

建立各成员之间良好的沟通和共享机制

准备充足的资源

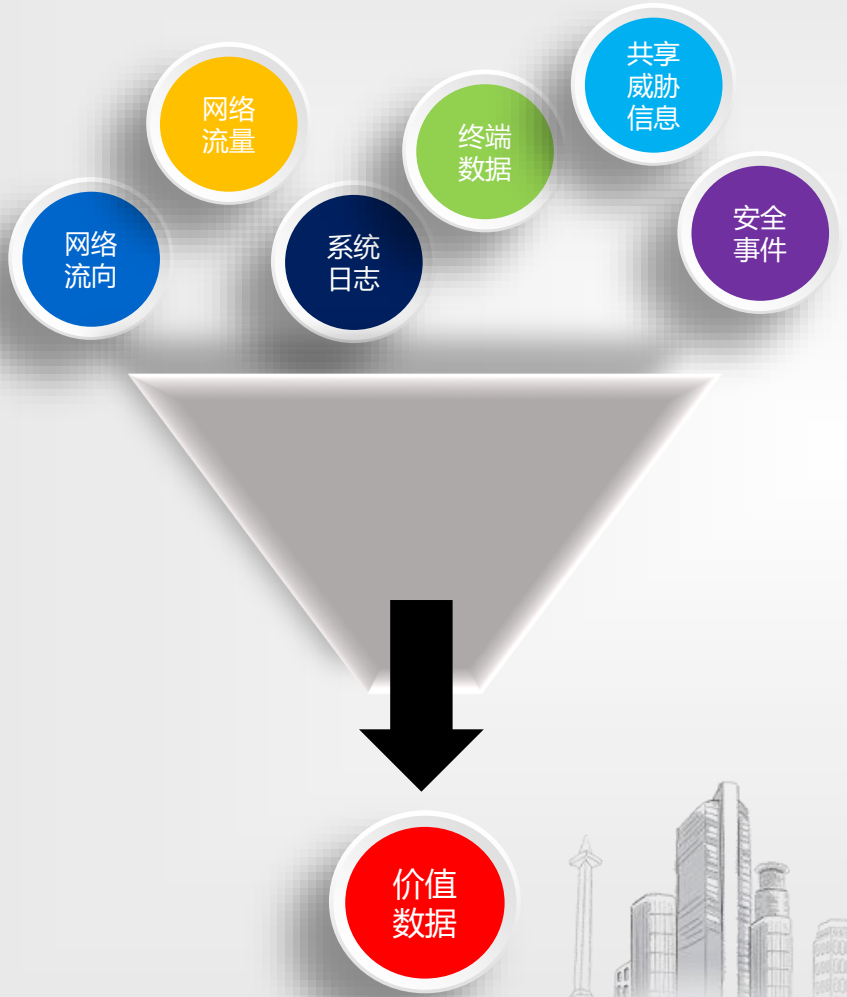
ansion
安 | 信 | 与 | 诚 |

迎战阶段的蓝队

重要的活动

- 监测和预警
- 分析和验证
- 应急处置
- 反制技术

监测和预警



重要的关注点：

监测机制的持续有效

演练期间的0day或者源代码泄露事件

防守方的信息共享机制

高危动作的合理性

东西向信息数据的合理性

难点：

过载信息的研判-利用工具、专家判断

分析和验证

分析和验证的目的：

进一步筛选，确认攻击阶段，确认攻击的有效性，为对症下药作依据

可参考工具：ATT&CK

能力要求：快速、准确

重要角色：决策者、传令兵

关键点：

区分人机、过滤扰敌行为

识别真实恶意攻击

应急处置

快捷遏制操作：

ACL访问控制、关闭服务、断网

取证、溯源：

攻击路线：通信分析、路径追踪等

攻击方法：安全设备日志分析、漏洞审查、恶意代码审查等

接续措施：

漏洞修复、策略优化、同类问题处理

总结上报：

给谁报、什么时候报、报什么信息

报告证据的原则：

可接受

可靠

完整

正确无误

有说服力

反制技术

- 利用蜜罐技术
- 利用社会工程学
- 攻击工具的漏洞
- 日志分析溯源目标位置

ansion
安 | 信 | 与 | 诚

战后阶段的蓝队

重要的活动

- 复盘总结
- 人才培养
- 策略优化

复盘总结

我觉得“复盘”本身其实很简单，一个事情完了，你只要有意识，然后把事情当初定的目标和现在做的情况做对比，是不是按照预定情况出现的，哪些地方没有，为什么没有，无非就是这么做。“复盘”的方式有多种多样，关键是要有这个意识，有了这个意识以后情况就会好得多。

------柳传志 2005年12月25日

复盘总结四步：

回顾、对比、分析、总结

复盘总结的关键：

避免出现同样或者同类的问题

找到问题的根本原因

基于事实的讨论

集思广益、接受或阐述不同的意见

人才培养

完善人才管理的机制：

明确目标、奖惩制度、优胜劣汰

人才特点的挖掘：

技术好、意识强、沟通良好

人才培养的方法：

传：提供安全技能、意识的培训和考试

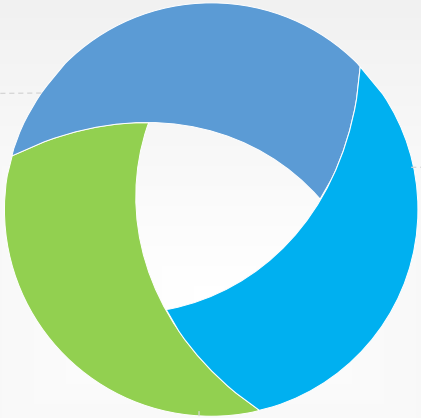
帮：能力强帮助能力弱的人对安全问题进行解答

带：能力强带着能力弱的人参与安全工作

策略优化

安全技术

缺什么补什么
不要拆东墙补西墙
定期优化策略
验证策略有效性



安全管理

岗位职责是否清晰
管理章程是否合理
管理制度是否缺失

安全运营

流程是否有缺陷
协作能力的提高
适应能力的提高

ansion
安 | 信 | 与 | 诚

攻防演练的意义

攻防演练的意义

- 应急响应能力得到了检验和提高
- 人才实战能力得到了培养和提升
- 网络安全风险意识得到了有效强化

ansion
安 | 信 | 与 | 诚 |

安信与诚，感恩有你！