



# 实战背景下的安全体系与核心能力建设

姓名：顾鑫

职位：奇安信集团安全服务子公司

## 目录

实战攻防演习的演进

当攻防演习从短期转化为长期应如何应对

实战背景下的核心能力建设



## 变化的战场



## 变化的目标



## 变化的对手



## 变化的武器与战术



## 变化的指挥监管

信息安全技术  
网络安全等级保护基本要求  
Information security technology —  
Baseline for classified protection of cybersecurity

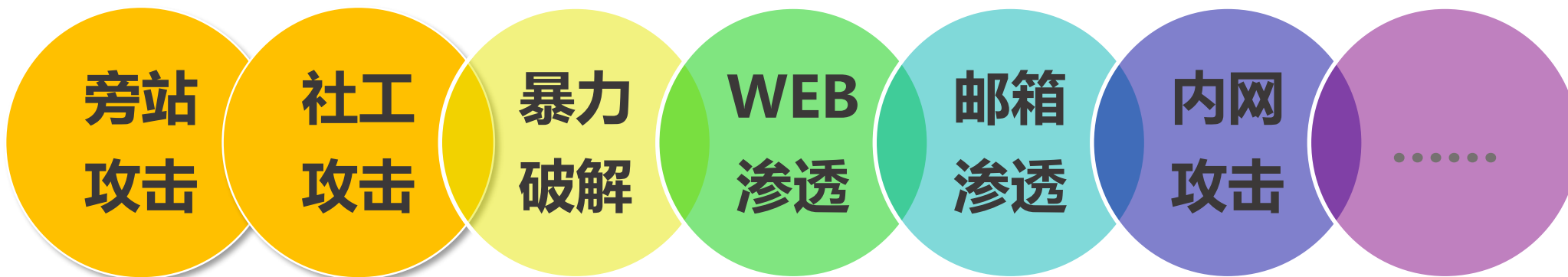


国家战略  
法律法规  
实战演练

**保障业务系统安全的前提**

**明确目标系统，不限制攻击路径，**

**以提权、控制业务、获取数据为最终目的**



# 攻防演习与渗透测试、风险评估的区别

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE

## 渗透测试

渗透测试人员

应用系统安全

## 安全风险评估

风险评估人员

主机安全

网络设备  
及集权类  
设备安全

内网环境  
安全

攻击队

应用侧人员

+

内网后渗透人员

+

反编译人员

+

社工人员

系统  
边界、  
应用  
安全

主机  
安全

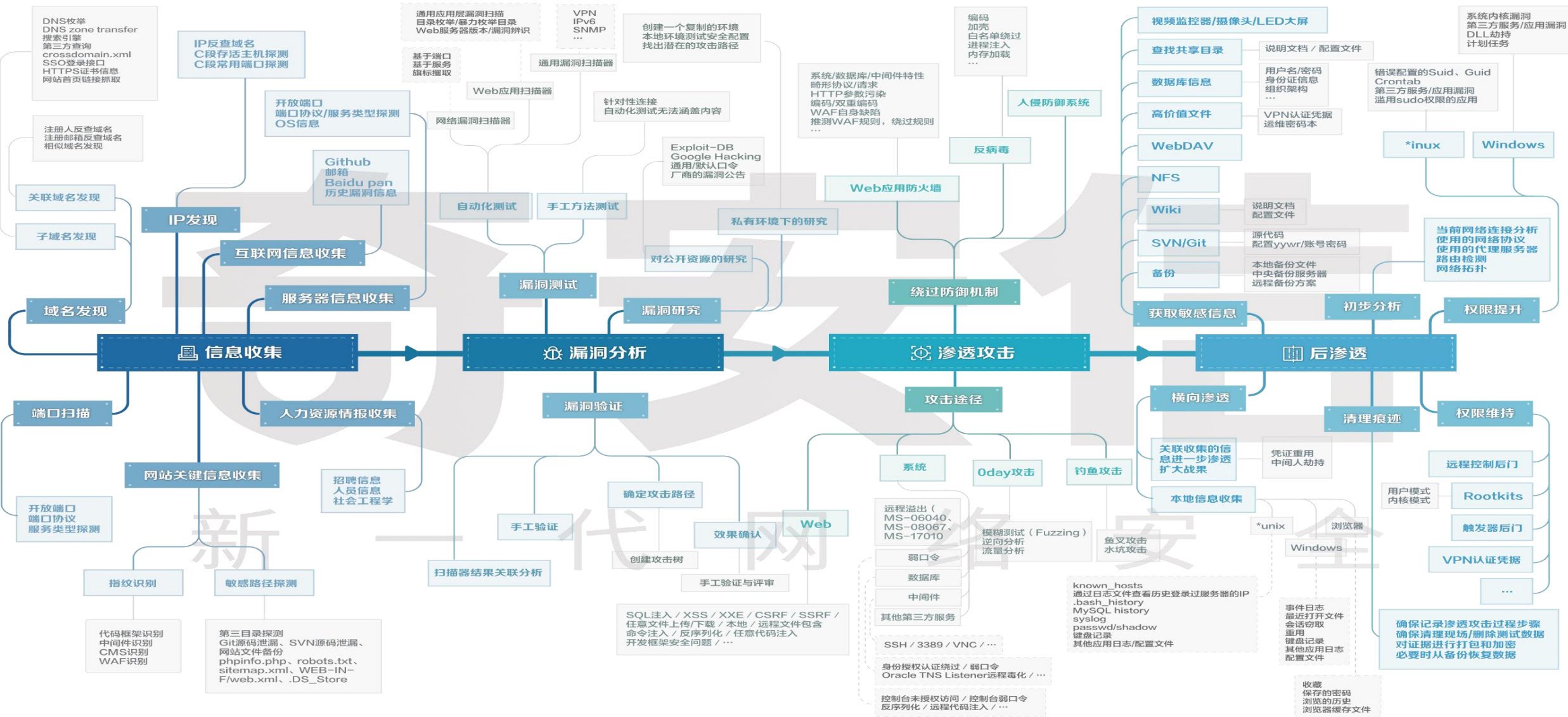
网络  
设备、  
集权  
设备、  
安全  
设备

生产  
网环  
境安  
全

控制核心业务  
获取核心数据



### — 实战攻防演习攻击线路图 —



	2016年	2017年	2018年	2019年
阶 段	<b>试点阶段</b> 认可度低，不了解，担心出问题。	<b>拓展阶段</b> 监管利器，被监管单位认知不足。	<b>头部客户认可阶段</b> 头部客户快速接受并认可，部分行业开始组织实战攻防演习。	<b>普及阶段</b> 信息化依托性大的机构，普遍尝试实战攻防演习。
典 型 攻 击 模 式	1. 互联网突破； 2. 旁站攻击； 3. 传统攻击行为； 4. 物理设备攻击； 5. 利用大型内网做跨区域攻击； 6. ....	1. 互联网突破； 2. 旁站攻击； 3. 传统攻击行为； 4. 物理设备攻击； 5. 利用大型内网做跨区域攻击； 6. 集权类设备攻击； 7. 0day； 8. ....	1. 互联网突破； 2. 旁站攻击； 3. 传统攻击行为； 4. 物理设备攻击； 5. 利用大型内网做跨区域攻击； 6. 集权类设备攻击； 7. 0day； 8. 供应链攻击； 9. 邮箱系统攻击（获取信息）； 10. 免杀、加密隧道等隐性攻击出现； 11. ....	4. 物理设备攻击； 5. 利用大型内网做跨区域攻击； 6. 集权类设备攻击； 7. 0day+1day； 8. 供应链攻击； 9. 邮箱系统攻击（获取信息）； 10. 免杀、加密隧道等隐性攻击出现； 11. 钓鱼、水坑，利用“人”的弱点； 12. 目标单位周边WIFI攻击； 13. 业务链接单位攻击； 14. ....
标 志	战场范围不仅局限于互联网边界，也涉猎于智能终端类的网络边界设备，打破传统安服模式。	攻击行为“组织化”状态明显，集权类设备是攻击队宝藏；防守不够严密，监测能力不足是较大短板。	防守方认知逐渐清晰，部分参与过的单位能力大幅提升，攻击队难度加大，开始尝试“更隐蔽”的攻击方式。	行业现象明显，能力强弱两级分化；传统攻击很难取得成效，钓鱼、水坑、供应链等攻击普遍；防守“应试性”显现，游戏规则出现了局限性。

## 实战攻防演习的目标：

模拟真实攻击行为，检验单位核心业务系统的实际安全防御能力。

## 实战攻防演习的周期：

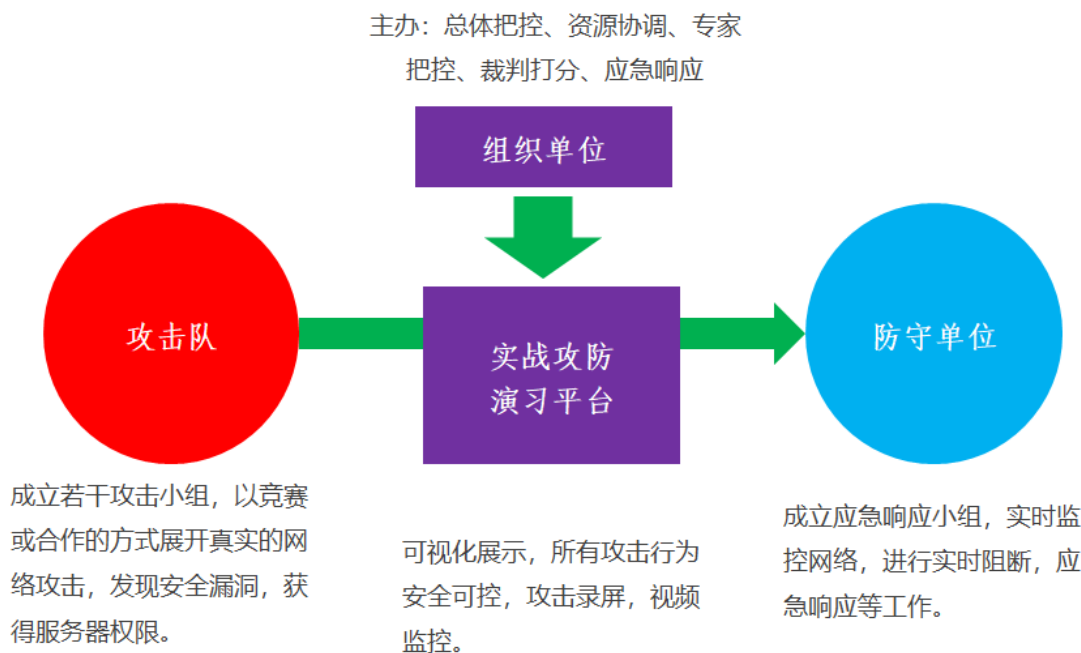
一般为1-3周

## 攻击队（红方）：

一支或多支攻击队做集中攻击

## 防守队（蓝方）：

安排重兵做针对性防守





## 在高压对抗情景下，容易产生极端型防守策略！

- 1、非重要业务系统全部下线；
  - 2、疯狂封IP，宁可错杀1000，不能放过1个；
  - 3、核心业务建立白名单机制，仅保留最核心的功能；
  - 4、应付监管，仅上报边缘业务系统；
  - 5、目标系统阶段性下线；
- .....

## 带来的问题：

- 1、过于应对，会变成“应试化教育”，违背了实战化演习的初衷；
- 2、脱离了真实的安全运营状态；
- 3、过分应对导致阶段性影响业务运营。

## 目录

实战攻防演习的演进

当攻防演习从短期转化为长期应如何应对

实战背景下的核心能力建设



## 如果模拟更真实的攻击：

演习周期由一周调整为三个月；

攻击时间由集中攻击变化为不预先通知；

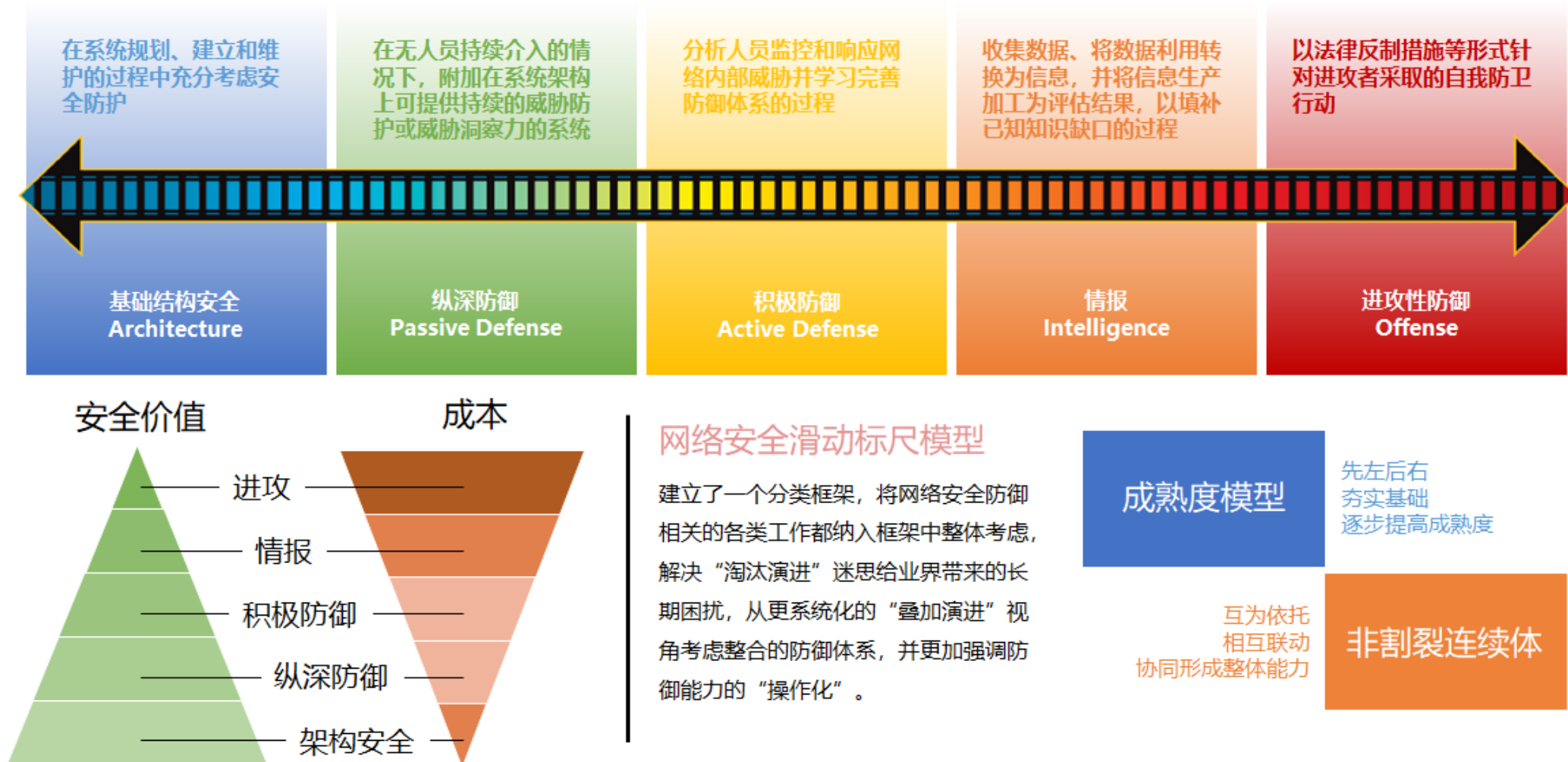
## 在高压对抗情景下的极端型防守策略将失效：

- 1、非重要业务系统全部下线；✕
- 2、疯狂封IP，宁可错杀1000，不能放过1个；✕
- 3、核心业务建立白名单机制，仅保留最核心的功能；✕
- 4、应付监管，仅上报边缘业务系统；✕
- 5、目标系统阶段性下线；✕

.....

*我们应该如何应对？*

## 通过网络安全滑动标尺，审视安全体系的有效性





# 实战化方式审视安全体系的有效性

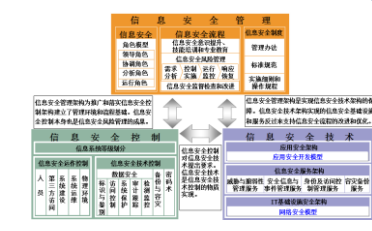
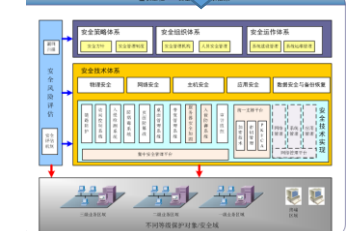
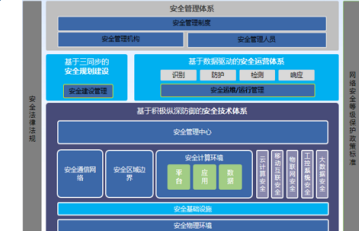
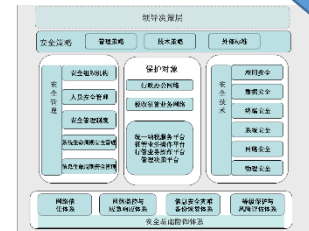
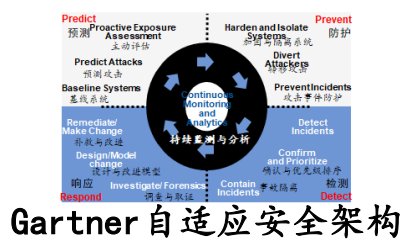
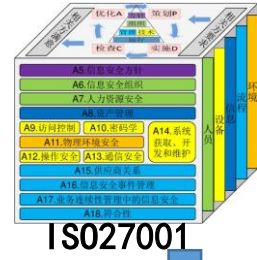
有效的安全运营体系是应对实战化攻击的基石；  
有必要采用网络安全滑动标尺模型，审视实际抗攻击能力，以便持续升级、优化安全运营体系。

政策标准

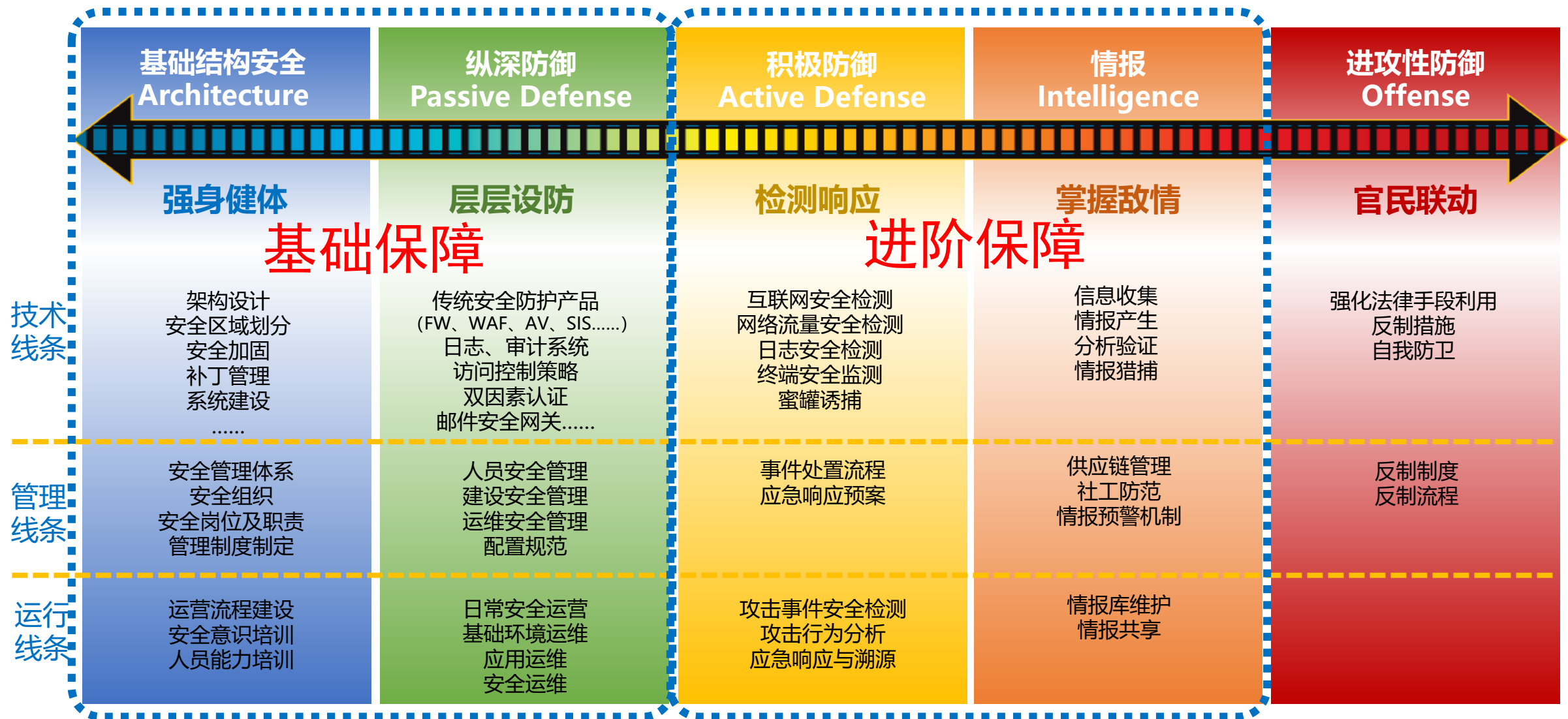
最佳实践

安全体系

滑动标尺



核心能力进阶：“积极防御”能力的充分运用。



## 目录

实战攻防演习的演进

当攻防演习从短期转化为长期应如何应对

实战背景下的核心能力建设



- 有效的安全运营体系是应对实战化攻击的基石
- 在基石的基础上，需关注以下关键节点：

1、**防微杜渐**

防范被踩点

2、**收缩战线**

收敛攻击面

3、**纵深防御**

立体防渗透

4、**守护核心**

找到关键点

5、**洞若观火**

全方位监控

滑动标尺



## 攻

**目标：**情报收集

**代表性攻击行为：**

- 互联网资产暴露
- 业务信息获取（公共信息平台等）
- 系统信息收集（供应链、源代码等）
- 人力资源情报收集（招聘、通讯录等）
- 钓鱼、水坑（目标预制）
- .....

## 防

**目标：**减少情报泄露

**核心防护动作：**

- 定期互联网资产扫描，台账清晰、风险可控；
- 核心文档严格管控，信息披露平台定期检测（DLP）；
- 供应链严格管理与审查；
- 内部人员及开发商纳入统一管理；
- 定期、多样的安全意识教育；
- 邮件安全；

.....

### 攻

**目标：**找到边界弱点，尝试突破边界

**代表性攻击行为：**

- 互联网类业务侧突破；
- 暴露服务器突破；
- 测试环境突破；
- 中间件、业务管理后台突破；
- 供应链突破；
- WIFI、VPN等隐蔽入口突破；
- 个人终端突破；
- .....

### 防

**目标：**让攻击面缩小到最小，缩小防守半径

**核心防护动作：**

- 定期梳理网络边界（尤其是全国联网的单位）；
- 互联网资产发现与清理；
- 测试环境管控（本地与开发商）；
- 供应链管控；
- 中间件、业务管理后台管控；
- WIFI、VPN等入口管控；
- 安全意识、防钓鱼、终端安全、权限管理；
- .....



## 攻

**目标：**深入敌后，寻求价值目标

**代表性攻击行为：**

- 主机、服务器攻击；
- 弱口令、口令同质化利用；
- 系统漏洞利用；
- 内网横向跨网段突破；
- 域控攻击；
- 内部应用攻击；
- .....

## 防

**目标：**避免“押宝式”防护，层层设防，全路径管控

**核心防护动作：**

- 日常主机安全管理（资产管理、补丁管理、口令管理）；
- 安全区域划分与区域间安全管控；
- 核心网段建立白名单机制的访问控制策略；
- 服务器加固（服务+产品）；
- 应用系统安全管理（尤其是内部工作支撑类应用，经常被人遗忘）
- .....

## 攻

**目标：**打击关键点，获取最大收益

**代表性攻击方式：**

- 攻击集权类系统
  - 域控、DNS服务器、运维管理系统、Zabbix、Nagios、堡垒机、VPN、研发个人终端、运维个人终端、领导终端.....
- 攻击重要信息来源
  - 邮件服务器、备份服务器、研发服务器、SVN、Git.....
- 攻击目标系统
- .....

## 防

**目标：**“集权类”系统、“目标”系统的管控

**核心防护动作：**

- 版本及补丁管理
- 核心资产权限最小化管理
- 核心资产白名单机制
- 访问行为分析
- 日志管理与审计
- .....

# 五、洞若观火：全方位监控

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE

在已有安全架构的基础上，通过全流量实时安全分析，全面发现真实攻击！





# 五、洞若观火：全方位监控

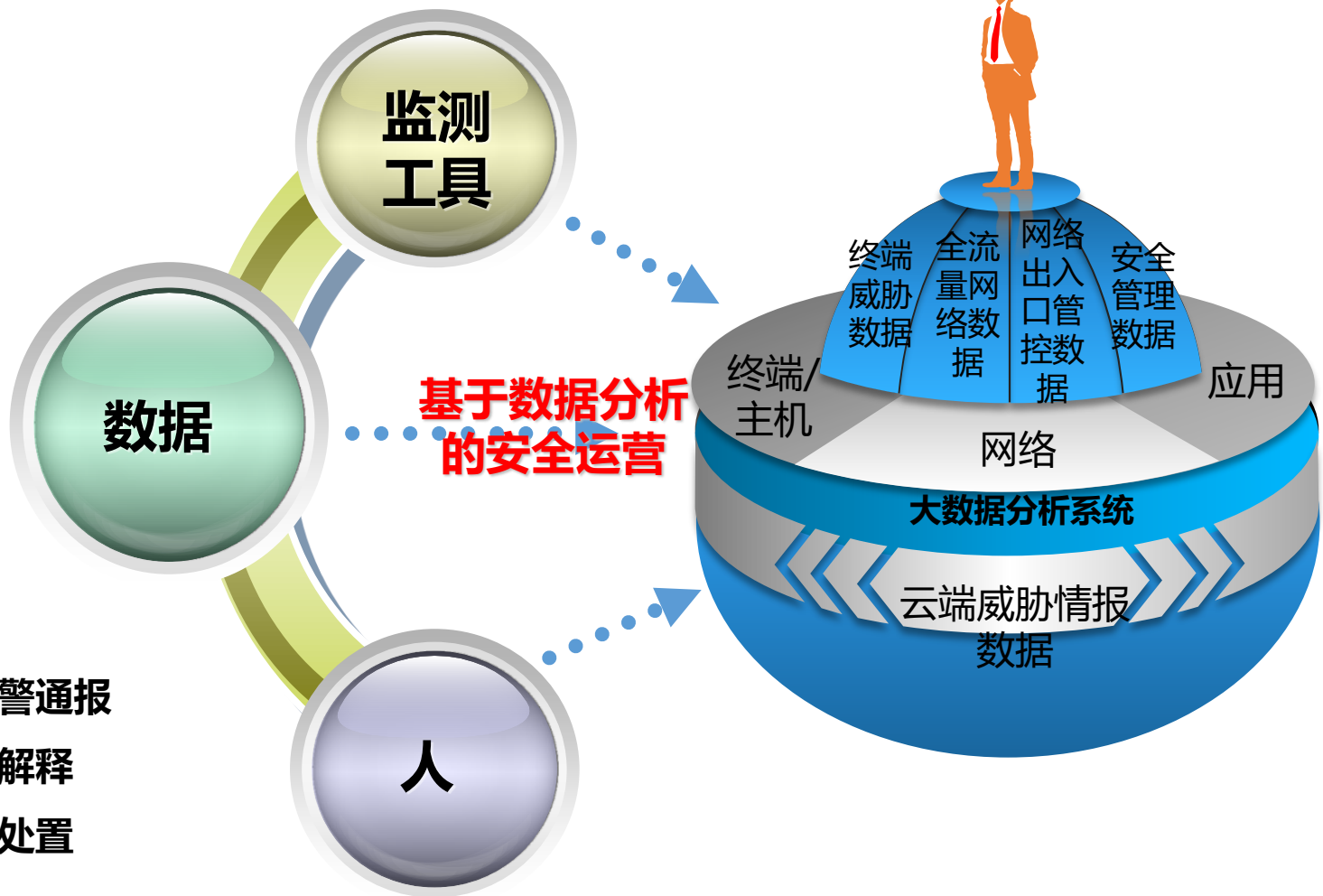
2019 北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE

- 1、基于全流量的威胁检测设备
- 2、蜜罐类设备
- 3、服务器安全检测与防御设备
- 4、邮件威胁检测设备
- 5、日志安全分析工具

- 1、资产情报
- 2、漏洞情报
- 3、威胁情报
- 4、分析样本
- 5、风险趋势

- 1、安全监控岗：实时监控，安全预警通报
- 2、数据分析岗：数据分析、验证和解释
- 3、事件处置岗：各类安全事件技术处置



示例：如何基于全流量开展网络攻击行为分析

1、互联网侧攻击行为分析

网站安全分析

网站业务分析

场景化分析

自助分析

已分析完成

概况

Web攻击信息

疑似 Webshell 后门文件

攻击者 IP 列表

攻击者 IP 威胁情报

导出报告

攻击者 IP 列表

搜索

刷新

列表

下载

攻击者ip	地区	攻击手法	攻击次数
124.205.167.219	中国北京北京	任意文件下载,敏感路径,XSS,扫描器探测,SQL 注入	5329
192.168.0.17		敏感路径,任意文件下载	3338
211.99.227.140	中国北京北京	任意文件下载,敏感路径,SQL 注入,XSS,Struts2 攻击	3105
125.96.160.140	中国北京北京	任意文件下载,敏感路径,Struts2 攻击,SQL 注入,XSS	566
220.181.158.108	中国北京北京	敏感路径	250
119.39.71.173	中国湖南长沙	敏感路径,WebShell,任意文件下载	164
124.126.244.146	中国北京北京	任意文件下载,敏感路径,SQL 注入	149
124.207.115.68	中国北京北京	敏感路径,WebShell	139
124.126.210.181	中国北京北京	敏感路径,WebShell	88
125.96.160.130	中国北京北京	任意文件下载,敏感路径,SQL 注入	77

共 20 条数据

10

条/页

1

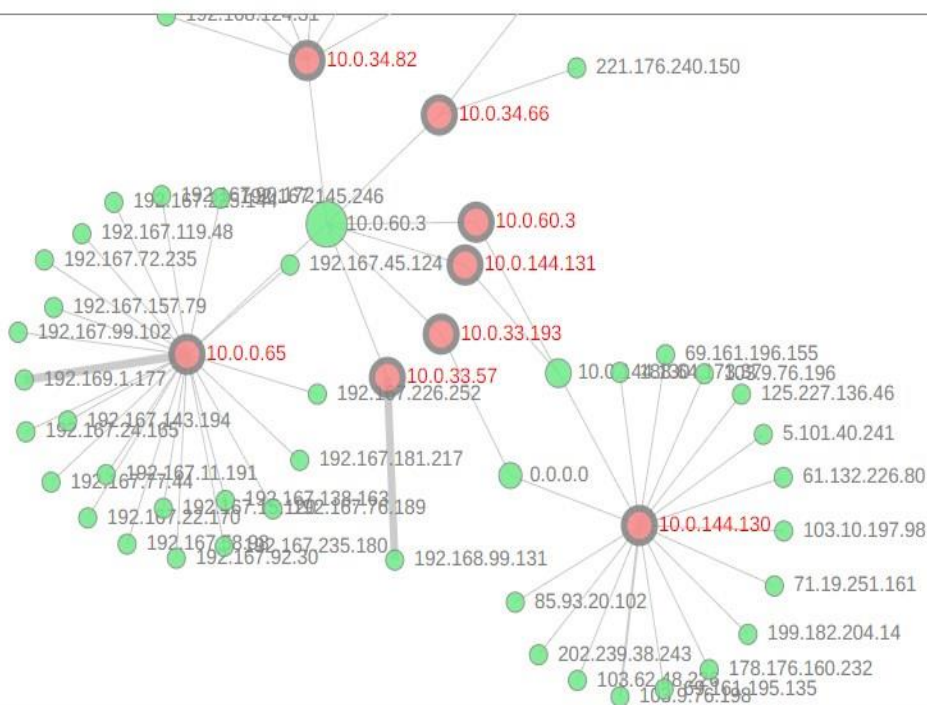
2

# 五、洞若观火：全方位监控

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE

示例：如何基于全流量开展网络攻击行为分析

## 2、内部攻击行为关联分析





# 五、洞若观火：全方位监控

2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE

示例：如何基于全流量开展网络攻击行为分析

3、主机事件关联分析	服务事件时间轴
2018-09-10 03:59:59 主机 :10.0.144.130 系统安装服务 :KProcessHacker3	7045
2019-01-17 19:31:52 主机 :10.0.0.65 系统安装服务 :KProcessHacker3	7045
2019-01-18 00:50:04 主机 :10.0.33.57 系统安装服务 :KProcessHacker3	7045
2019-01-18 00:57:17 主机 :10.0.34.66	7045

## 示例：如何基于全流量开展网络攻击行为分析


### 4、攻击链综合分析



**网络空间已经成为新的战场，  
围绕实战化场景审视网络安全体系已经迫在眉睫！**



**为“实战”在一线的网络安全工作者感动，  
希望网络安全工作者可以在实战化运营体系下，  
更从容的应对“真正”的攻击！**



# THANKS

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE