2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

企业信息安全
一场全员参与的战斗

新东方教育科技集团　杨宁

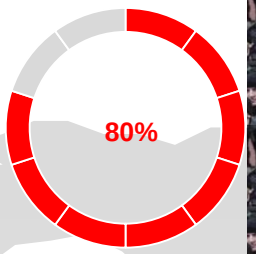
新东方教育科技集团，由1993年11月16日成立的北京新东方学校发展壮大而来，目前集团以语言培训为核心，拥有短期培训系统、基础教育系统、文化传播系统、科技产业系统、咨询服务系统等多个发展平台，是一家集教育培训、教育产品研发、教育服务等于一体的大型综合性教育科技集团。新东方教育科技集团于2006年9月7日在美国纽约证券交易所成功上市，成为中国大陆首家海外上市的教育培训机构。

杨宁：新东方教育科技集团信息安全负责人，19年信息安全从业经验，曾作为研究员及信息安全负责人就职联想研究院、新奥集团、龙湖集团。专注于企业信息安全管理体系和技术能力建设，致力于数字化安全运营。

ISC2信息系统安全专家(CISSP)
ISACA信息系统审计师（CISA）
ISO27001主任审核员
Webmaster网络安全分析师（CIW）
中安国发信息技术研究院安全研究专家

- 企业信息安全——攻防战争
- 信息安全意识——全面普及
- 信息安全责任——落实到人
- 攻防制胜之道——全员参与

企业信息安全—攻防对抗的战争



敌方力量

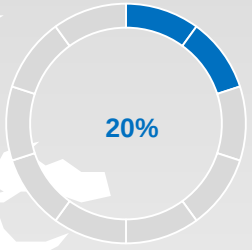
攻击武器
—病毒、蠕虫、木马、后门、DDoS、爆破、撞库、社会工程。。

攻击组织
—国家组织
—ATP/黑客团伙
—竞争对手
—小黑/小白
—内部恶意人员

攻击时间
—7X24X60X60（工具+人）

攻击范围
—任何存在漏洞/弱点的攻击点

VS



我方力量

防御系统
—防火墙、防病毒、NIPS、HIDS、NTA、EDR、DAM、DDM、加解密、SOC、SOAR、AI

防御人员
—通常1-10人团队规模

防御时间
—7*16 （人）7*24（系统）

防御范围
—网络、主机、应用、数据、终端、账号、人。。。需要面面俱到

一次攻防对抗中的血和泪

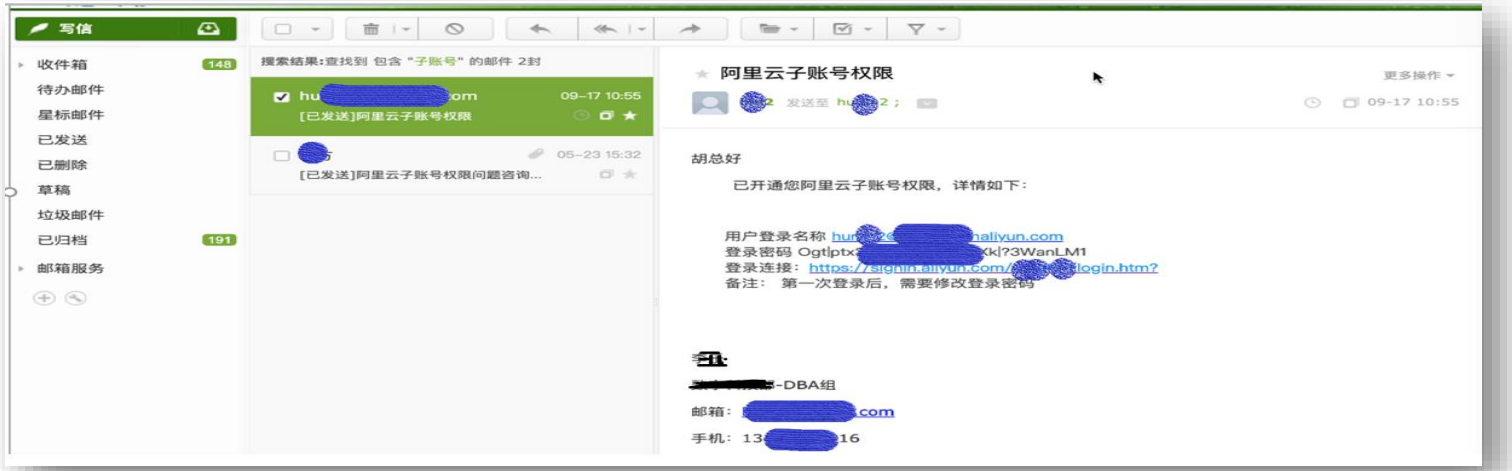
攻击路径1：突破应用系统进入内网，控制云管理平台，获取目标系统控制权。

攻击路径2：突破网络接入设备进入内网，控制域控服务器、堡垒机，获取目标系统控制权。

GitHub/Lab WIKI

```
'db'=>array(
        'connectionString' => 'mysql:host=[redacted]',
        'emulatePrepare' => true,
        'username' => 'li[redacted]',
        'password' => 'li[redacted]',
        'charset' => 'utf8',
),
```

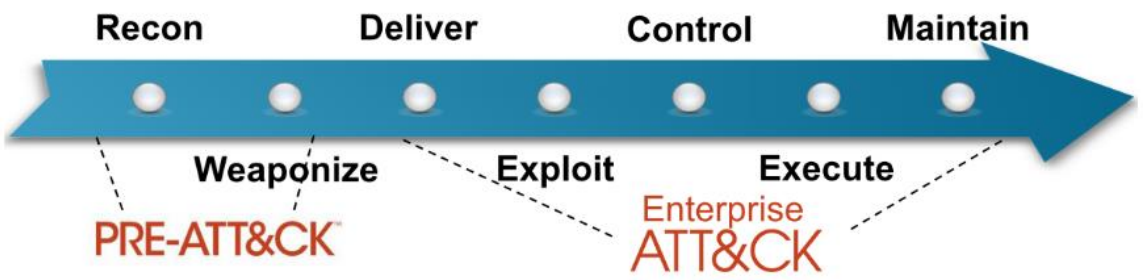
Email



攻防对抗的决定因素——人

在信息安全攻防对抗中，即使你通过狩猎及时发现并切断了攻击链，但一个人为的疏忽可能导致全盘皆输。

毛主席早就说过：“武器是战争的重要因素，但不是决定因素，决定的因素是人不是物。”



Kill Chain 防御

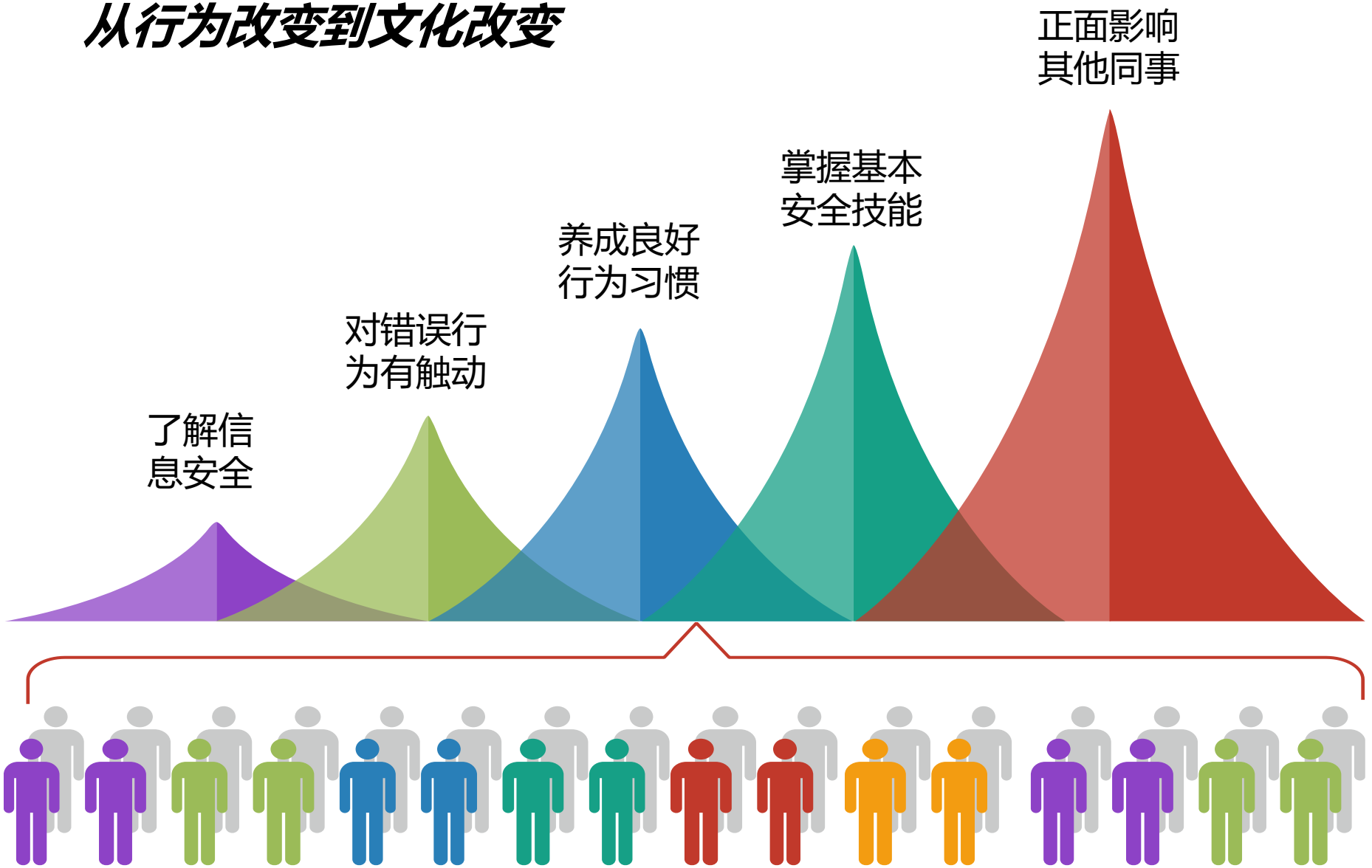
阶段	检测 (Detect)	拒绝 (Deny)	中断 (Disrupt)	降级 (Degrade)	欺骗 (Deceive)	毁坏 (Destroy)
Reconnaissance	Web analytics	ACL				
Weaponization	NIDS	NIPS	In-line AV	Queuing		
Delivery	Vigilant user	Proxy filter	DEP			
Exploitation	HIDS	Patch	AV			
Installation	HIDS	Chroot Jail	NIPS			
C2	HIDS	ACL		Tarpit	DNS redirect	
Action on Objectives	Audit log			Service	Honeypot	

社会工程学—屡试不爽的战术

- **伪装用户或员工**：伪装成一个看门人、雇员或者客户来获取物理访问权限。
- **冒充重要用户**：伪装成贵宾、高层经理或者其他有权使用或进入计算机系统并察看文件的人。
- **冒充第三方**：伪装成拥有权限的第三方服务人员。
- **假装寻求帮助**：向帮助台和技术人员寻求帮助并套取想要的信息。
- **偷窥**：通过偷窥获取登录密码。
- **垃圾箱搜索**：寻找在垃圾箱中记录密码的纸、电脑打印的文件、快递信息等。
- **网络钓鱼**：网站、邮件、电话钓鱼获取登录账号密码等。
- **诱骗点击或安装**：通过具有诱惑力的内容引诱用户去点击或安装木马。

安全意识提升—全员普及

从行为改变到文化改变



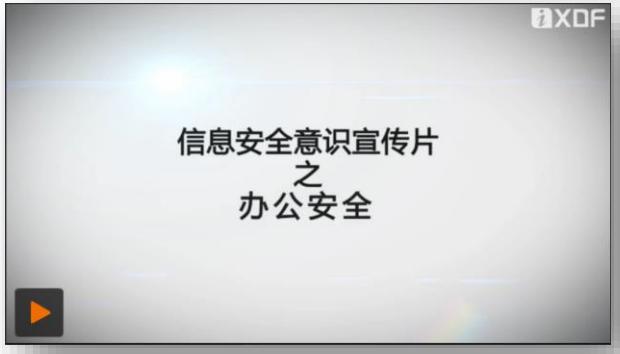
安全意识提升—持续多维度反复灌输

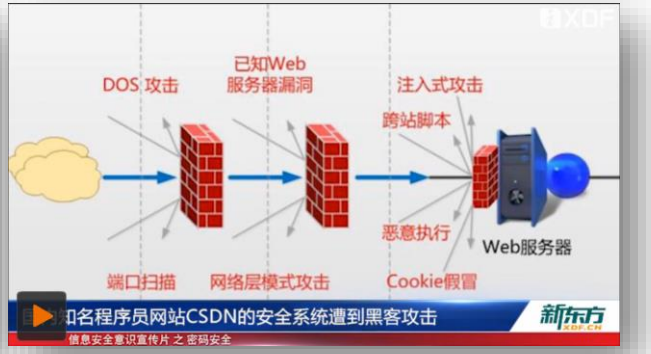
信息安全意识宣传邮件　　信息安全月刊　　信息安全培训课程　　信息安全宣传视频

信息安全意识-电子期刊

信息安全意识-培训课程

信息安全意识-宣传视频





安全意识提升—效果检验

测试通过

试卷1 信息安全意识测评（一） 共计 50 题，满分 100 分，及格分 100 分

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46
47 48 49 50

1. U盘里有重要资料，同事临时借用，如何做更安全？（2分）

- A. 同事关系较好可以借用
- B. 删除文件之后再借
- C. 同事使用U盘的过程中，全程查看
- D. 将U盘中的文件备份到电脑之后，使用杀毒软件提供的"文件粉碎"功能将文件粉碎，然后再借给同事

2. 微信上的好友以"手机刷机后微信登录需要验证"为理由跟你要短信验证码。以下哪项是错误的做法？（2分）

- A. 都是好朋友，应该帮他，直接验证码发给对方
- B. 电话跟朋友联系，提醒他微信是不是被盗了
- C. 验证码这个东西很重要，不能给他
- D. 刷机后登录的验证码是发到他的自己手机上，所以肯定是骗子

3. 在公共场所，如何连接公共wi-fi网络更为安全：（2分）

- A. 保持手机wi-fi功能键开启状态，只要是没有密码的公共wi-fi网络都进行连接
- B. 保持手机wi-fi功能键开启状态，只连接设有密码并提供密码的公共wi-fi网络
- C. 对于任何来自于公共场所的wi-fi网络都不进行连接
- D. 保持手机wi-fi功能键关闭状态，如果进入正规可靠场所的wi-fi网络，则开启手机wi-fi功能，并进行连接

4. 当你在电脑上使用完U盘后，正确移除U盘设备的方法是：（2分）

xdfhr@x-df.com [redacted]

疫情期间员工信息收集表

疫情期间形势严峻，公司为了保障大家上班期间的健康状况，要统计每一个员工的基本信息，请在周一下班前完成链接中个人基本状况的填写，方便公司对疫情进行应急管控和日常工作有序进行。填表地址：http://[redacted]/userinfo/index.html

xdfhr@x-df.com

新东方 XDF.CN

疫情期间员工信息收集表

因疫情期间形势严峻，在这个特殊时段，为保护我们每位员工的健康安全，HR部门会统计各员工的健康状况和基本信息，请在XX日之前完成个人基本状况的填写，方便公司对疫情进行应急管控和日常工作有序进行。

姓名： 邮箱：

电脑IP： 电脑密码：

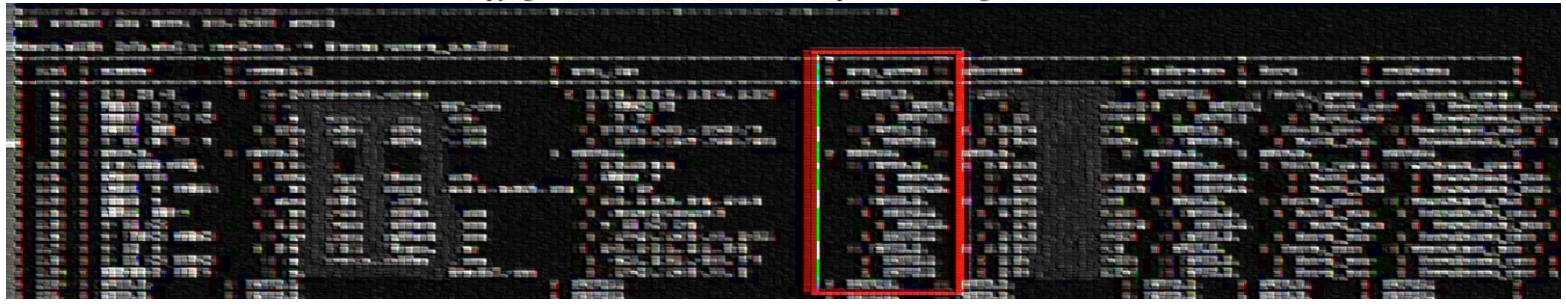
电话： 详细地址：

近期是否发热：是

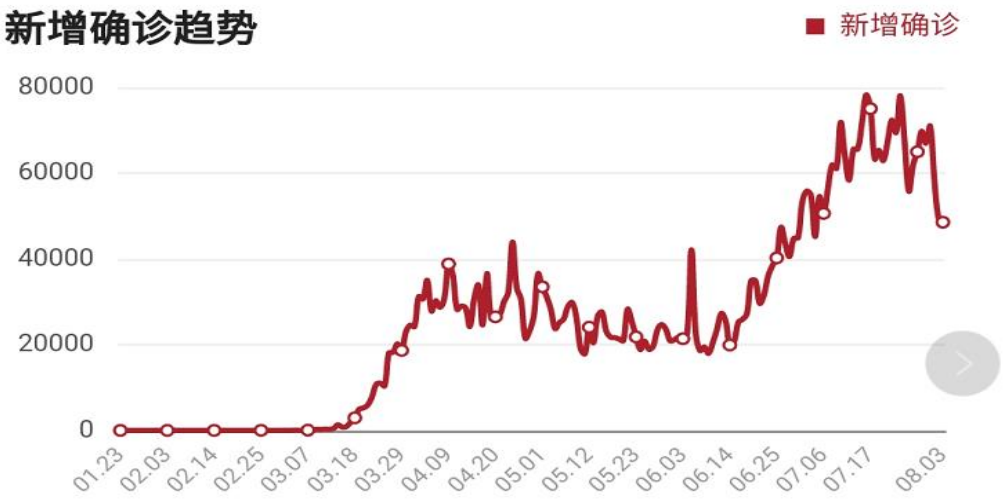
是否接触过武汉相关：是

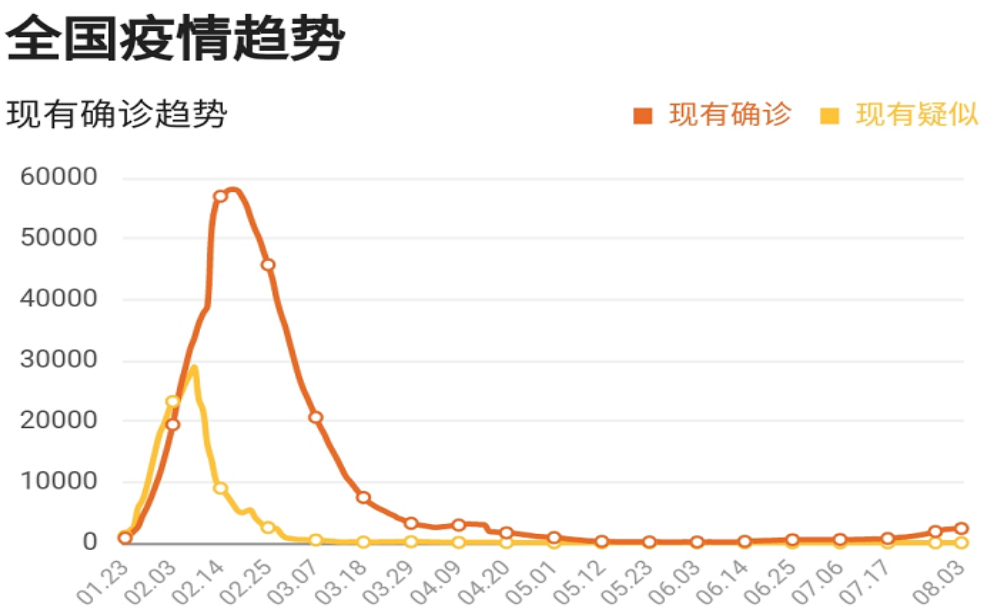
提交查询内容

经营许可证编号：京ICP备05067667号-32 | 京ICP证060601号| 京网文(2016)5762-750号 | 京公网安备11010802021790号



安全责任—驱动因素





国家
法律法规

网络安全法
网络等级保护要求
个人信息保护

。 。 。

企业
管理需求

客户丢失
业绩下降
声誉影响

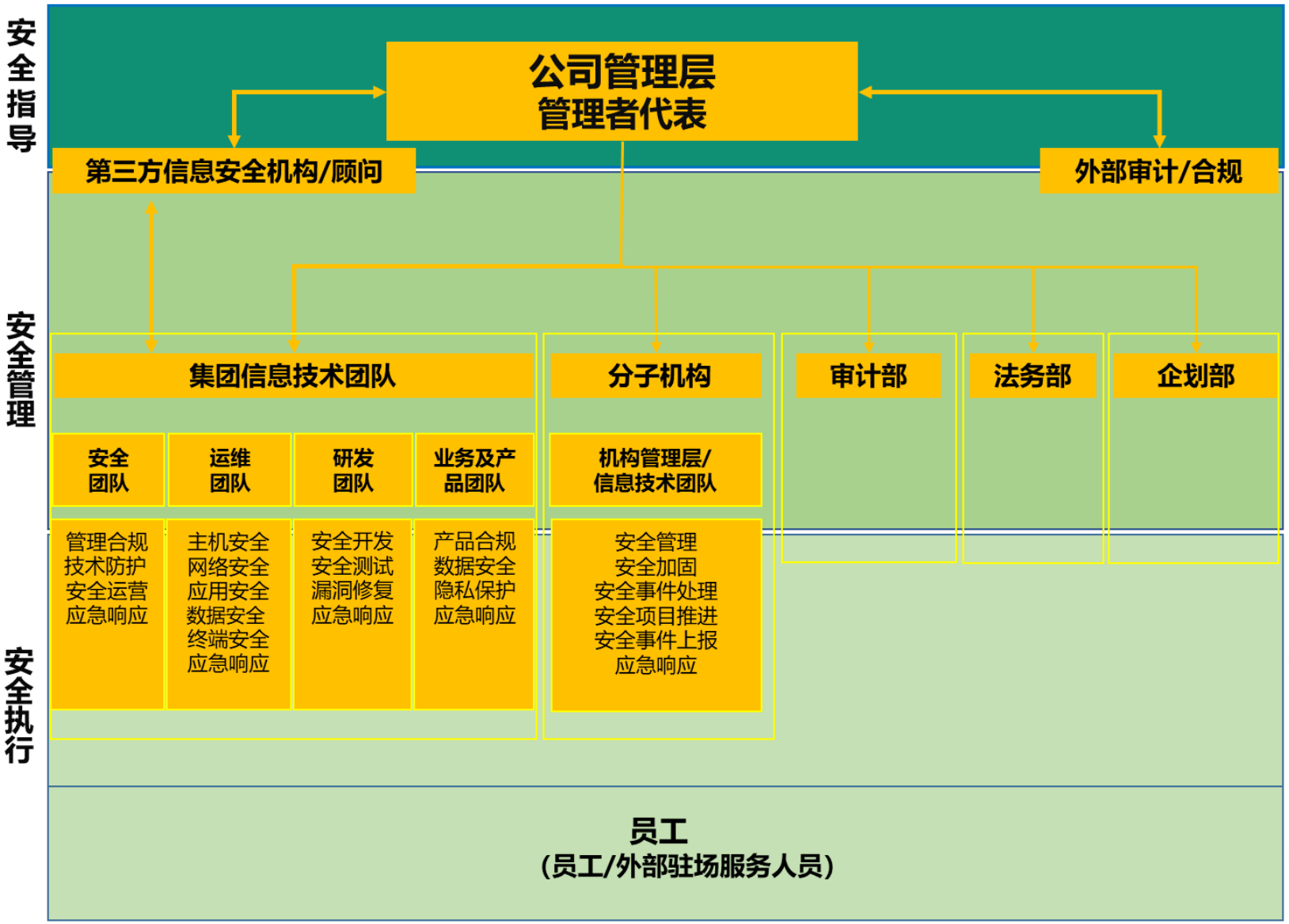
个人
切身利益

网络欺诈
财务损失

职业发展
绩效评价

安全合规	安全事件	安全漏洞	策略执行

安全责任—落实到人



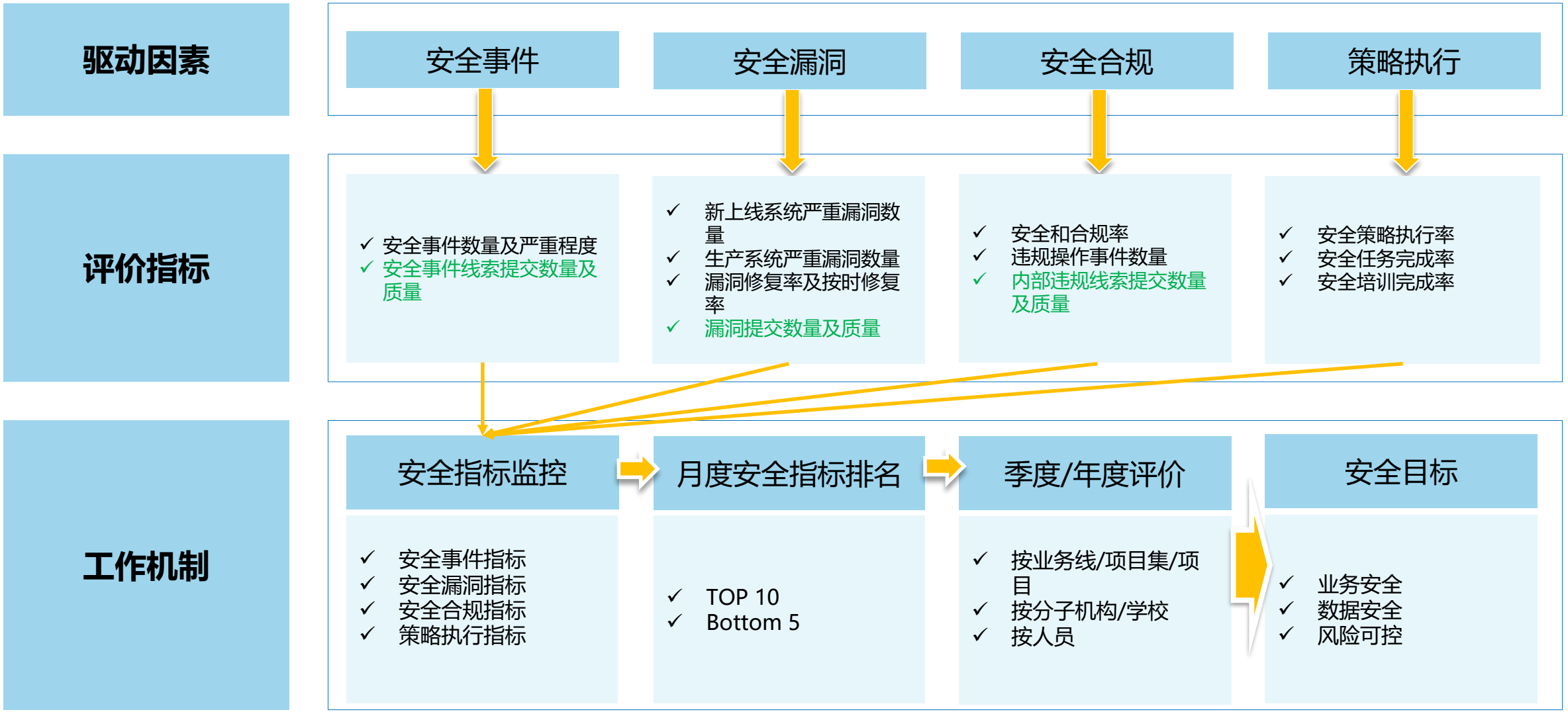
审核：重大安全事件、风险及合规评估结果
决策：信息安全架构、蓝图、风险处置方案
指导：信息安全战略、方针和体系建设
支持：信息安全投入和跨部门资源协调

管理：制定和执行信息安全策略、标准、规范；体系架构及蓝图规划
控制：风险管控和合规遵从
监督：信息安全体系的执行和监督
汇报：重大安全事件、风险、审计结果，及应对措施的整理和汇报

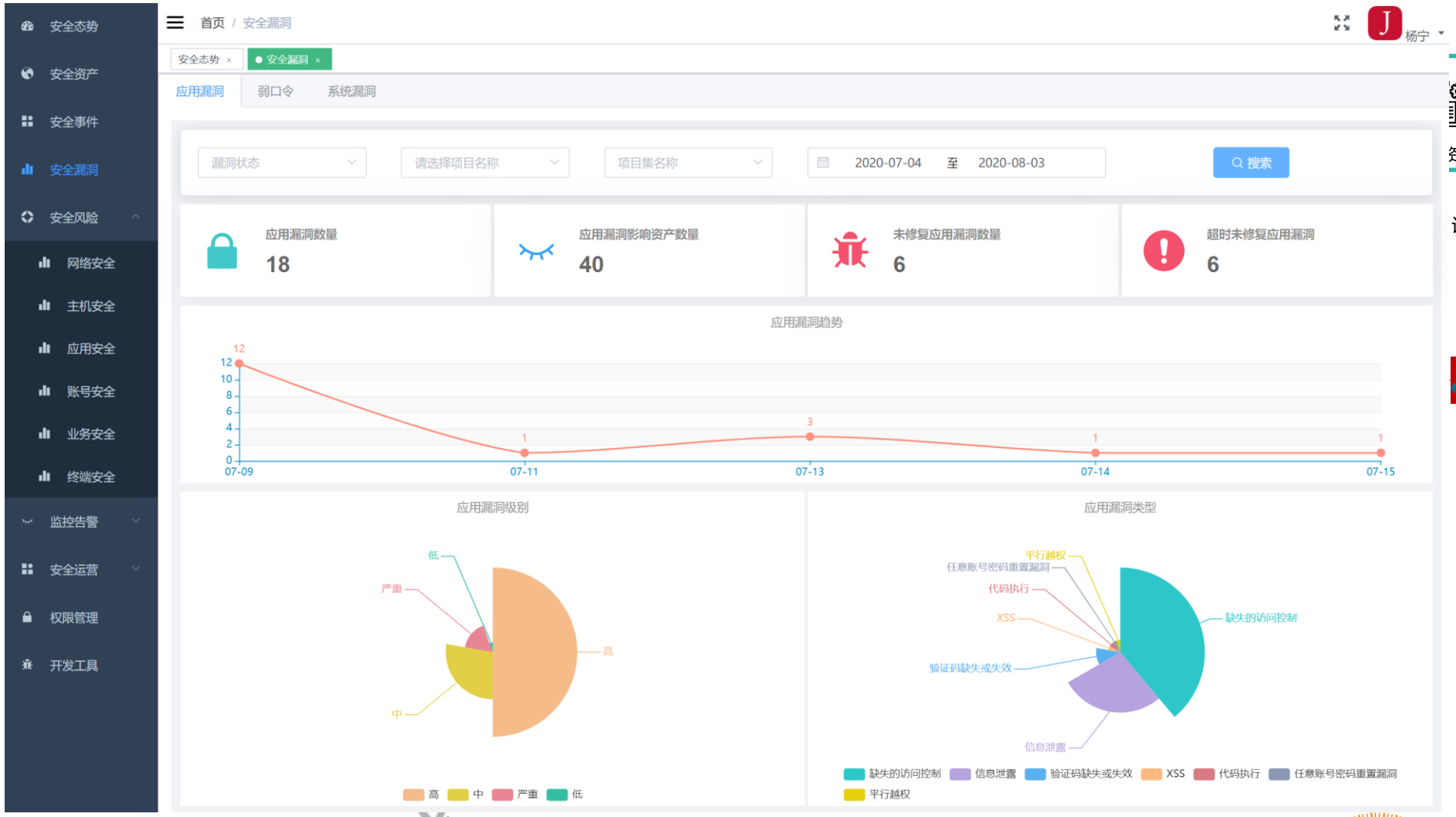
执行：执行信息安全标准、规范
监控：监控信息安全事件和态势
评估：风险评估和风险处置
响应：安全事件的应急响应和处置
上报：汇报安全问题或异常风险

执行：执行信息安全标准、规范
上报：汇报安全问题或异常风险

安全责任—评价机制

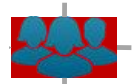

驱动因素
安全事件
安全漏洞
安全合规
策略执行
评价指标
✓ 安全事件数量及严重程度
✓ 安全事件线索提交数量及质量
✓ 新上线系统严重漏洞数量
✓ 生产系统严重漏洞数量
✓ 漏洞修复率及按时修复率
✓ 漏洞提交数量及质量
✓ 安全和合规率
✓ 违规操作事件数量
✓ 内部违规线索提交数量及质量
✓ 安全策略执行率
✓ 安全任务完成率
✓ 安全培训完成率
工作机制
安全指标监控
月度安全指标排名
季度/年度评价
安全目标
✓ 安全事件指标
✓ 安全漏洞指标
✓ 安全合规指标
✓ 策略执行指标
✓ TOP 10
✓ Bottom 5
✓ 按业务线/项目集/项目
✓ 按分子机构/学校
✓ 按人员
✓ 业务安全
✓ 数据安全
✓ 风险可控

安全运营—让每个人都看到风险



调查分析

自动响应



Tier2
安全专家

自动化指令

网络IP封堵
域名请求封堵
应用访问封堵
账号封堵
Hash文件封堵
。。。

安全防护系统

红蓝对抗—让每个人都参与防守

正面攻击

产品团队　研发团队　安全团队　运维团队　业务部门

员工

安全路漫漫。。。其修远。。。


顶峰
SUMMIT
8848 M
HILLARY STEP
希拉里台阶
SOUTH SUMMIT
南顶点
BALCONY
Balcony平台
日内瓦岭
GENEVA SPUR
南坳
SOUTH COL
CAMP 4
C4营地
黄带
YELLOW BAND
CAMP 3
C3营地
BERGSCHRUN
冰后隙
CAMP 2
C2营地
WESTERN CWM
西库姆冰斗

2020北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

THANKS

全球网络安全 倾听北京声音

简历投递：yangning10@xdf.cn