教育系统应急响应最佳实践

姜开达　　上海交通大学

2018 ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018　Beijing · China
（原“中国互联网安全大会”）

目录

- **教育行业安全现状**
- 应急响应体系建设
- 走向安全态势感知

教育行业网络安全特点

	机构	数量级
1	幼儿园	25 万 +
2	小学/教学点	27 万 +
3	中学	7 万 +
4	高等教育	2800 +
5	其他	8000 +

60 万教育机构，**小、散、乱**

各地区经济和安全意识发展不平衡

安全人员和团队普遍缺位

网站 20 万 +， IPV4地址 1300 万 +

学生 3.1 亿 +， 专任教师 1500 万 +

2018 教育信息化和网络安全工作要点

完善教育系统网络安全制度体系

- 健全考核评价和监督问责机制
- 出台教育系统网络安全事件应急预案
- 建立健全教育系统网络安全事件应急工作机制

推进关键信息基础设施保障工作

- 制定教育系统关键信息基础设施认定规则
- 开展关键信息基础设施现场检查检测和安全评估

持续推进教育系统网络安全监测预警

- 健全网络安全威胁通报机制
- 推进教育系统通用软件检测工作
- 建立基于大数据的教育系统网络安全预警机制

教育系统网络安全事件应急预案 发布

教　育　部　文　件

教技〔2018〕8号

教育部关于印发《教育系统网络安全事件应急预案》的通知

各省、自治区、直辖市教育厅（教委），新疆生产建设兵团教育局，部属各高等学校，部内各司局、各直属单位，中国教育和科研计算机网网络中心：

根据《中华人民共和国网络安全法》《国家网络安全事件应急预案》的要求，为健全完善教育系统网络安全事件应急工作机制，提高教育系统网络安全应急处置能力，我部制定了《教育系统网络安全事件应急预案》。现印发给你们，请认真贯彻落实。

教　育　部

2018年6月11日

工作原则：

- 统一指挥、密切协同
- 分级管理、强化责任
- 预防为主、平战结合

坚持事件处置和预防工作相结合，做好事件预防、预判、预警工作，加强应急支撑保障能力和安全态势感知能力建设。

提高网络安全事件快速响应和科学处置能力，抓早抓小，争取早发现、早报告、早控制、早解决，严控网络安全事件风险和影响范围。

网络安全事件应急响应分为Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级分别对应特别重大、重大、较大和一般网络安全事件

教育系统网络安全事件应急预案 之工作保障

- 明确网络安全职能处室，工作责任落实到具体部门、具体岗位和个人，建立健全应急工作机制
- 应明确或建立网络安全技术支撑单位，加强网络安全应急技术支撑队伍建设和网络安全物资保障
- 教育部建立教育系统网络安全专家组，各省级教育行政部门建立本地区的网络安全专家咨询队伍
- 教育部加强教育系统网络安全管理平台建设，建立教育系统网络安全态势感知体系
- 加强与网络安全职能部门、网络安全专业机构、行业学会和教育网网络中心等单位的合作，建立网络安全威胁的信息共享机制和网络安全事件的快速发现和协同处置机制
- 各单位应为网络安全应急工作提供必要的经费保障，利用现有政策和资金渠道
- 各级教育行政部门可对网络安全事件应急管理工作中作出突出贡献的先进集体和个人给予表彰和奖励，对不按照规定执行的对有关责任人给予处分

教育部网络安全保障工作要求

- 加强网络安全工作的组织部署
- 按需调整重要时期网络防护策略
- 加强内部网络的安全防护
- 切实做好监测预警通报工作
- 加强值班值守和信息报送
- 加强重要网络和数据中心的运维保障

如何理解这些具体防护策略?

- 各单位研判信息系统/网站现状，采取有效措施
- 确保安全隐患清零后方可上线，专人专岗24小时值守
- 门户网站和重要服务网站要保障访问通畅
- 限制互联网访问的几个前提

  1.假期期间；

  2.无业务加载，无专人运维；

安全保障工作常态化

2017 不平凡 全国性安全保障 62 天

三月　全国两会

五月　一带一路

六月　高招保障

八月 建军90周年

十九大

- 全国两会
- 改革开放四十周年
- 一带一路五周年
- 高招网络安全保障
- 上合组织峰会
- 中非合作论坛
- 中国国际进口博览会

2018 不太平，安全保障任务压力巨大

目录

- 教育行业安全现状
- **应急响应体系建设**
- 走向安全态势感知

平安校园 + 智慧校园

- 机构保障
- 意识形态
- 网络安全
- 态势感知
- 应急响应
- 安全教育
- 消防安全
- 安全检查
- 督办整改
- 安全值班

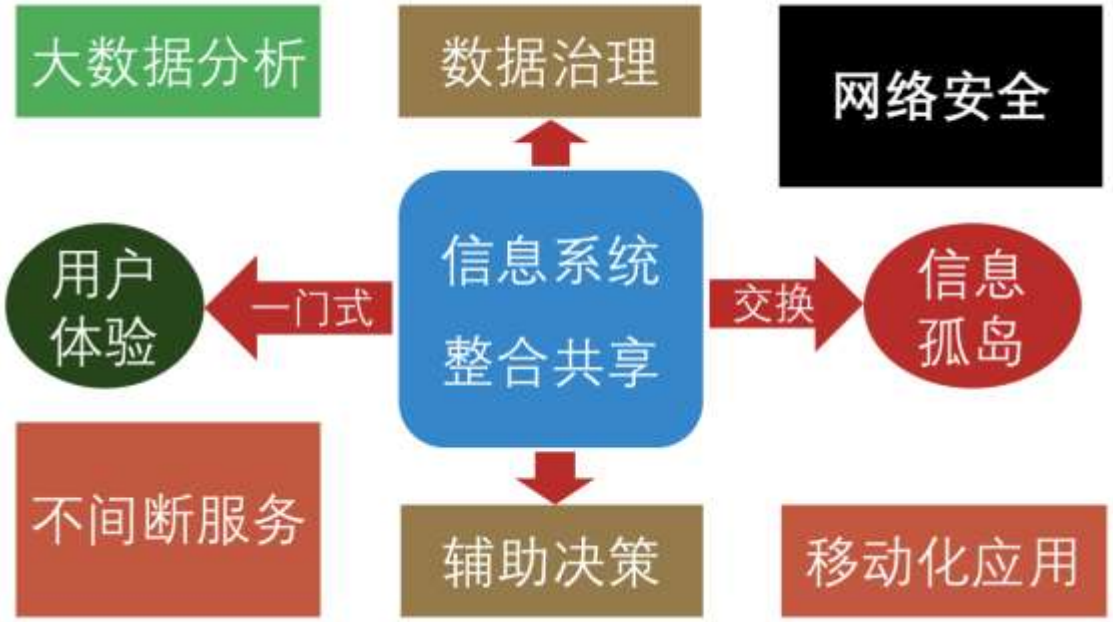
应急预案 / 安全演练

完善和落实安全管理责任制度

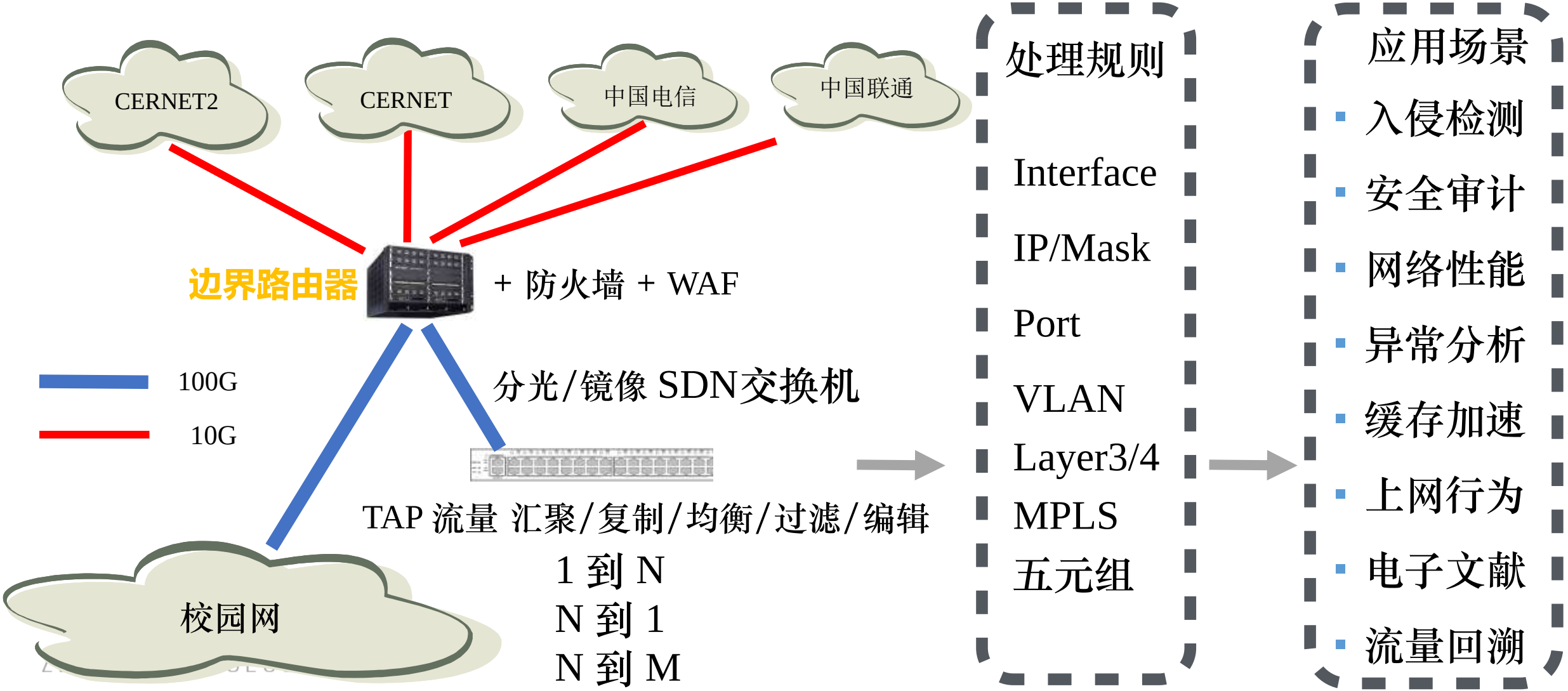
- **制度建设并加强落实**
  建设和完善校级网络信息安全管理制度
  严格落实安全漏洞和事件处置、网站管理相关规定
  对网络安全法相关要求执行情况开展自查和整改

- **网站备案管理和年审**
  校园网出口实施 WEB 服务白名单制度
  推进网站集中化部署（网站群、云平台）

- **加强数据安全管理和控制**
  敏感数据接触人员签署 NDA/保密协议
  开发测试、系统运维、数据分析数据脱敏
  数据库防火墙、运维审计、堡垒机精细化权限管控



校园网边界的网络安全架构



大数据时代的校园网络安全

- 大部分人凡走过必留下痕迹
- 攻击者在大数据下无所遁形
- 设备日志/系统日志/应用日志
- HTTP/DNS/SSL/FLOW 流量日志
- 安全威胁域名/IP 地址黑名单
- 可快速审计、可追踪溯源、可关联场景分析
- 有一定规模的学校，安全大数据平台不可少

初期建设 易 VS 长期运维 难

云计算时代的教育信息化安全

1 高性能

- 10秒钟完成一台任意大小的云主机创建
- 云硬盘实时快照，对一块1T的硬盘进行快照操作，耗时不到 1秒钟
- 万兆校园骨干网络接入

2 高弹性

- 随时按需获取任意数量的云资源
- 按秒计费，按需实时结算
- 云主机/云硬盘支持在线扩容
- 公网IP带宽随时调整

3 高灵活

- 支持Web面板/API/CLI
- 云主机部件如硬盘、网卡、防火墙等随意拆卸和组装
- 虚拟数据中心(VDC)支持完全自主定义网络架构和拓扑

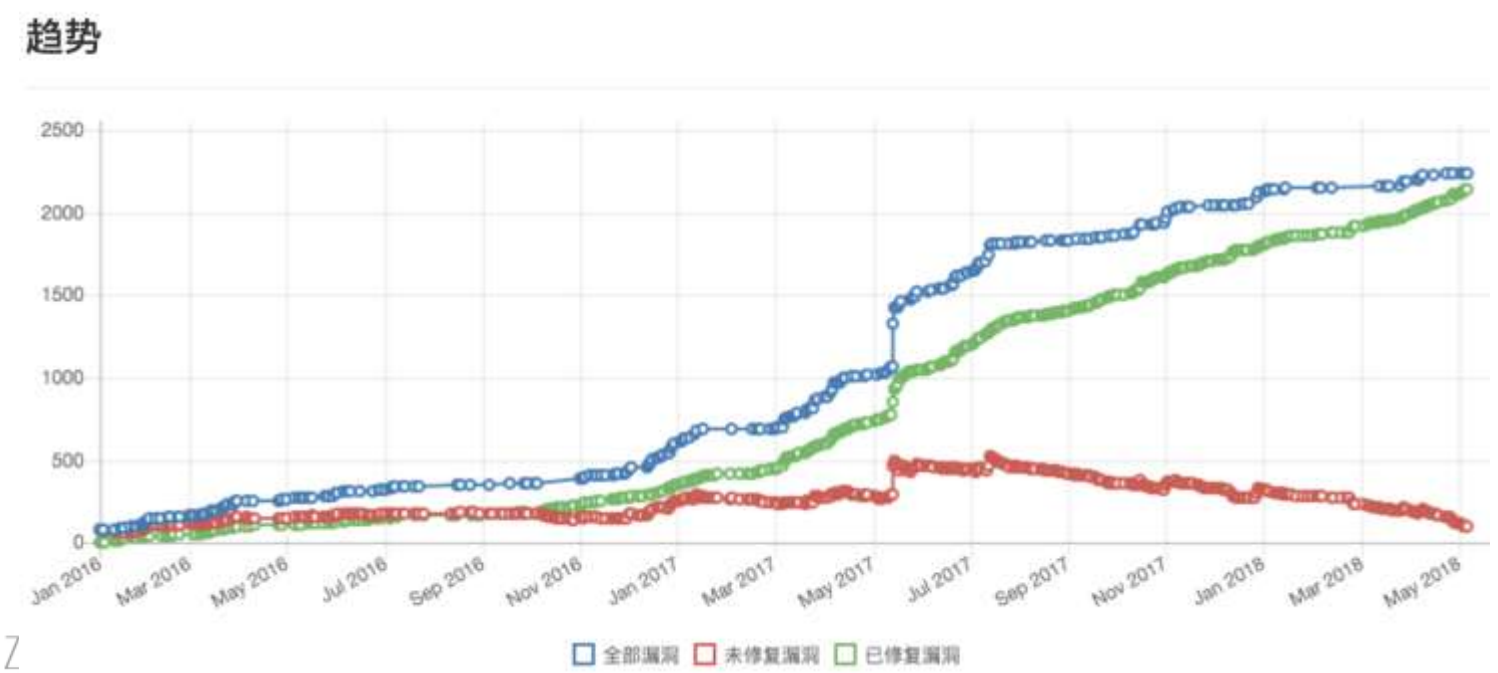
4 高安全

- 采用分布式存储，每份存储都有三副本
- 私有网络互相隔离
- Agent 常驻VM，全局安全集中管控
- 安全扫描，漏洞管理，详尽日志
- WAF，虚拟防火墙，蜜罐，堡垒机

安全扫描和漏洞管理常态化

校园信息资产自动发现、指纹识别、漏扫联动
掌握入网设备存量、全生命周期安全跟踪管理
持续扫描监测，及时发现篡改挂马等安全事件
关注师生隐私泄露，自动发现有害、敏感信息

97%
修复



安全工作是需要并且可以量化的

Vul Tracker 概况 机构 漏洞 地址 关于

机构	注入	上传	入侵	口令	执行	授权	泄露	风险	修复	总数
电子信息与电气工程学院	7 58	12	10	6 113	2 132	2 48	4 33	22	413	435
机械与动力工程学院	2 16	10	2	4 11	2 30	7	3 10	11	89	100
科研院	3 4			2 9	1		4	5	18	23
生物医学工程学院	4									
医学院	8	4	6							
生命科学技术学院	18	5	3							
船舶海洋与建筑工程学院	1 24	1								
材料科学与工程学院	21	1	6							
第一人民医院										
巴黎高科卓越工程师学院										
教务处	5									
物理与天文学院	12	2	1							
后勤保障处	1 6			3	1 6	1	1	2	17	19
先进产业技术研究院			3	1 2	1 1		2	2	8	10
图书馆	30	3	5	12	87	1 13	26	1	183	184

- 安全漏洞管理实现闭环，要越见越少
- 是工作抓手但绝不是安全工作的全部
- 辩证看待数量，并正确评估威胁等级
- 举一反三的智慧，再一再二不能再三

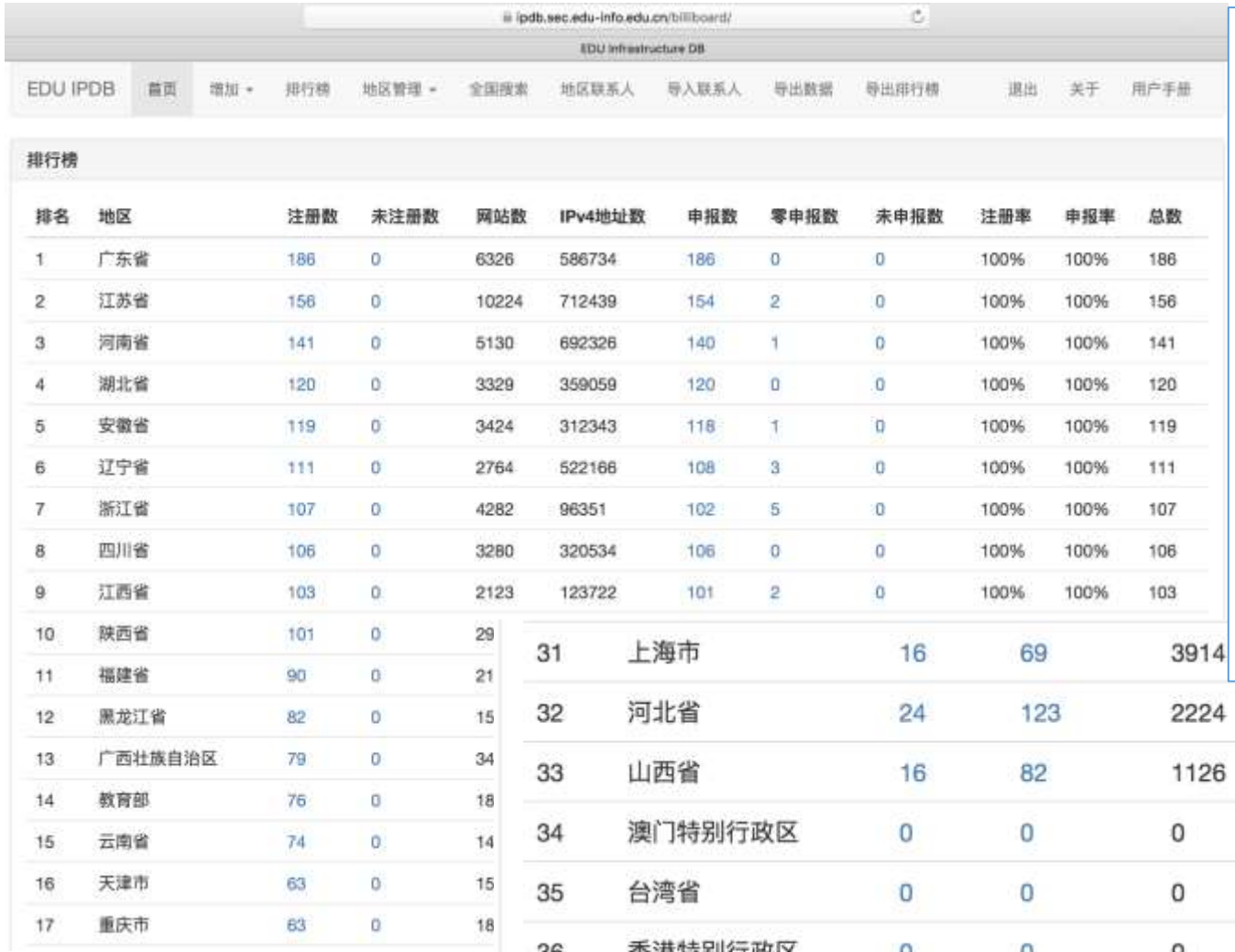
各类日志集中管理分析

适配各种服务软件的认证日志格式
LDAP 看不到客户端 IP 地址、User-Agent
记录失败的登录:用户不存在 / 密码错 / 验证码错

字段	Web SSO	邮件	无线	Eduroam	VPN	FTP	代理
Service	√	√	√	√	√	√	√
Timestamp	√	√	√	√	√	√	√
Address	IP	IP	MAC	MAC	IP	IP	IP
Target	目标网站	协议	SSID				
Software	UA	UA					
Username	√	√	√	√	√	√	√
Status	√	√	√	√	√	√	√
Extra Data			AP, IP				

特征	说明
N_{IP}	账号一天内来源 IP 地址数
N_{CC}	IP 地址所属国家数
N_{Loc}	IP 地址所属地区 (城市) 数
N_{ASN}	IP 地址所属自治系统数
N_{UA}	账号一天内 User-Agent 数
N_{Log}	账号一天内登录次数
N_{Svc}	账号一天内登录服务类别数
U_{Log}	未标记“安全”的登录次数
U_{IP}	未标记“安全”的 IP 地址数
U_{CC}	未标记“安全”的国家数
U_{Loc}	未标记“安全”的地区数
U_{ASN}	未标记“安全”的自治系统数
R_{Log}	标记“风险”的登录次数
R_{IP}	标记“风险”的 IP 地址数
RP_{Log}	标记“风险”的登录比例
RP_{IP}	标记“风险”的 IP 地址比例

高教行业网络信息基础数据库（IPDB）



排行榜

排名	地区	注册数	未注册数	网站数	IPv4地址数	申报数	零申报数	未申报数	注册率	申报率	总数
1	广东省	186	0	6326	586734	186	0	0	100%	100%	186
2	江苏省	156	0	10224	712439	154	2	0	100%	100%	156
3	河南省	141	0	5130	692326	140	1	0	100%	100%	141
4	湖北省	120	0	3329	359059	120	0	0	100%	100%	120
5	安徽省	119	0	3424	312343	118	1	0	100%	100%	119
6	辽宁省	111	0	2764	522166	108	3	0	100%	100%	111
7	浙江省	107	0	4282	96351	102	5	0	100%	100%	107
8	四川省	106	0	3280	320534	106	0	0	100%	100%	106
9	江西省	103	0	2123	123722	101	2	0	100%	100%	103
10	陕西省	101	0	29							
11	福建省	90	0	21							
12	黑龙江省	82	0	15							
13	广西壮族自治区	79	0	34							
14	教育部	76	0	18							
15	云南省	74	0	14							
16	天津市	63	0	15							
17	重庆市	63	0	18							
31	上海市	16	69	3914							
32	河北省	24	123	2224	273159	24	0	123	16%	16%	147
33	山西省	16	82	1126	123016	10	0	88	16%	10%	98
34	澳门特别行政区	0	0	0	0	0	0	0	0%	0%	0
35	台湾省	0	0	0	0	0	0	0	0%	0%	0
36	香港特别行政区	0	0	0	0	0	0	0	0%	0%	0
35	合计	2421	391	99412	12072283	0	0	0	86%		2812

25个省/市 100%全覆盖

成员高校 2421所

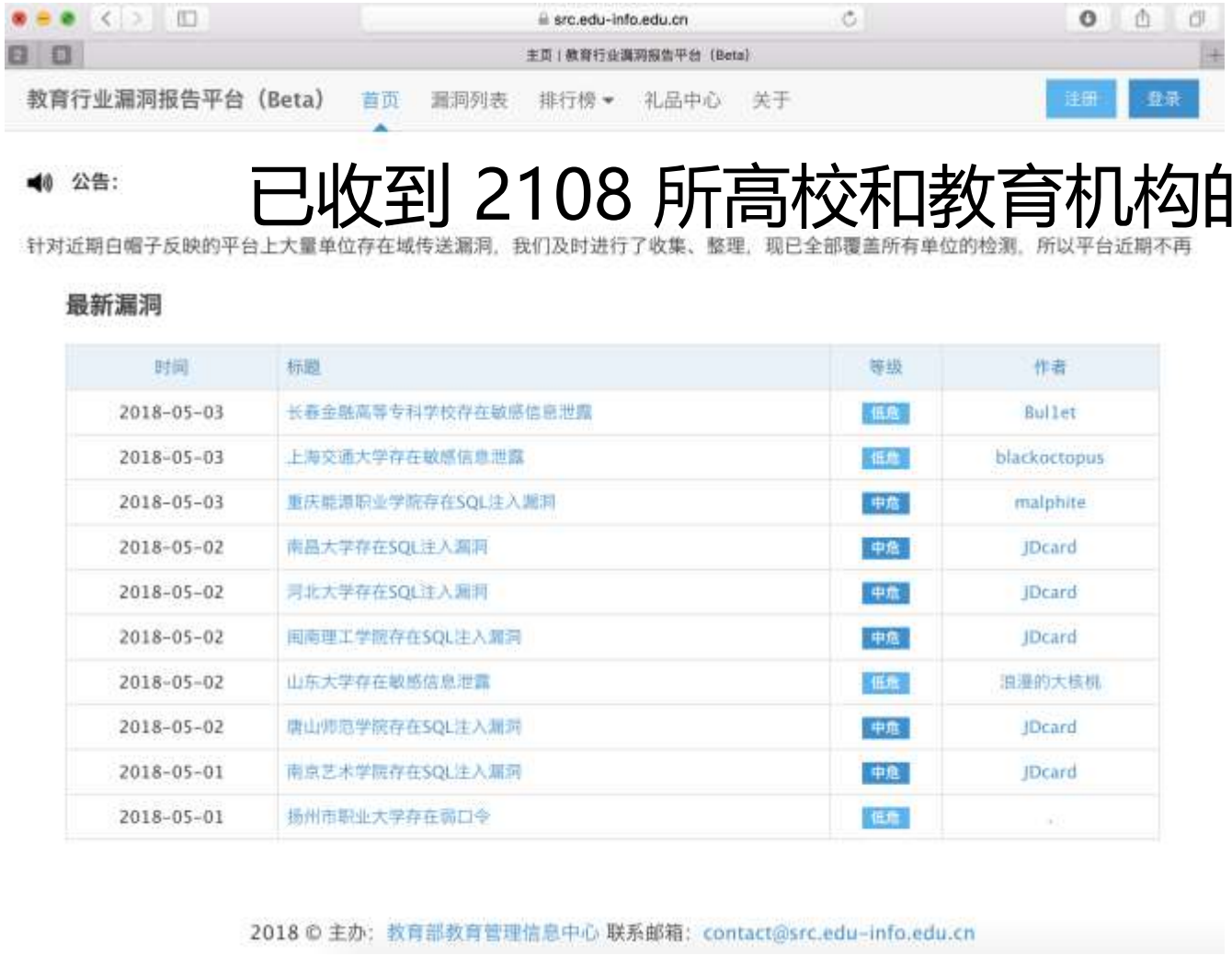
再也不怕找不到人了

基础教育行业基础数据平台

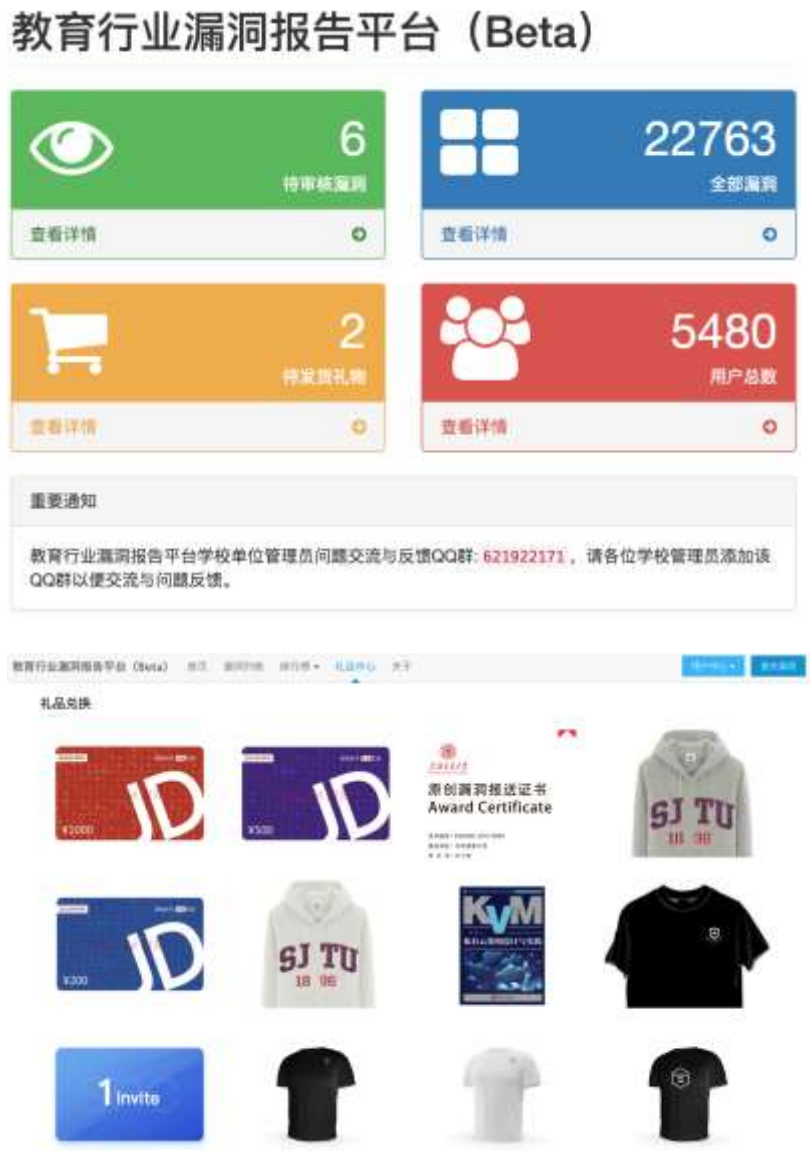
也初步完善

ZERO TRUST SECURITY

教育行业漏洞报告平台



已收到 2108 所高校和教育机构的漏洞



ZERO TRUST SECURITY

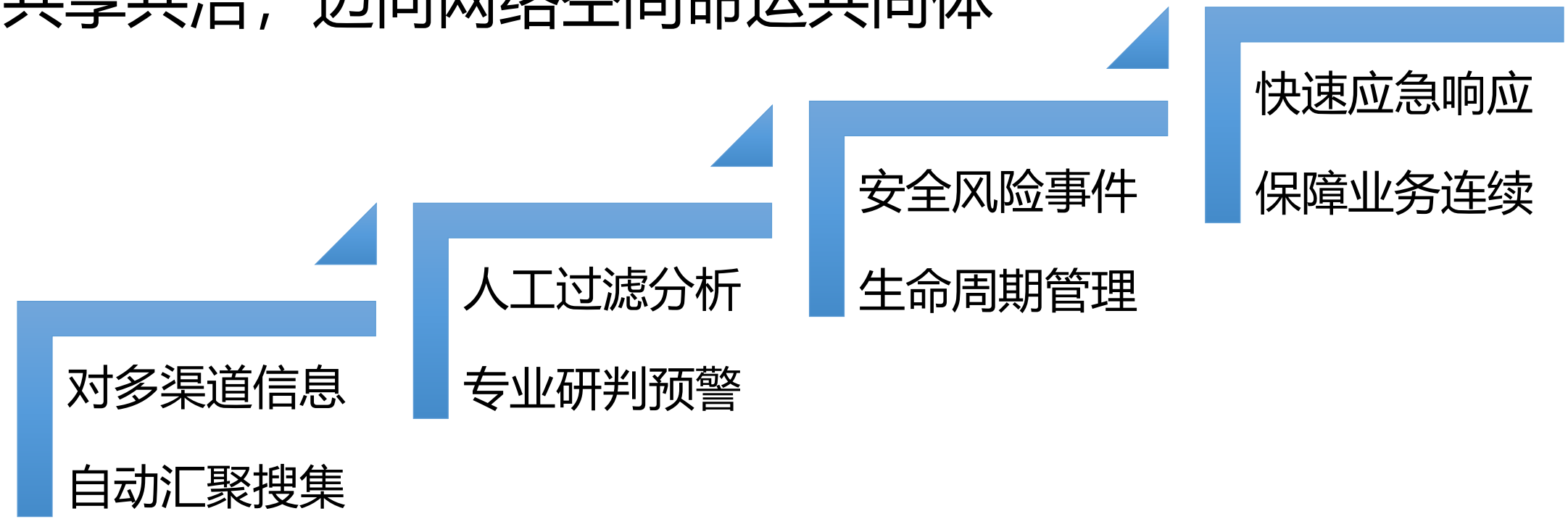
https://src.edu-info.edu.cn/

目录

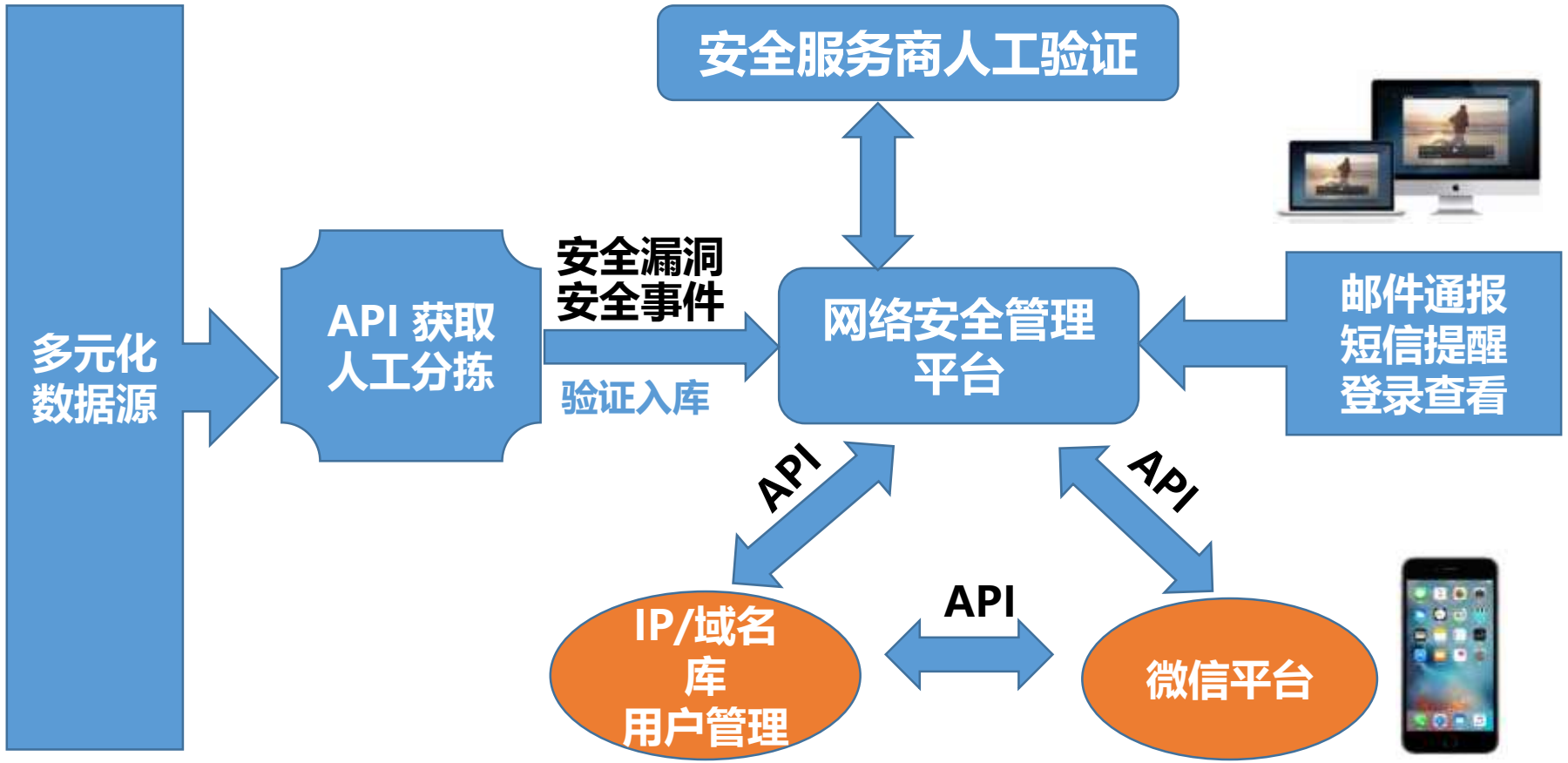
- 教育行业安全现状
- 应急响应体系建设
- **走向安全态势感知**

安全威胁情报共享与分析研判

网络空间安全事件和攻击信息的高效共享至关重要
各校自扫门前雪，谁也不能独善其身
共享共治，迈向网络空间命运共同体



教育部安全漏洞信息通报机制



学校的安全需求是什么？

- 不是软硬件安全产品的堆砌
- 不是孤立的一个个系统建设
- 不是高等级的安全渗透测试
- 不是一次次的救火应急响应

- 学校捧着金饭碗要饭吃
- 要机制创新，抱团取暖

有限投入成本 覆盖 无限安全需求？

- **管理、制度、咨询、规划、人员、培训、投入**
- **系统、运维、整改、应急、演练、情报、服务**

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

2018 ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原“中国互联网安全大会”）