

# 大数据安全在教育行业的应用与实践



安恒信息

1

大数据之眼

观教育行业安全几何



# 安全几何

## 教育行业整体安全态势

海量在线教育系统

存在安全风险

出现典型入侵事件

可用性问题突出

.....

### 网站量区域分布

网站总量: **66626** 个



返回上一级

反共事件  
16个

高中危网站  
6030个

安全事件  
148个

服务异常  
32832个



高 低

排行	区域	网站量
1	江苏	6466
2	北京	5595
3	广东	4111
4	山东	4004

# 安全几何

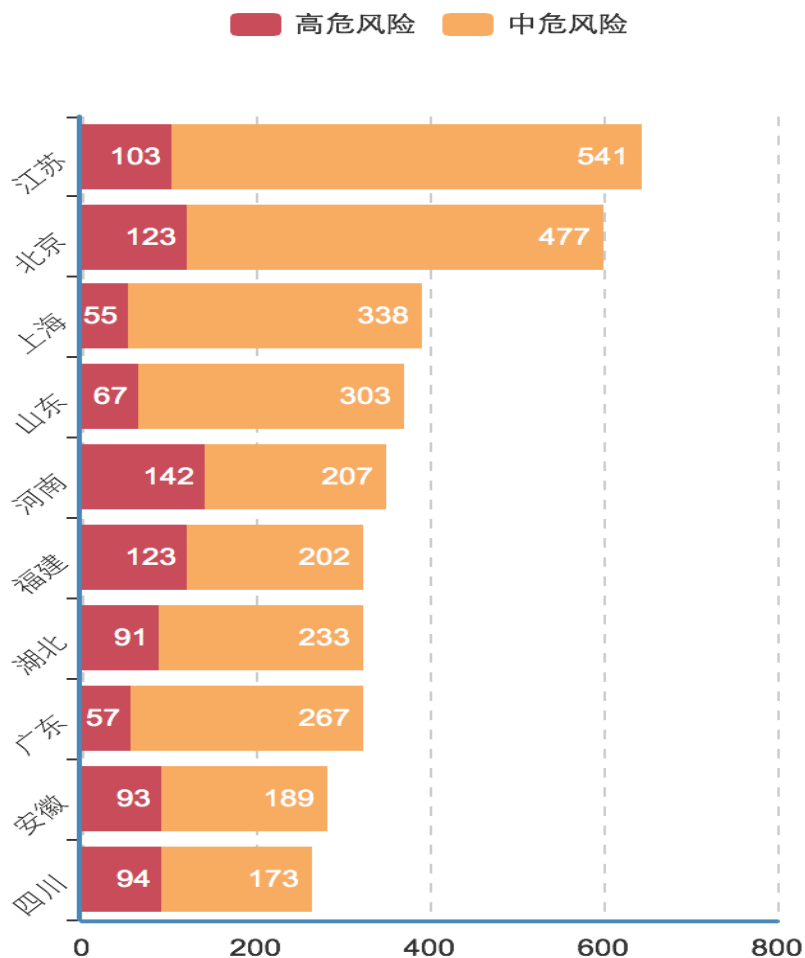
6030个教育网站(约10%)一攻即破

风暴中心监测教育行业安全风险：

208,394个漏洞

6030个网站受高中危漏洞影响

站点安全风险分布(Top 10)



# 安全几何

## 典型安全事件类型

The image shows a screenshot of a web browser displaying the Guilin Medical College (桂林医学院) campus welcome portal. The browser's address bar shows 'edu.cn/' and the page URL is 'x.glmc.edu.cn'. The page header includes the college's name and a date stamp: '今天是2016年10月31日 星期一 校园迎新门户欢迎您。' (Today is October 31, 2016, Monday, Campus Welcome Portal Welcome You).

The main content area features a large, bold, black defacement message: '中国共产党，爷没事就想训斥训斥你！哈哈' (Communist Party, I just want to scold you when I'm free! Haha). A blue callout box with white text '反共黑客入侵' (Anti-communist hacker intrusion) is overlaid on the right side of the message.

The page layout includes several sections:

- 入学须知 (Admission Notice):** A section with a gift icon and a link to '更多' (More). It contains a notice about stopping the online payment system for the迎新 system (迎新系统网银缴费) on September 1, 2016, at 00:00. The notice states that students should not use the online payment system after 22:00 on September 31 and should proceed with on-site payment at the financial office.
- 关于停止迎新系统网银缴费的通知 (Notice on Stopping Online Payment for the迎新 System):** A section with a red header and a link to '更多' (More).
- 报到须知 (Check-in Notice):** A section with a link to '更多' (More).
- 校园新闻 (Campus News):** A section with a link to '更多' (More) and a list of news items, including '校园风光' (Campus Scenery), '新校区建设进展情况通报' (Report on the Progress of the New Campus Construction), '我校召开发展定位规划征求意见座' (Our school held a meeting to solicit opinions on the development positioning plan), and '用心服务助“清洁卫生”人民心' (Dedicated service to help 'clean and hygienic' people's hearts).
- 用户登录 (User Login):** A section with a link to 'USER LOGIN' and a form for login. The form includes fields for '用户名: 身份证后六位' (Username: Last six digits of ID card), '密码: 初始为考生号后五位' (Password: Initial is the last five digits of the candidate number), and radio buttons for '学生' (Student) and '教师' (Teacher). There is a '重号' (Reset) button.
- 报到咨询 (Check-in Consultation):** A section with a link to '点击查看' (Click to view).
- 最新报到 (Latest Check-in):** A section with a list of students who have checked in, including '覃敏' (Tan Min), '韦春炎' (Wei Chunyan), and '张宁' (Zhang Ning).

The browser's right sidebar shows various advertisements, including '开户' (Open Account), '66R.COM', and 'bet365'.

# 安全几何

## 典型安全事件TOP1——暗链

共检测到暗链**2755**个

涉及暗链源站**1523**个

类型：**博彩、游戏、  
色情、广告**

各地区暗链数量分布

数据来自：风暴中心





# 安全几何

## 因为漏洞而失窃的数据

### [你懂的]上海市共青团学校部邮件打包下载

发表于: 2015年05月17日 • 120 条评论 • 20,672 次浏览 • 五毛 泄漏

在推特上预告过了..上海市共青团学校部的邮箱打包..大约13G左右,包含从2011至今上海市:校活动的统计信息,上海市部分学校网评员名单等等等等...



网曝字信网数据泄露 或涉及中国所有大学生个人信息

学信网

分享时间: 2016-04-05 15:41

返回上一级 | 全部文件 > 学信网

文件名	大小	修改日期
chsi fax_bak【...】 网友资源】 v00	100M	2016-04-04 23:24
chsi fax_bak【...】 网友资源】 v75	100M	2016-04-04 23:24
chsi fax_bak【...】 网友资源】 v72	100M	2016-04-04 23:24
chsi fax_bak【...】 网友资源】 v68	100M	2016-04-04 23:24
chsi fax_bak【...】 网友资源】 v64	100M	2016-04-04 23:24
chsi fax_bak【...】 网友资源】 v62	100M	2016-04-04 23:24



# 引发问题

## 大批量个人信息泄露与猖獗的电信诈骗

中国互联网协会《中国网民权益保护调查报告2016》显示，近一年的时间，国内6.88亿网民因垃圾短信、诈骗信息、个人信息泄露等造成的经济损失估算达915亿元。粗略估计，仅网络诈骗产业链上，就至少有**160万从业者（诈骗犯）**，其“**年产值**”超过**1152亿元**，超过了部分省份的年GDP。

### 2016年8月电信诈骗热点事件列举

12日，21岁山东大二学生宋振宁接到诈骗电话，被骗走生活费及大量现金，23日凌晨，宋振宁因心脏骤停而离世。

28日，潮汕女生蔡淑妍失联，此前曾遭遇电信诈骗，被骗走9800元学费和生活费后，最终选择自杀。

19日，山东临沂女生徐玉玉接到诈骗电话后，被骗走9900元学费，因悲痛欲绝，导致21日含恨离世。

29日晚，清华大学老师报案称，被冒充公检法电信诈骗人民币1760万元。警方已介入调查并开展工作。



# 安全 分析

## 大数据分析安全重灾区

我国院校公开植入黑页的安全事件达**319**起

发生在二级域名的安全事件就达**318**起，涉及主域名数量为**122**个。

由此可知，我国教育网站，尤其是大专院校网站的安全问题，多集中于该校网站的二级学院、部门子域名，且常发生顶级域名下所有二级域名被同时批量入侵的事件。

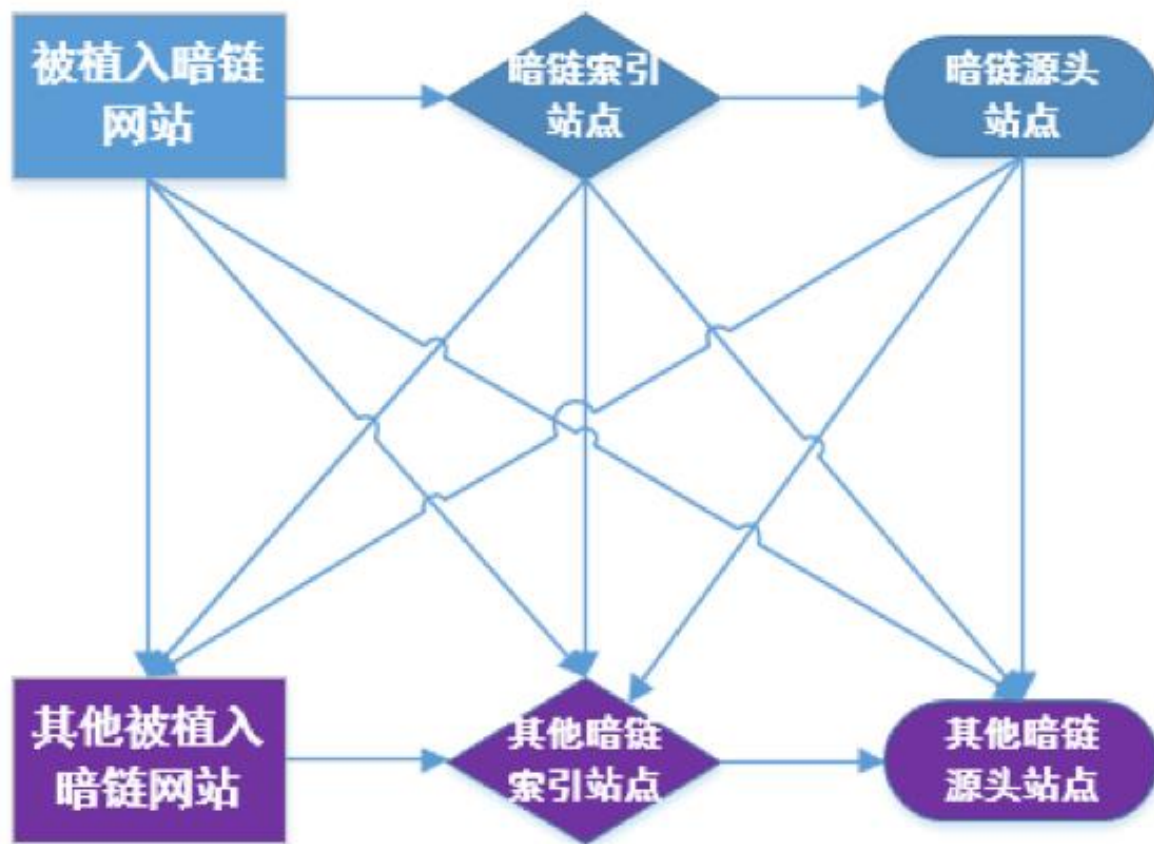
### 安全事件举证

 <p>浙江省湖州市数学学会 bxy.hutczj.cn 2016-11-08 09:26:48</p>	 <p>江西宜春职业技术学院 jy.ycvc.jx.cn 2016-11-02 10:42:50</p>	 <p>广西桂林医学院校园迎... yx.glmc.edu.cn 2016-10-31 20:36:06</p>	 <p>吉林艺术学院 zsb.jlart.edu.cn 2016-10-20 10:31:56</p>
---	---	--	--

# 安全分析

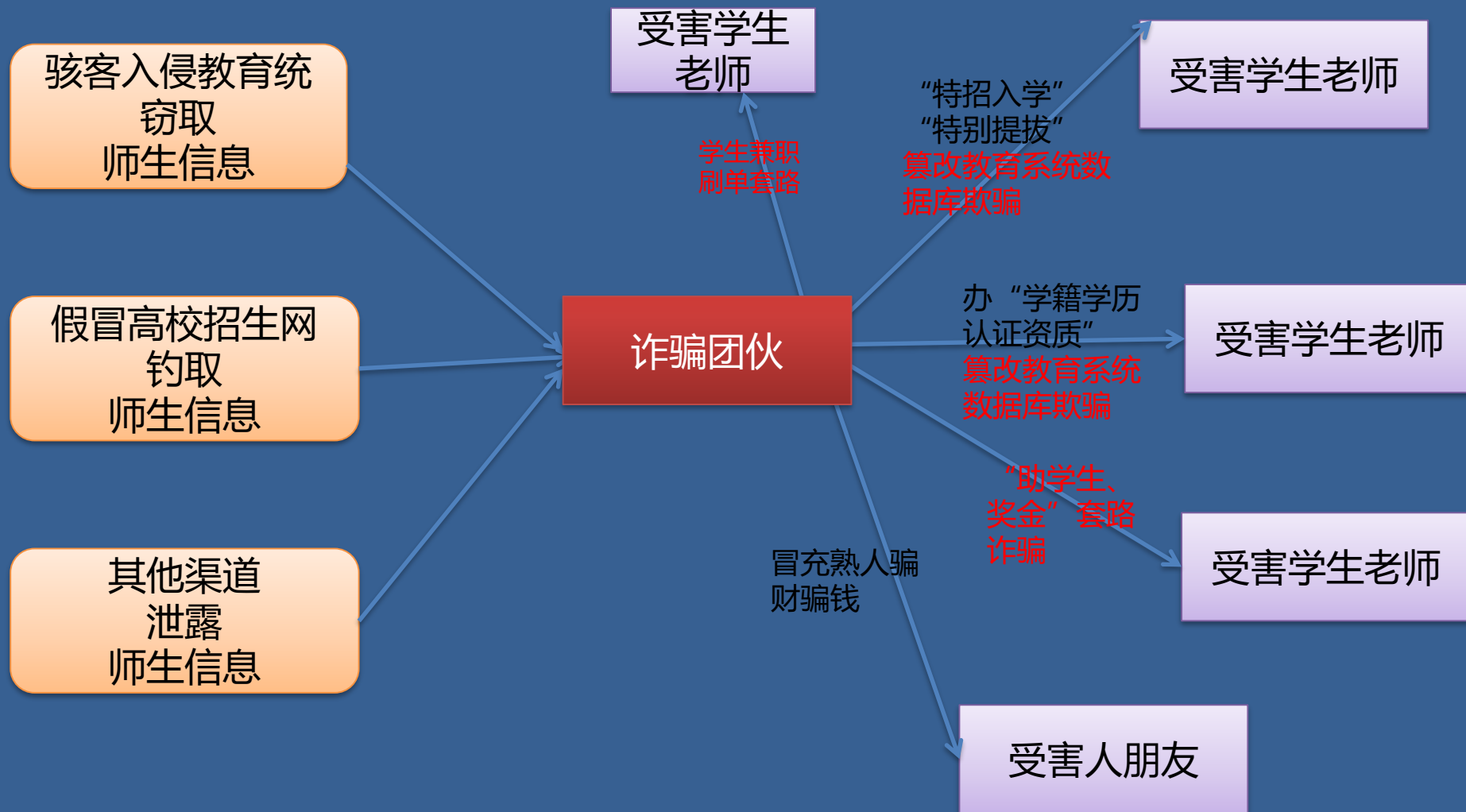
## 大数据分析暗链攻击行为

由过去网站暗链以单向链接指向暗链源头主机的形式，进化为遭植入暗链网站交叉互链、境内暗链索引主机交叉互链、暗链源头主机交叉互链以及遭植入暗链网站、暗链索引主机、暗链源头主机同时交叉互链的复合形式。



# 安全分析

## 教育行业常见黑色产业链



# 大数据之眼

# 教育行业的大数据安全实践



# 安全 要求

## 教育部网信工作安全行动

### 教育部网络安全和信息化领导小组第一次会议会议纪要

会议对网信工作提出如下要求：

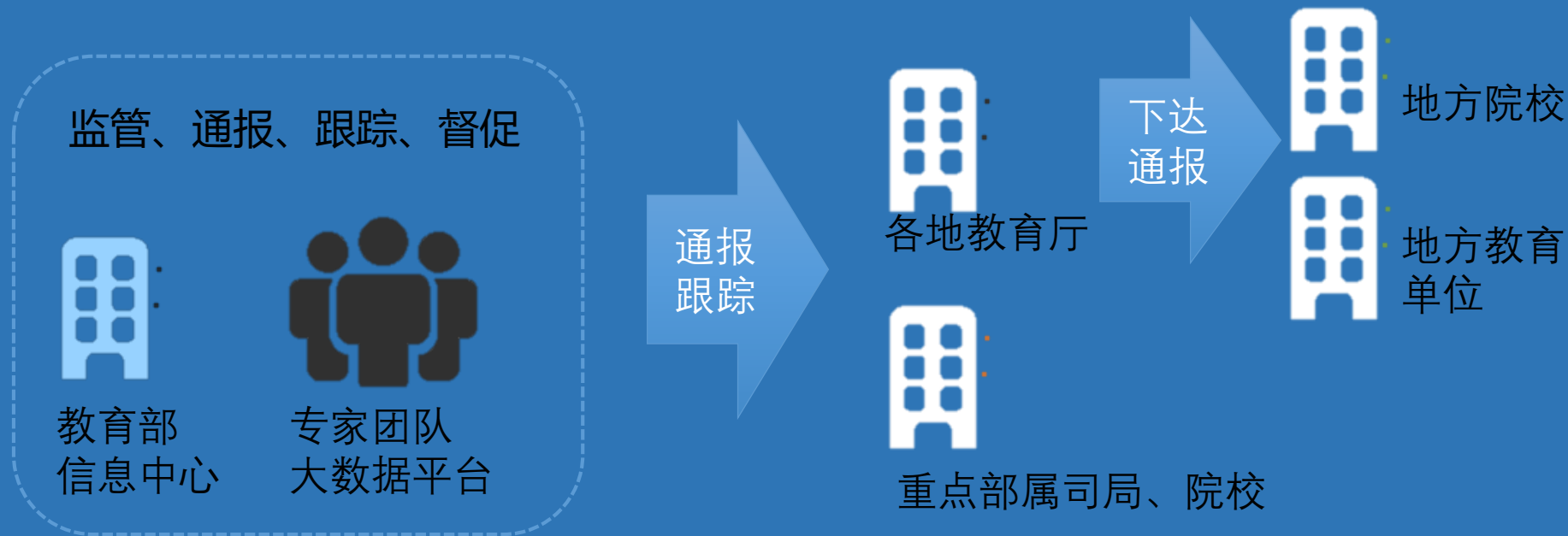
一要进一步提高对网信工作的认识。要把认识统一到习近平总书记的系列重要讲话精神上来，落实好十八大以来中央在网信工作方面的决策部署，将教育行业网信工作自觉纳入国家网络安全的大格局、自觉服务国家信息化建设的总部署，适应信息化社会对教育事业提出的新需求，进一步增强工作的自觉性和主动性。

二要进一步健全网信工作责任体系。网信领导小组办公室要做好统筹协调，推动领导小组议定的各项工作落实；成员单位从各自职能出发承担网信工作职责，落实领导小组议定事项。

三要落实好三个方面的工作。一是办公室牵头负责拿出各单位职责清单，建立端对端的责任保障体系。二是规划司负责尽快出台教育数据管理办法，与国家的相关法律法规保持衔接，使之成为今后一段时间数据安全工作的管总文件，办公室负责配合推动。三是办公室负责制定以“治乱、堵漏、补短、规范”为主的综合治理活动方案，规范数据使用，提升教育部的网络和数据安全水平。

# 安全实践

## 教育行业的安全实践



7\*24专家团队值守

远程/现场应急支持

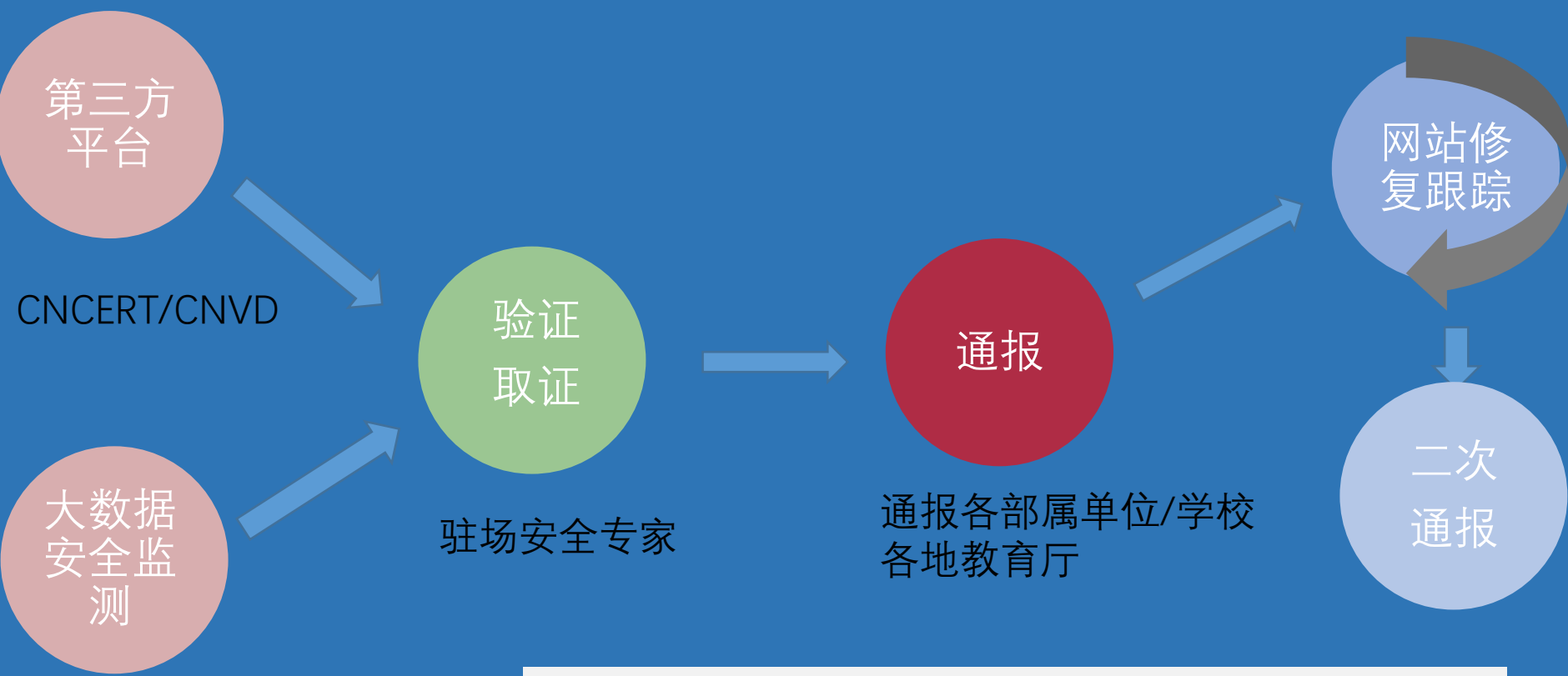
风暴中心监测

建立健全重要系统与单位职责体系  
初步形成重点单位端对端的安全保障机制



# 安全实践

## 教育行业安全实践



建成初步的安全通报整改跟踪机制，进行“治乱、堵漏”

# 安全 实践

## 教育行业安全实践

截至目前：

跟踪验证通报漏洞8755个

### 一期成果：

全面通报并整改消除180多个重点单位高危、  
中危漏洞，避免安全事件、数据泄露。  
初步实现“治乱”、“堵漏”。

截止目前，跟踪验证通报暗链事件1649个

# 安全工作

## 基于大数据能力可进一步推进监管工作

### 各教育单位职责清单梳理



大数据在线资产探测、识别梳理。  
网站、应用、端口、服务……



通过ICP备案信息、whois注册数据梳理资产所属单位



梳理各单位、组织信息，进行资产归类，明确负责人

#### 单位资产信息元素



单位机构、  
域名系统、  
IP地址、  
联系人、  
主管单位  
……

# 安全工作

## 基于大数据可实现的进一步安全工作

主管部门可依靠大数据监测开展“治乱”

大数据监测  
资产运维“乱像”

临时应用  
随意开放

开放  
高危端口

IP漂移海外

备案信息  
不准确

二级域名  
维护无序

僵尸站点

# 安全工作

## 基于大数据可实现的进一步安全工作

### 教育主管部门可开展“堵漏”工作

大数据实时监测  
跟踪通报、处置

漏洞扫描跟踪、  
及时通报堵漏

事件实时监测、  
促进响应效率

SQL注入、  
跨站、struts  
命令执行、0day  
各类漏洞

引发事件

暗链、篡改、  
黑页、反共黑客

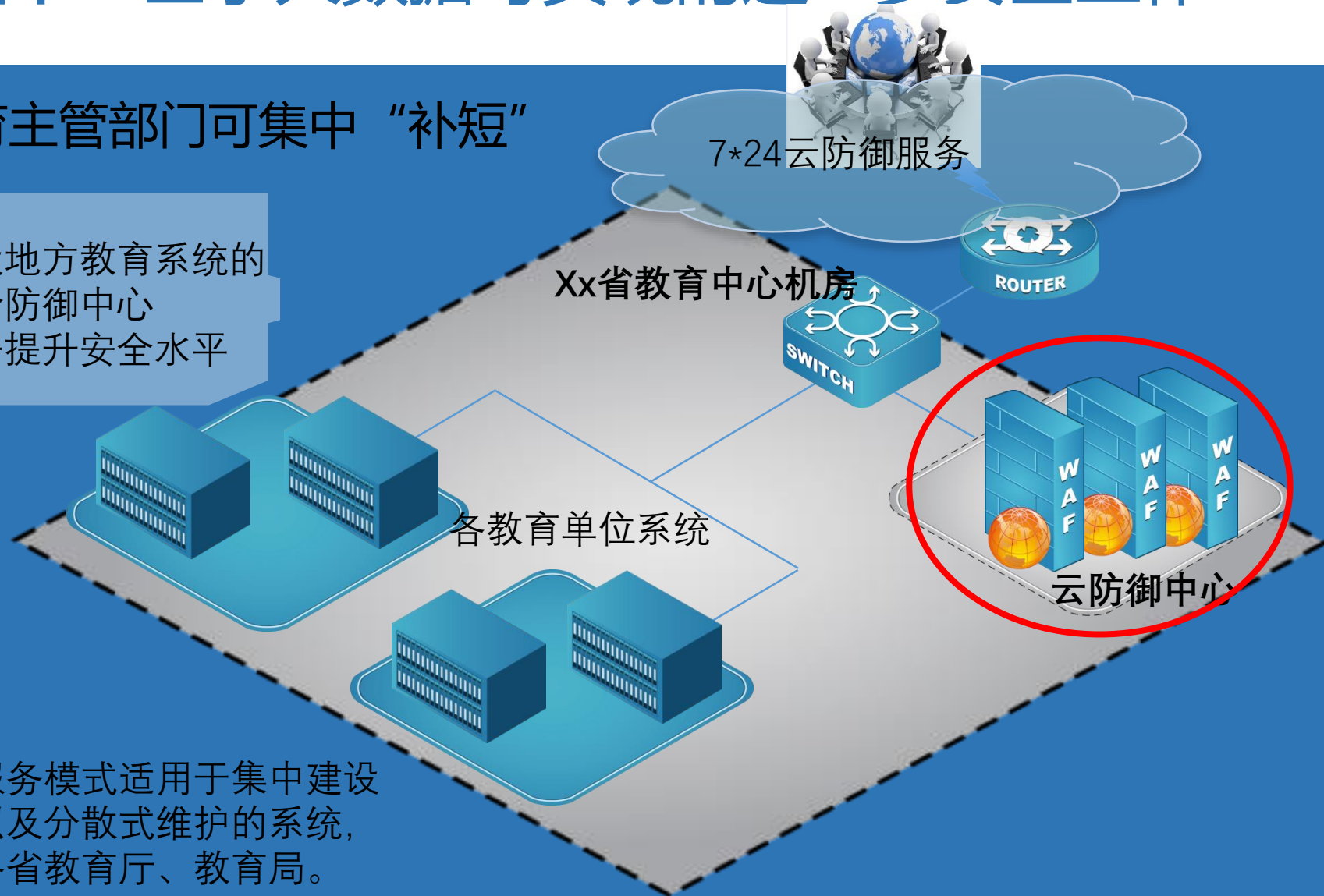
数据泄露事件

# 安全工作

## 基于大数据可实现的进一步安全工作

教育主管部门可集中“补短”

建设地方教育系统的安全防御中心  
统一提升安全水平



云防御服务模式适用于集中建设的机房以及分散式维护的系统，适用于各省教育厅、教育局。



## 先知——大数据安全监测实现方式

### 分布式基础网络

覆盖全国32个省市的监测节点  
自发现网络空间在线系统

### 海量数据处理性能

网络设备 12,339,390

发现漏洞 68,922,867

存储数据 465TB

安全事件 8500多起

基于HADOOP的大数据架构



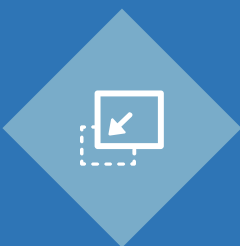
0day挖掘策略更新

事件取证与审核

威胁情报分析

安全资讯动态分享

## 先知——大数据安全监测实现方式



### 确认扫描系统范围

如检测浙江省政府站点  
教育行业站点  
上海市站点



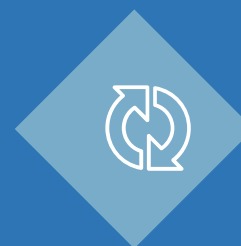
### 执行大数据扫描

海量任务检测，  
对单站点产生影响微小



### 深入策略验证

检测后对漏洞进行自  
动化精准验证、取证，  
确认漏洞存在



### 跟踪比较整改数据

历史漏洞遗留情况  
一定时长内的修复情况  
最新爆发的漏洞增加情况

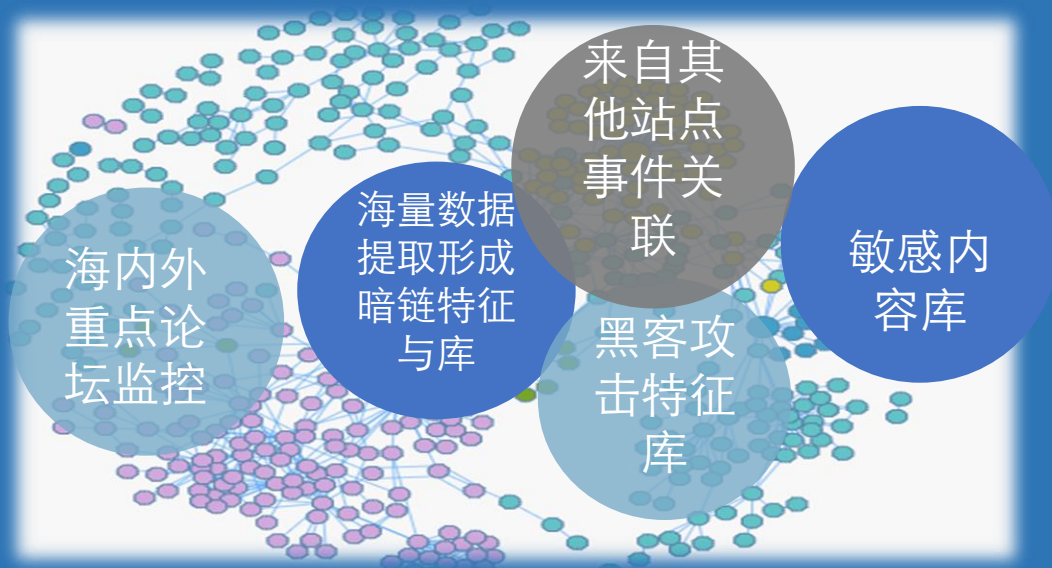
增加高精度验证环节，解决传统检测中，误报严重的问题，  
对扫描后的漏洞针对性验证，又能保障检测效率

## 先知——大数据安全监测实现方式

传统方式专注单站点自身页面，  
基准判断难于精准发现攻击事件



基于网络空间威胁的新型事件  
监测

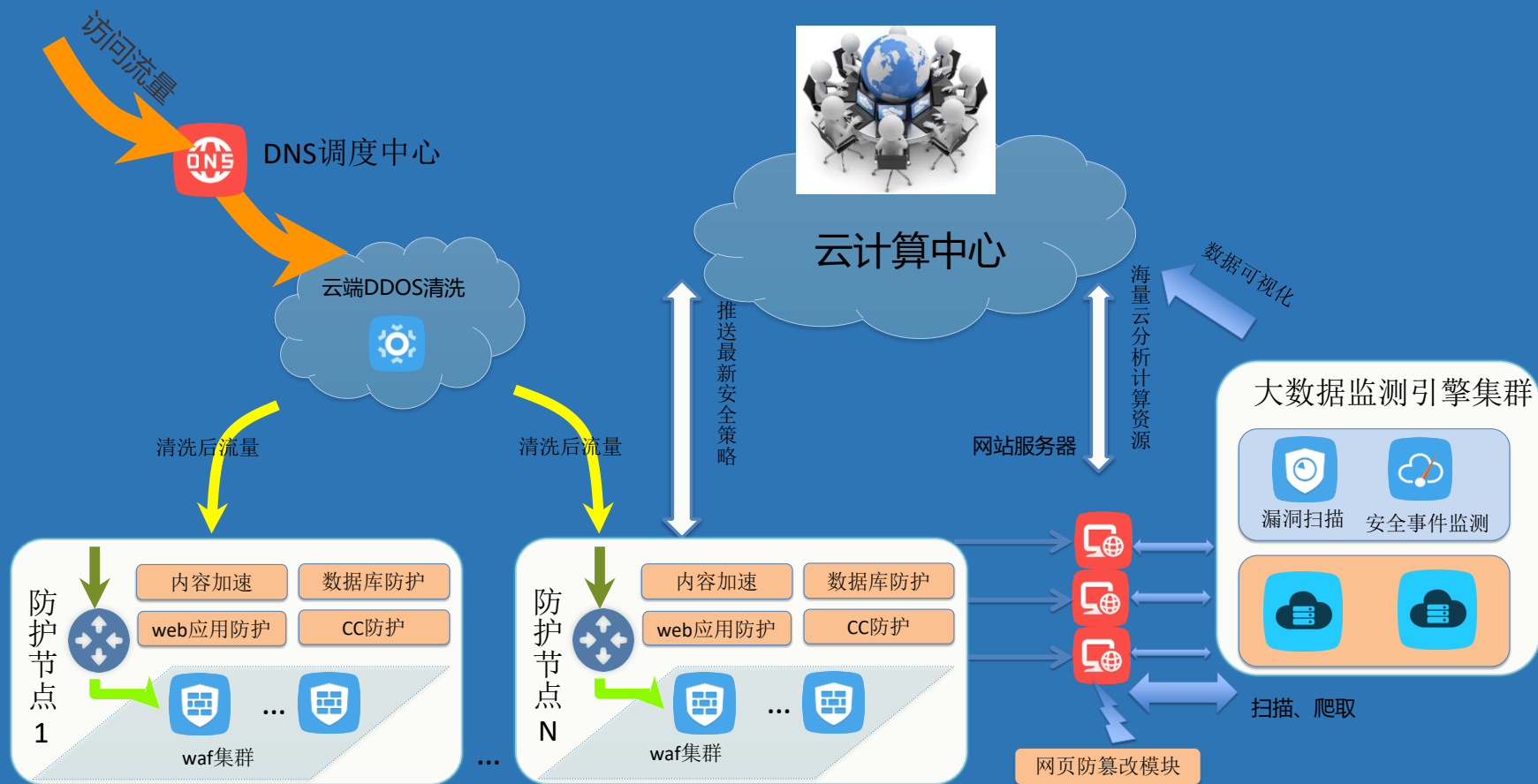


海量站点威胁信息提取，可对90%以上有组织的  
攻击特征匹配

大数据空间站点关联，发现更多被黑事件。如  
成为广告站点、暗链源、黑站被推广等事件。

## 云防御中心——玄武盾

事前安全检测” + “事中实时防护” + “事后分析加固” 整体WEB安全生命解决方案



## 云防御中心——玄武盾G20防护案例

### 官网安全态势分析



官网：自2015年12月1日0点开放以来，提供正常访问2亿多次，共拦截恶意攻击行为**300余万次**，阻断IP**近万余**。



注册网：自2015年11月18日开放以来，共计拦截非法访问2900万余次，抵御针对注册网的直接攻击**112万余**次，人工梳理阻断恶意攻击IP地址**近千个**。



# 安全实践

## 专业服务团队安全通报成果

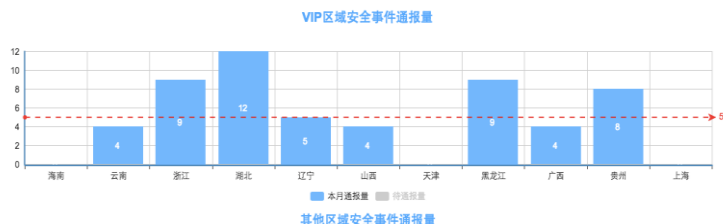
**3小时**内下发至受影响用户单位

公安部通报中心/地方公安

国家CNCERT/ 地方CERT

国家教育部/ 地方教育厅

当月事件通报统计



年度通报8000多起事件

CNCERT的通报支撑单位

公安部优秀通报支撑单位

29地CERT通报支撑



# 安全 实践

## 行业安全大数据分析

### 2016 年教育行业网络安全 态势感知报告



1	全国教育行业网站情况概述 .....	4
2	Web 服务器类型统计 .....	5
3	网站服务质量统计 .....	6
4	最新漏洞情况统计 .....	7
4.1	教育网站漏洞总体情况分析 .....	7
4.2	网站安全等级分析 .....	7
4.3	教育行业漏洞等级情况分析 .....	8
4.4	教育行业站点安全情况地域分布分析 .....	9
4.5	高危紧急漏洞简述 .....	13
4.5.1	SQL 注入漏洞 .....	13
4.5.2	跨站类漏洞 .....	15
5	历史安全事件类型简述 .....	17
5.1	历史安全事件通报分析 .....	17
5.2	安全威胁情报大数据专题分析 .....	18
6	暗链安全事件专项分析 .....	21
6.1	全国教育行业网站暗链情况分析 .....	21
6.1.1	全国教育行业网站暗链情况概述 .....	21
6.1.2	被植入暗链网站地域性分析 .....	21
6.2	暗链背景情况综述 .....	25
6.2.1	暗链价值及危害 .....	25
6.2.2	暗链攻击优势 .....	27
6.2.3	暗链攻击行为分析 .....	29
7	0day 漏洞情况简述 .....	32
7.1.1	漏洞影响概述 .....	32

欲获取报告更多分析结果，可联系安恒风暴中心获取。

管理系统任意文件读

# 安全 实践

## 网络安全人才培养平台——攻防实验室

### 前端展示层面 Application & Software Portfolio

#### 实战仿真

- ① 真实场景
- ② 各类仿真模板
- ③ 组件各类网络

#### 综合实训

- ① 漏洞库
- ② 综合实践靶机
- ③ 验证、研究、分析

#### 工具库

- ① 取证类
- ② 扫描类
- ③ 破解类
- ④ WEB类
- ⑤ 攻击类
- ⑥ 后门类
- ⑦ 明鉴类、0day类

#### 攻防对抗

- ① 单人闯关
- ② 多人对抗
- ③ 攻防竞技

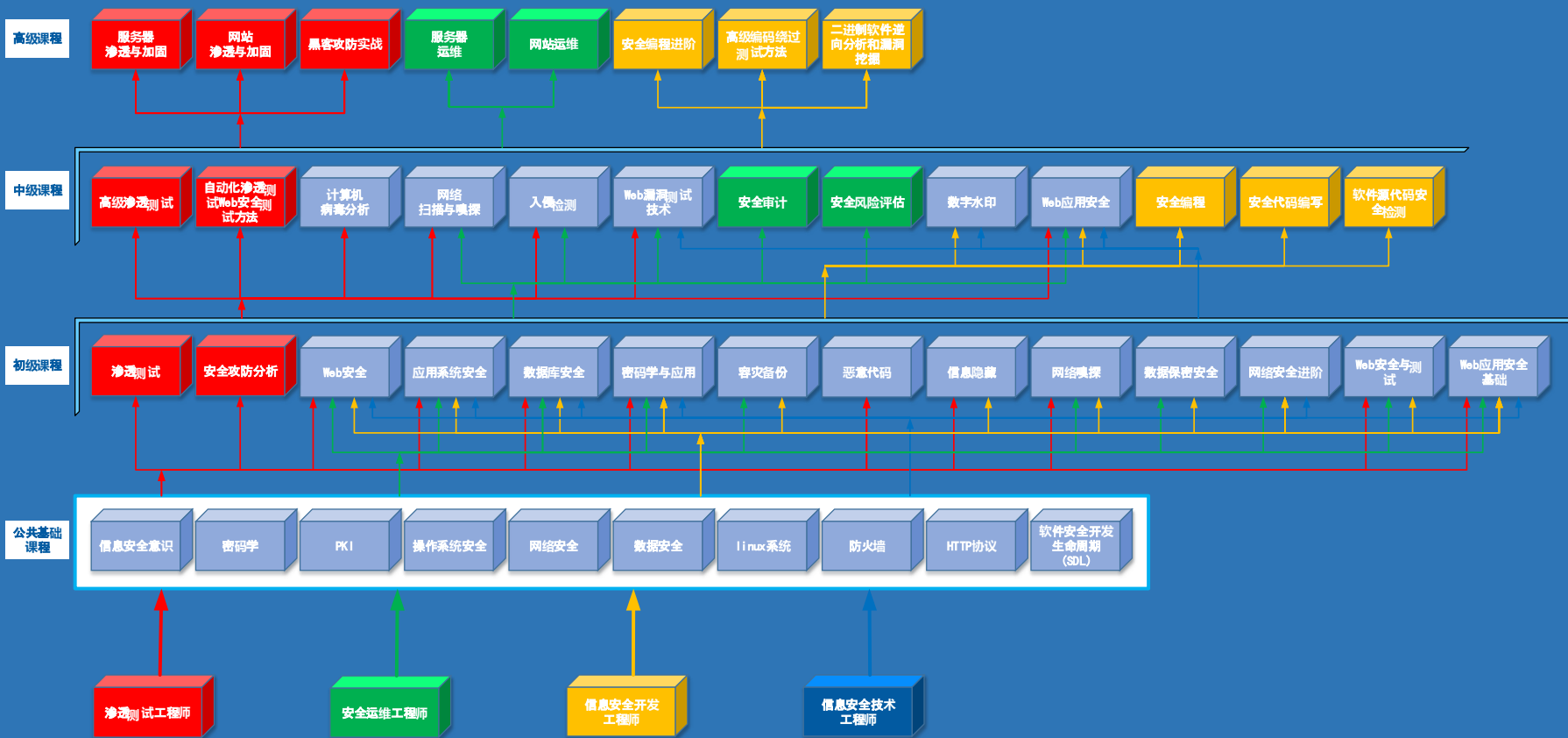
#### 教学实践

- ① 教学实验
- ② 丰富的资源库
- ③ 课程实验

### 综合管理-----软硬件基础设施层 (software and hardware infrastructure)

# 安全实践

## 网络安全人才培养平台——攻防实验室



# 安全 实践

## 网络安全人才培养平台——攻防实验室



- 同共培养网络安全师资力量
- 同共推行网络安全教学标准
- 同共培养复合型网络安全人才
- 同共创新教学、实训等手段

# 安全 实践

## 网络安全人才培养平台——攻防实验室

网络安  
全

主机安  
全

数据库  
安全

应用安  
全

数据安  
全

大数据  
安全

意识安  
全

移动安  
全

安全研  
究

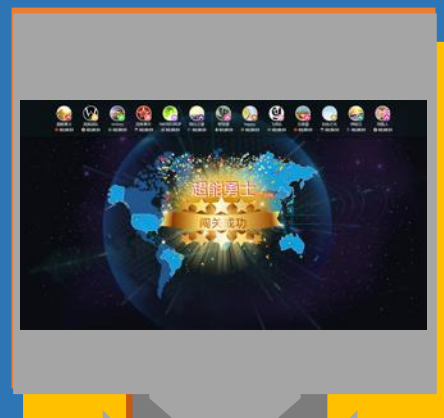
开发安  
全

管理安  
全

物理安  
全

# 安全实践

## 网络安全人才培养平台——攻防实验室



闯关赛

距离比赛结束: 01:43:42 第三届4.29首都网络安全日“安恒杯”技术大赛 (决赛)

距离第18轮结束: 03:27

**RANK** 总排行

团队	积分	得分	失分
长亭外	6755	+2115	-360
Nu1L	5645	+1065	-420
WildWolf	5600	+1200	-600
@Anpro	5595	+855	-770
宫爆鸡丁	5590	0	-900
LeetSpeak	5580	0	-1010
S42	3940	0	-20
宫爆鸡丁的靶机	0	+120	-40
pandora	0	+30	-20
宫爆鸡丁	-40	0	-20

恭喜 LeetSpeak 在第18轮攻占 +15

比赛平台技术支持: DBAPP Security 安恒信息

当前赛事得分前三名: 长亭外, Nu1L, WildWolf

© 14:46 LeetSpeak 在第18轮攻占 宫爆鸡丁 +15



感谢聆听，欢迎交流！



安恒信息