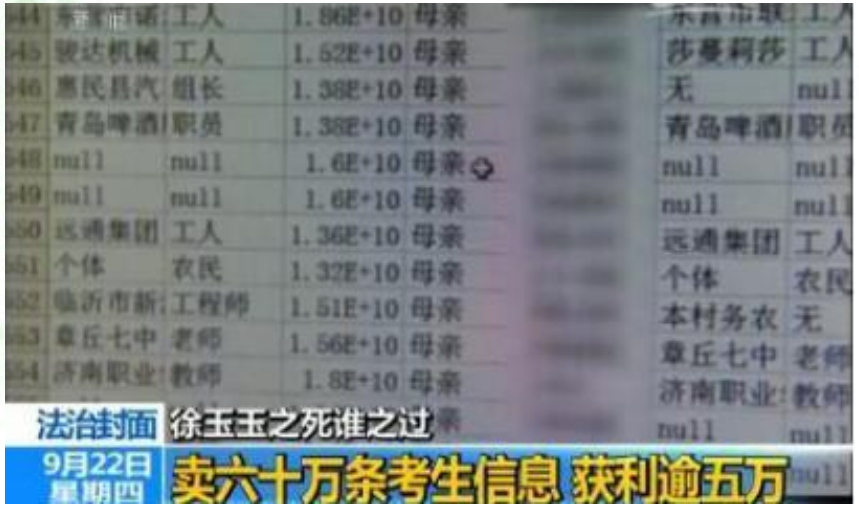
高校网络安全技术发展展望

山东临沂市徐玉玉电信诈骗案

2016年高考，徐玉玉以568分的成绩被南京邮电大学录取。
2016年8月21日，因被诈骗电话骗走上大学的费用9900元，最终导致心脏骤停，不幸离世。
2016年8月26日，临沂市徐玉玉电信诈骗案成功告破，主要犯罪嫌疑人熊超等4人被抓获
2016年08月28日，山东临沂徐玉玉电信诈骗案的头号犯罪嫌疑人郑贤聪投案自首。

临沂市罗庄区人民检察院审查后依法对上述7名犯罪嫌疑人作出了批准逮捕的决定，包括陈文辉、郑贤聪、黄进春、郑金锋、熊超、陈福地、杜天禹；**杜天禹非法出卖公民个人信息，涉嫌侵犯公民个人信息罪**，依法对上述7名犯罪嫌疑人作出了批准逮捕的决定。

电信诈骗的背后，个人信息的倒卖



此次精准诈骗案中至关重要的“窃取个人信息”环节，竟然出自一个同样只有18岁的四川宜宾少年杜天禹之手。目前，网名叫“法师”的黑客杜天禹已被警方在成都抓获，警方查实，年仅18岁的杜天禹，通过QQ先后10多次向陈文辉出售山东考生信息，非法获利1万4千多元。

杜天禹向警方交代，他于今年4月利用安全漏洞侵入“山东省2016高考网上报名信息系统”网站，下载了60多万条高考考生信息，高考结束后开始在网上非法出售，总计获取赃款5万多元，其中就包括徐玉玉的个人信息。

记者：上面都有卖什么样的信息呢?
犯罪嫌疑人郑金峰：我知道的有卖学生信息的，也有卖车主、购房信息的。
记者：价格方面?
犯罪嫌疑人郑金峰：学生个人信息比较便宜，几毛钱。

高考诈骗短信

今天刚从教育网站上“脱裤”获得的新鲜的考生信息，赶紧给这些孩子们发定向诈骗短信。

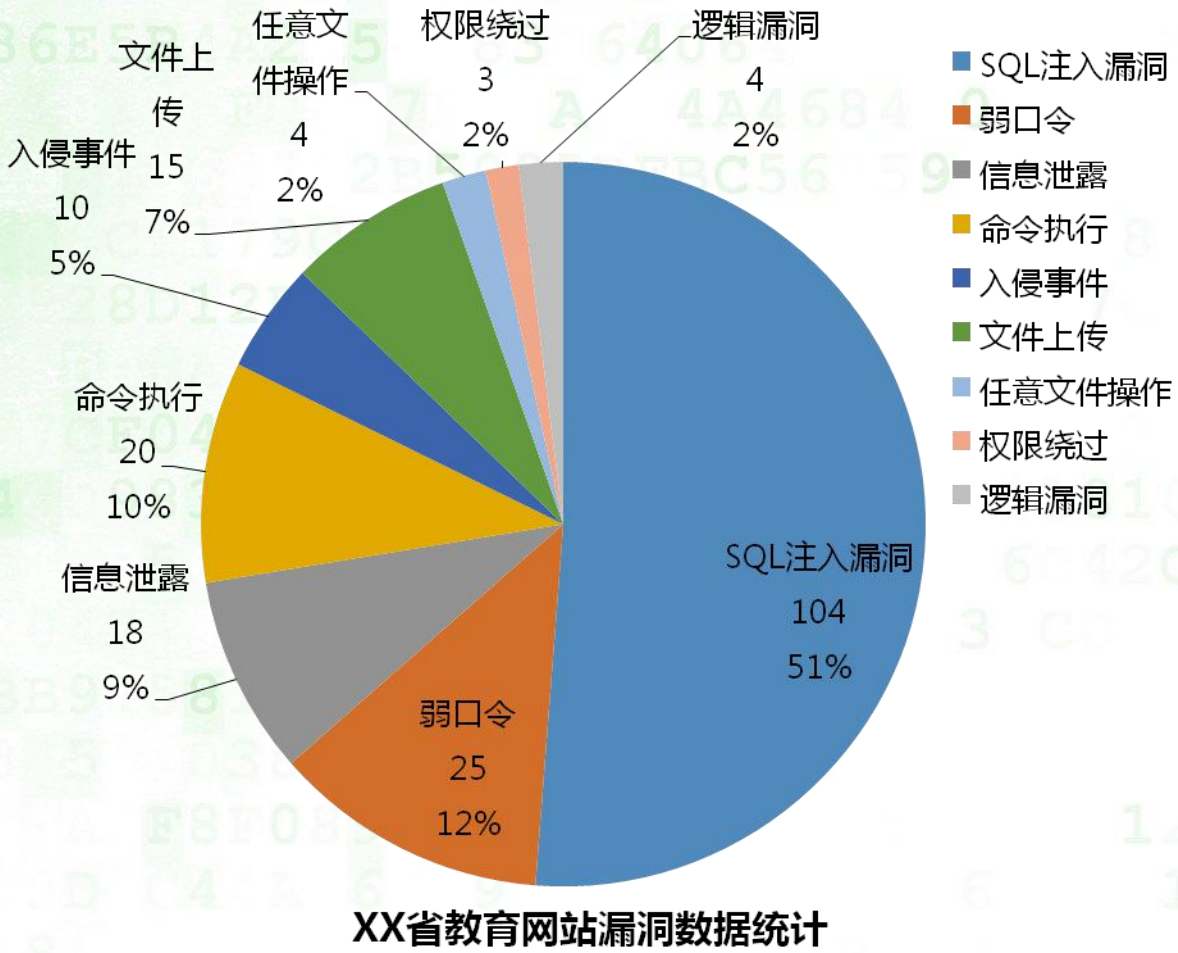
亲爱的同学
祝贺你被江西城市大学录取，请你在8月28日前到学校报到处报到。请携带报名费￥6000元及身份证等有效证件。学校地址：江西路25号

我跟你妈辛辛苦苦积攒的这些钱就是为了让你上个大学你可要争气啊！

学校网站成为沦落为“养马场”

从以往经验来看，高校网站在高考前后访问量会激增上百倍，黑客正是看中这一点，利用漏洞在高校网站植入钓鱼欺诈和木马，考生和家长在访问高校网站查询招生信息时，电脑会面临感染恶意软件、信息泄露等风险。更泛滥的情况是，高校网站已经被黑客作为发射恶意信息的炮台。据360网站安全专家介绍，“高校网站在搜索引擎中的权重很高，安全性又普遍薄弱，黑客在高校网站植入钓鱼网站或博彩和色情链接，在搜索引擎里就更容易被搜索到”。

XX省学校网站漏洞概要分析



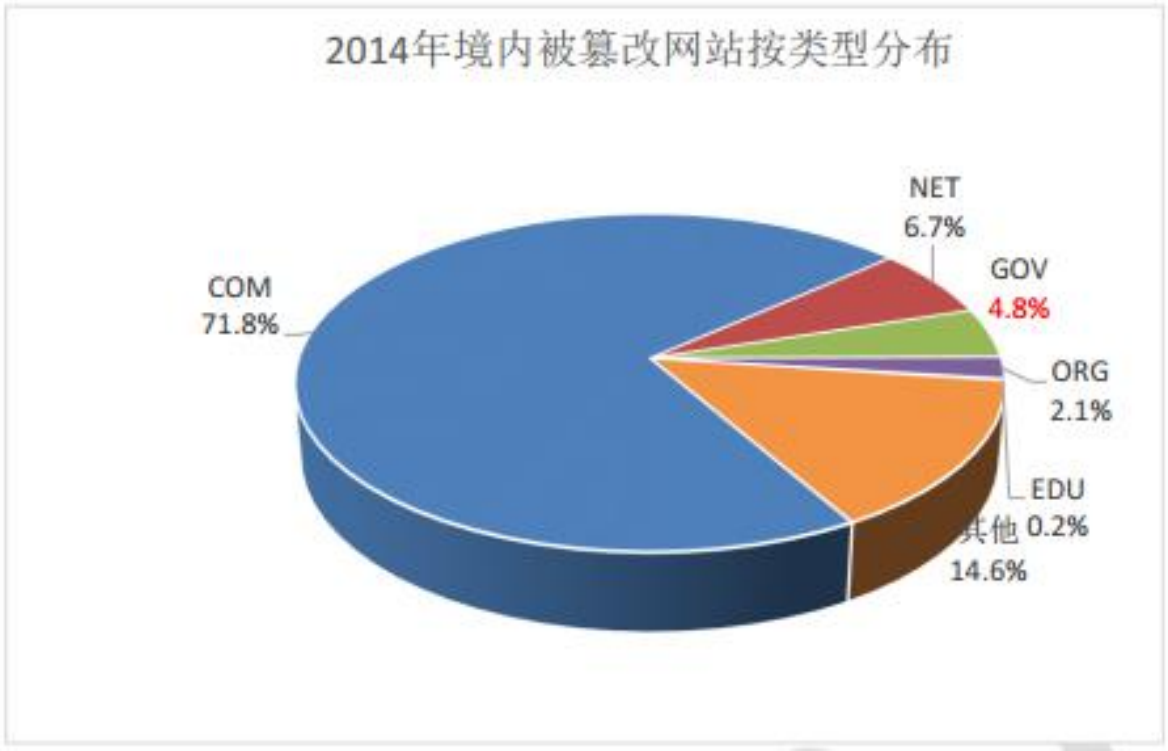
XX省教育网站漏洞数据统计

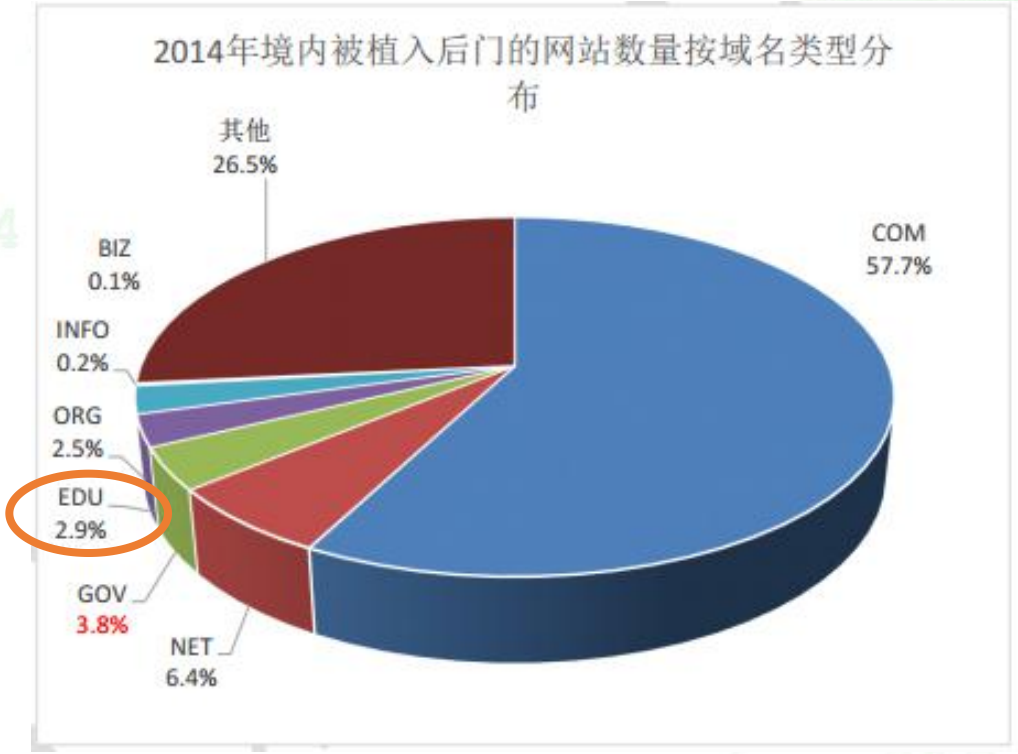
以下数据来自补天平台：

QTVA-2015-247046	**中华心理教育网SQL注入**
QTVA-2015-263966	**抚州市教育局成绩查询系统注入**
QTVA-2015-325070	**江西财经大学分站漏洞**
QTVA-2015-291716	**江西财经大学会计学院教师网站存在sql注入，80多位导师信息泄露**
QTVA-2015-147224	**江西财经大学旗下站点#配置不当，可getshell#**
QTVA-2015-195425	**江西财经大学SQL注入**
QTVA-2015-196190	**江西财经大学存在漏洞，可进后台**
QTVA-2015-216653	**江西财经大学某分站存在SQL注射可getshell**
QTVA-2015-238742	**江西财经大学国际经贸学院sql注入一枚**
QTVA-2015-242117	**江西财经大学分站SQL注入漏洞**
QTVA-2015-298283	**江西财经大学校友会存在漏洞导致同学信息泄漏**
QTVA-2015-310643	**江西财经大学团委网站存在注入，后台弱口令**
QTVA-2015-318233	**江西财经大学新闻网泄漏带整站源码**

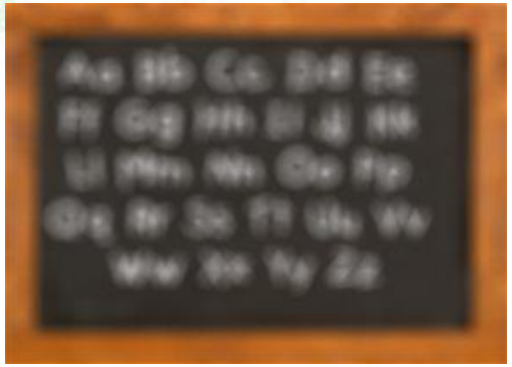
教育行业网站在后门植入方面并不低于政府

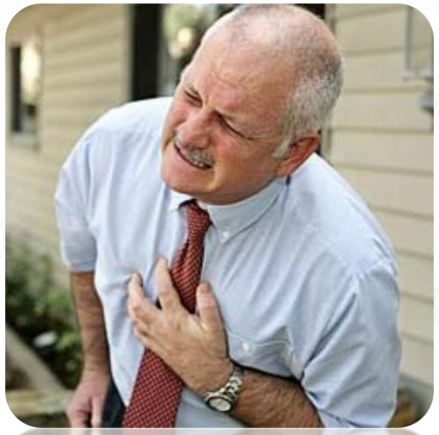
CNCERT/CC
国家互联网应急中心





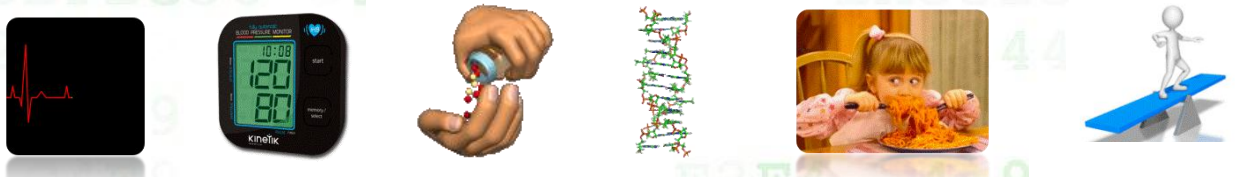
很多人只有在身体出现问题时才会去看医生！

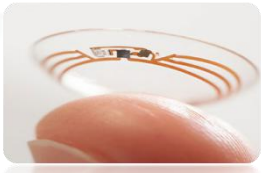




相比等待问题的出现，为什么我们不去每天持续监测个人健康

不只对一个人进行监测与数据采集，而是对每一个人






如果现在我们有能力分析这些聚合后的数据

我们可以识别潜在的健康问题

基于病人A，B和C的体征，这个人有72%的可能存在病症X

我们可以帮助病人了解他们是如何感染疾病的

病人A，B，G在食物中毒之前都在餐厅R进行了就餐

从日常状态中我们可以发现可疑的病状前兆

张三过去睡眠有8小时，但最近平均只睡了5小时，可能需要进一步检查

我们帮助保险精算了解其风险

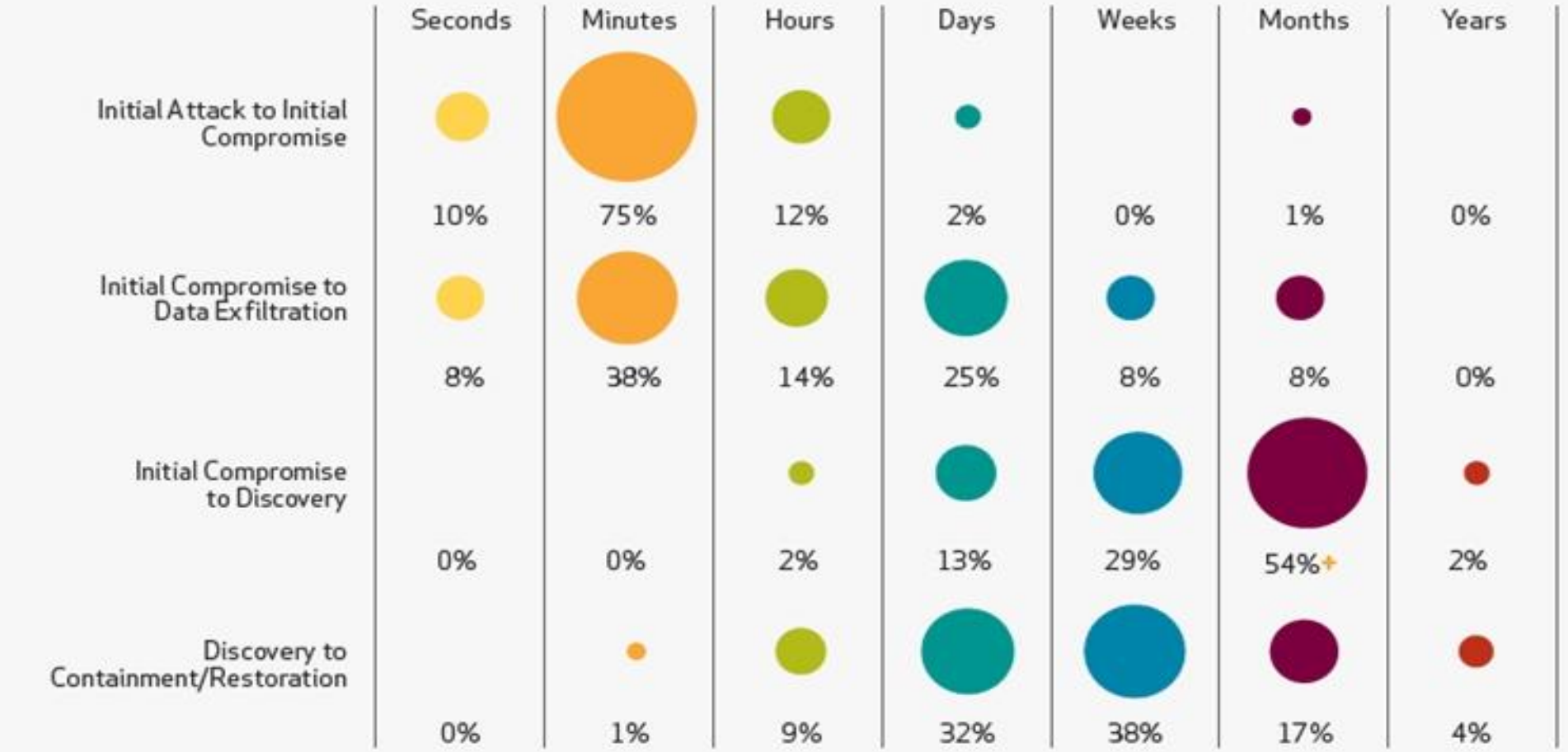
当某个病人具备以下基因组，在服食此类药物后，可延续至70岁的寿命

我们更积极主动的改善药物的使用效果

将药物X的分量从80mg改为100mg将有效降低32%的胆固醇

现今网络攻击过程的时间分布

Figure 40. Timespan of events by percent of breaches



源自于云端大数据分析的威胁情报落地

主防库
- 覆盖5亿客户端
- 总日志数189000亿条
- 每天新增380亿

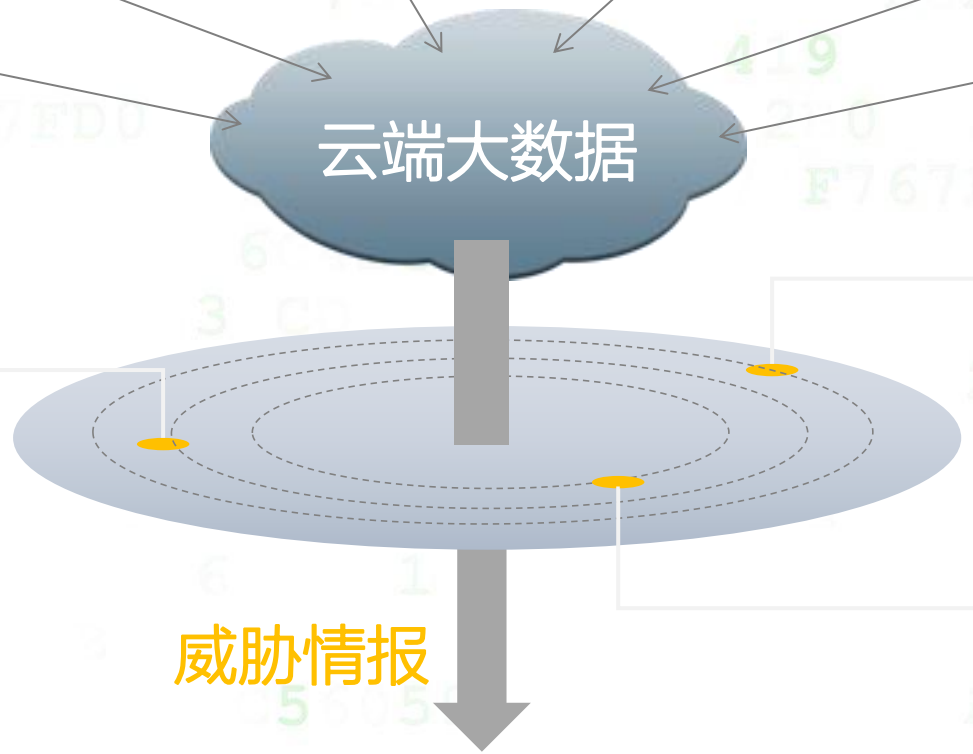
互联网域名信息库
- 90亿DNS解析记录
- 13年whois信息

最大的存活网址库
- 每天查询300亿条
- 每天处理100亿条
- 每天拦截用户访问钓鱼数超过1.4亿URL

最大中文漏洞库
- 总漏洞数超过47万
- 每天新增可达400个

全球独有的样本库
- 总样本95亿
- 每天新增900万

其他第三方数据源
100+



大数据分析
数据挖掘

云端重沙箱运行

专家分析
可视化分析

威胁情报

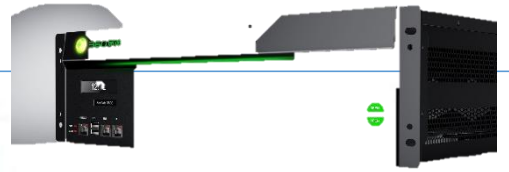
- 整体流量还原与海量日志存储
- **千亿条**日志**秒级快速检索**
- 多维度数据关联分析

网络设备日志、软件系统日志及其他安全软件日志

- ✓ 资产自动识别
- ✓ 操作系统日志
- ✓ 安全设备日志
- ✓ 网络设备日志
- ✓ 终端安全系统日志
- ✓ ……
- ✓ WEB服务器日志
- ✓ 数据库日志
- ✓ 中间件系统日志
- ✓ 应用系统日志
- ✓ Syslog/SNMP/Netfow
- ✓ ……

网络原始日志、安全日志

- ✓ TCP流量
- ✓ Web访问
- ✓ 域名解析
- ✓ 文件传输
- ✓ SQL行为
- ✓ 登录行为
- ✓ ……

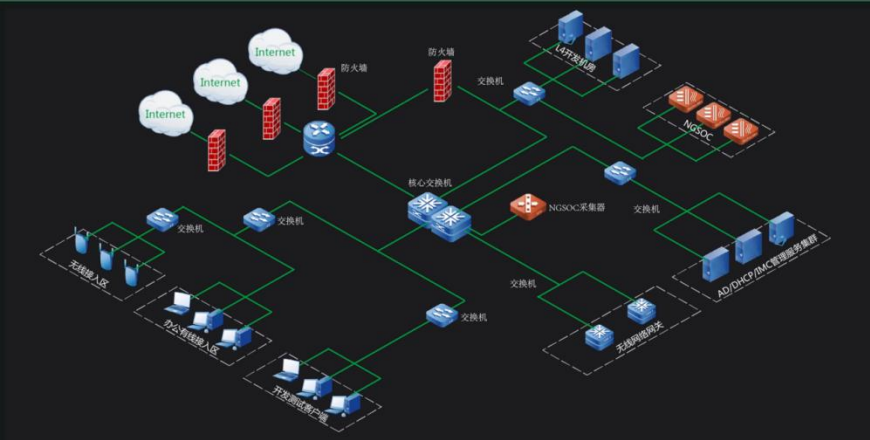


终端原始日志、安全日志

- ✓ 进程网络行为
- ✓ U盘行为
- ✓ IM文件传输
- ✓ 邮件行为
- ✓ ……

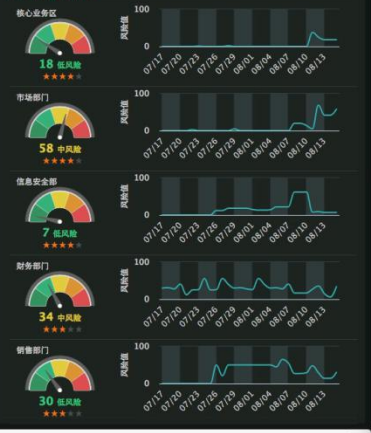
NGSOC 资产风险态势

15 : 28 : 29
2016-08-15



全局风险态势

安全域风险态势



攻击告警

违规告警

可疑事件

恶意文件

漏洞

NGSOC 高风险外连行为监控

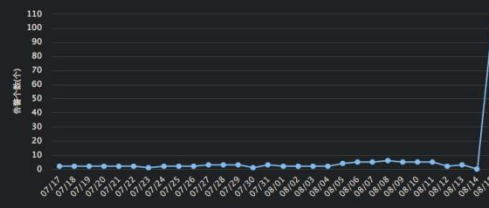
15 : 28 : 3
2016-08-

访问国家TOP 10

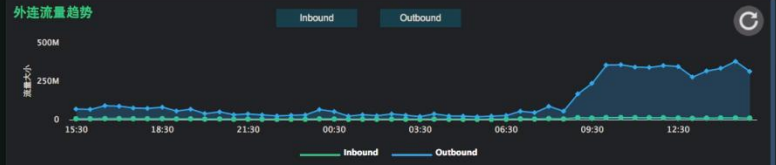
国家	外连计数
US	23
AU	10
CN	3
UK	2
UNKNOWN	1

APT C&C	恶意文件外连 C&C	攻击事件外部源	违规事件外部源	可疑事件外部
26	12	4	2	12
25	17	62	26	24

外连告警时间分布



外连流量趋势



外连端口TOP10

80	443	110	6379	993	8080
995	465	25	11469		

安全域流量TOP10

财务部门	销售部门	市场部门	信息安全	核心业务

最新外连安全事件

发生时间	严重级别	告警类别	告警名称	外部对象	处置状态
2016-08-15 15:06:11	高风险	恶意文...	外连-到内部主机通讯的多个高危...	1	已接收
2016-08-15 14:03:05	高风险	攻击告警	发现IP被某团伙控制	1	已接受
2016-08-15 13:58:32	高风险	攻击告警	发现IP被某团伙控制3005	1	已接受
2016-08-15 13:58:32	高风险	攻击告警	发现IP被某团伙控制3005	2	已接受
2016-08-15 13:58:26	高风险	攻击告警	发现IP被某团伙控制3007	2	已接受
2016-08-15 13:35:36	高风险	恶意文...	恶意外连事件	10	已接受
2016-08-15 13:24:54	高风险	恶意文...	恶意外连事件	10	已接受
2016-08-15 13:19:05	高风险	可疑行...	两意外连事件	10	已确认

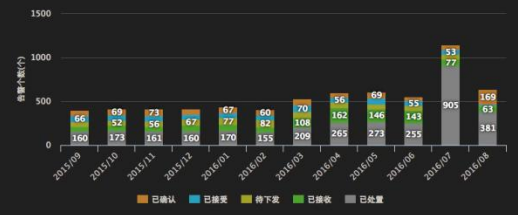
NGSOC 安全告警监控

15 : 28 : 30
2016-08-15

安全告警趋势

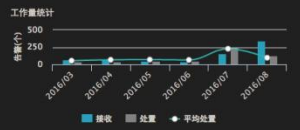
攻击告警 | 违规行为告警 | 可疑行为告警 | 恶意文件告警

告警处置统计



处置任务分配

admin
邮箱: kunpeng@360.cn
电话: 010-56821110
部门: 信息安全部
备注:



zhangzhimei
邮箱: zzhimei@360.cn
电话: 010-56821112
部门: 信息安全部
备注:

jiajun01@360.cn
工作量统计

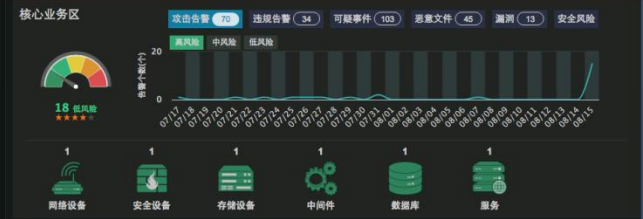
最新告警事件

发生时间	严重级别	告警类别	告警名称	攻击源IP数量	被攻击IP数量	处置状态
2016-08-15 15:06:11	高风险	恶意文件告警	外连-到内部主机通讯的多个高危级别事件	1	1	已接收
2016-08-15 14:51:16	低风险	违规行为告警	认证-针对本地的SSH进行暴力破解	1	1	已接受
2016-08-15 14:03:05	高风险	攻击告警	发现IP被某团伙控制	1	3	已接受
2016-08-15 13:58:32	高风险	攻击告警	发现IP被某团伙控制3005	1	1	已接受
2016-08-15 13:58:32	高风险	攻击告警	发现IP被某团伙控制3005	1	1	已接受
2016-08-15 13:58:26	高风险	攻击告警	发现IP被某团伙控制3007	1	1	已接受
2016-08-15 13:35:36	高风险	恶意文件告警	恶意外连事件	10	1	已接受
2016-08-15 13:24:54	高风险	恶意文件告警	恶意外连事件	10	1	已接受
2016-08-15 13:19:05	高风险	可疑行为告警	恶意外连事件	10	1	已确认
2016-08-15 12:19:21	低风险	可疑行为告警	两意外连事件	9	1	已确认

NGSOC 资产安全监控

15 : 28 : 2
2016-08-

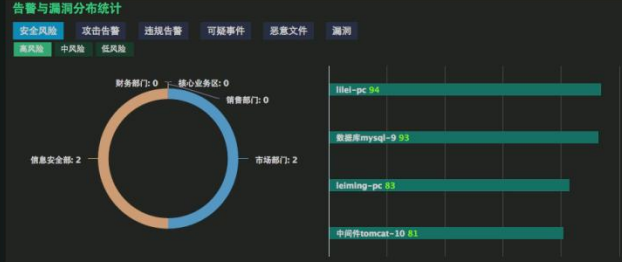
核心业务区



市场部门

信息安全部

告警与漏洞分布统计



安全漏洞列表

发现时间	严重级别	漏洞名称	影响范围	处置状态
2016-08-12 12:39:35	高	Microsoft XML Core Services 漏洞	17	已处置
2016-08-12 11:52:31	中	Internet Explorer HTML 呈现内存损坏漏洞	23	已处置
2016-08-12 11:52:31	低	Windows FTP 客户端可能允许基改文件传输位置的漏洞	23	已处置
2016-08-12 11:52:31	低	IE 不匹配的文档对象模型对象内存损坏漏洞	22	已处置
2016-08-12 11:52:31	低	通过SNMP获得系统信息	22	已处置
2016-08-12 11:52:31	低	通过SNMP获得系统UDP端口列表	21	已处置
2016-08-12 11:52:31	高	Windows 内核中允许特权提升漏洞	12	已处置
2016-08-12 10:56:06	中	DCOM 执行环境可改变威胁	12	已处置
2016-08-12 10:56:06	低	ICMP时间戳获取	12	已处置
2016-08-12 10:56:06	低	可以通过NetBios获取操作系统信息	12	已处置

发现

发现潜伏威胁、违规

- ✓ 基于已知威胁特征发现
- ✓ 威胁情报+本地大数据精准发现
- ✓ 流量建模发现异常
- ✓ 沙箱检测发现
- ✓ 协同检测发现

调查

关联、钻取、鉴定、溯源、拓展

- ✓ 终端、网络元数据采集
- ✓ 本地大数据安全分析
- ✓ 本地样本安全鉴定

处置

一键式处置、协同防御

- ✓ 基于情报信息的自动处理
- ✓ 手动完成的智能响应

《2016年教育信息化工作要点》

教 育 部 办 公 厅 文 件

教技厅[2016]1号

教育部办公厅关于印发《2016年教育信息化工作要点》的通知

（九）推进教育行业网络安全工作。

18.加强教育行业信息系统（网站）安全防护。

落实《教育部 公安部关于全面推进教育行业信息安全等级保护工作的通知》①基本完成教育行业信息系统（网站）的定级备案和第三级及以上信息系统（网站）的测评整改。（责任单位：科技司、教育管理信息中心、地方各级教育行政部门）

19.提升教育行业信息技术安全保障能力。

按照分级管理、逐级负责的原则，②健全信息技术安全通报机制，完善信息技术安全工作管理信息系统，加强对信息技术安全工作的统筹管理。研究制定信息技术安全应急预案。③加强对信息系统（网站）的监测和预警能力。④开展信息技术安全评估。面向部直属单位⑤直属高校和各省级教育行政部门的信息技术安全支撑部门负责人开展安全管理和技术培训，计划培训200人。（责任单位：科技司、教育管理信息中心、地方各级教育行政部门）

文章来自教育部官网:
http://www.moe.edu.cn/srcsite/A16/s3342/201602/t20160219_229804.html

18. 加强教育行业信息系统（网站）安全防护

① 完成顶级备案和三级及以上系统测评整改

19. 提升教育行业信息技术安全保障能力

② 健全信息安全通报机制

③ 加强对网站的监测和预警能力

④ 开展信息技术安全评估

⑤ 开展安全技术与管理培训

中国人民共和国网络安全法

网络安全法获高票通过 明确加强个人信息保护

十二届全国人大常委会第二十四次会议11月7日上午经表决
通过了《中华人民共和国网络安全法》

- 2015年6月：十二届全国人大常委会第十五次会议对网络安全法草案进行首次审议
- 2016年6月：十二届全国人大常委会第二十一次会议对网络安全法草案进行第二次审议
- 2016年10月31日：网络安全法草案提交十二届全国人大常委会第二十四次会议进行第三次审议

网络安全法的出台先后经过了全国人大常委会的三次审议

网络安全法共有7章79条 内容上有6方面突出亮点

1. 明确了网络空间主权的原则
2. 明确了网络产品和服务提供者的安全义务
3. 明确了网络运营者的安全义务
4. 进一步完善了个人信息保护规则
5. 建立了关键信息基础设施安全保护制度
6. 确立了关键信息基础设施重要数据跨境传输的规则

新技术的不断应用、新的标准计划

层面	云计算信息系统对象	传统信息系统保护对象
物理安全	机房及基础设施	机房及基础设施
网络安全	网络设备 网络结构 **虚拟网络结构** **虚拟网络设备**	传统的网络设备 传统的网络结构
主机安全	传统主机 **宿主机操作系统** **虚拟机操作系统** **虚拟机监视器** **云操作系统**	传统主机
应用安全	业务应用系统 **云应用开发平台** **中间件** **云业务管理平台**	业务系统
数据安全	管理数据（包含**虚拟机镜像文件**）、业务数据（包括**用户隐私**）和用户鉴别信息	管理数据、业务数据和用户鉴别信息

- **移动业务**
- **无线网**
- **云计算**
- **工业互联网**
- **…**

挑战

GB

中华人民共和国国家标准

GB/T XXXX-XXXX

信息安全技术
信息系统安全等级保护
第二分册 云计算安全要求

Information security technology—
Baseline for classified protection of information system
Part 2 to cloud computing requirement

（标准草案）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

2012年7月，中国工程院沈昌祥院士提出：当前，我国信息化发展正进入全面深化的新阶段，这些**新型信息技术发展应用**，给我国网络与信息安全保障工作提出了新任务，对**信息安全等级保护工作进行了全面挑战**

等保新技术标准编制工作情况

为适应新技术的发展，解决云计算、物联网、移动互联和工控领域 信息系统的等级保护工作的需要，**2014年3月开始**，由公安部牵头组织开 展了信息技术新领域等级保护重点标准申报国家标准的工作。

公安部第三研究所公安部信息安全等级保护评估中心承担技术指导 和工作推进的任务。

2015年初，标委会批准立项，建议形成基本要求和测评要求的系列标准。

2015年中，标委会批准设计要求修订立项，形成设计要求系列标准

《信息安全等级保护基本要求》

第1部分：安全通用要求

第2部分：云计算安全扩展要求

第3部分：移动互联安全扩展要求

第4部分：物联网安全扩展要求

第5部分：工业控制安全扩展要求

基本要求

测评要求

安全设计技术指南

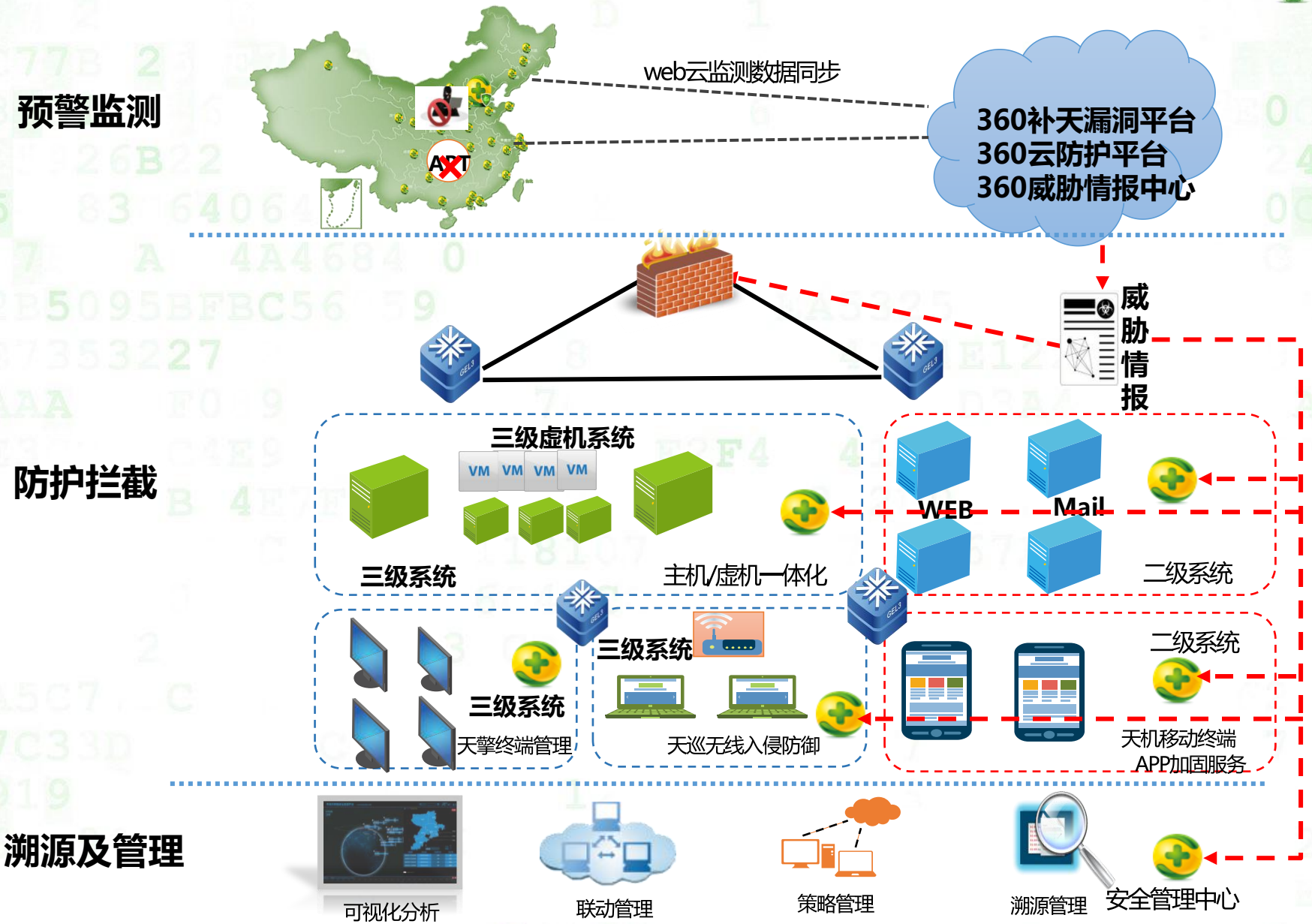
等保新技术标准会带来的一些变化，定级

- **定级对象**，信息系统

- 业务处理类对象，信息系统、工业控制系统、物联网系统
- 基础服务类对象，网络、云平台
- 数据资源类对象

- 云服务方的云平台与云租户的应用系统应分别定级，平台等级不低于应用的安全保护等级
- 移动终端、自建无线网络、无线网关等与固定终端和服务端业务系统作为整体定级
- 传感器、传感网、网关等与服务端业务系统作为整体定级。

新等保安全防护示意图


预警监测
web云监测数据同步
360补天漏洞平台
360云防护平台
360威胁情报中心
威胁情报
防护拦截
三级虚机系统
VM VM VM VM
三级系统
主机/虚机一体化
WEB
Mail
二级系统
三级系统
天擎终端管理
三级系统
天巡无线入侵防御
二级系统
天机移动终端
APP加固服务
溯源及管理
可视化分析
联动管理
策略管理
溯源管理
安全管理中心

360企业安全
助力校园安全建设

360企业安全 安全第一® 企业安全领军者