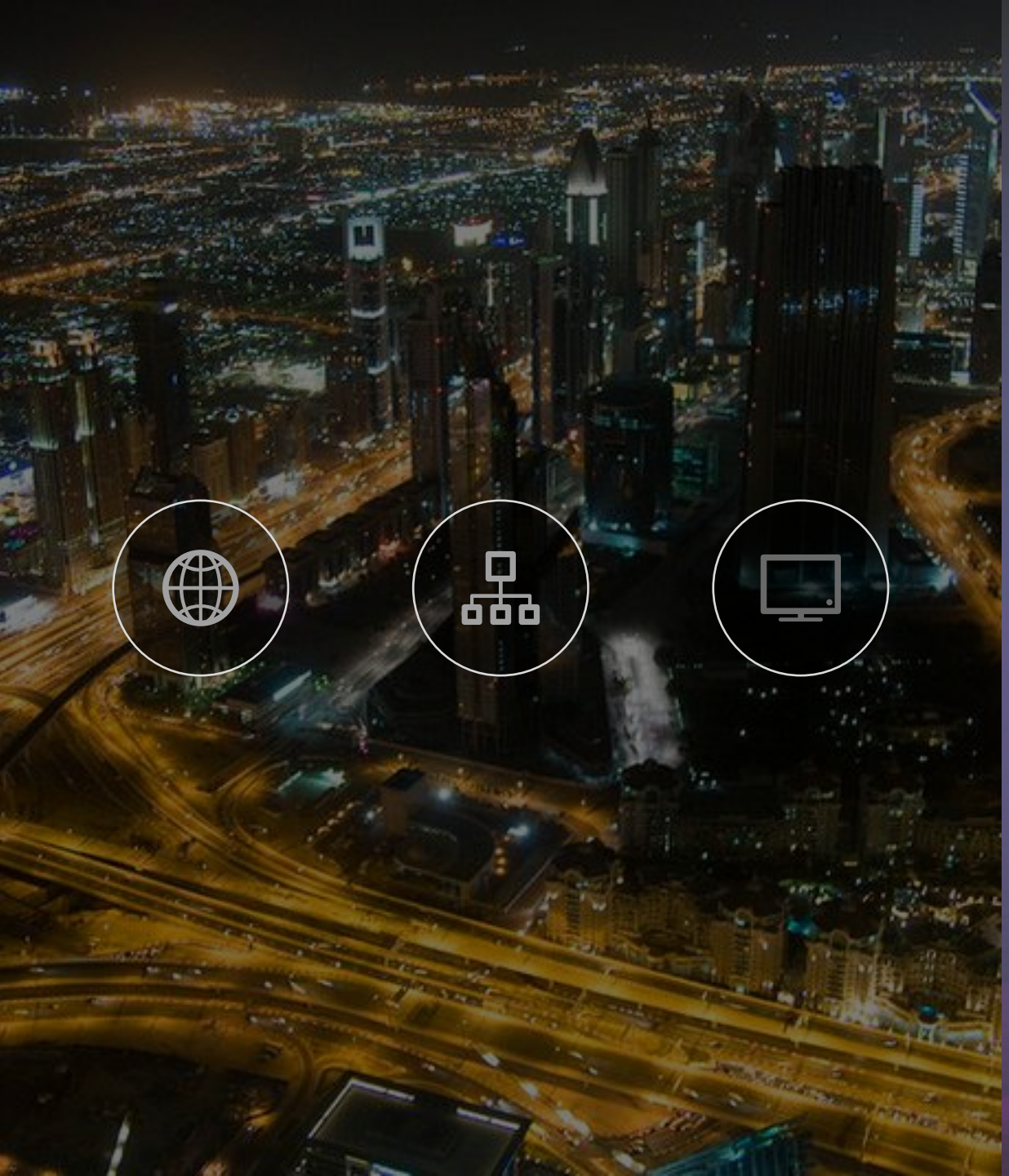
C3安全峰会
CYBER | CLOUD | COMMUNICATION

“永恒之蓝”事件警示与政务安全管理体系探讨

罗海龙
政府技术方案中心 副总经理



C3安全峰会
CYBER | CLOUD | COMMUNICATION

议题

01 永恒之蓝的启示

02 亚信安全的助力

03 亚信安全的政务安全实践

永恒之蓝 WannaCry/Wcry

- 2017年5月12日起，Wannacry 蠕虫勒索软件袭击全球网络
- 几小时内，全球近100多个国家，近万家组织和企业遭受攻击
- 英国国家医疗服务系统（NHS）遭到攻击，导致英国整个医院系统瘫痪
- 遭攻击电脑上文件被加密，需支付比特币解锁

我们的思考

技术层面的思考

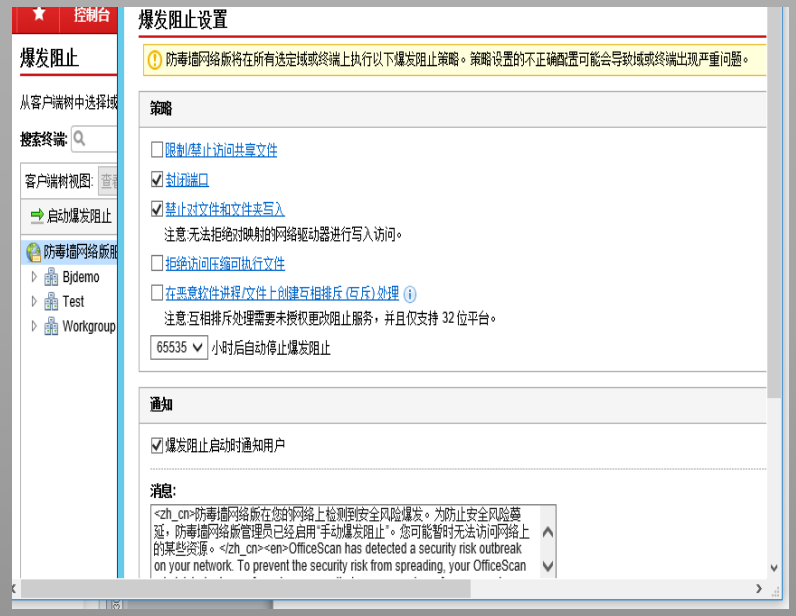
法律层面的思考

管理层面的思考

无法查杀的防护技术

F	G	H	I	J
日志类型	策略	主题	事件类型	目标
事件监控	未经授权的文件加密	c:\programc	文件系统	C:\Users\41710195\Desktop\2017年工作服发放全员尺寸统计表.xlsx
事件监控	未经授权的文件加密	c:\windows\	文件系统	C:\Users\41710195\Desktop\2017年工作服发放全员尺寸统计表.xlsx
事件监控	未经授权的文件加密	c:\programc	文件系统	C:\Users\41710195\Desktop\2017年工作服发放全员尺寸统计表.xlsx
事件监控	未经授权的文件加密	c:\programc	文件系统	C:\Users\41710195\Desktop\2017年工作服发放全员尺寸统计表.xlsx
事件监控	未经授权的文件加密	c:\programc	文件系统	C:\Users\41710195\Desktop\2017年工作服发放全员尺寸统计表.xlsx

出现病毒后的防护技术



阻止445、139、138等端口

拒绝病毒文件写入：
mssecsvc.exe
tasksche.exe b.wnry
c.wnry
r.wnry
s.wnry
t.wnry
u.wnry
Taskdl.exe
Taskse.exe

我们的思考

技术层面的思考

法律层面的思考

管理层面的思考

1. 个人信息保护	提出了个人信息保护的基本原则和要求,相当于一部小型的“个人信息保护法”,使后续的相关细则、标准有了上位法
2. 可信产品与服务	对网络产品和服务提供者提出了要求,针对的是当前一些企业任性停止服务或依靠垄断优势要挟用户、随意收集用户信息等问题
3. 实名登记	在电信用户实名制基础上,规定了信息发布、即时通讯等服务的实名制要求,但这个实名是指“前台匿名、后台实名”,不影响用户隐私
4. 网络安全信息发布	规范了重要网络安全信息的发布服务,现在很多企业或机构都在发布漏洞、安全事件等信息,有一些不实信息造成了很大范围的不良影响,国家将制定这方面的规定
5. 执法协助义务	明确了网络运营者的执法协助义务，并从法的层面规定了对网上非法信息的清理,使国家的互联网管理系统有了明确的法律依据
6. CII保护制度	确立了国家关键信息基础设施保护制度,特别是规定了运营者的强制性义务,并为主管部门开展监管作了授权
7. 应急响应体系	建立了网络安全监测预警、信息通报和应急处置工作体系,有利于解决目前存在的多个部门各自发布预警通报、应急预案体系不完整不协调等问题.
8. 通讯管制制度	建立了通信管制制度,以支持重大突发事件的处置,但同时也将通信管制的权限严格限制在了国务院
9. 网络安全工作体制	进一步理顺了网络安全工作体制,规定国家网信部门负责统筹协调网络安全工作和相关监督管理工作

不合规将导致

- 罚款
- 暂停运营
- 吊销营业执照
- 刑事处罚

我们的思考

C3安全峰会
CYBER | CLOUD | COMMUNICATION

技术层面的思考

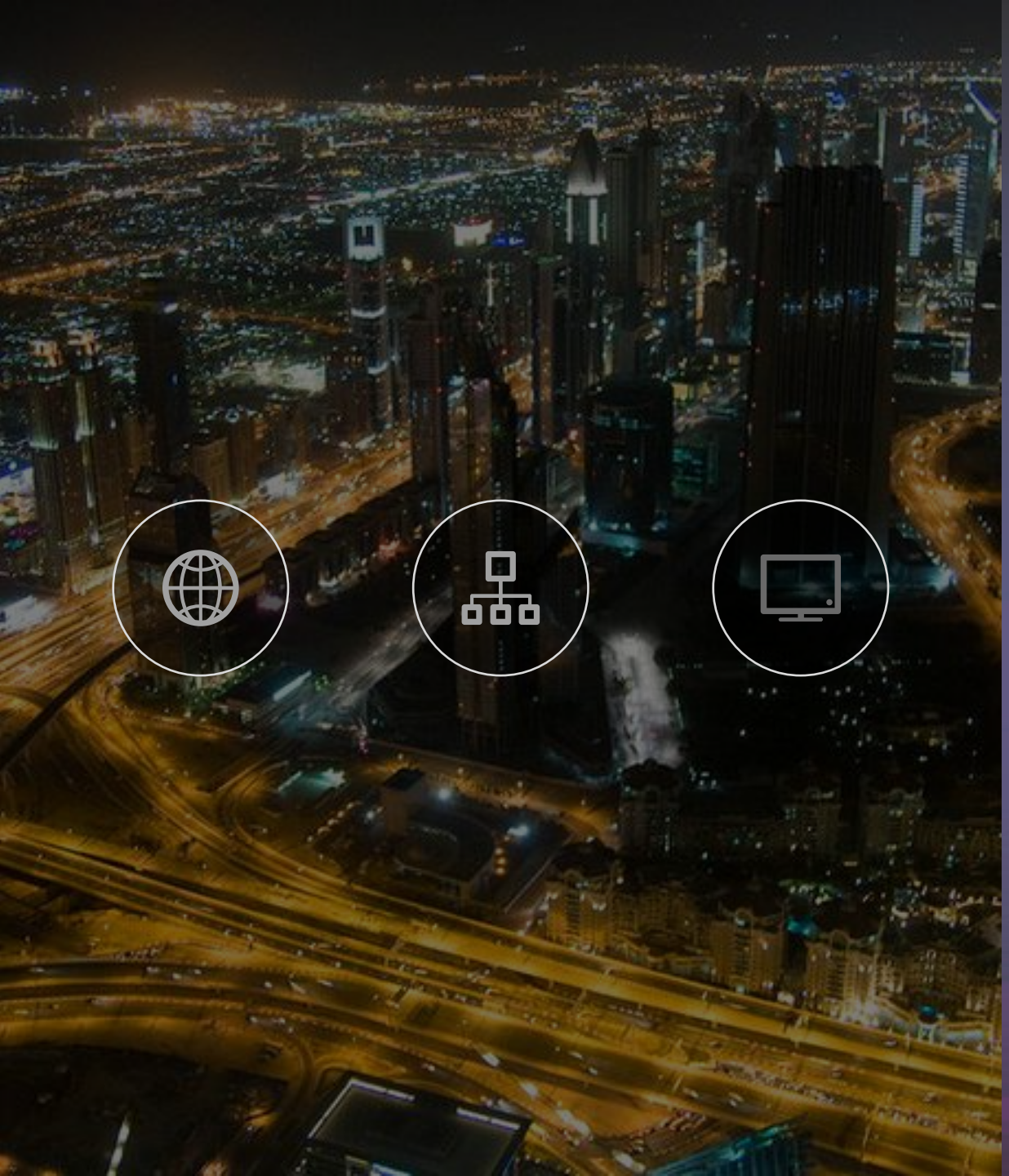
法律层面的思考

管理层面的思考

《国家网络安全事件应急预案》

事件分级	预警响应	应急处置
• 特别重大网络安全事件 • 重大网络安全事件 • 较大网络安全事件 • 一般网络安全事件	• 红色预警响应 • 橙色预警响应 • 黄色、蓝色预警响应 • 预警解除	• 事件报告 • 应急响应：I级响应、II级响应、III、IV级响应 • 应急结束

预防工作	保障措施	
• 日常管理 • 演练 • 宣传 • 培训 • 重要活动期间的预防措施	• 机构和人员 • 技术支撑队伍 • 专家队伍 • 社会资源 • 技术研发和产业促进	• 国际合作 • 物资保障 • 经费保障 • 责任与奖惩



C3安全峰会
CYBER | CLOUD | COMMUNICATION

议题

01 永恒之蓝的启示

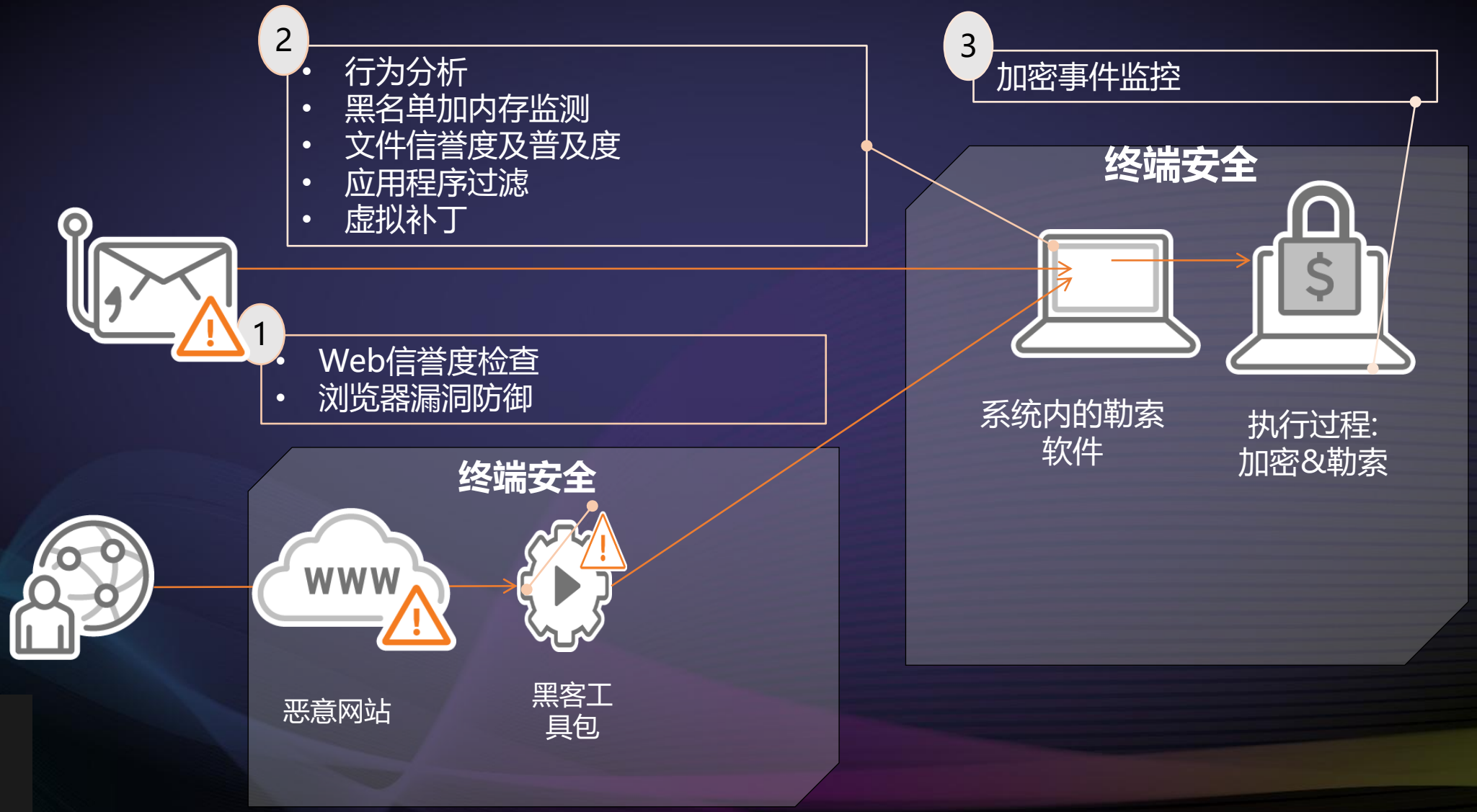
02 亚信安全的助力

03 亚信安全的政务安全实践

亚信安全技术能力

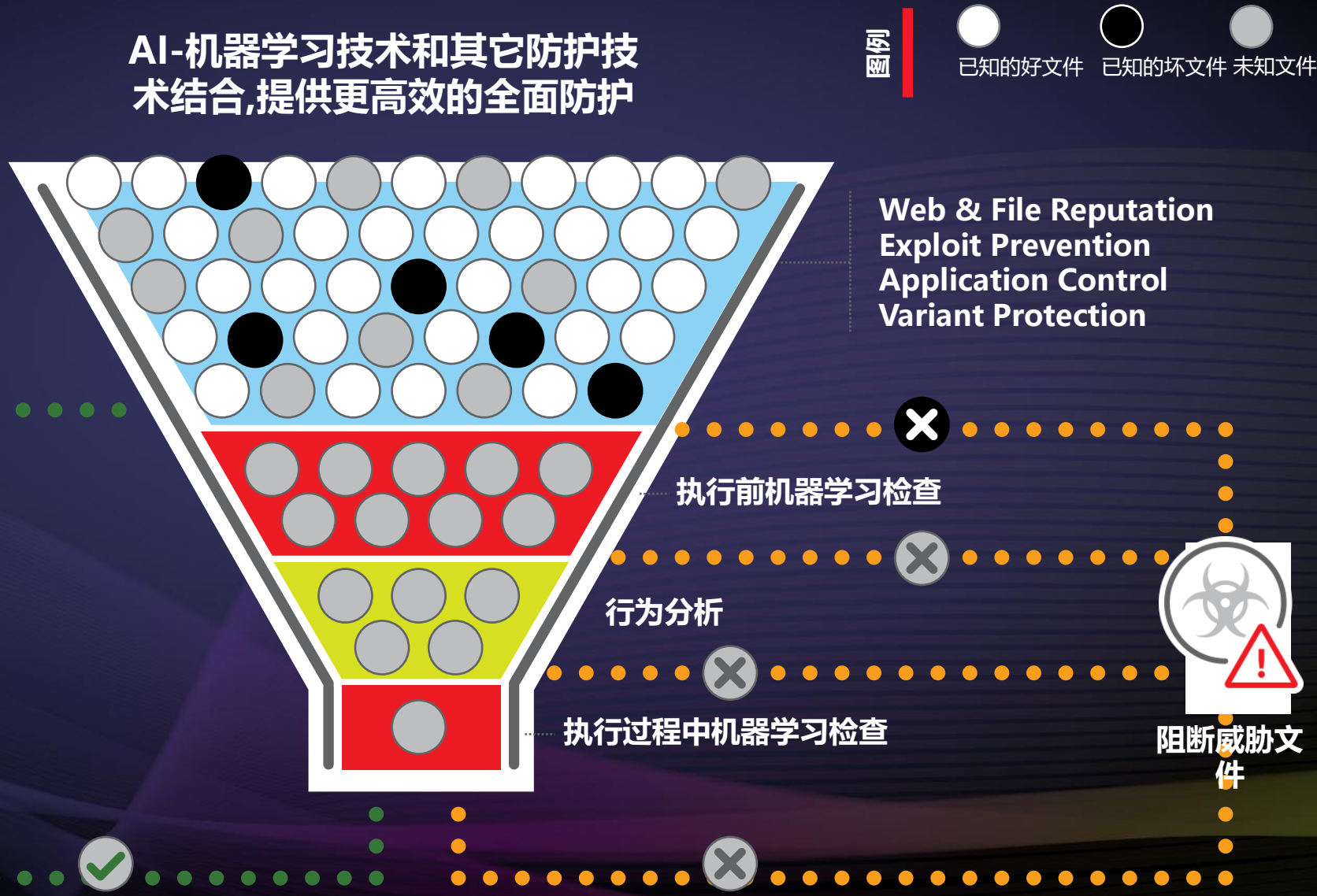

安全态势感知
安全审计分析
数据泄露防护
应用过程控制
恶意软件检测
身份与访问控制
云与虚拟化安全
APT治理
沙盒分析
IPS引擎
MDM
SaaS
URL过滤
协议分析
Web信誉
全天候SLA
大数据安全
移动安全办公
虚拟补丁技术
文件信誉侦测
电子邮件信誉
安全运维管控

勒索软件防御技术


2
行为分析
黑名单加内存监测
文件信誉度及普及度
应用程序过滤
虚拟补丁
3
加密事件监控
终端安全
1
Web信誉度检查
浏览器漏洞防御
系统内的勒索软件
执行过程:
加密&勒索
终端安全
WWW
恶意网站
黑客工具包

新一代终端防病毒技术

AI-机器学习技术和其它防护技术结合,提供更高效的全面防护

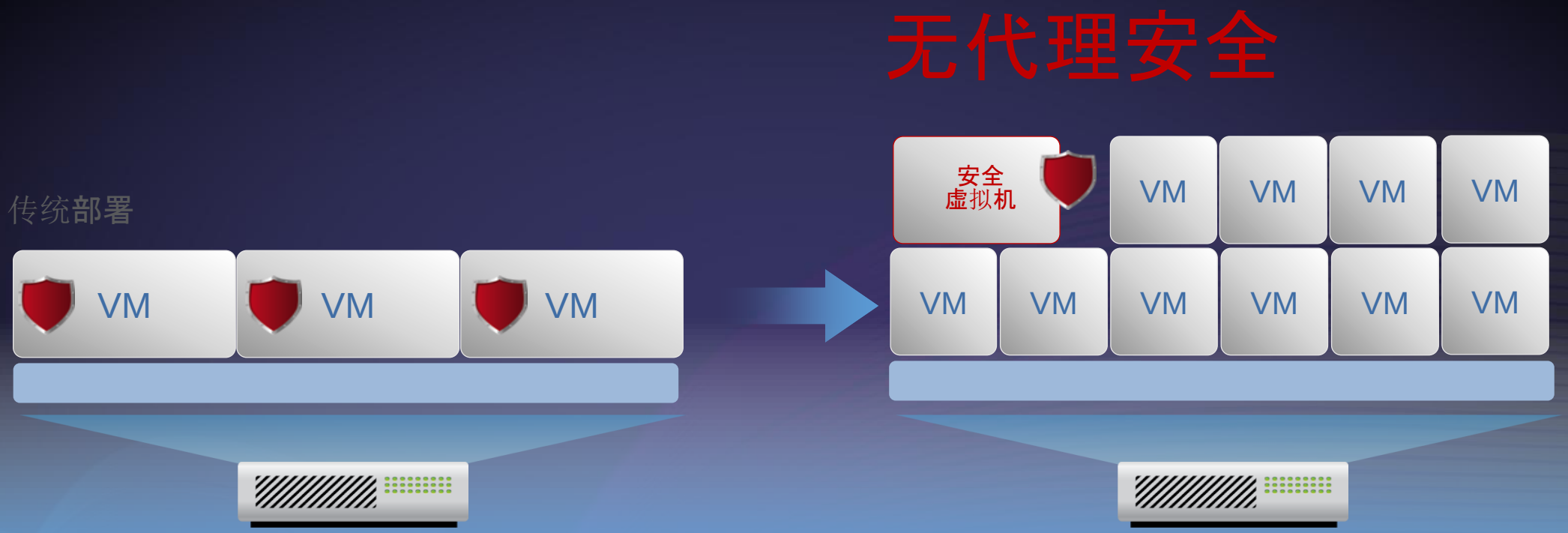


手机虚拟化技术

数据不落地

数据安全	手机本地完全没有应用数据
终端安全	移动应用安装文件不需要被下载，避免了移动应用漏洞被利用的风险
应用开发	不需要开发多平台APP，降低开发成本
网络安全	网络中传输显示信息，网络劫持无意义

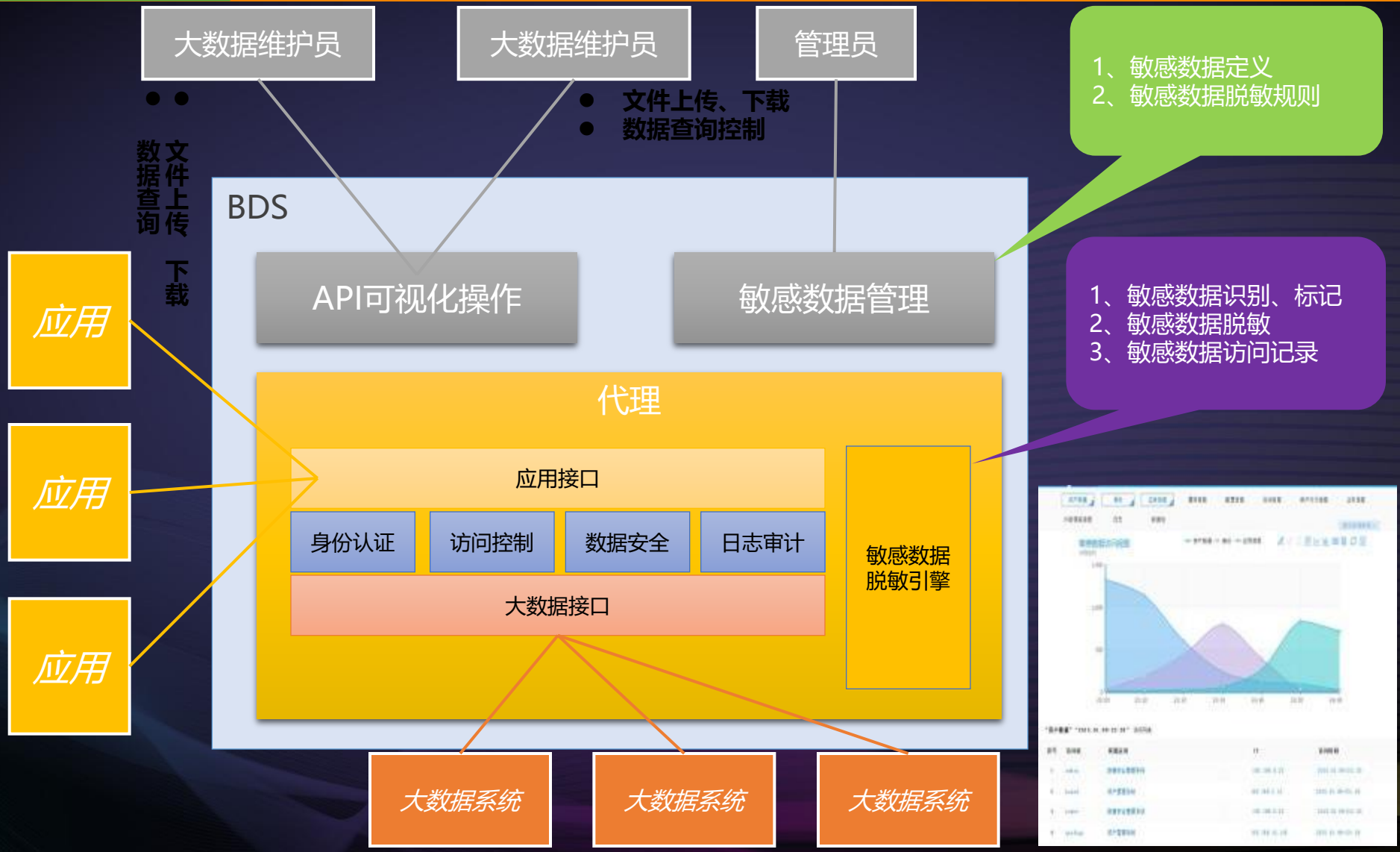
云安全无代理技术



VMware 环境的无代理安全 — 防病毒之外，其他的安全防护

- 防病毒
- 完整性监控
- 入侵检测
- 虚拟补丁
- 防火墙
- Web 应用防护

大数据安全技术


大数据维护员
大数据维护员
管理员
文件上传、下载
数据查询控制
数据查询
文件上传
下载
1、敏感数据定义
2、敏感数据脱敏规则
BDS
API可视化操作
敏感数据管理
1、敏感数据识别、标记
2、敏感数据脱敏
3、敏感数据访问记录
应用
应用
应用
代理
应用接口
身份认证
访问控制
数据安全
日志审计
大数据接口
敏感数据脱敏引擎
大数据系统
大数据系统
大数据系统

网络安全取证技术

API 接口

告警和报表系统

威胁智能建模

大数据分析和存储

Hadoop & ElasticSearch

态势感知与安全运维
服务监控/管理

管理界面

SIEM/SOC

第三方厂商

脆弱性发现取证

Web应用防护

分布式拒绝攻击防护

其它威胁发现取证

AsiaInfo

亚信安全
云端威胁情报

网络威胁发现取证

终端威胁发现取证

沙盒分析

事件日志Win/Linux

高级威胁知识库

告警规则编写和更新

安全事件调查分析过程描述

社会工程学邮件攻击检测技术

C3安全峰会
CYBER | CLOUD | COMMUNICATION

亚信安全深度威胁邮件网关DDEI

检测 — 分析 — 阻止

邮箱安全设备

- 附件分析及沙箱技术
- URL分析及沙箱技术
- 邮件策略控制
- 威胁分析

NSS 推荐

最优攻击检测

亚信安全深度威胁解决方案

NSS Labs 2014/2015 攻击检测测试

管理和部署 ▶ MTA（阻止）、BCC（监控）及SPAN/TAP（监控）部署模式可与任何现存邮件安全解决方案协同工作

IOC共享 ▶ 新的威胁标识（IOC）数据可以分享给亚信安全及第三方产品，用以阻止威胁

附件分析 ▶ 使用多个检测引擎和定制化沙箱检测附件，包括多种 Windows 可执行文件、Microsoft Office、PDF、Zip、Web内容和压缩文件类型

智能文件解密 ▶ 使用多种启发式密码提取技术对密码保护的文件附件或压缩附件进行解密

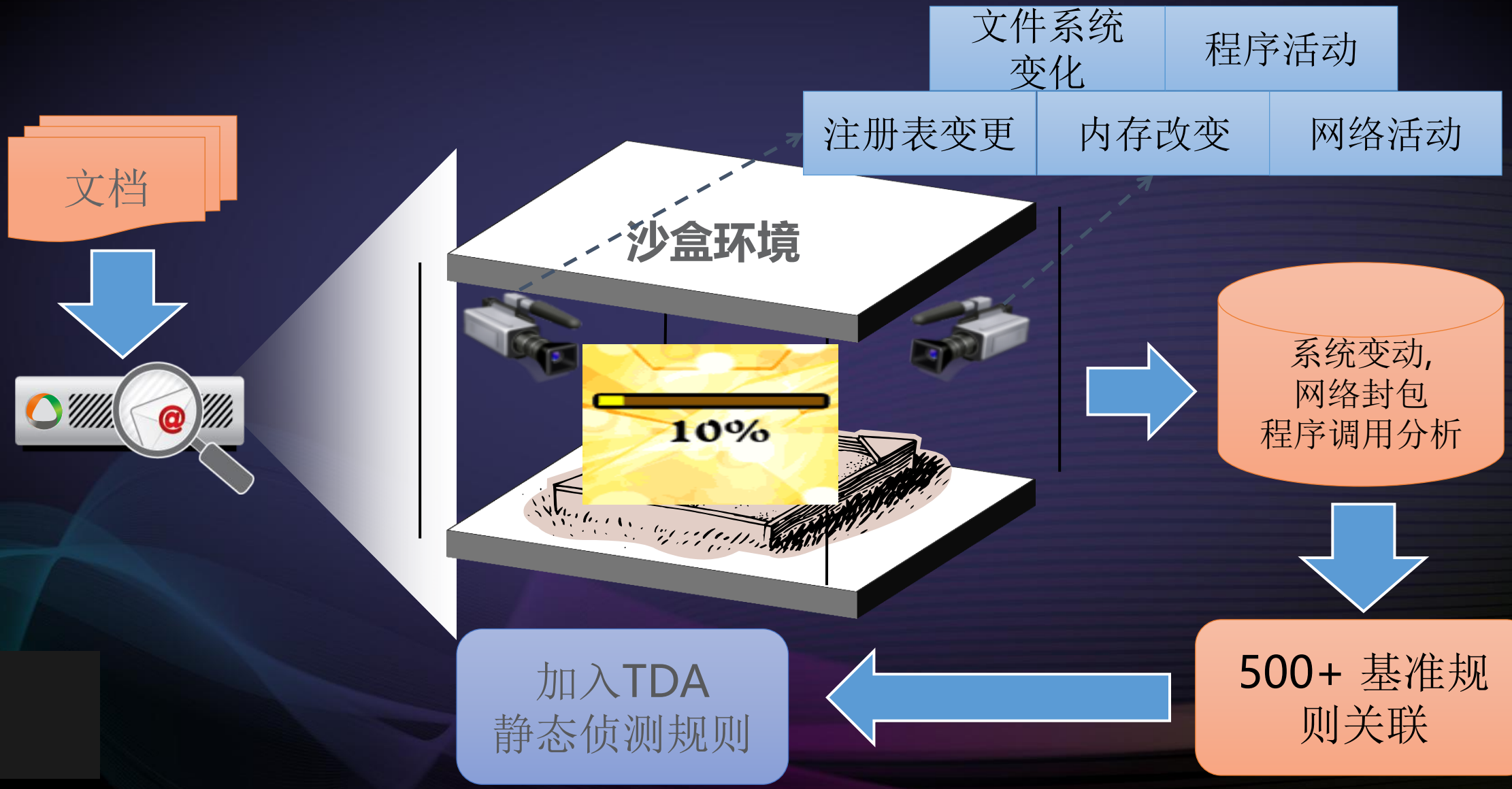
嵌入式URL分析 ▶ 多级嵌入式 URL 分析通过web信誉检查、内容分析和沙箱模拟可识别嵌入在社交工程钓鱼邮件以及文档附件中的恶意URL，必要时对目标内容进行扫描和沙箱分析，发现隐蔽下载中使用的重定向、高级恶意软件和漏洞

定制化沙箱 ▶ 定制化的沙箱可模拟与您桌面系统精确匹配的运行环境，准确地检测到针对贵公司的恶意软件

威胁分析 ▶ 详细的沙箱分析可用于深入威胁研究。此外，亚信安全云安全威胁百科门户提供了相关的趋势科技全球情报，可用于评估攻击的风险和起源

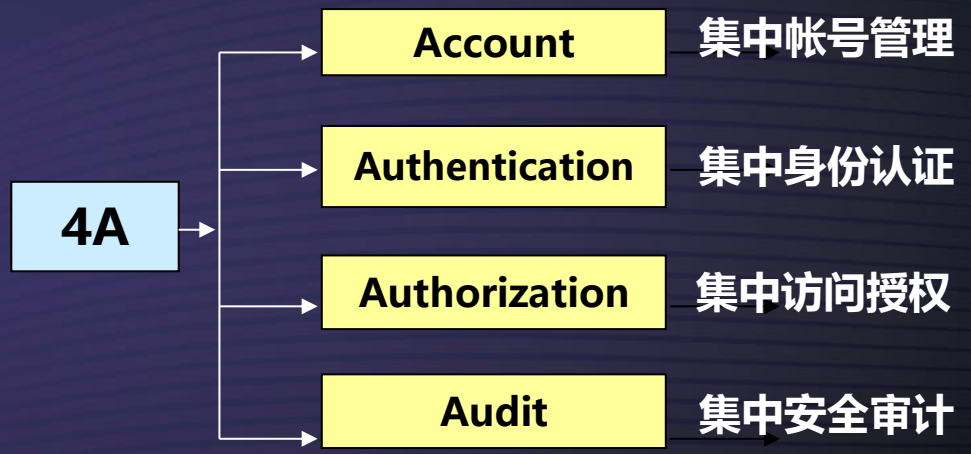
策略控制 ▶ 根据告警严重性级别，您可以配置多种选项来处理恶意邮件，包括隔离、删除和带标记转发邮件等操作。邮件的沙箱分析可以按附件类型自定义控制（例如，对所有的 PDF文件进行沙箱分析）

仿真分析系统


文件系统变化
程序活动
注册表变更
内存改变
网络活动
文档
沙盒环境
10%
系统变动,
网络封包
程序调用分析
500+ 基准规则关联
加入TDA
静态侦测规则

4A管理平台

4A安全支撑平台作为安全架构中的基础安全服务系统，侧重于用户安全层面实现统一访问控制、帐号管理、授权管理、密码管理、身份认证、数据安全与审计，提升IT系统安全性和可管理能力。

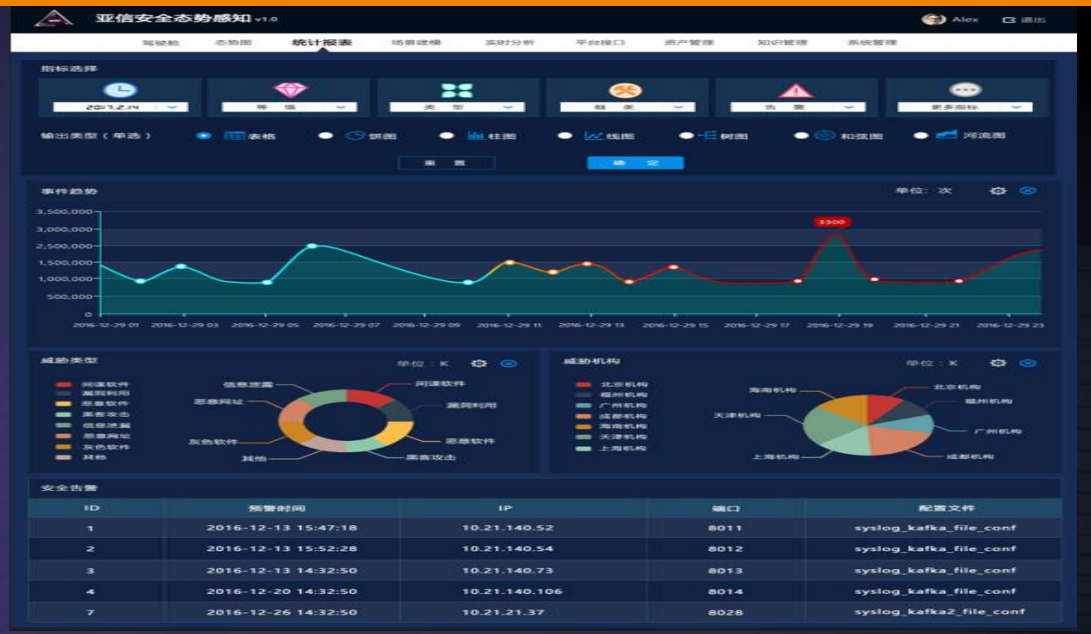


业务价值：

- 落实国内外以及企业的安全政策，降低安全事件的影响
- 降低日常安全管理工作压力，提升安全管理效率
- 安全、高效的使用各类IT资源，降低操作复杂度

网络安全态势感知技术

- **安全六段论：**
  支持分阶段划分攻击事件，包括侦查、投放、利用、安装、控制、攻击等阶段。
- **多源关联分析：**
  支持多数据源的关联分析。能够定义关联规则，把威胁、事件、资产之间日志关联起来进行分析。
- **离线机器学习：**
  支持对历史数据的分析功能，提供离线数据分析能力。
- **拓扑跟踪与溯源：**
  准确定位安全事件发生位置，快速锁定结症所在。



亚信安全服务能力

- 网络安全咨询服务
- 网络安全运维服务
- 应急响应服务
- 攻防演习
  - 演习规划
  - 实战演练
- 专业培训
  - 攻防培训
  - 专业认证

EOG 专家值守服务

MOC支持

- MOC工程师服务
- 7*24小时服务
- 产品使用咨询
- 病毒问题处理

TMSN现场服务

亚信安全在全国有授权服务商网络，可以提供本地化的安全工程师紧急现场服务

风险管理

- TMIC病毒监测
- 安全指标监控
- 日报月报分析
- 高危病毒通知

PSP 企业专属咨询服务

完善体系

- 流程制定
- 人员职责分配
- 体系规划
- 策略规划
- 新产品咨询建议

保障业务连续性

- 专属TAM+7*24支持
- 紧急现场服务
- 定期巡检服务
- PSC在线事件系统
- 病毒应急响应

知识转移

- ACSE培训
- 现场技术培训
- 安全小贴士
- 病毒预警
- 重大安全事件分享

体现业务价值

- KPI创建
- 绩效跟踪及总结
- 安全日志分析
- 前十位病毒分析
- 详尽的整体安全报告

驻点服务

- 专属驻点+5*8支持
- 监控安全威胁
- 现场响应安全事件
- 提供产品维护及支持

SLA服务

当新病毒攻击发生,我们承诺在两个小时之内提供解药(7*24)，并提供快速响应品质担保(SLA)

ACSE 培训及教育服务

安全专家培训

提供在线精要课程培训及TCSE安全专家认证

人员安全意识教育

针对最新安全问题，每月提供安全意识小贴士，提升员工的安全意识

反钓鱼服务

钓鱼网站监测

- 7×24小时钓鱼网站监测服务
- 及时的反馈到中国反钓鱼联盟中心
- 提供每日反钓鱼监测报表

钓鱼网站取证

- 对每个钓鱼网站制作取证表，内容包括相关网址和截图信息
- 汇总月度的钓鱼网站信息，总结钓鱼的攻击方式

亚信安全网络安全监测实验室

C3安全峰会
CYBER | CLOUD | COMMUNICATION

亚信安全病毒监控中心

亚信安全在北京、上海、广州构建销售平台中心，并在上海设技术服务中心、在天津设病毒处理中心、在南京设研发中心，在成都建立网络安全产业技术研究院，是惟一在国内构建有五大中心的防毒厂商。亚信科技配合病毒监控服务，分别在北京、天津和上海构建计算机病毒监控运营中心，为用户提供7×24小时不间断监控服务。

亚信网络安全产业技术研究院

C3安全峰会
CYBER | CLOUD | COMMUNICATION

产 HUAWEI Lenovo inspur 浪潮 H3C 中科曙光 Sugon 中科睿光 SVM

学 北京大学 PEKING UNIVERSITY 信息工程大学 北京邮电大学 哈尔滨工业大学 电子科技大学 四川大学

研 CNCERT/CC 国家互联网应急中心 国家信息中心 公安部信息安全等级保护评估中心 VERC 国家计算机病毒应急处理中心 中国科学院信息工程研究所 IACAS 中科院声学所 ICT

研究院学术委员会

- 院士领衔
- 科研院所专家
- 主管部门专家
- 行业专家

建设国际一流安全实验室

- 网络空间平安城市实验室
- 云安全实验室
- 大数据安全实验室
- 工业互联网安全实验室

技术转移与成果转化基金

成都网络安全态势感知平台建设内容

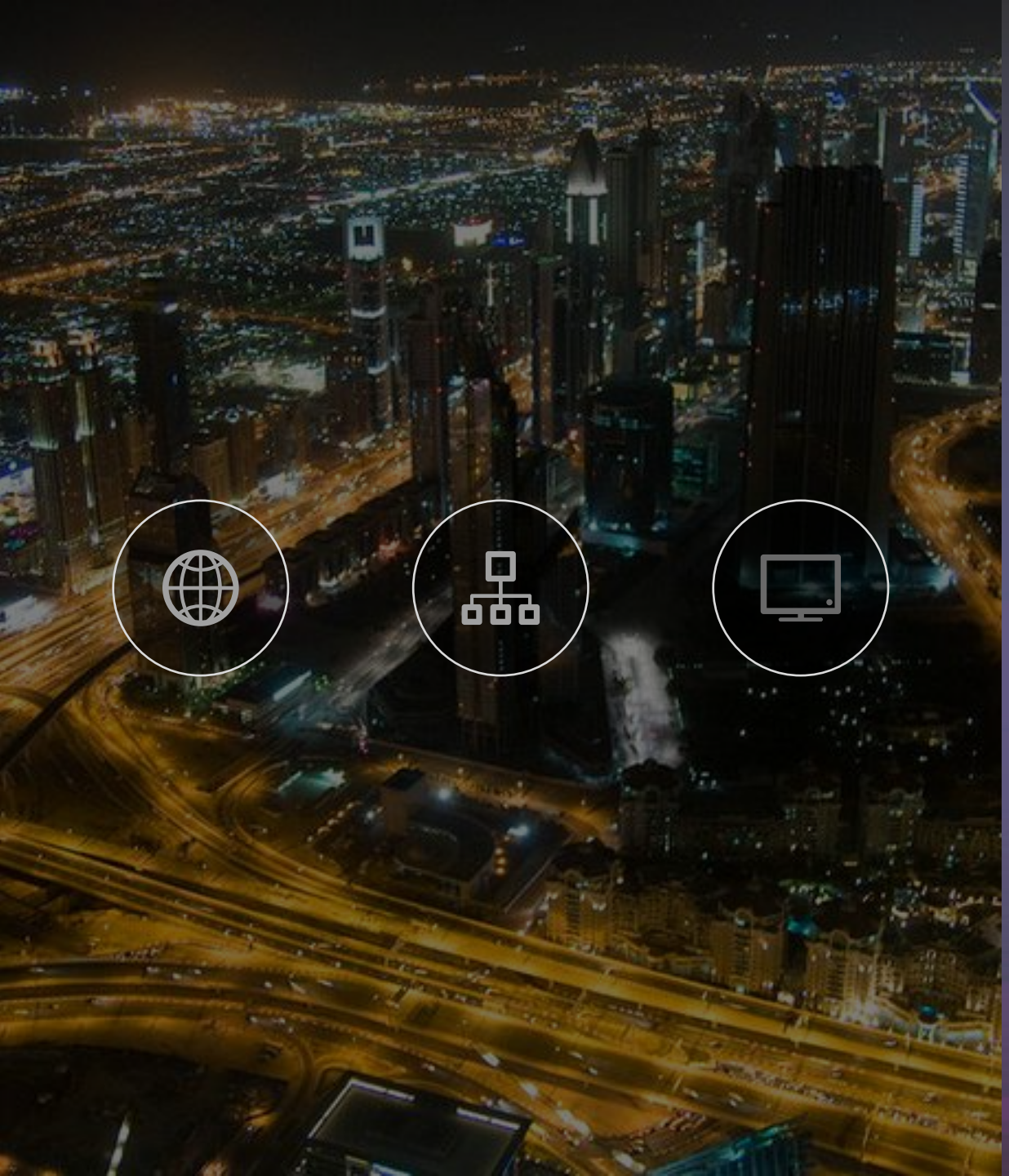
C3安全峰会
CYBER | CLOUD | COMMUNICATION

知己知彼，
百战不殆

调查取证，
研判处置

攻防演练，
培养人才

公众教育，
安全意识



C3安全峰会
CYBER | CLOUD | COMMUNICATION

议题

01 永恒之蓝的启示

02 亚信安全的助力

03 亚信安全的政务安全实践

网络空间平安城市的总体架构

C3安全峰会
CYBER | CLOUD | COMMUNICATION

网络安全公众教育与培训中心

公众教育基地

宣传机制

面向各单位的网络安全知识与技能培训

网络安全态势感知中心

网络安全事件通报应急处置平台

重大网络安全事件指挥调度系统

网络安全事件通报处置

网络安全案件侦察调查和情报挖掘系统

网络安全综合防控平台

智慧城市网络安全中心

应用安全

主机安全

数据安全

网络安全

4A认证授权审计平台

云计算安全

大数据安全

智慧医疗

智慧交通

数字城管

智慧政务

。。。

网络反欺诈中心

域名防欺诈

网页防篡改

恶意域名探测

监控警告

网站备案管理

域名防劫持

域名安全数据中心

数据源

数据源

数据源

网络安全公共服务中心

网站安全监控

文件病毒检测

App安全检测

资产威胁检测

DRLN

等保管理及服务

安全DNS云服务

安全信息发布

运营服务支撑平台

网络安全威胁调查取证中心

网络安全威胁调查取证平台

主机取证

网络取证

沙盒分析

专人服务

事件处置

流程完善

网络安全专家服务

物联网安全

感知层安全

设备准入

设备识别

网络层安全

设备定位

攻击检测

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You