WTC IV
网络安全冬训营

面向新兴威胁的终端防护技术

安天 端点安全研发部 徐翰隆

有效防护，价值输出

安天 | 智者安天下

课程提纲Contents

- 终端安全面临的挑战
- 安天智甲终端防御系统
- 终端安全技术发展路线

PC终端是关键基础设施防御的焦点

从震网到乌克兰停电

勒索者病毒的兴起

银行ATM频遭攻击

	2010年震网事件	2015年乌克兰变电站事件
主要目标	伊朗核工业设施	乌克兰电力系统
作用目标	上位机（Windows） PLC控制系统、WinCC	上位机（Windows） 办公机（Windows）
造成后果	大大延迟了伊朗的核计划	乌克兰大面积停电
使用漏洞	MS10-046等多个0day漏洞	未发现
数字签名	盗用了其他厂商的数字签名	未使用数字签名
通讯与控制	高度严密的加密通讯、控制体系	相对比较简单
抗分析能力	高强度本地加密，复杂调用机制	相对比较简单，易于分析
攻击成本	超高开发成本，超高维护成本	相对较低

引自安天技术报告《乌克兰电力系统遭受攻击事件综合分析报告》，2016年1月21日首发

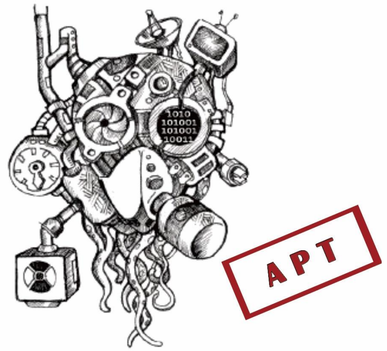
PC终端作为APT攻击的关键目标，同时也将是抵御攻击最后的防线

安天持续跟踪分析数十个APT组织的行动线索

安天网络安全冬训营第四期

安天针对“震网“事件的系列分析报告

安天安全研究与应急处理中心(Antiy CERT)

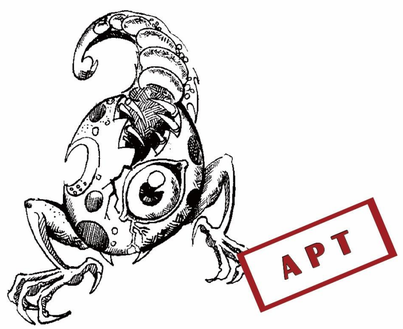


首篇发布时间：2010 年 09 月 27 日

最后发布时间：2012 年 12 月 07 日

乌克兰电力系统遭受攻击事件综合分析报告

联合编写：哈尔滨安天科技股份有限公司、北京四方继保自动化股份有限公司、
复旦大学网络空间治理研究中心



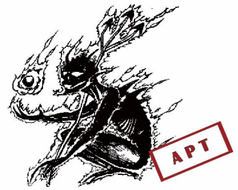
初稿完成时间：2016 年 1 月 18 日 17 时 30 分

首次发布时间：2016 年 1 月 21 日 14 时 30 分

本版更新时间：2016 年 2 月 24 日 11 时 30 分

Flame 蠕虫样本集分析报告

安天安全研究与应急处理中心(Antiy CERT)

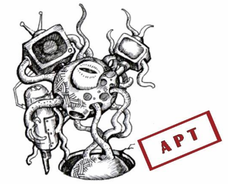


首次发布时间：2012 年 5 月 31 日

本版更新时间：2012 年 8 月 17 日

Duqu 和 Stuxnet 同源性分析系列报告

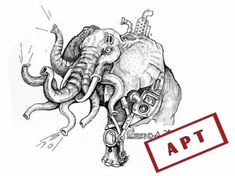
安天安全研究与应急处理中心(Antiy CERT)



首次发布时间：2012 年 5 月

白象的舞步——来自南亚次大陆的网络攻击

安天安全研究与应急处理中心(Antiy CERT)



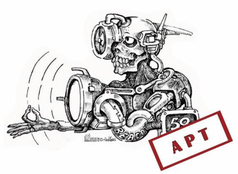
初稿完成时间：2016 年 07 月 04 日 17 时

首次发布时间：2016 年 07 月 10 日 10 时

本版更新时间：2016 年 07 月 10 日 10 时

一例针对中国政府机构的准 APT 攻击中所使用的样本分析

安天安全研究与应急处理中心(Antiy CERT)



首次发布时间：2015 年 05 月 27 日

本版更新时间：2015 年 05 月 27 日

沙虫(CVE-2014-4114)相关威胁综合分析报告

——及对追影安全平台检测问题的复盘

安天安全研究与应急处理中心（Antiy CERT）

首次发布时间：2014 年 10 月 15 日 21 时 40 分

本版更新时间：2014 年 10 月 24 日 14 时 30 分

安天针对“方程式”组织的系列分析报告

安天安全研究与应急处理中心(Antiy CERT)

首次发布时间：2015 年 3 月 5 日

最新更新时间：2015 年 4 月 16 日

有效防护 价值输出

安天 | 智者安天下

从震网到乌克兰停电

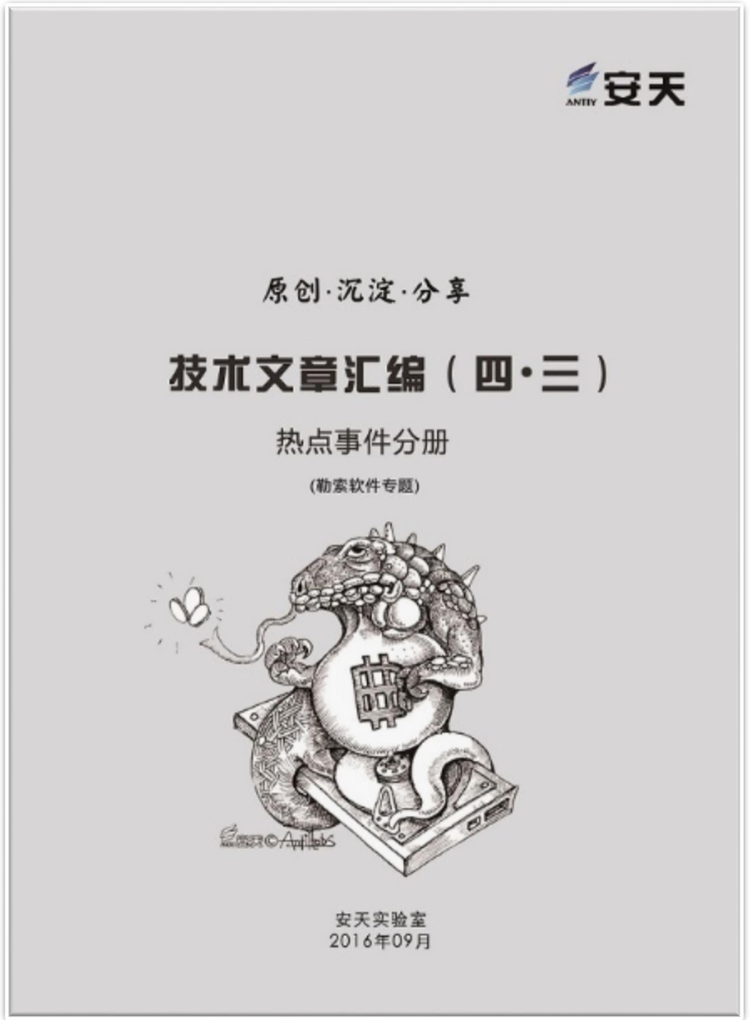
勒索者病毒的兴起

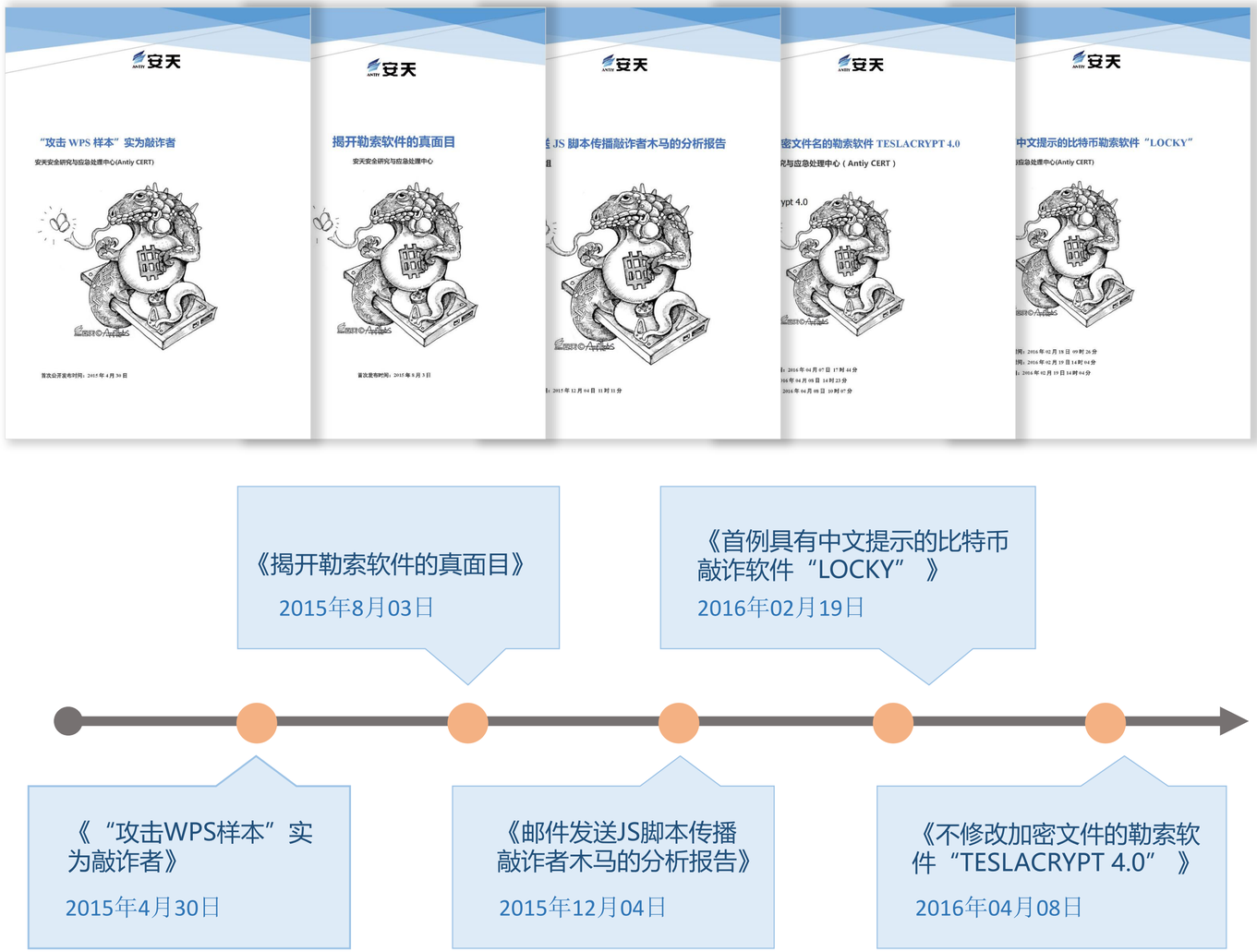
银行ATM频遭攻击

勒索者病毒兴起的原因

- 专门针对文档，**常规防护方式很难抵御**
- 借助比特币匿名支付和匿名网络，**获利风险低**
- 如果不支付赎金，被加密的文档**基本没有恢复的可能**

安天在国内较早的专门针对“勒索者”发布分析报告并持续跟进





有效防护 价值输出

看似安全的专用设备终端，面临着更大的安全威胁

从震网到乌克兰停电

勒索者病毒的兴起

银行ATM频遭攻击

最早从2008年开始

- **利用ATM skimmers(ATM分离器)**
- 全球超过十亿美元被窃取
- 需要物理入侵ATM

2016.7 台湾银行

- **通过植入恶意软件控制吐钞**
- 34台ATM，总计7000万新台币

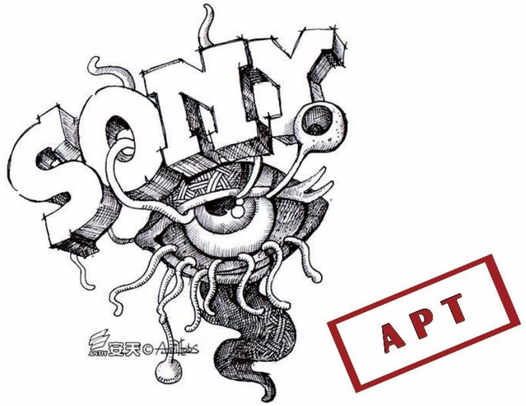
2016.8 泰国银行

- **恶意软件控制银行卡读写设备**
- 约1000台ATM，总计1200万泰铢

安天

索尼等攻击事件中具有破坏 MBR 功能样本的同源性分析报告

安天安全研究与应急处理中心(Antiy CERT)



首次发布时间：2015 年 1 月 8 日

本版更新时间：2015 年 1 月 15 日

安天

IoT 僵尸网络严重威胁网络基础设施安全

——北美 DNS 服务商遭 MIRAI 木马 DDOS 攻击的分析思考

安天实验室

初稿完成时间：2016 年 10 月 23 日 00 时 47 分

首次发布时间：2016 年 10 月 24 日 9 时 30 分

本版更新时间：2016 年 10 月 24 日 9 时 30 分

国产化操作系统带来新的防御空白点

- 针对国产系统的病毒很多都是**代码开源**的
- Linux漏洞很容易在国产系统中被复用，**且修复周期更滞后**
- **多种硬件架构和系统版本**，实时防御模块适配难度大
- 相对于Windows系统，国产系统防病毒**体系尚不成熟**

中标麒麟 NeoKylin

银河麒麟 KYLIN

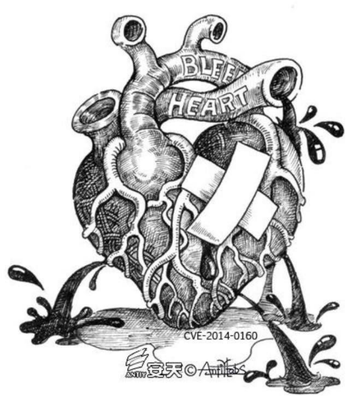
德 NFS-China

安天针对Linux和国产系统病毒和漏洞的分析

安天

Heartbleed 漏洞（CVE-2014-0160）FAQ

安天安全研究与应急处理中心(Antiy CERT)



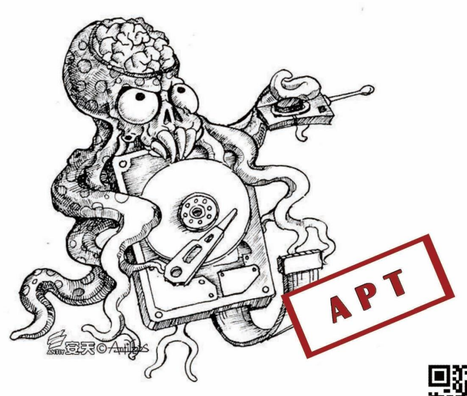
首次发布时间：2014 年 4 月 13 日

安天

从“方程式”到“方程组”

EQUATION 攻击组织高级恶意代码的全平台能力解析

安天安全研究与应急处理中心（Antiy CERT）



初稿完成时间：2014 年 1 月 15 日 16 时 43 分
首次发布时间：2016 年 11 月 4 日 10 时 00 分
本版更新时间：2016 年 11 月 5 日 15 时 30 分

安天

“破壳”漏洞(CVE-2014-6271)综合分析

——“破壳”漏洞系列分析之一

安天安全研究与应急处理中心(Antiy CERT)

首次发布时间：2014 年 9 月 25 日

安天

“破壳”漏洞相关恶意代码样本分析报告

——“破壳”漏洞系列分析之二

安天安全研究与应急处理中心(Antiy CERT)

首次发布时间：2014 年 9 月 29 日
本版更新时间：2014 年 10 月 19 日

安天

“破壳”漏洞的关联威胁进化与类 UNIX 系统的恶意代码现状

——“破壳”漏洞系列分析之三

安天安全研究与应急处理中心(Antiy CERT)

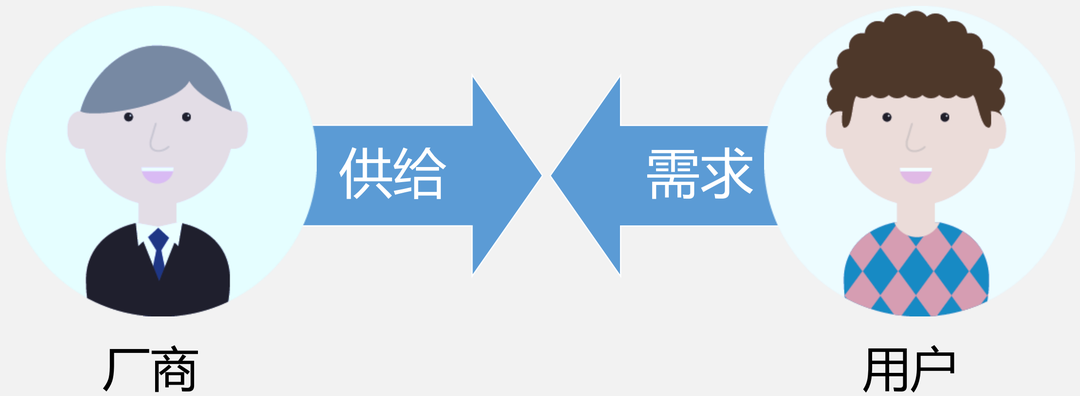
首次发布时间：2014 年 10 月 09 日
本版更新时间：2014 年 10 月 14 日

方程式已经针对各种操作系统（包括例如Solaris和Linux）准备好了对应的病毒版本

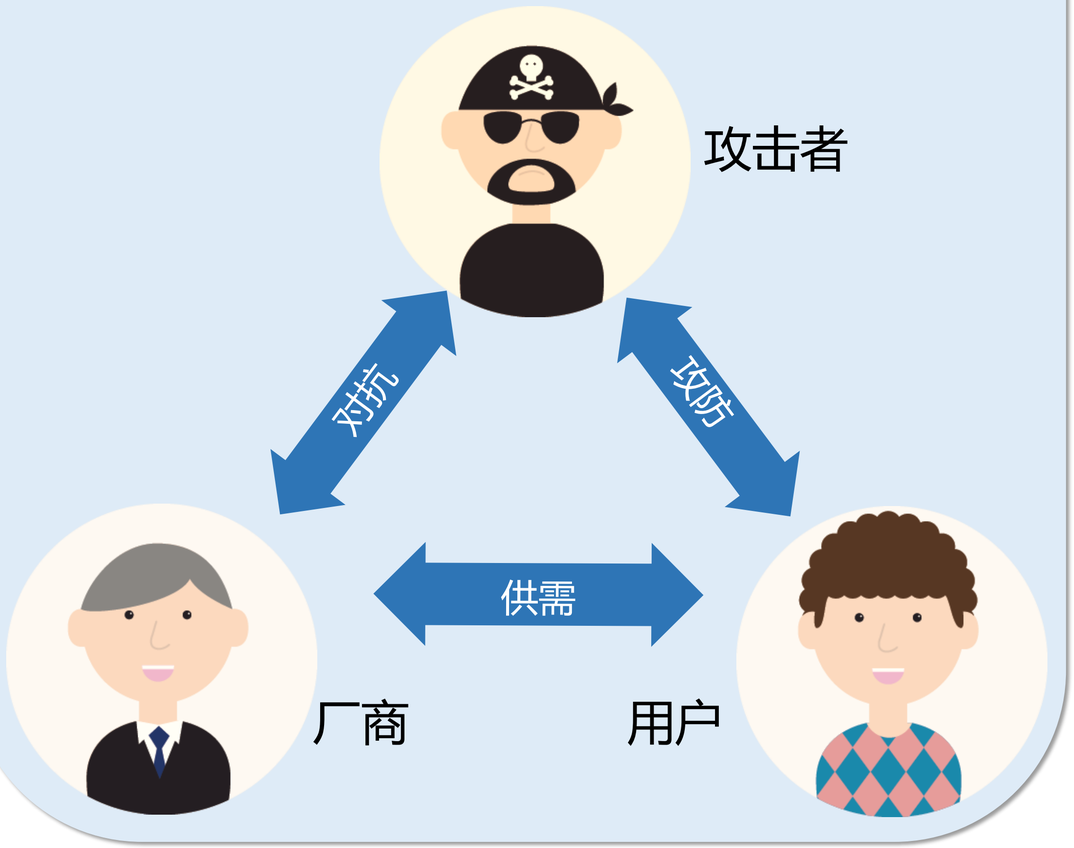
有效防护 价值输出

网络安全与传统领域的规律差异

传统领域



安全领域



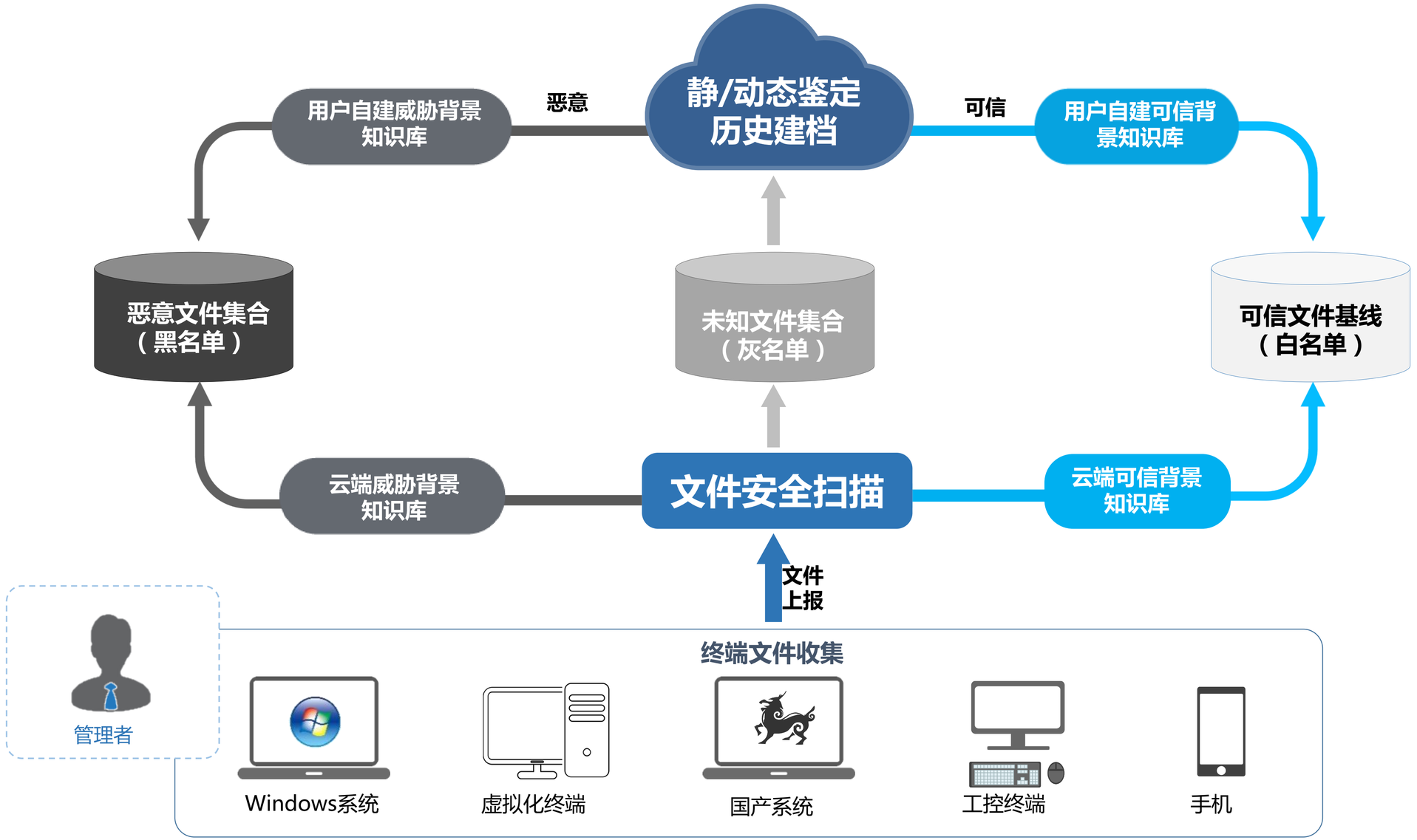
安天智甲终端防御系统三要素

以本地引擎和云查杀技术为基础，同时也支持未知程序的发现与防御。

除具有传统反病毒产品功能外，还具有纵深防御能力以应对新兴威胁。

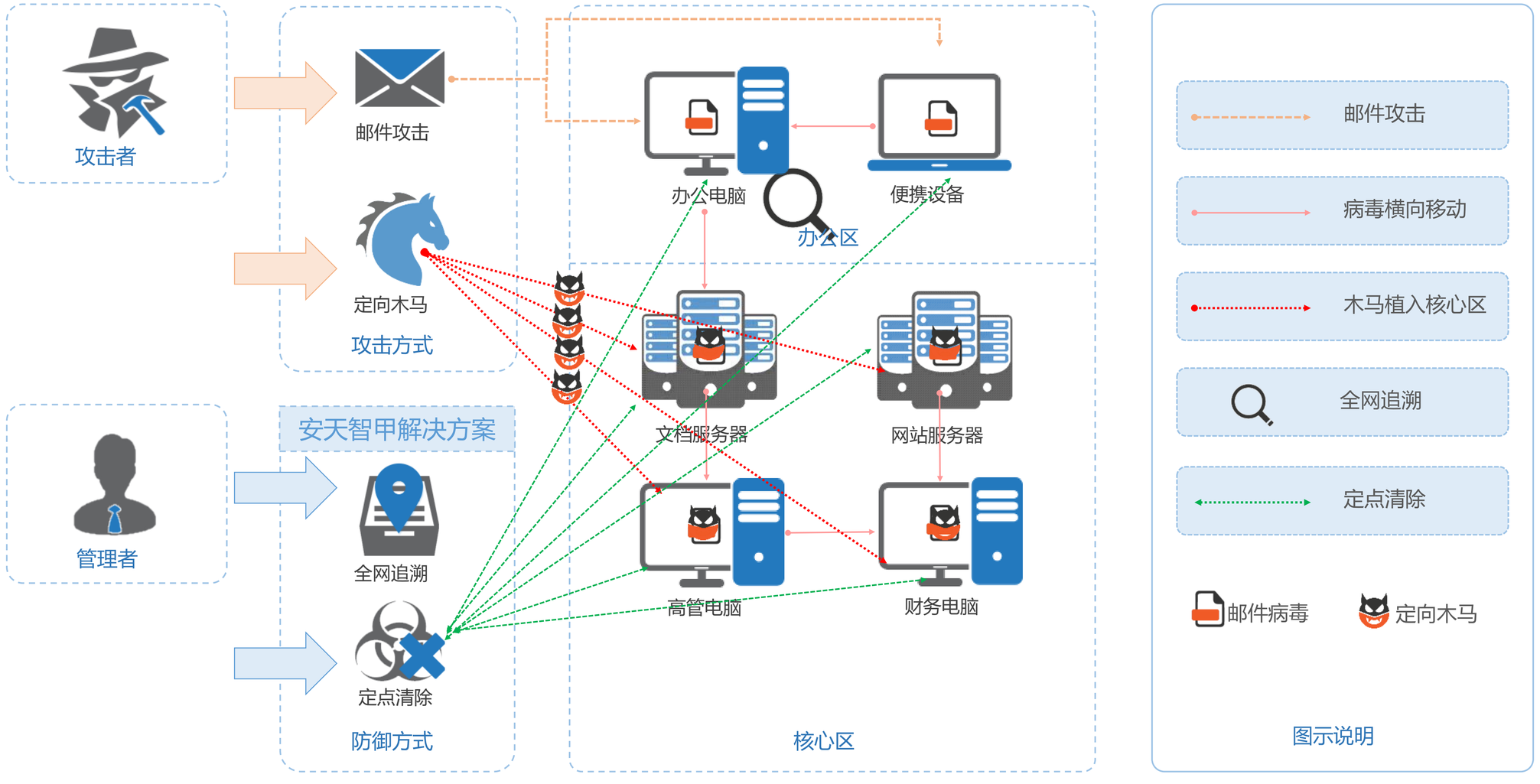
能够对多种类型的终端进行统一管理，并可持续扩展安全能力。

安天智甲终端防御系统 – 产品架构



有效防护 价值输出

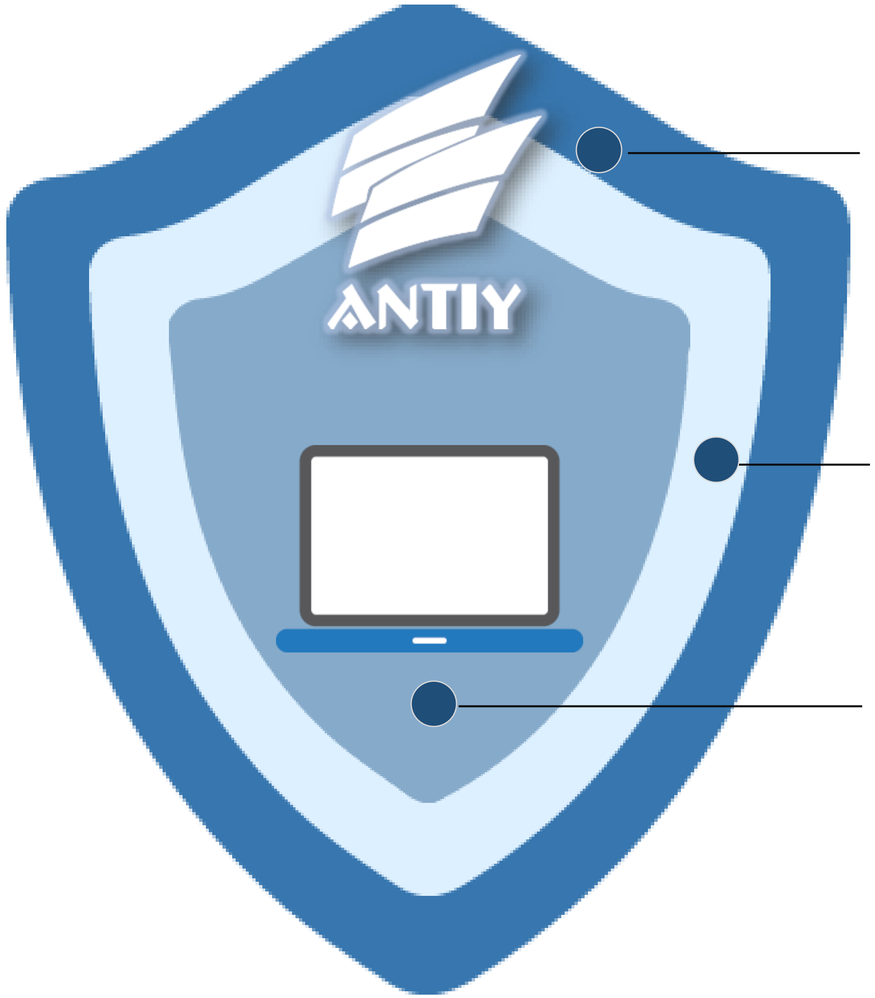
安天智甲针对APT攻击的全网威胁追溯和定点清除



一台终端发现威胁 -> 15分钟内全网追溯 -> 远程一键清除

有效防护 价值输出

智甲纵深防御：以勒索者病毒防御为例



边界防御

- 邮件附件防护
- 文件传输防护
- 文件下载防护

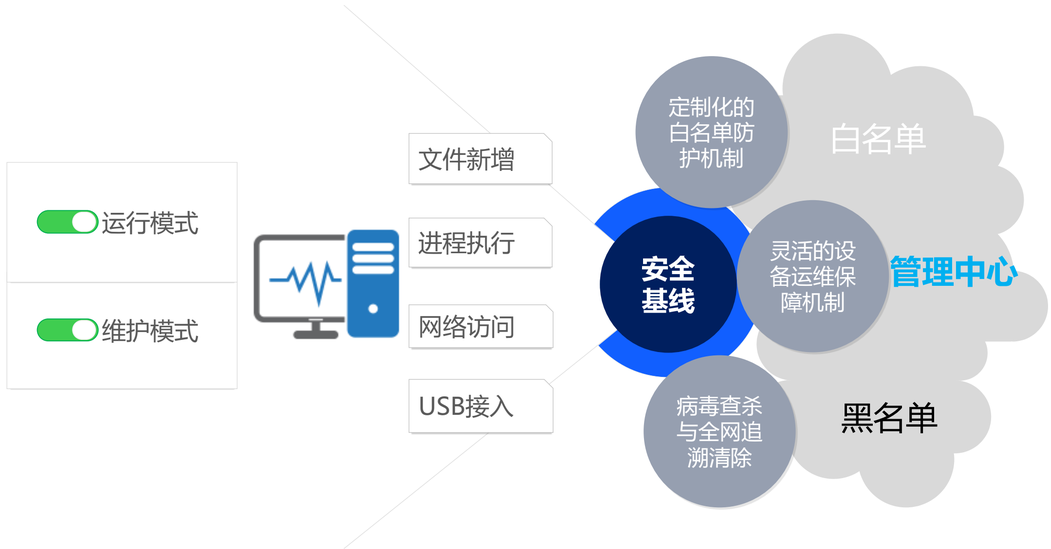
主动防御

- 监控可疑程序运行
- 监控可疑的注册表项

文档保护

- 访问控制：文档访问进程受信名单
- 文档预警：批量文件篡改行为监控
- 文档锁定：保护重要文档不被篡改

安天智甲面向专用终端的“安全基线+白名单”防御模式

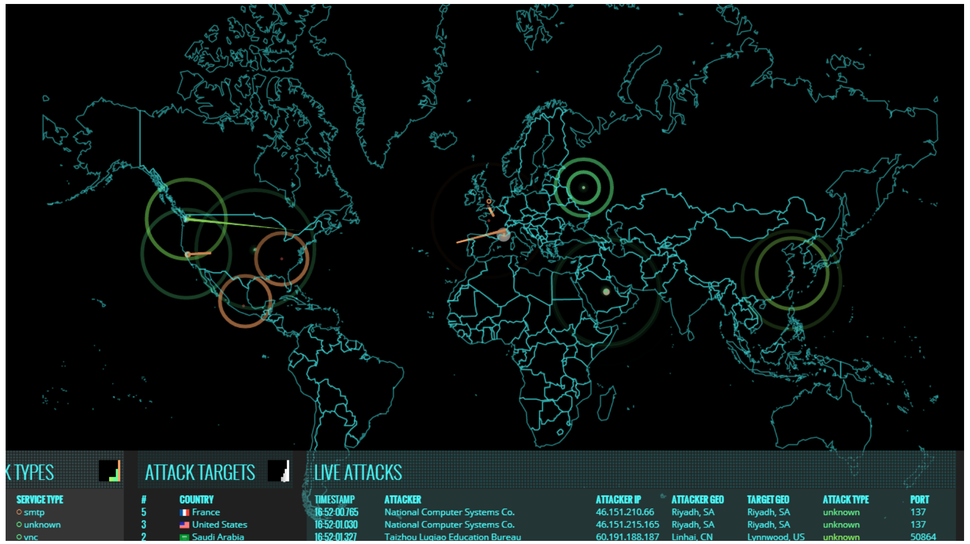


“白名单+安全基线”工作机理

可扩展的安全基线

- 文件基线
- 进程基线
- 外设基线
- 网络基线
- 驱动基线
- 服务基线
- ……

具有实用价值的交互式终端威胁可视化



有效防护 价值输出

总结：安天智甲终端防御系统的特点

全网追溯
定点清除

针对APT

终端纵深防御

针对新兴威胁

白名单+多种安全基线

ATM和工控上位机等

专用终端

领先的国产化系统
防病毒技术

Windows+Linux+国产系统
统一管理

安天智甲产品研发历程

Ghost Busters

木马防线

安天防线企业版

安天智甲终端防御系统

阶段：云查杀

列装我军某部

阶段：分级管理

该项目中唯一终端反病毒厂商

国产系统万套示范

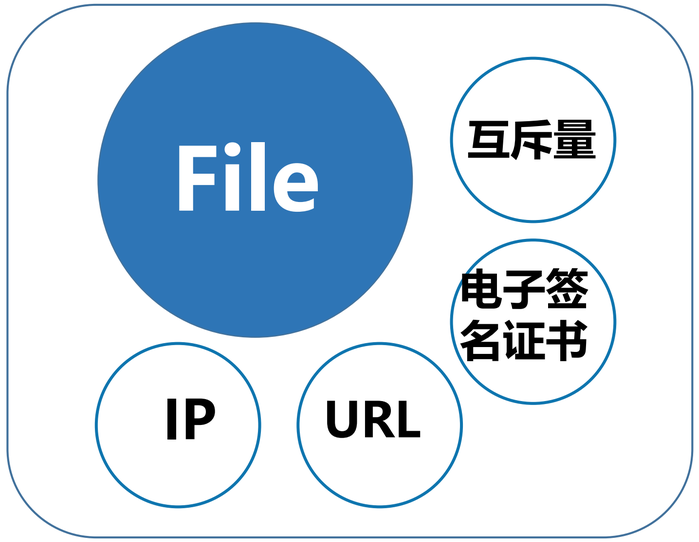
参与制定国产反病毒标准

某所国产终端项目

阶段：国产系统防护

2002年 **2012年** **2014年** **2015年** **2016年**

适配安天下一代威胁检测引擎

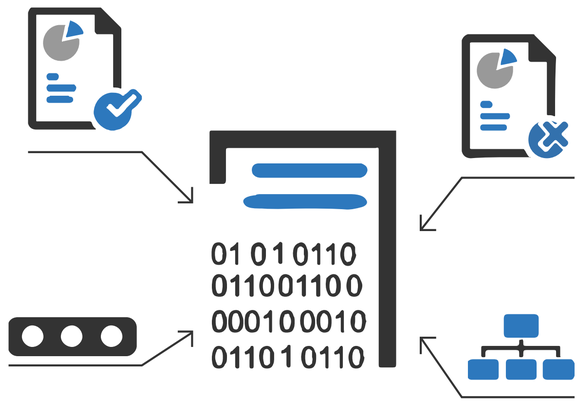


多种信标对象

关联的检测

向量拆解和输出

终端检测和响应技术（EDR）



扩充采集点

快速响应

有效补充

联动防御、知识融合，纳入态势感知系统

系统运维支撑

权限管理

身份认证　权限管理

访问日志　安全审计

运维管理

设备配置　策略配置

运行监控　数据备份

系统日志　错误告警

时钟管理

时钟同步

升级管理维护

升级管理　版本记录

态势感知

数据综合分析挖掘

掌握网络攻击情况

掌握自身网络安全隐患

安全监测

监测网络受到的攻击威胁

监测系统的安全状况

追踪溯源

可视化关联搜索

线索挖掘与分析

通报预警

汇总、分析、研判威胁情报

威胁情况的上报、通报、下达

深度分析、关联挖掘与业务逻辑处理

样本深度分析

可视化关联引擎

数据包深度分析与回溯

时间扩展字段索引服务

数据中心

样本文件库　安全威胁与事件库　IP/域名资源库　漏洞库　威胁情报库　资产库　其他库

事件与数据处理转化

主动获取数据下载与资源

URL库

下载URL管理

数据处理转化

事件、数据消重与合并　事件初始关联　预设条件比对标签化　日志泛化处理

事件标准化日志资源

木马病毒传播　系统攻击　APT攻击

事件临时存储　事件与系统资源接收处理　事件与系统资源接收

非标准日志

日志汇编　日志标准化　脚本模块管理器

非标准事件日志资源处理

二进制数据

二进制数据资源汇率

二进制数据资源处理

威胁信息采集

主机防御环节（智甲）

流量监测设备

扫描探测环节

蜜罐捕获设备

有效防护 价值输出

感谢大家参与本次交流