

安全威胁情报

如何敲开企业安全管理的大门

苏砧 产品总监 北京神州泰岳信息技术有限公司

2016.07

企业安全工作特点

- 合规性驱动力
- 以业务经营为优先
- 安全建设按多年规划滚动进行
- 安全建设成效？
- 各厂家各时期产品同时用
- 部门划分及岗位职责限制
- 安全岗位在企业内的地位



针对安全威胁情报 企业首先提出的问题是

- ① 有没有成功案例？
- ② 安全威胁情报中心？这不是企业该干的事。
- ③ 威胁情报从哪获得？来源稳定吗？及时性和质量如何？如何收费？
- ④ 怎么评价获得的情报与我司关系和作用？
- ⑤ 现有的防御体系怎么使用威胁情报？



安全威胁情报落地做什么

- 防御已知攻击源、可疑来源和僵尸网络，通过：IP地址、URL等
- 业务反欺诈：IP地址或URL
- 防护恶意软件感染：IP地址、URL、进程、文件路径、文件名
- 反钓鱼：IP地址、URL、邮件发送人、邮件标题或附件特征
-



安全威胁情报企业落地过程（简单看来~）

生态环境

企业应用

攻击行为产生



情报产生

- 采集
- 调查
- 分析
- 发布

情报获取

- STIX
- CybOX
- OpenIOC

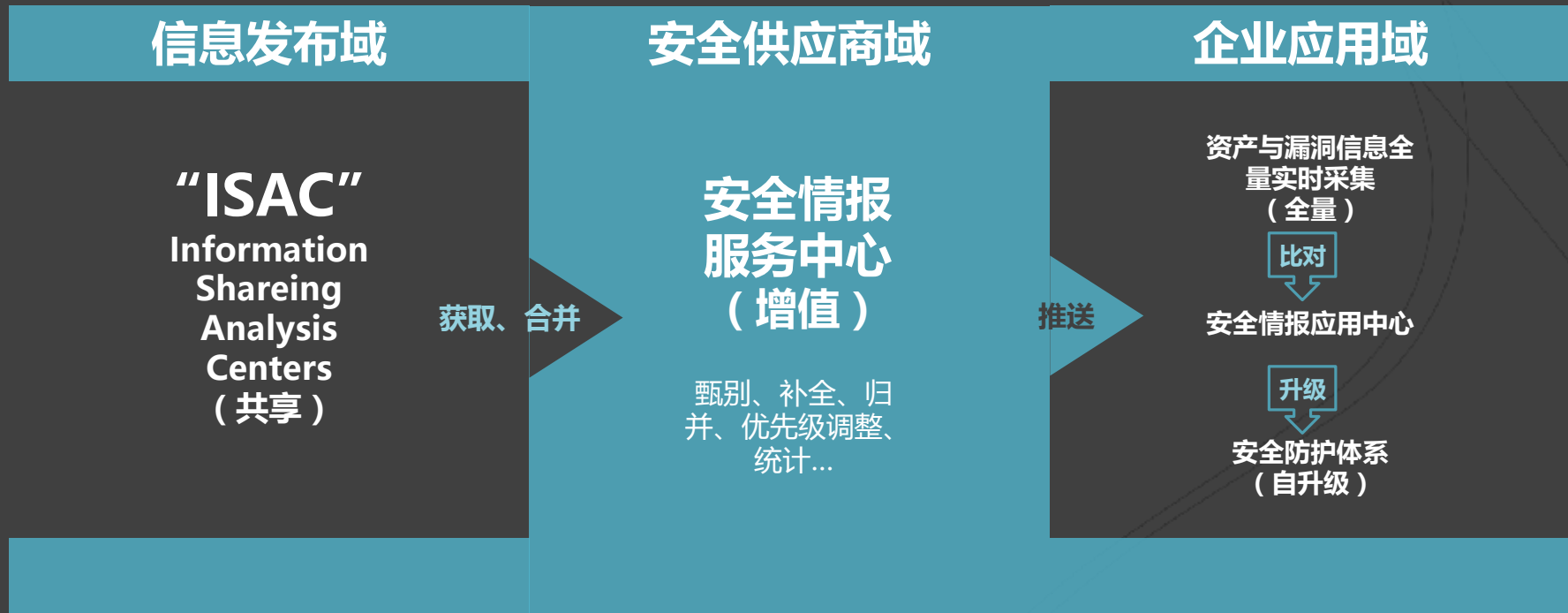


情报利用

- 影响分析
- 检测升级
- 监控升级
- 响应升级
- 安全管理平台



安全威胁情报企业落地过程（考虑了各种因素~）



安全威胁情报的企业需求分析

解决有无的问题：

- 1、外部威胁情报采集，随时同步国内外组织发布的威胁报告、恶意信息。
- 2、外部威胁情报展现，以资料库的形式随时查阅事件、黑客、方法、IP、URL等。
- 3、内部资产与漏洞信息采集（资产、网站、漏洞、指纹）

解决知道与否的问题：

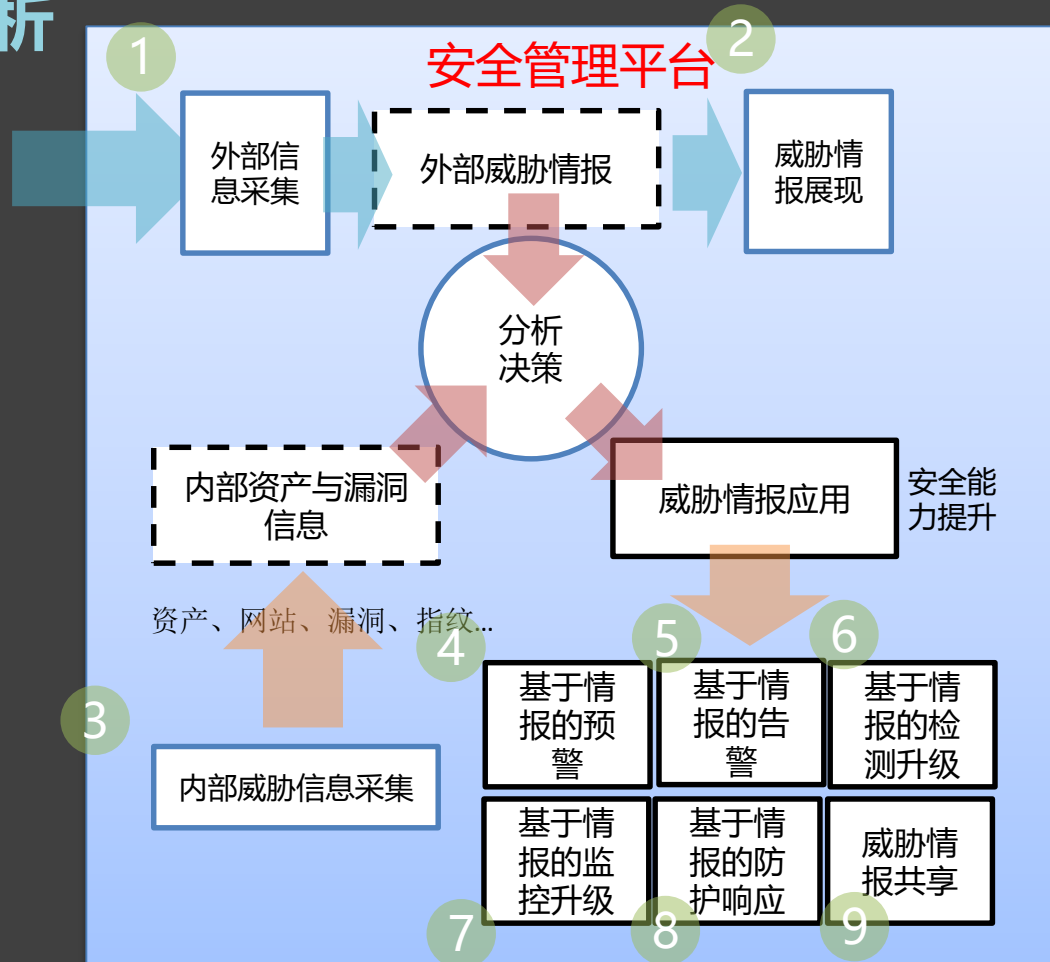
- 4、基于情报的安全预警，通过攻击手法的影响软件、利用漏洞，快速匹配本组织高风险资产。
- 5、基于情报的安全告警，通过恶意信息、受害者信息，分析本组织是否已经被侵害甚至成为攻击跳板。

解决自动提升自己的问题：

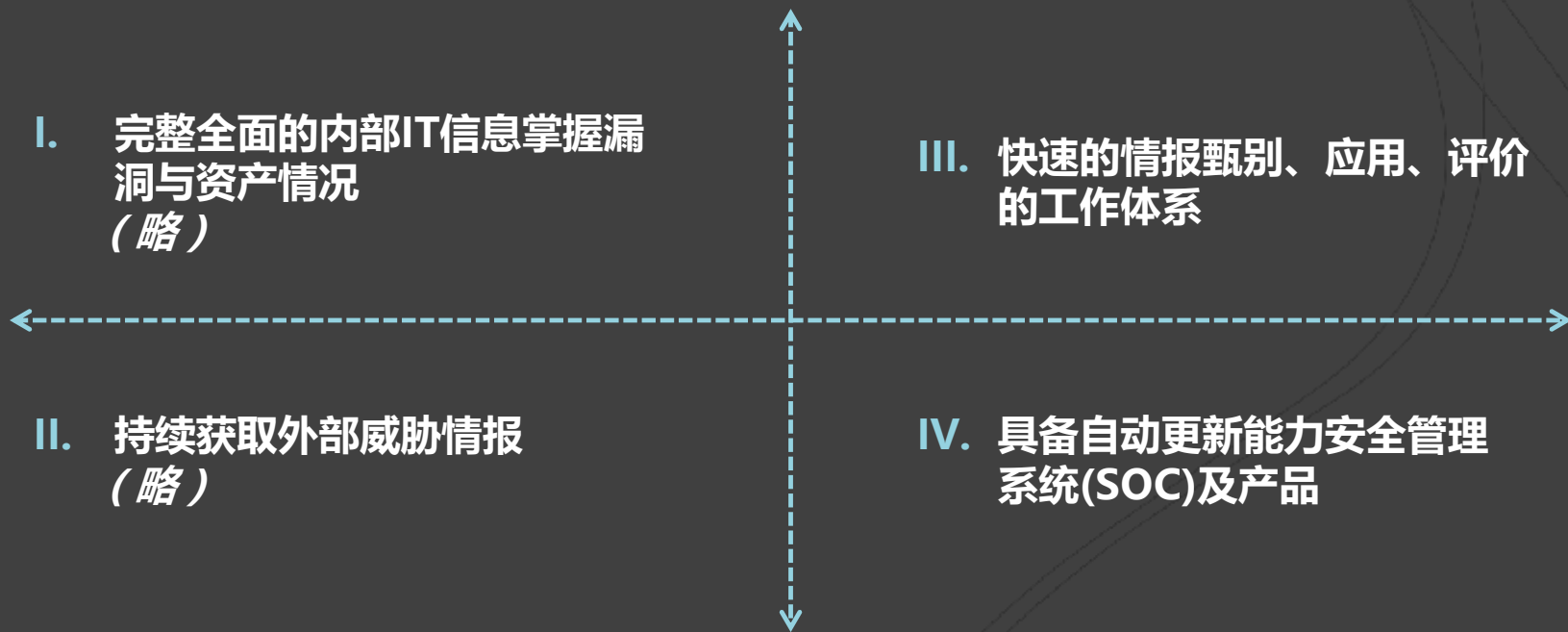
- 6、基于情报的检测能力升级，利用报告中的木马路径、文件HASH等、利用方法等形成新的检测。
- 7、基于情报的监控能力升级，利用IP、URL、邮箱、流量特征等，形成新的告警规则，通过其它平台。
- 8、基于情报的防护能力升级，通过其它平台，直接将恶意IP地址、URL、邮箱、流量的访问途径进行封锁。

解决能否对外输出：

- 9、威胁情报共享，继续向同行、国家、合作厂商进行输出



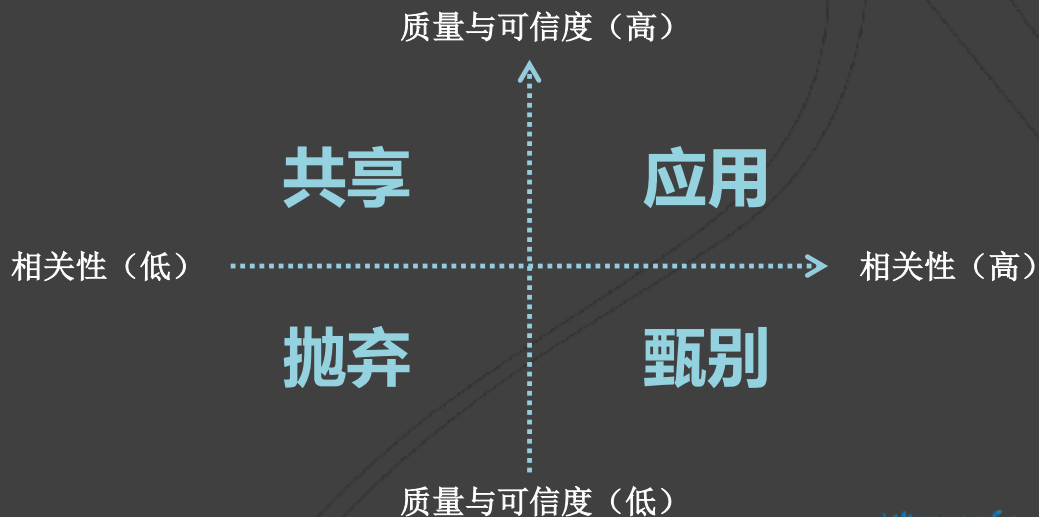
威胁情报在企业内部应用的过程





快速的情报甄别、应用、评价的工作体系

- 情报来源管理
- 情报匹配度分析（比对）
- 情报质量分析（测试）
- 情报应用
- 情报共享
- 情报评价



具备自动更新能力的“安全管理系统”及产品目标

安全管理类

外部威胁情报获取
内部威胁情报获取

威胁预警能力
自动升级

威胁情报工作流程支持
历史数据管理

检测类

- 新型漏洞检测
- 变种木马及代码检测

监测类

- 异常网络流量检测
- 入侵检测模式更新

防护类

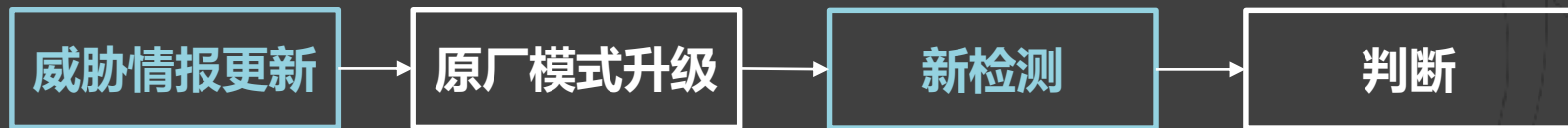
- 网络访问控制
- DNS解析防护
- 恶意域名防护

商业利益

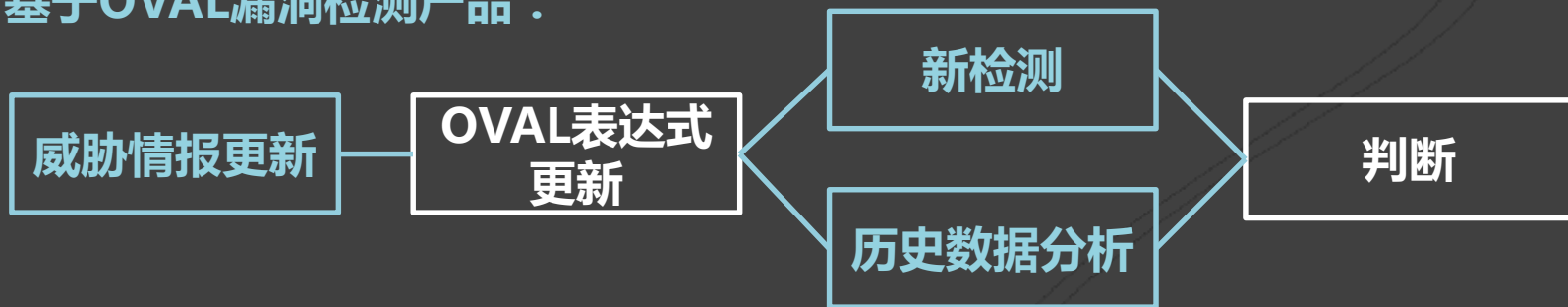
- 反欺诈
- 品牌舆论
- 社交媒体

基于CPE、OVAL的新型漏洞检测产品

- 传统漏洞检测产品：厂家漏洞库更新->检测->判断



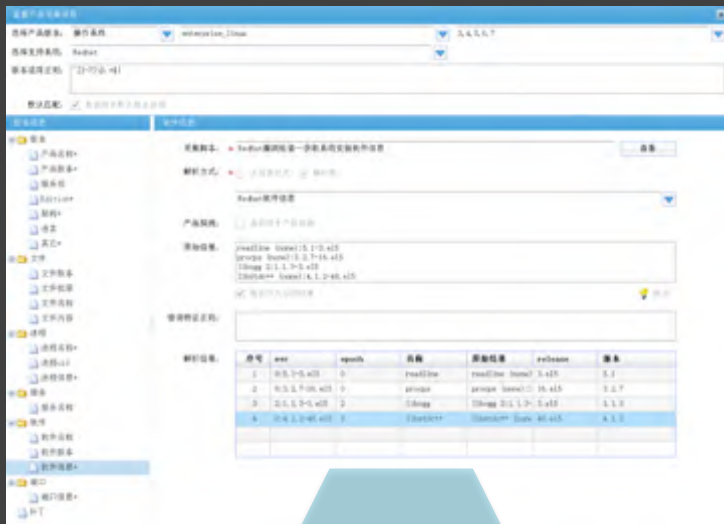
- 基于OVAL漏洞检测产品：



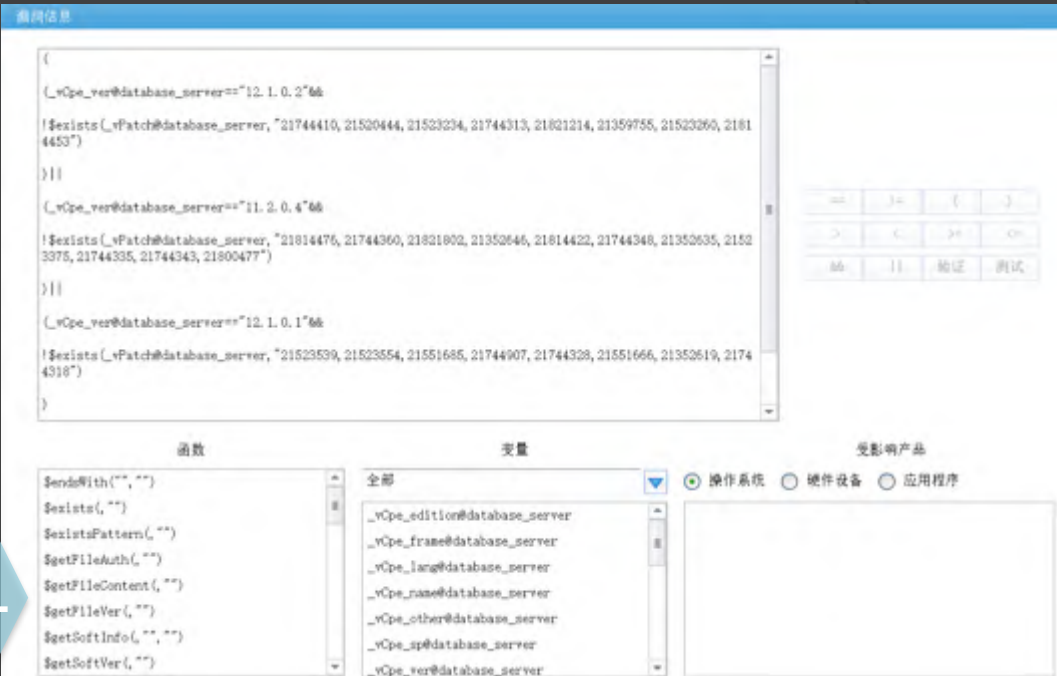
利用威胁情报信息与CPE、OVAL的结合，自动检测新型漏洞

CVE-2015-4873

Oracle Database Server Database Scheduler组件安全漏洞



基于CPE

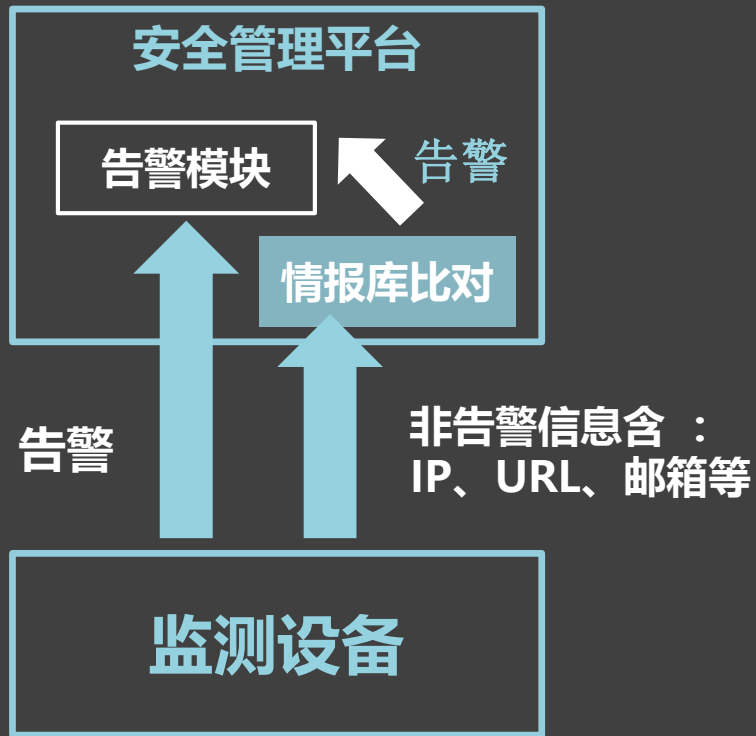


基于OVAL

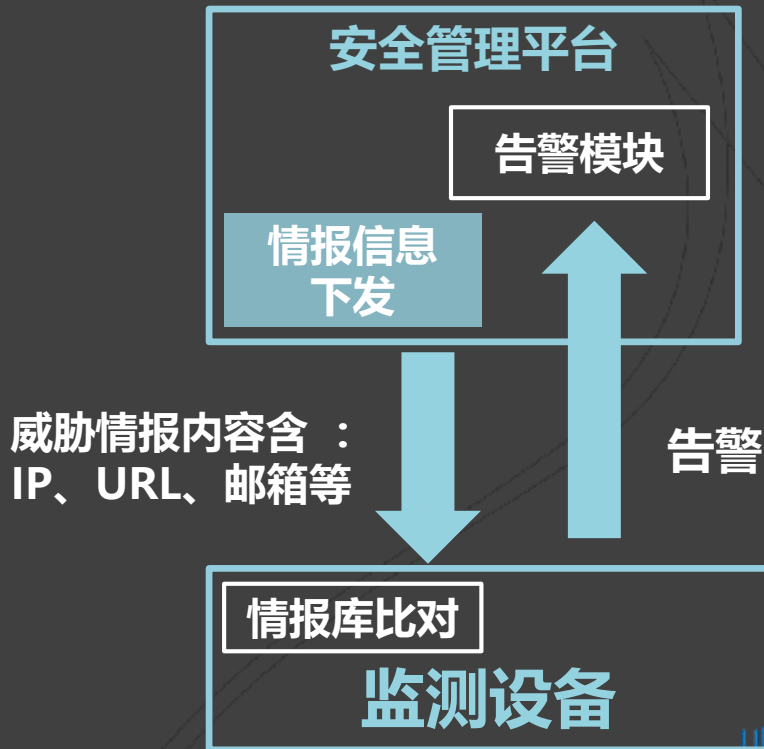
威胁情报

基于白名单的安全监测类产品（流量、URL、DNS、EMAIL）

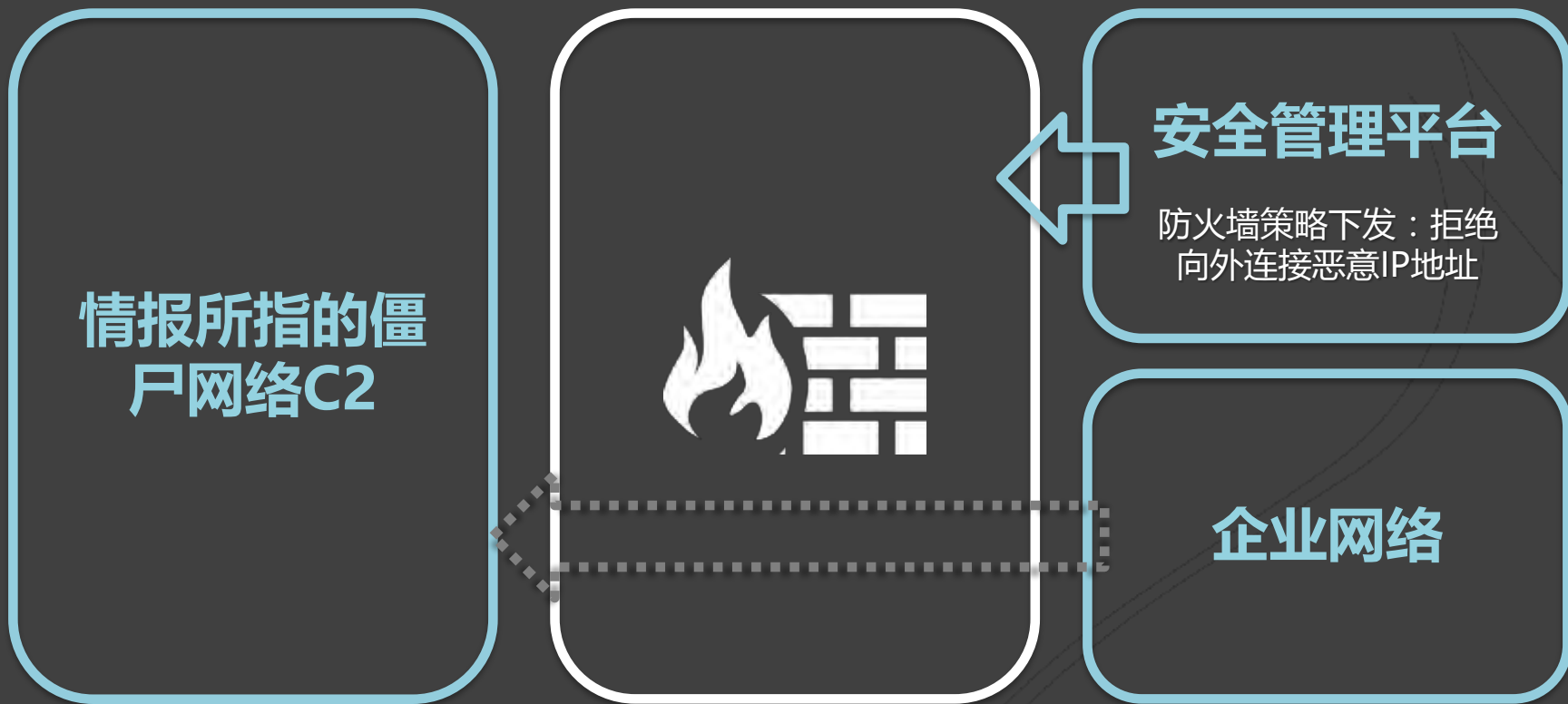
- 基于安全管理平台实现的威胁情报内容监测告警



- 基于监测设备实现的威胁情报内容监测告警



根据威胁情报进行快速的僵尸网络及恶意地址封堵





最后，难点分析

- 国内情报生成能力薄弱、国际情报水土不服
- 成本高而价值不明：情报获取困难、代价高；最终效果不明确；
- 数据获取缺少枢纽：企业直接从国内外安全公司获取数据效率低，利用不充分；
- 数据交换格式较多：多种格式并存，版本持续更新；
- 情报质量不明：全面？误报？
- 情报利用不充分，威胁披露后继续存在。
- 技术平台落地难：国内的主流安全建设与产品不具有自动化升级能力；

- 自主的威胁情报来源
- 权威的情报交换机构
- 情报兼容的安全系统产品