多源异构数据环境下态势感知体系构建

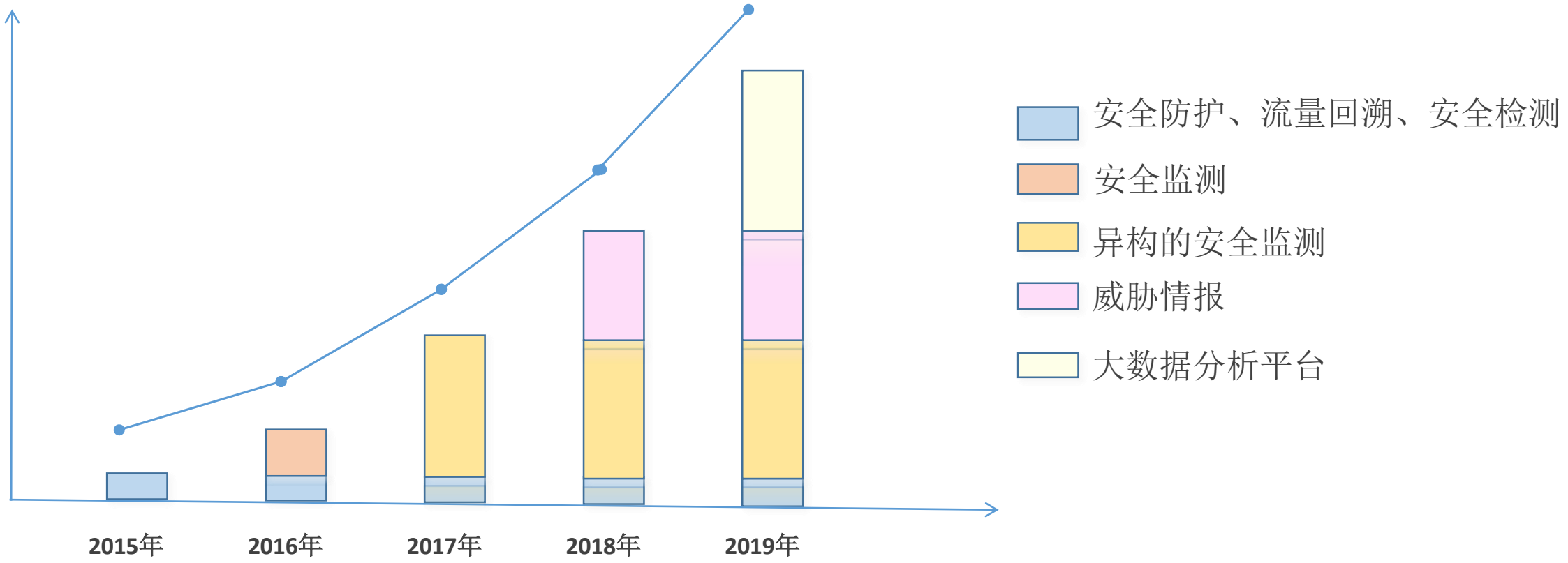
吕艳丽

科学技术部信息中心 高级工程师

目录

网络安全管理中的难题

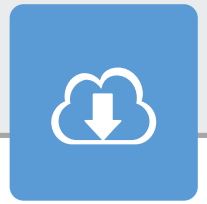
- 管理内容规模急速增长
- 数据来源日趋复杂



网络安全管理中的难题

- 管理监控措施不及时不完善

60%

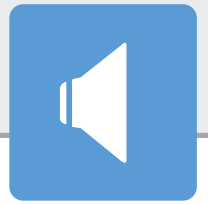


操作系统、中间件等补丁24h更新率

20%

漏洞24h修复率

60%



定期自查、评估和修复的比例

40%

系统变更后第一时间安全评估率

10%

系统变动致同类漏洞重现率

网络安全管理难题对策

提高网络安全管理效率

海量日志和告警信息中攫取真正威胁

海量日志和告警信息中获取网络安全整体态势

信息资产全链条跟踪

打通系统运维和网络安全管理

系统运维对网络安全状态的影响

漏洞通告传导系统防护任务

目录

体系建设原则

覆盖全域，统一分析。对全域系统各类关键信息基础设施、重要网络关口进行常态化统一监测和分析，形成全链条安全管理体系。

强化落实，常态化管控。以贯彻落实《网络安全法》和国家网络安全等级保护制度为主线，在系统建设、运行管理、组织保障等多方面同步推进网络安全工作，常态化监测，及时发现问题，确保落实安全管理细节。

技术特点1：实现分析级的数据融合

态势感知分析中心1

侧重于安全数据分析，与安全事件基础库平台联动，整合已有安全事件基础库的历史数据和在线数据，实现全网安全数据日志综合分析。

态势感知分析中心2

侧重于威胁管理综合分析，与现有终端管控系统对接，侧重管理流量、安全设备及终端日志的日志多源分析。

态势感知分析中心3

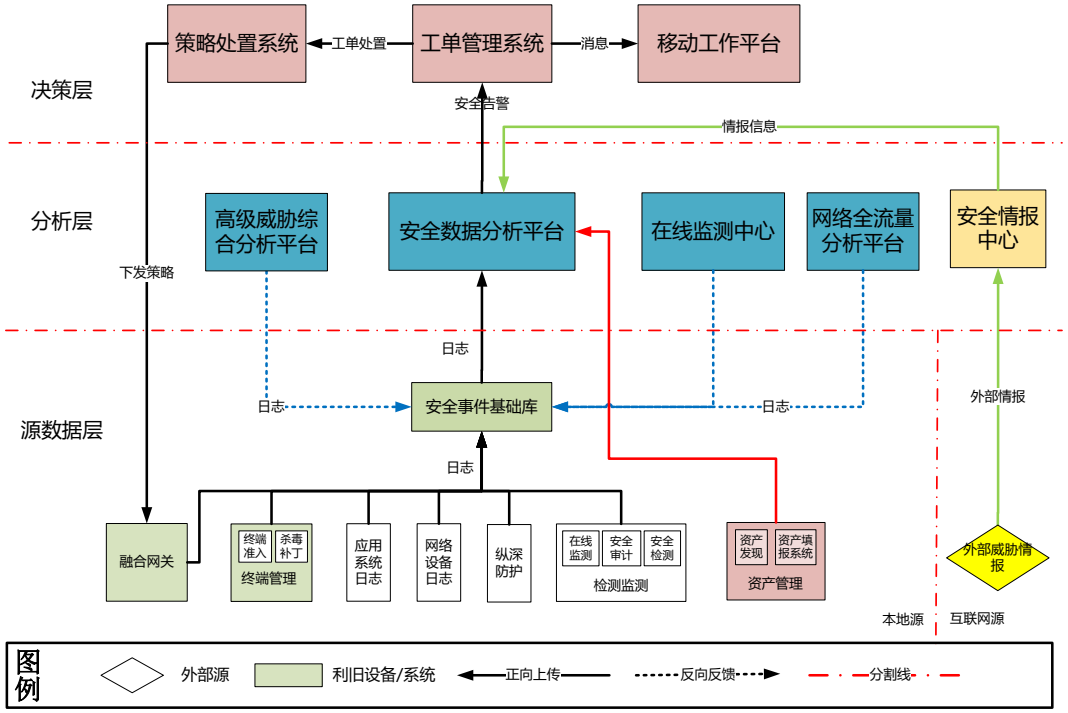
侧重于网络流量数据安全分析，对网络流量精确分析，监测网络攻击和恶意代码，提供网络元数据。

安全事件

事件场景更完整
准确率较高
定位更准确

安全数据分析平台（分析中心1）

- 对安全事件基础库进行全面整合，包括网关日志、终端管理日志、应用系统类日志、网络设备类日志、纵深防护类日志、检测监测类日志、高级威胁综合分析平台日志、在线监测中心日志、网络流量分析平台日志等。
- 将整合后的数据与威胁情报碰撞，得出恶意攻击行为。威胁情报主要包括恶意IP、恶意域名、恶意URL、恶意EMAIL地址、恶意样本哈希值等。

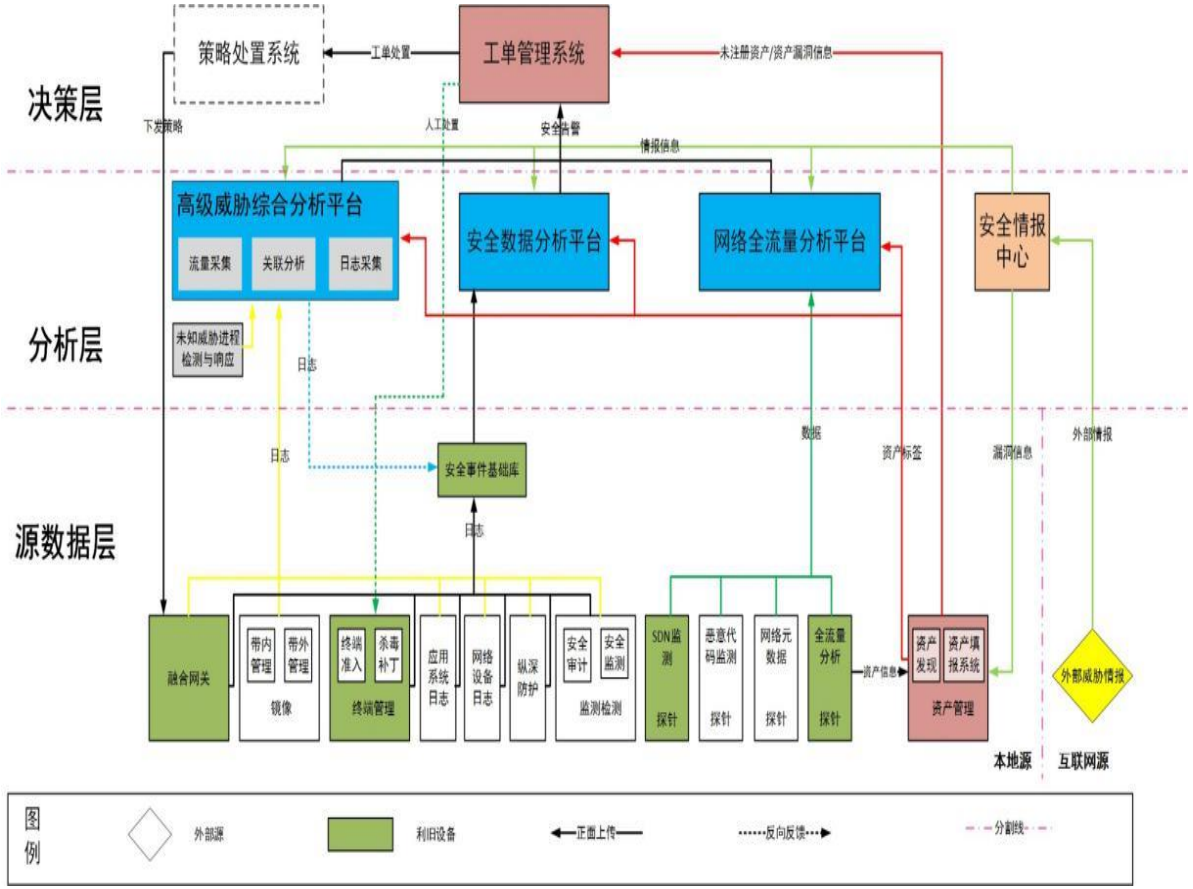


多源异构数据环境下态势感知体系

高级威胁综合分析平台（分析中心2）

基于日志和流量多源异构数据进行综合分析，提高未知高级威胁防护能力，集中呈现全网威胁情况。

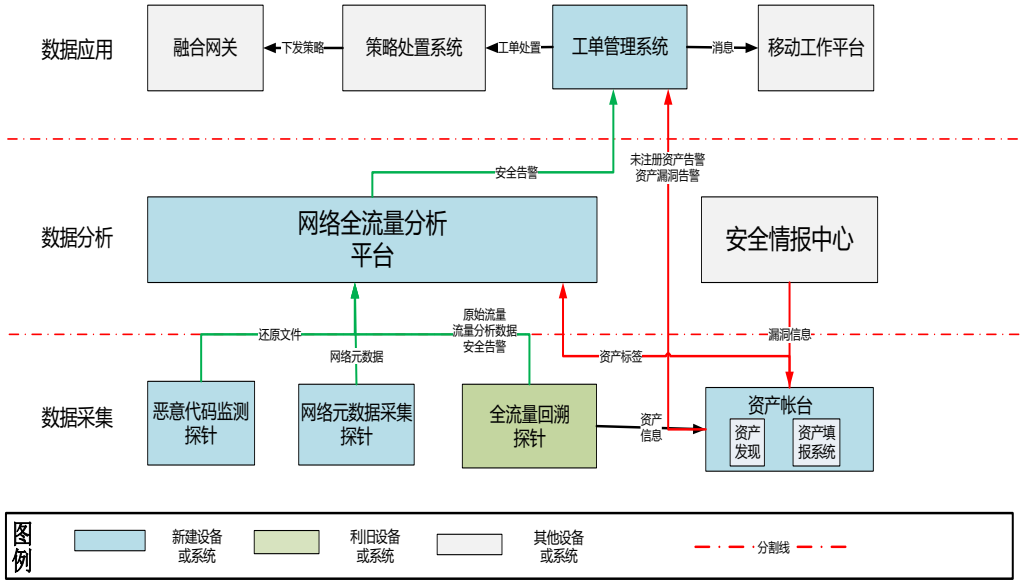
- 完成事件收集、告警分析、应急溯源分析
- 结合厂商的威胁情报能力，及时发现威胁情况
- 配合其余分析平台完成问题发现工作，并为处置提供技术依据



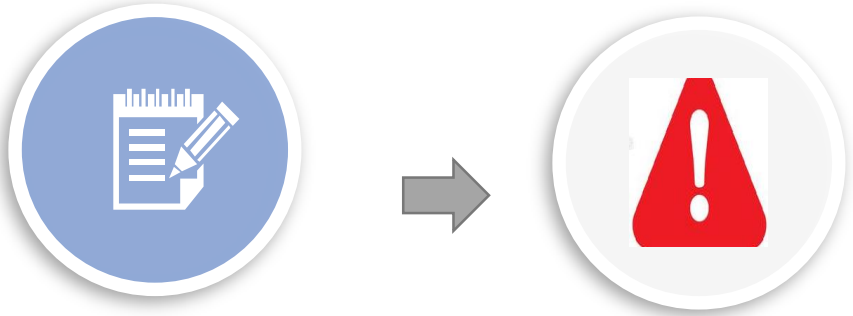
网络流量分析平台（分析中心3）

基于“流”行为数据和其他日志数据自动化分析各类异常行为。

- 建立异常行为模型，实时匹配网络流量，回溯分析历史数据
- 建立“文件样本”行为数据模型，识别未知攻击或恶意代码
- 提供“包”内容数据，还原事件过程，实现威胁的追踪溯源取证



技术特点2：实现决策级的数据融合



资产

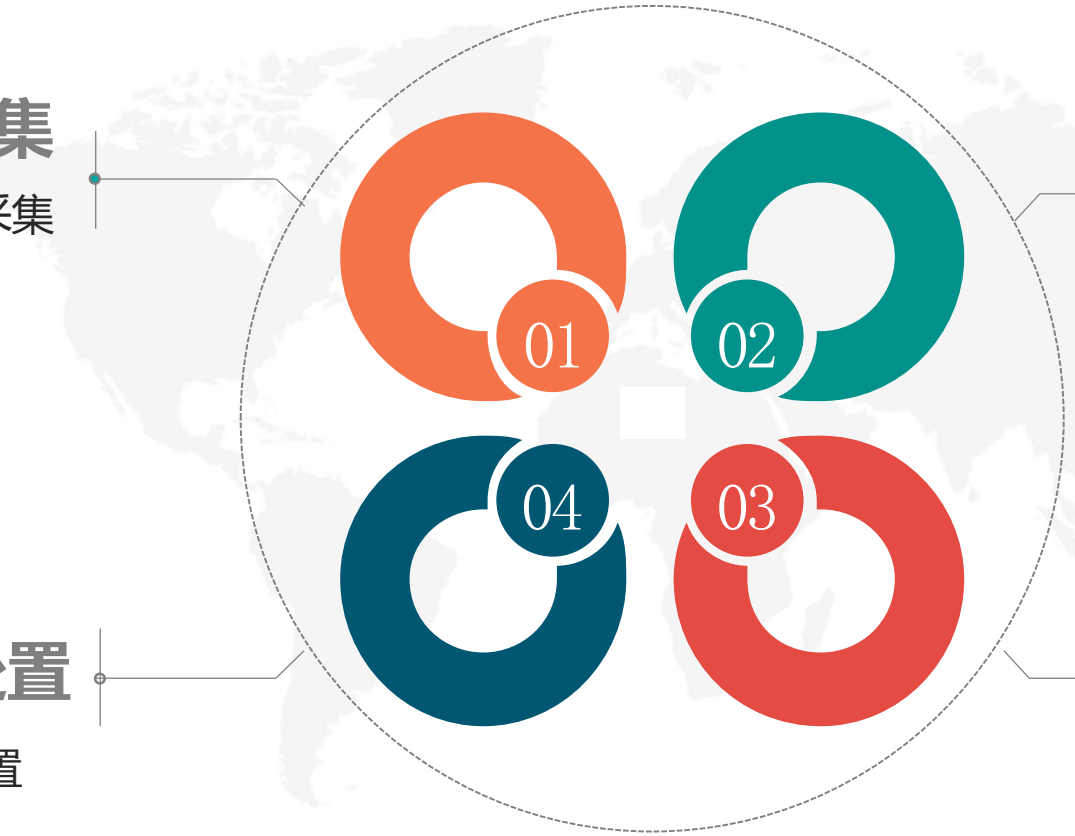
全部在网资产信息，包括基本属性、运行情况、配置情况、脆弱性情况等。

需处置的安全事件

对资产存在安全威胁的安全事件，为下一步的处置提供决策支持。

多源异构数据环境下态势感知体系

态势感知体系运行的主要环节



数据采集

基于全域流量的网络安全数据采集

资产探查

常态化资产探查、分析、脆弱性识别

应急处置

网络安全事件分级分类处置

融合分析

多维度的网络安全态势感知和风险分析

基于全域流量的网络安全数据采集

采集网络设备、安全设备、终端、应用系统的日志；采集关键网域东西向、南北向全域流量；采集原始脆弱性数据等。对采集到的数据进行清洗、过滤、识别、路径补充、格式化等，形成数据资源池。

常态化资产探查、更新和脆弱性识别

采用主动、被动、基于搜索引擎等方式实时探查在网信息资产及变化情况，形成资产库。通过与脆弱性扫描系统、威胁情报、通用漏洞库（CVE）、漏洞测试库（POC）碰撞，形成资产脆弱性数据。

数据融合分析

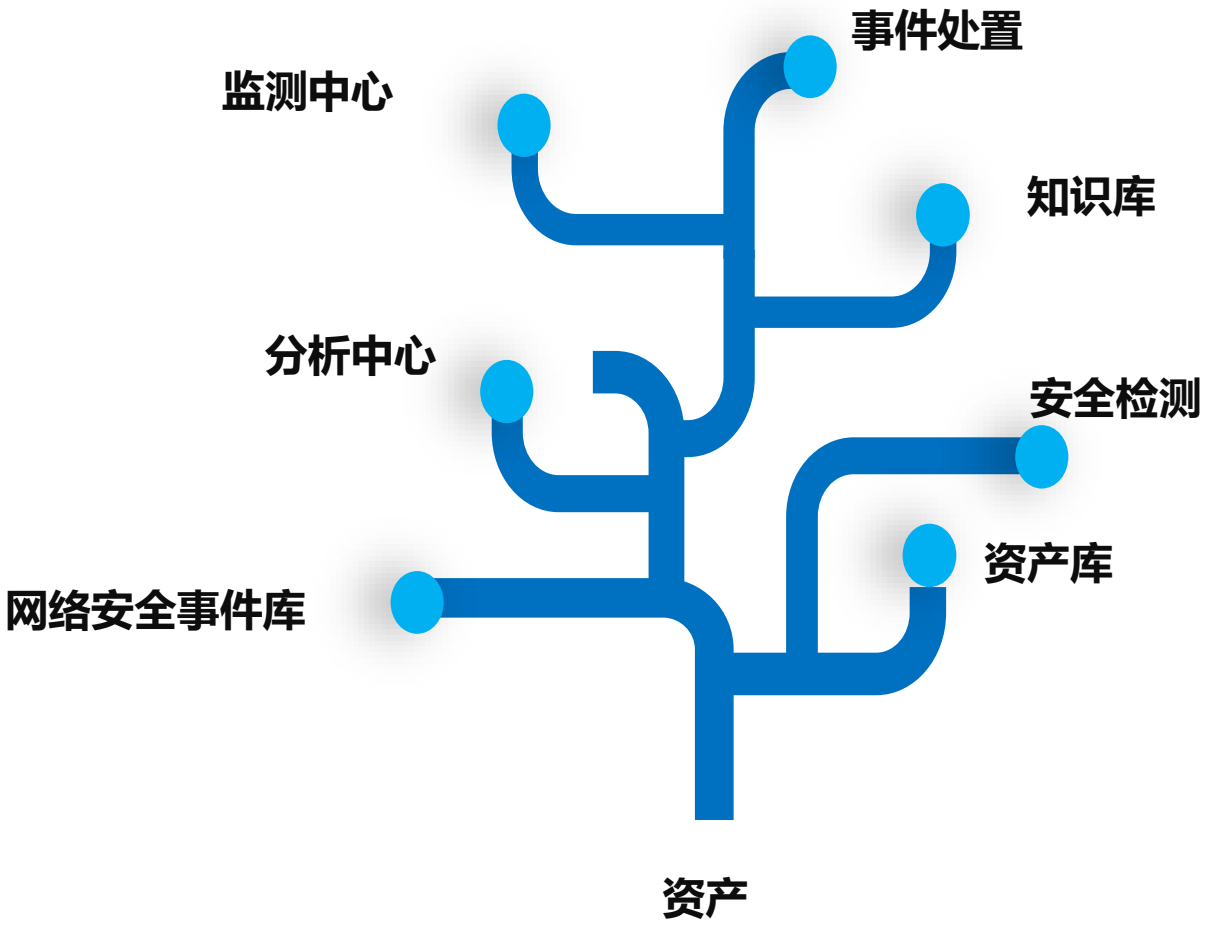
多分析中心的输出数据进行去重、补齐、建模等，与安全知识库、资产库等进行融合分析，形成真正具有威胁的安全事件。安全知识库包含内置检测规则、内置风险分析和处置规则、云端获取威胁情报、第三方威胁情报接入、离线威胁情报库导入、安全威胁自定义模板、本地威胁情报累计、大数据安全建模分析模型等。

安全事件应急处置

根据安全事件的事件类型和危害级别按照应急处置基线分类分级处置，第一时间自动处置可确定的高风险网络安全事件，自动处置手段包括阻断可疑互联网IP地址、URI、域名、邮箱等。

目录

资产的定义



资产主要属性

基本属性：主机名、操作系统、数据库、中间件及版本号。

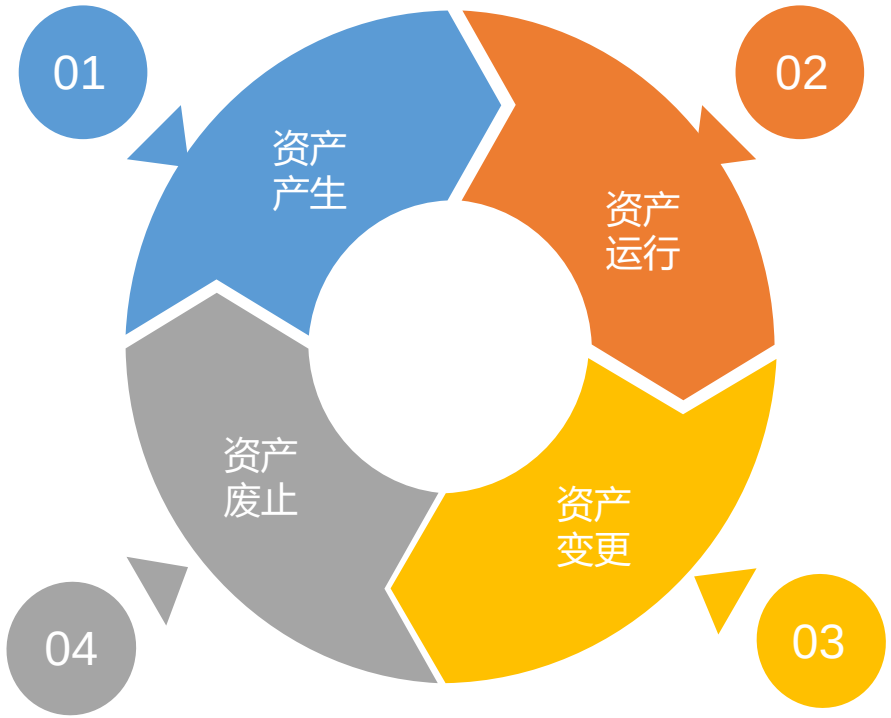
网络属性：域名、所属VLAN、公网IP、内网IP、开放端口、黑白网络地址名单等策略。

行为属性：用户行为模型、网络访问模型等。

漏洞属性：在近期安全检测中发现的安全漏洞及修复情况等。

资产的全链条态势感知和处置

1、采用主动、被动、基于搜索引擎、人工等方式采集资产信息；
2、检测操作系统、数据库、中间件的脆弱性以及信息系统自身的安全漏洞。



1、实时监测信息资产的受攻击情况和安全状态变化情况；
2、外部条件变化引起知识库更新，触发新的知识库与资产库碰撞，探测安全隐患；
3、漏洞测试库更新触发对近期网络流量的漏洞利用攻击行为回溯分析；
4、实时比对资产信息；
5、定期检测操作系统、数据库、中间件的脆弱性以及信息系统自身的脆弱性。

1、修改资产库及相应防护策略；
2、监测废止资产再运营现象。

更新资产信息：
1、自动触发新资产与知识库碰撞，探测安全隐患；
2、检测信资产的脆弱性。

与资产库碰撞的知识库内容主要有威胁情报（恶意IP/域名/URL、恶意软件散列值、不良信息、安全漏洞等、攻击者画像等）、通用漏洞库（CVE）、外部通报等。

THANKS

2019北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE