ThreatBook

聚焦威胁 情报驱动

2018 网络安全分析与情报大会

ThreatBook

安全运营中威胁情报的应用分享

2018 网络安全分析与情报大会

-- 姜明元 --

中信建投证券股份有限公司

信息技术部VP

安全规划

2016 基础建设

- 建立纵深防御体系，具备一定的安全防护能力
- 建立信息安全制度体系，提供信息安全工作标准

2017 安全运维

- 建立安全运营体系，提升安全事件，漏洞，问题主动发现能力
- 对信息安全体系文件进行可量化、可落地并贯彻执行

2019 深度感知

- 提升安全运营及响应能力，具备一定程度上对未知威胁的防御手段，进一步提升安全防护水平
- 全面提升安全体系管理与审计工作的自动化能力

2022 自主可控

- 组建自有的专业安全服务团队，根据公司实际情况研发安全防护产品，实现安全即服务

安全运营难点

漏洞发布

2小时
漏洞扫描

4小时
发现漏洞设备

8小时
入侵设备

24小时
内网渗透

40小时
数据收集

48小时
打包带走

扫描告警
（单位：万）

6小时
内部通报漏洞

入侵告警
（单位：万）

12小时
漏洞验证&变更
方案制定

内网渗透告警
（单位：万）

36小时
漏洞修复

数据库审计告警
（单位：万）

流量异常告警
（单位：万）

问题：漏洞修复是否纳入安全事件的应急响应动作?

安全运营数字

每天
收集日志
平均数量

84,528K

每天
告警日志
平均数量

5,303K

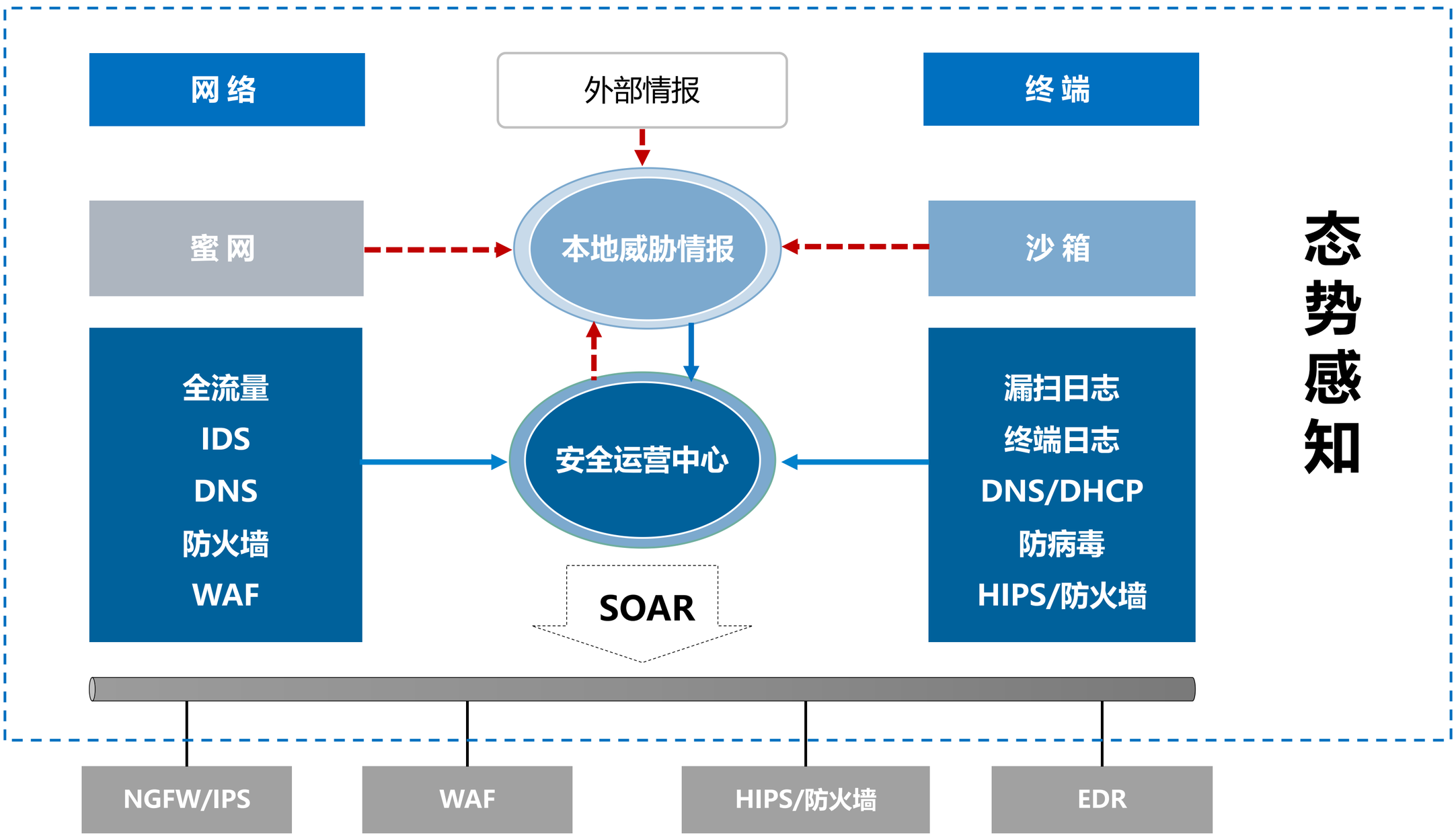
每天
通过SIEM分析
产生事件
平均数量

25

安全分析人员
数量

1

威胁情报引入


网 络
外部情报
终 端
蜜 网
本地威胁情报
沙 箱
全流量
IDS
DNS
防火墙
WAF
安全运营中心
漏扫日志
终端日志
DNS/DHCP
防病毒
HIPS/防火墙
SOAR
NGFW/IPS
WAF
HIPS/防火墙
EDR
态势感知

情报落地

Step 01

整合

建立本地情报中心，整合多源情报，给出可应用于各类场景的基准

Step 02

流转

打通情报流转网络及通路，消除情报孤岛

Step 03

应用

将情报广泛应用于安全分析、响应的场景，使情报真正落地

Step 04

分享

建立本地情报分享机制，具备威胁情报的自我发现及生成能力

情报整合

格式冲突

将格式各异的情报（如单行格式、自定义格式、XML格式和JSON格式等）统一为标准格式，普遍采用易于存储及交换的JSON格式

结果冲突

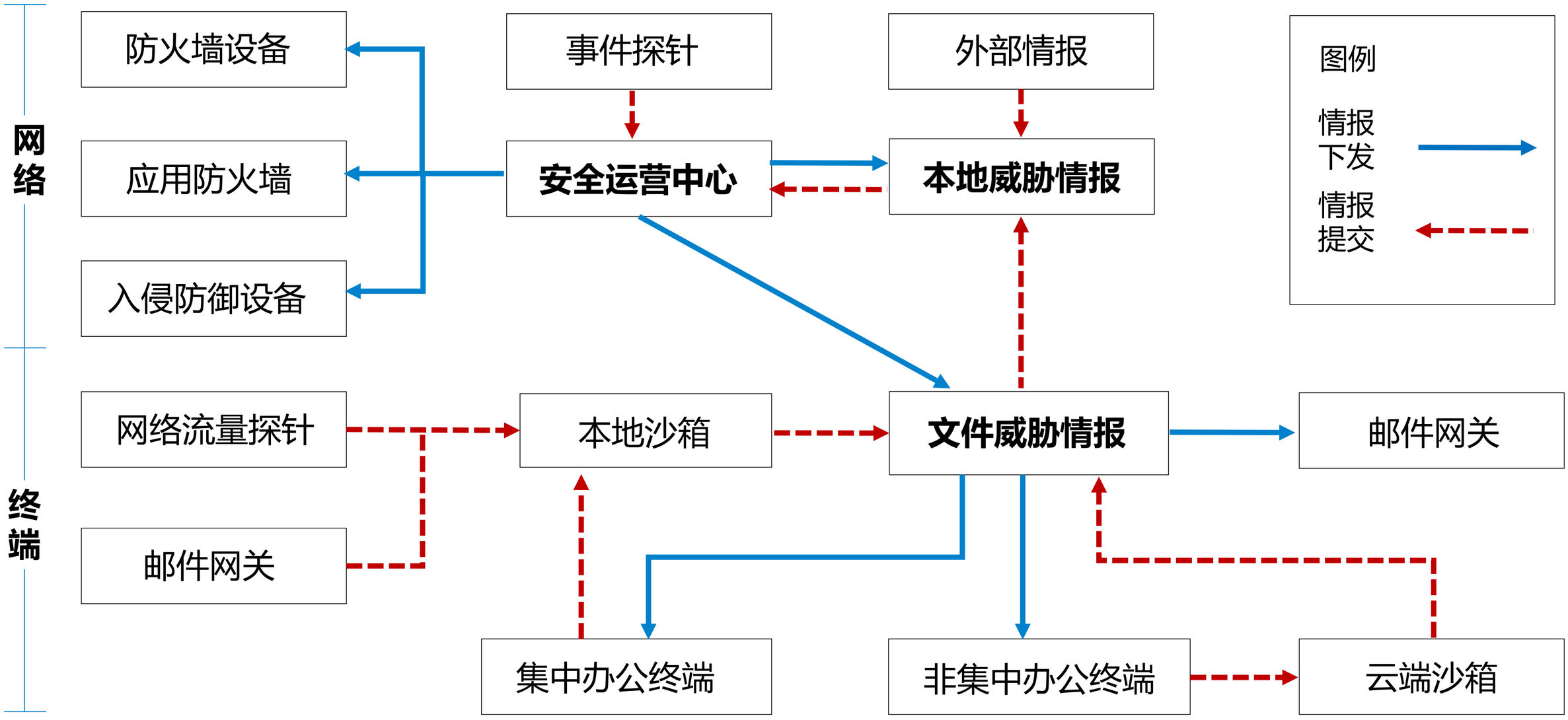
使用一定的算法产生唯一值：投票法、一票否决、一票通过、权重计算（根据不同情报源特征给出不同权重比例）

情报整合唯一结果

属性冲突

情报数据的整合通常遵循最大集合原则，既将所有情报源字段进行理解后，去重、合并并拼凑在一起，形成一个最大集合。

情报流转


网络
终端
防火墙设备
应用防火墙
入侵防御设备
网络流量探针
邮件网关
事件探针
外部情报
安全运营中心
本地威胁情报
本地沙箱
文件威胁情报
邮件网关
集中办公终端
非集中办公终端
云端沙箱
图例
情报下发
情报提交

攻陷分析

外连与情报进行碰撞比对，快速定位攻陷主机

溯源画像

利用威胁情报中的关联性、对黑客进行画像

决策支持

对海量告警事件的响应无从下手时，提供策略上的支持

主动防御

对热点情报的提前防护策略部署，降低外部入侵风险

攻陷分析

01 URL情报

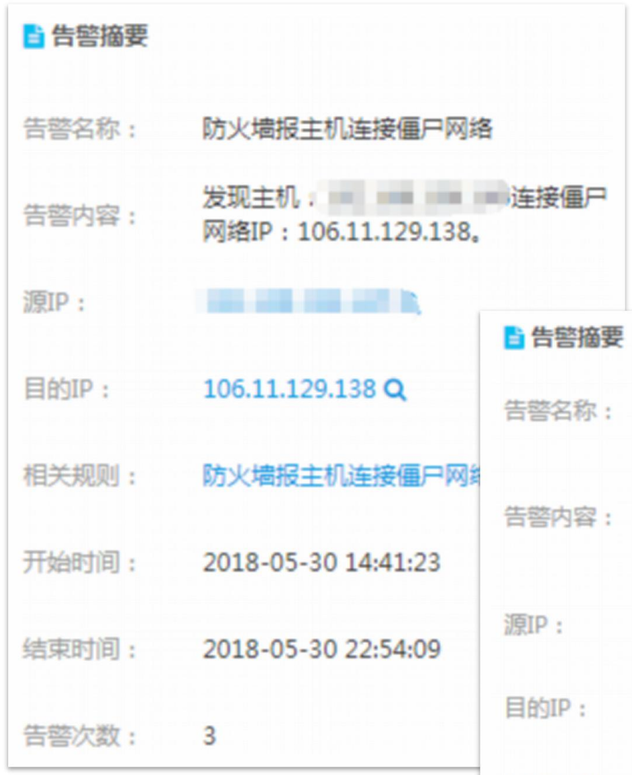
DNS、对外通讯日志

02 IP地址

对外通讯日志

03 文件情报

防病毒、网关/流量设备、沙箱



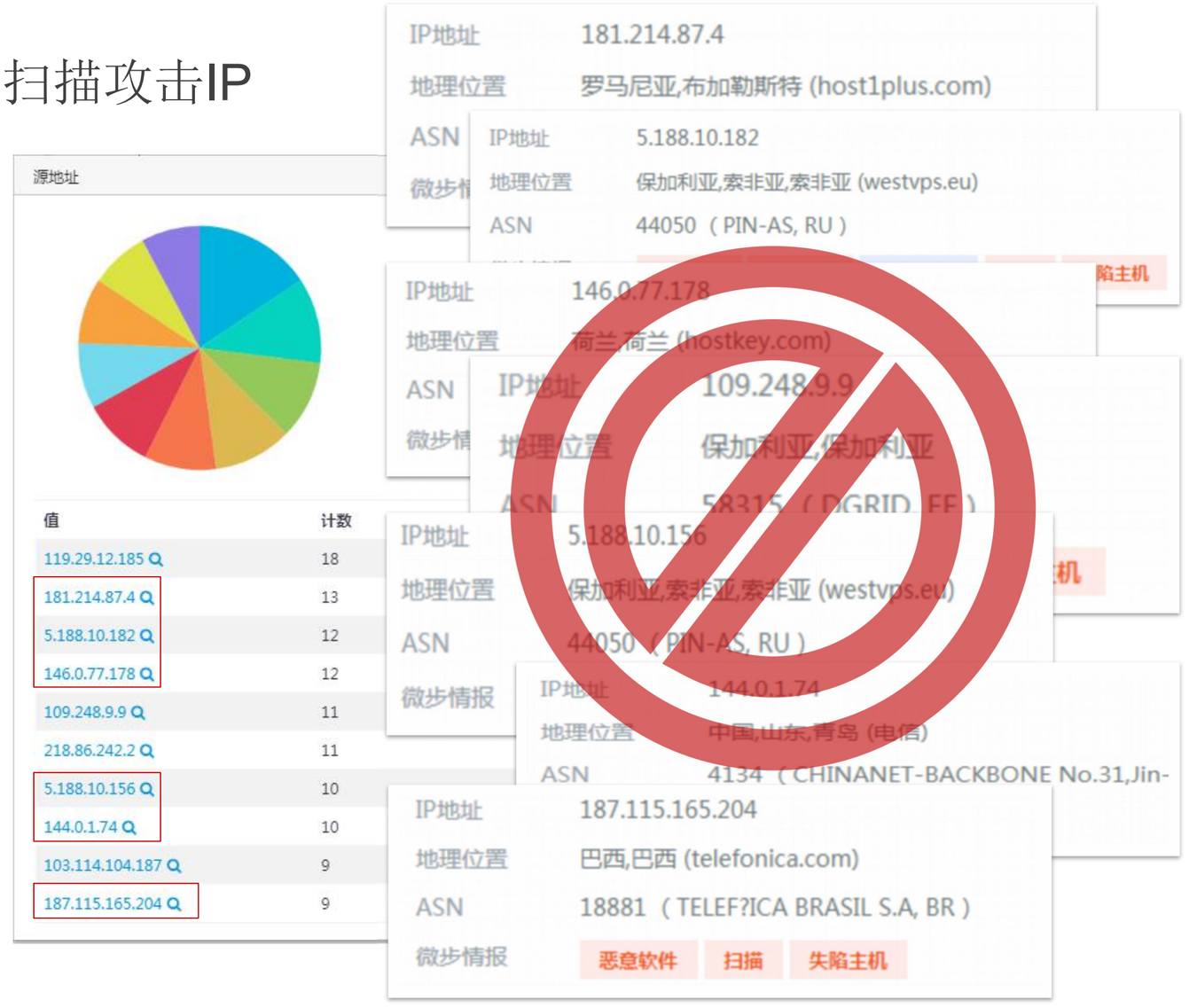
决策支持

01 针对攻击开展响应动作时提供参考

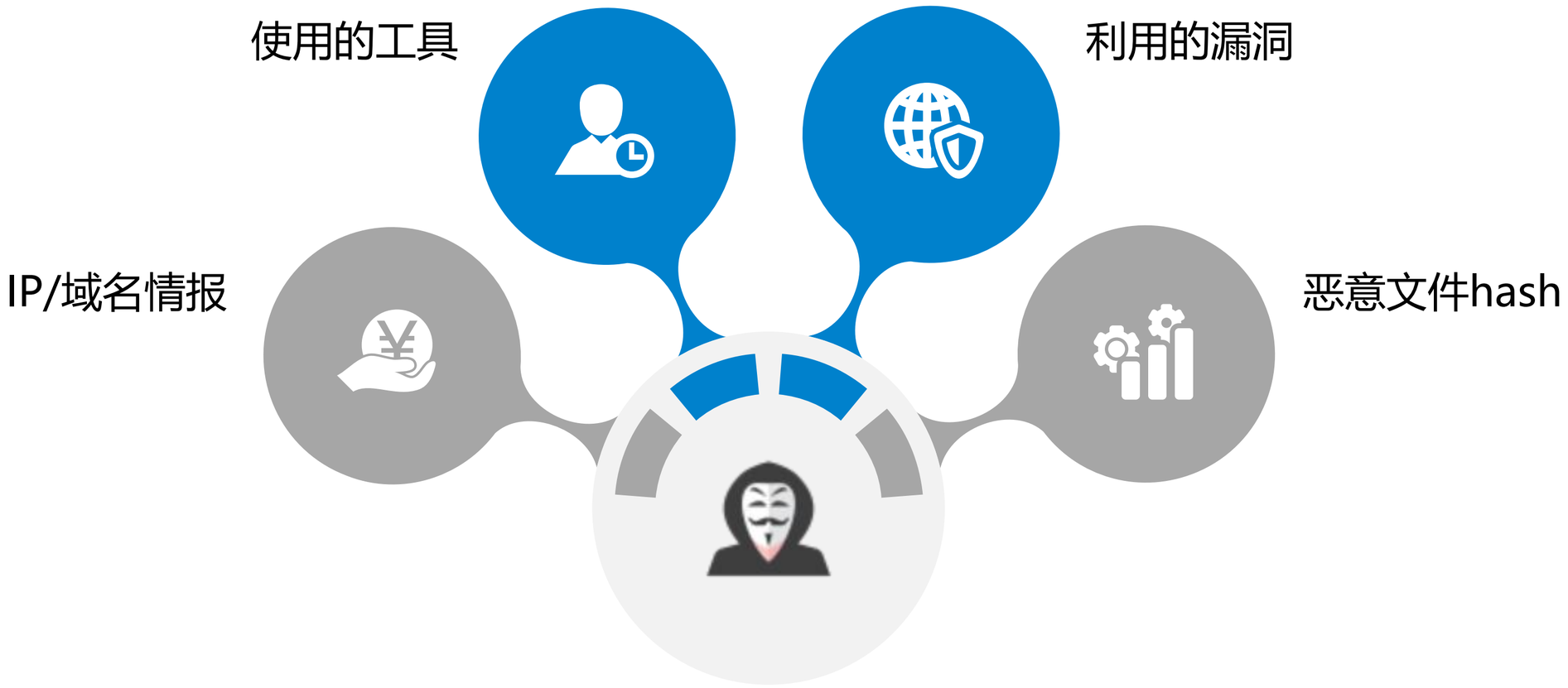
02 在事件定级时作为参考

03 在告警间的关联关系建立提供参考

扫描攻击IP



溯源画像



√ 利用黑客画像信息里的相关性信息挖掘衍生事件

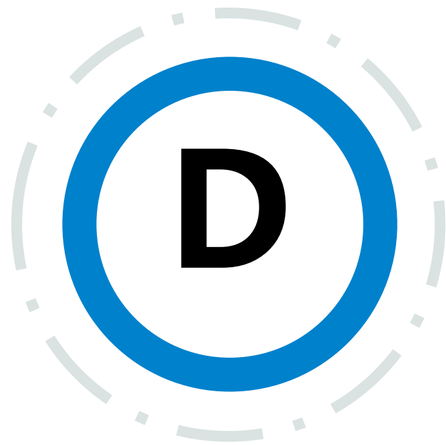
主动防御，自适应玩法

情报解析

高级战略情报、热点事件、热点漏洞都可做为输入项

策略加固

基于情报在防护设备增加对应策略，进行有效阻断



场景化监测

将情报场景化，建立基于该场景的监控参数及规则

响应恢复

开展响应动作，调整优化策略

主动防御

ThreatBook 微步在线

2018 网络安全分析与情报大会

01 情报获取

【微步在线报告】金融黑客团伙Cobalt2.0最新动向分析

微步情报局 2018-07-04 16:36:13 200人浏览

TAG：高级可持续攻击、APT、Cobalt、Cobalt2.0、鱼叉式网络钓鱼、JS后门、

TLP：黄（仅限接受报告的组织内部使用）

日期：2018-06-27

概要

2018年5月至今，微步在线监测发现，有金融黑客团伙持续针对俄罗斯、独
伙的TTP与Cobalt组织极为相似，因此有安全公司将之归因到Cobalt组织，但该
系。根据该团伙与Cobalt极为相似的TTP，以及Cobalt头目于2018年3月26日被
t演变而来，并将之称为Cobalt2.0。

本报告分析了该团伙近来的相关攻击活动，以及所使用的技术和工具，具体内容

- Cobalt2.0近来活动极为频繁，主要通过伪装McAfee等知名安全厂商、App
的银行供应链，针对俄罗斯、独联体和西方国家的银行进行攻击。

- Cobalt2.0在6月18日盗走了美国最大ATM机供应商Diebold Nixdorf的域名di
xdorf向多家银行发送钓鱼邮件。

- Cobalt2.0近来主要利用包含CVE-2017-8570、CVE-2017-11882和CVE-20

02 策略加固

域名(14)
api.asus.org.kz
api.outlook.kz
apple-istores.com
cloud-direct.biz
dieboldnixdorf.us
documents.total-cloud.
ecb-europa.info
mail.halcyonih.com
mail.xstorage.biz
mcafeecloud.us

- 防火墙
- IPS

Hash(10)
1247e1586a58b3be11
476c9d4383505429c1
4c51fd1242f93990718
4e78b0218d8bd445fe7
7762bfb2c3251aea23f
8656cbb114deb0f2e81
a30a00670c851162f28
af9ed7de1d9d9d38ee1
e4081eb7f47d76c57bb
e566db9e491fda7a5d2

- 防火墙
- IPS
- 防病毒
- 邮件网关

03

场景化监测

外连情报命中

病毒告警命中

告警：已攻陷
响应：下线

漏洞利用告警

沙箱检出告警

EDR告警

告警：被攻击
响应：阻断

安全响应前置

漏洞发布

2小时
漏洞扫描
扫描告警
（单位：万）

4小时
发现漏洞设备
6小时
内部通报漏洞

8小时
入侵设备
入侵告警
（单位：万）

12小时
漏洞验证&变更
方案制定

24小时
内网渗透
内网渗透告警
（单位：万）

36小时
漏洞修复

40小时
数据收集
数据库审计告警
（单位：万）

48小时
打包带走
流量异常告警
（单位：万）

安全响应前置

漏洞发布

2小时
漏洞扫描

4小时
发现漏洞设备

阻断

8小时
入侵设备

下线

24小时
内网渗透

40小时
数据收集

48小时
打包带走

2小时
漏洞利用阻断及
监测规则部署

4小时
漏洞利用告警

8小时
设备攻陷告警

36小时
漏洞修复

响应时间：36小时 VS <1小时?

情报分享

加强安全事件响应能力，提升行业整体安全水平

降低安全运营成本，促进安全运营能力的建设

掌握行业安全动态，提升行业间合作能力

情报分享原则

保密性	仅限特定范围内流转
相关性	非必要信息不可共享
最小传播	在情报信息必要最小范围传播
可追溯	准确记录共享内容、共享时间以及信息使用方
信息归属	信息共享者所有，有权要求使用者立即停止使用并销毁（销毁权归属）
依法执行	涉及执法机构依法进行案件调查时，应征得上级单位批准后，进入相关流程
隐私保护	在情报信息申请单位内最小范围传播（情报提供者隐私，情报指向者隐私）
分类分级	依法对隐私信息、敏感信息的收集及处理进行严格的管理及保护
技术依托	信息共享过程中需采取必要的技术手段对信息实施保护

ThreatBook

感谢您的观看

2018 网络安全分析与情报大会