中信建投证券
CHINA SECURITIES

安全运营中威胁情报的应用

汇报：姜明元　　**时间：**2018.7.20

现状&目标

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

流转

打通情报流转网络及通路，消除情报孤岛

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

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

情报几种分类

01

机读IOC情报

作为重要的运营情报形式，包含恶意IP、域名、文件Hash、IP信誉等

02

高级战略情报

完整的披露某个攻击团伙或攻击事件的具体细节

04

开源情报

互联网上各种公益组织公开的免费情报，广泛收集并未加工验证

03

商用情报

专人维护、提供情报上下文信息，精度高

自定义情报：企业可进行情报自生产、自使用、自评估，实现企业网络安全威胁 情报的外部能力快速吸收以及内部自身能力的成长

情报整合（评估）

基于外部收集的信息、多情报间对比判断情报信息的准确率。同时根据情报分析结果反馈的误报情况进行评估

对各个源当前的有效情报，针对情报的行业、地域、威胁类型等方面的覆盖度进行判定

每次情报更新时，对每个情报的及时性进行对比，对于其它源已经更新的情报数据，认定为及时性较差

每次情报更新时，对情报源之间的相互重叠度进行评估，定期计算一定时间段内的情报重叠度均值

情报整合（冲突）

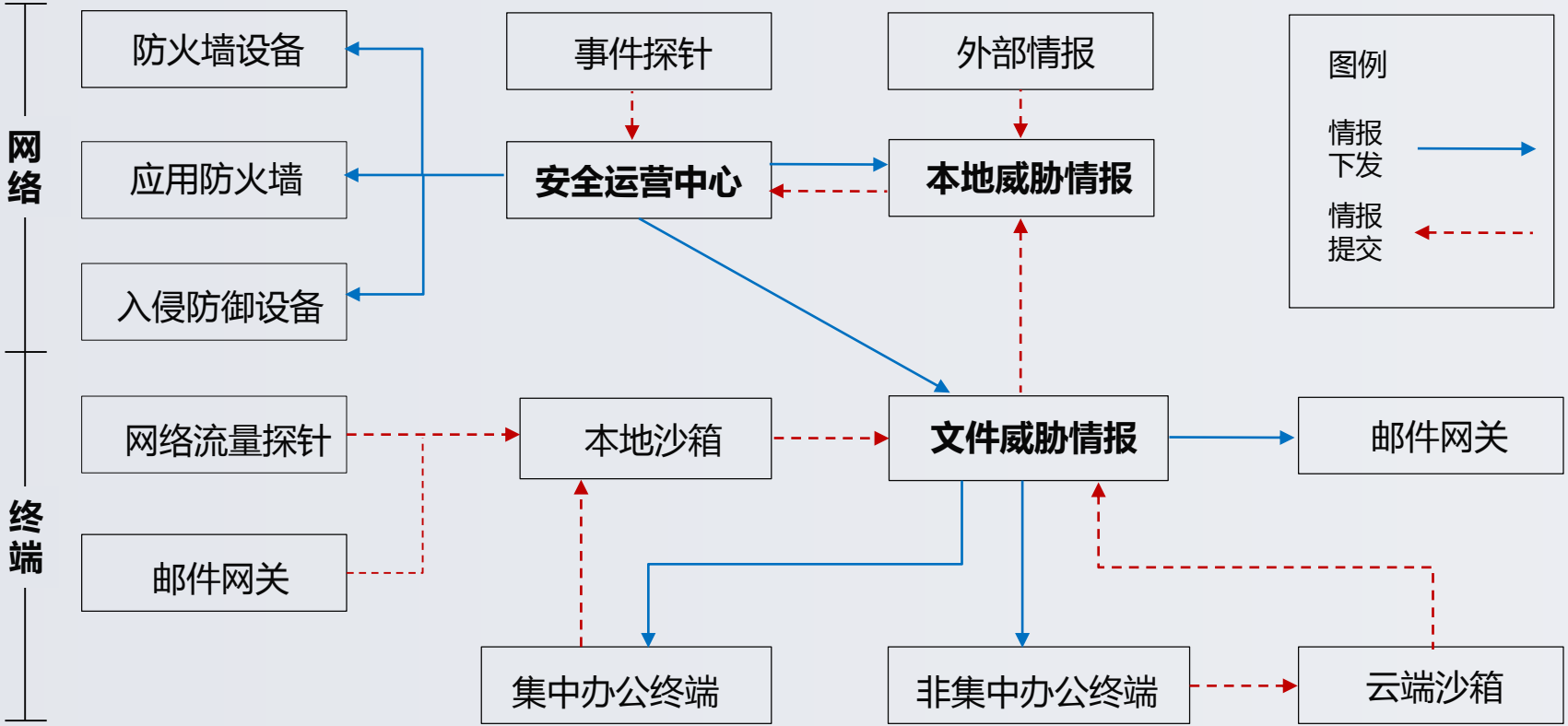
情报数据的整合通常遵循最大集合原则，既将所有情报源字段进行理解后，去重、合并并拼凑在一起，形成一个最大集合。

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

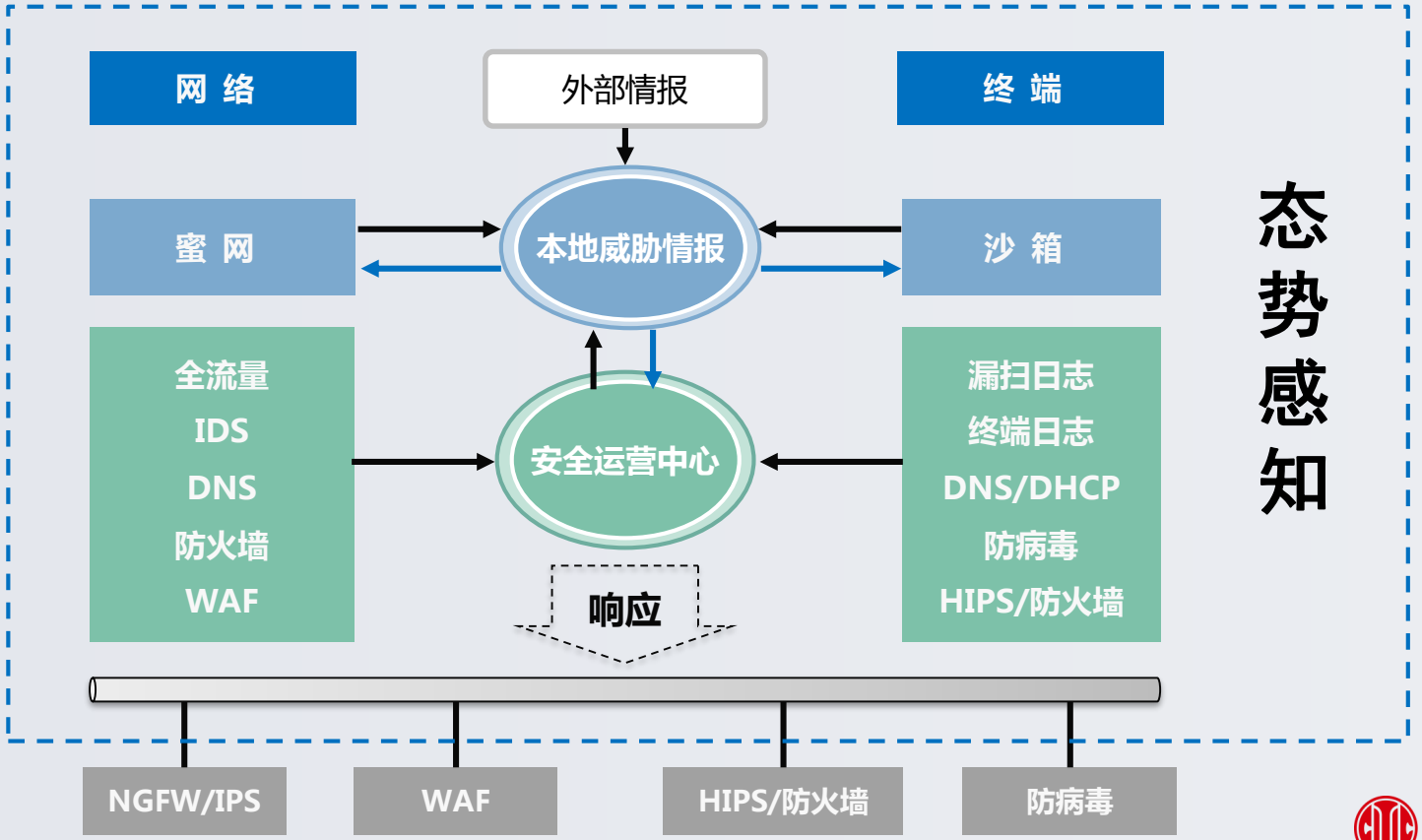
使用一定的算法产生唯一值：投票法、一票否决、一票认可、权重计算（根据不同情报源特征给出不同权重比例）

中信建投证券 CHINA SECURITIES

情报流转



安全运营



安全运营+情报

攻陷分析

外连与情报进行碰撞比对，快速定位攻陷主机

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

溯源画像

利用威胁情报中的关联性、对黑客进行画像

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

中信建投证券 CHINA SECURITIES

攻陷分析

01

URL情报

DNS、对外通讯日志

02

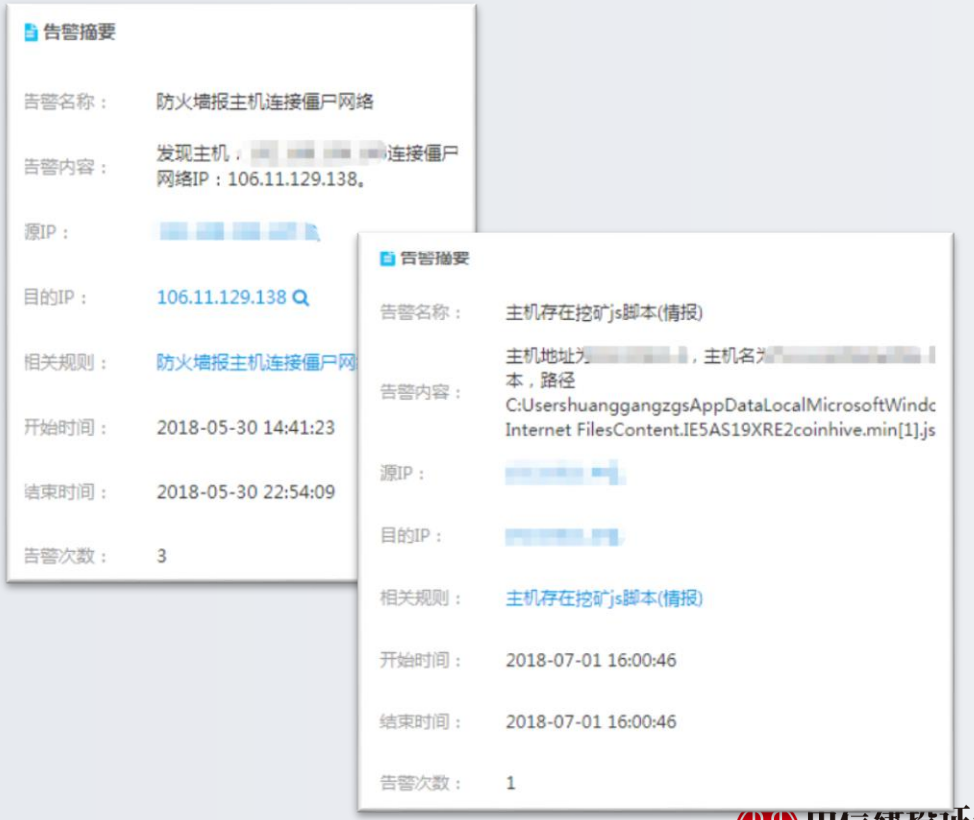
IP地址

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

XX黑客团体

IP：1.1.1.1

XX漏洞利用

域名：cc.hacker.com

扫描告警

入侵告警

外联告警

情报关联

通过黑客画像信息里的相关性信息，也可应用于安全分析工作中挖掘衍生事件

主动防御

高级战略情报、热点事件、热点漏洞都可做为输入项

基于情报在防护设备增加对应策略，进行有效阻断

将情报场景化，建立基于该场景的监控参数及规则

开展响应，调整优化策略，持续开展事件监控及运营

主动防御

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

中信建投证券 CHINA SECURITIES

主动防御

03 场景化监测

外连情报命中

病毒告警命中

已攻陷

下线

漏洞利用告警

沙箱检出告警

EDR阻断告警

被攻击

黑名单阻断

建立行业情报意义

01

加强对行业开展的定向攻击的安全抵御能力，提升行业整体安全水平

02

激励并促进机构成员的安全分析能力的建设

03

利于掌握行业安全动态，随时开展行业范围内的应急响应及追溯工作，提升行业间合作能力

行业情报共享原则

保密性	仅限行业内流转，不可跨机构共享
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

行业情报共享面临问题

01

行业运营机构权威性保障

由行业内权威的技术服务机构负责运营

02

提交情报质量保障

通过与外部情报源进行比对，行业内情报及命中比对评估情报质量

03

情报流转标准技术及知识产权保障

加工商业情报上报的情况及自主生成情报上传的知识产权需事先明确

04

情报下发准确度保障

机读情报通过结合外部情报进行加工整合，高级威胁情报通过人工确认验证进行下发

中信建投证券 CHINA SECURITIES

中信建投证券
CHINA SECURITIES

谢谢观看