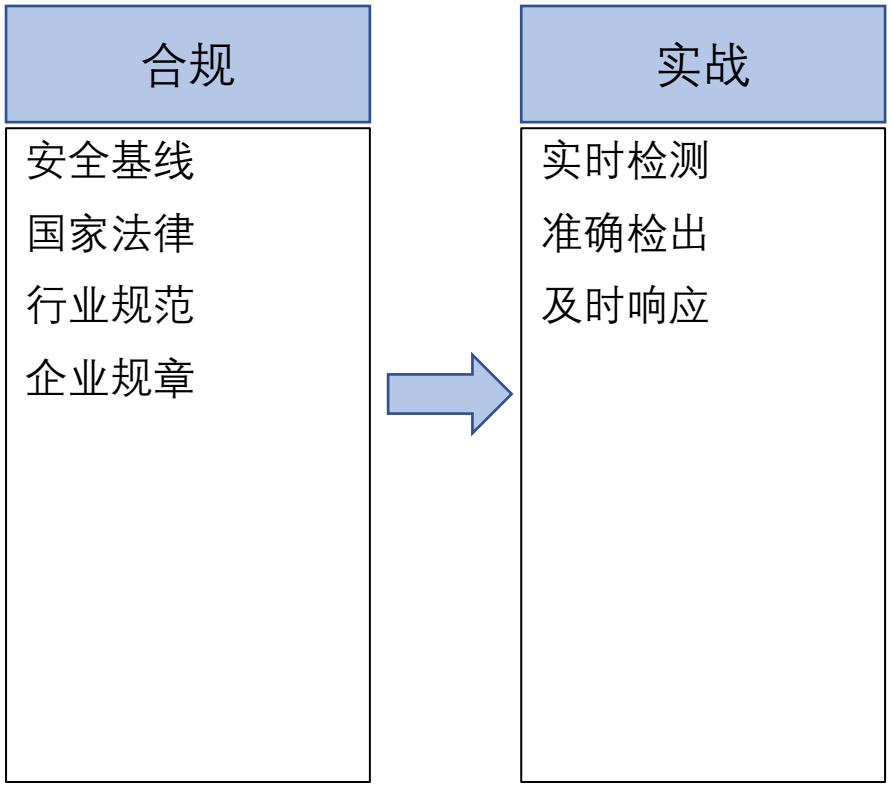
CSA Summit
云安全联盟峰会

基于威胁情报的云安全检测技术

演讲人：王亮

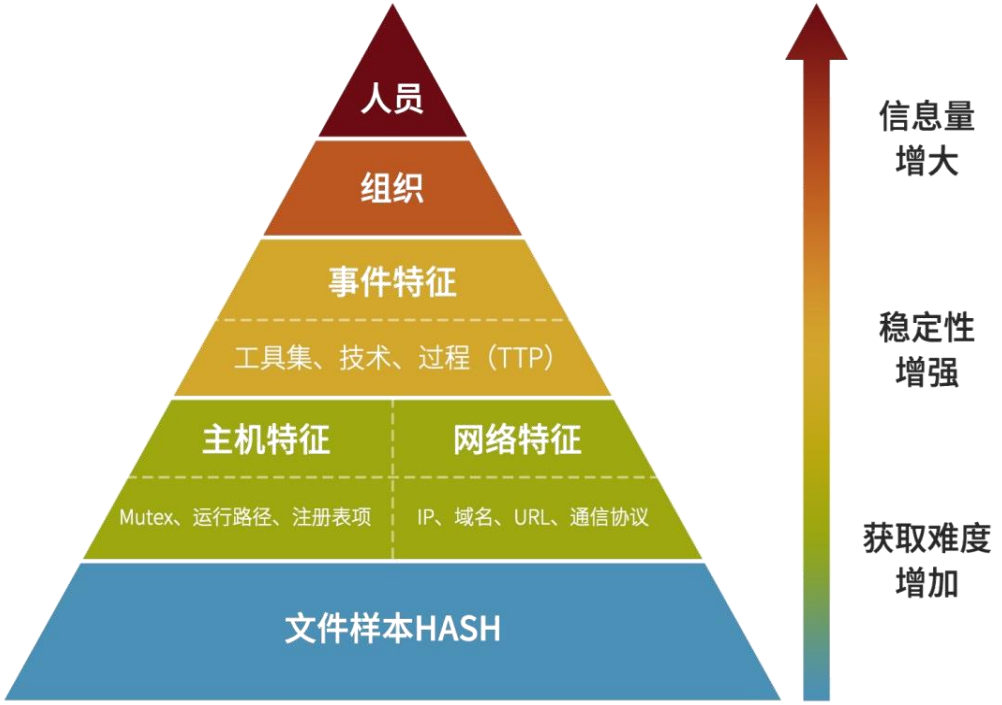
攻防实战能力在云安全重要性逐步提高



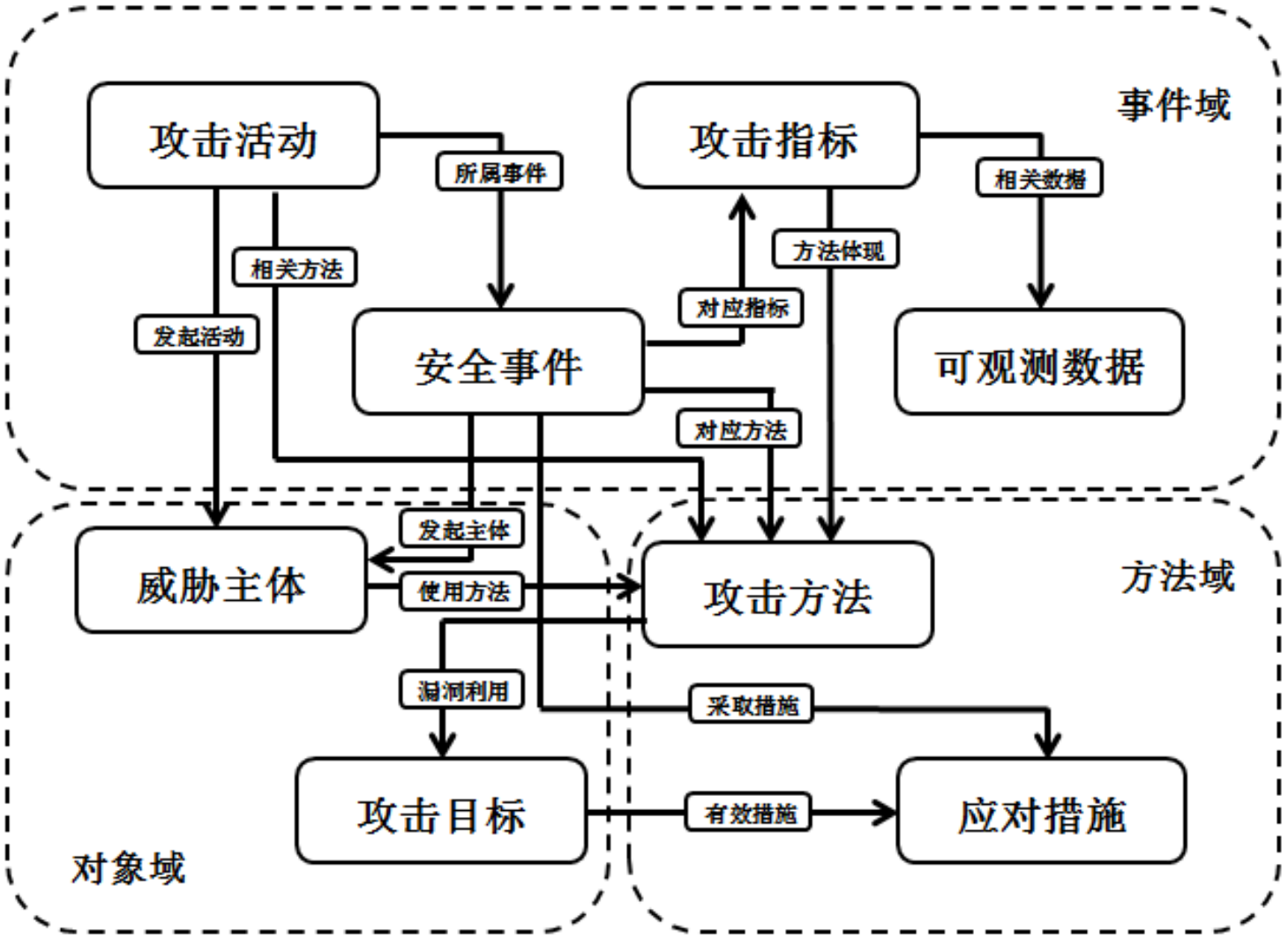
- 检测响应已经从传统企业环境转向云计算环境。
- 云厂商的安全体系已覆盖事前管理、准备，事中检测响应，事后恢复的闭环。安全团队已经不止关注传统的清理和被动防护的工作，开始向主动防御的工作转移；
- 威胁情报作为有效的威胁检测机制被广泛应用于云计算场景

威胁情报的定义

- Gartner的定义
  - 威胁情报是某种基于证据的知识，包括上下文、机制、标记、含义与可行的建议，这些知识与资产所面临已有的或酝酿中的威胁或危害相关，可用于对这些威胁或危害进行响应的相关决策提供信息支持。
- 一个泛化的定义
  - 信息安全的语境下，一切与威胁相关的数据、信息以及知识。



网络安全威胁信息模型



对象域-威胁主体和攻击目标构成攻击者与受害者的关系；

事件域-攻击活动、安全事件、攻击指标和可观测数据则构成了完整的攻击事件流程；即有特定的经济或政治目的、对信息系统进行渗透入侵，实现攻击活动、造成安全事件；而防御方则使用网络中可以观测或测量到的数据或事件作为攻击指标，识别出特定攻击方法；

方法域-在攻击事件中，攻击方所使用的方法、技术和过程（TTP）构成攻击方法，而防御方所采取的防护、检测、响应、回复等行动构成了应对措施；

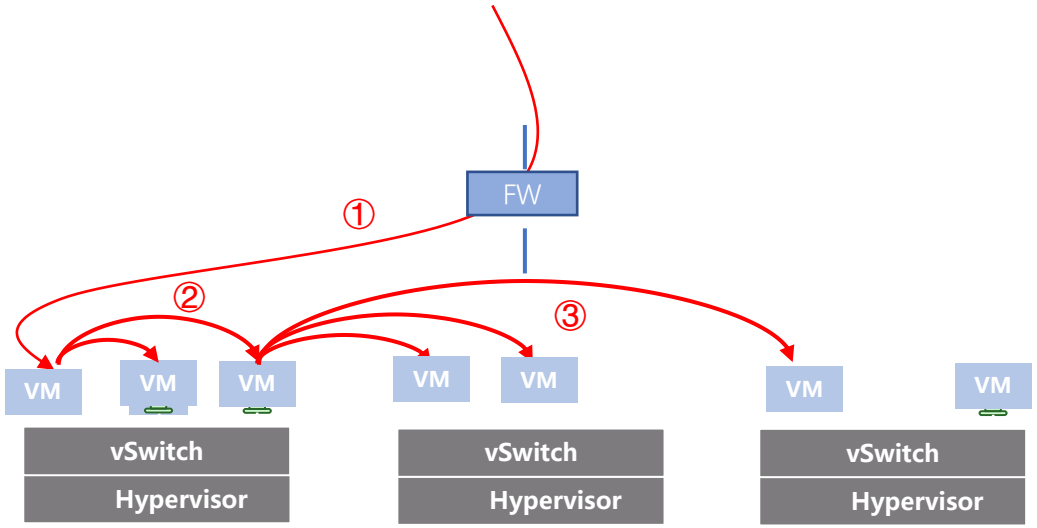
可机读威胁情报 - 失陷威胁数据

CSA Summit 云安全联盟峰会

- IOC（Indicator Of Compromise，失陷检测指标）
  - 主要类型：IP、域名、文件Hash、邮箱、数字证书等
  - 最基础最具可用性的威胁情报类型，标示已成功的攻击，少量，精准
  - 指示被僵尸网络、网络蠕虫、木马后门、APT攻击所控制的系统
- 威胁覆盖全面
  - 多维度来源安全基础数据
  - 开源及商业情报数据应收尽收
  - 强运营动静态自动化处理工具和平台
- 可指导行动的上下文
  - 专业团队整合攻击组织来源、目的、具体危害、所使用资源等判断处置所需的信息

fget-career.com::	black		Ramnit远控木马活动事件	493
maple110.3322.org::	black		Artemis Botnet C&C活动事件	188
imddos.my03.com::	black		Artemis Botnet C&C活动事件	184
bo.user-accounts.info::	black		FakeLPK Botnet C&C活动事件	133
www.mojimojimojimoji.com::	black		Nitol Botnet C&C活动事件	132
dingtao333.3322.org::	black		Artemis Botnet C&C活动事件	89
xmr.crypto-pool.fr::	black		MinerdPool矿池异常访问事件	74
cncert-sinkhole.net::	black		普通远控木马活动事件	65
fafa6.com	black		普通远控木马活动事件	59
x.hktianhong.com	black		普通远控木马活动事件	58
che521123.3322.org::	black		普通远控木马活动事件	54
a.cashspeedloanbank8282.com	black		普通远控木马活动事件	49
trafficconverter.biz::	black		Surge远控木马活动事件	47
kukutrustnet777.info::	black		普通远控木马活动事件	43
update.wanyou7.com::	black		普通远控木马活动事件	42
221.130.179.36:8080:	black		Zegost远控木马活动事件	42
www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com::	black		WannaCry勒索软件活动事件	42
kjwre77638dfqwieuoi.info::	black		普通远控木马活动事件	41
tlb1.3322.org::	black		DSL4 Botnet C&C活动事件	40
k00k58k70.ticp.net::	black		Gh0st RAT远控木马活动事件	37

云计算场景攻击路径



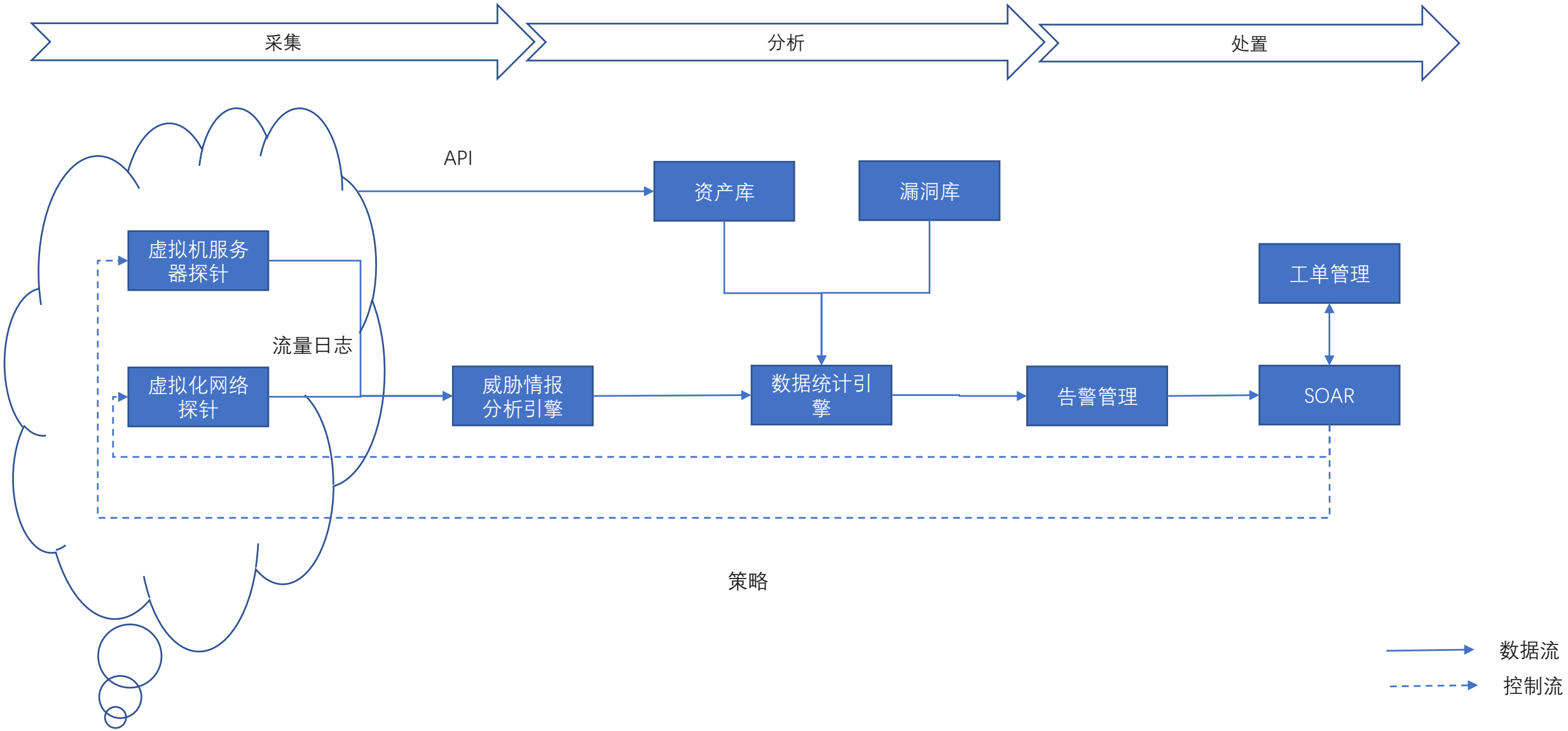
典型的攻击方式：

- 黑客通过正常登录方式登录到云内某台虚拟机，期间由于是正常登录流量，防火墙、IDS等基于规则的无法防护及告警
- 黑客通过与虚拟机加密的隧道，传输恶意文件；恶意文件运行后，开始对云内网进行信息扫描采集，并对其它虚拟机进行攻击感染，攻击结束后进行痕迹清理
- 被攻击感染的虚拟机作为跳板，继续对其它虚拟机进行攻击

整个感染攻击阶段，边界及主干网络中的安全设备：

- 网络攻击已经呈现弱特征性、多阶段性、高传染性，在东西向环境中高级威胁更加的多样化；
- 快速检出需要性能高检出率高的算法引擎；

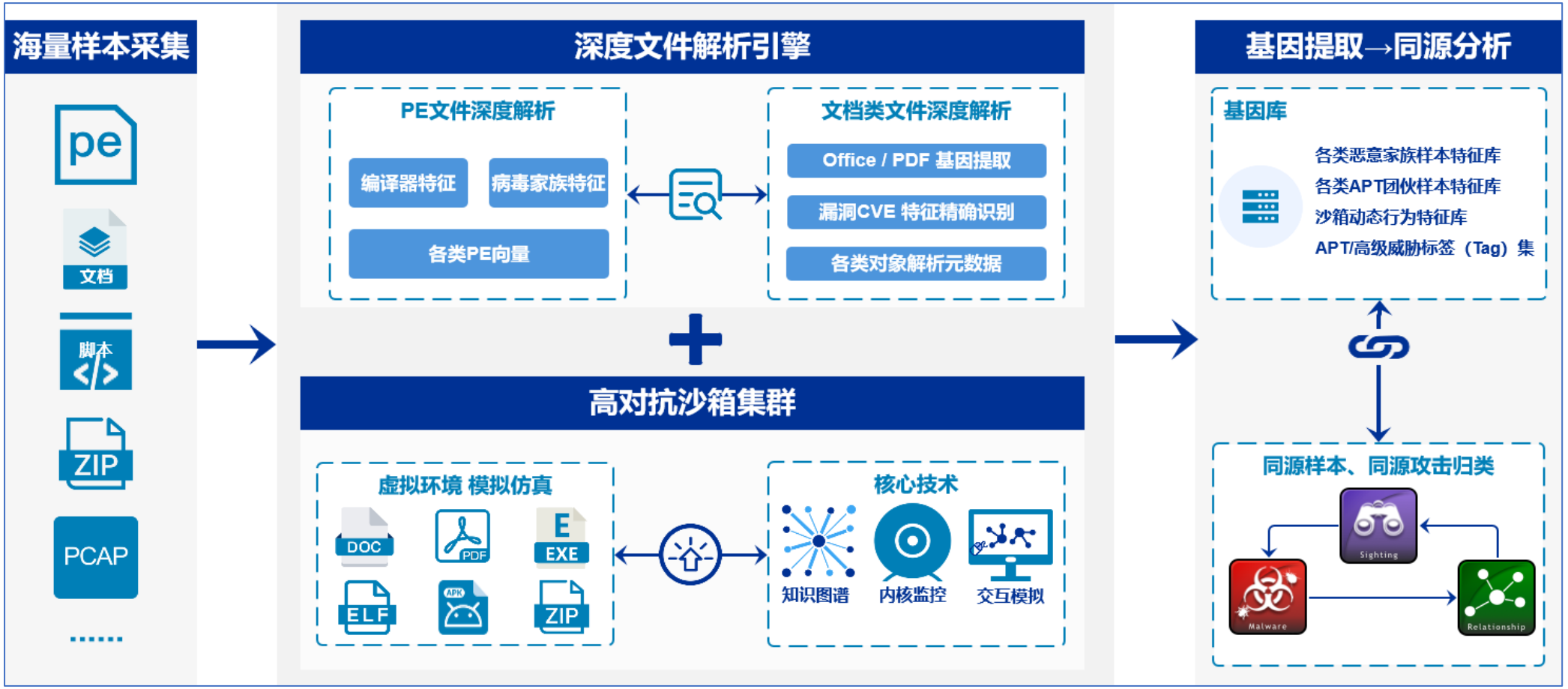
威胁检测业务流程


采集
分析
处置
API
资产库
漏洞库
虚拟机服务器探针
流量日志
虚拟化网络探针
威胁情报分析引擎
数据统计引擎
告警管理
工单管理
SOAR
策略
数据流
控制流

核心技术 – 动静态结合的文件深度分析

CSA Summit 云安全联盟峰会

- 基于样本静态深度解析提取的元数据和利用高对抗沙箱收集的动态活动信息，通过基于机器学习的同源分析发现和识别高级攻击相关的样本

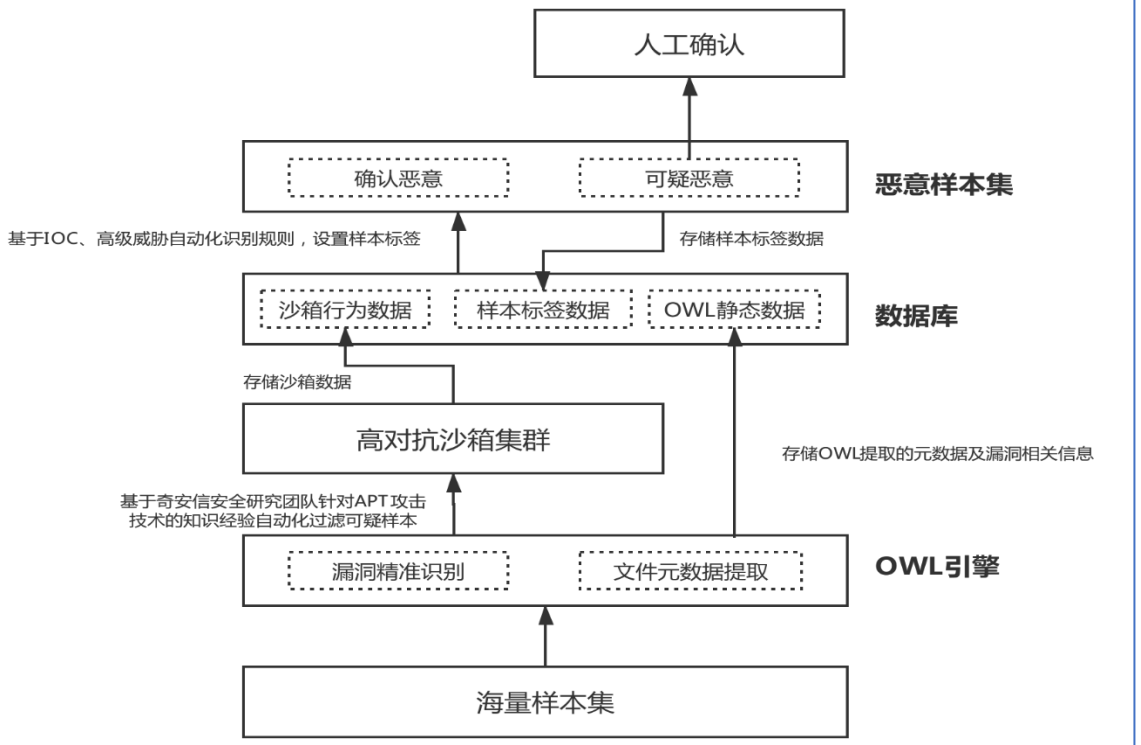


核心技术 – 高级威胁发现运营流程

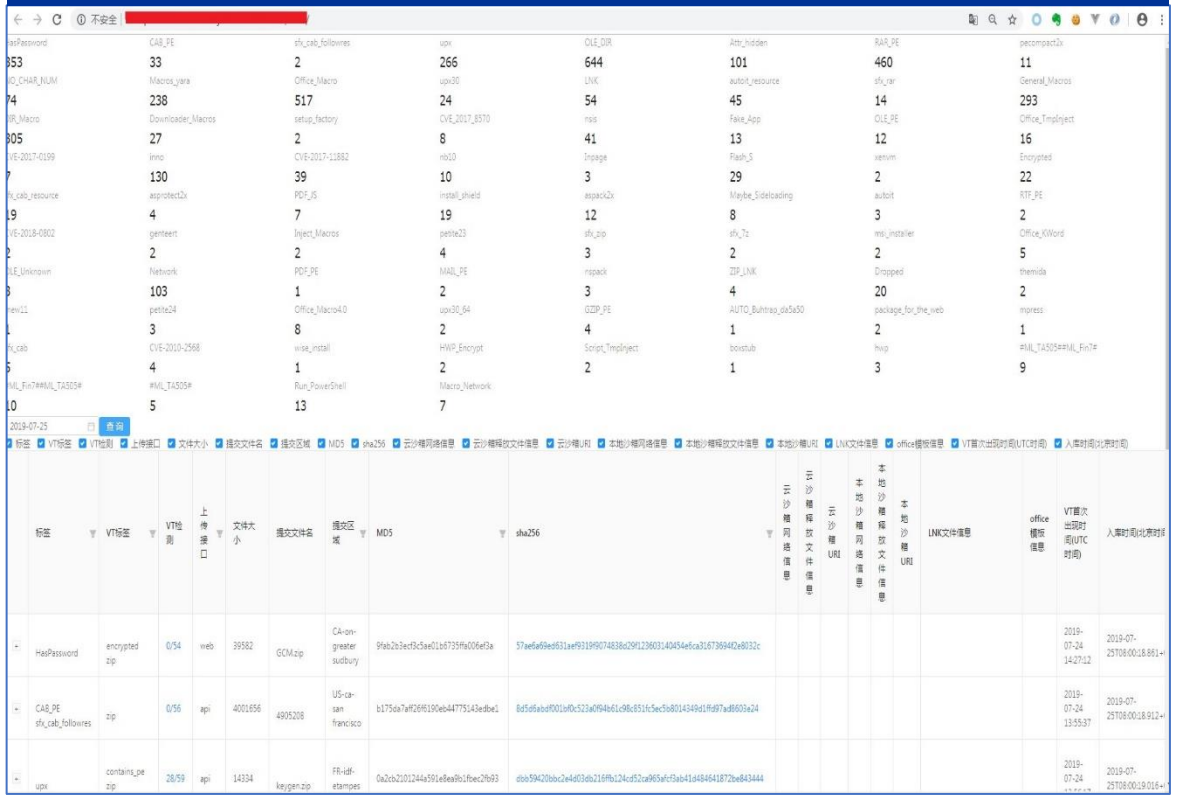
CSA Summit 云安全联盟峰会

- 深度文件元信息提取引擎，结合沙箱输出的网络行为数据，基于规则匹配和机器学习的同源分析输出对文件的TAG，最终由分析人员确认

高级威胁发现流程



运营流程：tags 特征关联驱动威胁发现



云内资产感染状态感知

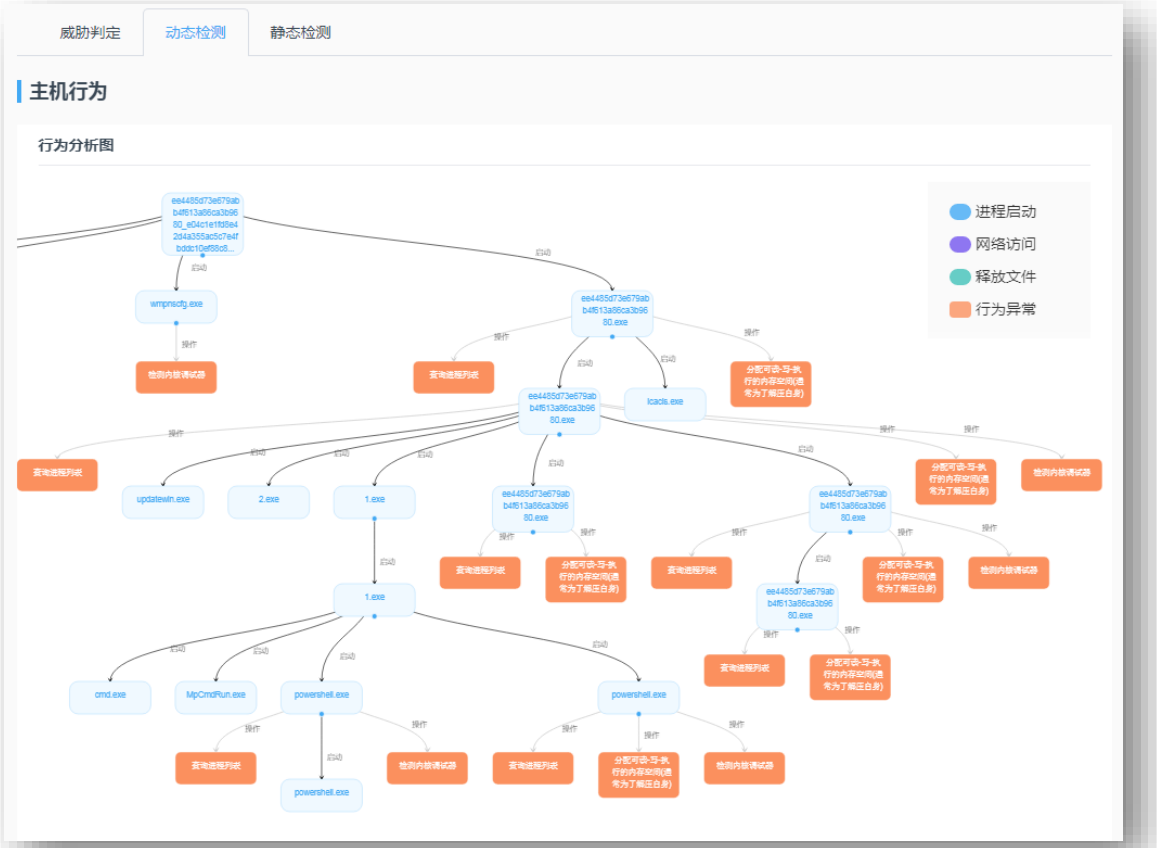
CSA Summit
云安全联盟峰会

- 通过对IP，Domain，URL比对获得外发数据感染信息
- 判断云内资产失陷情况


```
{
    "data": {
        "botnet_info": [
            {
                "botnet_family": "MinerdPool",
                "botnet_type": "黑市工具",
                "latest_botnet_time": "2018-11-30"
            }
        ],
        "geo": {
            "city": "北京",
            "country": "中国",
            "latitude": "39.904989",
            "longitude": "116.405285",
            "province": "北京"
        },
        "geo_detail": {
            "city": "",
            "country": "",
            "district": "",
            "latitude": "",
            "longitude": "",
            "province": "",
            "town": ""
        },
        "malicious_info": {
            "ddos_confidence": "40%",
            "is_brute_force": false,
            "is_ddos": true,
            "is_ddos_active_or_passive": "active",
            "is_malicious": true,
            "is_scanner": true,
            "is_spam": false,
            "is_web_attacker": true,
            "latest brute force time": "",
            "latest_ddos_time": "2019-01-07",
            "latest_malicious_time": "2019-01-07",
            "latest_scanner_time": "2017-08-10",
            "latest_spam_time": "",
            "latest_web_attack_time": "2018-12-22",
            "scanner_confidence": "40%"
        },
        "normal_info": {
            "asn": "AS23724",
            "asn_org": "IDC, China Telecommunications Corporation",
            "block_impact": "1",
            "is_idc": true,
            "is_proxy": false,
            "latest_domain": "",
            "latest_domain_time": "",
            "latest_proxy_time": "",
            "proxy_type": "",
            "user_type": "境内IDC"
        },
        "summary": {
            "block_impact": "1",
            "ip": "221.122.70.7",
            "is_botnet": true,
            "malicious_label": [
                "DDOS",
                "SCANNER",
                "WEB_ATTACKER"
            ],
            "network_type": [
                "IDC"
            ]
        }
    },
    "message": "success",
    "status": 10000
}
```

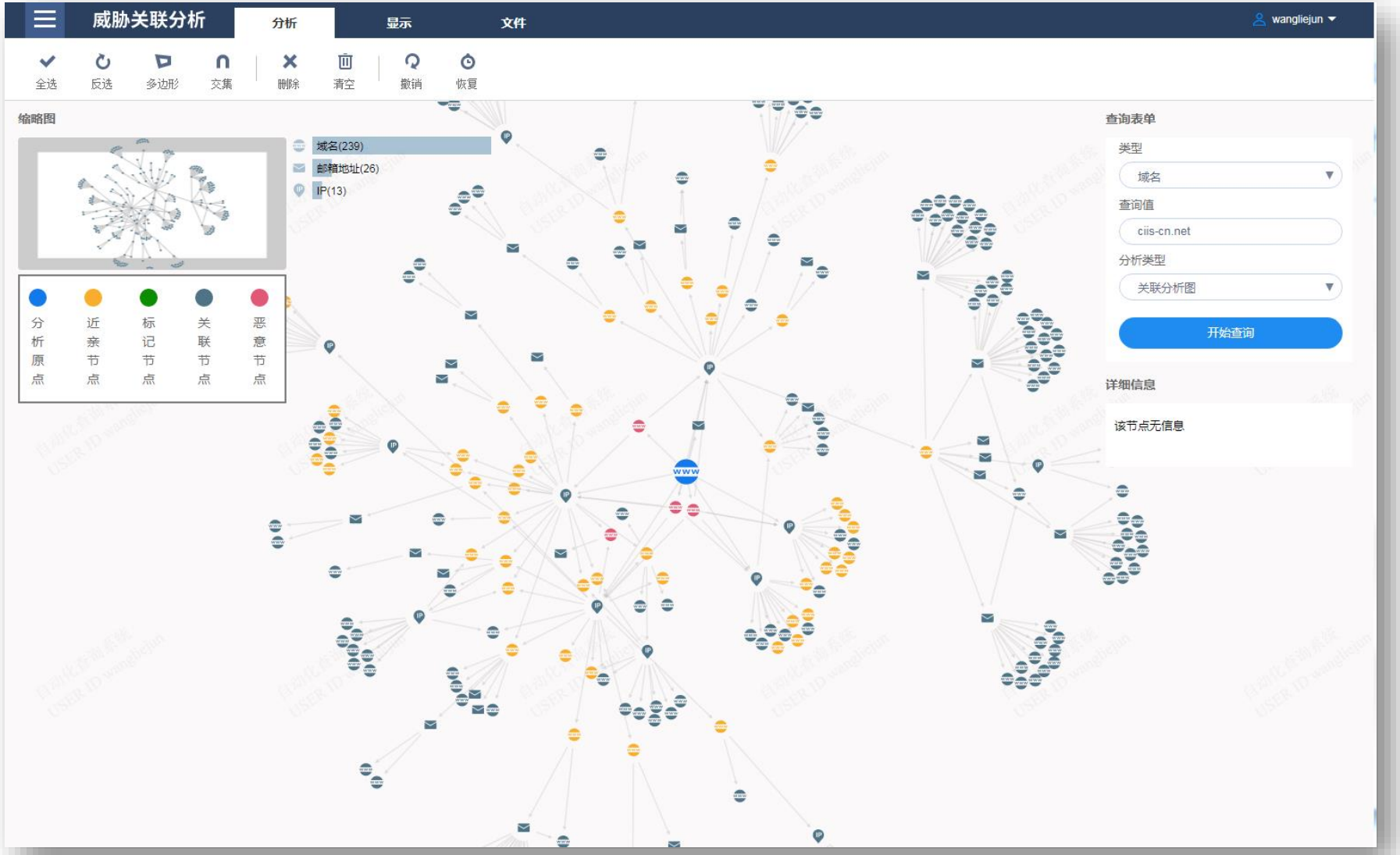
恶意文件传播途径绘制

- 文件类型与恶意代码家族
- 判断恶意文件感染路径



攻击路径分析溯源

- IP、域名、文件的可视化关联分析
- 进行攻击路径分析，维攻击溯源提供数据依据



2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

CSA Summit
云安全联盟峰会

THANKS

云助战疫，安全无疆