ADCONF

阿里云网络安全团队

保障阿里云基础设施安全+云平台管控安全。

最全最快的发现入侵行为，并在最短时间内完成响应止血，防止风险的进一步扩大的同时，逐步演进提升整体防控水位。

SPEAKER

> 阿里云安全专家

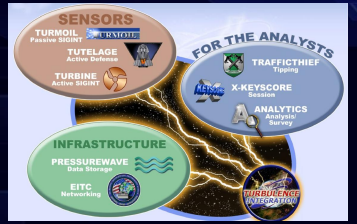
> 连续六年参加国家大型攻防演练活动

> 公安部一所特聘攻防讲师

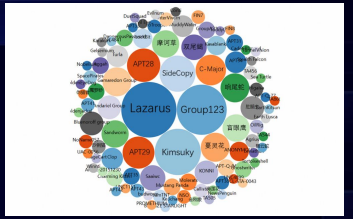
> 曾在POC，ISC等安全峰会分享攻防议题

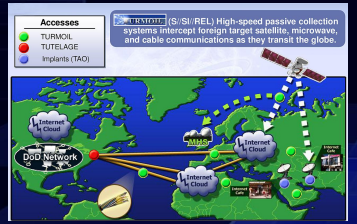
> 目前专注高级威胁检测与能力度量

网空威胁形势严峻

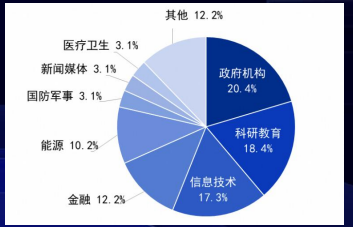

SENSORS
TURMOIL
Passive SIGINT
TUTELAGE
Active Defense
TURBINE
Active SIGINT
FOR THE ANALYSTS
TRAFFICTHIEF
Tipping
X-KEYSCORE
Session
ANALYTICS
Analysis/ Survey
INFRASTRUCTURE
PRESSUREWAVE
Data Storage
EITC
Networking
TURBULENCE
INTEGRATION


CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE


Lazarus
Group123
APT28
SideCopy
C-Media
Kimsuky
APT29


Accesses
TURMOIL
TUTELAGE
Implants (TAO)
(S//SI//REL) High-speed passive collection systems intercept foreign target satellite, microwave, and cable communications as they transit the globe.
Internet & Cloud
DoD Network
MHS


VS
BLUE TEAM
RED TEAM


其他 12.2%
医疗卫生 3.1%
新闻媒体 3.1%
国防军事 3.1%
能源 10.2%
金融 12.2%
政府机构 20.4%
科研教育 18.4%
信息技术 17.3%

攻击威胁变化趋势

人工智能辅助加持

WormGPT、FraudGPT等生成式AI暗潮涌动，降低攻击者上手门槛同时减少用户特征。

开源工具降低门槛

开源共享理念为攻击者提供了大量优质单兵作战工具，大幅降低学习、制作成本。

移动端攻击趋增

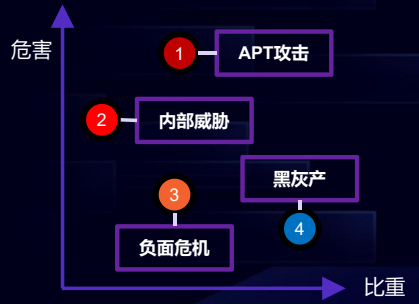
卡巴斯基曾披露了针对 iOS 设备的 Operation Triangulation 完整攻击链。其中串联了 4 个 0day 漏洞，具备极高隐蔽性和攻击复杂度。

供应链攻击不断

针对供应链组件攻击不断发生，一旦攻击者控制了供应链的一个节点，影响面就会覆盖到下游的所有用户且行为十分隐蔽。

企业面临风险威胁拆解

威胁象限



主要面临4类安全威胁，其攻击危害和攻击比重如图所示

威胁特点

1	1. 防御难度高 2. 目标明确，长期潜伏，有组织，有技术，攻击资源丰富
2	1.防御难度高 2.攻击门槛相对较低 3.伴随主观恶意情况下，不易被发现
3	1.防御难度中 2.对商誉、品牌或业务正在进行的商业行为造成影响
4	1.防御难度低 2.广撒网无差别式攻击，技术门槛不高

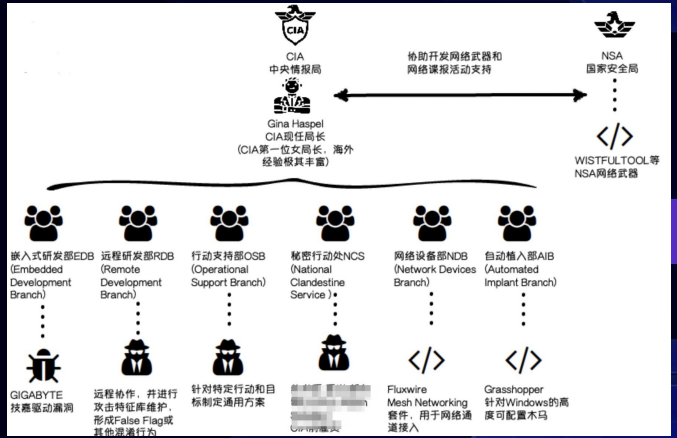
攻击对手

1.商业竞争对手 2.网络犯罪集团 3.国家背景组织
1.正式员工 2.外包员工 3.访客
1.商业竞争对手 2.安全自由职业者 3.来自监管等政府单位
1.中低端黑产从业者 2.脚本小子

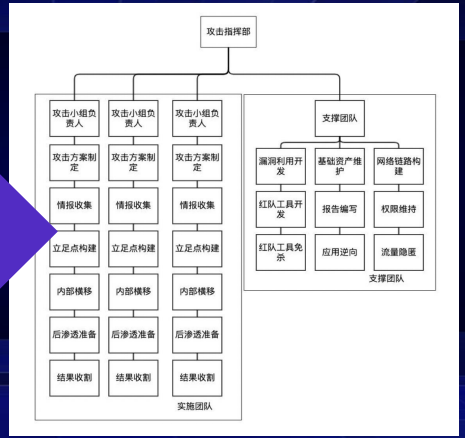
攻击手法

1.利用定向社工、钓鱼、水坑、web攻击结合内网渗透等复杂综合手段； 2.具备0day资源和针对安全设备的免杀、绕过等对抗能力
1.利用自身或借用他人权限，通过导出、拷贝、上传、爬取、截图、拍照、甚至口口相传等途径获取目标信息 2.离职员工凭据复用
1.利用一些安全事件，进行舆论炒作，达到影响品牌的目的； 2.监管单位举办大型攻防演练活动，失分可能对公司品牌造成影响
1.通过批量钓鱼、扫描传播诈骗、蠕虫、勒索病毒； 2.以破解、免费、绿色版等名义推广间谍、僵尸软件

某国谍报部门在网络战场景下角色划分->专业团队



师夷长技
以制夷



实施团队

攻击团队负责具体作战计划的实施、目标靶标攻击等工作

小组作战，TL统筹目标情况，组员能力覆盖不同方向

支撑团队

负责团队资产维护、链路构建

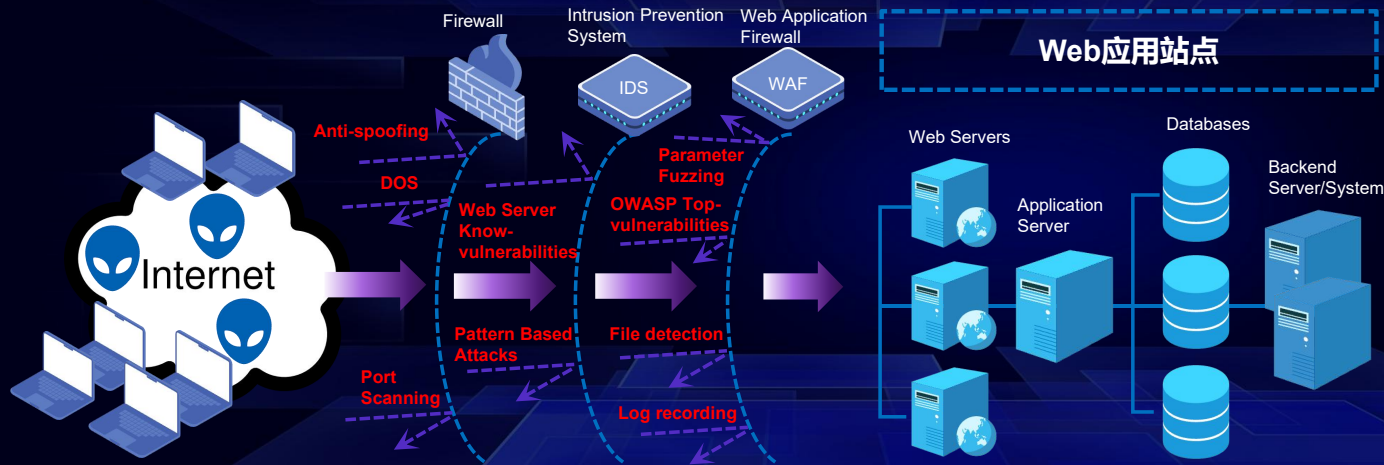
工具武器化、平台构建、后渗透维持

研究团队

技战术研究、漏洞武器化、攻击方案制定

前瞻性技术拓展、定制化0day挖掘

传统边界防御存在的不足



传统边界面临挑战：

1. 边界资产仍暴露在外部视线中，资产测绘/主动探测尽收眼底；

2. 不同产品能力参差不齐，检测手段多是基于规则和黑白名单，面对于未知攻击只是时间问题；

3. 业务系统难以统一身份认证，无法做到联动封禁、身份关联。

面对“专业团队”的攻击对抗

ADCONF

反侦查
（降低侦查获取的信息有效性）

网络信息搜索引擎对抗

资产识别对抗
端口存活性/应用指纹/域名/蜜饵服务

脆弱性识别欺骗
WEB漏洞探测/利用有效性欺骗

短兵对抗
（降低风险被发现的可能）

入向：漏洞EXP拦截
漏洞POC欺骗
分钟级接口止血
高风险接口止血

出向：DNS分析检测
异常模型检测
恶意域名劫持

攻击压制
（消耗攻击者资源）

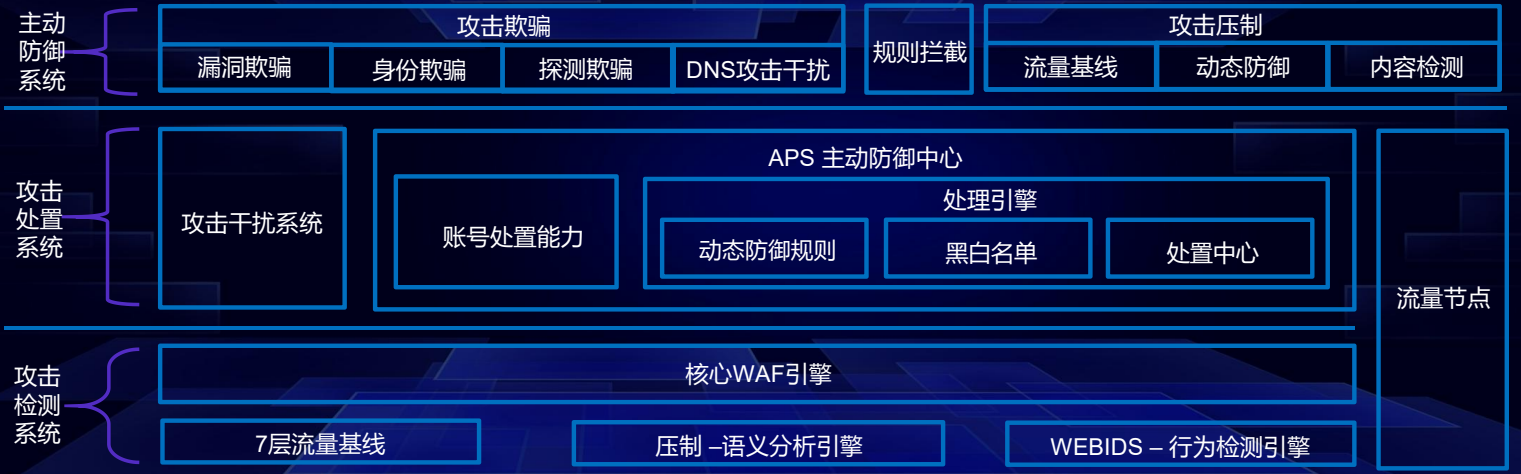
资产：全域一键封禁

账号：用户账号/子账号

域名劫持/流量特征封禁

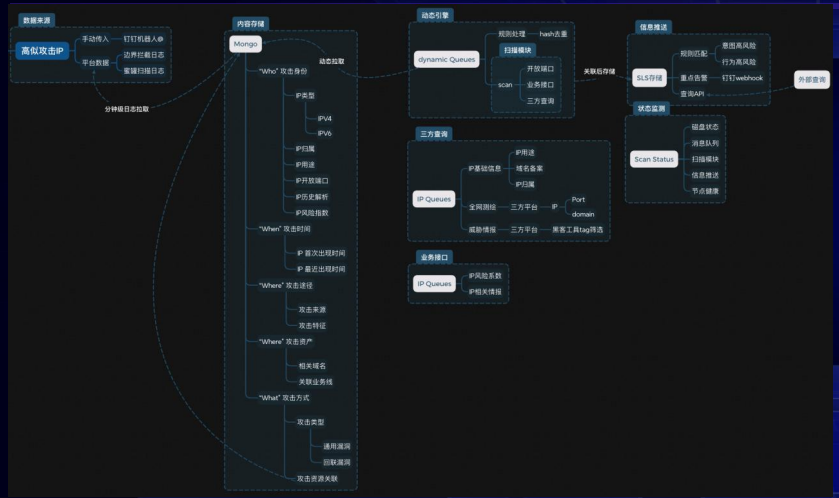
攻击特征识别/流量基线识别

面对“专业团队”的攻击对抗



基于“5W”攻击资源特征关联实践CASE

基于“5W”攻击资源特征关联实践CASE



ip: 8.8.8.8
attack_type: scan,revere_scan
attack_service: 业务线a
ip_location: 中国江苏南京某机房
ip_port: ["22/open/tcp/ssh"]
ip_ioc_score: 0
use_tools: xray
reverse_ip: 7.7.7.7

Host	Count
dataapi.a.cn	11
my.a.cn	11

Type	Count	Percent
RCE	12	0.54545
RFI/LFI	6	0.272727
SQLi	4	0.181818

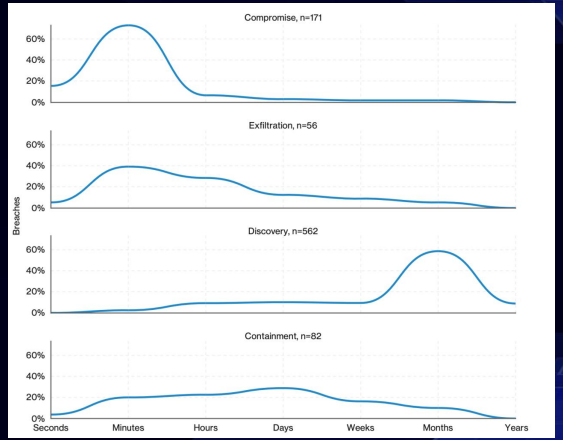
ip: 7.7.7.7
attack_type: scan
attack_service: 业务线b
ip_location:中国香港某云厂商
ip_port: ["80/open/tcp/http"]
ip_ioc_score: 8
ip_history_domain: test.hack.com
use_tools: burp

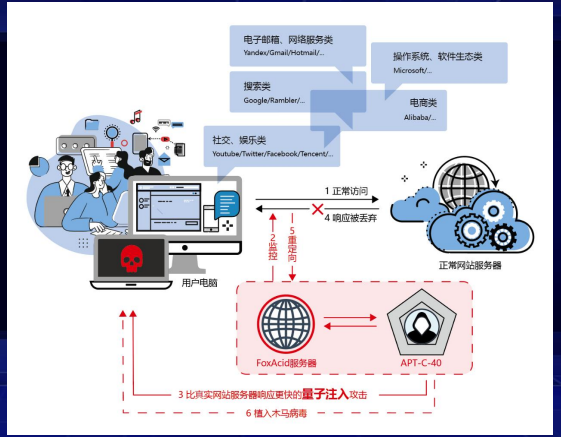
Host	Count
admin.b.cn	14

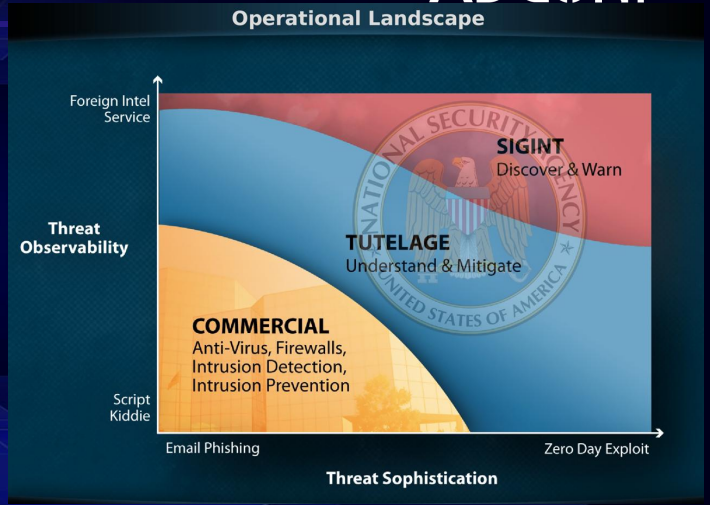
Type	Count	Percent
XSS	7	0.5
SQLi	7	0.5

联系人：张三 联系邮箱：wode@qq.com 所在公司：某公司攻击队

面对“特殊背景”的定向攻击







基于语言模型的WAF检测引擎实践CASE

ADCONF

> 使用“数据清洗-预训练-调优”技术路线，实现基于语言模型的 WAF 引擎，完全无正则，并具备可运营能力

> 上下文窗口 2K， 8 卡 V100 处理能力 600QPS

1. 亿级混合log预训练数据数据
2. 自训练分词器

1. 5 次预训练尝试
2. 8卡 V100 约3月预训练时长

1. 3 次模性调优尝试
2. 分层多步骤调优

1. 无法检出的攻击可快速添加检测能力，无需重训练
2. 每种攻击可根据需要调整检测敏感度

基于语言模型的WAF检测引擎实践CASE

ADCONF

```
GET /faq.php?action=grouppermission&gids[99]=%27&gids[100]
[0]=)%20and%20(select%201%20from%20(select%20count(*),concat((select%20con
cat(user,0x3a,md5(1234),0x3a)%20from%20mysql.user%20limit%200,1),floor(rand(0
)*2))x%20from%20information_schema.tables%20group%20by%20x)a)%23
HTTP/1.1
accept: */*
accept-encoding: gzip
host: mp[redacted]
ns-client-ip: [redacted]
proxy-client-ip: 5[redacted]
user-agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
```

```
POST /award/queryEventInfo?actId=1e7px902j5uq2atd&app=ucnews-
iflow&bi=800&bm=P3W&bt=UM&ch=uc%40uc_bdsem_origin&dn=48539916672-
f14bccf4&ds=bTkwBEK4yLdfSV9WBC9xIPlddkJwA2iieTVesXxih1IvZQ%3D%3D&eve
ntid=usercenter&fr=android&from=welfareagency&jb=0&kt=4%27and%2F%2A%2A%
2Fextractvalue%281%2Cconcat%28char%28126%29%2Cmd5%281901293064%29%
29%29and%27&la=zh-
cn&mi=ONEPLUS+A6000&mt=uJ8BymZLPEgNEwKSdjeL5M6%2F8agrRapv&nI=bTk
wBMzCGgWgGLdakXmzG4we6pNzVYlbwRVGvvtNuRcqcnY%3D&nt=2&nw=WIFI&nx
=&og=&pf=145&pi=1080x2154&pr=UCMobile&ss=411x820&uc_biz_str=S%3Acusto
m%7CC%3Afull_screen&uc_param_str=mtutdsdnfrpfbivesscpgimibtbmnijblauputog
pintnwktprchmt&uc_wx_params=mtutdsdnfrpfbivesscpgimibtbmnijblauputogpintnw
ktprchmt&up=&ut=AATyVUa7TOtGiREASCaP0EmS7rjr0PVXgBbet2xTJrO4Ng%3D%3
D&ve=17.1.1.1342&wv=5.7.188.3&xs=N96FH1msyq%2FdBzHB2VU8T3X9doFo1d29
GogVSYz2%2FLegbL%2FkIubKzDPrI9xbfXsdcfxe%2FjI3ttSY%2B9jO5wWGLXYtRZcM
LZxq8xhPaRqB5ZRe9svuhjvfotfV7N%2B2FjEeEubm9%2BIT%2FPLnzI6xUS9YpzgI
HTTP/1.1
accept: */*
accept-encoding: gzip
accept-language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
content-length: 0
content-type: application/x-www-form-urlencoded
hos[redacted]
ns-client-ip: [redacted]
proxy-client-ip: 5[redacted]
referer: https
user-agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
```

系统

生成特征向量

人工设置敏感度

AI引擎

检测结果

```
{
    attack_type : "SQLi"
    similarity : 0.8056640625
    token_len : 652
    similar_category : "SQLi"
}
```

可运营性

1、无需任何正则知识即可运营

2、训练样本中没有的攻击类型可快速添加。语言模型具备泛化能力，无需模型重训练

3、泛化敏感度可调，以适应准召

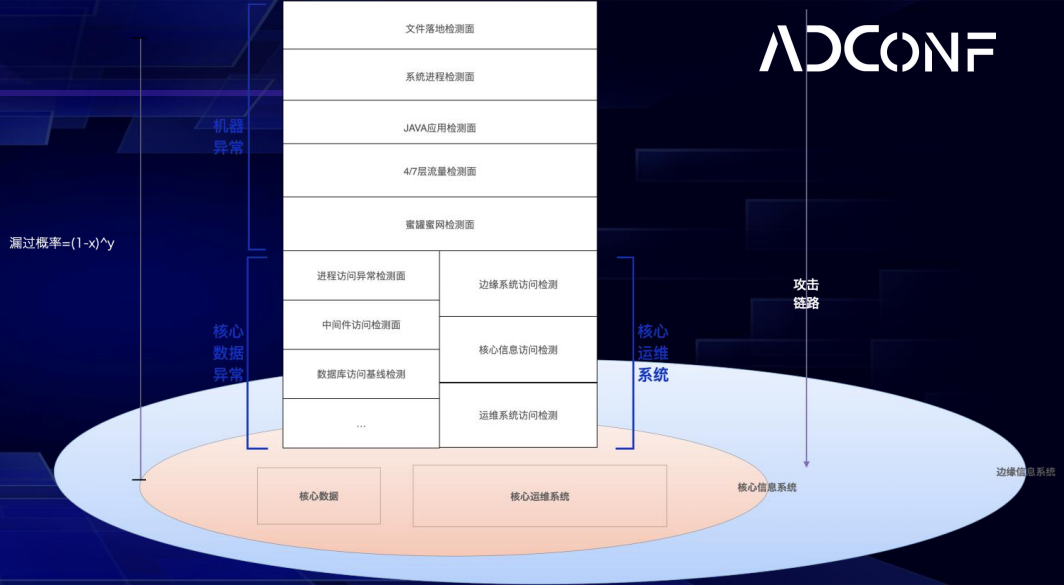
通过构造应用/机器的基线，解决新出现的攻击手法检测问题

应对漏过：

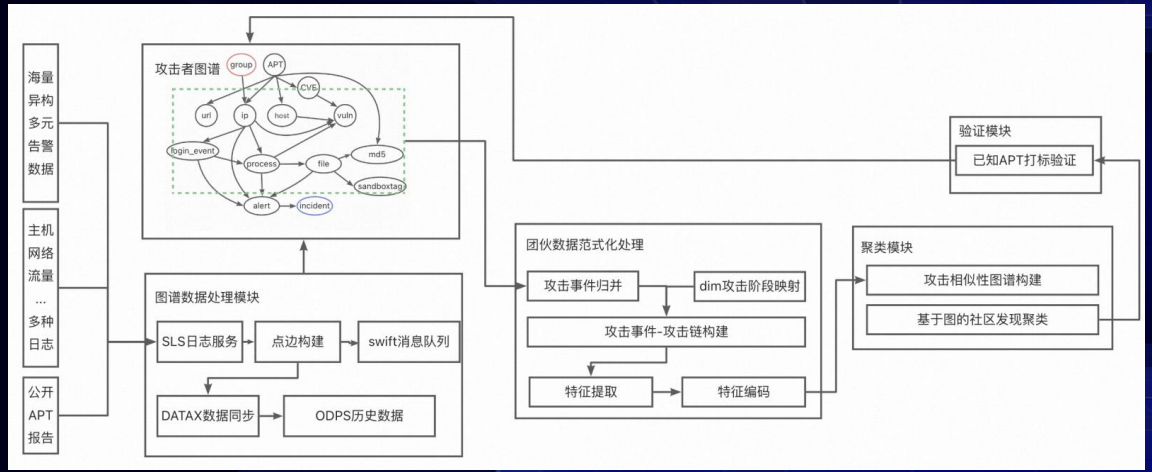
针对 **机器异常、核心运维异常、核心数据异常** 三层分层检测体系进行安全事件的兜底检测。

相信概率：

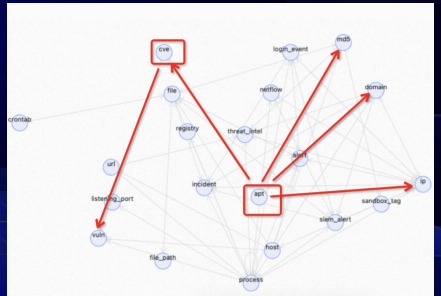
攻击者绕过检测可能
= (文件检测漏过概率)*(进程检测漏过概率)*(…)*(流量层漏过概率)
= 每一层检测面漏过概率的**乘积**

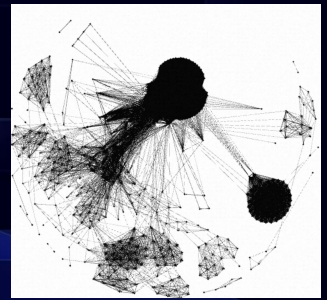


基于知识图谱攻击者意图团伙聚类分析实践



基于实时生成的包含多条攻击链的攻击源数据，以攻击源 IP 为核心，抽取其中的特征生成特征点，并连接特征点和核心点。





云上安全数字化建设

ADCONF

数智化趋势下的发展机遇与安全

- 数智技术驱动产业加快转型升级
- 数智化发展带来的隐患与挑战

公共云安全治理愿景与框架

- 治理理念：云上安全共同体
- 治理目标：更强安全性与更低成本
- 治理框架

云上安全重要支柱

- 1.全流程产品安全保障建设
- 2.全方位红蓝对抗反向校验
- 3.坚守数据主权的数据安全保护
- 4.全链路身份管控与精细化授权
- 5.安全防护能力高效弹性可扩展
- 6.面向线上威胁的快速响应与恢复
- 7.面向攻击的安全高可用
- 8.全球化背景下的合规支撑

云上安全建设最佳实践

- 全面上云：淘宝云上安全建设实践
- 助力发展： 关键行业云上安全最佳实践
- 迎接未来： AI大模型云上安全最佳实践

https://developer.aliyun.com/topic/download