KCon

KCon 2019 無界

云环境自动化入侵溯源实战

徐越 阿里云安全工程师

WHOAMI

- @cdxy_
- 安全工程师@阿里云
- 企业安全/入侵检测与响应
- 数据分析/机器学习爱好者

2015 2016

2019

响应速度是企业安全能力的核心体现

告警

安全运营

是否误报?

漏洞? 攻击路线?

黑客背景? 目的?

影响哪些资产和账号?

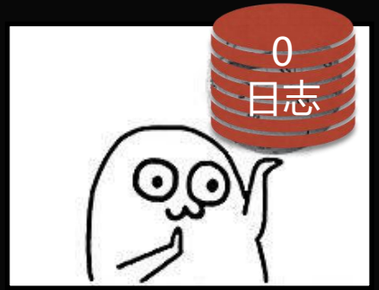
泄露哪些数据?

是否存在内部违规操作?

...

安全运营现状

又来告警了

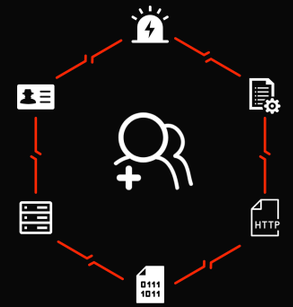


看看怎么被入侵的

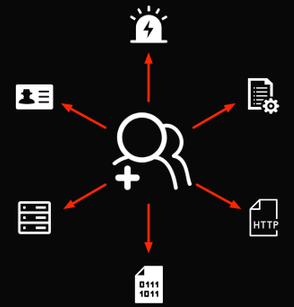
看看怎么被入侵的

安全运营流程中的技术问题

数据缺失



系统孤立



人工检索

[自动化入侵回溯] 多源异构数据的知识表达

采集

云原生的数据采集方案

满足90%以上事件调查

计算

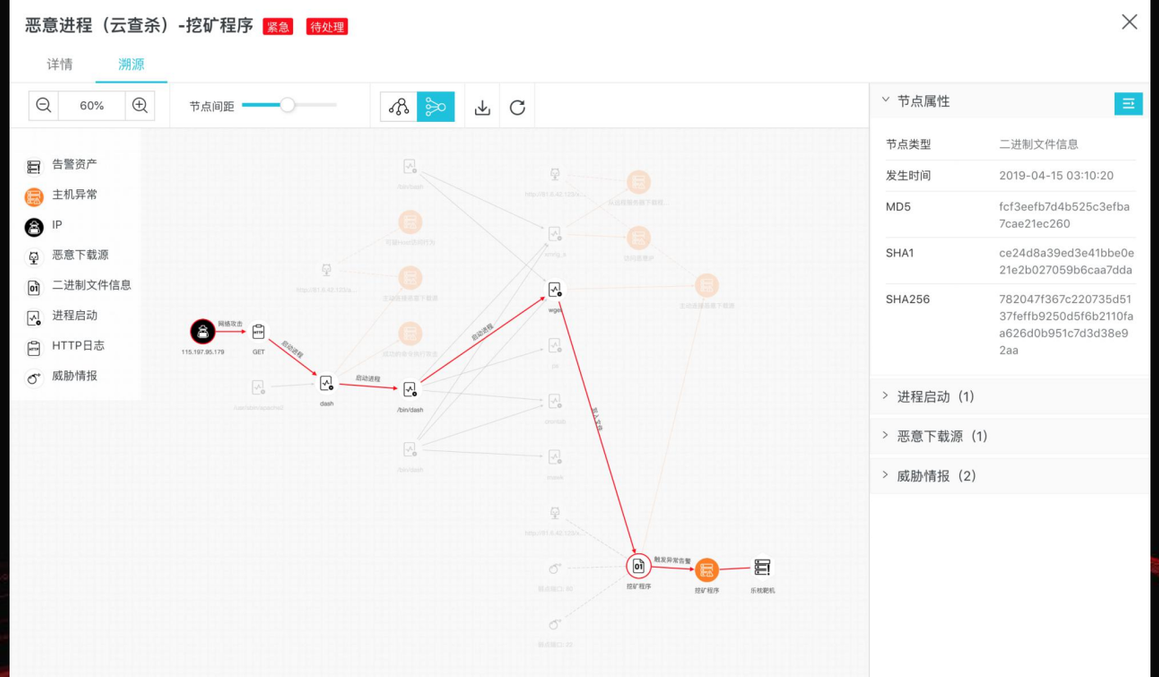
千万级RPS实时流计算

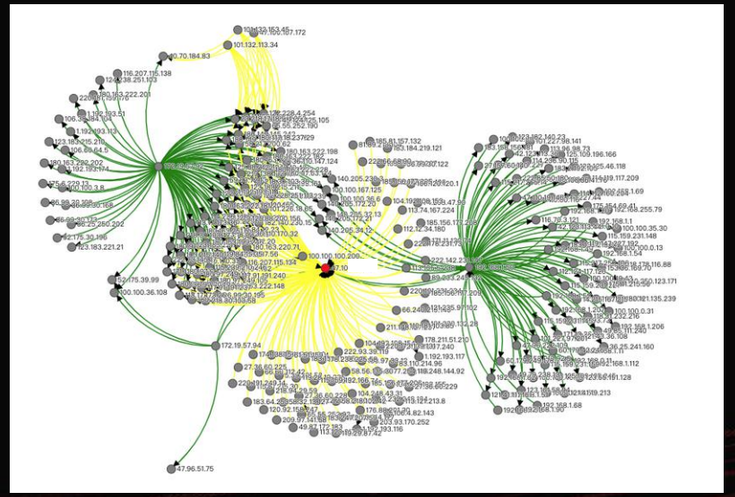
自动寻找入侵相关信息

交互

图结构可视化

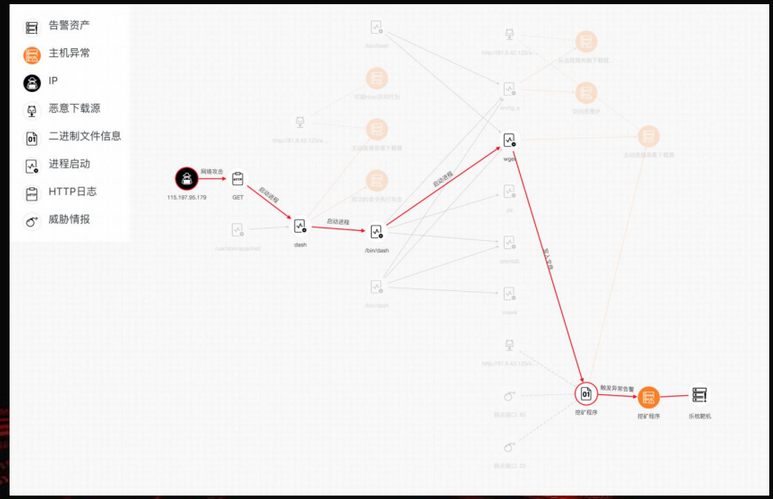
还原入侵链路


恶意进程（云查杀）-挖矿程序
紧急
待处理
详情
溯源
60%
节点间距
告警资产
主机异常
IP
恶意下载源
二进制文件信息
进程启动
HTTP日志
威胁情报
节点属性
节点类型
二进制文件信息
发生时间
2019-04-15 03:10:20
MD5
fcf3eefb7d4b525c3efba7cae21ec260
SHA1
ce24d8a39ed3e41bbe0e21e2b027059b6caa7dda
SHA256
782047f367c220735d5137feffb9250d5f6b2110fa626d0b951c7d3d38e92aa
进程启动（1）
恶意下载源（1）
威胁情报（2）

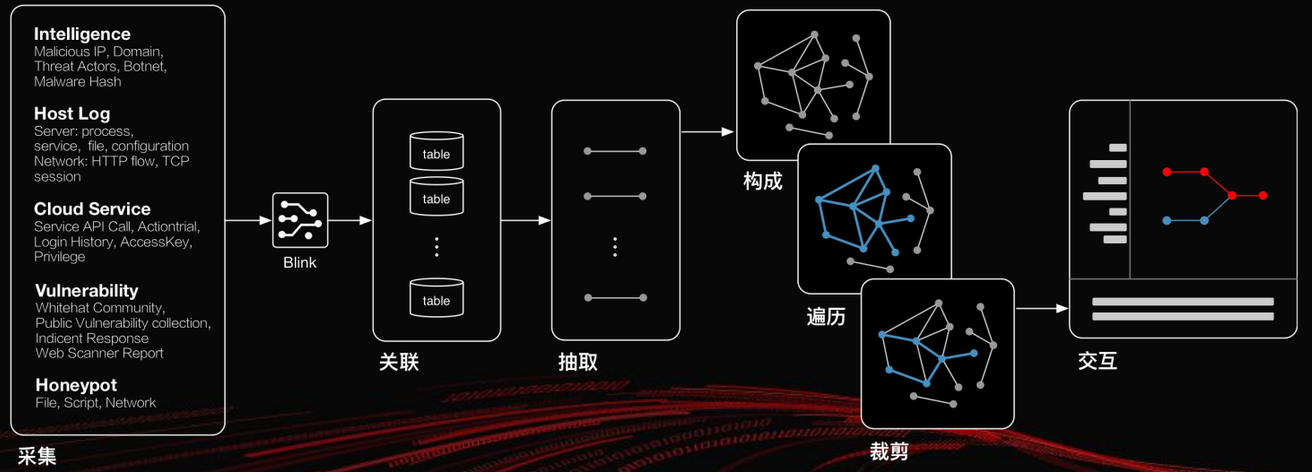


可视化

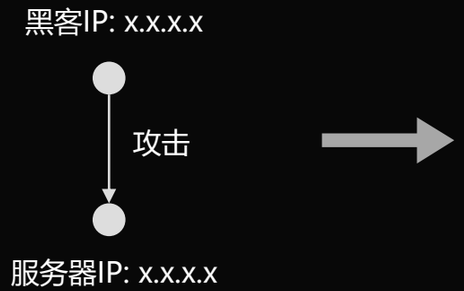
冗余	只展示有用的信息
粗糙	数十种行为细节
离线	分钟级延时



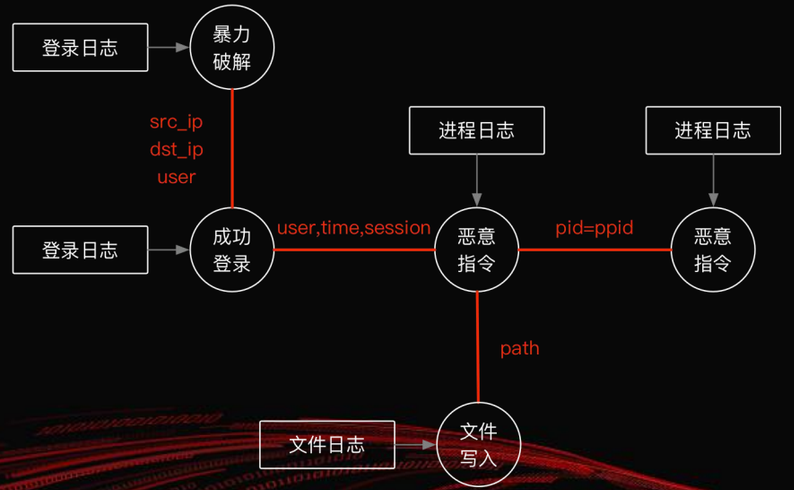
计算流程


Intelligence
Malicious IP, Domain,
Threat Actors, Botnet,
Malware Hash
Host Log
Server: process,
service, file, configuration
Network: HTTP flow, TCP
session
Cloud Service
Service API Call, Actiontrial,
Login History, AccessKey,
Privilege
Vulnerability
Whitehat Community,
Public Vulnerability collection,
Indicent Response
Web Scanner Report
Honeypot
File, Script, Network
采集
Blink
table
table
table
关联
抽取
构成
遍历
裁剪
交互

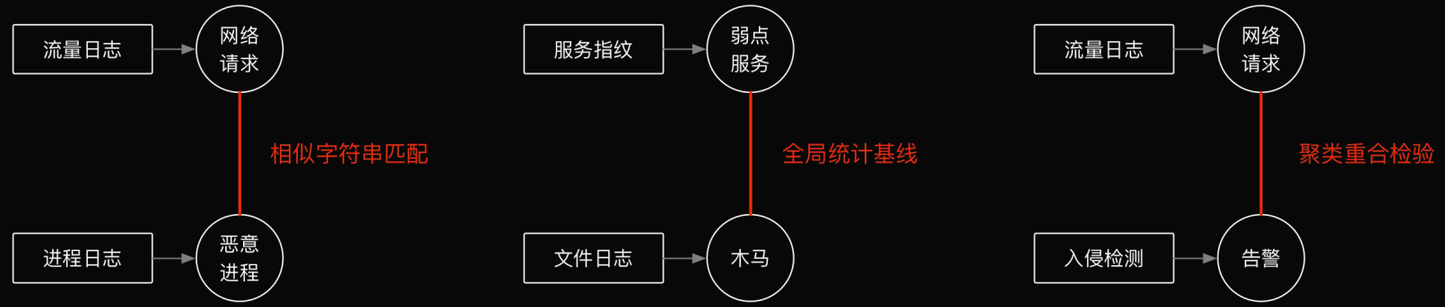
将行为抽象成实体，描述入侵细节



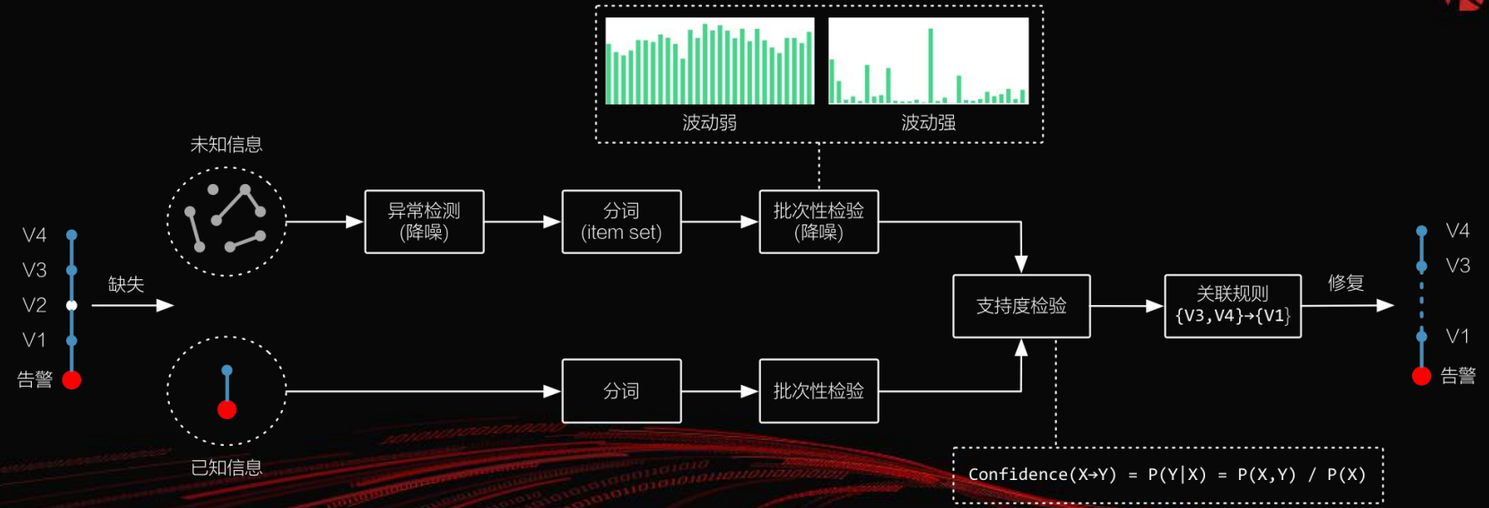
基于日志的被动关系构建



主动关系推理


流量日志
网络请求
相似字符串匹配
进程日志
恶意进程
服务指纹
弱点服务
全局统计基线
文件日志
木马
流量日志
网络请求
聚类重合检验
入侵检测
告警

断链修复：关联规则挖掘


波动弱
波动强
未知信息
V4
V3
V2
V1
告警
缺失
已知信息
异常检测
(降噪)
分词
(item set)
批次性检验
(降噪)
分词
批次性检验
支持度检验
关联规则
{V3,V4}→{V1}
修复
V4
V3
V1
告警
Confidence(X→Y) = P(Y|X) = P(X,Y) / P(X)

watchbog
蠕虫回溯案例

JIRA模板注入(CVE-2019-11581)

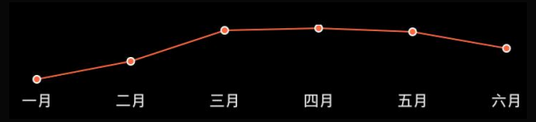
Solr RCE(CVE-2017-12629)

CouchDB RCE(CVE-2018-8007)

SSH暴力破解

宏观入侵原因统计

WEBSHELL植入方式Top

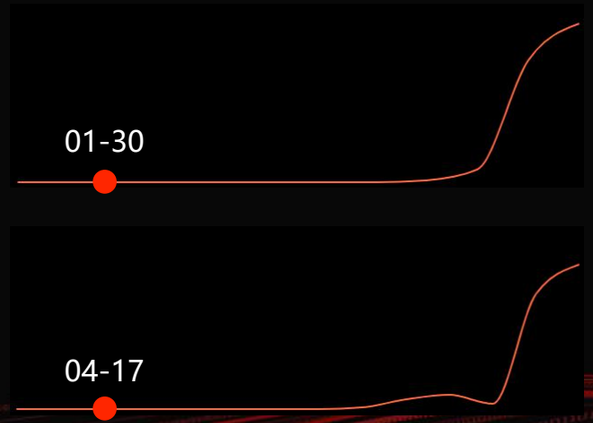


- 表单文件上传
- 老马上传新马
- WordPress插件写入
- SSH/RDP登录后写入
- Discuz插件写入

挖矿程序植入方式Top

- SSH/RDP登录后写入
- WebLogic RCE
- Kubernetes API Server未授权访问
- Struts2 RCE
- Hadoop YARN 未授权访问

自动化0day捕获



Jenkins RCE (CVE-2019-1003000)
2019-01-30 15:45:22 - 115.236.5.58

WebLogic RCE (CVE-2019-2725)
2019-04-17 18:09:45 - 211.94.162.245

现阶段问题

数据

复杂网络拓扑/内网

计算

长时间窗口/复杂模型

对抗

Agent被杀或定向绕过

Q&A

cdxy000 cdxy_