
2020 CTIC
网络安全分析与情报大会
共生
Symbiosis
共进
Success
共享
Sharing

情报加速响应

——基于威胁情报+SOAR的实战应用分享

傅奎

上海雾帜智能科技有限公司 CTO

议程介绍

三个案例 + 一个策略

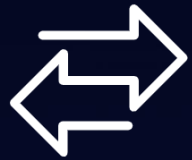
正确的方向 ＋ 快速的动作 ➡ 成功的响应

安全应急响应的痛点

沟通不畅

任务繁重

重复耗时



高频切换上下文

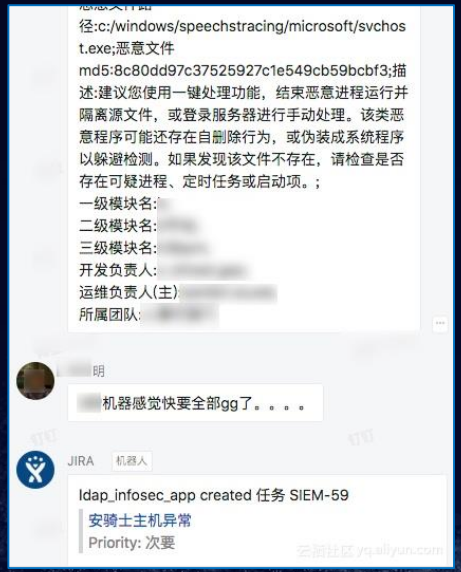
案例一：云主机病毒感染事件响应

云平台日常安全事件响应

5分钟

6台主机

一脸XX

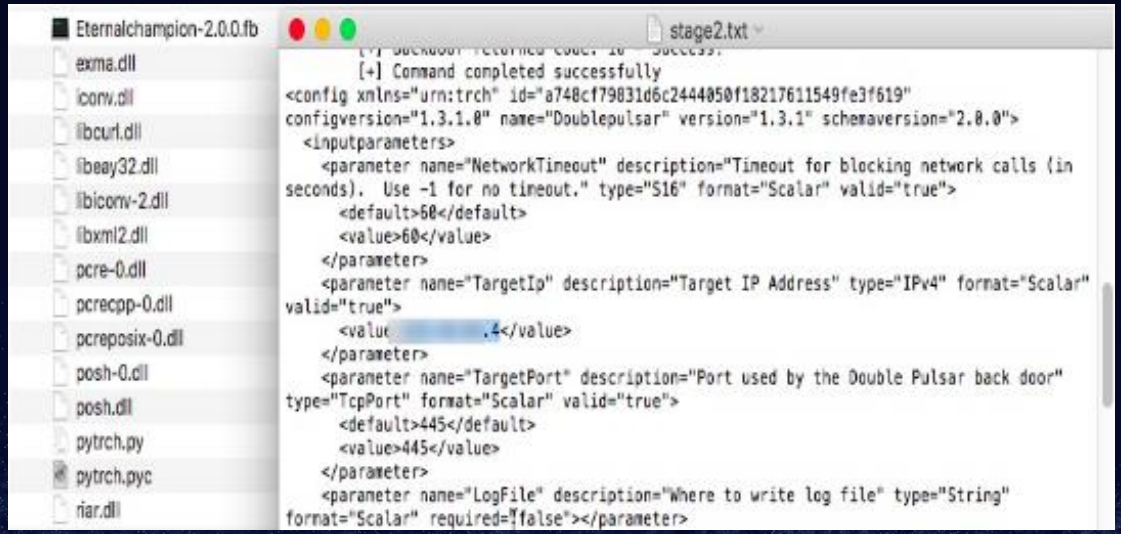


老司机就要翻车了.....

一条情报定方向

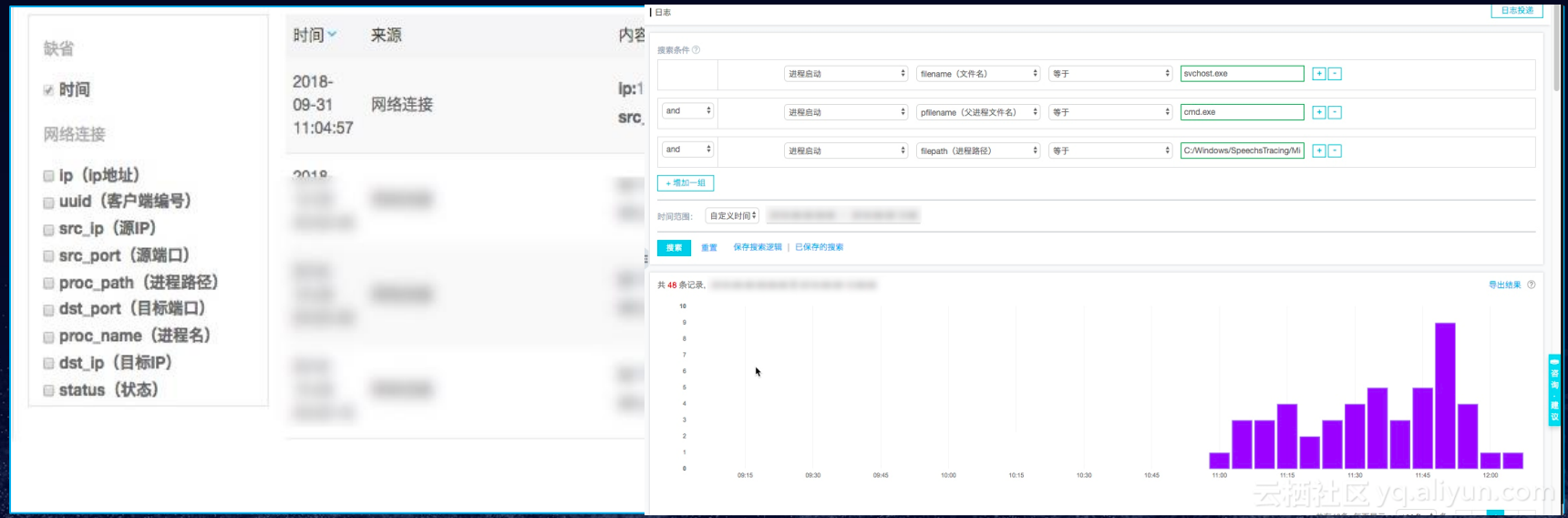

ThreatBook
中文
8c80dd97c37525927c1e549cb59bc
检出率
11 / 25
SHA256
85b936960fbe5100c170b777e1647ce9f0f01e3ab9
分析时间
2018-07-16 13:19:19
微步情报
Trojan
Eqtonex
恶意软件
社区用户情报
正常文件(0)
恶意文件(0)
添加用户情报
微步云沙箱
搜索或扫描 URL、文件 HASH(MD5/SHA1/SHA256)
上传
报告
云API
登录
多引擎检测
威胁情报IOC
行为签名
情报判定系统
基本信息
静态信息
执行流程
进程详情
运行截图
网络行为
释放文件
检测该文件为恶意
文件名称 svchost.exe
SHA256 85b936960fbe5100c170b777e1647ce9f0f01e3ab9742dfc23f37cb0825b30b5
运行环境 win7_sp1_en_x86_3
提交时间 2018-05-05 05:56:55
样本标签 Trojan Eqtonex PE32
EXE x86
100分
处置建议
重新分析
报告
PCAP
样本
收藏
多引擎检出率 15 / 25
API 接口
反病毒引擎
检测结果（最近检测时间：2020-08-27 13:33:39）
江民（JiangMin）
Trojan.EquationDrug.fe
360（Qihoo 360）
Win32/Trojan.Multi.daf
ESET
Win32/Exploit.Equation.EternalBlue.A trojan
GDATA
Trojan.GenericKD.4860918
大蜘蛛（Dr.Web）
BackDoor.Spy.3365
AVG
SCGeneric_c.AXRJ

发挥主观能动性，不放过任何细节

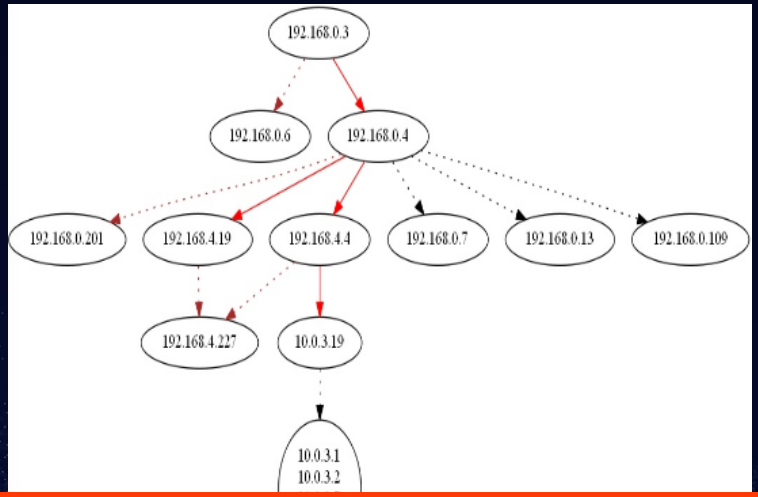


1. 隔离主机
2. Console访问云主机
3. 查看攻击记录
4. 根据源、目的、端口搜索活动记录
5. 持续分析，排查遗漏
6. 梳理攻击路径
7. ……

手工捞取态势感知日志


缺省
时间
网络连接
ip（ip地址）
uuid（客户端编号）
src_ip（源IP）
src_port（源端口）
proc_path（进程路径）
dst_port（目标端口）
proc_name（进程名）
dst_ip（目标IP）
status（状态）
时间
来源
2018-09-31 11:04:57
网络连接
日志
日志投递
搜索条件
进程启动
filename（文件名）
等于
svchost.exe
and
pfilename（父进程文件名）
cmd.exe
filepath（进程路径）
C:/Windows/SpeechsTracing/Mi
+ 增加一组
时间范围：
自定义时间
搜索
重置
保存搜索逻辑
已保存的搜索
共 48 条记录，
导出结果
09:15
09:30
09:45
10:00
10:15
10:30
10:45
11:00
11:15
11:30
11:45
12:00

这样的剧情几乎每天都在上演……



4名人员，**40分钟**止血，**4小时**复盘分析

1. 堡垒机
2. 阿里云
3. 态势感知
4. 安骑士
5. 日志服务
6. **微步威胁情报**
7. 搜索引擎
8. 内部工单
9. 群组沟通
10. SSL VPN
11. SSO
12. OTP Token
13. Graphviz
14. 操作系统
15. Office工具
16. 电话沟通
17. 邮件客户端
18. ……

关键点1：准确可靠的微步在线情报库

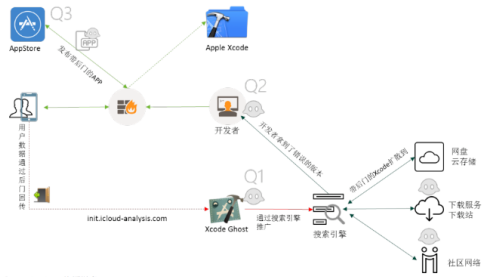
案例二：软件供应链安全应急响应

Xshell、XCodeGhost、Putty等工具/软件后门.....

XcodeGhost后门传播过程

考虑到XcodeGhost在传播机制上利用了搜索引擎进行优化推广（SEO），策划者至少在1年之前就开始了这个动作。

1. 开发者会从苹果官方网站上获取Xcode开发工具，但由于大家都知道的原因，下载速度较慢，或者有时候无法下载。这样就只能从搜索引擎尝试搜索下载资源了。
2. 某些人就看中了这个机会，对Xcode开发工具做了手脚，并通过搜索引擎进行推广，将这个版本散播到各种云存储、下载服务及社区网络
3. 开发者通过搜索下载做了手脚的Xcode，开发出的手机程序APP，就也带了后门，并向苹果应用商店APPStore提交
4. 出于某些原因，苹果商店审核通过了这些带有后门的程序，并将之在应用商店中公开发布
5. 广大的用户在苹果应用商店中下载安装了这些带有后门的程序，而且这些程序往往还都是比较热门的程序
6. 带有后门的手机程序安装数量越来越大，开始有批量的用户数据向这个网站发送，（init.icloud-analysis.com）



]1 xcodeGhost传播链条

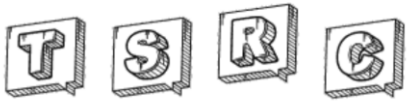
XShell官方软件存在后门

近日，据腾讯安全反病毒实验室监控发现，一款主流的远程终端软件XShell的官方版本中被打包了恶意代码，运行此版本软件后，受害者电脑上会被植入后门，存在被不法分子远程控制，导致个人信息遭窃的风险，目前已有国内用户中招。对此，腾讯安全反病毒实验室已发布了相应的后门专杀工具 下载查杀工具。广大用户也可通过腾讯电脑管家和哈勃分析系统来识别自己电脑中的XShell版本是否含有后门。

你永远不知道下一个会是谁

【安全通知】PyPI 官方仓库遭遇request恶意包投毒

原创 洋葱 腾讯安全应急响应中心 8月5日



作者：
腾讯洋葱反入侵系统
七夜、vspiders、conan

近日，腾讯洋葱反入侵系统检测发现PyPI官方仓库被恶意上传了request 钓鱼包，由于国内开源镜像站均同步于PyPI官方仓库，所以该问题不仅会通过官方仓库，还可能通过各个开源镜像站影响广大用户，腾讯安全应急响应中心（TSRC）秉承共建安全生态的原则，TSRC在此建议各开源镜像站以及对开源镜像站有依赖的公司，请尽快自查处理，确保恶意库得到清除，保障用户安全。

TSRC的情报明确了方向，接下来就有头绪了。

相关IoC：

1. 域名：
   dexy.top
   who.dexy.top:3500
2. ip：
   199.247.5.158
3. url：
   http://dexy.top/request/check.so
   http://dexy.top/x.pyx

- **先止血：**第一时间阻止域名解析或解析到指定服务器
- **同步查存：**查询企业内部是否有中招的终端
  - 查询过往的DNS解析日志
  - 查询防火墙会话列表历史记录，匹配CC服务器IP地址
  - 查询上网行为管理系统中恶意URL的访问记录
- **根治：**排查企业Python库是否受感染
- **监控：**对重点域名、IP进行访问监控或拦截
- **通知：**人员通知、修复通知、培训通知等

应急响应实战指导

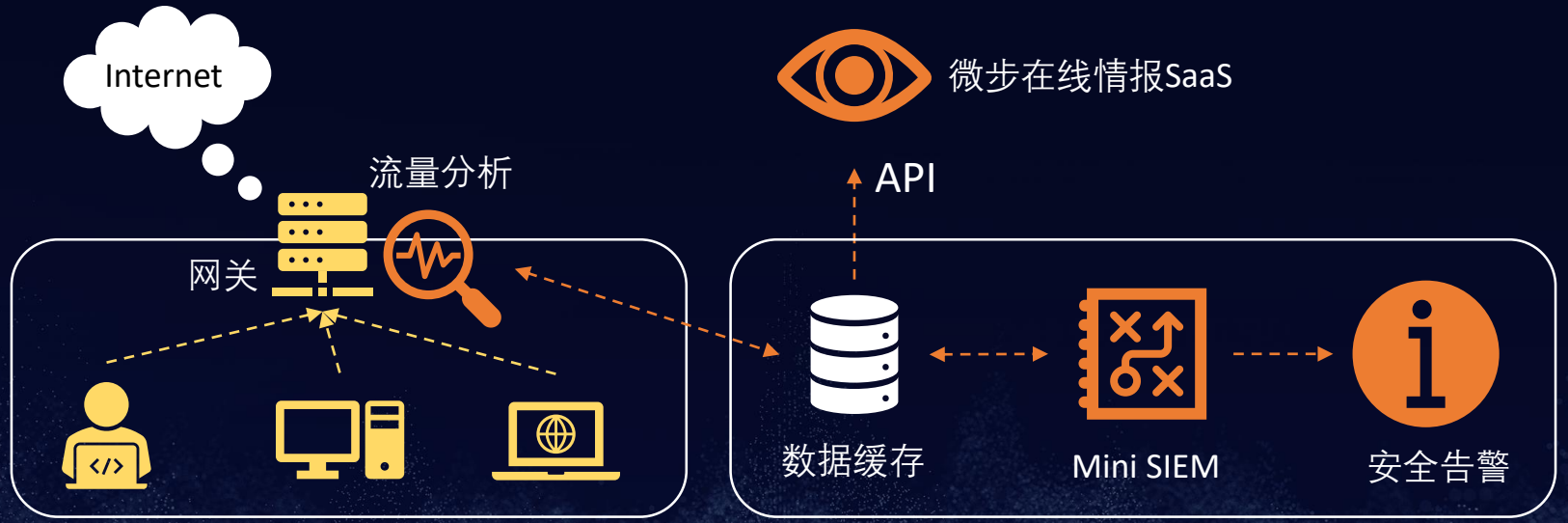
安全动作	相关系统	具体操作
DNS解析拦截	DNSmasq、**OneDNS**、Bind、Windows AD	DNS请求阻止、DNS请求污染
查询历史域名请求日志	DNSmasq、**OneDNS**、Bind、Windows AD ElasticSearch	查询指定域名的解析日志，至少需要输出源IP字段
查询历史IP访问日志	防火墙、日志管理系统	查询指定目标IP地址的历史访问记录，包括五元组信息。
文件或组件排查	EDR终端、青藤云终端、阿里云API、腾讯云API	在目标系统上执行问题组件的检查命令，如：“pip list|grep request|grep -v requests”
监控	流量审计系统、上网行为管理系统、DNS服务器	启动抓包功能、监控指定IP会话、监控指定域名解析
通知	钉钉、微信、Slack、蓝信、飞书、飞信	发送消息，内容根据具体需要确定

关键点2：稳定、安全的微步One DNS解析与管控

案例三：办公网异常流量监测分析

与其被动告警，不如主动发现

办公网流量实时分析：DNS流量+实时情报



微步在线情报与办公网流量准实时结合

企业网内实践：筛选并告警访问C2域名的行为

去重、缓存、白名单、联动准入、CMDB

情报+资产：丰富告警信息

客户端:192.168.0.1
解析目标: cc.com
类型：C2攻击

→

用户：傅奎
客户端：Windows 10

关键点3：持续稳定的微步在线云API

效果很惊喜，结果很满意

SOAR编排自动化加速威胁响应

一次常规的事件响应，

至少涉及10个以上系统或程序，

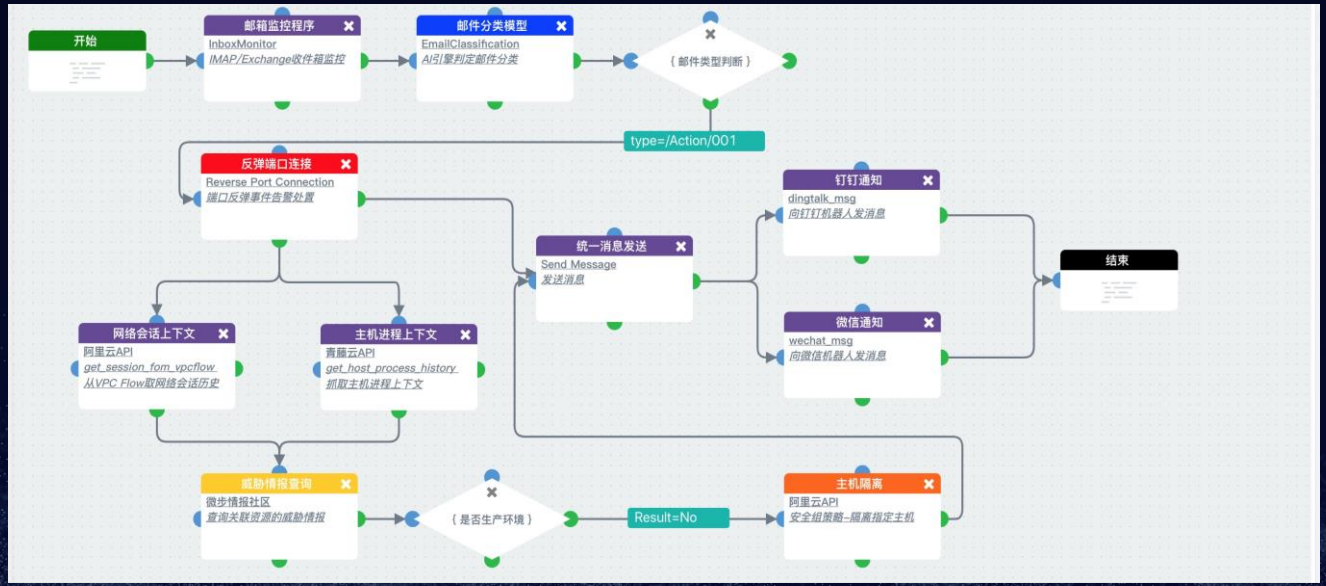
以及“人脑CPU”的上下文切换！

IACD集成自适应安全防护框架的愿景

通过**自动化**、**编排**和**情报共享**加快网络防御的速度和规模

精准的情报 + 自动化响应 ➡ 超越攻击的速度和规模

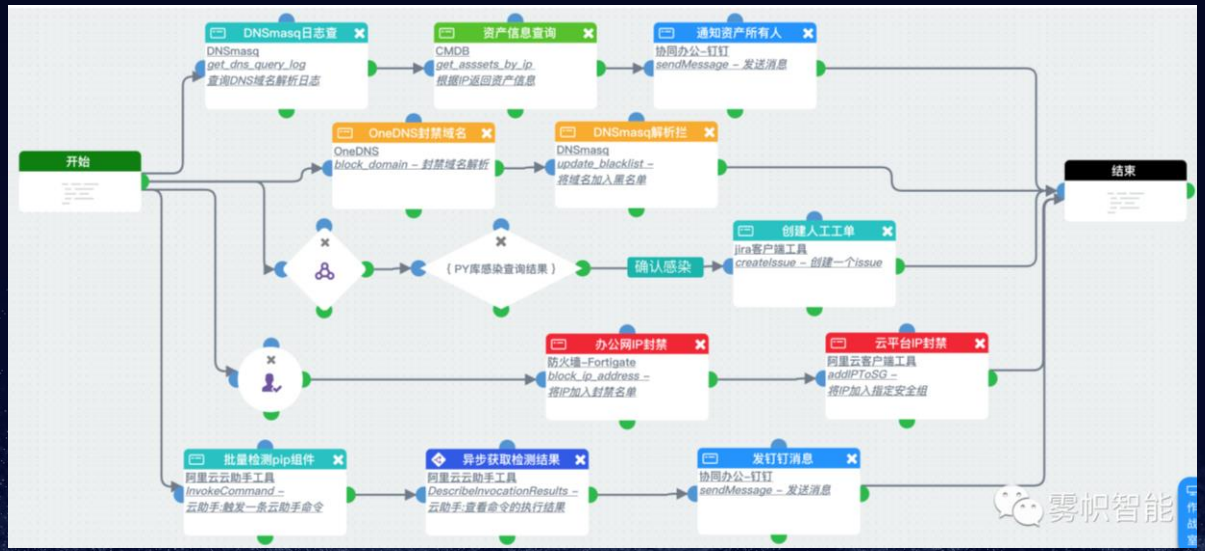
安全剧本：云上主机安全事件响应



4小时

20min

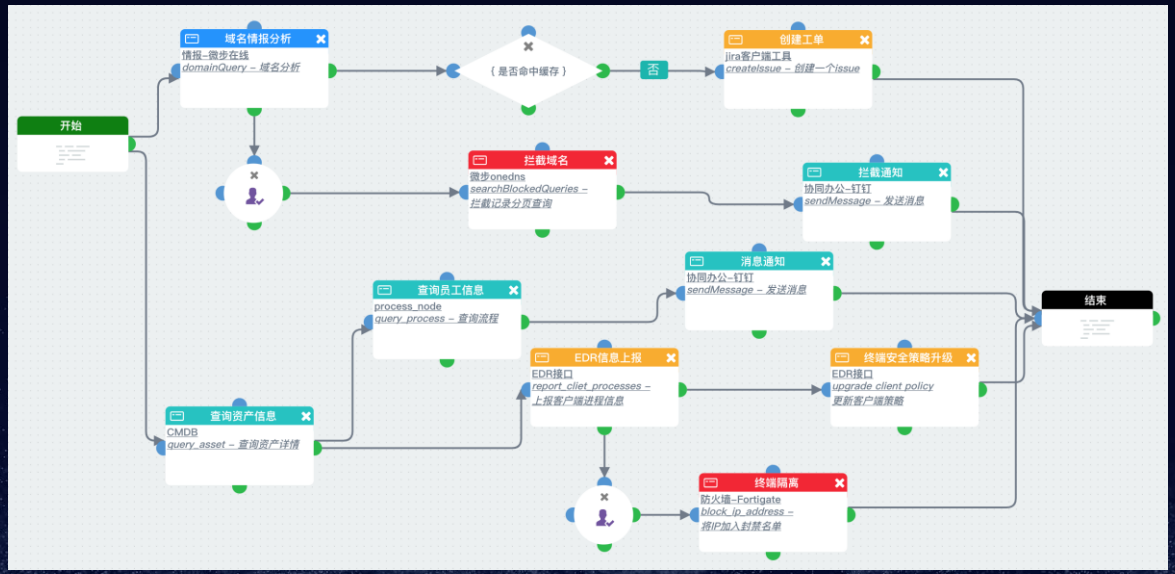
安全剧本：软件供应链安全漏洞应急处置



2天

4小时

安全剧本：办公网异常域名请求自动化响应过程



1小时

5min

情报+SOAR：加速安全事件运营

名称	人工耗时	情报+SOAR	类别
一键封禁IP	5 ~ 10分钟	30秒	响应
钓鱼邮件分析	0.5~2.5小时	5~10分钟	分析
入侵调查/攻击溯源	1~5小时	20分钟	分析
网络故障诊断	0.5~1小时	5分钟	诊断
快速找人/资产	15分钟 ~ 1小时	3分钟	协同
一键事件总结	1 ~ 2小时	1分钟	报告

关键点4：雾帜智能安全编排响、自动化响应能力

实战总结

情报要精准实时

响应要快速迅捷

专家经验必不可少

Threat Intelligence

+

Security Orchestration  utomation and Response

Thank you