SOAR如何编排指引细粒度的端点处置

安天平台产品部

威胁框架：细粒度对抗

長纓待展

CONTENTS

目 录

智者安天下

01 面临的挑战

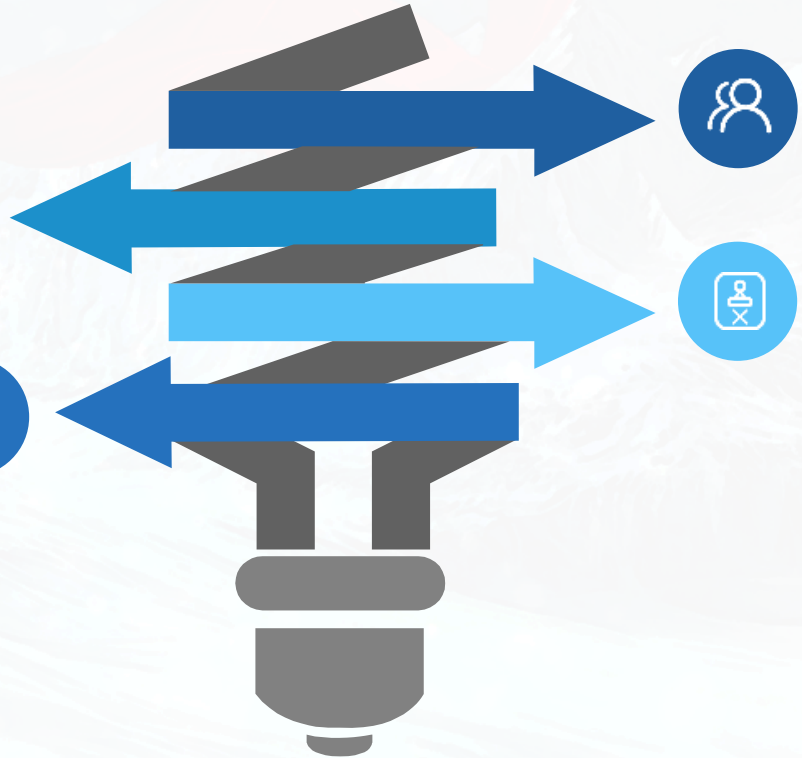
面临的挑战

响应时间过长

解决安全事件的平均时长约4.35天。

培养周期长人员流失大

培训初级安全分析师通常需要8个月，1/4的安全分析师2年就会转岗。



专业人员不足

约80%的公司企业没有足够的分析师运营其SOC，安全从业人员缺口约140万。

自动化程度不足

62%的受访者希望有自动化工具的辅助。

DEMISTO的SOAR行业报告

02 什么是SOAR

什么是SOAR

Security Orchestration, Automation and Response
安全编排自动化与响应

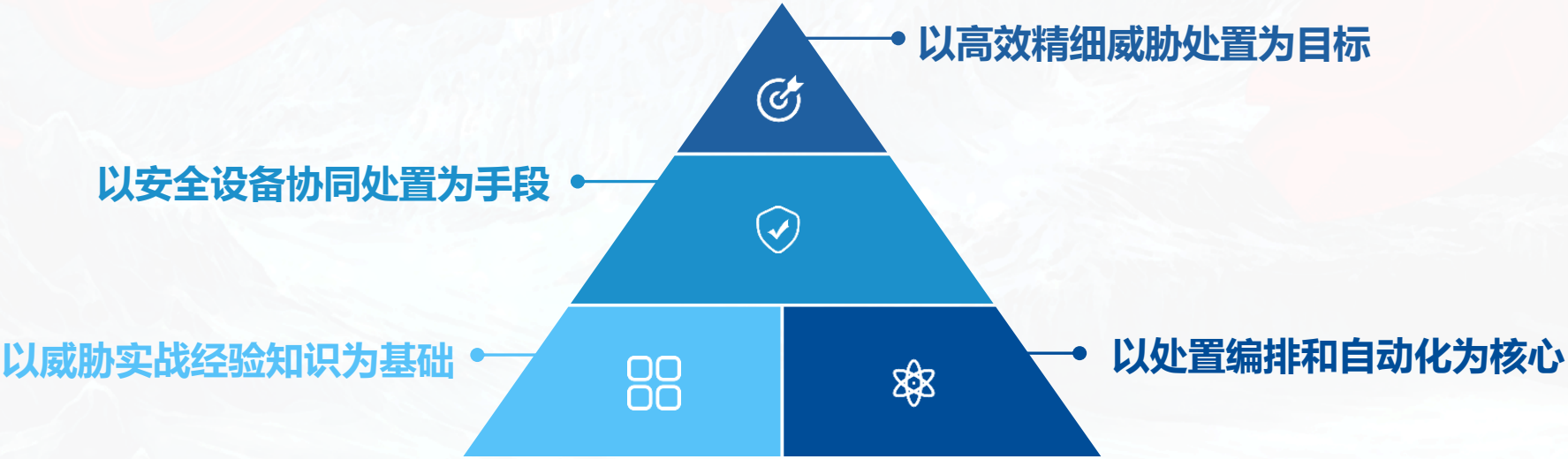
SOAR 是从安全编排和自动化（SOA），安全事件响应平台（SIR）和威胁情报平台（TIP）整合而来。

SOAR是一类从各种来源获取输入，并应用工作流来拉通各种安全过程与规程，从而为安全运营人员提供机器协助的解决方案。这些过程和规程可以被编排（通过与其它技术的集成）并自动执行以达成预期结果，譬如分诊管理，事件响应，威胁情报，合规性管理和威胁猎捕。

SOAR are solutions that add machine assistance to human security operators by taking inputs from various sources and applying workflows aligned to processes and procedures. Those procedures can then be orchestrated (via integrations with other technologies) and automated to achieve a desired outcome, such as triage management, incident responders, threat intelligence, compliance managers, and threat hunting.

来源：https://www.gartner.com

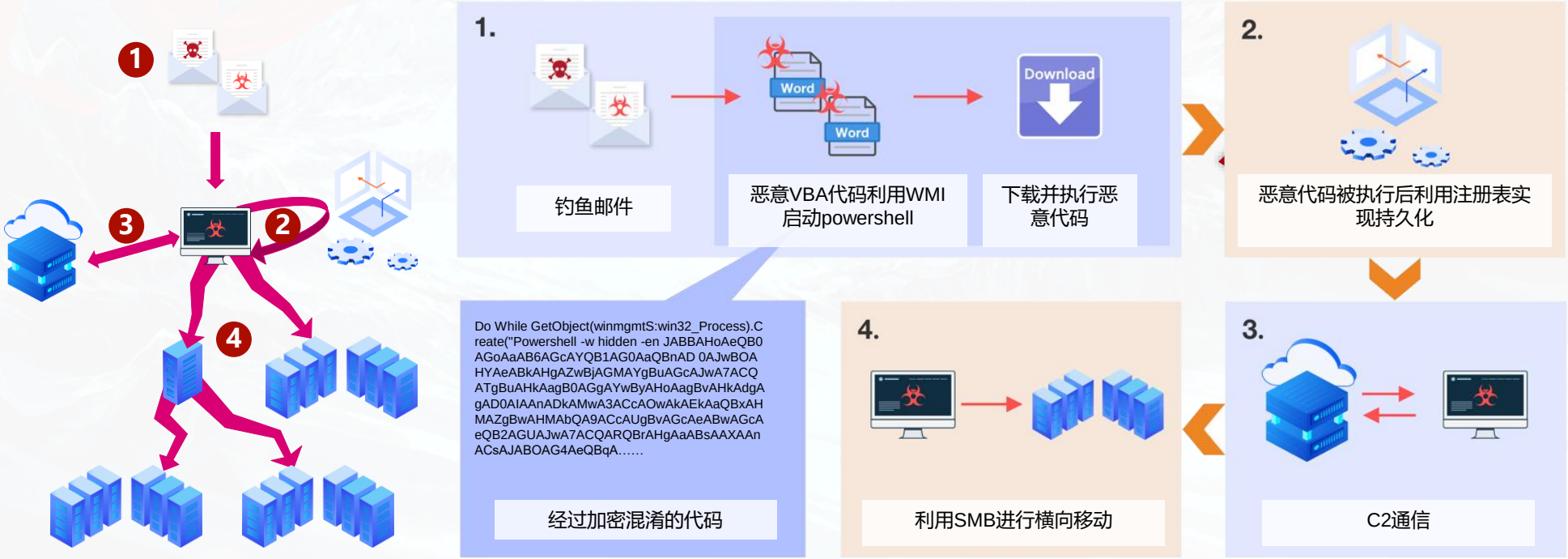
安天对SOAR的认知



03 安天SOAR案例

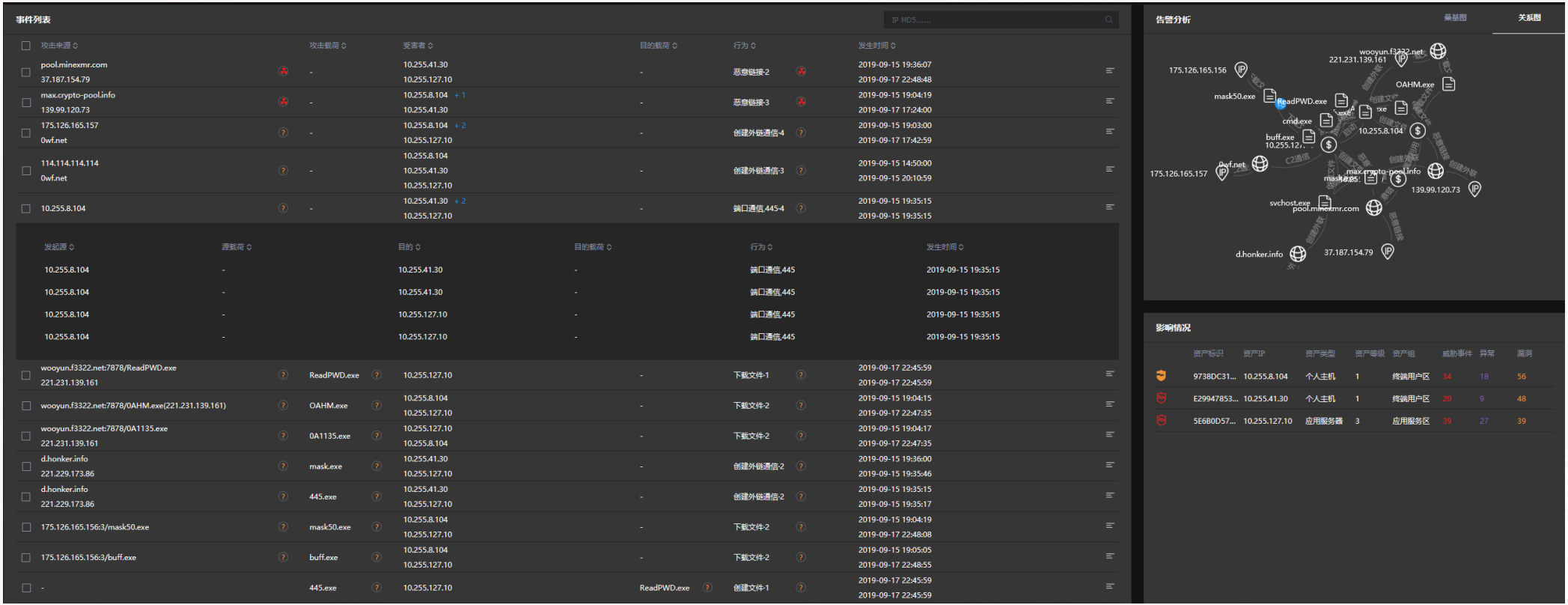
案例一内网Emotet传播事件：攻击过程还原

态势感知系统发现网域内突然出现大量的445端口请求，并伴有大量的使用自签证书的SSL通信，经专业应急响应人员排查后发现这是一起利用COVID-19为诱饵分发钓鱼邮件传播Emotet恶意代码的安全事件



来源《利用疫情传播Emotet银行木马攻击事件梳理与分析》

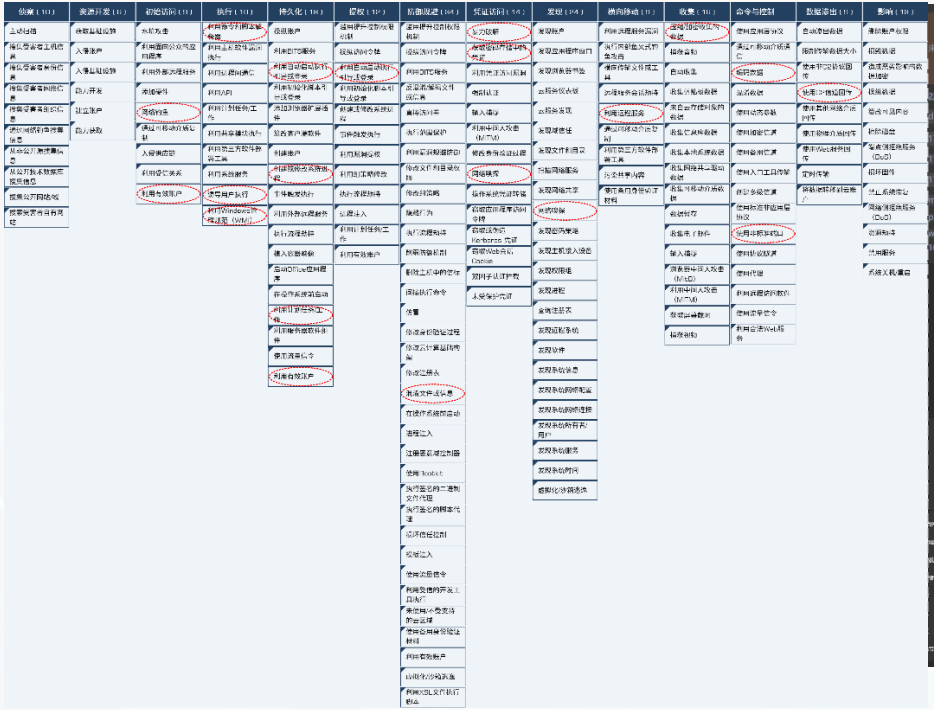
案例一内网Emotet传播事件：态势感知系统威胁告警



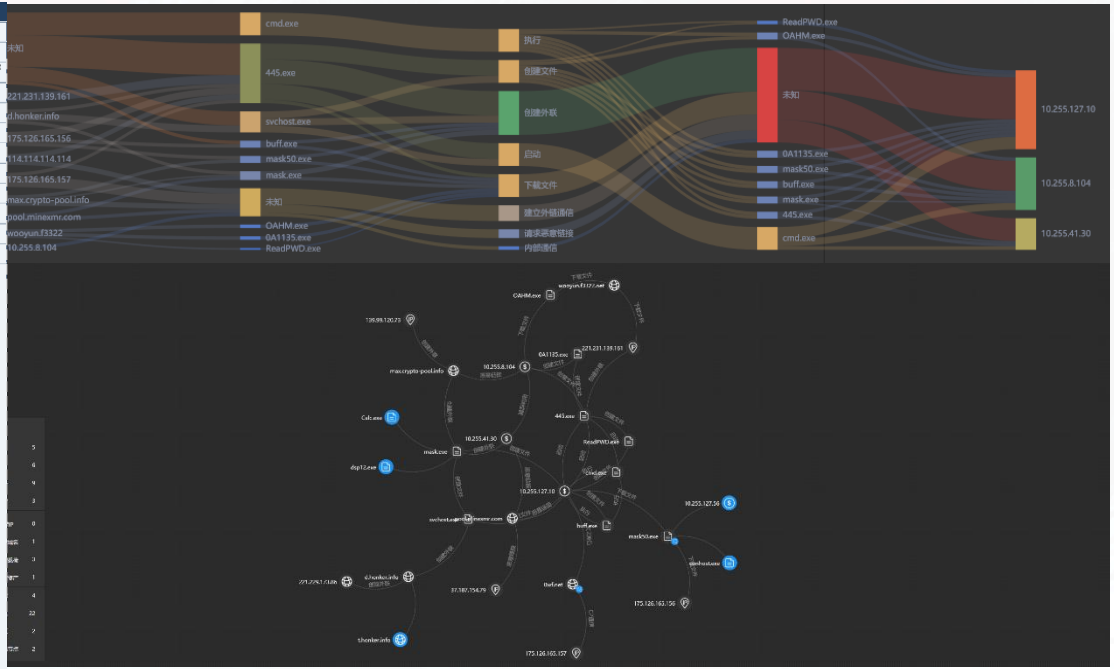
智者安天下

案例一内网Emotet传播事件：系统自动分析

基于ATT&CK框架融合分析

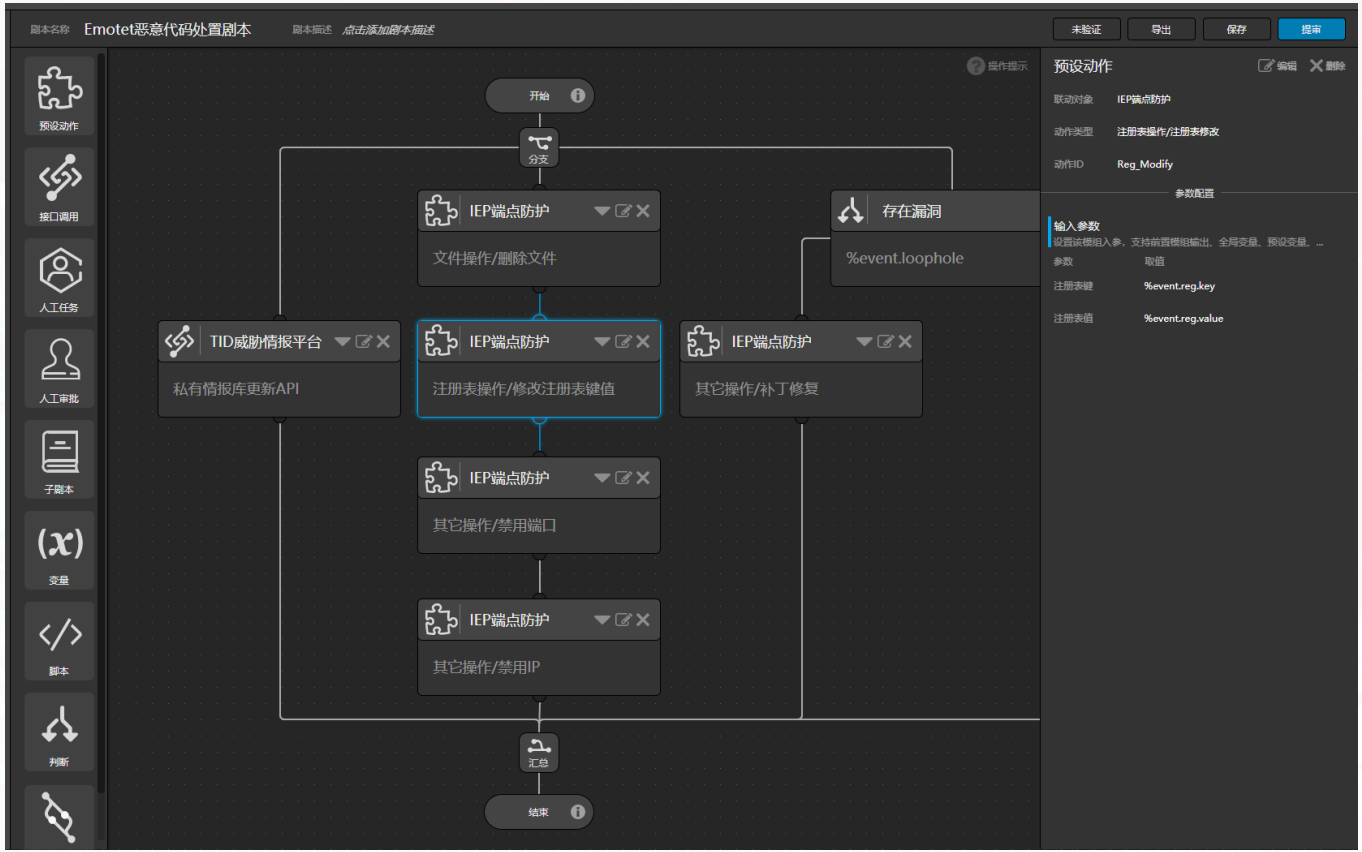


自动关联分析



案例一内网Emotet传播事件：处置流程的精细化编排

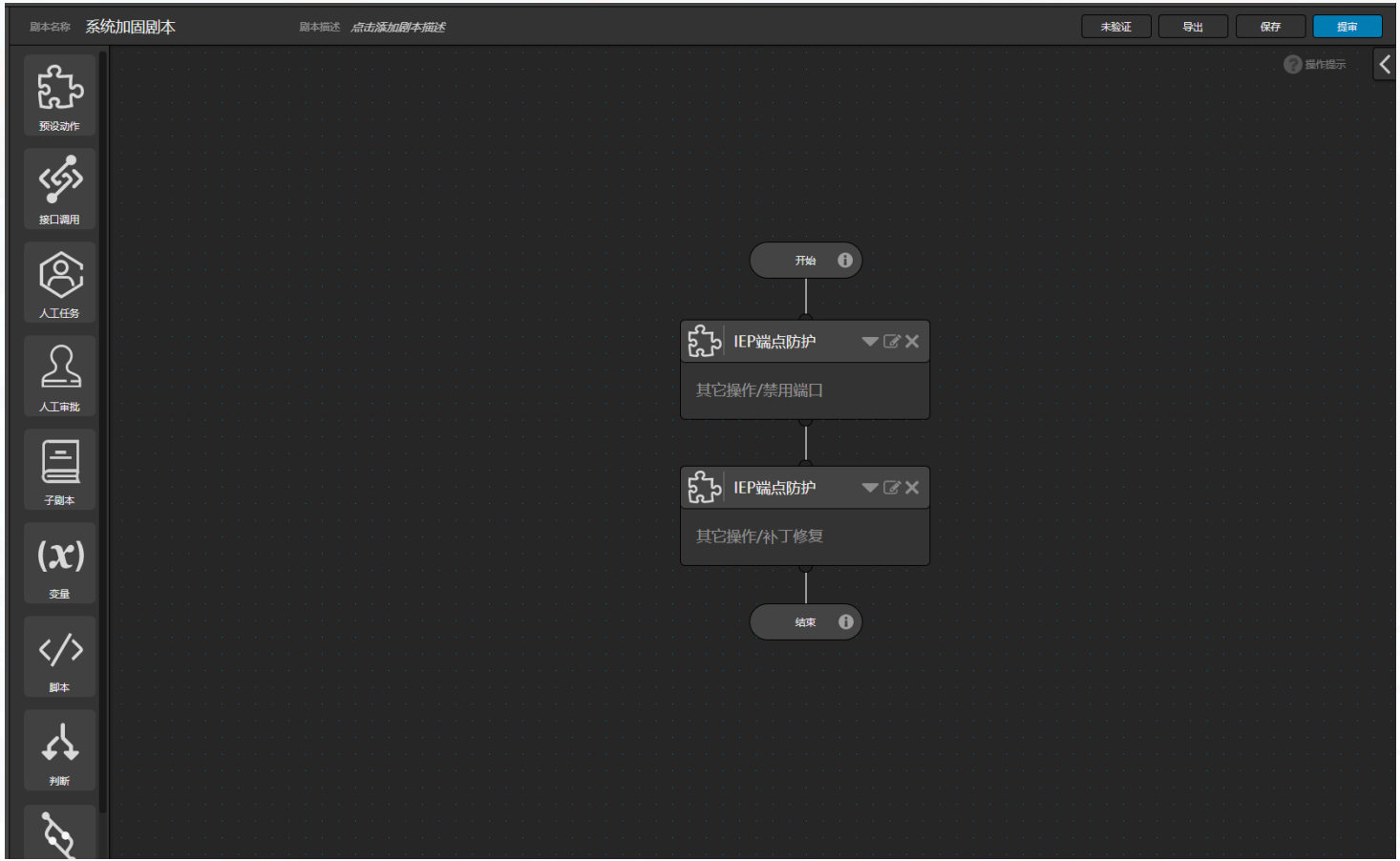
- 根据自动分析的结果，匹配处置剧本。
- 为尽可能复原威胁行为造成的影响，在原有剧本基础上，根据该恶意代码的行为，针对性调整。
- 将IoC等信息更新至威胁情报平台，用于后续内部相关事件的精准发现。



案例一内网Emotet传播事件：处置流程的精细化编排

为了实现系统的安全运营，不仅要对已感染主机进行恶意代码清除，也需要对其他未受影响的终端采取缓解、加固等预防性措施

- 对涉事资产及关联资产，封禁445端口
- 为网内存在此漏洞的资产更新漏洞补丁



案例一内网Emotet传播事件：处置脚本编辑器

- 提供细粒度可视化处置脚本编辑器
- 基于终端管控软件提供的处置操作原语编写处置脚本
- 提供注册表(4)、计划任务(3)、文件(4)、进程(4)、脚本(5)、其他(5+)等共25+种操作原语

安天ARR(Antiy Response Rule)开放式处置规则定义

ARR（Antiy Response Rule）的部分指令集		
一、注册表（可配自动处置规则）	1.创建注册表项/值	[Reg_Create]
	2.修改注册表项/值	[Reg_Modify]
	3.删除注册表项/值	[Reg_Delete]
	4.重命名注册表项/值	[Reg_Rename]
	5.删除注册表值	[Reg_Delete_Value]
二、计划任务（可配自动处置规则）	1.创建计划任务	[Task_Create]
	2.修改计划任务	[Task_Modify]
	3.删除计划任务	[Task_Delete]
三、文件（可配自动处置规则）	1.创建文件	[File_Create]
	2.修改文件	[File_Modify]
	3.删除文件	[File_Delete]
	4.重命名文件	[File_Rename]
	5.修改文件属性	[File_Attribute]
	6.删除文件指定内容	[File_DelText]
	7.MBR修复	[File_repairMbr]
四、进程（可配自动处置规则）	1.创建进程	[Proc_Create]
	2.挂起/恢复进程	[Proc_Modify]
	3.结束进程	[Proc_Terminate]
	4.挂起指定模块线程	[Proc_Module_Threads]
五、脚本	1.下发bat脚本并运行	[Script_Bat]
	2.下发shell脚本并运行	[Script_Shell]
	3.下发vbs脚本并运行	[Script_Vbs]
	4.下发powershell脚本并运行	[Script_PWL]
	5.下载文件并运行	[Script_File]
六、其他	1.外设弹出/规则	[Other_Device]
	2.断网处置	[Other_NetOff]
	3.禁用端口	[Other_Disabled_Port]
	3.禁用ip	[Other_Disabled_Ip]
	4.补丁修复	[Other_Fix_patch]
	5.创建互斥免疫	[Other_Create_Mutex]
	6.创建扫描并自动处置	[Other_QuickScan]

安天ARR开放式处置规则定义是安天为实现细粒度端点响应策略而定义的一组指令集合，包括了对扇区、注册表、文件、驱动、进程等进行相关操作的动作定义，并可以执行包括磁盘遍历，特征匹配搜索等逻辑动作。可以用于处理策略编排、专杀脚本生成，以执行细粒度的处置动作。

安天SOAR提供ARR编辑器，并可以在部分场景中自动生成处置脚本供网管审核。

ARR处置规则支持判定条件，用于触发相应处置:

File_Delete
condition:
全盘：alldisk，系统磁盘：systemdisk，磁盘根目录：diskroot，全盘指定深度：alldisk_deep:1-100
移动设备:udisk

File_repairMbr
condition:
[判定方式],[偏移],[对比内容]
[equal/Unequal],[offset:0],[31 c0 fa]

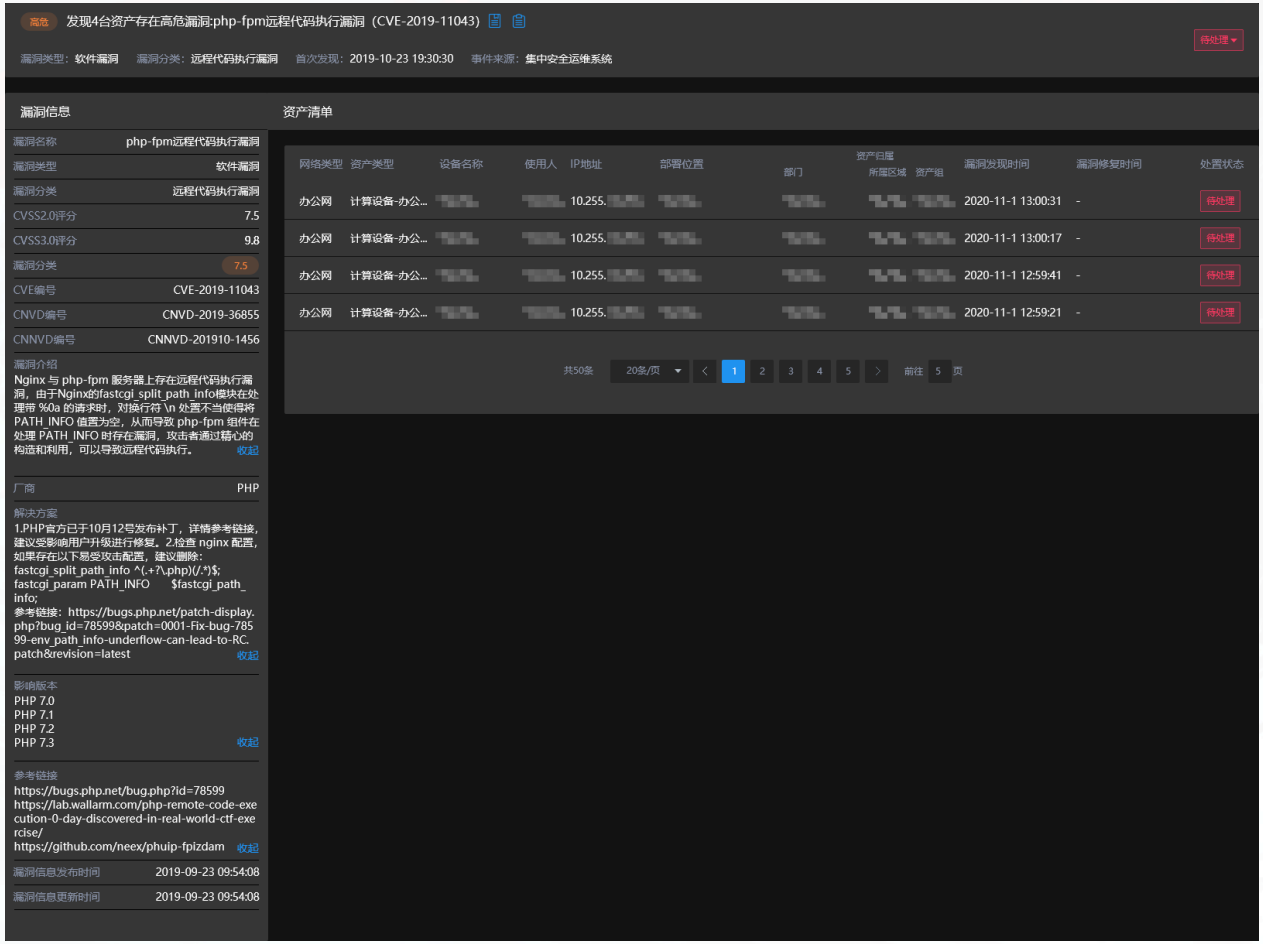
案例一内网Emotet传播事件：生成处置包

- 审批通过后系统自动生成处置脚本
- 根据编写者ID和私钥采用国密算法签名，并提交审核和永久留存，以降低处置能力被滥用风险。
- 派发处置包至验证设备进行功能测试并校验
- 按照可定义分发策略将处置包派发至相关设备，并将操作记录留存

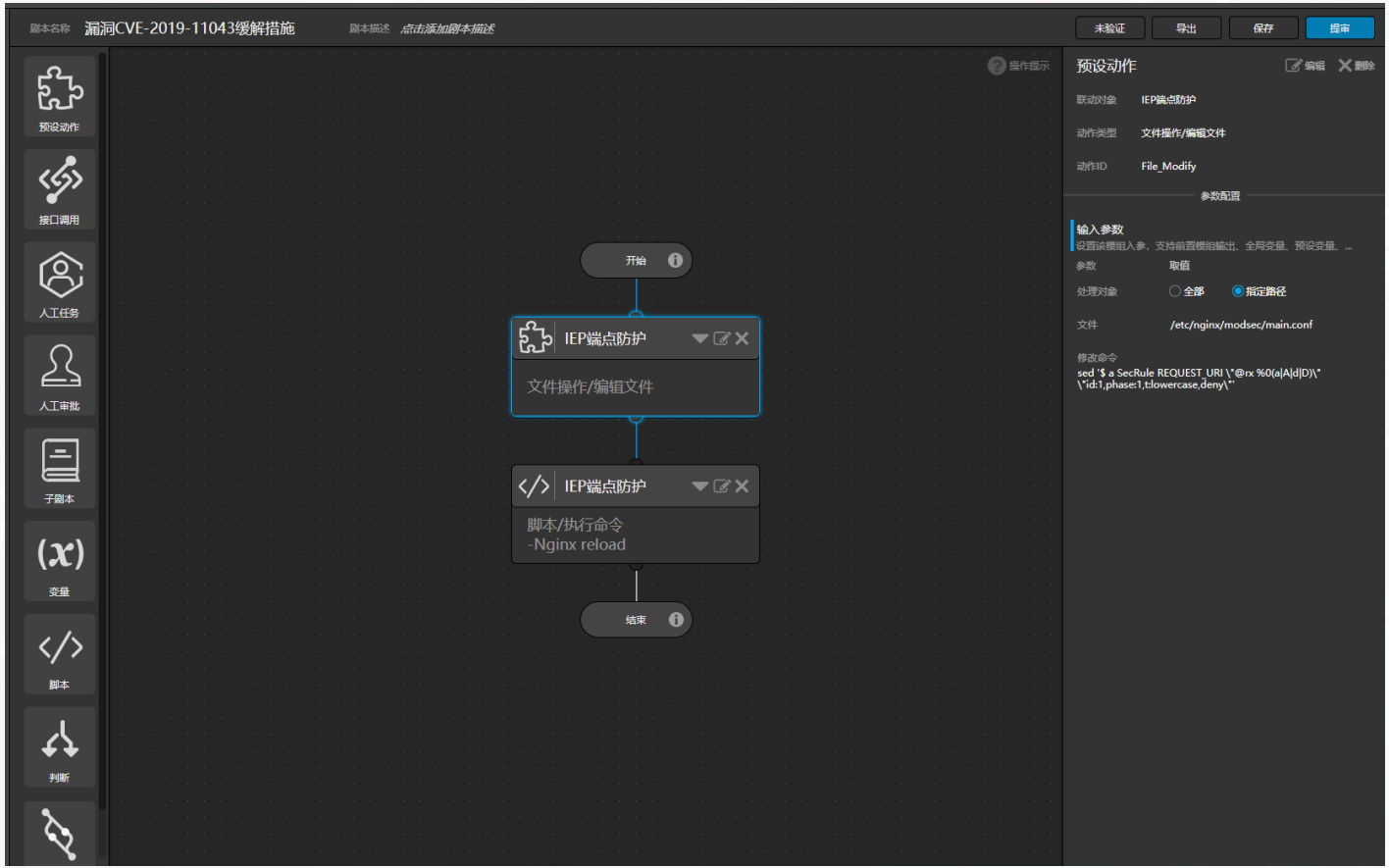
```
        },
        {
            "action":"Reg_Modify",
            "path":"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run",
            "key":"@",
            "value":""
        },
        {
            "action":"Other_Disabled_Port",
            "port":[445,3309]
        },
        {
            "action":"Other_Fix_patch",
            "kbname":["ms17-010"]
        },
        {
            "action":"Other_Disabled_Ip",
            "ips":["103.12.133.7","https://inovatips.com/9yorcan/wbfkk/"]
        }
    ]
}

-----BEGIN SIGNATURE SIGNATURE-----

iQEzBAEBCAAdF[redacted]3lDRgACgkQL7dAkK3u
CCA0CAgA1JVYk[redacted]FDlR4LrQxkS8KNH+i+
d//5V8s+TSqKh[redacted]LsjYfyNUt95C2gH0Un
kWUjluKRThiM/[redacted]dCvspYF6/Go5OFkLTA
1m0/Y+1AARJ7c[redacted]tFGjDRl8Lz2gs9DzBw
rT9AKvhDM5sdT[redacted]m0CzjM0F+vycqRFsss
v8thLRmduEK1m[redacted]
=UH5v
-----END SIGNATURE SIGNATURE-----
```

案例二CVE-2019-11043漏洞告警

安天铸岳资产管理平台通过漏扫发现业务服务器存在CVE-2019-11043漏洞，系统自动关联了存在相同漏洞的另外三台服务器，同时丰富了漏洞知识信息。



案例二CVE-2019-11043漏洞处置



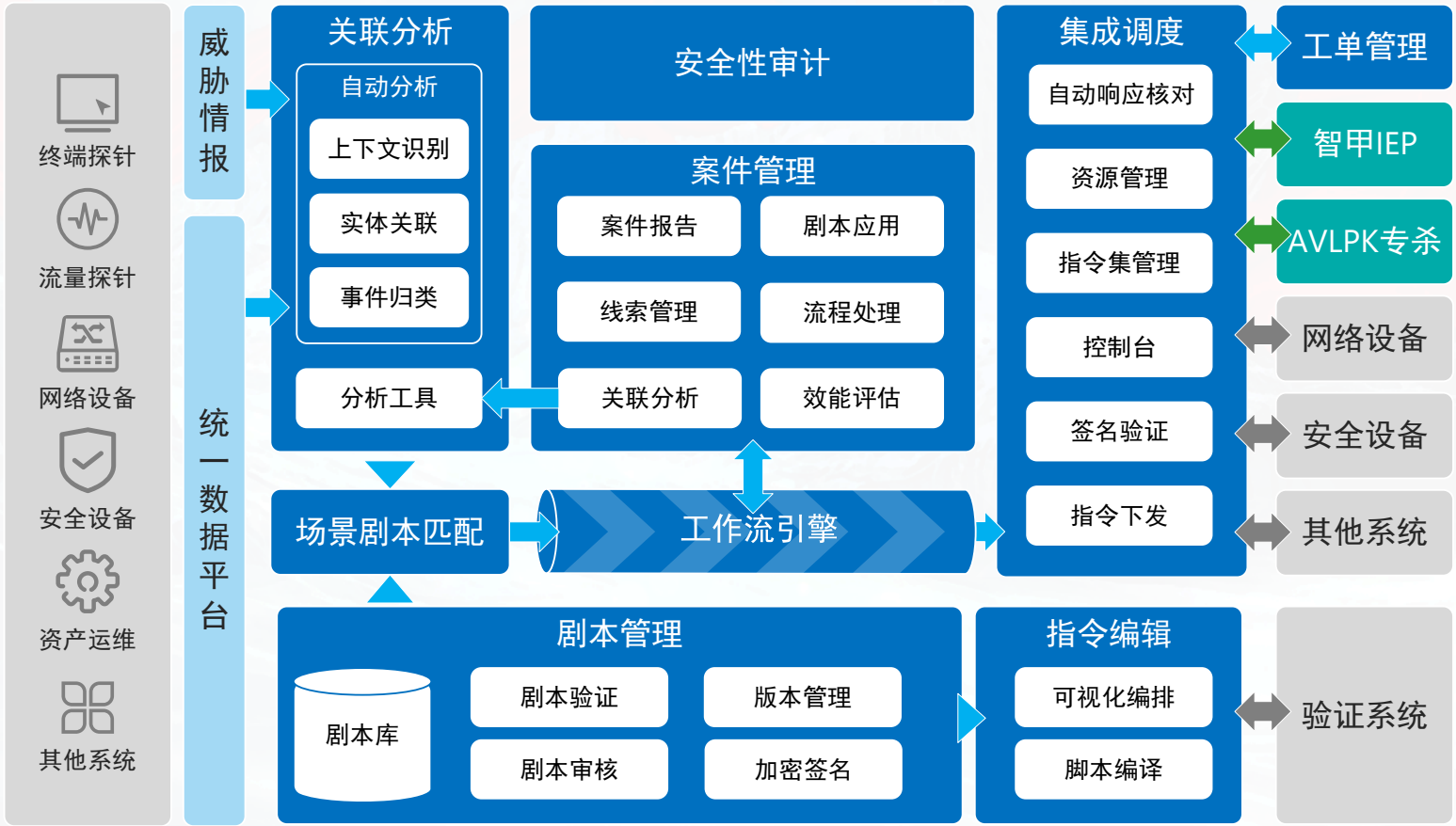
- 根据资产所属业务属性选择缓解措施
- 根据安天的补丁库、漏洞信息库生成缓解脚本
- 修改Nginx配置文件增加

  SecRule REQUEST_URI \"@rx %0(a|A|d|D)\" \"id:1,phase:1,t:lowercase,deny
- 重载Nginx

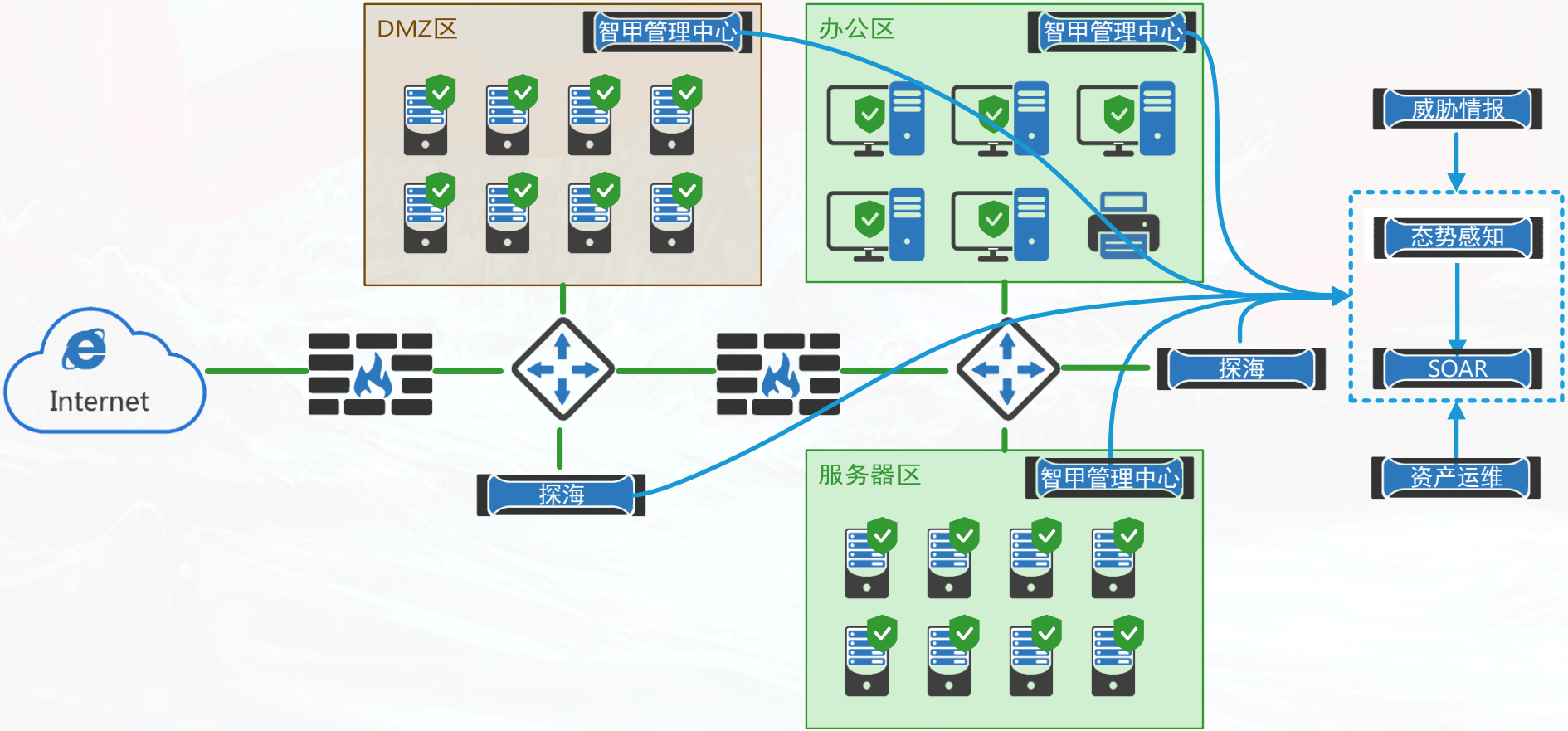
  reload Nginx

04 安天SOAR架构

SOAR功能架构

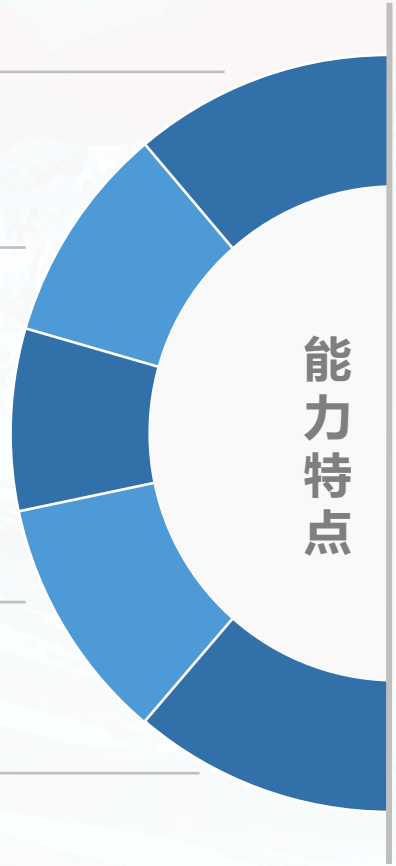

终端探针
流量探针
网络设备
安全设备
资产运维
其他系统
威胁情报
统一数据平台
关联分析
自动分析
上下文识别
实体关联
事件归类
分析工具
安全性审计
案件管理
案件报告
剧本应用
线索管理
流程处理
关联分析
效能评估
场景剧本匹配
工作流引擎
剧本管理
剧本库
剧本验证
版本管理
剧本审核
加密签名
集成调度
自动响应核对
资源管理
指令集管理
控制台
签名验证
指令下发
指令编辑
可视化编排
脚本编译
工单管理
智甲IEP
AVLPK专杀
网络设备
安全设备
其他系统
验证系统

SOAR部署结构


DMZ区
智甲管理中心
办公区
智甲管理中心
威胁情报
态势感知
SOAR
资产运维
Internet
探海
探海
服务器区
智甲管理中心

05 安天SOAR特点

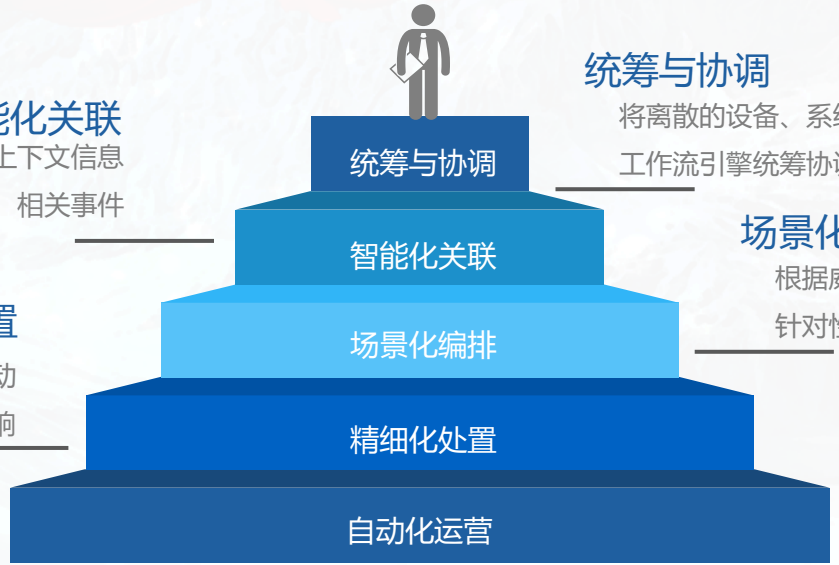
安天SOAR的能力



- 安全能力编排化
- 自动响应剧本化
- 脚本编辑可视化
- 关联分析流程化
- 响应处置自动化

- 效能可评估
- 效果可验证
- 能力可演进
- 操作可追溯

安天SOAR的价值



智能化关联

智能化分析威胁行为体活动的上下文信息

关联汇总相似、相关事件

精细化处置

根据行为体的活动

对威胁进行清除并复原其造成的影响

统筹与协调

将离散的设备、系统、人员通过SOAR的场景化剧本和

工作流引擎统筹协调，提高运营效率

场景化编排

根据威胁及威胁发生的环境等场景化信息

针对性编排

自动化运营

对已确认的威胁，无需人员参与、或仅需人

工审批即可自动化采取应对措施。

专业的威胁处置能力

安天SOAR建立在安天智甲终端防护软件提供的细粒度防御处置基础之上，结合安天CERT提供的恶意代码专杀工具为用户提供精细、灵活、高效的威胁处置能力。

谢谢大家