雾·帜·智·能

剧本最佳实践

Top 10 SOAR 安全剧本最佳实践

By 庄庆华@雾帜智能

2022 04/12

TOP 10 SOAR 安全剧本最佳实践

主编：庄庆华（雾帜智能剧本专家）

2022/04/12

前言

在SOAR系统当中，剧本承载的是结合人、工具、安全设备和工作流的数字化安全过程，是安全自动化和数字化的核心元素。

SOAR总的发展历程较短，真正开始起步的时间应该是2017年Gartner对其命名的确定，即安全编排自动化与响应（Security Orchestration Automation and Response）。因此，可以从公开领域获取的实践案例剧本数量非常有限，国内企业的实践剧本更是寥寥无几。

值得庆祝的是过去3年，随着国产SOAR产品的不断成熟，越来越多的国内企业也开始践行将SOAR平台作为安全基础架构的核心部分，帮助解决安全运营中的"安全、成本和效率"的三体问题，即在兼顾安全的情况下，平衡安全运营成本和效率。

我们邀请过去3年中部分已经部署或即将部署雾帜SOAR（HoneyGuide）的客户进行了一对一的访谈。在本次访谈中，我们一共收集了将近400个在用剧本。我们的专家团队对这400个剧本和我们已有的剧本仓库中的100多个剧本模板，总计约500个剧本进行了统计、分析和评估。最终，我们从中整理了10个被认为通用且最有价值的优秀剧本，借本次产品发布会的机会分享给大家。这些剧本涵盖事件响应、漏洞管理和应急预案等多个方面，希望能抛砖引玉，与大家探讨SOAR剧本的最佳实践。

剧本最佳实践

什么样的剧本是好剧本?

目前来说，这尚未有标准。结合我们客户的访谈反馈和分析结果，我们认为一个好的剧本至少具备以下特征中的一个：

- 集成联动型：这类剧本自动化调用多种安全设备/系统，实现自动化或半自动化的安全响应。可以在不增加或不更换设备的情况下，提升企业整体防御的安全性。
- 日常事务型：用于辅助处理如漏洞管理、威胁情报管理等日常运营事务的剧本。这类剧本融入到安全运营人员的日常事务和企业流程当中，或是能大大简化流程，或是能减少人工操作，以大幅减少运营人员的日常琐事。
- 综合工具型：这类剧本旨在简化某一种或多种工具的操作；一般是集合了多种技术的剧本。帮助安全人员以较低的学习成本，使用一种或多种复杂的技术，也帮助解决在实际运营中专家人手不足时，人员补位的痛点。

- 应急预案型：这类剧本通常是冷剧本，需要手动执行，用于推动一个或多个工作流的执行。帮助团队应对突发的紧急情况。

另外，我们把一个剧本的使用频率和通用性也纳入了考量当中。除了“应急预案型”的剧本，如果一个剧本在部署落地后，几乎没有被使用，那么我们可以认为该剧本没有达到它需要实现的目标或是实现的是一个伪需求。

当然，因实际客户的业务差异，相同的剧本在不同的环境的需求是不同的。如有部分开箱即用的剧本在A客户处完全没有被使用，但在B客户那却被频繁地使用。因此，我们尽可能地挑选通用性较高的剧本，至少是有一定的用户量的剧本。

本次分享的剧本都已经做了脱敏，并删除或替换了一些调用非通用或客户自研设备/系统的节点。我们通过对比和筛选，将多个相近的剧本做了一定整合，并进行了优化。

剧本列表

序号	剧本名称	特征类型	推荐指数
1	阶梯式自动化响应剧本	集成联动型	★★★★★
2	恶意软件事件预处置剧本	集成联动型	★★★★★
3	资产漏洞扫描管理	日常事务型	★★★★
4	临时策略自动化管理	日常事务型	★★★★
5	可疑邮件分析处置剧本	集成联动型+综合工具型	★★★★★
6	IP/域名多维信息查询剧本	综合工具型	★★★★★
7	恶意Web请求分析和响应	集成联动型+综合工具型	★★★★★
8	混合云环境响应剧本	集成联动型	★★★★
9	Web页面信息泄露事件响应	应急预案型	★★★
10	通用紧急呼叫剧本	应急预案型	★★★

<推荐指数>说明

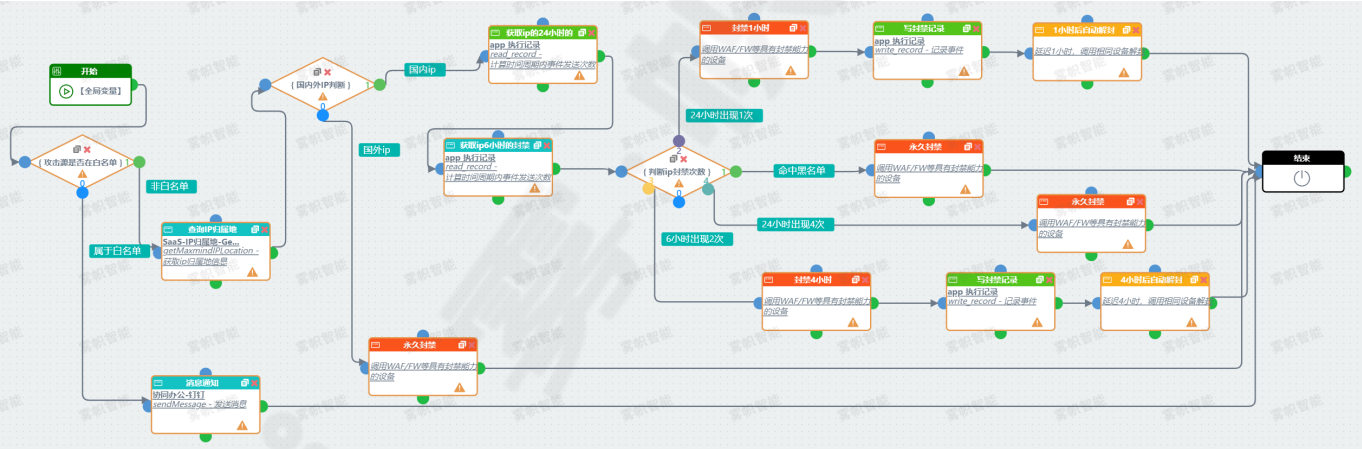
最高5颗星，是综合剧本在访谈对象中的部署占比、反馈评价、通用性和实施难度等得出的。

推荐指数	说明
★★★★★	强烈推荐，具备通用性，推荐优先实施
★★★★	非常推荐，具备通用性，实施难度不大
★★★	一般推荐，具备通用性，但有实施难度
★★	不具备通用性，且有实施难度（本次分享不包含此类剧本）
★	不推荐，伪需求（本次分享不包含此类剧本）

> 本次分享的剧本当中有些用到了雾帜HoneyGuide的高级编排功能，如异步节点、后置节点和数组循环展开等。日后，有机会给大家详细介绍。

剧本详细

No.1 阶梯式自动化响应剧本（集成联动型）



剧本描述

这是个比较典型的自动化响应剧本，也是比较典型的阶梯式封禁剧本，SOAR接收到上游的SIEM和态势感知等发送的特定类型的事件或者IP列表后，会自动触发该类剧本。

剧本主要步骤如下：

1. 查询IP白名单；存在于白名单内的地址，只向钉钉值班群通知，不做处理。
2. 查询非白名单内地址的归属地信息；根据归属地的不同实施不同的封禁策略。
    - 国外地址：永久封禁处理

- 国内地址：根据命中次数和黑名单命中情况，进行阶梯式封禁
  - 24小时命中1次：封禁1小时
  - 6小时命中2次：封禁4小时
  - 24小时命中4次：永久封禁
  - 命中黑名单：永久封禁（注：实际应用中，黑名单提取自威胁情报）

3. 自动解封：封禁时间到自动解封，通过延迟X小时（封禁时间）后执行解封动作实现。

实际应用中，也需要使用剧本对"永久封禁"的地址列表进行维护，大多数用户选择使用支持定期自动任务的剧本，每3个月执行一次清理；有些客户将该剧本中的归属地查询替换成威胁情报，通过联动威胁情报的IP分析功能，可以进一步提高封禁的准确度。当然也有些客户选择在上游SIEM联动威胁情报，将事件进一步过滤后发送给SOAR。这两种方法各有优劣，这里就不展开讨论了。

推荐指数: ★★★★★

主要对接设备/系统：SIEM/态势感知/SoC 、WAF/FW/IPS/ADS、IP归属地数据库/威胁情报系统

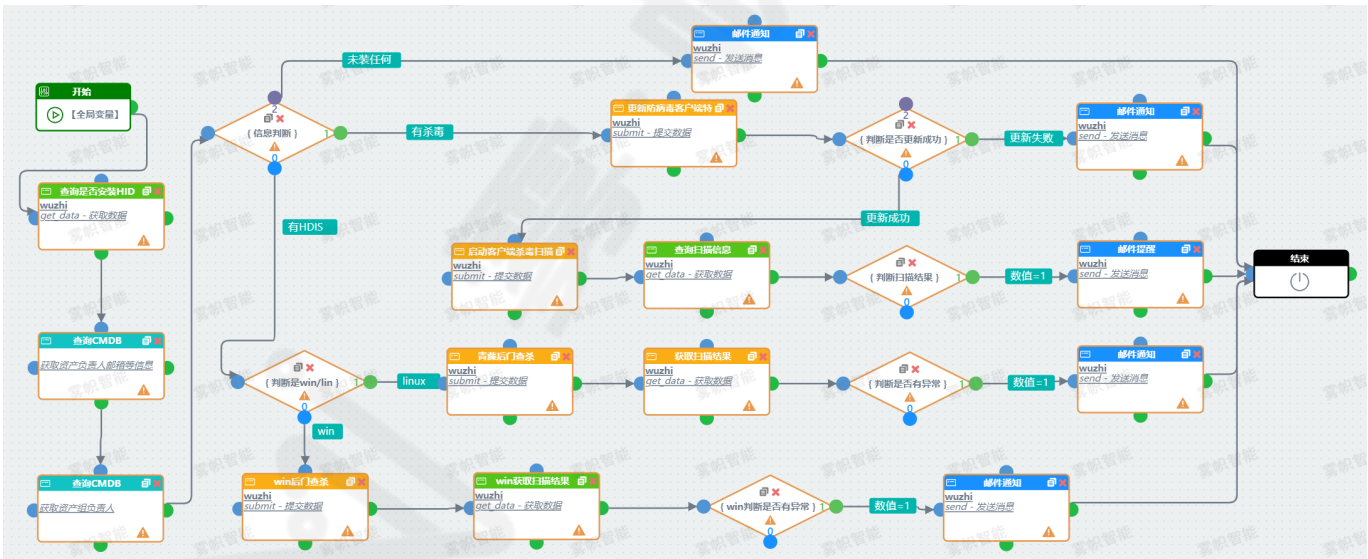
推荐理由和效果收益

封禁IP是一种常用且有效的遏制手段，无奈实际应用中工作量大、重复枯燥，还可能意外影响到业务。这个剧本应用阶梯式封禁和全局黑白名单， 这是一种业务友好的封禁方式，对有ACL长度限制的封禁设备的冲击也是比较小，全程无需人工参与，可以高效且准确地对攻击方实施打击遏制。另外，由SOAR统一维护的全局黑白名单，省去了不同设备间同步配置的麻烦；由SOAR控制的统一封禁策略，也使得原本不具备阶梯式封禁能力的设备同样实现阶梯封禁的效果，免去复杂配置或升级的麻烦。

	人工方式	剧本方式	剧本效益/提升
时间消耗	>8小时	<0.1小时	>8000%
响应及时率	视团队人数和事件数量，及时率普遍低于50%	100%	>200%
业务误封概率	较大机率	较小机率	精准防护
白名单	一定几率忽视	自动	准确匹配
黑名单/威胁情报	工作量巨大，不常用	自动	准确匹配
设备配置优化	困难低效，需要不定期手动维护ACL，地址组等	简易高效，定期自动维护	最优化

注：以每*100*条事件计算和评估；*5*分钟内完成响应；人工方式参与人数为*1*人

No.2 恶意软件事件预处置剧本（集成联动型）



剧本描述

这个剧本集成联动了HIDS服务器、防病毒服务器和资产管理系统。通过HIDS服务器/防病毒服务器主动将客户端更新、发起扫描等任务推送给客户端；并通过内部的资产管理系统（剧本中为CMDB）查找对应的资产负责人，并将结果通过邮件反馈给资产负责人/所有者/资产组管理员。

剧本主要步骤如下：

1. 查询HIDS服务器，并判断事件涉及的主机是否安装HIDS客户端或杀毒客户端
2. 查询CMDB获取资产负责人/所有者，及资产所在资产组管理员的信息（邮箱等信息）
3. 根据HIDS返回的客户端安装情况，执行相应操作：
    - 有杀毒客户端：更新并启动杀毒
    - 有HIDS客户端：启动后门查杀
    - 未装任何客户端：邮件通知资产负责人/所有者/资产组管理员
4. 将异常结果通知资产负责人/所有者，如果没有查询到资产负责人/所有者，则通知资产组管理员：
    - 未装任何客户端
    - 杀毒软件更新失败
    - 杀毒或后门查杀发现了异常

推荐指数: ★★★★★

主要对接设备/系统：SIEM/态势感知/SoC 、HIDS服务端、杀毒软件服务端

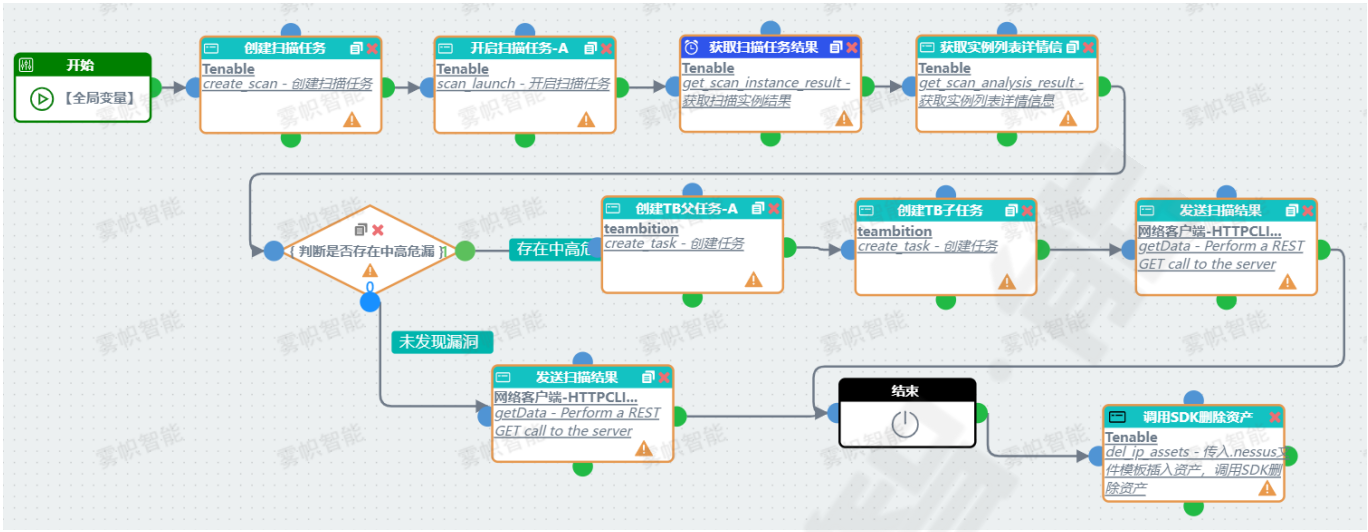
推荐理由和效果收益

这类响应工作流是处置"恶意软件事件"的初步工作，是最典型的需要自动化的工作。一方面这类工作几乎没有技术含量，而且在主机较多的环境中，发生的频率还是非常高的；另一方面操作步骤虽然简单但却非常繁多，需要在多个界面来回切换，还需将处置结果手工反馈给多方相关的人员，总体上非常的耗费人力；因此，这类工作正是满足了可以自动化且应该自动化的条件。

	人工方式	剧本方式	剧本效益/提升
时间消耗	>16小时	<1.6小时	>1000%
响应启动及时率	视团队人数和事件数量，加上需要耗时等待查杀结果，及时率普遍低于20%	100%	>500%
关联人员通知率	约80%，受CMDB数据的完备性影响较小	约90%，受CMDB数据的完备性影响	略有提升
查杀通知及时程度	不及时，一般在4小时左右，甚至更长	及时，查杀结束立即通知	明显提升

注：以每*100*条事件计算和评估；每条*60*分钟内启动响应；人工方式参与人数为*1*人；假设一次查杀约*1*小时，时间消耗包含查杀时间。

No.3 资产漏洞扫描管理（日常事务型）



剧本描述

该剧本的逻辑比较简单，通过SOAR剧本调用扫描器对主机进行漏洞扫描，扫描结束后，如果存在中高危漏洞，则启动相应流程（该剧本通过创建一个Teambition的特定任务来启动，实际应用中可以对接内部OA系统代替Teambition）并通知安全运营人员。

剧本主要步骤如下：

1. （其他剧本或父剧本）向某个资产组A添加需要扫描的资产
2. 调用Tenable为资产组A创建扫描任务；并启动扫描
3. 定时轮询Tenable的任务列表，如果任务结束，立即获取扫描结果
4. 使用规则判断扫描结果中是否存在中高危漏洞：
   - 存在 `N(N>0)` 个中高危漏洞：
     - 自动在Teambition上创建父任务-A；并指派父任务-A给相应负责人
     - 在父任务-A下创建 `N` 个子任务；并根据资产信息指派子任务给不同人员
     - 将扫描结果通过REST API发送给Teambition内的工作组
   - 未发现中高危漏洞或任务失败：
     - 将扫描结果通过REST API发送给Teambition内的工作组
5. 不论扫描失败或成功，移除该资产组A内的所有资产（后置节点实现，无论剧本成功与否，该节点都将被执行）

推荐指数: ★★★★

主要对接设备/系统：漏洞扫描器（Tenable等支持多任务、资产组的扫描器）、任务/流程管理系统（Teambition或OA等）

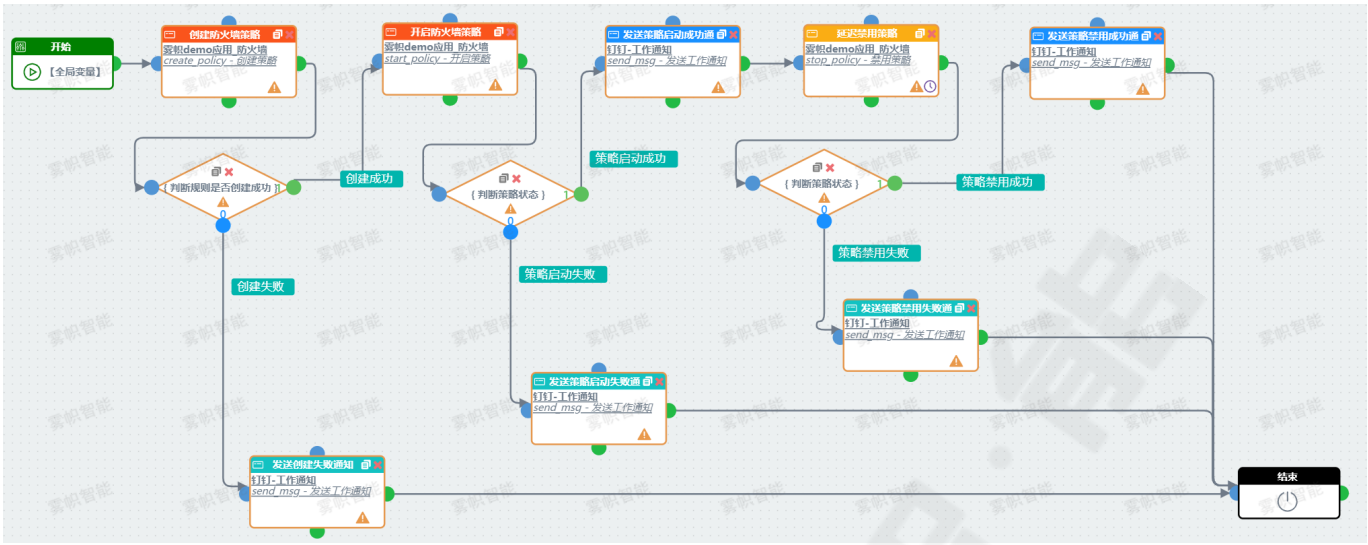
推荐理由和效果收益

漏洞管理这类日常工作，与恶意软件的查杀类似，从启动扫描到获得扫描结果往往需要漫长的等待，即使不计等待时间，筛选和阅读扫描结果和创建相关流程，一次至少也需要20分钟以上。在漏洞扫描这个场景中，不管操作扫描器、等待扫描结果以及发起相关修复流程，都是安全运营人员所头疼的耗时耗力的琐事，但却是每天都绕不开的工作。应用这样的剧本，可以让安全运营人员彻底从这类琐事从解放出来，专注于所发现的漏洞本身而不是被发现过程中的琐事所支配。

	人工方式/人	剧本方式	剧本效益/提升
报告筛选耗时	约2小时	约0.1小时	>2000%
修复流程启动耗时	>4小时	约0.1小时	>4000%
业务关联漏洞漏查机率	20%左右机会错过，取决于参与人与的个人专业水平	1%机会，不依赖人员的个人专业知识，依赖规则	明显改善
漏洞复查	几乎不开展，过程繁琐	完全自动开展，再次执行该剧本	极大提升

注：以每*100*条资产计算和评估；人工方式参与人数为*1*人

No.4 临时策略自动化管理（日常事务型）



剧本描述

该剧本上游连接了一个OA系统，OA系统有新的指定类型工单审批通过后，由OA系统调用SOAR的API，将工单信息打包成一条事件发送给SOAR。该剧本被事件触发后会从事件中提取与策略相关的参数如IP、端口、策略时效等，在目标防火墙上创建相关的策略。在策略时效到期后，再次调用防火墙关闭相关策略。

剧本主要步骤如下：

1. 创建防火墙策略，如已存在则覆盖更新策略信息；（新创建的和被更新的策略被防火墙自动设置成了未启用状态）
2. 判断策略是否创建成功；如果创建失败，则发送钉钉工作通知消息给指定人员，并终止剧本
3. 启动策略
4. 判断策略状态是否未启用；如果启用失败，则发送钉钉工作通知消息给指定人员，并终止剧本
5. 延迟与策略时效等长的时间后执行禁用策略(通过与no.1阶梯封禁中类似的延迟节点实现)
6. 判断策略状态是否未启用；如果禁用失败，则发送钉钉工作通知消息给指定人员，并终止剧本

推荐指数: ★★★★

主要对接设备/系统：SIEM/态势感知/SoC 、WAF/FW/IPS/ADS、IP归属地数据库/威胁情报系统

推荐理由和效果收益

这是整合OA流程与日常运维工作的典型示范。从OA流程触发到OA流程内容被执行，运维人员只需要参与OA流程的审批即可，再也不需要直接操作设备、维护"临时策略时效表"这样的额外

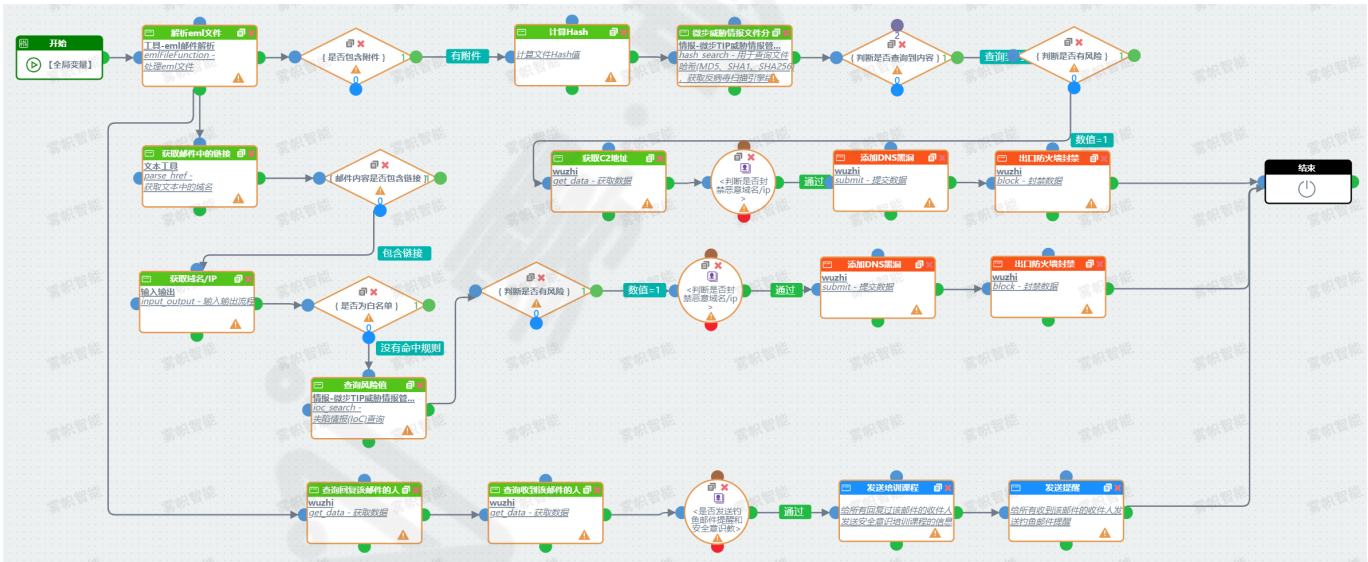
工作。

实践中，有些客户在OA的流程中添加了自动审批条件，或者在剧本中添加自动判断条件，实现对合规、紧急的需求的自动化审批和操作；有些流程发起者甚至产生一种错觉，以为这类流程是一种自助服务。

	人工方式/人	剧本方式	剧本效益/提升
用户等待时间	不定时，非紧急工单平均超过2小时/单	约0.1小时/单	>2000%
防火墙操作耗时	约1小时/10单	约0.1小时/10单	>1000%
受人员在岗状态限制	完全	部分，只受限于OA流程审批人员的在岗状态	极大改善

注：不计OA工单从创建到审批结束的时间

No.5 可疑邮件分析处置剧本（集成联动型+综合工具型）



剧本描述

这是一个借助SOAR的强大编排能力，重构的可一键执行的工具。可用于自动分析邮件提取关键信息和恶意内容，并联动了威胁情报系统进行自动研判；也可用于自动处置恶意邮件本身（发件人、发件域名等）以及与其关联的恶意内容（URL、域名等）。有些客户将这个工具与邮件网关协同工作（需要去除部分审批节点），扩展邮件网关的能力。如将首次出现的陌生发件人的邮件、包含特定关键字的邮件或者包含附件的邮件转给SOAR进行分析，由SOAR自动决策是否需要对该邮件进行拦截等 。有些客户则设置SOAR去监听一个公共邮箱（需要调整部分节点），

使得公司内所有人员都可以直接提交可疑邮件进行分析，并得到几乎实时的结果反馈，这让这个工具变成了一项7*24小时可用的公共安全服务，即减少了安全运营团队的工作，又提升了内部客户的满意度，可谓一举数得。

剧本主要步骤如下：

1. （手动传入或由父剧本传入）获取eml格式的邮件
2. 解析eml文件，提取需要检测的信息；提取以下信息：
    - 附件
    - 邮件主体内包含的URL链接
    - 发件人邮箱地址
3. 处置附件，如果有，则
    - 计算Hash值
    - 搜索威胁情报，并获取Hash值搜索结果
    - 判断搜索结果，如果存在风险，则查询是否存在C2地址
    - 如果存在C2地址，则发起审批；审批通过后添加DNS黑洞，并在出口防火墙进行封禁
4. 处置URL链接，如果有，则
    - 从URL中提取于域名和IP
    - 查询威胁情报，并获取URL域名、发件地址域名以及IP的风险值，
    - 判断风险值是否大于阈值
    - 如果风险值大于阈值，则发起审批；审批通过后添加DNS黑洞，并在出口防火墙进行封禁
5. 额外处置
    - 向邮件服务器查询，获取所有收到该邮件的收件人，包括密送的收件人
    - 向邮件服务器查询，获取所有回复过该邮件的收件人
    - 发起审批，审批人根据前面提取内容的处置结果，执行审批
    - 如果审批通过，将给所有收到该邮件的收件人发送钓鱼邮件提醒，并给所有回复过该邮件的收件人发送安全意识培训课程的信息，建议其参加培训

推荐指数: ★★★★★

主要对接设备/系统：邮件网关、威胁情报系统、DNS服务器、出口防火墙

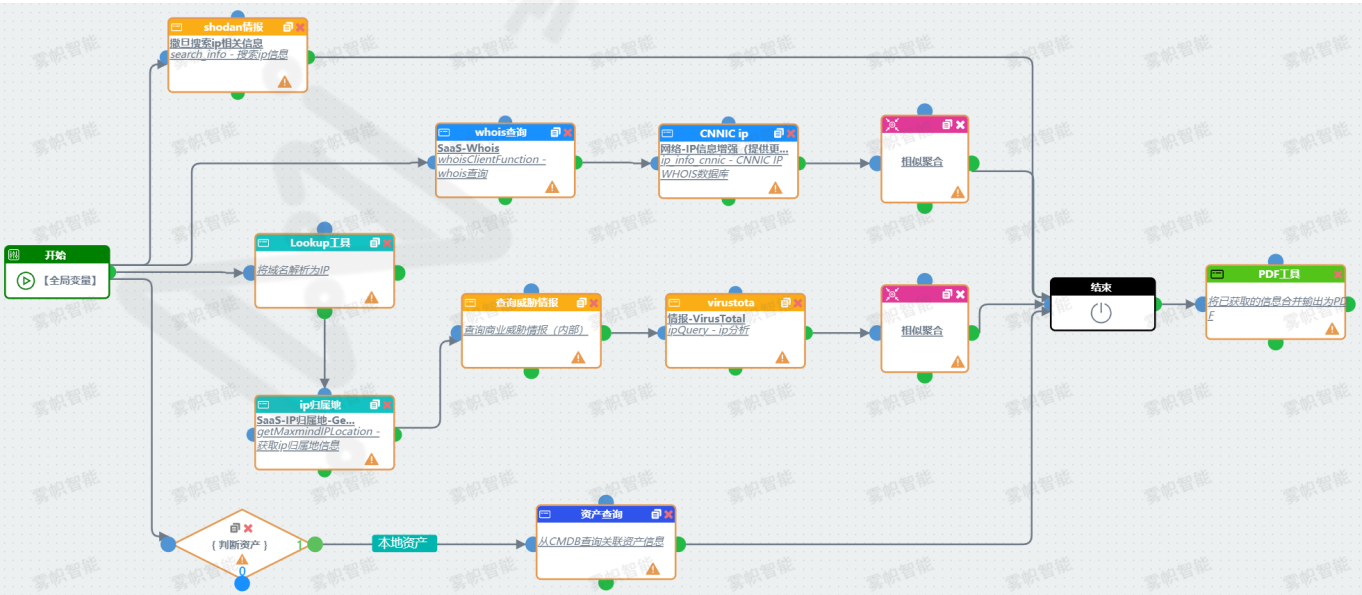
推荐理由和效果收益

对可疑邮件进行分析需要有合适的工具和一定的专业知识；如果从分析结果中发现威胁，必然需要采取相应的措施，以防安全意识较弱的用户意外造成不可控的损失。无论是分析或处置，都要求相应的专家在岗且参与，而采用剧本形式的工具几乎团队里的任何人都可以胜任这项工作，且可以以一当十进行人员补位，解决实际运营当中人员缺位的痛点。

	人工方式	剧本方式	剧本效益/提升
邮件分析耗时	>1小时/条	<0.1小时/条	>1000%
响应启动及时率	几乎不足1%	100%	极大提升
分析结果处置耗时	>0.5小时/条	<0.1小时/条（无审批节点）	>500%
恶意企图遏制机率	一般，视公司内普通用户的安全意识受教育水平	较大	明显提升
技能要求	中，需要有一定分析能力	无	极大提升

注：每条*60*分钟内完成响应；人工方式参与人数为*1*人

No.6 IP/域名多维信息查询剧本（综合工具型）



剧本描述

这是个典型的综合工具型剧本。一个剧本即覆盖了域名、Shodan情报、多源威胁情报以及资产信息等多维信息的查询。另外，还使用了一个后置节点生成了PDF。在实际使应用中，并不是每次查询都能成功，尤其是从外部查询信息时经常会遭遇失败，因此该剧本设计了一个后置节点来调用PDF工具，以生成信息汇总报告。这样使得即使部分查询节点失败了，也不影响报告的输出。整个剧本只有一个判断节点，主要是为减少对CMDB的调用。

剧本主要步骤如下：

1. 输入IP或域名，执行剧本
2. 并行步骤1：查询Shodan情报
3. 并行步骤2：依次查询国外whois服务和国内CNNIC，聚合本分支获得的重复的字段
4. 并行步骤3：使用lookup工具获得IP（无论输入是IP或域名都会返回IP）；查询归属地（防止后面节点失败后，本分支输出为空），查询商业威胁情报，查询公开威胁情报，聚合本分支获得的重复的字段
5. 并行步骤4：判断输入是否为资产，如果是资产则CMDB获取资产信息
6. 后置节点（无论是否存在执行失败的节点，都会执行）：汇聚信息生成PDF

推荐指数: ★★★★★

主要对接设备/系统：内/外部情报源、whois工具/服务、CMDB等

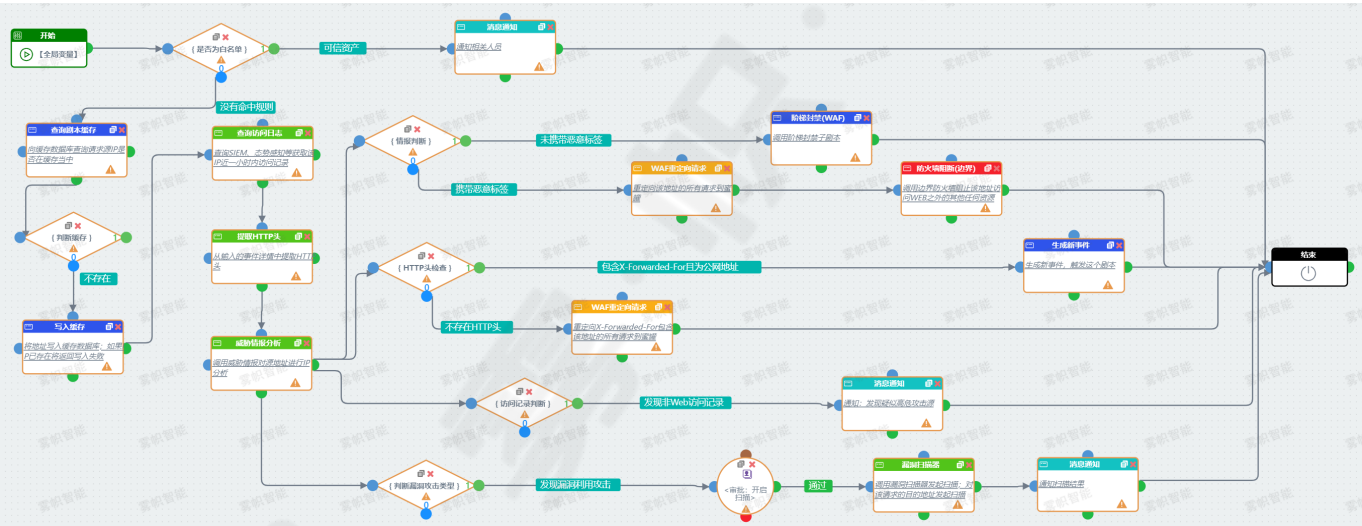
推荐理由和效果收益

在日常工作中，有些事件需要人工进行分析，那免不了需要查询IP/域名的相关信息。这剧本中涉及工具和查询系统就达9个，去除可能有重复信息的工具，日常工作中也将涉及至少5个。可见，看似简单的工作，实际上会消耗工作人员的大量时间；而且正是因为操作繁琐，在任务繁重的时段，工作人员不得不舍弃一些维度的信息。而使用剧本能将这一繁琐过程，简化成一键执行获取，不必取舍。

	人工方式	剧本方式	剧本效益/提升
查询耗时	>0.5小时/次	<0.1小时/次	>500%
结果复用	几乎不，查完不一定记录	完全可，保留剧本执行记录和PDF报告	极大提升
分析结果耗时	>0.2小时/条	<0.1小时/条	>200%
漏查机率	一般，但在繁忙时段更易漏查	极小机率，除非多个系统同时失败	明显提升

注：假设人工方式涉及工具为*5*个，进行评估和计算；人工方式参与人数为*1*人

No.7 恶意Web请求分析和响应(集成联动型+综合工具型)



剧本描述

这是复合型剧本，把漏洞扫描器、蜜罐、封禁设备（WAF、防火墙）等多个系统关联协作的剧本。只需输入一个Web请求的文本（支持大多数WAF设备的日志或tcpdump解析的结果）或是包含Web请求完整HTTP头的事件，就可用完成对Web请求的分析，如果发现异常内容，将执行一连串的响应动作。

非常特殊的是会将确定存在发起过恶意请对的IP地址做请求重定向，该IP地址后续的请求都将重定到蜜罐，一方面为了方便做后续更进一步分析攻击者的意图，另一方面是为阻止起对任何真实业务发起请求或触发其他告警。

更为特殊的是，这剧本还是个 `递归函数` ，可以自己触发自己对 `X-Forwarded-For` 字段值进行递归处理。

在实际应用中，部分客户将该剧本与上游检测系统对接获取事件进行自动响应。而其他用户更倾向于作为一个工具使用，对部分事件或IP进行分析和处置；因为涉及系统较多，如果上游产生的事件过多，很容易拖垮剧本内联动的设备。

剧本主要步骤如下：

1. （手动输入或从上游WAF、SIEM等）获取Web请求文本
2. 检查请求源地址 `IP1` 是否为白名单地址；如果是白名单内的可信资产，将在发送通知后，结束剧本
3. 向缓存数据库查询请求源地址 `IP1` 是否在缓存当中
4. 判断缓存结果，如果返回已存在，则结束剧本
5. 把请求源地址 `IP1` 写入缓存，如果写入失败，剧本会终止。写入失败有可能是其他剧本或本剧本的其他运行实例异步写入的。
6. 从上游日志汇聚的SIEM/态势感知等获取 `IP1` 近一小时内的所有访问记录
7. 提取输入包含的HTTP头
8. 调用威胁情报接口分析 `IP1`
9. 并行分支1，判断威胁情报查询结果：
    - 未携带恶意标签：将 `IP1` 作为参数，调用阶梯封禁子剧本（如本文No.1）
    - 携带恶意标签：修改WAF设置，重定向 `IP1` 的HTTP请求到蜜罐，在边界防火墙阻断 `IP1` 非Web应用的访问。
10. 并行分支2，判断HTTP头：
    - 判断HTTP是否包含 `X-Forwarded-For` 字段；如果 `X-Forwarded-For` 字段值是一个公网地址 `IP2` ，则创建一个新事件（不含HTTP头），递归触发这个剧本。新事件可能会触发并行分支1、2、3。
    - 如果不存在HTTP头，则调用WAF重定向X-Forwarded-For包含该地址 `IP1` 的所有请求到蜜罐（输入为本剧本产生的的事件）
11. 并行分支3：判断历史访问记录中是否有非Web的访问记录，如果有则向值班群发送"疑似高危攻击源"的预警。
12. 并行分支4：判断事件中的攻击类型字段，如果是漏洞利用型攻击，则发起审批，审批通过后会调用漏洞扫描器对该请求的目的地址发起扫描。

推荐指数: ★★★★★

主要对接设备/系统：SIEM/态势感知/SoC 、WAF/FW/IPS/ADS、IP归属地数据库/威胁情报系统、漏洞扫描器

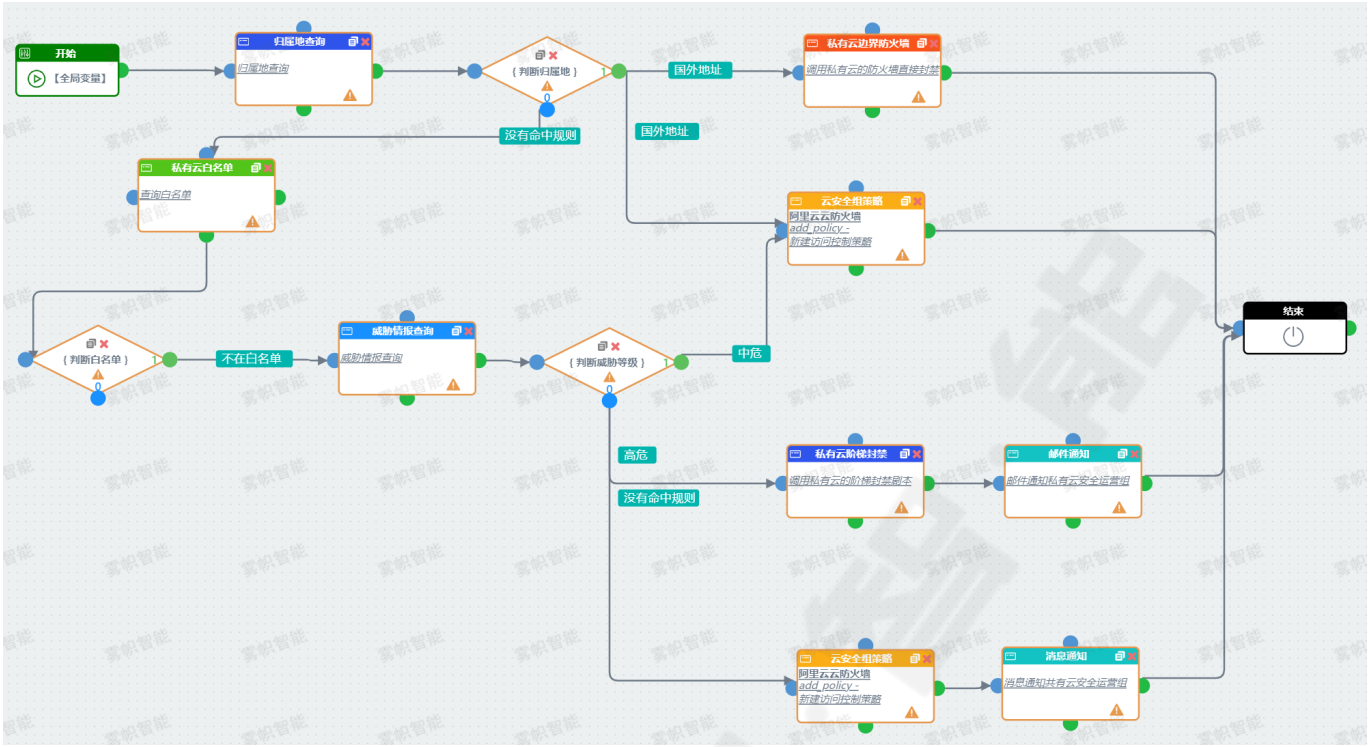
推荐理由和效果收益

剧本中涉及的流程和操作，在日常情况下，只会对相对确定是高危的Web请求进行如此全面的分析和操作，而放弃对中危以下的Web请求进行分析。因为完成相关流程和操作的工作量巨大，一个人几乎无法在有限时间内完成，只能选择性执行。而使用该剧本，一个人即可完成，且几乎不耗费多少时间，甚至操作人员连基本的HTTP协议常识都无需具备。

	人工方式	剧本方式	剧本效益/提升
时间消耗	>20小时	<0.1小时	>20000%
响应及时率	视团队人数和事件数量，及时率普遍低于10%	100%	>1000%
业务误封概率	较大机率	较小机率	精准防护
白名单	一定几率忽视	自动	准确匹配
黑名单/威胁情报	工作量巨大，不常用	自动	准确匹配
设备配置优化	困难低效，需要不定期手动维护ACL,地址组等	简易高效，定期自动维护	最优化
技能要求	中，至少要有相关协议分析的能力	无	极大提升

注：以每*10*条事件计算和评估；每条*60*分钟内启动响应；假设人工方式参与人数为*1*人

No.8 混合云环境响应剧本(集成联动型)



剧本描述

这个剧本主要运用于混合云安全运营的场景。该剧本对私有云和公有云安全策略在统一白名单的同时分别应用不同的封禁策略。公有云支持几乎无限长度的策略地址表/黑名单，因此对中危及其以上都直接进行封禁处理。而私有云内的设备只支持有限长度的策略地址表/黑名单，需要更严格地控制，防止超出设备容量。该剧本的主要特色是对不同云环境使用相同的安全策略，但同时根据不同云环境的特点使用不同的封禁策略。

剧本主要步骤如下：

1. 查询输入地址的归属地
2. 判断归属地
3. 对海外地址直接在以下位置执行封禁
    - 私有云的边界防火墙
    - 公有云的安全策略组
4. 对国内地址执行：
    - 匹配白名单（部署于私有云内，因私有云需要更频繁地调用）
    - 查询威胁情报
    - 判断威胁等级

5. 对中危和高危地址用以下方式执行封禁
    - 公有云的安全策略组
    - 私有云调用阶梯封禁剧本（如本文No.1剧本）
6. 对高危地址执行封禁后，分别通知公有云安全运营组和私有云安全运营组。

推荐指数: ★★★★

主要对接设备/系统：SIEM/态势感知/SoC 、WAF/FW/IPS/ADS、IP归属地数据库/威胁情报系统

推荐理由和效果收益

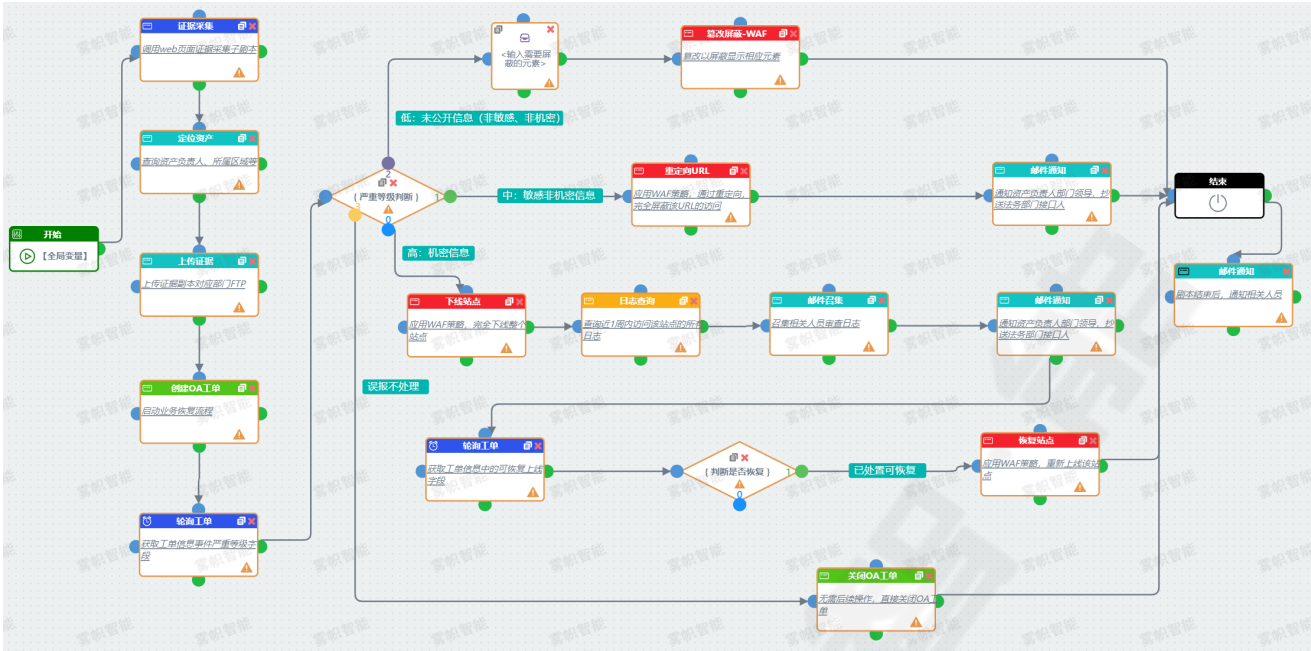
现今越来越多的企业都有着公有云和私有云，以及其他传统网络同时存在的情况。多环境、多网络区域的的存在给安全运营带来了不小的挑战。该剧本给我们提供一种即可以统一不同网络区域的策略，又可以根据其环境特点分而治之的新思路。剧本还免去了不同运营组之间不必要的沟通。

	人工方式	剧本方式	剧本效益/提升
时间消耗	>8小时	<0.1小时	>8000%
响应及时率	视团队人数和事件数量，及时率普遍低于50%	100%	>200%
业务误封概率	较大机率	较小机率	精准防护
白名单	一定几率忽视	自动	准确匹配
黑名单/威胁情报	工作量巨大，不常用	自动	准确匹配
设备配置优化	困难低效，需要不定期手动维护ACL,地址组等	简易高效，定期自动维护	最优化
跨组协同	需要	减少	改善

注：以每*100*条事件计算和评估；*5*分钟内完成响应；人工方式参与人数为*1*人

更多云上案例

No.9 Web页面信息泄露事件响应（应急预案型）



剧本描述

这是个预案型的剧本，其特点是通过OA和邮件，把一个紧急事件的响应流程通过剧本来推动。并在流程开始前，自动收集必要信息，供法务等流程相关人员参考。该剧本主要针对的是一些企业自营的公开Web站点发生信息泄露事件的响应工作。

剧本主要步骤如下：

1. （人工输入或泄密预警系统）获取发生泄密的url链接
2. 调用子剧本完成Web页面的证据采集（截图和内容爬取）
3. 定位资产信息，如负责人、所属区域等
4. 上传已采集的证据到内部FTP服务器
5. 创建一个OA工单，用于获取额外信息和恢复业务
6. 轮询OA工单是否包含事件严重等级的字段（通过异步方式轮询工单信息，直到人工输入并保存该字段）
7. 判断事件严重等级：
    - [误报]不处理，立即关闭OA工单
    - [低]涉及未公开的（非敏感、非机密）：由工作人员输入需要屏蔽的HTML元素XPATH或关键字，调用WAF对指定内容进行屏蔽

- [中]涉及敏感但非机密信息：调用WAF通过重定向屏蔽改页面的访问，邮件通知资产负责人的上级领导，抄送法务。
- [高]涉及机密信息：
  - 调用WAF屏蔽整个站点的访问
  - 查询WAF上近1周该站点的访问日志
  - 邮件召集相关人员，对访问日志进行审查
  - 邮件通知资产负责人的上级领导，抄送法务
  - 轮询OA工单是否包含可恢复上线的字段（通过异步方式轮询工单信息，直到人工输入并保存该字段）
  - 判断工单信息，如果工单包含可恢复上线的字段信息，将调用WAF解除屏蔽。

8. 后置节点：剧本结束后邮件通知相关人员

推荐指数: ★★★

主要对接设备/系统：工单系统（OA等）、WAF/NGFW、邮件系统、泄密预警系统（可选）

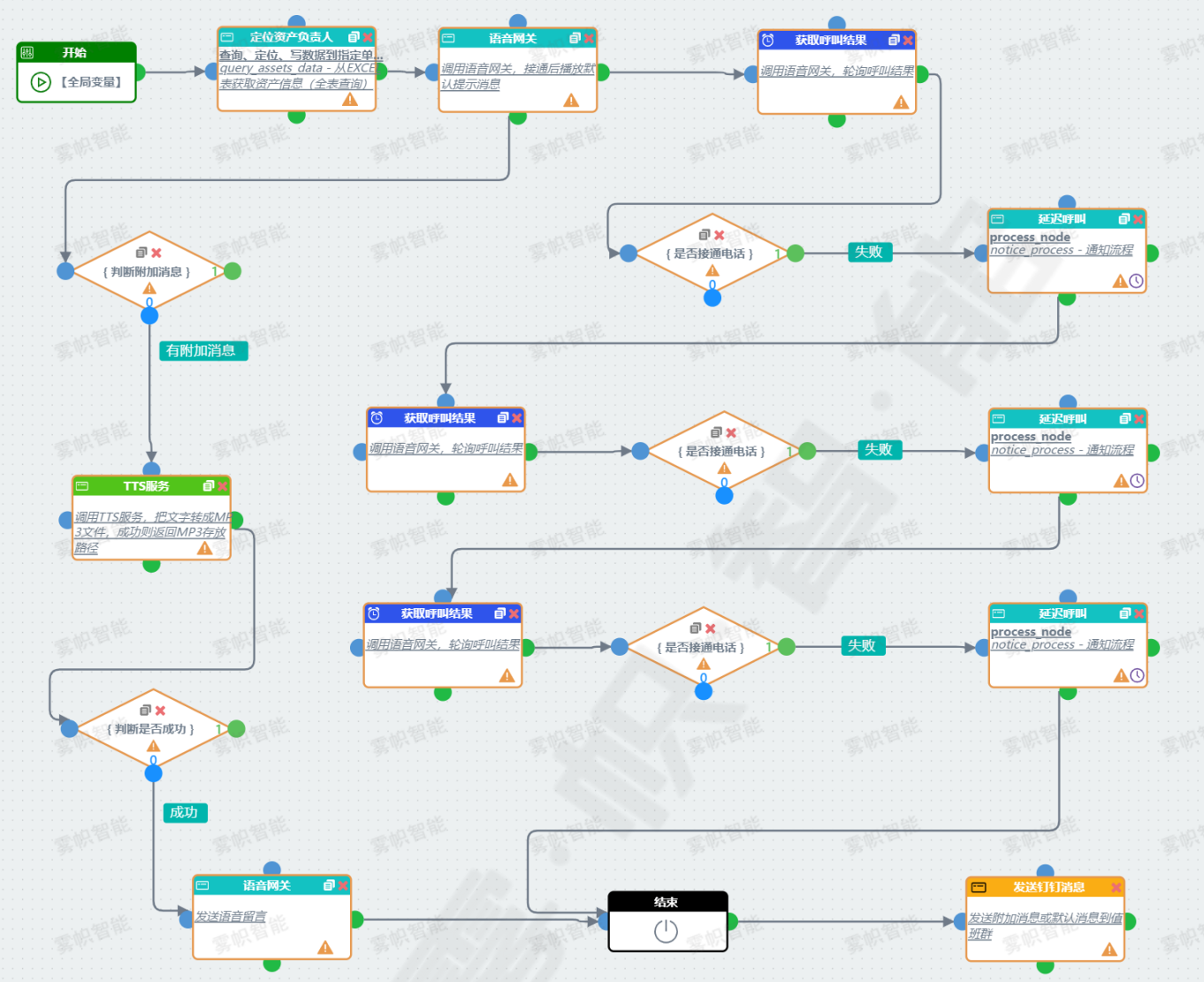
推荐理由和效果收益

对于这类较为复杂、又涉及多方人员的应急预案，往往会因为相关人员不熟练或协同困难，在启动时手忙脚乱，流程不能有效及时地开展。该剧本结合OA和邮件等对中、低危的事件进行全自动处置，对高危事件逐步推动响应的开展，并联动WAF及时屏蔽涉密信息。有了剧本的帮助，相关人员在面对这类事件时，无须慌乱，只需执行剧本和OA推送任务即可完成事件响应。

	人工方式	剧本方式	剧本效益/提升
总时间消耗	约4小时	约2小时	>200%
流程推动方式	指定人员	自动	更加可靠
屏蔽及时程度	不定，中，高危普遍及时	立即	改善
工作量	工作量巨大	极大减少	极大改善
跨组协同	需要	减少	改善

注：*60*分钟内完成屏蔽；人工方式参与人数为*1*人；假设*OA*流程等待时间为*1*小时；

No.10 通用紧急呼叫剧本（应急预案型）



剧本描述

这个剧本是个通用剧本，不仅适用于发生紧急安全事件的场景，也适用于其他需要紧急呼叫相关人员的场景，如发生重大网络故障，需要紧急联系网络运维人员等。该剧本包含了发起语音呼叫和语音留言的动作。语音留言需要TTS（Text To Sound,文本转声音 ）服务和具备语音留言的功能语音网关支持。TTS不是安全运营场景中常用的工具，但如今已有众多基于深度学习实现的开放服务，已经非常容易获得。剧本逻辑较为简单，可根据实际情况很方便地进行调整。

剧本主要步骤如下：

1. （人工输入）获取资产名称、附加消息
2. 查询预存的excel表格，获得需要通知的资产负责人；获取失败则终止剧本。
3. 启动语音呼叫分支，最多循环尝试4次以下流程：
    - 发起呼叫

- 轮询呼叫结果（异步方式）
- 判断呼叫结果，如果成功则中断循环

4. 启动语音留言分支：
   - 判断是否有附加消息，如果无则结束分支
   - 调用TTS服务，把文字转成MP3文件
   - 判断是否转换成功，失败则结束分支
   - 调用语音网关发送语音留言
5. 后置节点在剧本结束后，发送消息到钉钉（无论剧本失败或成功都会执行）

推荐指数: ★★★

主要对接设备/系统：语音网关、IM工具、TTS服务（可选）、联系人Excel文件

推荐理由和效果收益

虽然这个剧本实现的工作流非常的简单，但我们发现很多参与访谈的企业都存在类似的剧本，可以说是广受认可的直接有效的应急预案。我们也认为这类剧本是十分有必要的，因为在紧急事件发生时，留给工作人员的时间不多，可能根本没有足够的时间去翻查手册，逐一联系相关负责人等。显然以执行剧本来启动应急预案，由剧本来推动流程将会是即快速又有效的。

总结

企业所处行业不同、规模不同、安全体系建设进度不同、安全管理策略不同，所需要的自动化安全运营需求也不尽相同。因此，优先部署符合企业当前安全运营需求的剧本才是适合SOAR安全剧本实践的最佳策略；剧本应当随着企业自身安全体系的不断完善进行更新迭代，只要能以较低的成本最大程度提升安全运营团队效率和加固企业安全防御体系的剧本，就是企业自身的最佳实践SOAR剧本。

以上就是本次分享的所有内容。

鸣谢

本次报告调研对象包括但不限于银行、证券、运营商、互联网、汽车制造、烟草、电力、石油石化、房地产、轨道交通、医疗等行业客户。

十分感谢所有参与调研访谈的客户，感谢你们对我们调研工作的大力支持，以及对雾帜智能的服务和产品的认可！

版权所有

上海雾帜智能科技有限公司（简称雾帜智能）是一家以人工智能为核心驱动的新生代科技公司，正式成立于2019年4月。公司专注于将人工智能技术和现实应用场景结合，通过显著提升自动化水平助力企业解放生产力。该公司的主要产品HoneyGuide智能风险决策系统是首款以AI+SOAR为核心的安全协同作战平台，通过虚拟作战室、AI机器人和可视化剧本编排，帮助安全团队加速威胁响应与处置，提升运营自动化，实现风险自适应治理。产品已广泛应用于金融、运营商、能源、烟草、汽车制造等行业。2020年公司获得耀途资本天使轮投资，2021年再获腾讯、琥珀资本投资。

扫码关注**雾帜智能**官方微信公众号，可获取更多最新SOAR相关信息