物联网安全编排、自动化与处置响应技术研究

Research on Security Orchestration, Automation and Disposal Response Technology of Internet of Things

谢国涛，常超杰，范云飞（中讯邮电咨询设计院有限公司，北京 100048）
Xie Guotao, Chang Chaojie, Fan Yunfei (China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China)

摘　要：
针对物联网的安全编排、自动化与处置响应，提出一种集检查、响应、阻断、预防于一体的高效实现方案。构建针对物联网安全的SOAR系统，即基于提前预置的场景化策略，对可调度安全对象进行编排，生成剧本；系统运行中，通过态势分析预警触发编排预案执行，调度资源，下发安全指令，实现剧本自动执行；同时，该方案能够通过自学习，实现场景适应性的自动化编排，进而达到减少人工成本，缩短平均威胁处置时间，提升安全运营生产力的目的。

关键词：
物联网安全；SOAR；自动化编排；安全响应
doi：10.12045/j.issn.1007-3043.2023.04.009
文章编号：1007-3043（2023）04-0038-04
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract:
Aiming at security Orchestration, automation and disposal response technology of the Internet of Things, it proposes an efficient implementation scheme integrating inspection, response, blocking and prevention. Building a SOAR system for IoT security, which is based on the preset scenario strategy, arranges schedulable security objects and generates playbooks. During the operation of the system, through the situation analysis and early warning, the execution of the plan is triggered, the resources are scheduled, the security instructions are issued, and the playbooks are automatically executed. At the same time, the scheme can realize automatic arrangement of scene adaptability through self-learning, so as to reduce labor costs, shorten the average threat disposal time, improve the productivity of secure operations.

Keywords:
Security of Internet of things; SOAR; Automated orchestration; Security response

引用格式：谢国涛，常超杰，范云飞. 物联网安全编排、自动化与处置响应技术研究[J]. 邮电设计技术，2023(4)：38-41.

0 前言

2017年，Gartner重新将SOAR（Security Orchestration, Automation and Response）定义为安全编排、自动化与响应。Gartner认为，SOAR技术仍在快速发展演化，未来其内涵仍可能会发生变化，但其围绕安全运维、聚焦安全响应的目标不会改变[1]。然而，SOAR技术在物联网安全方面的应用也存在一些不足。本文提出一种集检查、响应、阻断、预防于一体的高效实现方案。SOAR系统收集不同来源的数据和警报，通过对可编排能力单元的统一调度指挥，实现标准化事件响应。SOAR系统能够实现人员、设备、资源、流程之间的协调统一，帮助安全人员完善、增加企业安全防护体系。

收稿日期：2023-03-07

1 物联网SOAR现状与解决思路

1.1 物联网安全现状

物联网技术的飞速发展使得物联网承载的价值越来越高，网络的规模越来越大，复杂度也越来越高。据统计，2021年全球物联网连接数量增长8%，达到122亿个活跃端点[2]。因此，黑客有更多的动机和手段来窃取信息和资源，对资产造成破坏，导致巨大损失。

面对这些挑战，只有建立完善的网络安全防御机制，才能有效地进行信息安全管理，为企业和个人提供更好的安全服务。

IoT Analytics 首席执行官 Knud Lasse Lueth 预测：到 2025 年，随着供应限制的缓解和增长的进一步加速，将有大约 270 亿台联网物联网设备[2]。卡巴斯基的一份报告《突破极限：如何解决特定的网络安全需求并保护物联网》显示，有 43% 的企业，其物联网基础设施的某些部分尚未得到任何保护。越来越多的物联网安全事件，促使企业寻求更加简便的物联网安全整体应对措施。因此SOAR也逐步走入人们的视野。

SOAR 系统可以提高安全威胁的可视性，可以通过自动化提高运营效率，能够更准确地识别安全威胁并提升安全防御能力。SOAR 中的编排也能够大大提高效率并降低对安全人员技术能力的要求。

1.2 物联网SOAR存在的问题

随着物联网产业的不断发展，SOAR 专用产品数量越来越多，但也出现了不少问题和矛盾。目前，SOAR存在以下几个突出问题。

a）未标准化。物联网信息安全检测、评估和准入均无统一标准。不同分析检测引擎对于同一风险事件的优先级划分不同。且管理不统一最终造成产品安全标准参差不齐和漏洞频出。

b）处置验证方式单一。通过处置验证对威胁处置效果进行验证，其验证方式单一，不能保障效果验证的准确性和客观性，从而不能从根源上确保威胁处置措施的准确性。验证主体单一，缺乏双重验证机制。

c）编排不够智能化。现有剧本的编排，基本由人工生成。随着物联网设备的增加，解决方案不断地更新迭代，人工的压力也会越来越大。

1.3 解决思路

a）针对告警标准化的解决思路。告警标准化主要考虑告警字段标准化、告警关联标准化、告警调查标准化等。

b）针对处置验证方式单一的解决思路。提出“响应验证+告警验证”的双重处置验证方式。响应验证，即对响应执行结果的成功或失败进行验证。告警验证，即处置后一段时间内，不再有相同告警，即验证成功。

c）针对编排不够智能化的解决思路。编排是提升协调和决策效率的核心，实现编排智能化的关键是能够智能生成剧本，可以从剧本库、动作库、知识图谱及安全人员处置经验考虑，使用AI智能生成剧本并进行模拟、优化、校验。

2 物联网SOAR设计

SOAR 的本质是实现从“人与安全工具”向“机器与安全工具”交互转变。将安全告警和事件以可以编排的工作流的形式进行自动处置和自动验证，这种工作流又被称为剧本（PlayBook）。剧本由 1 个或多个应用或动作组成。通过分析告警信息选择要触发执行的剧本，执行时按照编排的方式自动执行剧本中的应用或动作。自动化工作流的好处在于减少大量的重复性工作，提高安全处置效率。

如图 1 所示，总体架构主要包括告警管理、案件管理、剧本管理、编排引擎、安全响应以及对象管理。

2.1 告警管理

告警管理主要包括告警分诊、告警调查、告警响应和告警库。

a）告警分诊包括告警预处理、告警分析和告警合并，告警预处理就是对告警进行预处理操作。告警分析是为了确定处置方法。告警合并就是针对海量告警进行合并去重，以防误报和重复告警。

b）告警调查包括告警总览、告警统计和告警溯源，告警总览是为了方便了解总体状况。告警统计是为了多维度了解告警状况。告警溯源可方便安全人员更深入分析安全事件。

c）告警响应包括告警处置和对接管理，并把结果输出到告警库。告警处置就是对告警分诊的结果进行处置，触发下一步的处理步骤。

d）告警库是所有告警的合集，服务于告警响应和告警分诊等。

告警是物联网安全防护的必要条件，是网络运维支撑的重要组成部分。针对物联网SOAR告警标准化的解决思路如下。

a）字段标准化。可参照国标《入侵和紧急报警系统告警装置技术要求》（GB/T 36546-2018）。

b）关联标准化。涉及告警预处理、告警分析和告警合并的标准化。

c）调查标准化。涉及告警总览、告警统计和告警溯源。

d）告警库管理的标准化。对告警的分类、去重、合并和管理等的标准化。

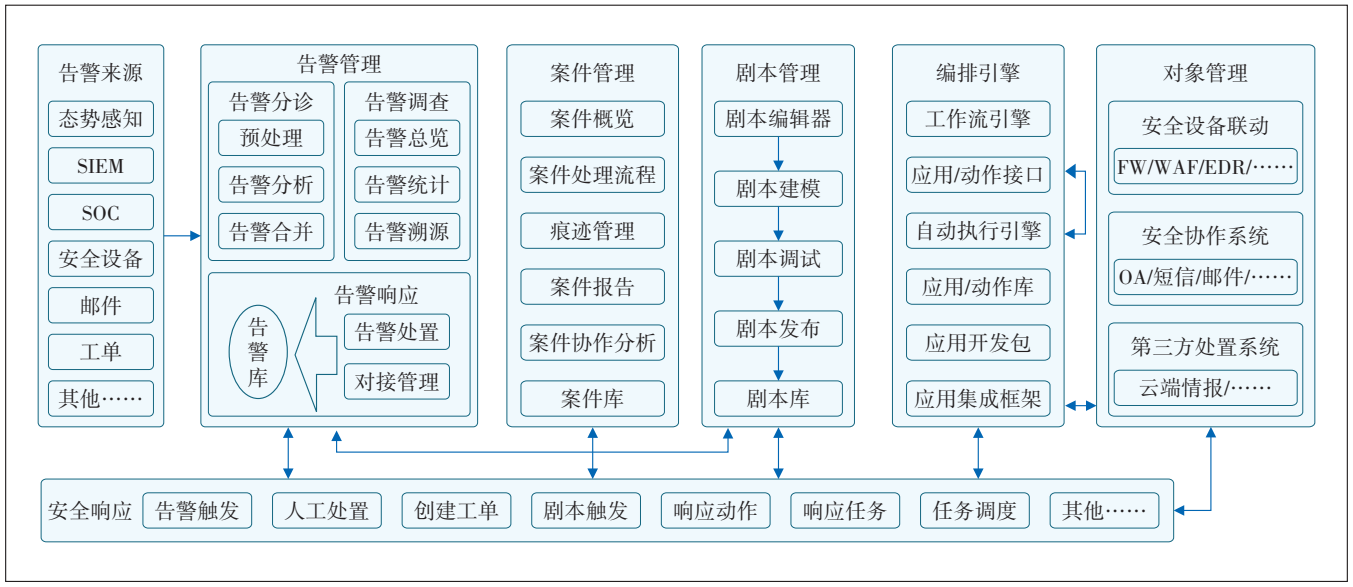

图1　物联网SOAR整体架构图

e）触发规则的标准化。对规则的触发条件和处置内容进行标准化。

2.2 案件管理

案件管理包括案件概览、案件处理流程、痕迹管理、案件报告、案件协作分析和案件库等组件。案件管理用来帮助用户对一组相关的告警进行流程化、持续化的调查分析与响应处置。案件处理流程应该能够对不同性质的案件安排不同的案件处理流程，并监督执行；通过告警管理不断积累案件相关的痕迹物证（IOC）和攻击者的战技过程指标信息（TTP）；通过编排功能进行调查和响应，可以针对案件中的所有告警执行剧本或者动作进行追踪，深挖疑点，深度挖掘案件中的疑点信息，以使案件信息更加丰富。

2.3 剧本管理

剧本管理是SOAR的核心能力和基本能力。剧本是面向编排人员的，其只关注编排逻辑本身。剧本管理模块包含剧本编辑器、剧本建模、剧本调试、剧本发布和剧本库等。

剧本是对安全告警事件处置时关联处置应用和动作的手段。剧本底层驱动的是工作流引擎，进而进行安全防护设施的调用。剧本处理流程如图2所示。

对已知威胁，SOAR可以自动根据已有的安全剧本进行处置。但是针对新型威胁，没有成熟的处置剧本的情况，需要人工进行处置并固化为相应的剧本。剧本支持系统内置和人工自定义编排多种方式。剧本处置过程中，工作流支持与人工配合，自动处理与人工决策能够进行互补。更进一步地，对于产生的新型威胁，系统可以使用案例库和剧本库，自动生成处置剧本。

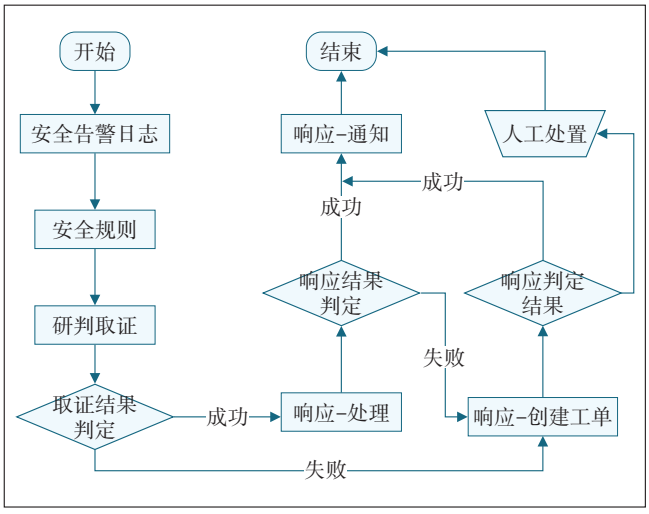

图2　剧本处理流程

因此实现编排智能化的关键是能够智能生成剧本。具体来说，就是系统可以根据剧本库、动作库和知识图谱及安全人员的处置经验，使用机器学习进行分析，智能生成剧本。并且可以模拟安全事件对剧本进行有效性评估，以优化和校验剧本，最终生成可行有效的智能剧本。

2.4 编排引擎

编排是指将多个系统或者1个系统内不同组件的安全能力通过接口按照一定的逻辑关系组合到一起，

用以执行指定的一系列安全操作流程。编排是提升协调和决策效率的核心。编排引擎包括工作流引擎、应用和动作接口、自动执行引擎、应用和动作库、应用开发包和应用集成框架。

编排是通过剧本来进行表述的。支撑剧本执行的是工作流引擎。工作流引擎解析剧本并调用自动执行引擎以实现按照剧本编排的工作任务；应用和动作接口通过API统一封装涉及SOAR的安全技术、工具、平台、系统、流程以及管理机制等安全设施；自动执行引擎支撑自上而下的落地，自动执行工作流中对应的应用和动作接口任务；应用和动作库、应用开发包和应用集成框架用于对应用的统一管理。

目前市场上的SOAR系统基本上只实现内置和手工编辑剧本，还未实现智能自动的生成剧本。编排的智能化可使SOAR的使用更加简便、高效、处理能力更强，是下一阶段发展方向。

目前情况下实现编排智能化生成剧本，还需要以下条件。

a）需完善应用/动作库，增强与物联网系统对接的能力。

b）需要增强响应能力，丰富响应手段和验证手段。

c）需要构建SOAR所在物联网环境的完善的安全威胁知识图谱。

2.5 安全响应

安全响应能够做到根据需要处理的安全事件和策略自动选择相应的剧本，并自动执行剧本中的操作流程，还可根据决策结果自动联动相关设备，实现防护阻断等动作。

安全事件响应包括告警管理、对象管理、工单管理、案件管理等功能。此外，隔离和修复是响应之后的一个重要操作。

将自动化安全验证环节纳入到SOAR的编排及响应体系中，相对于原来的人工验证，在效果上有以下提升：可实现验证经验的固化、积累和优化，大幅提升验证的效率，降低人工验证产生的误差。

针对物联网SOAR处置验证方式单一问题，本文提出“响应验证+告警验证”的双重处置验证方式。

a）响应验证。对响应执行结果的成功或失败进行验证。

b）告警验证。在响应成功后一段时间内，没有相同告警，即验证成功。否则验证失败，生成工单，并标记安全编排。若响应验证成功后，还有新的告警，则需要人工介入。结合响应结果、新的响应告警信息、人工验证和AI智能学习进行处理，以避免重复执行编排流程。

3 结束语

在物联网市场日益发达的今天，物联网安全问题势必成为首要问题。本文讨论了现今物联网SOAR中一些突出问题，提出一种针对物联网的SOAR架构方案。从告警管理、案件管理、剧本管理、编排引擎和安全响应等方面进行阐述，通过多种标准化设计，实现物联网安全事件处置流程标准化；通过双重处置验证方式，实现对响应执行的全面验证；通过高智能剧本管理模块，实现高效智能编排。

SOAR通常与企业的安全防护运维中心（SOC）一起协调实施。SOAR监控威胁情报源并触发针对安全问题的自动响应，帮助IT团队快速有效地解除众多复杂系统中的威胁。通过自动化能力，大大降低消除安全威胁所需的资源和时间，提高运营效率；同时更准确地识别安全威胁，降低对安全人员技术能力的要求。

安全是有成本的，SOAR带来的优势，也是有前提的，对威胁的洞察将作为SOAR的输入，对可编排能力单元的梳理与标准化是SOAR实现其功能的基础条件，同时企业架构的复杂性、运营的动态性、威胁的进化等都是SOAR实际运营中需要面对的挑战。

参考文献：

[1] 邢家鸣，王贵智. SOAR技术在银行业应用浅析[J]. 中国金融电脑，2020(7)：66-69.

[2] 千家网. 2022年物联网现状：全球联网物联网设备数量增长18%，达到144亿台[EB/OL]. [2022-12-20]. https://www.51cto.com/article/709485.html.

[3] 千家网. 43%的企业没有保护他们的物联网基础设施[EB/OL]. [2022-12-20]. http://bas. qianjia. com/html/2022-03/04_388288.html.

作者简介：

谢国涛，毕业于浙江大学，工程师，硕士，主要从事5G物联网密码与数据安全创新技术研究与应用工作；常超杰，毕业于安阳工学院，工程师，学士，主要从事5G物联网数据安全创新技术研究与应用工作；范云飞，毕业于西华师范大学，工程师，学士，主要从事5G物联网态势感知创新技术研究与应用工作。