奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

第1期

安全运行
迎来SOAR时代

Gartner

安全运行迎来SOAR时代

1. 安全运行的新趋势

1.1 安全运行面临挑战

什么是安全运行?

（网络空间）安全运行是一系列操作级别的日常安全活动的统称，它是一个整合相关的流程、技术、人员和服务，对企业和组织中网络空间资产的安全要素信息（资产、弱点、威胁、风险、情报等）进行持续地配置、感知、监测、检测、测试、分析、预警、告警和响应、恢复，并不断优化的过程，以确保网络空间安全、弹性地支撑企业和组织的业务战略。

不同的企业和组织中安全运行范围可能有所不同，按照滑动标尺模型[1]，总体上涵盖基础架构安全、纵深防御、积极防御、威胁情报四个领域。其中，基础架构安全运行活动包括以资产为主线的资产、漏洞、配置、补丁管理和以身份为主线身份、凭证、权限管理；纵深防御安全运行活动以安全策略为主线；积极防御安全运行活动以事件和威胁为主线；威胁情报安全运行则以情报共享为主线。每个领域的每个活动都强调闭环化。

安全运行是安全保障体系的重要组成部分，是安全治理和安全管理的基础支撑性工作。安全治理和安全管理工作能否落实到位，关键在于日常安全运行工作的成效。

为了实现有效的安全运行，企业和组织进行了大量的投入，纷纷成立了安全运行中心，建立了安全运行团队，搭建了安全运行平台，并逐步积累了一些安全运行流程。随着网络空间安全形势日趋恶化，网络安全地位日益提升，以及受限于传统安全运行中心的建设理念，现有的安全运行工作面临诸多挑战。以下列举部分典型的挑战：

[1] https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240

1) 安全运行人员紧缺且仅技能不足，工作压力大，流失率高，重复性劳动量大，效率低下。

当下安全从业人员匮乏已是众所周知[2]，安全运行人员尤其紧缺[3]，而且政企单位对安全运行人员的需求量最多[4]。同时，安全运行的岗位技能要求日益复杂，在岗人员普遍技能不足，有经验的安全分析师更是稀缺。

另一方面，企业和组织的安全运行人员工作负担沉重，有的还要7*24*365随时待命，且工作平台和工具不给力，要处理的信息太多，直至筋疲力尽，人员流失率往往很高[5]。如果遇到重保任务，更是捉襟见肘。

2) 告警太多，处理起来费时费力，告警消除的速度远远低于告警产生的速度。

安全运行工作中最主要的工作之一就是告警处理。安全工具不断叠加部署造成告警数量与日俱增。如何高效处理海量告警信息已经成为安全运行的一个永恒话题。每种工具都在尽力减少警报，而SIEM和传统的SOC也花费了大量的精力在消除告警上：大数据分析技术、机器学习和人工智能技术纷纷引入，试图从多个维度降低告警，但效果依然有待改善。

3) 网络从被攻陷到被攻击被遏制的空白时间依然太长，安全检测时长，以及安全响应与修复的时长急需缩短。

历年来Verizon的《数据泄露调查报告》揭示了一个事实，就是网络从被攻陷到攻击被遏制的空白时间始终存在，并且改善不大。平均检测时长、平均响应时长和平均修复时长都需要不断努力缩短。在2019年的报告[6]中，平均失陷时长在分钟级，平均检测时长和平均遏制时长在天、周，甚至月级，中间的时间差很大。

4) 安全运行的流程难以转化为知识，不利于积累和传承，容易流失。

铁打的营盘流水的兵，安全运行团队的更迭是不可避免的。对于企业和组织而言，安全运行的知识管理十分重要，依靠安全运行过程中积累下来的各种知识，能够极大地加速安全运行能力的持续提升，加快新人上手的速度。

现在很多安全运行平台都有知识管理，或者叫安全内容管理，譬如安全信息数据标准化策略、关联分析规则、分析算法、分析场景、安全情报，等等，但对于安全运行流程的知识转化却很少提及[7]。事实上安全运行的很多流程都是安全实战对抗的技战术过程的凝练，具有很强的实战价值。这些流程往往留存在有经验的分析师脑子里，通过言传身教的方式进行传递，极易流失，也不利于持续改进。

5) 安全运行相关的人员、流程和工具互相割裂，缺乏整合，缺少协同，制约了安全运行成熟度的提升。

前面提及的人员不足问题、告警疲劳问题、响应时长问题，以及运行流程知识转化的问题，都说明了当前安全运行工作的同一个深层次挑战，即安全运行相关的人员、流程、工具之间的鸿沟问题。

- 人缺少真正面向实战化安全运行的工具，运行工作碎片化现象严重，存在大量断点，效率难以提升。同时，运行团队内部和内外部之间均缺乏有效的沟通与协作工具，被迫求助于各种非安全协同软件，难以有效传递安全信息。
- 有效的安全运行流程要么缺乏，要么难以顺畅高效地将人和工具连接起来。流程真正执行起来涉及大量人工操作，重复性操作，制约了人的工作效率和积极性。

[2] Ponemon《在自动化时代如何分配IT安全人员的工作》调研报告，2019。
[3] SANS《SOC的通用和最佳实践》，2019。
[4] https://www.sohu.com/a/332925502_609556
[5] Ponemon 《SOC的经济学：出效果到底要花多少钱》调研报告，2020。
[6] Verizon《2019年数据泄露调查报告》。
[7] SANS《SOC的通用和最佳实践》，2019。

- 工具的设计更多关注解决具体技术问题而忽略了如何让人运行起来，结果给运行人员的感觉往往就是一堆功能的罗列。更严重地，工具和工具之间缺乏整合，缺少协同接口，运行人员在工作中被迫不断地在不同的工具之间来回手工切换，以复制粘贴的形式传递数据。

综上所述，企业和组织急需一套真正整合人员、流程和工具的安全运行平台。

1.2 安全运行三大趋势

随着网络空间安全对抗的持续升级，当前企业和组织的安全运行工作在人员组织、告警处置、快速响应、知识沉淀、整合协作五个方面面临的挑战越来越突出。为了应对这些挑战，新的思路和技术不断涌现，凸显了未来安全运行发展的三个新趋势。

趋势 1: 安全能力编排化

面对层出不穷的安全威胁，企业和组织部署了大量安全设备和系统，并且还在不断增加。安全运行人员每天都需要跟这些设备和系统，以及其它工具反复打交道，一个完整的安全运行流程往往涉及到多个设备和系统，需要在这些工具之间来回切换。尽管企业和组织可能已经部署了SIEM、SOC平台或者大数据安全分析平台，能够集中化的采集和分析安全数据，但在实际环境中，仅仅依靠这类平台也不足以做出分析结论，还需要依据安全流程调用其它工具，获取其它信息来辅助决策。更重要地，以数据为中心的集成无法真正整合现有分散的安全工具和技术，无法对它们进行配置、控制和查询。因此，未来的安全运行还需要一个全新视角的技术集成。

如果将企业和组织的各种安全设备、系统，以及云端的安全服务和相关运行工具看作一个个安全能力，那么将企业和组织现有的安全能力通过编排集成到一起已经成为未来安全运行的重要趋势。借助安全编排技术，可以对安全运行流程进行形式化地描述，并映射到安全能力以及安全运行参与者上，促成人与人、人与工具、工具与工具之间的有机协作，同时也促成安全运行流程的知识转化。

趋势 2: 安全流程自动化

安全自动化并非新技术，已经存在了许多年。但目前为止，我们更多实现的是某个安全技术和能力的自动化，譬如资产发现自动化、数据采集处理自动化、安全分析自动化，等等。这些安全技术自动化普遍缺乏从安全运行视角的考量。安全运行人员在执行安全流程的时候，需要一种端到端的自动化能力，将一个流程中涉及到的多个技术点自动地衔接起来。

安全运行流程的自动化已经成为了安全自动化领域的热点，也是未来安全运行的发展趋势。安全运行流程自动化是建立在当前分散的安全技术自动化基础之上的，从运行视角出发的，端到端的安全流程自动化。在安全能力和安全流程编排化的发展背景之下，安全流程自动化与安全流程编排化相互结合，表现为安全编排的自动化。

趋势 3: 安全运行闭环化

安全运行的体系设计从一开始就强调闭环化，不论是经典的防护、检测与响应（俗称PDR）体系，还是NIST的网络安全框架（CSF）定义的IPDRR（识别/保护/检测/响应/恢复）6个阶段，都将闭环化视为一个基本的安全架构设计原则。尽管如此，直到近几年，安全投资的重心主要集中在防御和检测上，对响应的投入明显不足[8]。另一方面，包括Verizon和SANS在内的大量分析研究表明，对于企业和组织而言，响应时长是安全防护体系中的主要短板。

可以预见，安全运行的未来重要趋势之一是增加对安全响应的投入，而安全编排与自动化将首先应用于安全响应。

1.3 SOAR应运而生

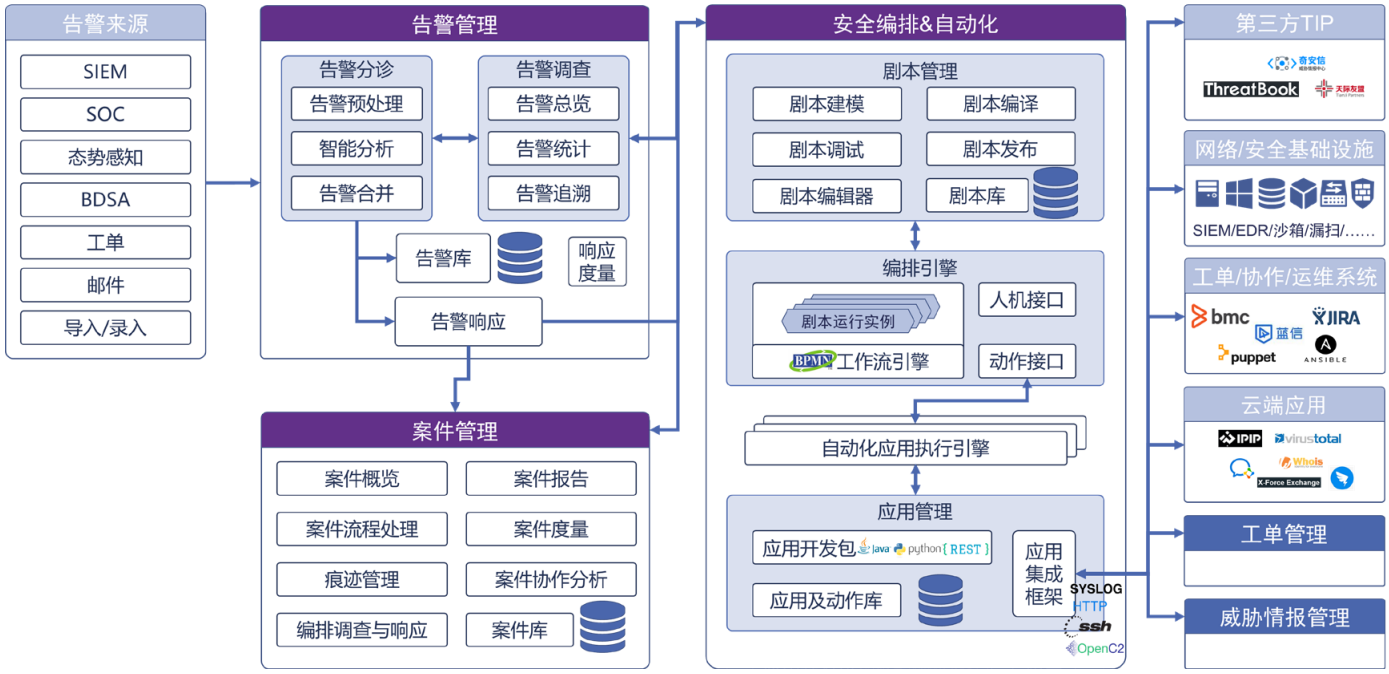
为了应对安全运行面临的挑战，顺应安全运行未来发展的新趋势，SOAR（Security Orchestration, Automation and Response，安全编排自动化与响应）应运而生。

Gartner将SOAR定义为“一种从各种来源获取输入，并应用工作流来处理各种安全过程与规程，从而为安全运行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”。[9]

SOAR这个概念一经Gartner提出来，得到了极大的关注，目前处于炒作曲线的顶峰。Gartner 预计，“到2023年SOAR市场收入将达到5.5亿美元”。[11]

[8] https://owasp.org/www-project-cyber-defense-matrix/
[9] Gartner Inc., Hype Cycle for Security Operations, 2020, 23 June 2020, G00467096
[11] Gartner Inc., Forecast Analysis: SOAR, Worldwide, 29 May 2019, G00390834

图 1: 奇安信SOAR功能架构



资料来源: 奇安信集团

2. 奇安信SOAR

奇安信SOAR是一个真正的实战化安全运行平台，它将安全运行相关的团队、工具、流程和领域知识通过编排和自动化技术整合在一起，有序处理多源数据，持续进行安全告警分诊与调查、威胁猎捕、案件处置、事件响应，并最终实现高效、有效安全运行的智能协作系统。

奇安信SOAR具有以下显著特征:

- 面向SecOps，以高效、有效为目标;
- 以编排和自动化为核心;
- 是一个智能化协作运行系统;
- 关键功能包括: 安全告警分诊与调查、威胁猎捕、案件处理、安全事件响应;
- 实现了团队、工具和流程的无缝整合。

2.1 系统功能架构

奇安信SOAR的功能架构如图 1 所示:

系统功能总体上分为4个部分，分别是: 安全编排与自动化、告警管理、案件管理和工单管理。

安全编排与自动化: 系统的核心功能，实现了安全能力的集成、安全流程的编排与自动化执行，包括剧本管理、编排器和应用管理功能。其中，工作流引擎驱动的编排器是安全编排与自动化的中枢，实现了基于剧本的安全运行流程编排调度和活动执行; 自动化应用执行引擎实现了已集成安全能力的自动化调用。

告警管理: 帮助用户进一步对各类告警信息进行智能化分析和编排化调查，核实告警、降低误报，提升后续安全响应的准确度与有效性，包括告警分诊、告警调查、告警响应和告警库四个功能。其中最核心的是告警分诊和告警调查，这也是区别于传统SIEM/SOC平台的告警管理功能的关键之处。

案件管理: 帮助用户对一组相关的告警进行流程化、持续化、协同化的调查分析与响应处置，包括案件概览、案件处置、案件协同、案件报告、痕迹管理等功能。

工单管理：涵盖用于突发性告警响应的一次性工单和日常反复自动执行的周期性工单，包括工单处置、工单流转等功能。

2.2 系统用户视图

图 2展示了系统的用户视图：

从用户视角来看，系统包括了5种使用者，分别是：流程设计与剧本编制人员、应用开发人员、运维人员、协作团队、管理层。

流程设计与剧本编制人员：负责将传统的安全运行流程和规程转换为SOAR平台可识别的编排化剧本和任务。他们对企业和组织的安全流程十分了解，并清楚一个落地化的安全流程需要集成/调用那些现有的安全能力。

应用开发人员：负责将企业和组织现有的安全设施和系统通过应用程序接口（API）进行应用化封装，转换成一系列安全能力（服务化功能）。他们对安全基础设施和各类流程工具的API调用十分熟悉，具备基于解释性编程语言的使用与开发能力。

运维人员：负责企业和组织日常安全运行的运维人员，包括一线运维、二线分析师。他们使用SOAR提升安全运行工作的自动化水平和运行效能，节约运维时间与人员成本。

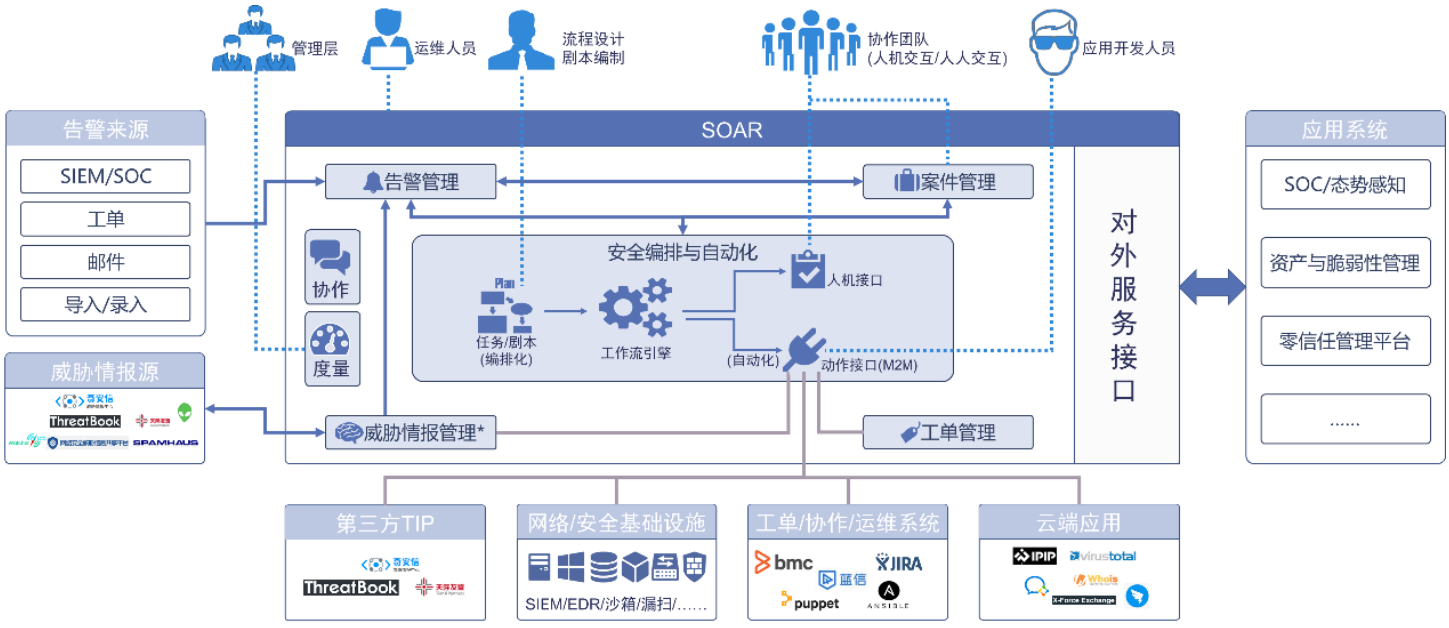
协作团队：指与企业和组织安全运行团队在安全运行过程中的利益共担方，譬如其它专门的应急响应团队、威胁猎捕团队，以及相关业务部门安全团队、公司管理层、外部协作单位、下级单位、上级主管部门等。

管理层：是指企业和组织安全运行部门的中高级管理者，包括安全运行三线经理、CSO、CIO等。他们使用SOAR来对安全运行的过程和效果进行度量，对自动化与编排的效果进行度量，并对安全运行过程做出优化与改进决策。

3. SOAR的关键能力

奇安信SOAR具备5大关键能力，使得其区别于其它同类产品。这5大特点及能力分别是：安全能力编排化、安全流程自动化、告警响应智能化、案件管理全程化、系统架构开放化。

图 2：奇安信SOAR用户视图



资料来源：奇安信集团

3.1 安全能力编排化

安全能力编排化（Orchestration）是指系统一方面可以通过自底向上地通过安全设备接口化和安全接口应用化实现安全应用编排化；另一方面则自顶向下地将安全运行团队的安全运行过程和规程进行形式化落地，实现运行过程的剧本化。最后，借助运行过程剧本化和安全应用编排化，实现安全能力的集成与编排，并为安全流程的自动化执行奠定基础。如图 3 所示，展示了安全能力编排化的不同层次。

通过安全能力编排化，真正实现了将不同的设备和系统协同联动起来的目标，就像一个交响乐队的指挥。

安全能力编排化包括了几个重要且相关的概念：安全编排、剧本、应用。

安全编排是将企业和组织在安全运行过程中涉及的不同系统或者一个系统内部不同组件的安全功能通过可编程接口（API）封装后形成的安全能力和人工检查点按照一定的逻辑关系组合到一起，完成某个特定安全运行流程的过程。安全编排是将安全运行相关的工具/技术、流程和人员等各种能力整合到一起的一种协同工作方式。

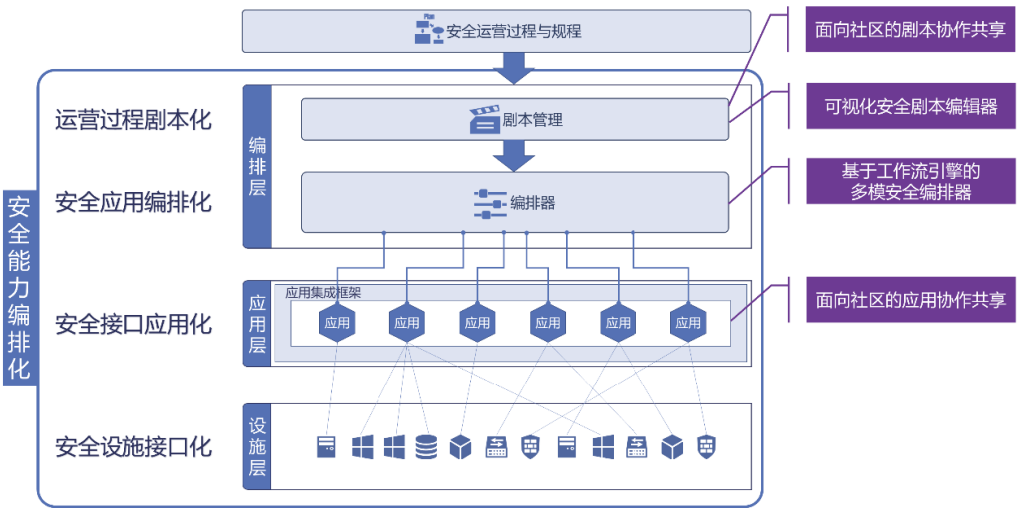
剧本是安全运行流程在安全编排系统中的形式化表述，并能够在编排器中的工作流引擎驱动下运行。编写剧本的过程就是将安全运行流程转换为剧本，并在剧本中将各种应用编排到一起的过程，也是将人读安全运行流程转换为机读工作流的过程。

应用是指企业和组织安全运行过程中需要用到的各种安全工具、协作工具及其它工具通过API或UI暴露出来的功能，经过标准化统一封装后形成的安全能力，并以服务的方式对外呈现出来。应用执行的最小操作单元是动作，即这个应用中所包含的操作指令。通常，一个应用包括多个动作。

奇安信SOAR的安全能力编排化具有与众不同的技术特点，包括：

1) 基于符合BPMN2.0规范的工作流引擎驱动的多模安全编排器；

图 3：安全能力编排化



资料来源：奇安信集团

2) 真正可视化的安全剧本编辑器；

3) 面向社区的剧本及应用协作与共享。

3.2 安全流程自动化

安全流程自动化（Automation）是指安全运行流程与规程尽可能地自动化执行，从而大大提升安全流程的执行效率，节约时间和人力成本，并确保能够持续达成预期的效果。

安全流程自动化不等于安全编排。实际上，安全编排得到的任务和剧本指明了一系列操作的步骤和下一步走向的判定条件，跟自动化无关，既可以人工执行，也可以自动执行。如果安全编排中的任务和剧本的某些个步骤或者判定条件以自动化的方式执行，则将可以称作安全编排执行过程的自动化，简称安全编排自动化。在实际应用场景中，几乎所有安全编排任务和剧本的执行都或多或少地涉及自动化，否则安全编排的价值十分有限。因此，通常将安全编排等同于安全编排自动化。

还需要指出的是，安全编排自动化不等于安全编排任务和剧本执行的完全自动化，所有否认人在安全运行工作中的决定性作用的观点都是不现实的。在实际应用场景中，安全编排自动化基本都是半自动化。

奇安信SOAR的安全流程自动化体现在以下几个方面：

1) 自动化告警分诊：系统能够基于一些列预定义的预处理策略、关联分析策略和合并策略自动化对告警严重性和处置优先级进行划分；

2) 自动化安全响应：针对需要进行调查/响应的告警信息，系统能够基于预定义的响应策略自动化地执行匹配的剧本和应用动作；

3) 自动化剧本执行：系统所有的剧本都通过编排器进行加载，并在工作流引擎的驱动下自动化的执行；

4) 自动化应用执行：剧本在工作流引擎里执行过程中如果某个活动需要调用集成化的安全能力，系统会自动激活应用执行引擎，并通过应用集成框架对相关能力进行接口调用，并将返回结果送回工作流引擎；

5) 自动化案件处置：将告警或者相关痕迹物证信息加入案件中后，系统会根据预定义的处置策略自动化地执行匹配的剧本和应用动作；

6) 自动化服务调用：系统对外提供API调用接口，供外部第三方应用系统调用，为它们提供编排、自动化与响应服务。

3.3 告警响应智能化

对来自企业和组织的各种告警信息进行基于编排与自动化的响应是SOAR的基本能力。此外，系统还提供了智能化告警响应的能力，进一步提升了告警响应的精准度和有效性。

奇安信SOAR的告警响应智能化体现在以下几个方面：

1) 智能告警分诊：包括智能化、规约化的告警预处理，以及基于策略的告警合并。同时，系统还系统可选的高级告警分析功能，帮助用户进一步提升告警价值，减少告警数量。告警分析采用基于关联规则的分析技术，能够将不同来源的告警信息连同外部的情境数据进行交叉比对与关联。

2) 智能告警调查：安全运维人员和分析师可以对告警信息进行深入调查，支持交互式调查分析，支持基于剧本和应用动作的编排化调查分析，支持告警统计与追溯下钻。通过告警调查丰富告警信息、核实告警原因、对齐处置对策。

3) 智能告警响应：一旦确认某个告警信息为安全事件（Incident），可以自动触发响应剧本，或者自动添加到相关的案件中，也可以提醒分析师进行人工响应。

3.4 案件管理全程化

案件管理（Case Management，也称作案例管理）是指一组人针对一系列相关的安全事件按照预先设定的规程，进行专门地持续调查与响应的协作过程，以及这个过程中产生的各种情境数据与痕迹物证的管理，还有过程本身的全生命周期活动记录。案件管理过程综合应用了编排与自动化技术，体现了团队、工具和流程的融合。通过案件管理，实现对一系列安全事件的快速响应，相关痕迹物证的保留与关联，并通过“卷宗”（活动记录）对案件处置过程进行复盘、总结，以及处置预案、规程和响应技战术的持续改进。

奇安信SOAR具有完整的案件管理功能。

1) 基于案件的全生命周期响应处置

2) 编排化案件协同调查分析与痕迹管理

3) 案件处理全过程记录与复盘

3.5 系统架构开放化

作为一个对企业和组织现有以及未来可能具有的安全能力进行集成和编排的系统，其自身的系统架构开放性至关重要。只有开放性的系统架构才能确保企业和组织安全编排与自动化的需求能够持续得到满足。

奇安信SOAR产品在系统架构层面具有4个方面的开放化特点：

1) 开放可扩展的应用集成框架

系统具备开放可扩展的应用集成框架，使得应用开发人员可以方便地进行应用开发与集成，将各种安全基础设施与应用工具进行能力化封装。

系统内置开发环境SDK，提供完善的开发手册与指南，允许开发人员以Python、Java语言进行应用开发。

2) 基于API的双向集成、支持多种协议接口、支持OpenC2

开发人员在集成安全基础设施与应用工具的接口，实现能力化封装的时候，既支持单向API集成，也支持双向API集成。

应用集成框架允许开发人员以几乎任何协议远程调用安全基础设施和应用工具，默认支持Rest API、SQL、SSH、TELNET、WMI、HTTP、SYSLOG等协议，同时也可支持OpenC2。

3) 编排器可扩展、剧本可自定义

系统的编排器采用遵循BPMN2.0规范的工作流引擎来驱动，符合国际标准，具有很强的扩展性，能够适应不断发展、日益复杂的安全运行流程的形式化表达的需求。

与此同时，系统具有开放的剧本自定义功能，剧本设计师既能够通过可视化剧本编辑器编写所见即所得的安全剧本，也可以直接通过Python等语言直接编写特定目标的安全剧本，剧本的表达能力仅取决于设计师和应用环境自身。

4) 开放的对外接口

系统对外提供丰富的南北向接口，包括告警采集接口、编排接口、工单接口、案件接口、剧本执行接口。系统可以为其它第三方安全系统与应用提供基于API的按需使用的编排、自动化与响应服务。

4 SOAR助力全局态势感知与实战化安全运行

随着数字化转型的深入推进，政企机构网络安全形势愈发严峻，网络安全能力不仅要达到监管要求，更需要面向实战，保障数字化业务。网络安全防防护必须转变为体系化规划建设模式。

奇安信采用系统工程的方法论，结合“内生安全”的理念，发布了面向未来五到十年的新一代网络安全框架。该框架从顶层视角出发，帮助各行业建立与数字化与信息化环境的深度融合、全面覆盖的网络安全能力，构建出动态综合的网络安全防御体系，全方位保障业务安全。

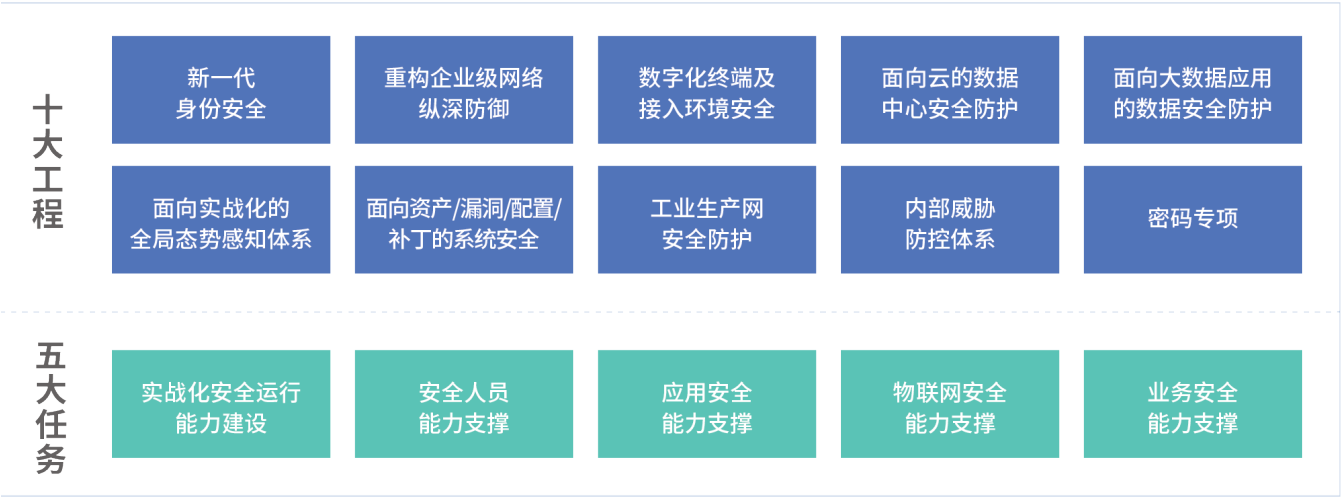
框架以促进政企数字化业务为使命，以网络安全能力建设为导向，先依据叠加演进的滑动标尺模型设定安全能力目标，然后以工程和任务的形式形成规划，再从安全技术体系和安全运行体系两个方面进行建设落地，以达成安全能力目标。

新一代网络安全框架在规划层面，以实体工程和支撑能力两个维度，将网络安全体系规划内容划分为十大工程和五大任务（参见第10页图4）。

以往态势感知系统重视安全数据展现却忽略安全运行所需要的安全数据分析能力，更缺少基于分析结果的决策与处置响应能力，难以形成有效防护的闭环。在奇安信提出的面向实战化的全局态势感知体系工程中，强调建设安全运行流程化的能力，针对可预定义、可重复执行的的分析和处置操作建立安全预案和安全剧本，通过自动化编排引擎来提升安全运行人员的工作效率。

此外，在面向能力支撑的五大任务中，实战化安全运行能力建设任务首当其冲。奇安信认为，数字化时期的威胁瞬息万变，按次开展的安全检查与测评模式无法达到业务安全保障要求。该任务要建立实战化的安全运行体系，全面涵盖安全团队、安全运行流程、安全操作规程、安全运行支撑平台和安全工具等，并持续地评估、优化，持续提升安全运行成熟度，以达成对信息系统的持久性防护，保障业务运营。

图 4：新一代网络安全框架规划的十大工程、五大任务



十大工程、五大任务

资料来源：奇安信集团

奇安信SOAR在全局态势感知与实战化安全运行能力建设任务中扮演了重要的角色。依托SOAR的开放式架构和对安全能力的编排，将安全团队、安全运行流程与操作规程、各类安全运行技术与工具整合到一起，增强了人防与技防的融合，并通过自动化和智能化提升安全运行的效果和效率，进而提升整体安全运行体系的成熟度。

5. 结论

借助安全编排与自动化解决方案，能够帮助企业和组织将繁杂的安全运行（尤其是安全响应）过程梳理为任务和剧本，将分散的安全工具与功能转化为可编程的应用和动作，然后借助编排和自动化技术，将团队、工具和流程的高度协同起来，从而有力支撑起实战化安全运行能力的建设。

SOAR重点帮助企业和组织解决安全运行响应人员匮乏、安全告警多、安全事件响应不及时、重复性运维工作多、安全设备之间缺乏协同且联动性差等。导致安全运行人员工作压力大、运行效率低下、运行效果难以度量的问题。

以编排为核心，充分地使用自动化技术手段，将人、技术和流程协同起来，并应用到防护、检测与响应的每个环节，实现闭环，提升效率，是未来安全运行能力的关键组成部分。

安全运行正迎来SOAR时代，你准备好了吗？

资料来源：奇安信集团

Gartner 的调研报告

确保您组织成熟到可以接受SOAR

只有在安全运营流程中具备适当等级准备的组织才能借助安全编排、自动化和响应工具集，提升安全流程效率。安全和风险管理负责人必须准备充足，确保从此类工具集中获取价值。

主要挑战

- 如不进行大规模定制，则无法使用众多 SOAR 工具所提供的有效即用型剧本、场景和集成。
- 如果最终用户试图在未完善内部安全运营流程的情况下集成 SOAR 工具来提高效率，就会白白浪费宝贵的安全预算资源。
- 一定程度而言，由于缺乏意识，SOAR 用户通常未能充分利用整套功能，而是仅使用了：安全自动化和编排、威胁情报平台/事件响应平台。
- 安全团队通常缺乏充足的内部开发技能组合，因而无法正确执行复杂的剧本或应对缺少的集成功能。
- 与自动化生产线不同，SOAR 并非核心角色的替代选项，而是以逐项任务为基础的效率推动因素。

建议

安全和风险管理负责人考虑采购 SOAR 解决方案来改进安全运营时，应采取以下举措：

- 评估当前安全运营中效率较低但行之有效的内部流程，以此评定此类流程的自动化能否通过 SOAR 工具实现明确规定的效益。
- 仔细制定符合内部流程的自动化需求，从而确保在就 SOAR 工具的使用纳入 MSSP 时，任何执行都能为内部流程带来效益，而不仅仅是使提供商更轻松地交付。
- 通过审核所有可能符合资格的流程，让整个安全团队参与是否引入并执行 SOAR 工具的决策，从而确定适合的自动化候选方案。
- 与内部开发团队合作，或确定团队内所需的编程技能组合，从而确保充分利用 SOAR 产品。

介绍

自 2017 年底开始，市场中就涌现出了标榜为安全编排、自动化和响应 (SOAR) 的一些特定产品，其中大部分着重于如何使安全检测功能效果更佳、效率更高。在此类解决方案中，大部分解决方案的关键卖点是直接提供能自动修复问题的功能，无需在流程循环中引入人工主导的分析任务。然而，要成功执行此类功能，事实远非简单二字能够形容。此类功能的范围被过分夸大，全面自动化安全响应也尚属神话。此项研究可帮助安全和风险管理负责人确定其是否适合实施 SOAR 技术，并且以合理且实际的方式更有效地为此进行准备。

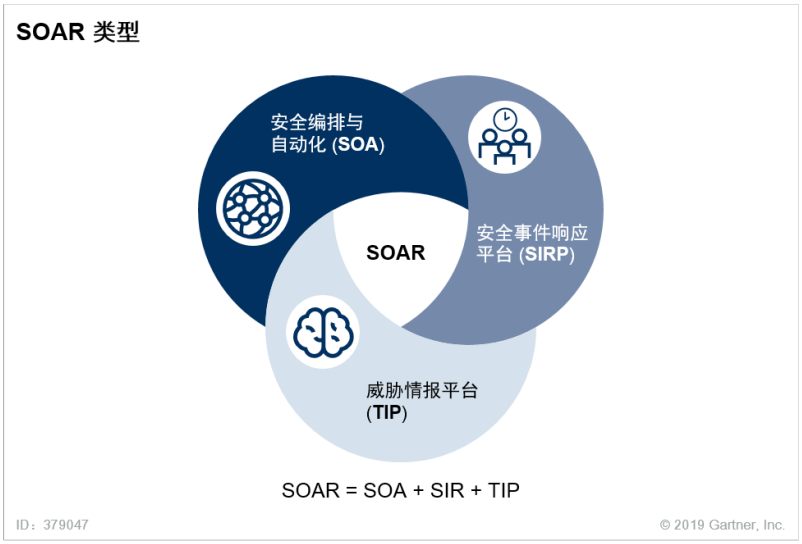
SOAR 常被误认为是“万能药”：实施后即可将报警功能连接到防护工具集，例如防火墙、入侵检测和防御系统 (IDPS)，以及端点保护平台 (EPP)。但事实恰恰相反，SOAR 技术的功能是帮助组织收集受安全运营团队监控的输入信息（例如报警），以及部分实现事件分析和分类流程的自动化。这些功能旨在根据预定义的工作流，帮助定义标准化事件响应活动、为其设置优先级并驱动这些活动。

因此，SOAR 包含以下功能：

- 安全信息自动化处理。（安全数据自动化处理可包括安全信息和事件管理 [SIEM] 报警或威胁情报。）
- 工作流元素编排，其中涉及数据收集、批准和其他基于审计的标识。
- 对响应程序或操作的补充实施或支持（参见图 1）。

组织和流程成熟度是成功实施 SOAR 技术的对于想要购买 SOAR 技术的组织而言，主要考虑事项如下：

图 1. SOAR 构成要素



资料来源：Gartner（2019 年 3 月）

- 是否有想要使之更有效或实现自动化的可靠安全流程?

- 现有的安全技术和订阅能否通过 API 与第三方工具集很好地集成?

SOAR 市场中的解决方案仍然处于新兴阶段。因此，预计那些拥有可靠的现有流程和良好结构的安全运营中心 (SOC) 环境的组织，会在实施 SOAR 产品并从中受益方面取得最大程度的成功。

随着数字世界越来越复杂，自携电子设备 (BYOD)、物联网 (IoT) 和云计算等领域都呈现出了高度规模化、高度动态的特点，并且超出了传统的以安全为导向的控制形式。这就导致缺乏可见性并且无法执行策略。这种复杂性也在组织中造成了技能差距；大部分组织尝试利用自动化程度更高、更智能的技术来填补这一差距。对大部分组织而言，减少安全运营的复杂性是其主要目标。实现流程自动化本身是一项复杂的工作，并且要成功实现这一目标还会遭遇众多阻碍，因为目前还没有现成的解决方案能满足各组织可能拥有的所有定制的安全自动化需求。

大部分 SOAR 产品都只有一个核心重点和一些附加益处。此核心重点通常为以下三大类别之一:

- **工作流**: 市场上的大部分产品都旨在简化安全事件管理流程、改进变更授权，或将工单正确分类并分配到正确区域。它们还确保在预定义的时间范围内，以一致的细化等级解决问题。

- **扩充**: 无论是在事件识别之后，还是在数据收集和处理过程中，SOAR 解决方案都能帮助集成外部威胁情报、执行内部环境查找或运行流程来进一步收集有关问题的数据。

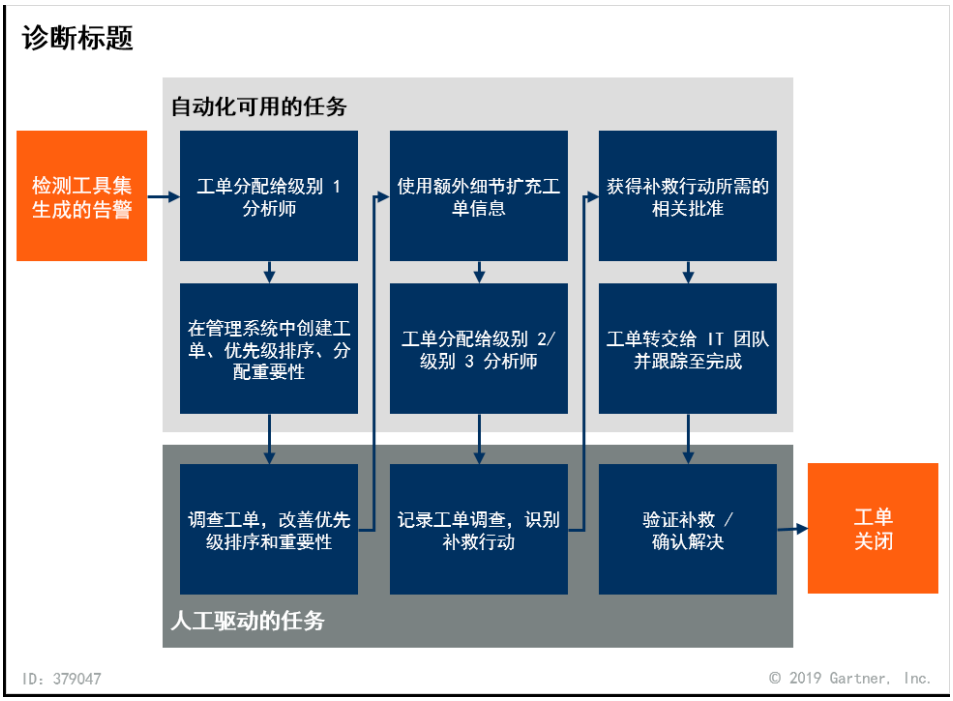
- **响应**: 自动化响应可通过对组织内 IT 资产的安全技术应用某种形式的执行措施，从而对常见问题提供“无需分析”的解决方法。部分方法可能会锁定用户，而其他方法则会对邮件网关应用变更。此功能最具成效却也最为复杂，并且很少仅针对一两个不重要的使用案例执行此功能。

可应对上述三种主要场景类型的随附即用型剧本并非专为您组织解决问题而设计。这些剧本并不会考虑您特定的内部流程、技术集成要求或业务关键型需求。安全和风险管理负责人在考虑这些技术时，也要预期未来需要对即用型功能进行定制。与产品捆绑的功能十分重要，因为该功能有助于增加与内部流程的适用性 (参见图 2)。其还有助于差距分析，从而确定负责人需要 SOAR 提供何种帮助，以及需要从头开始进行何种开发。

SOAR 平台的确能免去由现有员工执行日常重复任务的需求。不过，这些任务 (以及用于确保任务一致性的支持文档) 应具有一定的细化程度，以便它们能在经过调整纳入自动化元素，这一点十分关键。这种方法几乎肯定会减少员工的工作量，但通常也只会为这些员工创造空间，使其适应自己的角色并且执行更多的安全运营功能。与自动化生产线不同，SOAR 并非核心角色的替代选项，而是以逐项任务为基础的效率推动因素。

理解作为安全运营的一部分而执行或需要的流程和任务十分重要，即使这些角色尚未划分时，也是如此。无论是否利用 SOAR 这样的技术，安全自动化都面临着重重挑战。但是，如果执行安全功能需要先完成大量的任务，那么自动化则是以后唯一一个实际的解决办法。自动化能让工作流程更便捷，并且能为专

图 2. 工作流驱动型简单流程和潜在自动化益处示例



资料来源: Gartner (2019 年 3 月)

注于基本职能留出空间。尚未迈向自动化的组织会很快发现，其无法从自己现有的安全投资和尚未进行的未来投资中获得有效价值。

分析

审查内部安全运营流程来识别益处

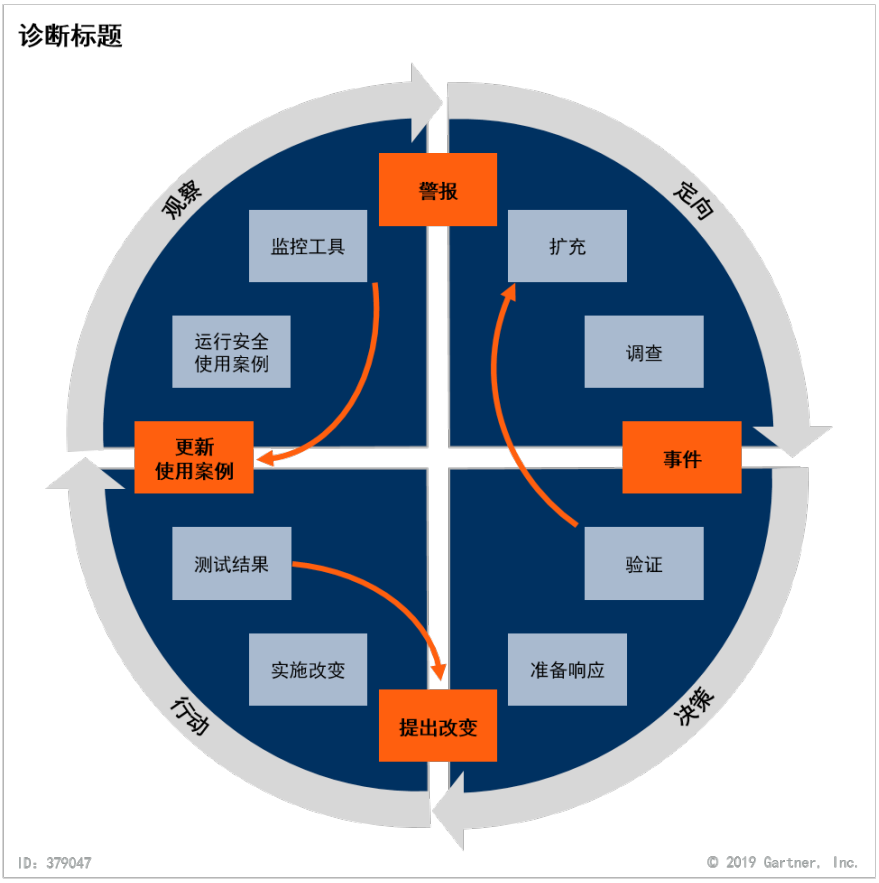
虽然 SOAR 产品确实能提供诸多优势，但 SOAR 本身并非人力的替代选项。SOAR 的关键词是编排，这也是在使用自动化和响应之前必须构建的关键部件。就定义而言，编排是指安排或操控，尤其是以明智或周密的计划或策略进行安排或操控。就像乐队指挥必须协调编排乐队才能奏出乐曲一样，安全运营团队必须计划、安排并决定如何响应不同类型的安全事件才能得到想要的结果。

希望在环境中纳入 SOAR 平台的安全运营团队必须拥有定义明确的内部流程，才能开始使用 SOAR 平台。构建这些内部流程则需要内部员工具备相应技能，而这无法在平台上购买。待编排的每个事件类型都需要人工分析，从而确定对于业务风险容忍度而言最合理的后续步骤，或者确定接收事件上报的合适团队。每个事件都应遵循流程来建立适合特定事件的编排，通常称为剧本（参见图 3）。可构建自动化来加快重复流程和/或响应事件。在定义流程时，安全运营通常使用观察、定向、决策和行动 (OODA) 循环。应以同样的方式使用 SOAR 工具来增强此框架：

- **观察**事件并确定发生了什么。
- **定向**观察结果，并添加环境来确定观察结果的含义。
- **决策**出适当的响应措施（基于业务风险容忍度和能力）。
- **行动**以决策为基础，将所学知识应用于观察过程并重复执行。

需要 SOAR 进行增强的技能完全对应于安全运营团队成员具备的能力和进行的训练（其目的通常为实现更有效地识别、跟踪和解决安全问题）。SOAR 技术能帮助安全运营团队更快地从决策点 A 前进到决策点 B，但其过程以及如何在过程中进行决策是需要人类互动的技能。这同样适用于响应措施。SOAR 产品中定义明确的剧本能创造更有效的决策达成速度。然而，对于如何响应事件的决策需要先由内部安全运营团队和更大的组织部门同意。这些针对响应方式作出的决策由环境中事件所处的环境、业务风险容忍度和安全运营外的其他团队的响应能力（如必要）所驱动。因此，我们只能将 SOAR 应用于我们预期发生的以及已知晓响应方式的事件和场景。一些供应商可针对特定使用案例提供预定义剧本，这些剧本可以“拖放”到响应场景中；也有供应商可提供相应服务，能帮助在其工具中构建剧本。这些功能和服务对于应对构建整体编排和响应措施方面的挑战而言可能很有用，但是这并不是维护 SOAR 平台的长期解决方案。

图 3. 涉及 OODA 的 SOC 检测流程



资料来源：Gartner（2019 年 3 月）

编排和自动化对安全运营团队十分具有吸引力，但认为基于自动化的供应商产品能在不定制的情况下有效运行，这显然是错误的。在完全理解并准备好您的内部流程之前，切勿在 SOAR 产品上浪费资金和精力。正如介绍部所述，仅仅是确定安全运营团队应如何运作就需要投入大量的时间和资源。因此，请注意，对不完善的流程进行自动化只会更快地破坏流程，而成熟的运营流程可以让安全运营团队做好更充分的准备来使用 SOAR 技术。安全和风险管理负责人必须确保在这方面的工作中恪尽职守。对小型运营团队而言，即便是构建几个剧本也可以成为采用和发现 SOAR 平台效率的重要催化剂。

除了需要花费时间来构建内部流程，内部团队成员往往还需要具备编码和脚本编写方面的特定技能组合，才能使用 SOAR 平台。需要这些技能的原因是，尽管不同组织对特定类型的安全事件响应方式存在一定共性，但组织之间的构建并非完全相同。这意味着，为了构建自动化行动或剧本来编排事件，安全运营团队需要在 SOAR 平台上定制和维护每一个使用案例。除了维护剧本和响应，维护用于将各种安全工具（例如，SIEM、端点检测与分析 [EDR]、下一代防火墙 [NGFW] 以及用户和实体行为分析 [UEBA]）连接到 SOAR 平台的 API 连接也需要大量工作。如果内部流程和平台要求都需要团队成员具有特定技能组合，那么为了有效地利用 SOAR，SRM 负责人则必须确定并准备好应对挑战。

确保使用 MSSP 时组织能够受益于 SOAR

SOAR 一词经常出现在受管安全服务提供商 (MSSP) 主导型服务的语境中，而且 MSSP 有完善的安全运营流程。因此，他们应该能够很好地利用 SOAR 平台执行各种各样的任务，提升他们以更快更丰富的方式为客户提供服务的能力。这对 MSSP 和客户端都有益，因而十分实用。

了解使用 SOAR 平台的供应商的含义非常重要，例如：

- 自动化应促使供应商将一组更具可定制性但详细且一致的输出集作为其标准产品的一部分。
- 供应商应该能够更迅速地提供一些事件详情，以便您更快采取补救措施。
- 在某些情况下，根据对您组织内的预防措施的控制程度，供应商会报告结果，而非提出问题或进行互动。
- 如果 MSSP 提供自动响应，则应提供扩展到补救和响应活动的 SLA，并衡量所执行操作的及时性和准确性。

“SOAR 即服务”的价值尚未在市场上体现出来

在受管服务市场的供应商中试用过一个术语“SOAR 即服务”（SOAR as a service，SOARaaS），意即受管 SOAR。此类服务的价值在于，它们与技术集成和流程驱动型咨询服务（而非情报驱动型受管服务）更加契合。显而易见的是，如果有较高程度的自动化来控制处理、决策和结果，那么除了最初的实施和简单的设备维护外，几乎不需要管理或专业知识。这种小规模互动可能表示以独立方式使用 SOAR 技术会更有效，即只需使用咨询便可有效地实施该技术。运营支出 (opex) 驱动型服务通常不会按所需的频率或细节来增加价值，并且与传统 MSSP 通常提供的杠杆化、商品化受管服务不一致。

安全和风险管理负责人应谨慎对待 MSSP 提供的自动化驱动型服务。此类服务的价值源于技术的正确实施，而此类服务的输出结果仍然需大量解释才能产生价值。受管服务空间内的自动化功能仍然很不成熟，正如直接供应商解决方案一样。您必须确定，服务在可操作和可用的通信方面将提供的内容与实现所需结果的内部需求之间的差距。明智的做法是，明确在组织内使用咨询机构建立技术与根据运营支出利用受管服务提供商进行同样操作之间的差异。当然，只要利益、计划条款和结果得到恰当理解和同意，长期支持和管理以及将资本支出 (capex) 转为运营支出的能力就很有价值。

在确定 SOAR 要求范围时让整个安全组织参与其中

在处理来自安全工具集的警报时，自动化和编排的要求远远超出了简单的流程驱动型功能。组织不能只关注简单地将新技术插入 SIEM，还要与更广泛的安全

社区（从编写和实施安全策略之人到履行补丁管理职能之人）互动。如果您侧重任务自动化或减少人员配置开销，则需要提供与使用人员配置时所耗费时间相同或更大的时间节省量。例如，要花费 100,000 美元，而一个工时要花费 200 美元，您便需要找到相当于约 500 小时或约 12.5 周工作的任务来证明该投资的价值。为了更好地量化投资，您不妨问问自己如下问题：

- 任务/流程的效率会提高多少？
- 需要多大规模的团队来实现效率？
- 实施 SOAR 后需要倚重哪些指标？

SOAR 是一个具有内置用例的相当通用的框架解决方案。有必要考虑到这样的情况，虽然组织内部围绕调查、预防或补救安全问题的想法是相对通用的，但这些工具的工作环境对您来说应该具有特殊性。它们无法直接解释企业 IT、内部流程、合规要求或文化和地理需求的细微差别。您在 SOAR 方面的投资不仅仅是与技术相关的价格标签。这也是员工配置和维护该配置的时间，以及有效地进行配置所需的技能要求和安全知识的成本。某些流程的元素需要基于业务的决策，而 SOAR 工具无法应用这些元素。有许多可以自动化的辅助任务，这些任务不一定存在于安全团队的职责范围内，但是可以利用安全工具收集的数据并从中受益。表 1 提供了安全领域之外的 SOAR 工具可能会有所帮助的一些高级别示例。

表 1. 可能受益于 SOAR 的非安全专用内部职能示例

部门	需求
治理风险与合规团队	与履行业务和合同义务所需的关键标准相关的定期报告和审计，这些标准包括 PCI、《健康保险携带和责任法案》(HIPAA) 以及国际标准化组织 (ISO) 的相关标准。
身份和访问管理团队	定期报告、控制以及用户访问审核和管理。与内部流程和标准保持一致。
IT 支持职能	故障排除、数据扩充、使用情况报告、与管理用户帐户相关的一般操作流程。更改管理授权。
人力资源职能	员工入职和离职及其用户数据和帐户，以及纪律调查

资料来源：Gartner（2019 年 3 月）

许多工具集中已经存在 SOAR 功能

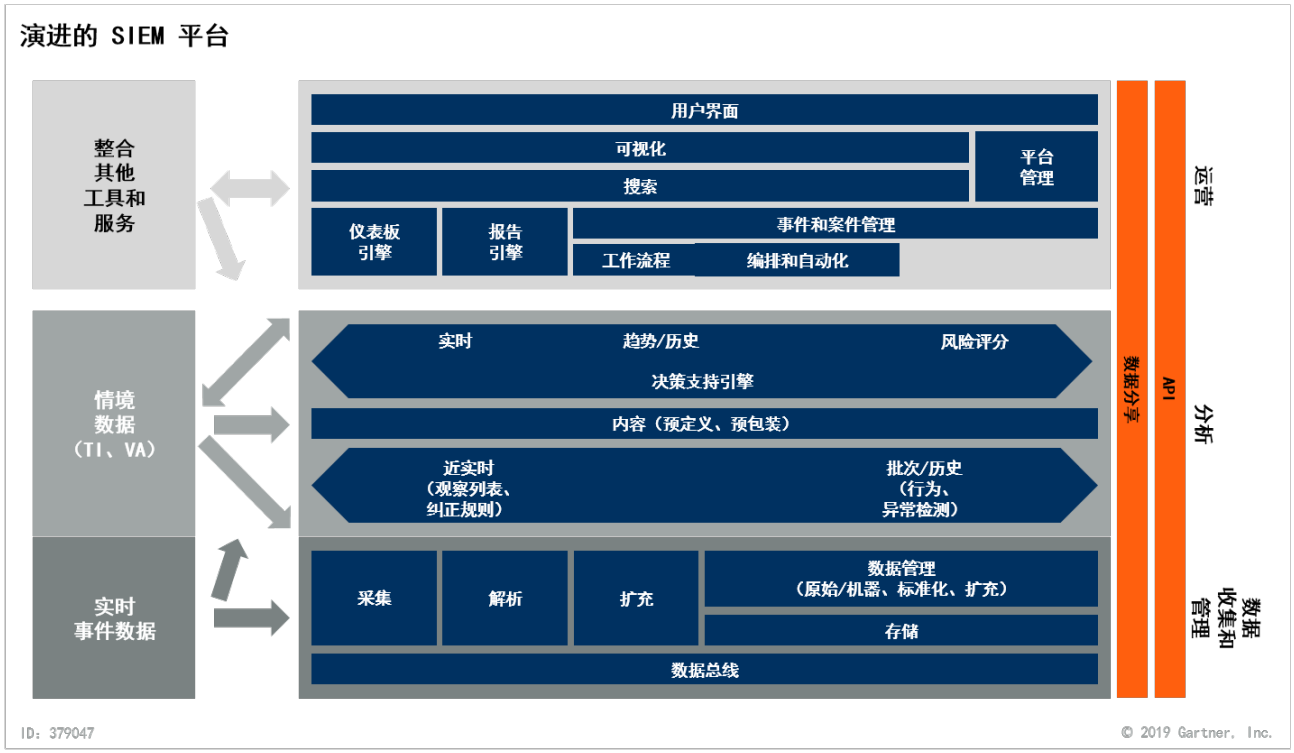
随着安全技术的发展，自动化功能显然正与安全专业人员已经投入的工具集直接协调一致。示例包括已成为统一威胁管理 (UTM) 的工具集的组合，或 SIEM 产品中包含的附加特性和功能的组合，以便实现直接响应或与其他产品（如端点保护）集成。在自动化方面，组织需要考虑是否已经满足了自动化需求，部分原因是已经存在相应功能。在考虑现有工具集是否具有此方面的功能时，需要考察三个方面：

- 技术供应商是否对小众的或主流的 SOAR 供应商进行了任何关键性收购？
- 已经投资的技术供应商与其他供应商解决方案之间存在哪些专门的技术联盟伙伴关系？
- 所需功能是否以原生方式存在于产品集中并且未得到充分利用？

SIEM 便是很好的例子：其中已经存在一定程度的自动化、与第三方技术供应商的集成以及工作流自动化。有些例子仅存在于简单的形式中；而存在于在这些领域进行了广泛投资的组织中的其他例子，可能已经比独立的 SOAR 产品更加成熟。这是一个已经并将继续快速发展的领域（参见图 3），因为其用户社区所消耗的数据量可能非常高。早在 SOAR 出现之前，“误报减少”“自动响应”和“案例管理”等术语便已存在。

已管理企业 IT 部分工作流功能的工具集，也是预购技术资产中已经存在的自动化功能的来源。该功能可能是固有的，也可能是作为额外的可购买模块提供的。在某些情况下，可能需要利用产品现有的 API 框架或允许扩展的特定自定义开发功能在内部进行开发。

图 4. 实例：SIEM 平台的演变



资料来源：Gartner（2019 年 3 月）

确保组织拥有可以有效利用 SOAR 的恰当开发技能组合

值得注意的是，并非所有安全工具集都考虑了其他供应商产品和解决方案，它们必须与之一起使用才能提供全面的安全保护和认识。在没有任何自动化手段的情况下有效地操作如此广泛的工具所需的努力，使许多组织只有能力以有效和有价值的方式利用其中的一些工具。在考虑互补安全工具集的跨功能价值时，可能根本不支持将它们与 SOAR 工具集一起使用或将自动化功能与其集成在一起。

这种兼容性通常是安全技术供应商与 SOAR 技术供应商之间关系的一种作用，如果无法获得更广泛的兼容性，则不太可能存在这种关系。因此，有必要考虑您的现有安全技术对于第三方接口的开放性，检查这些技术是否对 API 功能有文档，这是一项有效指标。安全和风险管理负责人还应该考虑到，此要求对于利用在线资源、开放论坛和开源开发库的广大社区来说有多普遍。这是为了理解您需要的（针对所需流程增强的特定元素的）特定功能/集成随时可用的可能性。

在许多情况下，您所需的 SOAR 工具集的特定功能将不能作为标准提供。即用型剧本中可能包含一些元素，或者作为现有例程和功能一部分的元素，可以用来提高开发效率。因此，功能上并非不可能实现，但可能会变更加复杂。安全和风险管理负责人应考虑开发所需功能的内部技能组合的可用性，以及可能增加拥有 SOAR 工具集总成本的时间和成本。许多 SOAR 工具集具有内置开发环境和大量文档来支持可能需要的开发，这种情况并不少见；事实上，如果存在，这便是指示 SOAR 工具的功能和兼容性的好

迹象。即便此类文档非常丰富，并且与当前工具集的集成已经存在，组织也需要有能够支持使用 Python 和 Java 等语言进行开发的人员，才能获得工具集的流动性和真正益处。

明白大多数 SOAR 产品附带的内容并不是为了满足组织可能需要的特定用例而设计，这一点非常重要。此类内容通常包含一组简单的可自定义的高级别工作流或剧本。这些项目旨在演示概念并支持初始开发工作，确保平台尽早开始显示价值。在某些情况下，它们为运营和开发团队集成其特定用例提供了必要的构建基块。常见情况是，安全团队仍然主要依赖手动创建和维护的基于文档的运营流程，以及陈旧程序和“部落文化”。这属于积极现象，因为它确保此类程序得到充分理解、可以更新，并且运行安全操作所需的知识更容易获得，从而将其转移到通用介质中。

与实施和配置 SOAR 工具集相关的交付周期通常很长，常常超过三个月，并且可以将时间范围延长到大约 12 个月，有时甚至超过 12 个月。为了启动并运行工具集，供应商或其合作伙伴可能会提供广泛的咨询意见。此阶段的核心考虑因素应该是工具集的未来开发和调整。这也适用于与现有（以及未来可能有的）安全工具集的维护和兼容性相关的日常开销，这些工具集可能会在日后用于取代现有的基础结构。

资料来源：Gartner Research，G00 379047，Pete Shoard，Ryan Benson，2019 年 3 月 27 日。

奇安信集团介绍

奇安信科技集团股份有限公司（以下简称**奇安信**，股票代码688561）成立于2014年，专注于网络空间安全市场，为向政府、企业用户提供新一代企业级网络安全产品和服务。凭借持续的研发创新和以实战攻防为核心的安全能力，已发展成为国内领先的基于大数据、人工智能和安全运营技术的网络安全供应商。同时，**奇安信**是2022年冬奥会和冬残奥会网络安全服务与杀毒软件的官方赞助商；此外，公司已在印度尼西亚、新加坡、加拿大、中国香港等国家和地区开展网络安全业务。

奇安信面向新型基础设施建设、面向数字化业务，运用系统工程的方法论，结合“内生安全”思想，将新一代网络安全框架作为顶层设计指导，以“数据驱动安全”为技术理念、以打造网络安全颠覆性和非对称性能力为目标、以“人+机器”协同运营为手段，创建了面向万物互联时代的网络安全协同联动防御体系。奇安信拥有完备的网络安全产品和创新的网络安全服务，完善的研发、采购、生产和销售模式。针对云计算、大数据、物联网、移动互联网、工业互联网和5G等新技术下产生的新业态、新业务和新场景，为政府与企业等用户提供全面、有效的网络安全解决方案。

近年来奇安信以高投入研发下的技术创新为引领，特别针对云计算、大数据、移动互联网、工业互联网、物联网等新技术运用下产生的新业态、新场景，为政府与企业等机构客户提供全面有效的网络安全解决方案，率先提出并成功实践“数据驱动安全”“44333”“内生安全”等先进的安全理念，推出了“天狗”系列第三代安全引擎，零信任、“天眼”等创新的安全产品，并于2020年发布面向新基建的新一代网络安全框架，此框架下的"十大工程五大任务"，可以适用于各个应用场景，能指导不同的行业输出符合其业务特点的网络安全架构。

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

奇安信重点涵盖了网络安全行业多个前沿领域，包括建设云和大数据安全防护与管理运营中心、物联网安全防护与管理系统、工业互联网安全服务中心、安全服务化项目、基于“零信任”的动态可信访问控制平台，以及网络空间测绘与安全态势感知平台。其中，工业互联网安全服务中心将构建全国性的三级工业互联网安全服务中心体系，为4000家以上工业互联网企业及工业关键基础设施建立安全管理中心，提供工业安全防护、监测、安全托管服务；针对目前市场上云安全和大数据安全的有效防护产品和方案稀缺的现状，**奇安信**的云和大数据安全防护与管理运营中心项目将通过构建能力平台、产品体系和服务中心三部分，全面提升奇安信全方位安全防护的服务能力。