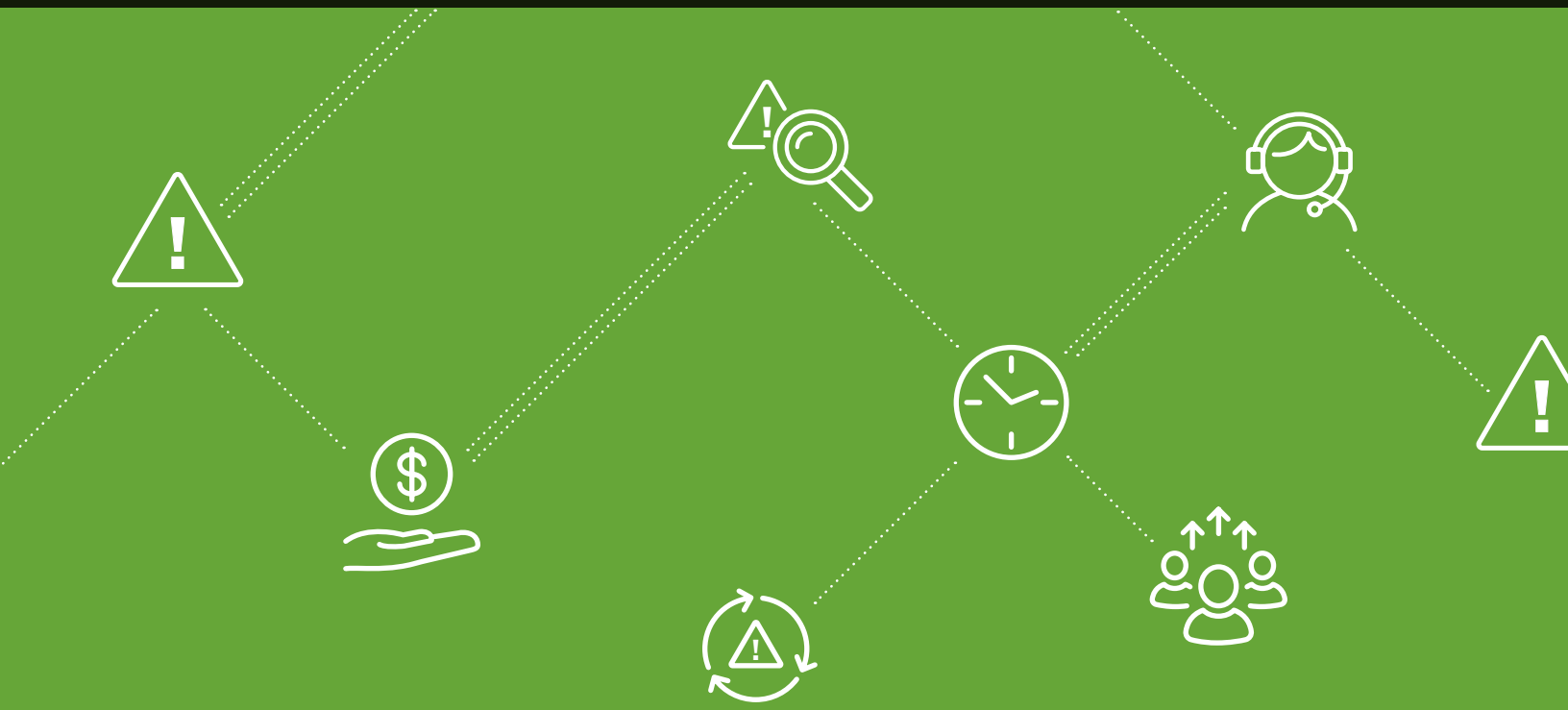
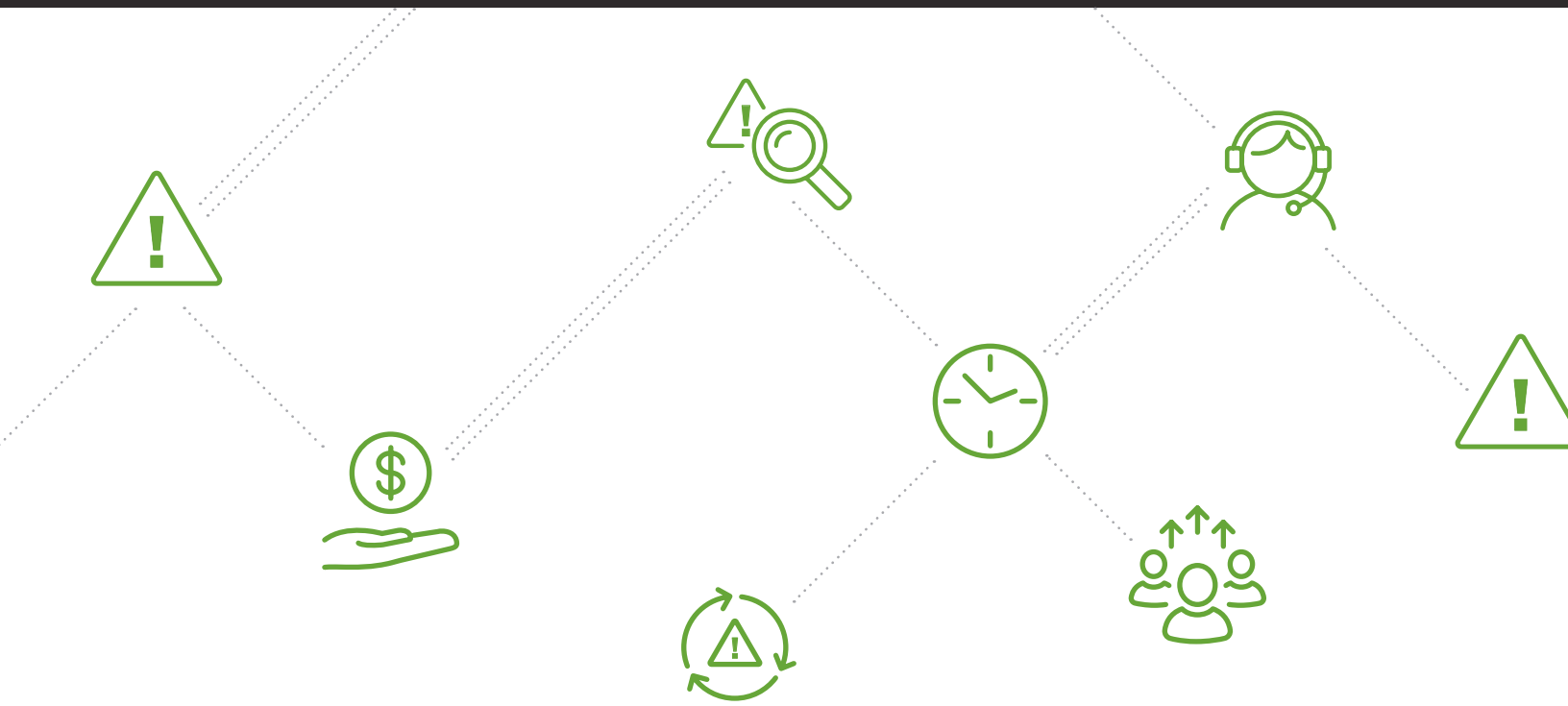


SOAR 买方指南

购买安全编排、自动化和响应解决方案的人员、内容、地点、时间和原因

目录



1.简介

投资安全编排、自动化和响应 (SOAR) 平台是一个明智和具有高度战略意义的决策。毕竟，选择该平台来构建您的安全运营中心 (SOC)，可能比选择任何单点安全产品更重要。您选择的 SOAR 平台将成为安全基础架构的核心部分，有效地充当安全投资的操作系统。

本指南旨在概述评估 **SOAR** 平台时应考虑的重要标准。

定义安全编排、自动化和响应

尽管自动化在其他软件领域已经流行多年，包括销售人员自动化、营销自动化、人力资源自动化和 IT 自动化，但安全团队刚刚开始意识到自动化和编排的好处。这一发现反过来又推动了买家对 SOAR 平台的兴趣。因此，许多安全供应商正转向 SOAR 类别以获取品牌影响力份额；使用他们在相邻细分市场推出的现有产品。遗憾的是，随着对 SOAR 细分市场的大肆宣传，观点不同的供应商数量日益增加，他们模糊了市场定义，使得难以对产品进行比较。

为了清楚起见，我们提出以下定义：

安全编排
安全编排是复杂基础架构中一系列相互依赖的安全操作根据机器进行的编排。

安全自动化
安全自动化是基于机器执行安全操作。

安全响应
安全响应是基于策略的事件、案例和事件工作流的人工和机器活动协调。

我们将在本指南中使用这些定义来进一步研究哪些功能、属性和考虑因素共同构成一流的 SOAR 平台。

识别安全使用案例

团队通常会识别安全使用案例，以便在 SOAR 平台上实施。使用案例按照现有的手动工作流进行建模，通常代表了它们最大的操作难点。工作流通常包含许多手动任务，需要跨多个产品工作才能完成。

除了痛点之外，在开始评估之前，列出所有潜在的使用案例也很重要。这项工作应该让安全运营团队中的主要利益相关者参与进来。识别全面的使用案例，即使它们没有立即实施，对于确保今天选择的平台也能支持未来的需求非常重要。

以下是一系列安全使用案例，涵盖调查、改进、遏制和补救类别：

警报分类
警报分类的目标是验证传入的警报并确定其优先级。专注于分类传入的警报的使用案例包括使用额外的上下文丰富事件。它们还可能包括逻辑，以消除进一步处理中置信度非常高的误报。

事件响应
事件响应使用案例可能因事件类型而有很大差异。例如，应对网络钓鱼企图事件与应对成功的跨软件攻击有很大不同。

攻击指示器 (IOC) 搜寻
通过自动化 IOC 搜寻，团队可以充分利用他们收到的威胁情报，而不是因为资源限制而限制他们搜索的 IOC。他们也可以实施情报评分来帮助决定使用哪些威胁情报来源。

漏洞管理
实现漏洞识别、分类、补救和缓解周期的自动化后，不仅提高了团队效率，而且能够确保每次都以相同的方式执行该过程，从而获得更一致的结果。

网络访问控制 **(NAC)**
SOAR 平台可以增强动态访问控制策略。一个例子是集成以前不属于 NAC 决策逻辑的检测系统。

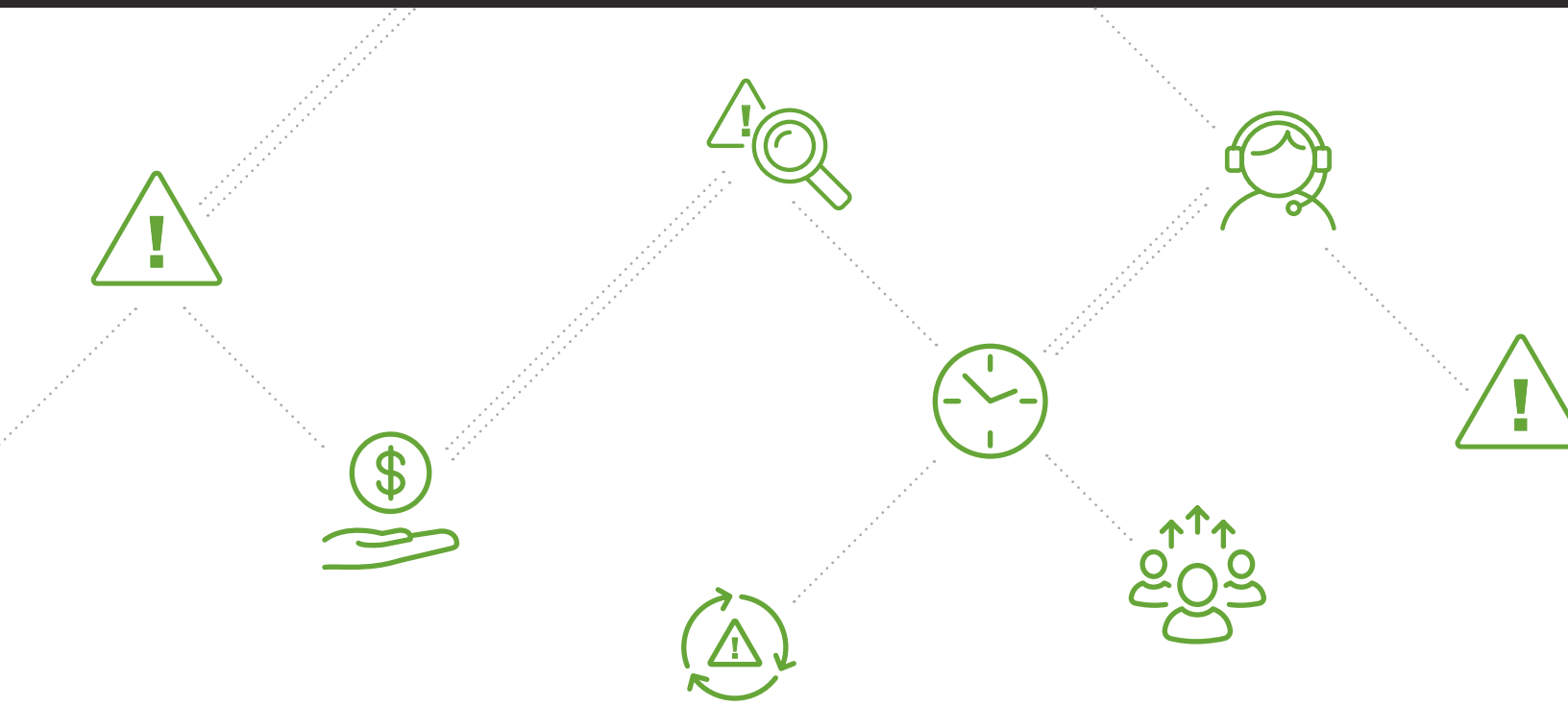
用户管理
确保准确、快速和系统地启用和禁用用户，可以消除实施威胁的行为者恶意使用用户账户的可能性。

渗透测试
资产发现、分类和目标优先级排序等活动可以自动化，从而提高渗透测试团队的生产力。

情报共享
拥有情报共享计划的组织可以从自动化辅助行动手册中获益匪浅。自动化还可以提高分析师的工作效率，并以比手动流程更快的速度向社区提供对时间敏感的信息。

其他使用案例

其他自动化使用案例候选来自众所周知的场景，在这些场景中，安全操作团队可以编纂标准，用于自动做出决策和采取适当的行动。



2.评估标准

我们建议将 SOAR 评估标准至少分成三个部分：核心能力、平台属性和业务考虑。核心能力通常是功能性的，在平台中很容易识别。平台属性更微妙，例如架构特征，它们形成了影响平台选择的标准。业务考虑涉及产品的方方面面，包括公司提供的增值服务，以增强其核心技术，例如培训和支持。

核心能力

核心能力可以被视为 SOAR 平台的基本组成部分。我们将列举每个能力或组件，并提供一些考虑来帮助评估和选择。

编排程序

编排程序应从头到尾指导和监督与给定安全场景相关的所有活动。在所有情况下，编排程序都必须始终如一地提供可预测的结果和可用资源的最佳利用。

数据摄取

安全自动化和编排从安全数据摄取开始。编排程序应该能够接收来自任何数据源和任何格式的安全数据。它应能够接收推送至平台的数据，并且必须能够轮询数据源并将数据拉入平台。如果接收了非结构化数据，编排程序应允许用户提供数据处理程序来解释数据，并使其可被 SOAR 平台使用。编排程序还应能够摄取来自多个来源的数据，并且可以选择保持摄取的数据在逻辑上分离。

决策

用户应能够选择应用于数据源的自动化行动手册。例如，电子邮件钓鱼行动手册可以应用于基于电子邮件的摄取源，而恶意软件调查行动手册可以应用于 SIEM 警报摄取源。该决策步骤与警报管理能力密切相关，这将在后面描述。

任务执行

编排程序的角色通常是在适当和最佳的时间从队列中分派自动化任务，并将它们传递给自动化引擎执行。

人为监督

编排程序应有效地平衡基于机器的自动化和必要的人为监督。有三种常见的情况需要分析师：当需要资产所有者批准对目标执行安全操作时，当需要分析师审查以确保安全与业务连续性平衡时，以及当分析师需要扩充成文决策逻辑时（例如，当发生错误时）。

数据管理

编排程序还应确保来自一个操作的输出数据被正确地解析、规范化和结构化，以便将来的操作可以利用它。编排程序还应支持在需要时缓存相关数据，以避免对其他资源造成负担。

容错

SOAR 平台定期与许多独立的产品和服务交互，以执行自动化行动手册。编排程序必须预计到，产品和服务的可用性并不总是得到保证。对外部服务的访问可能会中断。在这些情况下，编排程序应按照配置正常地执行可预测的恢复操作。

自动化引擎

自动化引擎是大多数 SOAR 平台的工作工具，从编排程序接收操作或任务，并可靠地执行它们。因为自动化任务是独立运行的，很大程度上不需要人工交互，所以平台的可伸缩性和可扩展性等属性是需要考虑的重要标准。

可伸缩性

了解自动化引擎将如何垂直和水平扩展非常重要。预计随着时间的推移，用户将自动化更多的使用案例。每增加一个使用案例，自动化引擎就会有额外的处理负载。 自动化引擎的设计应允许垂直扩展（例如增加 CPU 和 RAM 资源）和水平扩展（例如增加服务器实例），以提高性能并保护自动化投资回报（ROI）。

可扩展性

安全性发展很快，因此自动化引擎应该支持新的功能，而无需进行重大的重新设计。自动化引擎应支持适应其环境独特功能的能力。

警报管理

正如前面所讨论的，就在数据摄取之后，SOAR 平台中的警报管理功能应该排队并排定入站警报的优先级，以帮助分析师更高效地执行分类。可以使用手动或自动执行操作来执行警报调查，以产生最高级别的分流生产率和准确性。警报管理功能的界面应该以这样的方式构建，使得安全警报的所有方面能够被快速使用并有效地采取行动。界面还应以在正确时间显示正确信息的方式来安排信息，这避免了导致分析师在上下文之间进行大量搜索或切换。

警报详细信息

安全警报技术属性的组织方式应允许分析师快速领悟它们以理解安全场景。这包括有组织的数据视图，例如：IP 地址、域名、文件哈希、用户名、电子邮件地址和所有其他相关数据字段。使用标准格式，例如公共事件格式（CEF）或等效格式对数据交换非常有益。

发布行动

在调查警报时，安全分析师应能够向使用警报数据的平台发布手动操作。这包括调查、遏制、纠正或一般性操作。界面应该允许用户通过选择要操作的数据来执行操作。这种行为有时被称为上下文操作执行，能够围绕新发现的信息进行枢转分析。

与手动操作执行一样，分析师还应能够针对警报发布一系列操作。该操作集合通常被称为行动手册。

操作结果

当针对警报采取手动或自动操作时，结果不仅对分析师是可见的和有意义的，而且对可能使用操作结果做出自动决策的 SOAR 平台来说也是有意义的。操作结果应该以摘要格式（例如表格视图）以及更全面的格式（例如 JSON）提供。

活动日志

该平台应提供全面的活动日志，显示针对警报执行的所有操作的记录，无论这些操作是手动启动的还是通过自动化行动手册启动的。每个操作都应显示其结果，包括操作成功或失败的指示器，以明确操作是否完全执行。

警报状态、严重性和敏感性

平台管理的每个警报都应包括状态指示器（例如新的、打开或关闭）、严重性指示器和敏感性指示器（例如交通灯协议或 TLP 称号）。每个指示器应该可以在警报管理界面以及行动手册中修改。

警报协作

该界面应该提供一个分析人员可以协作、评论和提供有关警报其他信息的区域。这是捕获和组织这种协作记录以及所有其他警报数据的理想之选。

案例管理

一旦警报或事件得到确认和上报，案例管理组件应该推动从创建到解决的更广泛的跨职能生命周期。此组件应包含案例的其他属性，以区别于警报。多个警报可能已被确认、汇总并作为单个案例上报。警报管理通常是技术性的，而案例管理通常将技术性和非技术性步骤纳入流程。最后，与警报相比，案例数量往往更少：许多组织每天都会收到数百或数千条警报，而案例数量则趋向于每天一位数。

案例数据组织

案例管理组件应汇总与案例相关的所有数据。在单个位置显示信息使用户能够有效地消费信息并避免上下文切换。

将数据添加到案例中

案例管理界面应支持将相关技术数据（例如警报的源数据和操作结果）附加到案例中。该界面还应支持附加相关的非技术数据，例如笔记、备忘录、电子邮件、截图、录音或与案例相关的任何其他任意文件。还应可以从行动手册中自动将信息附加到案例中。

将案例链接到警报

在案例调查期间，通常会发现需要额外调查的数据，或者需要立即采取遏制措施的场景。因此，如果分析师确定应该采取行动，案例管理界面应该将分析师无缝链接到相应警报的警报管理界面。从警报管理界面，可以执行额外的操作，相关数据的更改应反映在案例管理界面中。

映射到现有流程

许多组织已经为事件响应、紧急情况、灾难和其他重要情况制定了标准操作程序 (SOP)。案例管理功能应该为用户提供根据他们的流程定义阶段并将其保存为模板的能力。用户应有能力将 SOP 分解成多个阶段，每个阶段都有一个或多个任务，每个任务都可以被分配一个所有者。与任务相关联的附加上下文信息可以与任务描述结合。与任务管理应用程序非常相似，任务在由代理人完成时应该标记为已关闭。该界面应提供案例进度以及案例状态的指示。

活动审计

信息的添加或修改以及状态的改变是案例的重要细节。对案例的任何更改都应记录在审计跟踪中，并且可以导出。

对案例的更改可能包括：

- 添加数据
- 修改数据
- 修改阶段或任务
- 添加文件或注释
- 修改文件或注释
- 完成任务
- 案例的任何其他活动或修改

行动手册管理

行动手册管理有助于 SOP 的维护。理想情况下，该组件应该提供修订控制，并能够管理组织内部以及可能跨社区的行动手册形式的 SOP 联合。

行动手册组织

行动手册管理应允许对行动手册进行适当组织和分组。用户应该能够根据什么对他们的组织最有效来定义他们自己的分组。例如，您可以选择根据主题、敏感度、组织部门或资产类型来组织和分组行动手册。

批量编辑行动手册

每个行动手册的内部工作方式可能是独一无二的。然而，在管理层面上，许多行动手册具有共性。

行动手册管理系统应允许批量编辑行动手册，例如：

- 摄取来源
- 启用/禁用自动执行启用/禁用安全模式操作
- 启用/禁用增强日志记录
- 设置行动手册类别分组

修订控制和分发

强烈建议与版本控制系统（VCS）集成，例如 Git，以便大规模成功管理行动手册。在部署级别，利用 VCS 可以跨多个系统系统分发行动手册。这对于在开发系统和生产系统之间同步行动手册，或者跨多个站点的多个生产系统同步非常有用。 在开发级别，VCS 对于跟踪修订变更以及在必要时可以回滚变更非常重要。第二个好处是使开发人员能够在他们选择的编辑器中编辑行动手册，并轻松地将修改后的行动手册同步回平台。

自动化编辑器

自动化编辑器是分析师或经理将他们的流程编成自动化行动手册的地方。视觉自动化编辑器的前身是基本源代码编辑器。专门在源代码编辑器中编辑自动行动手册使得构建行动手册成为一个繁琐而困难的过程，只有相对较小的程序员群体才能完成。通过视觉自动化编辑器，所有安全专家（他们可能不具备在源代码级别编写行动手册的专家能力）都可以构建全面而复杂的行动手册。视觉编辑器应遵循业务流程模型和符号（BPMN）标准，这是一种用于指定业务流程的图形符号。BPMN 支持业务用户使用直观符号，同时为技术用户提供了表示高度复杂流程的能力。

用户界面元素

用户界面元素应该从可以构建视觉行动手册的画布开始。界面的这一部分应提供一个可以指定所需操作的区域（例如 block_ip 或 file_reputation）。一旦选择了某个操作，可能需要一些参数来正确配置该操作。应能够通过该界面手动输入参数或从列表中选择参数。警报数据和/或操作结果数据也可以用作参数。

界面还应拥有可以进行测试和调试的位置，允许从编辑模式无缝过渡到测试模式。最后，如果用户想要查看自动行动手册的源代码，源代码视图应该是可访问的。

基于块的代码表示

使用块来表示自动化平台中有意义的步骤后，用户可以编写全面、复杂的行动手册，而不涉及底层源代码。块应该以一对一、一对多或多对一的方式连接，以规定执行顺序。从视觉上看，用户应该能够构建行动手册，其中包括操作执行、平台 API 调用、条件语句（如果/然后）和将一个行动手册连接到另一个行动手册的分支语句。

将人类融入决策过程

受监督的自动化支持是一个常见的需求，在这种情况下，可以将人插入自动化序列中，以批准、审查或增强行动手册的持续执行。自动化编辑器应该通过在一个或多个安全操作旁边的行动手册中插入批准点来支持这个人工监督步骤。行动手册的作者应该能够指定哪些人将被插入自动化循环，以及所需的通知或批准类型。行动手册编辑器和底层平台应能够定义错误处理逻辑，这也将使人进入自动化循环，就像一个或多个信誉服务不可用于支持决策时一样。

行动结果的信息交流

自动化编辑器界面应该允许由先前行动执行产生的新信息作为输入或参数提供给下游操作或决策块。当填充上游操作的参数时，前面操作的行动结果应该是可视的，并且可以从下拉列表中选择。

访问行动手册源代码

在视觉编辑器中构建行动手册时，生成的行动手册源代码应该是实时生成的，并且作者可以访问。有些用户可能更喜欢通过传统的源代码方法来构建行动手册的全部或部分内容。该界面应该允许折叠可视编辑器并用源代码编辑器替换它。应能够无缝而轻松地实现视觉模式和源代码模式之间的切换。

同时构建视觉和非视觉行动手册

使用行动手册的源代码时，自动化编辑器应该允许作者在源代码级别修改行动手册，并保留在视觉块级别修改行动手册的能力。有时，作者要求在源代码级别修改单个块（例如操作、决策块），以便进行超出可视编辑器范围的定制。当这些修改完成后，用户仍然应能够自由地在视觉上修改行动手册。

内置测试和调试以及运行时日志记录

提供执行和调试功能是集成式开发环境（IDE）的标准。在自动化平台的情况下，用户应该能够根据安全警报执行行动手册，并观察执行活动和结果。如果作者喜欢源代码，日志记录和错误代码应该显示在调试窗口中，该窗口可以与可视块编辑器或源代码编辑器同时显示。目标是使作者能够在一个界面内快速编辑、测试和调试行动手册。

安全模式

自动化编辑器还应为需要生产前测试的新行动手册提供安全模式。该模式模拟在自动化目标上的执行情况，而不影响对它们的更改。一旦作者或其他平台用户对行动手册的逻辑有了足够的信心，便可以禁用该安全模式，行动手册可以开始以正常的方式运行。

应用程序框架

应用程序框架为新的集成提供了可扩展的界面，将平台与当今证券市场上数千种单点产品中的任何一种连接起来。

开放式生态系统

如果不集成到新的市场产品中，SOAR 平台可能会随着时间的推移而失去价值。 为了确保可以预测应用程序集成的路线图，平台应采用允许任何人开发集成的开放式生态系统。 这为用户提供了自主权，并允许他们避免供应商锁定。 技术可以移入和移出，而不会对自动化行动手册产生负面影响。 新技术必须快速集成到平台中，而不需要对核心平台进行任何修改。 最后，用户必须有控制权来吸引对额外平台的支持，而不依赖 SOA 供应商进行额外开发。

度量和报告

度量和报告对每个自动化平台都很重要，SOAR 平台也不例外。自动化有望提高生产率和质量。度量对于理解自动化平台的有效性和确定在哪些方面可以改进以增加投资回报至关重要。

灵活的仪表板

度量特定于组织和个人。因此，用户需要能够以对他们的组织最有意义的方式组织他们的度量。SOAR 平台应该能够以高度定制的方式组织度量信息。这包括配置仪表板上显示的命令信息，指定显示哪些度量以及显示在哪些时间窗口中。

性能报告

部署自动化以提高运营效率。至关重要的是，理解自动化提供的量化性能增益和资源节约，并通过仪表板随时获得这些信息。

平台上应该提供的关键性能度量示例：

- 平均解决时间 (MTTR)
- 平均停留时间（MDT），这里定义为受到影响（由威胁行为者实施）和采取适当回应之间的时间
- 通过自动执行节省的分析时间
- 通过自动执行获得的全时当量 (FTE) 数
- 每次行动手册运行节省的平均时间
- 节省的资金（FTE-成本 x FTE-增益）

安全有效性报告

自动化也被部署来提高组织的安全有效性和态势。了解管理的安全警报总数及其管理速度，对于理解自动化提供的有效性至关重要。

平台应提供的关键安全有效性度量示例：

- MTTR 和 MDT（如上所述）
- 开放的警报总数
- 每天开放的警报（小时、周或月也适用）
- 每天关闭的警报（小时、周或月也适用）
- 服务级别协议（SLA）的性能

应用程序集成和行动手册性能

了解最常被调用的行动手册有助于阐明在哪里可以进行进一步的自动化投资。理想情况下，行动手册设计应该努力自动关闭误报或可信度高的真阳性警报。如果自动化没有缩小警报分类差距，可能有必要修订行动手册。

为了确定自动化方面的差距以及工具集成的有效性，自动化平台应该提供以下示例度量：

- 警报通过自动化关闭（每小时、每天、每周、每月或其他时间窗口）
- 最活跃的应用程序集成
- 最活跃的操作（手动和自动）
- 最活跃的自动化行动手册
- 行动手册执行时间
- 操作执行时间
- 人工工作负载

虽然自动化旨在缩小人力资源的差距，但仍有一些情况下，人类需要参与 SOAR 平台的日常活动。这些情况包括警报需要手动分类和其他操作，或者将人工批准插入行动手册以实现“监督自动化”。 了解人工工作负载也有助于确定可能需要进一步自动化和调整的领域。自动化平台应提供以下示例度量，以了解自动化过程中涉及的人工工作负载：

- 分配给个人的警报
- 个人关闭的警报
- 平均批准时间
- 未批准的数量
- 需要的批准（每小时、每天、每周、每月或其他时间窗口）

平台属性

如前所述，平台属性在本质上可能更加定性。考虑到这一点，这些标准更经常通过观察和与平台的交互来评估。

社区支持

SOAR 平台重点侧重于安全运营社区，这对于其长期成功至关重要。对于一家公司来说，有太多的产品、服务和平台而无法提供集成。不断变化的安全性质也促使需要一群专业人员一起分享行动手册、最佳实践和应对最新威胁的战略。因此，SOAR 平台必须支持强大的社区模型，并简化应用程序集成和行动手册的共享。

大型活跃社区

对平台的安装基础进行衡量是一个很好的度量，表明其相关社区的合作潜力。大多数用户更喜欢借鉴其他志同道合的用户的经验。大型活跃用户社区提供了分享行动手册、应用程序或集思广益的机会，以应对新的自动化用例。此外，供应商对社区的参与是他们对社区和合作承诺的有力标志。

为了促进思想交流，连接社区中的用户至关重要。这通常是通过提供像 Slack 这样的社区通信工具来实现的，该工具支持群发和直接消息传递。消息传递工具对于技术和设计支持、快速回答问题以及关于自动化用例的集思广益非常有效。传播新想法的其他交流工具包括社区用户 Github 页面（个人在此发布他们的作品），以及集中的社区存储库，该存储库托管用户演示文稿、社区行动手册和贡献的应用程序集成。

协作

协作通过以下方式极大地改善了平台的实质：功能完整性、应用程序集成覆盖面和自动化行动手册，这些行动手册可以应对不断变化的场景。

跨社区协作

从内容角度来看，用户和供应商提供的内容应该可以从社区中所有用户都能访问的集中存储库中访问。这包括技术贡献，例如行动手册和应用程序集成，以及非技术贡献，例如演示文稿、技术说明、博客和其他文档方法。正如社区规模所反映的那样，信息库应该处于持续增长的状态。

跨平台协作

如果平台没有将协作结合在一起，协作难题就不完整。SOAR 平台有责任让用户能够利用跨不同信任圈的协作。该平台必须支持最敏感的协作 – 组织安全团队之间的通信。这包括内置聊天功能，以及将笔记和相关数据附加到警报和案例中。

认知

认知 SOAR 平台应该利用人类的知识和以前的观察来指导未来的决策。来自人类的知识必须编码到系统中，以行动手册的形式实现自动化。该平台还可以通过跟踪执行统计数据、摄入数据的特征和行动结果来利用以前的观察结果。这些信息可用于推荐个人行动、行动手册或一系列将形成行动手册的行动。因此，了解 SOAR 平台当前的认知能力，以及该平台未来版本的认知策略和路线图非常重要。

可拨号自动化

随着时间的推移，将自动化融入安全操作通常会增加。最常见的情况是，团队采用自动化一次一个用例来获得对平台的信任。为了帮助建立对自动化的信任，SOAR 平台应该支持一系列功能，允许有选择地与自动化行动手册进行人机交互。

基于每项资产（点安全工具或技术）或者基于每项操作，应能够将人员插入工作流。前者（每项资产）应使资产管理员能够在每次对该资产执行操作时得到通知。后者（每项操作）应通过在自动化行动手册中的任何一点插入人类提示动作来实现。提示为接收者提供了继续、暂停或中止执行的选项。有了这种级别的监督，用户可以对编程的自动化步骤获得信心。

安全

安全自动化和编排平台最重要的方面之一是其自身的安全性。由于 SOAR 平台拥有身份验证凭据和其他高度敏感的信息，因此它经过强化，加密敏感信息，并支持强大的基于角色的访问控制工具。

SOAR 平台需要寻找的关键安全最佳实践包括：

- 加密安全凭证
- 确保凭据不存储在内存中
- 对身份验证管理系统的支持
- 支持多重因素身份验证

可扩展

重要的是要了解 SOAR 平台将如何垂直和水平扩展。由于组织会随着时间的推移增加使用案例，平台上会增加额外的处理负载。该平台的设计应允许通过增加硬件资源（例如 CPU 和 RAM）进行垂直扩展，以及通过增加支持部署的服务器实例数量进行水平扩展。

开放和可扩展

安全总是在不断发展，今天有大量的单点产品可以证明这一点。应该为开放性和可扩展性设计 SOAR 平台。它应很容易支持整合新的安全场景、新产品、新行动和新行动手册。

开放式集成框架

开放式集成框架的净效果是，技术应该能够在不负面影响自动化操作的情况下进出平台。

用户还应能够控制开发对额外集成的支持，而无需依赖 SOAR 平台供应商。这包括授权用户编写他们自己的集成（如果他们选择这样做）。这可能适用于本地开发的应用程序、来自供应商的定制或早期访问 API，或者如果他们选择扩展自动化平台的功能，就是很好的例子。这个开放的框架应该遵循共同的标准和编程模型。应该有大量的文件和例子可用。

没有接口限制

一些技术使用 REST API、SSH、syslog、自定义 API 或其他协议或方法公开接口。可扩展集成框架不应该对接口类型实施任何限制。如果从自动化平台连接到点产品或应用程序，接口方法不应影响应用程序集成 – 允许使用任何接口方法。

易于使用

虽然企业软件从来都不简单，但是有可能减少部署和使用 SOAR 平台的摩擦。

安装和设置

虚拟设备外形简化了部署，因为大多数组织已经利用虚拟化和其他基础架构。

加载

通过使用加载流程帮助用户配置系统设置、连接数据源并激活他们的前几本行动手册，SOAR 平台可以极大地帮助克服初始学习曲线。

加快自动化的速度

SOAR 平台应该能让用户快速开始自动化。这是通过提供一套强大的现成自动化行动手册来实现的。增强用户快速起草、测试和部署自动化行动手册的能力是另一个重要的加速器。

可视化 IDE 使非程序员更容易创建和编辑行动手册。SOAR 平台可以通过提供可视化地创建或修改自动化行动手册的工具来实现这一点。行动手册的可视化构建通过避免编码错误和提供促进行动手册一致性的编码标准，减少了开发时间并提高了质量。

业务考虑

不管一家公司的核心技术有多棒，除了传统上被视为对买方决策过程有重大影响的因素之外，还有其他考虑因素。一个主要考虑因素是产品营销公司的属性。另一个重要的考虑因素是公司提供的一系列服务，这些服务增强了核心技术，形成了买方最终体验到的整个产品。

公司属性

在做出采购决策时，重要的是要考虑您选择的公司的概况、质量和未来潜力。 现实是，许多在新细分市场拥有新解决方案的新公司将会失败。您应该选择一家有实力履行承诺的公司。

公司历史

您选择的公司应该在开发安全解决方案方面有着深厚的历史。虽然安全编排、自动化和响应是市场中相对较新的细分，但其起源可以追溯到几十年前。重要的是要了解公司是如何成立的，以及他们如何决定追求 SOAR 的细分市场。

执行能力

您应该寻找由经验丰富的专业人员组成的团队支持的公司。预测公司未来的执行能力很可能与团队成员的历史记录直接相关。

客户群

公司客户群的质量和形象反映了公司本身。 经验丰富的企业客户在购买前会在几个领域对潜在供应商进行严格的调查。

奖励和表彰

检查公司的奖项和他们可能获得的其他类型的表彰。奖励和表彰是贸易和行业对公司及其产品符合其要求的认可。和公司本身一样，奖项的质量也不尽相同。

辅助服务

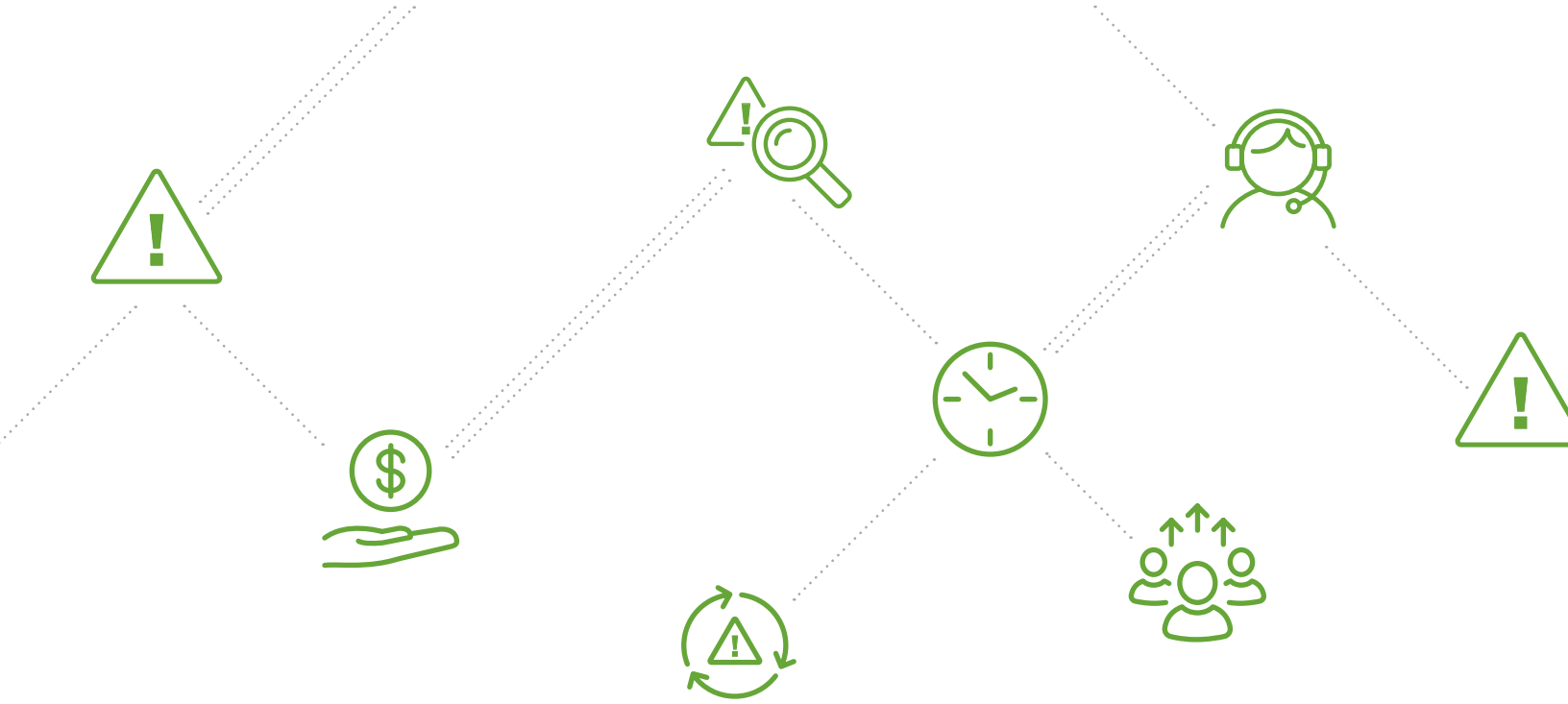
一家公司为其技术提供的辅助服务可以极大地影响采购组织的部署经验，最终影响项目的成功。

专业服务

安全运营成熟度级别因组织而异。因此，重要的是要考虑公司是否提供专业服务来增加成功部署的机会。同样重要的是，主题专家能够参与服务项目，帮助构建流程（如果缺少），并帮助将手动工作流转换为自动化行动手册。

售后支持

许多初创公司提供卓越的技术和售前支持，但在售后支持方面却步履蹒跚。检查支持选项的范围，并确定公司是否提供您需要的支持类型。



3.结论

本指南包括许多评估 SOAR 平台时需要考虑的标准。从核心组件到平台属性，再到业务考虑，重要的是在开始评估流程和选择平台之前，充分制定评估标准。

若要了解有关 Phantom 安全自动化和编排平台的更多信息，请下载免费的 Phantom 社区版 或联系销售人员索要 更多信息。

WP-Splunk-Phantom-SOAR-Buyer's-Guide-103x

评估清单

在评估各种安全自动化和编排平台时，请使用这个方便的核对表。

平台名称：_____

核心能力

- ☐ 编排程序
  - ☐ 数据集成
  - ☐ 决策
  - ☐ 执行
  - ☐ 人工监督
  - ☐ 数据管理
  - ☐ 容错
- ☐ 自动化引擎
  - ☐ 可伸缩性
  - ☐ 可扩展性
- ☐ 警报管理
  - ☐ 警报详细信息
  - ☐ 发布行动
  - ☐ 行动结果
  - ☐ 活动日志
  - ☐ 警报状态、严重性和敏感性
  - ☐ 警报协作
- ☐ 案例管理
  - ☐ 案例数据组织
  - ☐ 将数据添加到案例中
  - ☐ 将案例链接到警报
  - ☐ 映射到现有流程
  - ☐ 活动审计
- ☐ 行动手册管理
  - ☐ 行动手册组织
  - ☐ 批量编辑行动手册
  - ☐ 修订控制和分发
- ☐ 自动化编辑器
  - ☐ 用户界面元素
  - ☐ 基于块的代码表示
  - ☐ 将人类融入决策过程
  - ☐ 行动结果的信息交流
  - ☐ 访问行动手册源代码
  - ☐ 同时构建视觉和非视觉行动手册
  - ☐ 内置测试和调试以及运行时日志记录
  - ☐ 安全模式
- ☐ 应用程序框架
  - ☐ 开放式生态系统
- ☐ 度量和报告
  - ☐ 灵活的仪表板
  - ☐ 性能报告
  - ☐ 安全有效性报告
  - ☐ 应用程序集成和行动手册性能
  - ☐ 人工工作负载

平台属性

- ☐ 社区支持
  - ☐ 大型活跃社区
- ☐ 协作
  - ☐ 跨社区协作
  - ☐ 跨平台协作
- ☐ 认知
  - ☐ 可拨号自动化
- ☐ 安全
  - ☐ 可扩展
  - ☐ 开放和可扩展
  - ☐ 开放式集成框架
  - ☐ 没有接口限制
  - ☐ 易于使用
  - ☐ 安装和设置
  - ☐ 加载
  - ☐ 加快自动化的速度

业务考虑

- ☐ 公司属性
- ☐ 公司历史
- ☐ 执行能力
- ☐ 客户群
- ☐ 奖励和表彰
- ☐ 辅助服务
- ☐ 专业服务
- ☐ 售后支持