为什么安全编排、自动化和响应（SOAR）是安全平台的基础

2020 年 5 月 19 日 | 作者 :Ted Julian 及 Chris Meenan | 阅读时间 :4 分钟

由于最近的全球健康危机所造成的“新常态” ,如今的安全团队面临着越来越多的挑战。那些在太多工具、太多数据中苦苦挣扎的团队发现，协作和交流变得更加困难，因为他们的员工必须转到虚拟安全运营中心（SOC）模型中，同时还要应对越来越多的威胁并投入更多的时间来满足家人和家庭需求。

互不关联的团队加速了对开放、互联平台的安全方法的需求。借助这种方法，组织可以：将新的安全工具与现有安全工具整合在一起，进而实现投资最大化；将 SOC 分析人员的工作流转移到单个位置 ,进而提升他们的生产效率 ;随着 IT 和安全计划的变化为组织提供灵活性。我们对下一代开放、集成安全平台的愿景围绕下述三个主要原则而构建：

1. **开放架构：**如今，组织会使用越来越多的不同工具和云平台，因此下一代安全平台必须具有足够的开放性 ,才能轻松与来自不同供应商的不同工具进行协同。整合现有工具或移动数据通常由于成本过高、过于复杂而让组织无法实施，但是采用基于开源技术并由开放标准机构支持的平台，便能够让团队以标准化的方式将所有工具整合在一起 ,进而实现现有投资的最大化。
2. **集中式中心 :**SOC 分析人员可以使用单个主记录系统来管理其工作流程，进而提升工作效率。在开放架构之上而构建的集中式中心提供了一种融合人员、流程和技术的方式。这使得分析人员可以摆脱他们所用的单个工具，

并将其工作简化到单个位置，同时仍可从现有工具中发掘有价值的数据，并减少就所有的已部署工具对整个 SOC 进行训练的需求。目标在于在适当的时间自动将适当的信息呈现到适当的人员面前，让问题得到有效而果断的解决。

3. **灵活部署：**大多数组织都使用多个云平台和内部解决方案来管理其安全和 IT 环境。此外，每个组织通常都处在自己独特的云之旅中。可在任何位置部署的下一代安全平台能够让企业灵活选择目前和将来的最佳选项，同时避免锁定到特定的部署模型。

SOAR 是下一代安全平台的核心

安全编排、自动化和响应（SOAR）解决方案基于 Gartner 定义的四个引擎而构建，分别是：工作流和协作、凭证和案例管理、编排和自动化以及威胁情报管理。结合采用这些功能可以将人员、流程和技术融合在一起，进而提高 SOC 生产效率、缩短事件响应（IR）时间。因此，这些引擎也能够为强大的安全堆栈提供理想的基础。的确，基于开放架构并采用灵活混合云部署的 SOAR 功能是构建符合这一愿景的安全平台的理想方法。

将 SOAR 置于安全平台的核心有助于团队以集中、协调的方式开展工作，进而实现整个生态系统以及所有安全流程的价值扩展和最大化。将 SOAR 功能整合到下一代安全平台之中，将能够提供一个坚实的基础，进而帮助组织实现诸多优势。

加强安全团队内部和外部的沟通

任何 SOC，尤其是虚拟 SOC，都需要通过无缝协作来指导响应并组织任务 - 这是 SOAR 平台的关键功能之一。团队无需从头开始，只需要遵循动态运行手册中嵌入的工作流程以智能的方式开展工作即可。此外，安全团队可以利用 SOAR

的工作流和协作引擎与不同的职能部门（如 IT、法律、人事或 PR 等）的关键参与者进行沟通，进而促进协调一致且有效的响应。

通过集中式案例管理提升效率

SOC 分析人员可以通过案例管理功能提升效率，此类功能可以通过 SOAR 解决方案的集中式中心进行管理，无需在多个工具和仪表板之间来回切换。在案例管理从 SOAR 解决方案扩展到更广泛的安全平台之后，便可为分析人员提供一种通用格式，以供在所有连接的功能中使用。强大的案例管理功能还包括仪表板和报告功能，用以跟踪指标和 KPI、突出显示趋势和差距并提升 SOC 的业务价值。

生态系统深度和广度的最大化

安全团队可以通过开放架构实现其生态系统深度和广度的最大化。借助开放的、基于标准的方法，SOC 团队可以通过跨各种数据源和工具的集成来利用多样化生态系统的功能，同时充分利用现有投资。这些技术的编排能够扩展 SOAR 功能，同时为安全分析人员提供对生态系统的更高可视性。

将 SOAR 置于下一代平台的核心，有助于让客户将 SOAR 的优势扩展到创建 SOAR 所针对的 IR 流程之外，进而将漏洞管理、身份管理、DevSecOps 等安全流程涵盖在内。如此一来，不仅从逻辑上扩展了该项投资，进而产生额外的 ROI，而且还能够生成有关这些流程的 KPI，用于推动持续改善并转变安全部门与组织其他部门的关系。

基于 IBM Cloud Pak for Security 的 SOAR

IBM Cloud Pak for Security 是一个开放的集成式安全平台，它具有诸多 SOAR 功能，使您可以连接到现有数据源，以生成更深刻的洞察力，并快速编

排针对这些威胁的行动和响应 - 所有这些都是在将数据留在原位的情况下完成的。

若要了解有关 IBM Cloud Pak for Security 如何提供以 SOAR 作为基础和核心组件的平台方法的更多信息，请参与我们即将举行的网络研讨会。在该网络研讨会上，IBM Security 的产品负责人将会概述安全团队如何利用 IBM Cloud Pak for Security 平台及 IBM Security Resilient 久经验证的成熟 SOAR 功能来改善跨不同数据、工具和团队的安全事件协作和管理。

Ted Julian

IBM 产品管理副总裁、Resilient 联合创办人

Ted Julian 是安全与合规领域一位备受推崇的知名人物。在过去的 12 年中，他构想并创办了多家成功的跨软件、硬件和专业服务的安全初创公司。他曾担任过数据库安全解决方案领先提供商 Application Security 的市场营销副总裁。在加入 Application Security 之前，Ted 曾是 Arbor Networks（已被 Danaher 收购）的公司创办人之一兼首席战略师（担任营销副总裁一职）；Arbor Networks 是一家领先的网络安全公司，致力于保护全球几乎所有提供商的骨干网络。在加入 Arbor 之前，Julian 曾是 @stake（一家领先的数字安全咨询公司，已被 Symantec 收购）的公司创办人之一兼营销副总裁。在最初进入技术领域时，他曾担任 International Data Corporation (IDC) 和 Forrester Research 的行业分析师。