IBM Cloud Pak for Security

SOAR | 安全编排、自动化和响应

通过编排和自动化缩短响应时间并补救复杂的网络威胁

组织面临着日益严峻的安全运营挑战 - 网络攻击的数量和严重性都在不断增加，同时在聘请和留住 IT 安全专业人员方面依然存在困难。这些因素加上其他一些因素导致组织需要采用 SOAR 工具，以帮助他们的安全团队响应和补救复杂的网络威胁。

IBM Cloud Pak for Security 上的 SOAR 服务能够实现常见安全运营和事件响应 (IR) 流程的自动化，并通过必要的步骤对其进行引导来解决复杂情况，以此方式为安全分析人员提供支持。安全分析人员可以快速访问重要的安全信息及相关的事件情境信息，进而作出准确的决策、果断采取措施。该服务利用自动化来提升安全分析人员的工作效率以及已部署技术的效率，进而缓解技能差距、避免疲劳问题。

解决方案亮点

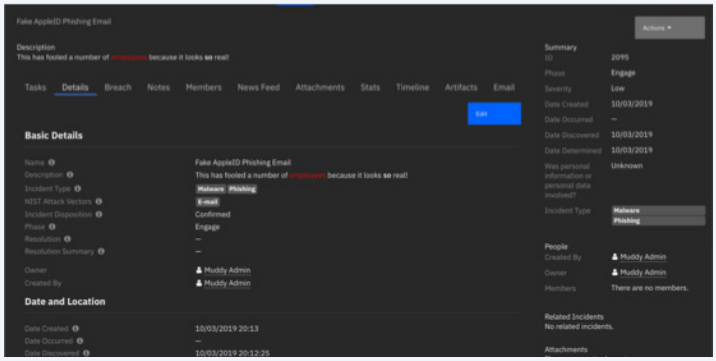
缩短补救所需时间：实现手动任务和重复性任务的自动化

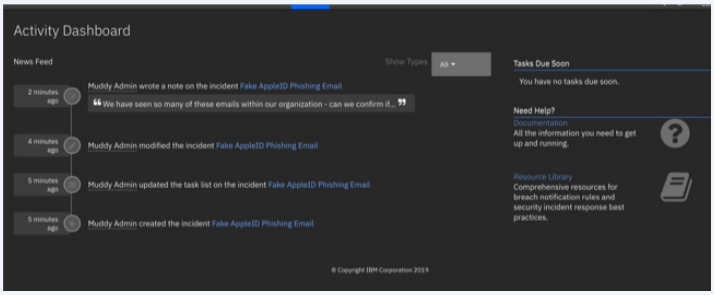
改善安全效率：实现事件响应流程中的编排和自动化

对分析人员的工作负载进行优先排序：通过自定义运行手册引导分析人员的操作

改善团队协作：确保统一的流程和工作流

嵌入最佳实践：借助面向常见威胁的事件响应运行手册





衡量并改善安全运营中心 (SOC) 的效率：通过安全编排和自动化减少事件响应流程中的手动步骤（在事件响应流程中的任何步骤均可调用编排和自动化功能），进而提高 SOC 的生产效率、提升流程水平并缩短解决时间。

简化安全运营管理：管理 IT 复杂性是一个常见的安全运营挑战。Cloud Pak for Security 上的 SOAR 可通过广泛的第三方应用以及面向通用安全和 IT 运营工具的集成件，帮助安全分析人员管理整个组织中不同的安全产品。

确立标准 IR 流程：安全编排和自动化是一种流程，而不是产品。它需要强大的基础支撑，包括经培训的人员、成熟的流程和集成技术。借助 Cloud Pak for Security 上的 SOAR，您可以针对常见威胁编写并维护事件响应手册，其中已经融合了行业最佳实践和内部程序。

主动管理事件响应：支持安全团队自动调整其 IR 流程以适应实时事件状况，并通过动态运行手册实现快速、完整的响应。借助基于复杂逻辑引擎构建的敏捷、自适应工作流，动态运行手册会使用组织的安全工具来摄取与事件相关的数据，在发现有关事件的新信息时自动更新 IR 计划。

为安全团队赋能：支持安全团队基于任务和技术集成件，以直观的方式构建复杂的工作流，以编排事件响应，而无需特殊的编程或编码技能。