高级安全编排、自动化和响应

通过高级安全编排和自动化加速事件响应。

亮点

- 支持事件响应团队快速作出决策并采取行动
- 与 100 多种安全工具相集成
- 实现重复性繁琐任务的自动化
- 利用 OODA 循环方法
- 快速响应复杂攻击

概述

当今的组织正在与复杂的网络攻击作斗争，这些攻击会随着他们的发展和更多智能的积累而变化。随着技术环境的日益复杂以及技能差距的不断加大，高效响应攻击已变得比以往更加复杂。

为了解决这个问题，安全团队开始采用安全编排、自动化和响应（SOAR）平台来应对这些不断增长的威胁，因为此类平台能够帮助分析人员做出明智的决策并迅速采取行动。高级事件响应编排功能可以协调安全运营中心（SOC）以及整个组织中的人员、流程和技术。

经过实践检验的 IBM Resilient® SOAR 平台通过精心设计而构建，可通过简化响应流程将响应时间从数小时缩短至数分钟。

为响应团队赋能

IBM Resilient SOAR Platform 提供了一个高级编排平台，可促进动态和加速响应。

Resilient 的编排功能可以自动执行重复性和琐碎的任务，并在适当的时间向适当的分析人员提供适当的信息，进而降低平均响应时间，让分析人员的工作变得更加有效、更加高效和更具战略性。

我们的一家大型制药客户通过对其关键威胁响应流程的编排和自动化，将获取取证图像所需的时间从 84 分钟缩短至不到 2分钟。

“借助 Resilient，我们应对新出现威胁所需的时间从 84 分钟缩短至不到 2分钟。”

- 某家全球性医药公司的网络安全总监

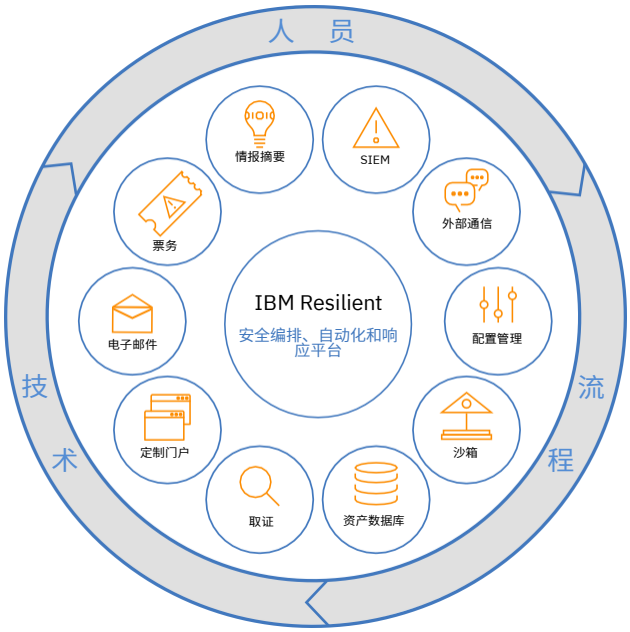

图 1： IBM Resilient SOAR Platform 如何充当事件响应编排的“中央枢纽”。

编排平台的功能

借助 IBM Resilient SOAR Platform 的最新创新，组织可以获得构建经编排的动态、加速响应计划所需的各种工具。Resilient SOAR Platform 受美国军方所用 OODA （观察、定向、决定和行动）循环方法的启发，能够让分析人员更快、更准确地完成 OODA 循环过程。

Resilient 能够与 100 多种安全工具相集成，可将您现有安全环境中的各个方面与您的 IR 流程连接在一起，从而形成事件响应编排的中央枢纽。

Resilient SOAR Platform 的最新编排创新包括：

- **动态运行手册：**提供应对复杂攻击所需的敏捷性和高级功能。动态运行手册能够自动适应实时事件状况，甚至可以确保在分析人员打开事件进行处理之前便已完成了重复的初始分类步骤。
- **视觉工作流：**支持分析人员基于任务和技术集成，以视觉化的方式构建复杂的工作流。
- **事件可视化：**以图形化的方式显示组织环境中的事件工件或威胁指示器 (IOC) 与事件之间的关系。
- **定时程序：**支持工作流中基于时间的规则，以帮助团队确保及时响应、识别瓶颈并确保与组织 SLA 的合规性。
- **工件工作流：**支持工具到工具的自动化工作流，同时还支持以人为中心的任务和批准。
- **任务和脚本：**向工作流中添加平台内脚本编写功能，以实现平台内自动化。

优势

借助 Resilient SOAR Platform，CISO 及其安全团队可以：

加快对复杂攻击的响应

通过与 100 多种不同技术的集成，能够让安全部门应对复杂的攻击、展示安全支出的业务价值，并提升整个安全堆栈的 ROI。

改善和衡量 SOC 生产效率

通过与现有安全工具相集成，能够让 SOC 管理人员改善和衡量 SOC 生产效率，并自动调整响应流程，以高效应对攻击。强制执行 SLA，并确保适当的分析人员使用适当的工具来执行适当的任务。

缓解技能差距

让初级分析人员能够通过分类和扩充任务的自动化管理复杂的威胁并将精力集中在调查和响应上，而无需在各种工具之间反复轮换，进而实现倍增作用。

改善数据泄露通知流程

提供即时反映最新法规的全球法规与响应计划知识库，简化隐私响应管理，进而消除履行隐私违反法规和义务过程中的复杂性。

编排您的响应并为安全团队赋能，使其能够更快、更明智地采取行动。

有关更多信息

访问以下网站，立即预约 Resilient Incident Response Platform 演示：**ibm.com**/us-en/marketplace/resilient- incident-response-platform

IBM Corporation Security Group
Route 100
Somers, NY 10589

美国印刷
2019 年 4 月

BUD03063-CNZH-00