版本 2.0

IBM Cloud Pak for Security

专为混合多云世界而构建的互联安全解决方案

您的安全数据经常会分散在不同的工具、云平台和内部 IT 环境中。这就造成了一些会导致威胁被忽略的缺失，而这些缺失通常通过成本高昂的复杂集成来解决。IBM Cloud Pak for Security 所提供的平台能够借助一个可在任何位置运行的、与基础架构无关的通用操作环境来帮助您更快地集成现有安全工具，进而更深入地了解混合多云环境中的威胁。您可以快速搜索威胁，编排操作并自动执行响应，而所有这些均无需移动数据。

在不移动数据的情况下获得安全洞察力

通过自动化更快速地响应安全事件

随处运行，开放地连接各种安全工具

解决方案亮点

更快发现潜藏威胁：连接和搜索所有数据源，更全面地了解您的安全环境

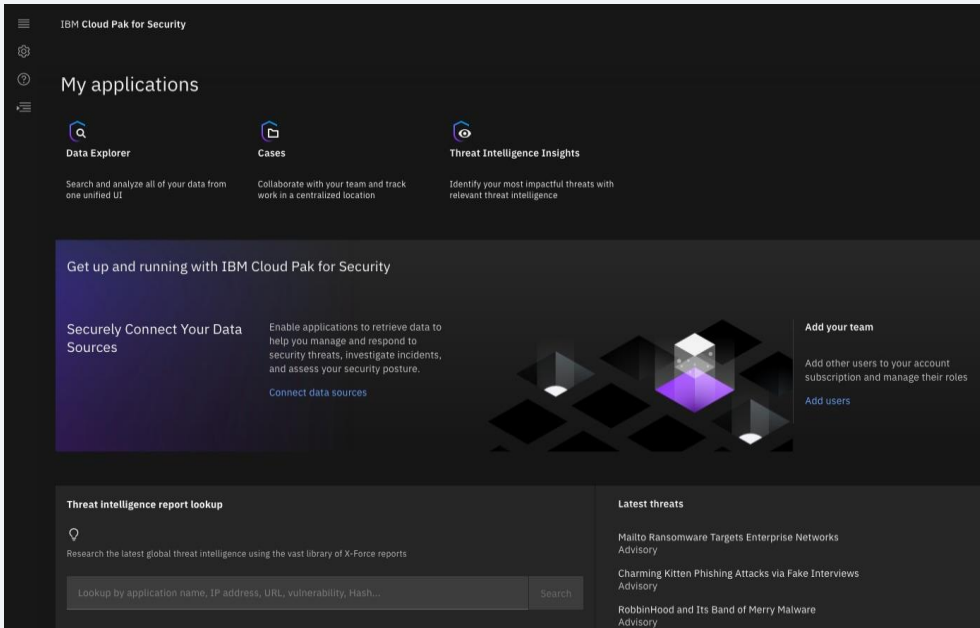
随处运行（内部、公有云或私有云）：预先与 Red Hat OpenShift 企业应用平台集成的容器化软件

降低安全数据成本：使用开放标准连接到现有安全工具，而无需移动数据

提升安全可视性：借助与 IBM 和第三方的数据连接器实现与开放生态系统相连的解决方案

缩短响应时间：编排和自动化手工和重复性任务，通过第三方集成推动开展调查

扩展团队能力：借助额外技能（由 IBM Security Expert Lab 提供的按需咨询服务到自定义开发）



更多信息，敬请访问：

ibm.com/products/cloud-pak-for-security

IBM Security

IBM Cloud Pak for Security 产品与服务

IBM Security Threat Intelligence Insights

面向 IBM Cloud Pak for Security 的 Threat Intelligence Insights 可提供详细的可执行的威胁情报，根据您的组织概要信息和环境数据帮助识别与组织最相关的威胁并对其进行优先排序。一旦检测到威胁，它便可跨多个分散数据源无缝地调查威胁和失陷指标 (IOC)，并通过统一控制台使用 IBM Cloud Pak for Security 上的集成化应用对网络威胁进行补救。

IBM Security Data Explorer

IBM Security Data Explorer 能够让分析师跨 IBM 数据源和第三方数据源执行联合调查。该解决方案能够将来自安全信息和事件管理 (SIEM) 和终端检测和响应 (EDR) 等安全工具、存储在 Elastic 等数据湖中的数据的洞察力互联到一起。此外，它还能够从您的 SIEM 工具（如 QRadar 和 Splunk）所监控的多云环境中发掘洞察力。您可以使用简单的查询构建器和单一工作流查询多个数据源，进而显著缩短调查时间。它能够使您的安全运营中心（SOC）更快地执行更多操作，使分析人员在所有数据源中搜索失陷指标 (IOC) 和威胁。

IBM Security Resilient

内置在 IBM Cloud Pak for Security 的 IBM Security Resilient 解决方案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。安全分析师可以快速访问重要的安全信息及相关的事件上下文信息，进而作出准确的决策、果断采取措施。它利用自动化和第三方集成来提升安全分析师的工作效率以及已部署技术的效率，进而缓解技能短缺、避免疲劳问题。

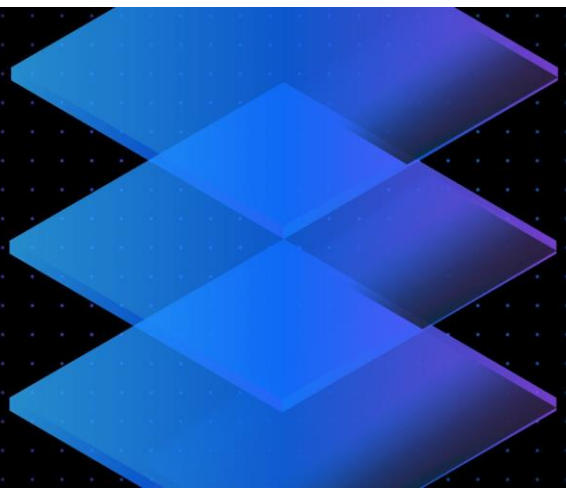
IBM Security Expert Lab 提供的服务

IBM Security Expert Lab 可为 Cloud Pak for Security 提供支持服务。该团队可提供 IBM Security 产品生命周期的各个阶段（采用、扩展和优化）所需的业务和技术洞察力。IBM 深知每个客户的安全规划都是不相同的，因此提供了从平台使用、连接器开发到支持等各类服务，确保 Cloud Pak for Security 能够增强您的安全规划。

更多信息，敬请访问：

ibm.com/products/cloud-pak-for-security

IBM Security



IBM

IBM Cloud Pak for Security

Data Explorer

通过单个统一的界面调查多个孤岛式解决方案中的威胁和威胁指示器 (IOC)

如今，安全团队面临的挑战在于每天如何从不同的安全工具、云环境和数据湖的成百上千个事件中识别洞察力。若要实现有效的调查和威胁捕获，就需要分析来自所有工具的洞察力。如今，分析人员会浪费宝贵的时间来尝试分别登录到不同的工具，使用这些工具的原生语言进行搜索或借助各个工具的主题专家来收集所需的信息。这种低效的手动流程通常会拖慢调查速度，而且导致分析人员不得不根据部分信息做出决策。若要确保强大而高效的网络安全态势，企业需要对潜在的风险和威胁进行广泛而深入的调查，这对于当今负担沉重的安全分析人员来说是一个挑战。

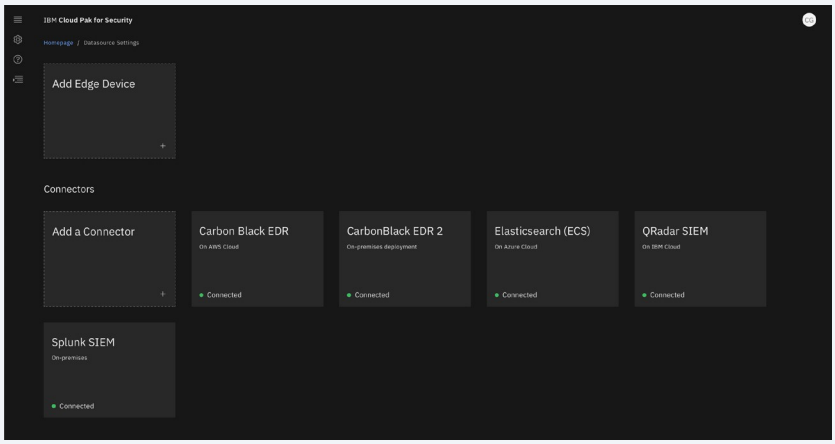
如果您能够使用单个工具、使用单个语言来搜索所有数据源，情况将会怎样？

作为 Cloud Pak for Security 的一部分，IBM Security Data Explorer 能够让分析人员跨 IBM 数据源和第三方数据源执行联合调查。将来自安全工具（例如：安全信息和事件管理（SIEM）和终端检测和响应（EDR））的洞察力与存储数据湖（例如：Elastic）中的数据互联到一起。[图 1]

此外，它还能够从您的 SIEM 工具（如 QRadar 和 Splunk）所监控的多云环境中发掘洞察力。您可以使用简单的查询构建器和统一工作流查询多个数据源，进而显著缩短调查时间。它能够使您的安全运营中心（SOC）更快地执行更多操作，使分析人员在所有数据源中搜索和威胁。

IBM Security Data Explorer 可以加快 IOC 调查，将调查所需时间从数小时缩短到数分钟，还能够通过联合搜索和调查消除盲点。它能够通过单个统一界面连接您的各个数据源并运行查询。

图 1 | 连接器



解决方案亮点

从现有安全工具中**发掘更多价值**

支持分析人员进行更多操作，进而**提升生产效率**

通过数据联合将数据保留在原处，**无需移动数据**，也无需其他数据湖

可通过单个屏幕搜索不同的数据集，进而**更快地发现隐藏的威胁**

减少将数据复制到数据湖的**隐私风险**

借助预构建的集成**避免在内部构建成本高昂的产品集成**

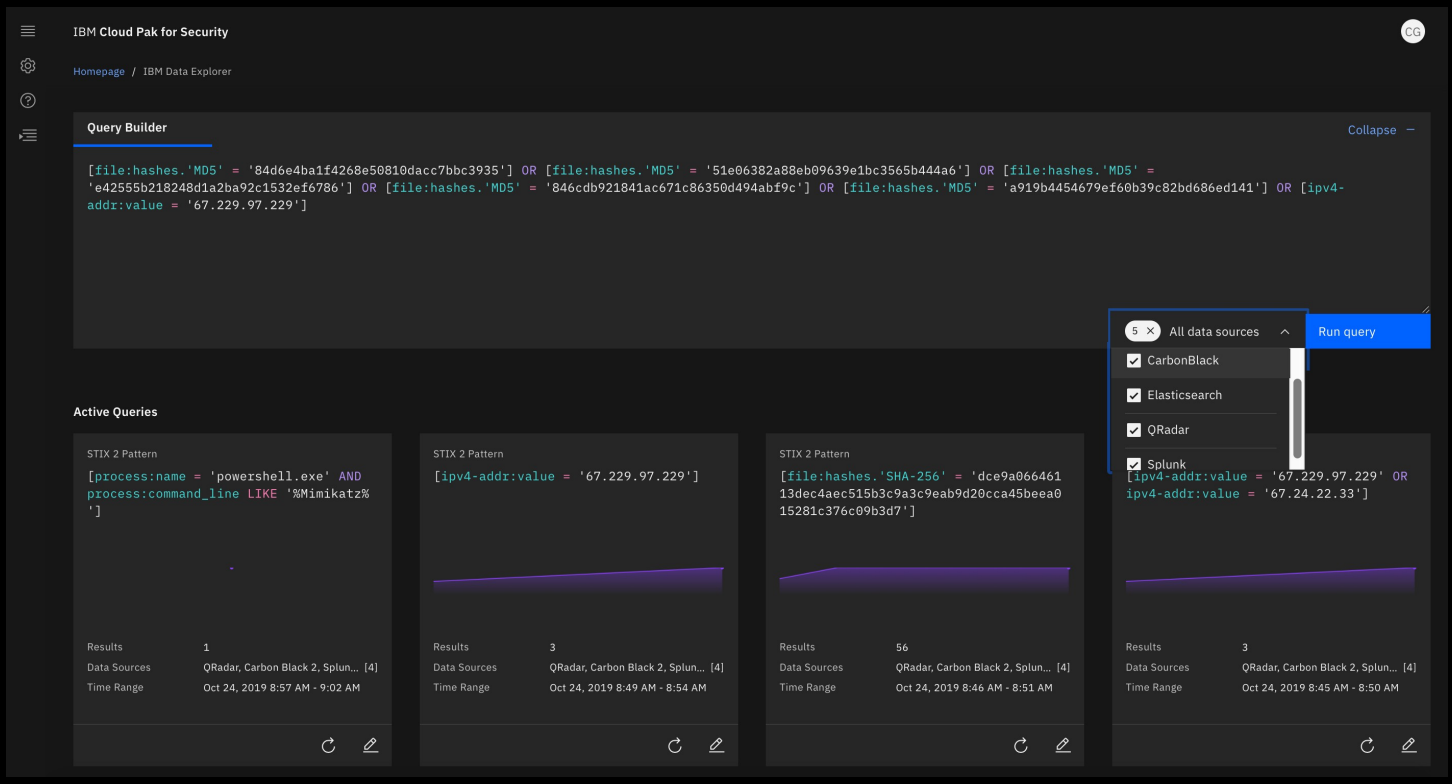
消除数据孤岛：不同的工具、云平台和本地环境中出现了越来越多的数据孤岛，这使得确保跨所有数据源的可视性成为了一个挑战。IBM Security Data Explorer 能够访问所有数据，无论其位于何处。

让威胁捕获和事件调查变得更加高效：SOC 分析人员在捕获威胁或调查安全事件时必须搜索多种工具。借助 IBM Security Data Explorer，他们只需通过单个界面进行一次查询即可获得所需的洞察力和信息。[图 2]

简化运营：一旦发现某个 IOC，SOC 分析人员就必须在其安全编排、自动化和响应 (SOAR) 工具中开启一个案例。借助 Cloud Pak for Security 内置的案例管理功能，SOC 分析人员可以通过单个用户界面执行这些操作。

轻松管理多个客户：对于托管安全服务提供商 (MSSP) 来说，他们可以通过单个界面搜索多个客户端环境和数据存储库。

图 2 | 查询构建器



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

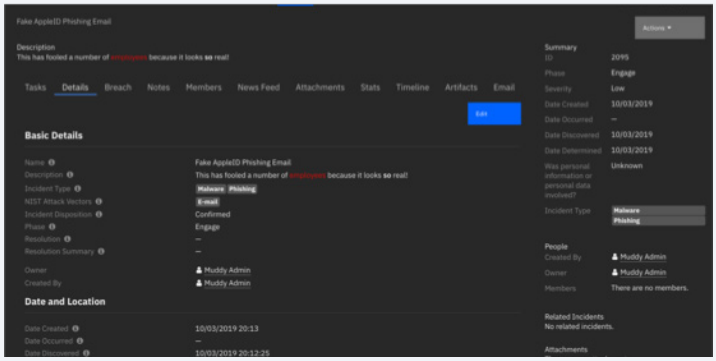
缩短补救所需时间：实现手动任务和重复性任务的自动化

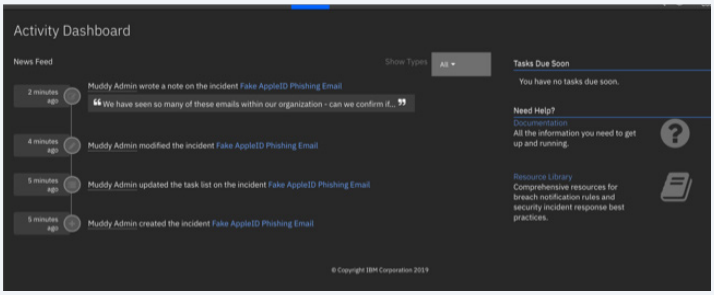
改善安全效率：实现事件响应流程中的编排和自动化

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





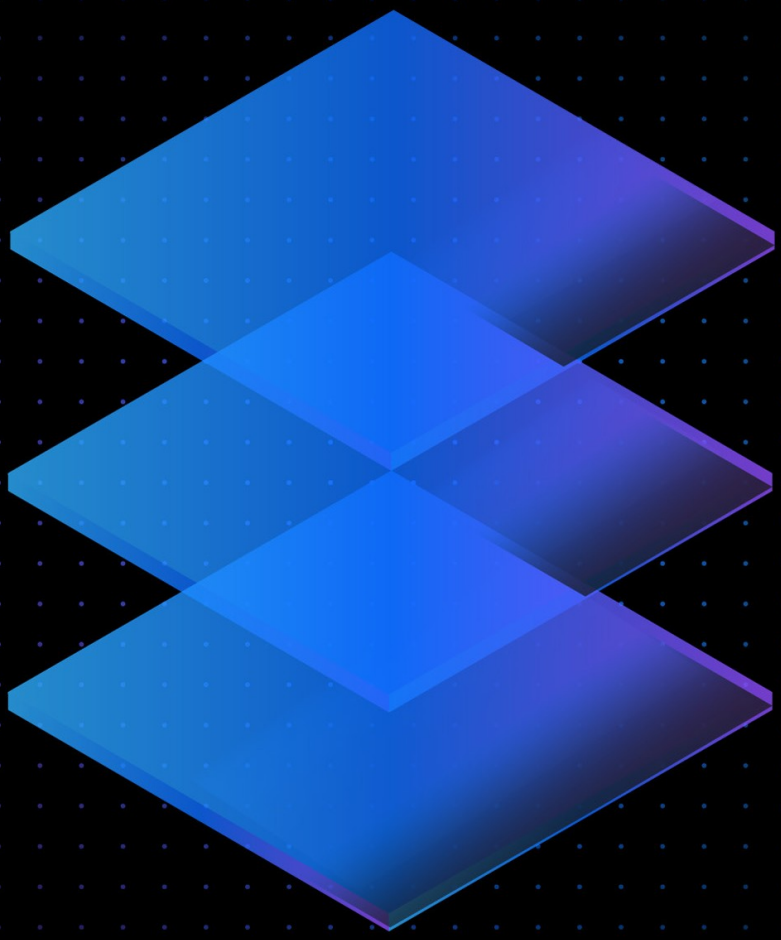
衡量并改善安全运营中心 (SOC) 的效率：通过安全编排和自动化减少事件响应流程中的手动步骤（在事件响应流程中的任何步骤均可调用编排和自动化功能），进而提高 SOC 的生产效率、提升流程水平并缩短解决时间。

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。



IBM Cloud Pak for Security

服务选项

通过 IBM Security Expert Lab 提供的服务充分发挥 Cloud Pak for Security 部署的价值

安全环境变得越来越复杂。安全分析人员对此不知所措，无法分析来自众多不同安全工具的数据，这些限制了他们的工作效率、数据的可视性以及保护范围。反过来，这会对组织的整体安全态势带来负面影响。

IBM Cloud Pak for Security 所提供的平台能够借助一个可在任何位置运行的、与基础架构无关的通用操作环境来帮助您更快地集成现有安全工具，进而更深入地了解混合多云环境中的威胁。客户可以快速搜索威胁，编排操作并自动执行响应，而所有这些均无需移动数据。

IBM 深知每个客户的安全计划都是互不相同的，因此提供了从注册、连接器开发到支持服务的各种服务，确保 Cloud Pak for Security 能够增强您的计划。

按需型专家服务

您的安全环境非常复杂。IBM 可以围绕威胁运营、编排和自动化的行业最佳实践建议提供咨询服务。IBM 还可以与您的组织一道为您的独特环境量身定制威胁运营、编排和自动化的成熟度模型。

快速入门服务

如果定义了正确的用例和流程，Cloud Pak for Security 便可发挥最大价值。为了帮助组织最大程度地发挥投资的价值，IBM 提供了快速入门服务，可在 Cloud Pak for Security 的部署过程中为您提供帮助。将您的技术团队与专家配对，来解答您在 Cloud Pak for Security 部署方面遇到的问题。Cloud Pak for Security 随附有多个面向云和安全产品的预构建连接器，IBM 可以通过这些连接器协助您完成环境配置和定制，并就联合搜索查询的创建提供指导。

战略和运营服务

此类服务建立在快速入门服务的基础上，同时提供了额外的服务选项。除了配置和定制化连接器、创建联合搜索查询以帮助您进行威胁调查之外，IBM 还可以帮助您简化补救措施、采用业内标准的事件响应最佳实践。作为平台上安全编排、自动化和响应功能的一部分，IBM 可以帮助您开发定制化运行手册、实现安全事件响应的自动化。此外，IBM 还提供了可供选购的设计思维研讨会，旨在了解您的组织优先事项并根据业务优先事项对编排和自动化运营进行调优。

连接器开发服务

尽管 Cloud Pak for Security 平台已经支持多个连接器，但您的组织正在使用的某个产品或数据源可能在启动时没有可用的连接器。IBM 可以与您合作开发此类数据源的连接器，使您在所有工具中均可充分利用 Cloud Pak for Security 的全部功能。

IBM Security Expert Lab

IBM Security Expert Lab 可为 Cloud Pak for Security 提供支持服务。该团队可提供 IBM Security 产品生命周期的各个阶段（采用、扩展和优化）所需的业务和技术洞察力。

Security Expert Lab 进行了独特定位，旨在帮助您推动 Cloud Pak for Security 旅程。借助资产和集成模式，我们的专家顾问可以帮助您加快 IBM Security 解决方案的部署，确保其在规模上的匹配性，进而满足您的业务目标。我们的 3,700 多名顾问和 3,300 名服务交付专家均已接受了敏捷和 DevOps 方法方面的培训，能够优化 IBM Security 的产品组合，确保您可以快速完成项目。

业务代表为您服务：
400 810 1818 转 2395

注册告诉我们您的需求：
https://ibm.biz/Bdqy8R

敬请访问网站：
https://ibm.biz/Bdqy8E