KuppingerCole 报告

执行观点

作者：Martin Kuppinger | 2019 年 11 月

IBM Cloud Pak for Security

IBM Cloud Pak for Security 是一款创新型解决方案，可以在多种部署模型中运行，为当今的复杂的混合和多云环境提供安全分析和事件响应支持功能。它能够针对来自 IBM 和其他供应商的多种来源中的安全和威胁信息提供统一视图。它支持跨数据联合搜索，以及用于跨多个系统进行事件响应的合并工作流。通过这些功能，它可以帮助每个 SOC 大幅提升效率。

作者：**Martin Kuppinger**

mk@kuppingercole.com

2019 年 11 月

目录

相关研究

执行观点：IBM MaaS360 with Watson - 79067

执行观点：IBM Cloud Identity - 79065

执行观点：IBM Security Access Manager (ISAM) - 79066

领导力指南：身份即服务 (IDaaS) - IGA - 80051

领导力指南：基础架构即服务 - 全球提供商 - 80035

领导力指南：访问管理和联合 - 71147

架构蓝图：混合云安全 - 72552

1 引言

在过去的几年里，网络安全已经从企业 IT 安全部门面临的一个技术挑战演变为业务领导者的一个主要关注点。从小型企业到全球领先企业，网络安全事件都会对其造成巨大破坏。了解企业整个 IT 格局中攻击的当前状态，同时快速识别并立即做出响应，对于减轻此类攻击可能造成的潜在损害而言至关重要。

另一方面，IT 基础架构从集中式内部数据中心到在本地环境和多云环境中运行的混合 IT 的演变，也增加了收集和处理相关数据的复杂性。DevOps 环境还为 IT 基础架构增加了新的易变元素。此外，容器化环境（尤其是在多云和混合场景中运行的情况下）也增加了复杂性，在此类环境中，甚至是业务关键工作负载也以非常敏捷的方式运行。

由于数据的监控和分析或事件响应的自动化不可能通过单个工具来实现，也增加了复杂性。大多数企业都有几种这样的工具，通过一种或多种此类工具来应对应用运行所在的每个环境。在这个混合世界中，与安全性相关的数据来自于多种来源，而很少或很多工具都会使用此类数据。安全性和威胁分析所用的许多数据源，以及使用和处理此类数据并帮助企业进行响应的许多系统都给企业带来了挑战。

构建流程并为其配备人员，以及构建为这种复杂环境提供支持的基础结构，已经变得极为困难。SOC (安全运营中心) 就是这方面的示例之一，它从混合、易变的分布式 IT 环境中收集所有相关数据。如此一来，便存在相关数据丢失、未及时识别事件导致响应失败这样的风险。此外，由于此类工具非常多样化，因此也难以实现统一、高效的响应。从组织和技术角度来看，事件响应都变得极为复杂。

网络安全必须解决当今 IT 环境的现实窘境和复杂性。将数据源与分析解决方案和事件响应解决方案进行点对点集成往往由于太复杂、成本太高、速度太慢而以失败而告终。因此需要确保所有相关源数据的可视性，使得系统可以基于此类数据高效地检测、识别和响应网络事件。

到目前为止，并未定义此类解决方案的明确类别，因为到目前为止，市场上还无法提供此类解决方案。尽管一些供应商自身的技术可提供良好的集成度或提供了分析应用接口，但到目前为止，仍旧缺乏一个涵盖针对相关来源和分析工具的广泛开箱即用集成的综合性集成框架。

IBM Cloud Pak for Security 是目前市场上的第一款开放平台，它支持与现有安全工具的集成，进而针对跨混合、多云环境的网络事件生成相应的洞察力。它是 IBM 推出的面向企业的容器化软件解决方案系列（Cloud Pak 系列产品）中的产品之一。

2 产品描述

IBM Cloud Pak for Security 平台旨在连接来自 SIEM、EDR、数据湖等不同工具的安全相关数据源。它可以访问来自各种来源的各种数据，而且可实现跨所有这些来源的同构访问。基于这一点，它可以将合并的信息传回到平台上的安全应用。此外，它可以编排事件响应工作流程，并实现手动任务和重复性任务的自动化。通过基于所有可用数据的协作，可以帮助安全团队更快地执行工作、做出响应，并进行更好的协调。IBM Cloud Pak for Security 旨在为集成式 SOC 和安全团队提供一个坚实的基础，从使用完全不同解决方案的不协调流程转变为协调的集成式响应。IBM Cloud Pak for Security 专注于促进可互操作性，并不是要替代现有工具成为“超级工具”，而是增强这些现有工具作为一个集成平台所能实现的价值。它是一个数据联合平台，目的在于提供跨多个工具的合并访问，而不是提供一个中央数据存储。如此一来，不仅可以帮助企业保留现有投资，还能够使安全团队应对异构 IT 环境的复杂性，以及所部署异构 IT 安全工具的范围。它为解决不断增长的网络攻击提供了一种更好的协调方法。

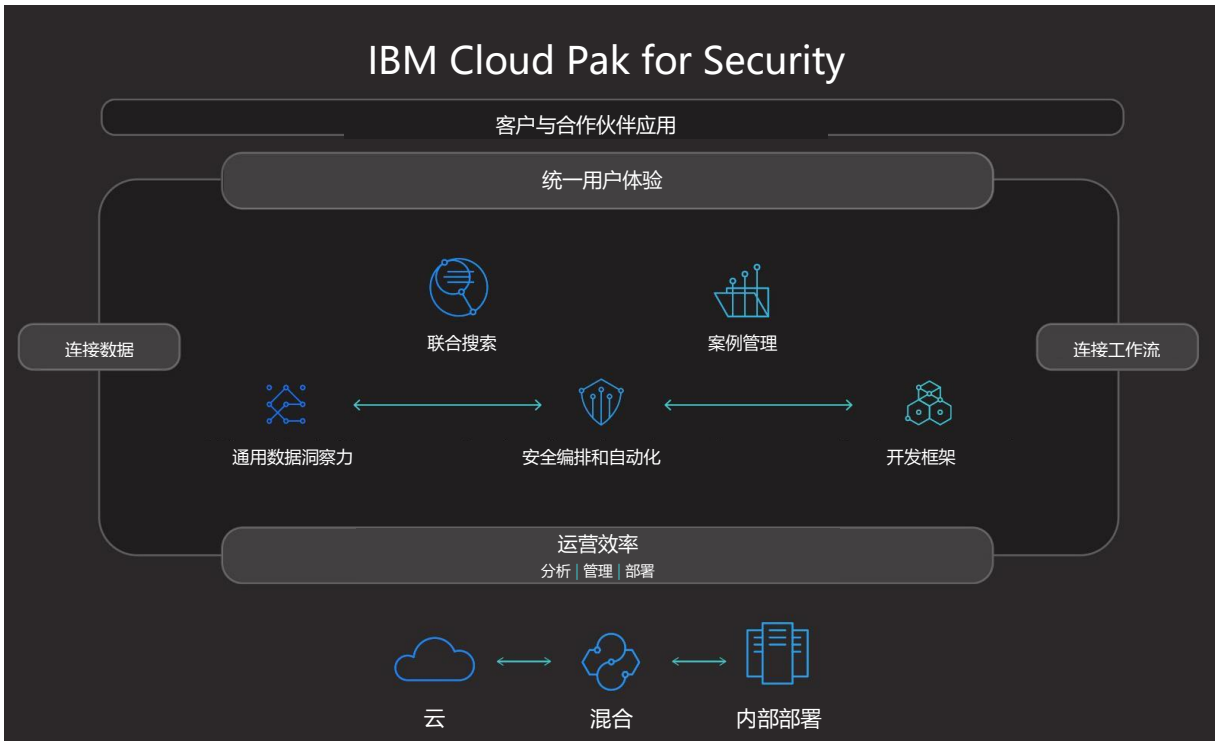

图 1：IBM Cloud Pak for Security 概述（本图经 IBM 许可后复制）

IBM Cloud Pak for Security 可在涵盖内部环境、私有云或公有云的混合环境中运行。它可以访问来自各种环境和源系统的数据，并且它是一个开放的环境，可以轻松连接多个安全工具。它专注于联合数据调查，以及跨各种安全工具编排流程和工作流。

IBM Cloud Pak for Security 采用混合多云方法，与其他最新发布的 IBM Cloud Pak 系列解决方案保持一致。所有这些解决方案都是基于 Red Hat OpenShift、面向容器平台和运营服务而构建，因此是自收购 Red Hat 以来，IBM 交付的首批具体集成之一。Cloud Pak 系列解决方案以 OpenShift 平台为基础，属于基于微服务的容器化解决方案，而且尽可能基于开源组件进行构建，不过会将这些组件扩展并组合为一个全面的打包解决方案。

IBM Cloud Pak for Security 会连接到大量工具。这些工具涵盖了网络安全工具市场中的许多相关供应商，例如 Splunk、Tenable、Carbon Black、Elastic、BigFix、AWS 或 Microsoft Azure 等。所有这些第三方解决方案都可以连接到 IBM Cloud Pak for Security，通过该平台的统一界面进行访问。您可以利用该平台的通用数据服务和开源代码技术访问安全数据，而且可以从单个位置进一步分析相关调查结果。

除了与数据源相集成之外，IBM Cloud Pak for Security 还可通过 API 和 UI 提供对此类信息的统一访问。在 API 访问方面，IBM Cloud Pak for Security 提供了自己的 SDK。使用该功能，企业还可以更轻松地构建自己的集成和应用。IBM 以开箱即用的方式所交付的重点功能包括：安全工作流、将多个现有解决方案编排到集成的工作流以及自动化支持。这些功能旨在实现更好、更高效的事件响应，这些也是当今企业及其 SOC 的关键需求。

IBM Cloud Pak for Security 的另一个关键功能是联合搜索，这是实现安全相关信息统一访问之后所带来的必然结果。基于这种联合搜索，您便可轻松地跨多种工具提取和分析信息。同样，IBM Cloud Pak for Security 并不会将数据移动到中央存储，而是将信息访问联合到一起。不过，如果可以跨所有数据中心和云服务在来自不同提供商的各种工具（以及此类工具的多个实例）中运行查询，便可大幅简化针对当今企业复杂 IT 环境的调查。

在 IBM Cloud Pak for Security 推出之初，它便受到了其他供应商的广泛支持，这不仅证明了这种方法的有效性，也证明了这是一个经过深思熟虑的集成平台，并非是现有投资的替代品。

IBM Cloud Pak for Security 尽可能基于开放标准进行构建，这与新解决方案的开源基础保持一致。该解决方案可以在各种平台上运行，包括内部环境、私有云和公有 IaaS 基础架构，例如 AWS、Microsoft Azure、Google Cloud Platform 或 IBM 自己的云平台。

3 优势和挑战

IBM 通过 IBM Cloud Pak for Security 为网络安全市场提供了一项重大创新，解决了三个主要问题：

- 当今 IT 环境不断增加的动荡性；
- 支持复杂的异构 IT 运营环境（即跨多个云平台的混合环境）的需求；
- 当今企业普遍部署了多个网络安全工具，但缺乏对数据和流程的集成。

基于 IBM 所选择的方法，企业可以更好地集成其现有工具和数据，而且可以轻松地构建和扩展其事件响应流程。借助 IBM 所选择的方法，企业可以保留其在现有网络安全解决方案上的投资，同时增加附加值。

我们预计，支持 IBM Cloud Pak for Security 的合作伙伴网络将会超过已有的令人印象深刻的初始合作伙伴名单。从竞争的角度来看，IBM Cloud Pak for Security 的最大竞争将来自于事件响应解决方案的供应商。不过，即使是这些解决方案，也可以基于 IBM Cloud Pak for Security 提供的集成和联合搜索功能进行构建。

总而言之，IBM Cloud Pak for Security 是一款备受许多企业关注的解决方案，尤其是那些运行有自己的 SOC 的企业。对于需要集成各种解决方案的 MSSP（托管安全解决方案提供商）而言，似乎也非常关注该款解决方案。我们强烈建议客户评估在其网络安全计划中使用 IBM Cloud Pak for Security 的可行性。

优势	挑战
• 该款解决方案是一款允许跨多种系统统一访问安全和威胁信息的独特产品； • 它拥有强大的合作伙伴生态系统，得到了大多数领先安全供应商的支持； • 它无需数据移动，而是通过数据联合避免形成新的数据孤岛； • 它提供了 SDK 和其他选项，可用于开发其他应用、构建灵活的事件响应工作流； • 它可在各种云环境中运行，支持企业的多云和混合需求； • 它采用基于微服务和容器化的现代架构。	• 尽管它被构建为可与任何第三方解决方案协同运行的更广泛平台，但容易与现有的事件响应解决方案相混淆 • 联合搜索功能能否成功实现取决于数据源的可用性。

4 版权

信息安全的未来 - 当前形势

KuppingerCole 在 IT 战略制定及相关决策流程方面具有深厚的专业知识，可为 IT 专业人员提供一流的支持。作为一家领先的分析机构，KuppingerCole 致力于提供第一手信息，不会偏向于任何供应商。我们的服务旨在帮助您轻松、安全地做出对业务至关重要的决策。

KuppingerCole 创立于 2004 年，是欧洲的一家领先分析机构，致力于确保传统环境和云环境中专注于身份的信息安全。KuppingerCole 以不偏向于任何供应商为原则，致力于提供针对信息安全市场细分领域的专业知识、思维领导力和观点，涵盖了所有的相关方面，比如身份和访问管理（IAM）、治理、风险管理与合规（GRC）、IT 风险管理、身份验证和授权、单点登录、联合、以用户为中心的身份管理、eID 卡、云安全和管理、虚拟化等等。

有关更多信息，请联系 **clients@kuppingercole.com**

KuppingerCole Analysts
AG Wilhelmstr.20-22
65185 Wiesbaden | 德国

电话：+49 (211) 23 70 77 – 0
传真：+49 (211) 23 70 77 – 11
www.kuppingercole.com