# IBM Security QRadar

## 集可视性、检测、调查和响应能力于一体

安全团队面临着各种各样的挑战：狡猾的网络攻击的数量不断增加；数据呈爆炸式增长；攻击面不断扩大；安全工具脱节；以及技能娴熟的安全人员匮乏。事实上，许多组织每周都要花费数百小时来调查可疑的警报，然而，尽管投入如此之多的时间，但仍有近 17% 的警报没有受到调查。[1] 因此，对于那些希望保护客户身份和知识产权并避免业务中断的组织而言，必须主动监控自身环境，以便在攻击者对其造成经济和声誉损失之前快速检测到威胁并准确做出响应。

IBM Security QRadar® 是市场领先的 SIEM 解决方案，通过将可视性、检测、调查和响应能力集于一体，帮助防范日益增长的威胁，同时实现安全运营现代化，并扩大其规模。QRadar 帮助安全团队集中管理企业范围的安全数据，针对最高优先级的威胁挖掘切实可行的洞察。安全分析人员可从一站式界面了解安全态势，发现最严重的威胁，并深入挖掘更多详细信息，这有助于简化工作流程，而且无需在不同的工具之间进行切换。利用 QRadar 的异常检测功能，安全团队可以快速发现用户行为的变化，从而及早揭示未知的威胁。

### 亮点

- 从一站式界面全面掌握安全数据
- 缩减事件规模，精简为最重要警报的优先列表
- 利用自动化的高级分析和威胁情报，加快调查速度
- 利用现成可用的用例和集成，实现快速扩展
- 加强合规性，管理监管风险

1 IDC，“Insights from IDC’s EDR and XDR 2020 Survey: Operational Challenges and Initiatives Are Abundant”，文档号 US47357921，2021 年 1 月

该解决方案从整个企业范围采集海量数据，帮助用户全面了解本地和云环境中的活动。采集数据后，QRadar 可应用自动化的实时安全情报，快速准确地检测威胁并确定其优先级。切实可行的警报为潜在事件提供丰富的背景信息，使安全分析人员能够快速做出响应，最大程度限制攻击者造成的影响。QRadar 是专为满足广泛的安全用例而构建的，可以轻松扩展，只需少量的定制工作。

## 获得全面、集中的可视性

企业网络可能覆盖传统的本地 IT、云环境和运营技术 (OT) 环境，所有这些环境都需要某种程度的监督，以有效保护资产、准确检测威胁并保持合规性。安全团队必须首先集中掌握不同的安全数据，才能开始分析数据以检测和应对威胁。QRadar 帮助组织收集、解析和标准化日志和流数据，全面集中地了解各个孤岛环境的状况。安全分析人员可通过一站式界面监控本地环境、云环境和混合环境。

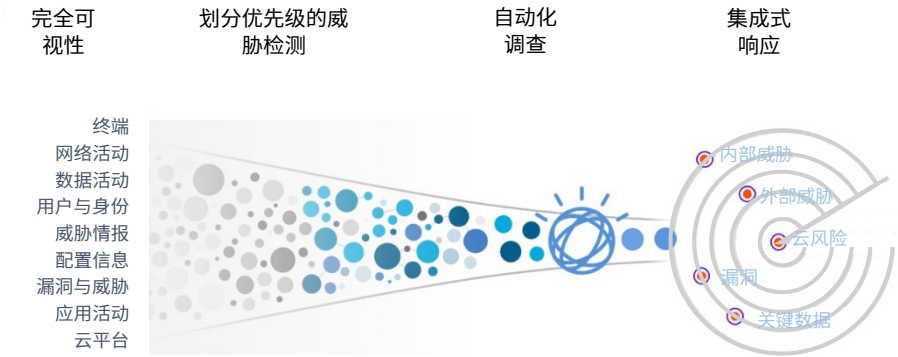
该解决方案包含超过 450 个预先构建的“设备支持模块”(DSM)，提供与其他安全投资的默认设置集成。客户只需将日志指向 QRadar，该解决方案就可以自动检测到日志源类型，并应用适当的 DSM，对日志数据进行解析，并使其标准化。因此，相较于其他解决方案，QRadar 客户的动作要快很多。其他集成可通过 IBM Security App Exchange 中的应用轻松添加。QRadar 还提供一个简单的 DSM 编辑器，具有直观的图形用户界面 (GUI)，使安全团队能够轻松定义如何解析自定义应用中的日志。

为了帮助组织轻松建立资产数据库，从而能够定义关键资产或网段，QRadar 还会检查网络流数据，以根据使用的应用、协议、服务和端口，自动识别网络上的有效资产并对其分类。

QRadar 支持范围广泛的技术、应用和云服务，帮助客户全面了解企业范围的活动。将这些数据集中起来之后，QRadar 就可以执行自动分析，以发现已知的威胁、可能预示未知威胁的异常，以及可能导致敏感数据泄露的严重风险。

## 自动提供安全情报，快速检测威胁

QRadar 能够自动分析和关联多个数据源中的活动，这些数据源包括日志、事件、网络流、用户活动、漏洞信息和威胁情报，从而发现已知和未知的威胁。

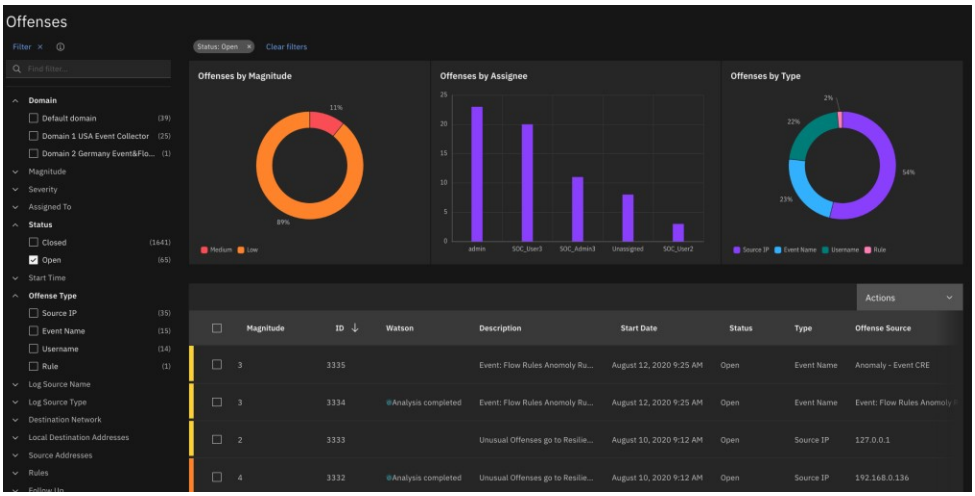



QRadar 可从各种各样的来源收集、分析和关联数据，以检测需要调查的最严重的威胁，并对其划分优先级。

QRadar 可以智能化地关联和分析来自各种数据源的各种类型的数据，包括：

- 终端数据：来自 Windows 事件日志、Sysmon、EDR 解决方案等
- 网络活动数据：来自防火墙、网关、路由器或传感器
- 漏洞数据：来自杀毒工具、漏洞扫描程序、入侵检测系统、入侵防御系统、数据丢失预防系统等
- 云活动数据：来自 SaaS 和 IaaS 环境，如 Office365、SalesForce.com、Amazon Web Services (AWS)、Microsoft Azure 和 Google Cloud
- 用户及身份数据：来自 Active Directory、LDAP 或其他身份和访问管理解决方案
- 应用数据：来自企业资源规划（ERP）解决方案、应用数据库、SaaS 应用等
- 威胁情报：来自 IBM X-Force® 和第三方威胁情报订阅源
- 容器活动数据：来自容器管理和统筹技术软件，如 Kubernetes

QRadar 包含数百个预先构建的安全用例、异常检测算法、规则和实时关联策略，用于检测已知和未知的威胁。发现威胁后，该解决方案将相关的安全事件整合为称为“攻击”的单一警报列表，并划分攻击的优先顺序。该解决方案根据威胁的严重性和所涉及资产的关键程度，自动对攻击划分优先级。




QRadar 中的“攻击”视图提供了划分了优先级的威胁列表

安全分析人员可在一站式界面中，查看每次攻击的完整威胁活动链。分析人员可轻松地深入研究特定事件或网络流，以展开调查，将攻击分配给特定的分析人员处理，或将其关闭。当发生新的相关活动时，攻击会自动更新，因此分析人员随时都可以看到最新信息。这种独特的方法为每个潜在事件提供端到端洞察，同时减少警报总量，从而帮助安全分析人员轻松了解环境中最严重的威胁。

## 发现异常的网络、用户和应用活动

随着攻击者的手段越来越狡猾，只检测已知威胁已经不足以保护环境了。组织还必须能够检测网络、用户或系统行为的细微变化，因为这些变化可能预示着未知的威胁，例如恶意的内部人员、凭证被盗用或无文件式恶意软件。

QRadar 包含多种异常检测功能，可发现行为变化，从而尽早锁定未知威胁。QRadar User Behavior Analytics 用于分析用户活动，旨在发现恶意内部人员，确定用户的凭证是否已被盗用。安全分析人员可以轻松了解存在风险的用户，查看他们的异常活动，并深入研究涉及用户风险的底层日志和流数据。

通过选择 QRadar Network Insights 作为 SIEM 部署的一部分，组织可以深入了解哪些系统彼此通信、涉及到哪些应用，以及数据包中交换了哪些信息。通过将这些信息与其他网络、日志和用户活动关联在一起，安全分析人员可以发现异常的网络活动，这些活动可能预示着主机或用户受到攻击，或者数据有泄露的可能。

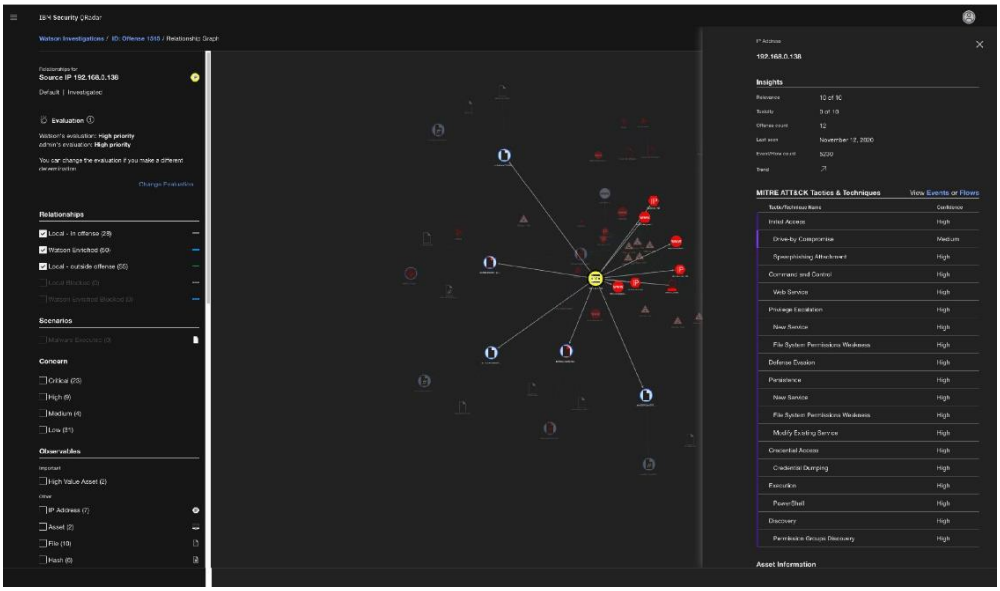
作为默认设置，QRadar 随附多项异常和行为检测规则，安全团队也可创建自己的规则，自定义异常检测设置，以及从 IBM Security App Exchange 下载超过 265 个预先构建的应用以增强部署。

## 利用 AI 和自动化，加快调查速度

大量的警报、繁琐的人工任务和有限的人手让安全团队不堪重负，经常导致组织的安全态势变得岌岌可危。QRadar Advisor with Watson™ 使用 AI 和自动化技术，显著减少了调查威胁警报所用的时间 — 从几天或几周减少到几分钟或几小时。Advisor 提供划分了优先级的警报研究和相关数据，使分析人员能够集中精力执行更有影响力的战略分析和威胁搜索，同时使用业界标准的 MITRE ATT&CK 映射来改进根本原因分析。这样就能够更快地修复漏洞，缩短业务停顿时间，减少错失的关键事件，降低分析人员的疲劳程度，以及提高 SOC/分析人员的效率。

QRadar 可对一次攻击中的所有相关事件进行分组和划分优先级，从而帮助安全分析人员全面了解不断发展的攻击场景。交叉调查分析通过在相互联系的事件中自动关联调查，提供有关警报的丰富背景信息，从而减少重复工作，并将调查扩展到当前可能的事件和警报之外。

此外，Advisor with Watson 将认知洞察和本地数据挖掘结合在一起，旨在发现关联的攻击迹象 (IOC)。QRadar 可在调查中绘制关系图，以直观呈现经过扩充的调查数据，并探索与其他 IOC、资产、用户或调查的联系。




QRadar 可以绘制 IOC、资产、用户或其他调查之间的关系图

Advisor 还可将调查映射到 MITRE ATT&CK 框架，以使安全团队能够直观了解攻击者的战术和方法，按 ATT&CK 阶段深入研究事件和流程，并更有信心地做出决策。

## 通过有指导的响应和案例管理，加快响应速度

IBM Security QRadar 通过与 IBM Security SOAR 集成，可以为安全团队提供逐步演练手册，使人工任务实现自动化，确保与案例管理团队开展协调一致的协作，从而加快事件响应速度。安全分析人员可以快速高效地将可疑攻击从 QRadar 升级到 IBM Security SOAR，触发额外的自动化扩充功能，推动整个调查过程加速实施。随着事件的发展，所有信息都会在 QRadar 和 IBM Security SOAR 之间同步，完全确保数据的完整性。IBM Security SOAR 发现的任何新信息都会反馈到 QRadar，以改进检测流程。

## 利用预先构建的内容、规则和报告，更好地管理合规性

QRadar 提供了透明度、问责机制和可衡量性，这对于组织成功地满足法规要求和报告合规情况而言至关重要。该解决方案能够关联与整合威胁情报订阅源，为审计人员提供更完整的 IT 风险报告指标。该解决方案预先构建了数百个报告和规则模板，可帮助组织更轻松地满足行业合规要求。

一系列网络资产可按业务职能分组（例如，受 HIPAA 法案合规审计约束的服务器），以帮助团队更轻松地根据需要报告相关活动。

QRadar 具有丰富的经验和资源，针对《通用数据保护条例》(GDPR)、《联邦信息安全管理法案》(FISMA)、《萨班斯-奥克斯利法案》(SOX)、《健康保险可移植性和责任法案》(HIPAA)、ISO 27001、《支付卡行业数据安全标准》(PCI DSS) 等法律法规提供默认设置合规数据包，帮助组织消除风险和法规漏洞。这些数据包免费提供，可根据 QRadar 许可证使用，可从 IBM Security App Exchange 获取。

## 轻松扩展，满足不断变化的需求

QRadar 采用可扩展的灵活架构，可满足不同规模的企业的各种需求。规模较小的组织可从单一的一体化解决方案着手，随着需求的发展，轻松升级到分布式部署。规模较大的企业组织可以部署专用组件，以支持具有海量数据的全球分布式网络。

IBM Security QRadar 包含以下组件：事件收集器、事件处理器、流收集器、流处理器、数据节点（用于低成本存储和提高性能）以及中央控制台。所有组件都可作为硬件、软件或虚拟设备的形式提供。软件和虚拟设备选项可部署在本地或 IaaS 环境中，也可分布在混合环境中。

无论采用哪种部署模式，组织都可以在需要的地点和时间，选择添加高可用性和灾难恢复保护功能，以帮助确保运营的连续性。对于希望增强业务弹性的组织，QRadar 可提供集成式自动故障转移和系统间全盘同步功能，无需额外的第三方故障管理产品。对于希望获得数据保护和恢复能力的组织，QRadar 的灾难恢复功能可将实时数据（如流和事件）从主 QRadar 系统转发到位于独立场所的辅助并行系统。

## 结束语

IBM Security QRadar 是市场领先的 SIEM 解决方案，它将自动化的智能分析应用于海量安全数据，为安全分析人员提供有关最严重威胁的切实可用的洞察，使他们能够更快地做出更明智的分类和响应决策。

这种全面的解决方案将日志管理、网络分析、用户行为分析、威胁情报和基于 AI 的调查整合到单一解决方案中，并与 IBM Security SOAR 集成以提供事件响应能力，实现覆盖本地、云和混合环境的全面可视性。

## 为何选择 IBM?

IBM Security 提供业界最先进的集成式企业安全产品与服务组合之一。该组合由世界知名的 IBM X-Force® 研究作为强大后盾，提供安全解决方案，帮助组织将安全纳入业务架构，确保在充满不确定性的市场环境中蓬勃发展。

IBM 运营着全球最广泛、最深入的安全研发和交付组织之一。IBM 每月在 130 多个国家或地区监控超过 1 万亿起事件，拥有 3000 多项安全专利。要了解更多信息，请访问 ibm.com/security。

## 更多信息

如欲了解有关 IBM Security QRadar 的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：
https://www.ibm.com/security/security-intelligence/qradar

---



---

所有关于 IBM 未来方向或意图的声明随时可能发生变更或撤销，恕不另行通知，它们仅仅表示目的和目标而已。