IBM QRadar Network Insights

通过智能网络流量分析实时检测威胁

亮点

- 使用深入的数据包检查来识别高级威胁和恶意内容
- 实时检测钓鱼攻击、恶意软件入侵、横向移动攻击和数据外泄
- 记录应用活动，捕获工件并识别参与网络通信的资产、应用和用户
- 通过第 7 层内容分析来获得高级安全洞察力
- 将经扩展的网络和文件元数据添加到 IBM QRadar SIEM

当今的高级威胁比以往任何时候都要复杂，而且难以检测。它们隐藏在日常网络流量中。这些流量通常来自于应用、网站、电子邮件和文件传输。恶意攻击实施者一旦侵入网络后，他们就会在您的网络上隐秘地进行横向移动，收集您的宝贵数据，以达到数据外泄的目的。不幸的是，威胁检测解决方案通常缺乏解决网络安全挑战所需的速度、深度和情境。日志和网络流很重要，但通常无法在整个生命周期内确保足够的威胁可视性。此外，数据包捕获数据主要用于事后取证分析，而不是用于实时检测威胁。最后，孤立的网络分析部署与安全解决方案的大规模（且通常是地域分散的）部署之间的集成也较为有限。

借助 IBM QRadar Network Insights (QNI)，QRadar 客户可以实时、深入地了解网络通信。如此一来，恶意活动便会在网络中无所遁形，而且有助于捕获威胁，进而避免威胁或最大程度地降低威胁的影响。您可以收集基本威胁指示器，以及与应用、资产、工件和用户有关的活动信息。借助 QNI，组织可以在高级威胁、钓鱼电子邮件、恶意软件、数据外泄、横向移动、合规缺口以及 DNS 和其他应用滥用对其造成损害之前对其进行检测和分析。

与 QRadar 的无缝集成还能够让网络分析成为安全运营人员的一项重要增值。他们可以通过关联网络洞察力与日志和事件数据来识别威胁，还可以使用最新威胁情报信息进行分析来揭示隐藏的攻击。QRadar Network Insights 还可以重建和分析会话内容，进而构建一个取证信息存储库，还可以获得应用级数据，用以在元数据中添加情境信息。他们可以自动对可疑内容进行全面分析，同时进行有针对性的数据提取，进而使借助传统方法无法检测到的威胁和恶意活动无所遁形。Network Insights 还可以建立正常的使用模式，以帮助他们检测可能属于内部威胁迹象的异常。

QRadar Network Insights 使用深度数据包检查来分析流入网络或在网络内部流动的数据，并实时查找已知威胁和恶意活动。一旦它识别出了威胁、恶意软件或潜在数据丢失，就会在 QRadar 中生成攻击信息，以便相关人员快速采取后续措施。

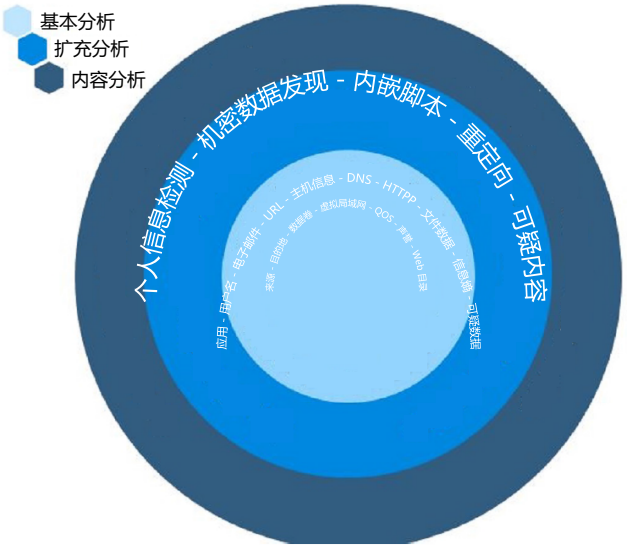
QRadar Network Insights 支持的用例

组织目前所面临的挑战	
横向移动攻击检测	跟踪异常通信 - 侦查、数据传输、流氓软件和恶意攻击者
恶意软件检测和分析	观察和分析工件 - 名称、属性、移动、可疑内容
钓鱼电子邮件和活动识别	预先制止并做出反应 - 通过分析来源、目标、主题和内容来处理恶意电子邮件
内部人员威胁	识别高风险用户 - 钓鱼攻击、负面情绪和可疑行为的目标
识别合规缺口	持续监控 - 与企业策略、行业策略和法规的合规性
数据外泄检测	识别和跟踪文件 - DNS 异常、敏感内容、异常连接、别名

来源 - 目的地 - 数据卷 - 虚拟局域网 - QOS - 声誉 - Web 目录

您可以配置和自定义 QRadar Network Insights 所提供的内容分析级别，包括：

- 基本流洞察力 - 包含来源和目的地信息、网络协议、字节/数据包计数、第一个/最后一个数据包的时间、QoS、虚拟局域网信息、Web 目录和 IP 声誉。
- 扩充流洞察力 - 应用识别、用户名、电子邮件和图表 ID、URL、搜索参数、主机信息、HTTP 分析、DNS 查询/响应、文件信息（名称、类型、大小、哈希值、信息熵）、可配置的可疑内容
- 内容流洞察力 - 个人信息检测、机密数据检测、内嵌脚本、重定向、可疑内容



QRadar Network Insights 使用深度数据包检查来分析数据流、端口使用情况、文件类型和传输内容，以检测已知威胁。此外，由于 QNI 使用的是实时深度数据包检查（而非数据包捕获），因此它仅会提取和存储相关的有效负载信息。此类数据加上预定义的签名可用于检测恶意软件和钓鱼攻击，而且所收集的信息（如用户 ID、消息和文件）可用于构建一个元数据池，您可以快速对该元数据池进行搜索和检查，以支持恶意活动的快速响应。

QRadar Network Insights 包含有开箱即用的智能功能，这些功能可帮助您立即自动发现恶意内容，进而快速实现价值。QNI 能够为安全团队提供用户身份验证凭证、近期通信信息，以及进出网络的可疑流量的活动详情。通过这种方式，QNI 可以确定所发生攻击的类型，确定受影响的系统或数据，同时支持快速调查和采取纠正措施。

有关更多信息

如欲了解有关本产品的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：ibm.com/cn-zh/security

良好的安全实践声明：IT 系统安全涉及通过对来自贵企业内外部的非法访问进行阻止、检测和响应来保护系统和信息。非法访问会导致信息变更、损毁、盗用或滥用，或导致对您的系统的破坏或滥用，包括用于对他人的攻击。没有任何 IT 系统或产品可被视为完全安全，也没有单一产品、服务或安全措施可完全有效地阻止非法使用和访问。IBM 系统、产品和服务设计为合法、全面的安全方法的一部分，该方法必然涉及其他操作程序并可能需要其他系统、产品或服务，以达到最大效力。IBM 不保证任何系统、产品或服务可免受，或使贵企业免受任何一方的恶意或非法行为的影响。

IBM Corporation
Software Group
Route 100
Somers, NY 10589

美国印刷
2016 年 12 月

请回收利用