QRadar Network Insights
以独特的方式交付实时洞察力

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) 白皮书

专为 IBM 而编制

2017 年 3 月

EMA™ *IT 与数据管理研究、行业分析与咨询*

QRadar Network Insights 以独特的方式交付实时洞察力

目录

QRadar Network Insights 以独特的方式交付实时洞察力

概要

如今，安全事件的检测和解决需要比以往更快的速度，也需要更多的数据。从传统上来说，应对这两个挑战会使安全团队意见相左。若要以足够清晰和详细的方式解决事件，确保事件不是误报，同时为分析人员提供充足的详细信息，使事件得到妥善解决，意味着需要由专家深入分析事件，以从中检索必要的数据。这一调查过程可能需要数小时到数天的时间才能完成，而若要加快响应速度，则意味着缩减甚至提前进行深入的调查，以处理手头的问题。

安全运营团队每天都面临着两个相互矛盾的选择 - 是节省时间还是通过深入调查获得详细的情境信息，而且通常他们还必须决定哪个选择更为重要。为了帮助企业解决这一问题，IBM 推出了 QRadar Network Insights (QNI)。QNI 解决了安全运营团队所面临的两难选择，既能够加快事件响应速度，缩短驻留时间并降低事件的总体影响，还能够收集足够的情境信息，确保分析人员了解事件的实情，并拥有妥善解决问题所需的信息。QNI 提供了捕获数据包流的能力，实时剖析其中的可疑内容，然后使用经扩充的内容来增强 QRadar 中的数据。

本文讨论了 QNI 所用方法的相关性、QNI 所用技术的优势、QNI 的技术差异化优势，以及围绕其功能需求的几个主要用例。

QNI 在识别攻击和泄露方面的价值

对于经验不足的安全专业人员而言，他们要了解的第一件事就是，无论在何处发生什么事情，超过 99% 的攻击都会在网络上留下痕迹。问题在于：“安全和/或网络团队是否做好了充足的准备来捕获这些痕迹？”除了内部攻击者收集本地系统数据并将其复制到可移动媒体，抓取屏幕截图并予以记录或在本地进行打印之外，所有的其他攻击活动都会在网络中留下足迹。通过电子邮件或 Web 交付、攻击命令和控制、侦查方法以及跨系统数据收集所进行的攻击都会留下网络工件。

这就是我们为何要使用 IBM® QRadar Network Insights® (QNI™) 的原因所在。IBM 认识到，安全运营团队需要持续收集网络遥测数据并提供对这些数据的分析结果，如此才能将其与其他日志工件进行实时整合。为了实现这一方法，QNI 解决了几个一致的问题。

提升情境与可视性

上一节所述的各种因素会由于一些常见工具的不足而加剧。安全人员表示，他们在获取情境信息及获取环境可视性方面的能力会受到多个因素的影响：

1. 百分之六十五 (65%) 的受访者表示，他们的工具缺少进行数据耦合以实现关联和分析所需的集成件或 API。
2. 百分之三十八 (38%) 的受访者表示其管理控制台所提供的信息不足。
3. 百分之三十七 (37%) 的受访者表示其报告工具所提供的信息不足。

大多数警报都是作为严重警报和关键警报而创建的；由于缺乏前期分析，在实际操作中，关键警报最终都淹没在庞大的警报“海洋”中。这就像一句古谚语所说的那样：“如果一切都是重点的话，也就无所谓重点了。”造成这种情况的直接原因在于缺乏高质量且及时的数据以及适当的前期分析。

QRadar Network Insights 以独特的方式交付实时洞察力

线速度的详细数据包剖析

尽管各种 IDS 和 IDP 技术似乎在很早以前就解决了数据包剖析问题，但如果将它们与 QNI 进行逐功能对比的话就会发现事实并非如此。尽管 IDS 和 IDP 传感器也能够拆分数据包，但它们在指定时间内处理信息的方式却与 QNI 大不相同。首先，内联部署的 IDS 和 IDP 会在短短几毫秒的时间内准予通过或做出决策，因此它们无法以与 QNI 相同的级别对每个数据包进行剖析。由于 QNI 以被动模式部署，只会嗅探数据包而不是截获数据包，因此能够显著增加在评估数据包的内容和情境信息上所投入的时间。除了基本的常见功能（如协议识别、IP 报头解析、字节和数据包计数、会话定时、VLAN 信息以及针对数据包的攻击行为评估等）之外，令 QNI 在同类产品中脱颖而出的功能还包括：

1. 将实时的应用级洞察力运用到会话和数据的情境中。
2. 实时深度内容分析（大多数 IDS/IPS 产品无此功能）。
3. 在前端实时进行多会话工件分析、关联并创建全面的相关元数据，以减少误报并增强事件分类。
4. 提供可由运营人员定制的可疑数据供应，以增强监控、持续调查和追溯分析功能（通过 YARA 规则进行配置）。
5. 通过资产、应用和用户的情境信息识别恶意内容。
6. 开箱即用的内容使得 QRadar 可以利用 QNI 的数据对关键用例进行高级检测，包括钓鱼攻击、横向移动和数据外泄等。
7. 基于实时网络活动来洞察用户和应用行为，有助于实现更深入的内部威胁检测。

这些数据可用于增强 QRadar 对相关警报的优先排序，以引起运营人员的注意，还可以添加到事件中，以加快警报处理的研究和解决流程。

QNI 可以在创建事件时交付广泛的已扩充元数据

元数据对于数据泄露调查的成功而言至关重要。EMA 的研究人员就元数据对安全事件调查的重要性对安全专业人员进行了调研。百分之七十四 (74%) 的受访者表示，元数据对于安全事件调查而言非常重要或至关重要。

QNI 不仅能够交付从协议、数据包、会话和应用信息中提取的主要数据，还会创建大量的元数据添加到 QRadar 的数据存储库中。QNI 实际上会生成数十种元数据。在下文中，EMA 列出了 QNI 针对事件的初始评估而提供的一些最有趣和有用的数据：

1. 与主机和会话相关的 DNS 信息
2. 会话中涉及的 HTTP 元数据、URL 和重定向
3. 文件数据、文件哈希值、文件信息熵（尤其是图像文件和音频文件）
4. 电子邮件服务器使用信息、发送者和接收者、主题行及文件附件（按类型）
5. 基于已定义的标准检测到的 PII 和机密数据
6. 检测到的内嵌脚本
7. 已知资产标识信息

一旦分析了这些元数据并将其输入到 QRadar，分析人员便可获得深层网络数据，用以检测高级威胁、执行历史分析，以及利用 IBM 提供的更多分析功能来改善其安全态势。

QRadar Network Insights 以独特的方式交付实时洞察力

QNI 改变了防御模式（从被动防御到主动防御）

EMA 通过调研发现，只有 14% 的组织在所有调查中使用了完整的数据包数据。这一状况是由两个问题造成的。首先，完整的 DPI 工具成本非常高昂，不仅捕获功能非常昂贵，而且获得全部价值所需的分析工具也非常昂贵。其次，即便是对于小型组织而言，存储持续收集的完整数据包检查信息所需的成本也会是一个天文数字。

大多数完整数据包检查的实施中面临的另一个问题是完整数据包检查系统无法实时提供信息，即便它们在事件发生时正在运行，也无法做到这一点。分析人员必须单独访问系统才能导入数据。在数据自动导入到中央数据存储库的情况下，也是分批导入，而非流式导入；此外，分析人员还必须通过创建和执行查询将数据与其他日志信息缝合到一起。同样，这也仅支持事件/泄露发生后的取证方法。这也暴露出安全运营的另一个障碍。如果完整数据包检查系统是一个单独的系统，或需要手动导入数据，那么将会耗费宝贵的调查时间。

在事件调查过程中引入经过扩充且通过情景信息进行了增强的数据，可为 SOC 带来诸多运营优势。首先，它有助于加快事件检测和响应速度。通过提升可视性，使您可以发现以前不可见的低速和慢速攻击、多阶段攻击以及其他形式的攻击。以前隐藏在 Web、电子邮件和文件传输等正常应用流量中的威胁，现在也可以更容易地识别。使用多态代码、有效负载轮换以及其他手段来躲避基于签名的检测的攻击，也将会变得无所遁形。此外，滥用 DNS 和 HTTP 流量来躲避检测的攻击也不再成为威胁。

由于运营人员可以更快地收到更多遥测信息，因此在早期阶段（例如侦查阶段或泄露早期阶段），攻击会被中和，从而消除或大幅缩短攻击者的驻留时间。反过来说，如果确实发生了泄露，即使是在全自动攻击中，也能够大幅减少甚至是消除攻击通过横向移动扩大影响范围的机会。一旦减少了泄露的影响范围，便意味着调查和补救所需的人力也会更少。所有这些因素相结合，便能降低泄露事件的机会成本和实际成本。

QNI 会首先获取数据，然后对其进行预处理或预分析，再将其实时注入到 QRadar 中。它所呈现的元数据包括攻击的网络组件，以及 QRadar 中已经存在的应用、系统和用户相关信息。这些信息为 SOC 提供了一个优势，即在事件*开始*时（而非结束时）便可拥有详细程度更高的数据！

QNI 可为安全运营提供的价值

及时获取适当的数据

安全团队面临的另一个重要问题是如何在适当的时间获取适当的数据。对于数据泄露检测而言，需要在一开始就拥有准确的情境数据。如果在一开始时就能提供此类数据，便可提升事件分类的准确性，也有助于更快速、更高效地解决事件。不同的工具、数据处理系统和交付架构在数据的及时性方面会有很大差异。这通常意味着数据是在事件生命周期的后期交付的。尽管数据在泄露后取证流程的后端也会非常有用，但如果缺乏对收集到的数据进行前端集成分析，就会限制其在前端的作用。百分之五十八（58%）的安全人员在 EMA 调研时表示，他们的工具集没有足够的分析功能来提供适当的数据相关性；因此，他们必须耗费大量的工时进行人工研究和分析。

QNI 以线速度运行，可进行水平扩展，以满足更大的处理需求。

SOC 挑战

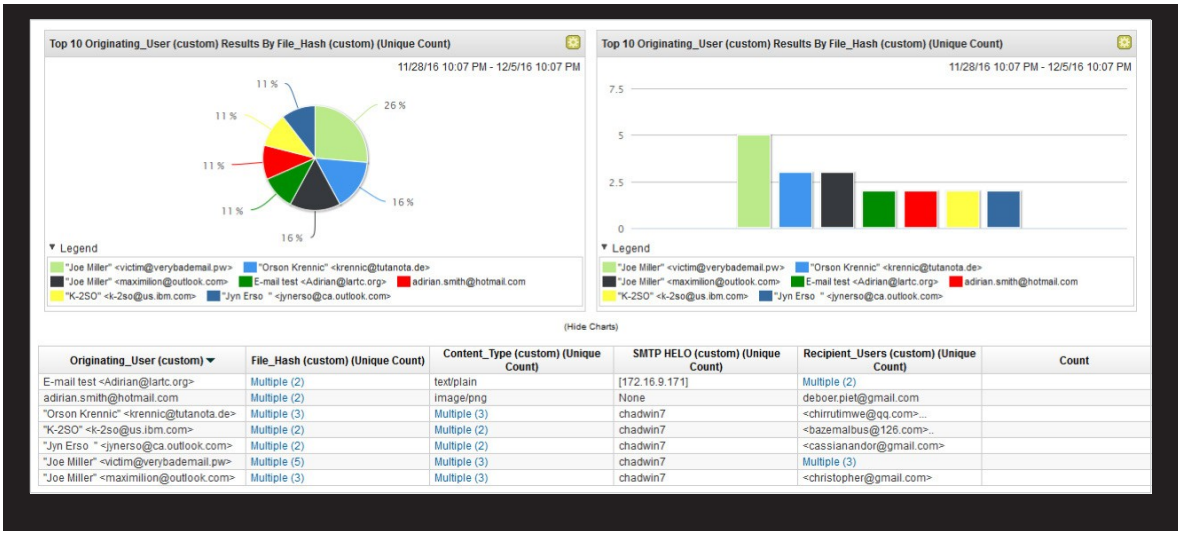
QNI 对于整个 SOC 而言都极具价值。每个运营角色都可以利用 QNI，而且理应如此。无论是通常负责初始事件分类的一线运营人员，还是负责威胁捕获的四线高级分析人员，都可以从 QNI 中获取价值。

对于一线运营人员来说，早期分析和数据扩充意味着他们收到的误报更少，而且能够收到经过更好的优先排序/分类的警报。拥有更高质量的事件相关数据还意味着分析人员可以更快地访问关键数据。一线运营人员所看到的改进包括：事件数量更少、事件响应速度更快、事件处理更高效。

二线和三线运营人员会发现工作交接环节变得更少。借助经增强的事件数据、可定制的数据馈入以及可自动化的数据收集，这些宝贵的运营资源可以减少他们在收集所需数据上所耗费的时间。如此一来，他们便可对复杂事件进行更快、更准确的诊断，进而加快一次解决问题的速度。

借助经扩充的数据，四线运营人员可以深入分析文件和内容，以区分正常活动和可疑活动。他们还可以识别与事件或泄露有关的人员、时间和方式。这样一来，他们就能快速关联数据相关性，加快调查速度，并将以前由于数据不可用而被视为不相关的事件关联起来。通过快速关联数据相关性，运营人员可以更好地识别隐匿的泄露尝试并量化泄露的范围。这样就减少了攻击者实施攻击的机会。

QNI 的关键用例



Originating_User (custom)	File_Hash (custom) (Unique Count)	Content_Type (custom) (Unique Count)	SMTP HELO (custom) (Unique Count)	Recipient_Users (custom) (Unique Count)	Count
E-mail test <Adirian@lartc.org>	Multiple (2)	text/plain	[172.16.9.171]	Multiple (2)	
adirian.smith@hotmail.com	Multiple (2)	image/png	None	deboer.piet@gmail.com	
"Orson Krennic" <krennic@tutanota.de>	Multiple (3)	Multiple (3)	chadwin7	<chirrutimwe@qq.com>...	
"K-2SO" <k-2so@us.ibm.com>	Multiple (2)	Multiple (2)	chadwin7	<bazemalbus@126.com>..	
"Jyn Erso " <jynerso@ca.outlook.com>	Multiple (2)	Multiple (2)	chadwin7	<cassianandor@gmail.com>	
"Joe Miller" <victim@verybademail.pw>	Multiple (5)	Multiple (3)	chadwin7	Multiple (3)	
"Joe Miller" <maximilion@outlook.com>	Multiple (3)	Multiple (3)	chadwin7	<christopher@gmail.com>	

图 1 带有 QNI 增强数据的 QRadar 仪表板

网络钓鱼攻击

对针对企业实施的所有攻击中，有 95% 来自于成功的鱼叉式钓鱼攻击。这些包含有恶意链接和附件的电子邮件会诱使收件人点击它们。如果收件人点击的话，用户将会受到损害，而攻击者也会顺利实施攻击。

QNI 能够检测、提取和分析电子邮件发件人域、主题行、内嵌链接以及附件内容和哈希值等信息，进而使 QRadar 能够在用户访问其收件箱之前检测出钓鱼攻击活动。

内部人员威胁

在过去的几年里，内部威胁作为一种威胁向量获得了广泛的关注。实际上，尽管内部威胁是一个严重的问题，但不诚实员工的数量并没有增加。更大的问题在于内部人员的身份由于各种手段而受到损害，导致外部威胁实施者可以伪装成可信的内部人员，进而利用合法身份进行侦查、横向移动，并最终进行数据外泄。

为了解决这一迫在眉睫的问题，QNI 会收集与单个活动有关的网络活动数据，包括未经批准的 Web 浏览或搜索、对存在危险的域或可疑域的访问，进而解决由可疑内容触发的别名和特权身份，同时将活动详细信息提供给 QRadar 以进行指示异常行为的用户行为分析。一旦确定了存在异常行为，便会将这些有风险的用户放置在仪表板上，跟踪他们的活动，直到不再存在风险为止。

横向攻击移动

几年前，运营人员以攻击者升级到管理员特权并在系统中或针对系统执行“操作”的速度作为判断攻击成功与否的标准。如今，如果确实需要调用管理员级别访问权限的话，许多攻击会集中精力躲在雷达下收集信息，最大程度地提升其收集数据的效率。网络环境中的大多数数据都可供普通用户使用，因此攻击者无需提升特权便可达成目标。

在侵入到网络后，他们需要继续探索和了解与网络环境相关的更多信息，以强化其系统的立足点和数据收集能力。QNI 能够识别此类行为并对其进行分类。它能够深入分析设备间的通信，检测表明存在恶意横向移动的侦查、支点攻击和设备间传输。无论横向移动的开始方式如何，它们都必须要穿越网络才能实现，而 QNI 则会一直对网络进行严密分析。之后，详细的分析信息将会发送到 QRadar，用于创建新事件或确认之前存在的事件，以便分析人员立即做出响应。

恶意软件和勒索软件检测与分析

当攻击者将恶意软件发送到目标系统时，QNI 会一直监控和分析数据流，以识别威胁。QNI 了解每个文件的详细信息，包括文件名、文件类型、信息熵、内嵌脚本和文件哈希值、文件来源和发送目的地等。通过将此类信息提供给 QRadar，同时借助 X-Force Exchange 的威胁情报，便可清楚地看出恶意软件何时避开了其他检测方法。如此一来，便可减缓网络环境中恶意文件所有实例带来的威胁。

在勒索软件完成对所连接存储的加密并危害到其他系统之后，它才能达到最大效果（即获得最大的勒索收益）。为了侵入其他系统，勒索软件会通过侦查来找到目标系统，并借助已受感染用户的权限来连接并感染环境中的其他系统。QNI 结合采用针对钓鱼攻击、内部威胁、横向攻击活动、恶意软件的检测方法来识别勒索软件攻击活动。

数据外泄

现如今，大多数攻击的最终目标都可以归结到某种形式的金钱收益，这其中便涉及到数据捕获。若要通过数据获得金钱收益，勒索软件必须从环境中提取数据，而不是对其进行加密。QNI 会对此进行密切监控。在剖析网络对话时，它会识别敏感数据，并通过电子邮件、聊天消息、文件上传、社交媒体等方式离开网络，而且所有操作都是实时进行的。IT 人员甚至可以检测出以非标准格式和协议（如异常 DNS 有效负载）隐藏的数据。如果攻击者获得了适当的访问权限，则 IT 人员可以拦截并解密 SSL 隧道。

QRadar Network Insights 以独特的方式交付实时洞察力

EMA 观察

没有其他“安全智能”供应商提供类似于 IBM 的技术：以相同的详细程度和及时性扫描进出网络的数据包中是否潜藏着恶意意图。QNI 在“流”数据中添加了 30 个新字段，扩展了协议定义的元数据，进而将 7 层内容包含在内，充当数据包带有异常信息时的预警信号。

QNI 不仅仅是一种组合式技术。IBM 设计 QNI 的目的在于构建一套全面的事件检测、优先排序和分析功能，进而改变分析人员的安全运营方式。在整个事件生命周期中，它能够尽早为分析人员提供更多的高质量取证数据。就网络攻击链而言，QNI 所提供的数据能够让分析人员实现事件可视化的时间从“行动和目标”阶段之后提前到“侦查”、“武器化”和/或“交付”阶段，因此有助于他们及早发现威胁。如此一来，分析人员便可更早采取行动并制止攻击，或者说至少能够缩短发生数据泄露时的攻击侵入时间。尽早采取行动可以缩短侵入窗口期，还可以减少清理威胁所需的时间和整体资源投入。QRadar 的接口能够增强数据流，确保简化安全运营流程。此外，还可以在报告引擎中充分利用数据来支持 QRadar 所提供的各种报告功能。

关于 IBM Security

IBM Security 可以提供最先进、集成的企业安全产品和服务组合。由世界著名的 IBM X-Force® 研究进行支持，该组合使企业能有效地管理风险并防范新威胁。IBM 作为世界上覆盖范围最广的安全研究、开发和交付企业之一，每天对 130 多个国家/地区的 350 亿个安全事件进行监控，并拥有 3,000 多项安全专利。有关更多信息，敬请访问 www.ibm.com/security，或在 Twitter 上关注 @IBMSecurity，或访问 IBM Security Intelligence 博客。

关于 Enterprise Management Associates，Inc.

Enterprise Management Associates (EMA) 创立于 1996 年，是一家领先的行业分析公司，致力于为各种 IT 和数据管理技术提供深刻洞察力。EMA 分析师利用独特的综合实践经验，洞察行业最佳实践，深入了解当前和计划的供应商解决方案，从而帮助 EMA 的客户实现他们的目标。有关 EMA 针对企业业务线用户、IT 专业人员及 IT 供应商所提供的研究、分析与咨询服务的更多信息，敬请访问：www.enterprisemanagement.com 或 blogs.enterprisemanagement.com 。您也可以在 Twitter、Facebook 或 LinkedIn 上关注 EMA。

公司总部：

1995 North 57th Court, Suite 120

Boulder, CO 80301

电话：+1 303.543.9500

传真：+1 303.543.7687

www.enterprisemanagement.com

3534.030917