IBM Security

IBM

IBM QRadar

借助最先进的安全分析平台感知并检测各种现代威胁

IBM 安全白皮书

征服未知问题

安全专业人员生活在一个不断出现悬念的世界中。其组织的每个角落时时刻刻都在遭受各种威胁和攻击。执著的攻击者攻破防线后，他们就会缓慢地潜行。他们搜寻有价值的数据并掩盖自己的一切行踪。事实上，最近的一项调查发现，识别一次攻击的平均时间为 256 天，而阻止它的平均时间为 82 天。[1] 所以，安全操作中心 (SOC) 的压力非常大；许多团队就是不知道对他们来说到底哪些是未知的。

安全团队只要封锁边界，就能禁止许多形式的互联网访问并对抗最新威胁的时代已一去不复返。如今的企业要求用几乎无处不在的连接来保持企业运行，同时阻止高级威胁，识别欺诈和恶意的内部人员，并确保持续合规。新的需求要求企业分析尽可能多的信息，以检测潜伏在表面下的威胁性活动 — 并更快地进行响应。SOC 分析师必须具备一种敏锐的能力，可检测与正常活动的偏差，并且他们选择的解决方案必须能够扩展，可触及企业的每个角落且只使用单个紧密结合的平台。

[1] “2015 年数据泄露成本研究：全球分析” *Ponemon Institute 研究报告*，2015 年 5 月。

感知威胁并采取行动

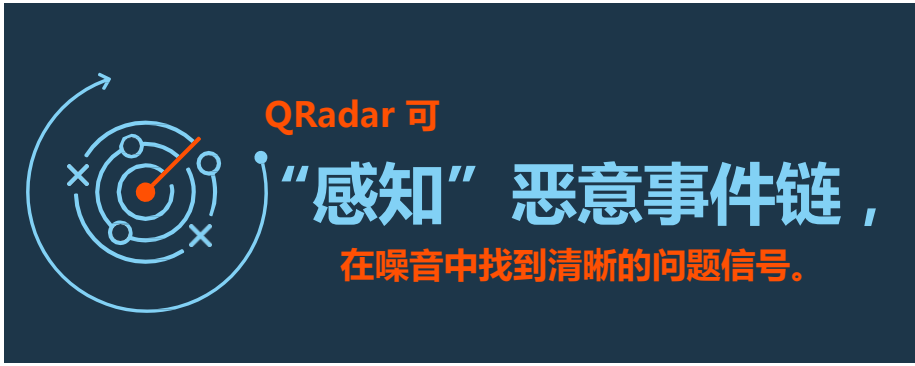
要想始终领先一步，企业要能够“感知”到恶意活动链，就像人们在看到、听到、嗅到或感觉到棘手状况时感知危险一样。因此企业需要的安全平台要能够：

- 快速部署在整个网络中，包括基于云的资源
- 检测环境中的细微差别，比如潜伏的入侵者或恶意的内部人员
- 在不依赖少数训练有素的专家的情况下发现攻击
- 收集、标准化和关联数十亿个事件，确定少数优先考虑的问题
- 识别重要漏洞和风险，防止数据泄露

从好的方面讲，如今的 SOC 分析师不必再单枪匹马地战斗。就像攻击者联合起来共享其洞察和技术一样，安全社区也以类似的共享资源作为响应。这些新的威胁情报和应用共享工具的出现，帮助人们限制了新恶意软件和漏洞攻击工具包的有效性，并且限制了零日或一日漏洞的影响。许多 SOC 分析师仍受限于老旧的日志管理系统或基本的安全信息和事件管理 (SIEM) 解决方案，一个可疑行为实例就会让这些解决方案生成大量的警报。

使用分析消除威胁

最严重的安全破坏不是突然出现的。相反，网络罪犯会发起可能持续数月的“低频而缓慢的”攻击。如果您能找出环境中细微但相关的变化，然后在开始发生怪异的事情时提醒安全团队，岂不是更好？



IBM® QRadar® Security Intelligence Platform 是唯一由 IBM Sense Analytics™ 提供支持的安全解决方案，它可以：

- 开发用户和资产概要信息作为合法活动的基准
- 在人员（包括内部人员、合作伙伴、客户和访客）、网络、应用和数据间检测异常行为
- 将当前活动与历史可疑活动关联起来，提高事件识别的准确性
- 检索并重放网络活动，以最初的数据包格式调查数据包内容
- 在薄弱环节被人利用之前找到并优先进行处理

执行即时分析的单点解决方案是不可靠的；它们不能将新的网络活动与“危险”用户关联起来，比如那些声誉不佳的已知过往站点访问者。Sense Analytics 可将用户行为与日志事件、网络流、威胁情报、漏洞和业务上下文相匹配，从而帮助企业消除威胁。通过在噪音中找到清晰的问题信号，让企业能够专注于最直接和最危险的威胁 — 并指导他们执行补救工作来最大限度降低任何潜在的损害。

Sense Analytics 的工作原理

没有数据，分析就毫无用处；没有大量的数据，分析也会软弱无力。一些数据来自您的网络操作，一些数据存储在应用中，一些源自以前的分析，还有一些作为信息提要来源于外部。QRadar 从网络内的每个设备、应用和用户处收集原始安全数据 — 无论这些设备、应用和用户位于企业的内部还是托管在云环境中的系统上都是如此。

Sense Analytics 能够：
- 分析安全数据
- 理解上下文
- 探查使用情况

收集数据后，QRadar 设备执行实时分析来搜索直接的危险信号，然后将结果与已存储的其他有关任何所涉及网络、用户或文件元数据的情报进一步融合。QRadar 让安全团队能够理解当前活动与过去已发生的活动有何关联，而且感知变化的一个重要方面是能够为基准活动提供正确的参数。

分析安全数据以感知威胁

有了 Sense Analytics 作为后盾，QRadar 使用基于状态的高级分析将当前的安全数据转换为有意义的洞察。安全团队可定义多种类型的条件，帮助他们感知潜在的恶意活动，包括：

- 行为变化，以捕获与正常模式的偏差
- 可能揭示新网络流量或突然终止的流量的异常
- 阈值违反情况，以查找哪些活动超出了既定的级别

使用 QRadar，一家国际能源公司每天能够分析

20 亿个事件–

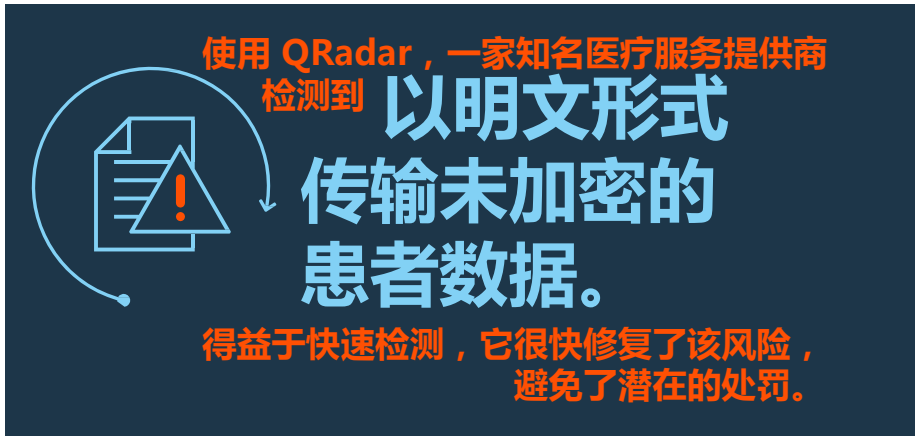
实时关联数据 — 以识别

20 到 25具有最大危险的潜在攻击。

用户或身份的常规行为变化，常常是网络被破坏或某些个人凭证可能被损害的初期迹象之一。Sense Analytics 不仅会对比实时活动与历史模式，它还检测新的应用使用情况、新的网站访问和新的文件传输活动。它还能从企业身份系统中拉取数据，允许 SOC 分析师查看最新报告或个人的角色变化，从而帮助企业排除误报结果。

通过分析事件、数据流和数据包来理解上下文

一种强大且常被忽视的上下文来源可能源自原生网络流数据 — 标识 IP 地址、端口、协议，甚至应用或流经网络的“载荷”内容的数据 — 所有这些数据都通过直接的深入数据包检查或事故后的完整数据包恢复来捕获。这让安全团队能够：



- 探查“正常的”网络流量并在条件变化时收到报警
- 找到与恶意 IP 通信的新的或已被攻陷的主机
- 检测新的安全威胁，而不使用签名
- 回放被检测到的入侵者或恶意用户的逐步操作
- 深入了解应用层并检测可疑内容或不当的使用情况

Sense Analytics 使用网络数据来提供每个事件、事故或相关攻击的上下文。它可以检测 Web 服务器是否停止对通信的响应，识别常用服务的活动水平是否有重大变化，以及在网络上出现新服务或协议时生成警报。此分析还会揭示应用的类型，识别端口和协议失配 — 这可帮助企业加快调查速度。

探查使用情况，以存储洞察并帮助管理风险

一个为快速搜索实时数据而设计的安全解决方案会遗漏大量的事故，要捕获这些事故，需要提前了解关键应用及其使用人员、典型性能水平和关联的主机，还需要了解这些关键应用何时处于快速活动周期、何时处于缓慢活动周期。知晓这些参数对获得可操作的洞察至关重要。

QRadar 帮助一家信用卡公司

保护其关键数据

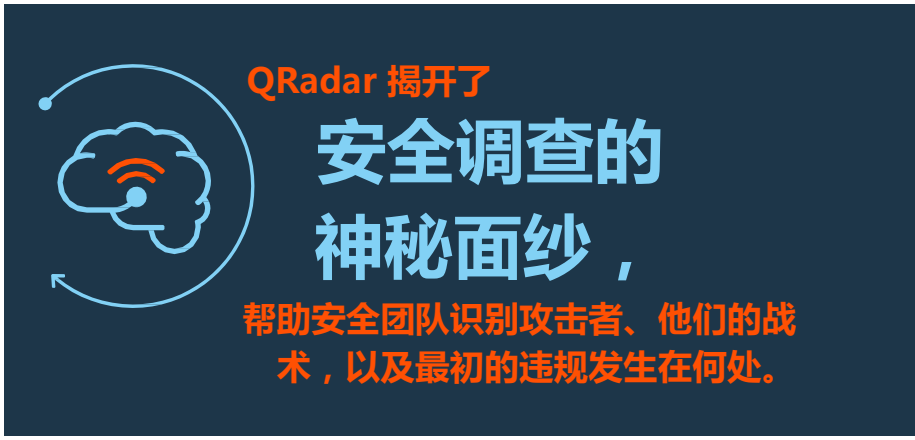
和基础架构远离高级威胁 — 同时还实现高达 50% 的部署、调优和维护成本节省。

能够通过探查资产和个人来获得知识，是 Sense Analytics 的一个基本特征。QRadar 使用网络流数据和漏洞扫描来自动发现资产并创建资产概要文件。此概要文件定义了资产是什么，识别它如何与其他资产通信，列出允许操作的应用和存在的任何已知漏洞。然后 QRadar 使用所有这些情景来减少噪音，提供高度准确的事故信息。

积累网络用户当前行为的知识，对攻击和破坏检测同样宝贵。QRadar 可跟踪 IP 和 MAC 地址、电子邮件 ID 和聊天句柄等信息，并且可以利用其他 IBM 或第三方身份和访问管理程序来为事故调查提供宝贵的情景资料。它可使用所有这些关联信息来限定其分析的范围，包含或排除与（当前发生或最近观察到的）可疑活动有关的个人或角色。

可展现 Sense Analytics 强大功能的用例

在许多环境中，安全实践方面的自满和过失意味着关键资产的安全性不一定达到了它们能够达到或应该达到的水平。企业需要限制不可避免的违规情况所造成的负面影响。他们需要涵盖整个环境且没有任何盲点的解决方案。



从安装那一刻开始，QRadar 就开始构建可操作的安全洞察，这些洞察可帮助您加强企业的防御。该解决方案提供了快速价值的用例包括：

- 高级威胁检测
- 关键数据保护
- 内部威胁监视
- 风险和漏洞管理
- 未授权流量检测
- 取证调查

用例：
高级威胁检测

使用实时分析，安全团队可以检测主机是否访问了一个潜在的恶意域，但仅仅一次访问可能不需要发出警报。然而，如果同一主机开始表现出报警行为 — 使用长期历史分析检测出来 — 而且它也开始传输异常高的数据量，与其行为基准不符，所有这 3 个条件相结合，QRadar 就能生成单个加强型警报。

QRadar 也可以感知网络流量的突然变化，比如主机上出现一个新应用或一个典型服务终止了，并捕获它作为异常条件。安全团队在搜索系统日志时不太容易发现异常 — 这些异常不同于恶意软件签名或针对已知漏洞的其他既定攻击。根据定义，异常是指一种奇怪现象，它只能被可监视和探查所有用户与实体操作的安全解决方案所发现。

用例：
关键数据保护

在晚上，一个新应用开始在一个网络主机上运行。此活动可能是一个新的业务需求或某人安装了一个聊天应用所导致的。但是如果该主机能够访问关键数据，而且还有一个相关的已知漏洞，QRadar 可创建一个高优先级警报来提示安全团队调查该事件。

QRadar 快速检测事件流量何时超出特定的活动水平并生成一个警报。可根据 QRadar 中已收集的任何数据来确定该阈值或限制，如网络设备配置、服务器、网络流量遥测、应用，以及最终用户及其活动。而且像行为改变或异常一样，QRadar 可使用用户身份、正在使用的端口和协议、IP 声誉和已报告的威胁活动来提供更多警报线索，为安全团队提供该事件更深入的信息。

用例：
内部威胁监视

一位客户服务代表突然开始从客户信息系统下载两倍于正常数量的数据，这可能是某个新的销售分析活动的一部分。但是如果 QRadar 知道该代表最近访问了一个潜在的可疑网站，而且现在正看到少量数据被发送到竞争对手的网站，就可在大量信息被泄露之前通知安全人员。

通过在单位和个人中的评测，QRadar 在众多安全产品中脱颖而出。一组全面的数据、业务情景和威胁情报的组合 — 加上能够检测与正常行为的偏离并识别哪些行为不被允许或者是不当的 — 提供了非常强大的事件检测能力。

用例：
风险和漏洞管理

网络上出现一个新实体时，QRadar 通过探查日志和流数据可自动感知它的存在。借助其无缝集成的漏洞扫描器，QRadar 可触发对这个新实体的一次扫描，以发现它是否有任何紧急或高风险的漏洞暴露给潜在的威胁来源。

例如，将一个新服务器添加到网络时，QRadar 可检测它是否遗漏了关键的补丁或者具有默认的管理凭据。然后 QRadar 可通知合适的团队进行补救和/或计划一次修补，如果没有及时执行该任务，则升级该问题。

而且，会自动地将新公布的漏洞与现有数据相关联，而无需重新扫描，这有助于提高检测的速度和准确度。这样所带来的操作节省让安全分析师能够将更多的时间集中在主动战术上，比如风险分析和漏洞修补活动。

用例：
未授权流量检测

随着大部分企业现在都支持自带设备 (BYOD) 端点，安全团队正看到越来越多与社交媒体应用相关的网络流量。用户常常访问他们的企业电子邮件系统，通过 Facebook、LinkedIn、Twitter 和其他服务与好友保持联系，所有这些都在同一台设备上完成。QRadar 收集和分析此数据，并留意互联网聊天会话何时开始通过端口 80 连接（举例而言），该端口通常用于传输 HTTP 流量。与已知的僵尸网络服务器的进一步连接可快速证实恶意软件已被注入，应提示安全团队采取行动。

QRadar 从网络层和端点管理系统收集和分析来自移动以及 BYOD 设备的数据。它可检测潜在的威胁 — 比如一个被越狱的设备、安装在设备上的可疑应用或潜在的恶意互联网通信 — 然后触发对设备进行隔离和/或将问题升级到合适的安全团队来采取行动。

用例：
取证调查和威胁搜寻

在攻击调查期间，安全分析师发现一位或多位员工受到了网络钓鱼攻击，攻击者已成功入侵并扩展到一个内部服务器主机。该模式与 X-Force 已识别的一种模式相符，称为注入远程访问特洛伊 (RAT) 软件，该软件很难检测。

通过单击几次鼠标，QRadar 恢复了所有与该事件相关的网络数据包并重构了攻击的逐步过程 — 向安全分析师清晰透明地展示出安装该 RAT 软件的位置和时间。取证工作流让分析师能够快速且轻松地构建丰富的恶意软件概要信息，并通过链接分析将注入路径衔接起来，识别出“第一感染源”和任何其他受感染方。结果是，安全团队能够快速补救损害，将此事件的再现几率降到最低。

IBM 提供了可操作的情报来实现主动出击和更强的防护

信息安全是董事会级的优先事项，但许多企业仍依赖于数十个单点产品来获取即时洞察。受过深入培训的人员正在使用搜索引擎来筛查海量数据，但攻击者越来越普遍地在成功打开缺口后，通过将IP、协议、端口和应用切换到锁存状态来逃避检测，进而大肆收集宝贵数据。

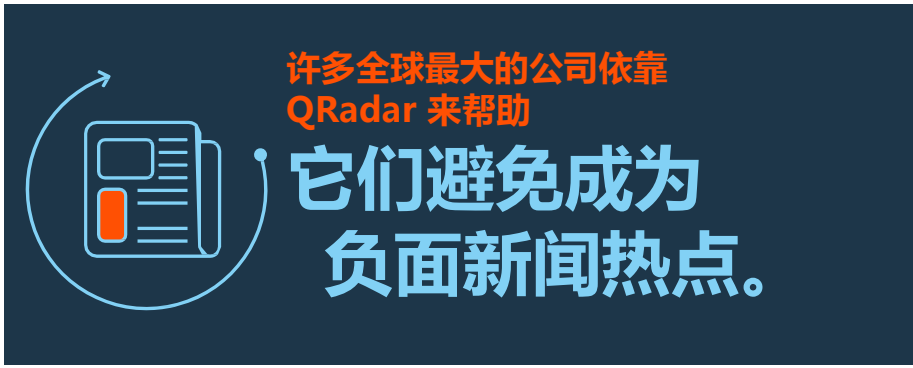
IBM QRadar 与众不同。无论网络的规模如何，它都可以快速部署并在几小时内开始交付结果。它的认知能力和已存储的情报可关联从同一来源传来的或对应于相同目标数据的相关攻击。QRadar 提供了这些可操作的洞察来满足当前和未来的需求 — 从高级威胁检测到内部威胁监视、欺诈检测、风险和漏洞管理、取证调查以及合规性报告。

安全领导者选择 QRadar 的主要原因包括：

- 一个易于使用的安全仪表板，突出显示了最重要的威胁，支持快速、有效的调查和补救工作流
- 几乎无限的可伸缩性，由 X-Force 威胁智能和 IBM X-Force Exchange 的协作功能提供支持
- IBM Security App Exchange，包含 IBM 和合作伙伴开发的应用，它扩展了 QRadar 的功能而没有增加复杂性
- 具有全局可见性的单个集成平台，提供了有关网络、应用和用户活动的洞察

让最重要的威胁无处遁形

一旦检测到威胁、攻击或破坏，就是采取行动的时候了。QRadar 为安全团队提供了一个基于 Web 的用户界面，该界面在整个平台上外观一致。platform.在监视日志活动、观察网络活动、审核高度相关的攻击，运行风险和漏洞分析，或执行取证分析之间进行切换非常容易，只需单击一个选项卡就能显示一个信息丰富的仪表板屏幕。每个仪表板都拥有丰富的安全情报信息，这些信息被组织到高度直观的最新活动显示界面中，只需单击几次鼠标即可轻松开始调查工作。



您可以花几分钟时间查看突出的事件或深入研究所报告攻击的细节。安全团队可快速了解重要问题的性质；被利用的任何漏洞；注入的任何僵尸网络、RAT 或其他恶意程序；以及任何数据丢失的程度。现在是时候在造成实际损害之前采取行动了。

获得大规模采取行动的能力

使用更大的 QRadar 平台，安全团队可清晰地理解已发生的事件，以及不快速采取行动会面临哪些风险。通常只需一次单击即可使用威胁监视、风险和漏洞管理及合规性报告等关键功能，并且可以在彼此之间传递相关数据。而且，QRadar 与 X-Force 威胁智能紧密集成，能够每小时更新全球攻击技术和恶意软件种类。

QRadar 包含各种硬件、软件和虚拟应用模型，可实现

更快的部署速度。

发生破坏事件时，QRadar 集成的取证技术为 SOC 分析师提供了相关攻击的成套数据，详细且准确清晰地描述了入侵者的逐步行动。打败一些威胁只需拦截与一个外部 IP 地址的通信，但其他威胁需要动员应急响应团队来隔离和重新配置主机，禁用恶意软件并修补漏洞。但是如果您的团队不知道要做什么怎么办？此时就应该寻求帮助，与同行协作，寻求一个解决方案，甚至雇佣专业服务团队了。

QRadar 开放框架以及 IBM Security App Exchange 有助于促进与 IBM 和第三方解决方案实现更紧密的集成。例如，站点上的一个应用将 QRadar 攻击数据传递给 Resilient Systems 的事故响应平台，以便立即采取行动。另一个应用通过 Carbon Black Enterprise Response 端点管理解决方案提供一种类似的数据共享功能。

借助 IBM Security App Exchange 扩展各种功能

IBM Security App Exchange 显著提高了 QRadar 的灵活性。这个最重要的协作站点允许客户、开发人员和业务合作伙伴共享应用、安全应用扩展和对 IBM Security 产品的增强。

借助 IBM Security App Exchange，企业能够：

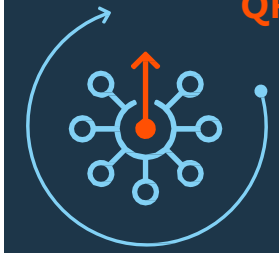
- 获取各种应用，扩展 IBM Security 解决方案的功能
- 共享最佳实践并向他人学习
- 找到各种解决方案和用例，增强安全操作的战略价值

IBM 会针对已设定的条件审查所有代码，然后才会将代码上传到站点上。安全团队可独立下载和安装解决方案 — 在官方产品发布周期外。这样，他们就可以应用新的安全用例，而不会添加不必要的解决方案的复杂性。

具体来讲，QRadar 用户可从 IBM Security App Exchange 下载特定于行业、威胁、设备和供应商的内容。而且，他们可以访问定制报告、仪表板、专业分析和威胁信息。

部署一个具有全局可见性的平台

当今的安全环境充满着复杂性 — 安全数据常常分散在不同供应商的多款产品中，这些产品具有不同的接口和数据存储格式。要想有效地检测现有和新兴的威胁，安全团队需要此数据的统一视图，并且还要结合使用全面的威胁检测分析和响应功能。QRadar 使用单个连锁的数据库来存储所有安全数据，该数据库专门从内部部署系统和云系统可扩展地收集数据，并且具有出色的存储、报告和非常快的调查搜索性能。此外，QRadar 针对实时和历史事故分析进行了优化，在事故发生后几秒即可检测出来 — 而不是几小时、几天或几周。



QRadar 可以快速部署而无需众多专家，提供了一个

单一的控制台指挥中心

QRadar 还提供了一组紧密整合的安全用例，更多的用例可通过 IBM Security App Exchange 获得。安全团队可使用单个基于仪表板的控制台控制所有功能，这些功能包括实时安全监视，主动风险和漏洞管理，以及事故检测、取证和补救。这个安全操作和响应中心融合了来自 IBM 和第三方产品的智能 — 由一个一致的用户界面和工作流提供支持 — 使您的安全操作团队工作更加富有成效。

更多信息

要了解由 Sense Analytics 提供支持的 IBM QRadar Security Intelligence Platform 的更多信息，请联系您的 IBM 销售代表或 IBM 业务合作伙伴，或者访问：**ibm.com**/security

关于 IBM Security

IBM Security 提供了最高级和一体化的企业安全产品和服务组合之一。该产品组合（由享誉全球的 X-Force 研发团队提供支持）提供了安全智能来帮助企业整体性地保护其人员、基础架构、数据和应用，为身份和访问管理、数据库安全、应用开发、风险管理、端点管理、网络安全等提供了解决方案。这些解决方案让企业能够有效地管理风险，为移动、云、社交媒体和其他企业业务架构实现一体化的安全保护。IBM 运营着全球最大的安全研究、开发和交付组织之一，每天监视着 130 多个国家的 150 亿个安全事件，拥有超过 3,000 项安全专利。

IBM Security
Route 100
Somers, NY 10589

美国印刷
2016 年 4 月

WGW03211-CNZH-00