IBM Security

IBM

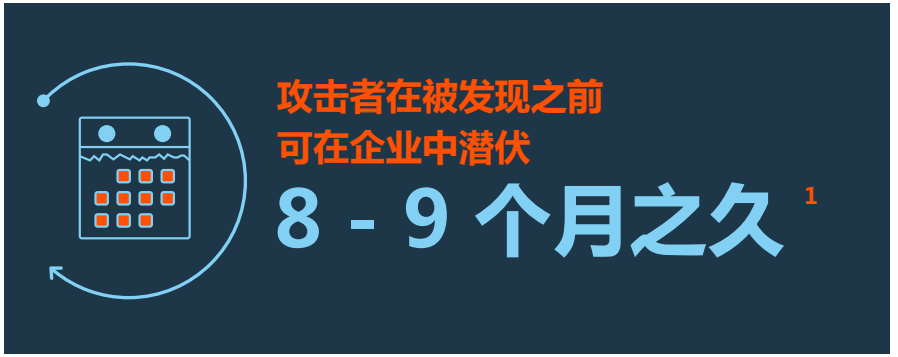
IBM QRadar

借助最精良的安全分析平台，感知并检测各种现代威胁

IBM Security 白皮书

攻克未知难题

安全专业人员生活的世界处处充满悬念。威胁和攻击随时随刻都会从四面八方向他们的企业发起进攻。绵绵不绝的攻击者破门而入之时，他们会悄然缓慢地采取行动。他们会搜寻重要数据，并掩藏自己的踪迹。事实上，最新一项调研显示，识别一次攻击的平均时间为 256 天，而遏制攻击的平均时间为 82 天。[1] 因此，安全运营中心 (SOC) 的工作压力很大；许多团队压根不知道他们的认知盲点是什么。

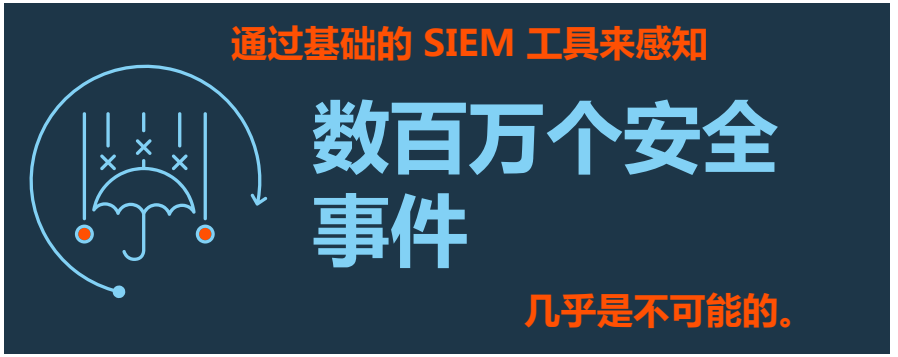


过去，安全团队只需封锁边界，就能禁止各种形式的互联网访问并防御最新威胁，而现在这种日子已经一去不复返了。当今的企业需要实现几乎无处不在的连接，以使业务持续运营，同时阻止高级威胁，识别欺诈和恶意的内部人员，并确保持续合规。新的需求要求企业分析尽可能多的信息，检测潜藏在表面之下的威胁活动，并更加快速地做出响应。SOC 分析师必须培养敏锐的洞察力，检测出偏离正常活动的情况，而他们所选的解决方案必须能够实现扩展，借助一站式综合平台，覆盖企业的每个角落和缝隙。

[1] “2015 年数据泄露成本调研：全球分析”，《Ponemon Institute 调研报告》，2015 年 5 月。

感知威胁并采取行动

要想抢先一步，企业需要能够"感知"到恶意活动链，就像人们看到、听到、嗅到或感觉到麻烦状况时感知危险那样。他们需要一个具备以下功能的安全平台：

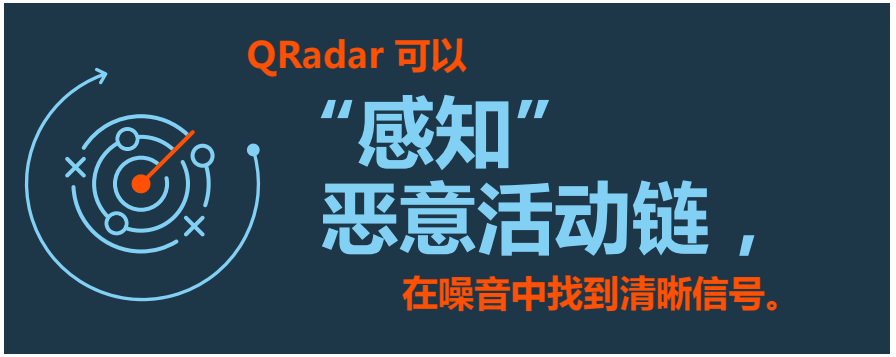


- 在整个网络中快速部署，包括基于云的资源
- 检测环境中的细微差异，比如潜藏的入侵者和恶意的内部人员
- 无需依靠一些训练有素的专家即可发现攻击
- 收集、规范和关联数百万个事件，确定少数高优先级的问题
- 识别重要漏洞和风险，防止数据泄露

从积极的方面来看，当今的 SOC 分析师不必再孤军奋战。正如攻击者联合起来共享他们的洞察和方法一样，安全社区也通过类似共享资源的方式做出响应。这些新威胁情报和应用共享工具的出现，有助于限制新恶意软件和漏洞攻击工具包的效力，遏制零日漏洞或一日漏洞的影响。但是许多 SOC 分析师仍被束缚住了手脚，不得不使用过时的日志管理系统或基础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

最严重的安全破坏开始时并不会轰轰烈烈，相反，网络罪犯会发起可能持续数月的"低频且缓慢"的攻击。如果可以发现环境中微妙的相关变化，然后在发生怪异事件之前向安全团队发送警报，岂不是很棒？



IBM® QRadar® Security Intelligence Platform 是唯一一个由 IBM Sense Analytics™ 支持的安全解决方案，它可以：

- 开发用户和资产概要文件，作为合法活动的基准
- 检测人员（包括内部人员、合作伙伴、客户和访客）、网络、应用和数据当中的异常行为
- 将当前和历史可疑活动关联起来，提高事件识别准确性
- 检索并回放网络活动，调查初始形式下的数据包内容
- 提前找到薄弱环节，并对其划分优先级

执行实时分析的单点产品并不可靠，它们不能将新的网络活动与"存在风险的"用户关联起来，比如那些之前访问过声誉不佳的网站的人员。Sense Analytics 可将用户行为与日志事件、网络流、威胁情报、漏洞以及业务环境匹配起来，进而帮助消除威胁。它支持企业在噪音中找到清晰信号，让企业集中精力处理最直接最危险的威胁，并指导他们采取补救措施来最大限度减少任何潜在损害。

Sense Analytics 工作原理

没有数据，分析也就毫无用处；没有大量数据，分析也会疲软无力。数据有些来自您的网络运营，有些存储在应用当中，有些来自过去的分析，还有些来自外部来源反馈。QRadar 可从网络中的每个设备、应用和用户处收集原始安全数据，不管这些设备、应用和用户位于企业内部环境中，还是被托管在云环境中。

Sense Analytics 可以：
- **分析安全数据**
- **理解背景信息**
- **探究使用情况**

收集到数据之后，QRadar 设备就会执行实时分析，搜索直接的危险信号，然后通过关于所涉网络、用户或文件元数据的其他存储情报，进一步丰富这些结果。QRadar 让安全团队能够了解当前活动与过去发生的事情有何关系，感知变化的一个关键方面就是为基准活动设置正确的参数。

分析安全数据，以便感知威胁

QRadar 由 Sense Analytics 提供支持，使用基于状态的高级分析，可将当前的安全数据转换为重要的洞察。安全团队可以定义多种条件类型，帮助他们感知潜在的恶意活动，包括：

- 行为变化，以捕获偏离常规模式的情况
- 异常情况，以发现新的网络流量或突然中断的流量
- 阈值违规，以找到超出规定级别的活动

借助 QRadar，
一家国际能源公司每天可以分析

20 亿个事件 —

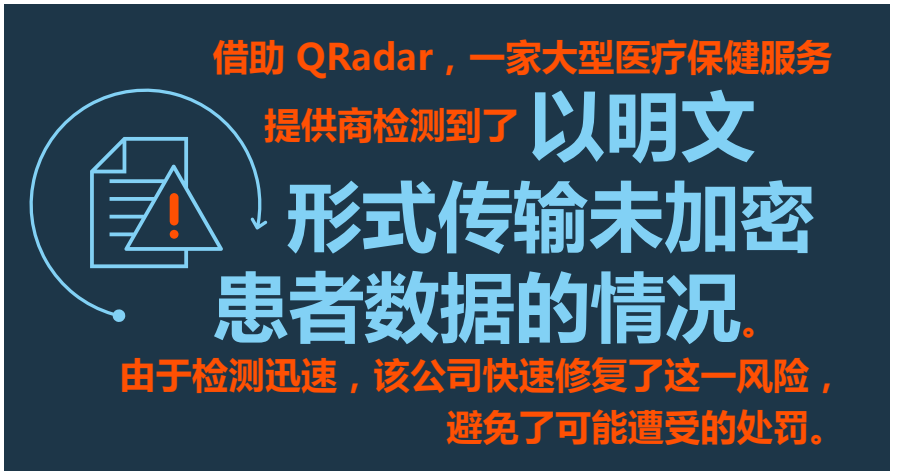
实时关联数据，找到可能引发
最大风险的 20-25 个潜在攻击行为。

用户常规行为或身份的变更，往往是网络被破坏和某些人的凭证被损坏的早期迹象之一。Sense Analytics 不仅可以将实时活动与历史模式进行比较，还可以检测新的应用使用情况、新的网站点访问以及新的文件传输活动。它还可以从企业身份管理系统提取数据，让 SOC 分析师看到个人的最新职位或角色变化，从而帮助排除误报结果。

通过分析事件、数据流和数据包，理解背景信息

一种强大却常被忽略的背景信息来源可能源自原生网络流数据，也就是标识 IP 地址、端口、协议，甚至应用或流经网络的"有效负载"内容的数据。所有这些数据都可以通过直接的深度数据包检测或事故后完整数据包恢复而捕获。这可让安全团队：

- 探究"常规"网络流量，在情况变化时获得警报
- 找到与恶意 IP 通信的新主机或受损主机
- 检测新安全威胁，而无需使用特征码
- 回放被检测到的入侵者或恶意用户的逐步操作
- 洞悉应用层并检测可疑内容或不当使用情况



Sense Analytics 使用网络数据来提供每个事件或相关攻击的背景信息。它可以检测到 Web 服务器是否停止响应通信，识别常用服务的活动水平是否出现重大变化，并在网络上出现新服务或新协议时生成警报。这种分析也可以揭示应用类型，发现端口和协议不相匹配的情况，从而帮助加快调查。

探究使用情况，储备洞察，帮助管理风险

一种旨在快速搜索实时数据的安全解决方案往往会遗漏大量的事件，而要捕获这些实践，需要预先了解关键应用及其使用人员、典型性能水平以及相关主机，还要了解这些应用何时处于慢速活动周期、何时处于快速活动周期。掌握这些参数对于获得切实可行的情报洞察至关重要。

Sense Analytics 的一个基本特征是能够通过分析资产和个人来储备知识。QRadar 使用网络流量数据和漏洞扫描，自动发现资产并创建资产概要文件。概要文件可定义资产内容，识别一项资产与其他资产的通信方式，列出获得准许的应用，并概述存在的任何已知漏洞。然后，QRadar 使用所有这些背景信息来减少噪音，提供高度准确的事件信息。

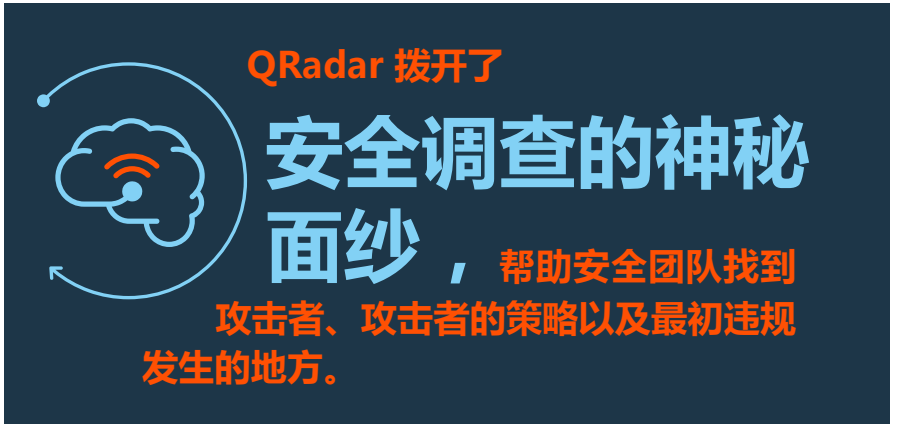
积累关于网络用户行为的知识，对于攻击和违规检测来说同等重要。举例来说，QRadar 可以跟踪 IP 和 MAC 地址、电子邮件 ID 以及聊天内容等信息，并可以利用其它 IBM 或第三方身份和访问管理程序，为事件调查提供宝贵的背景信息。它可以使用所有这些联系来限定分析范围，包含或排除与目前正在发生或过去观察到的可疑活动相关的个人或角色。

探索展示 Sense Analytics 威力的用例

在许多环境中，安全实践中的自满和失误表明，关键资产不一定像它们本可以或本应该的那样安全。企业需要限制不可避免的违规情况所造成的负面影响。他们需要覆盖整个环境且没有任何盲区的解决方案。

从安装的那一刻起，QRadar 就开始构建切实可行的安全情报，帮助加强企业的防御能力。有关该解决方案快速交付价值的用例包括：

- 高级威胁检测
- 关键数据保护
- 内部威胁监控
- 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

通过实时分析，安全团队可以检测到主机是否访问了可能潜在的恶意域，但是仅仅一次访问可能并不需要发出警报。但是，如果通过使用历史长期分析检测到，同一个主机开始表现出报警行为，并且开始传输异常大量的数据，严重偏离行为基准，那么结合所有这三个条件，QRadar 就会生成单个增强的警报。

此外，QRadar 还可以感知到网络流量的突然变化，比如主机上出现一个新的应用或者一种典型服务发生了终止，并将这些变化作为异常情况进行捕获。安全团队在搜索系统日志时无法轻易发现异常情况，因为这些异常与恶意软件特征码或针对已知漏洞的其他明确攻击有所不同。顾名思义，异常情况就是一种怪异现象，只有通过能够监控和分析所有用户和实体行为的安全解决方案才能被发现。

用例：
关键数据保护

一夜之间，新的应用开始在网络主机上运行。这个活动的出现可能是因为新的业务需求或某个人安装了聊天应用。但是如果该主机可以访问关键数据，而且还存在与之相关的一个已知漏洞，QRadar 就可以创建一个高优先级的警报，提醒安全团队调查这个事件。

QRadar 可以快速检测到事件流量超出特定活动级别的情况，并生成警报。安全团队可以根据 QRadar 中收集到的任何数据来确定阈值或限制，比如网络设备配置、服务器、网络流量遥测、应用以及最终用户和他们的活动。和行为变化或异常情况一样，QRadar 可以通过用户身份、使用中的端口和协议、IP 声誉和报告的威胁活动等背景信息来丰富警报内容，为安全团队提供关于该事件更加深入的洞察。

用例：

内部威胁监控

一个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 ,这可能是某些新销售分析活动的一部分。但是如果 QRadar 了解到该代表最近访问了一个潜在的可疑网站，现在又发现少量数据被传输到了竞争对手的网站，那么就会在大量数据泄露之前通知安全工作人员。

通过对大量实体和个人进行测评，QRadar 从众多安全产品中脱颖而出。QRadar 不仅可以结合利用一系列综合数据、业务背景和威胁情报，还能够检测出偏离正常行为的情况，并识别哪些行为是被允许的或哪些是不当的，最终提供极其强大的事件检测功能。

用例：
风险和漏洞管理

当网络上出现新实体时，QRadar 会通过被动分析日志和流数据，自动感知实体的存在。通过无缝集成的漏洞扫描器，QRadar 可以触发对新实体执行扫描，看看其中否存在任何暴露给潜在威胁源的紧急或高风险漏洞。

例如，将一个新服务器添加到网络上时，QRadar 可以检测到它是否遗漏了重要补丁或者是否具备缺省的管理凭证。随后，QRadar 可以通知合适的团队来修复和 / 或安排打补丁，如果任务没有及时执行就上报问题。

此外，QRadar 会自动将发现的新漏洞与现有数据相关联，而无需重新扫描，这可帮助加快检测速度并提高检测的准确性。这样可以省略很多不必要的操作步骤，让安全分析师腾出更多时间来关注前瞻性策略，比如风险分析和漏洞修补活动。

用例：
未授权流量检测

随着大多数企业现在都支持自带设备 (BYOD 终端，安全团队发现了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，并通过 Facebook、LinkedIn、Twitter 以及其他服务与朋友保持联系，所有一切都在同一个设备上完成。QRadar 收集并分析这些数据，然后通知互联网聊天会话何时通过 80 端口开始连接，这个端口通常用于传输 HTTP 流量。与已知僵尸服务器进一步连接可快速证实恶意软件已被注入，进而提醒安全团队采取行动。

QRadar 会从网络层和终端管理系统中的移动和 BYOD 设备收集数据并进行分析。它可以检测潜在的威胁，比如越狱设备、安装在设备上的可疑应用或者潜在的恶意网络通信，然后触发设备隔离操作和 / 或向合适的安全团队上报问题，以便采取行动。

用例：

取证调查和威胁狩猎

在对一项攻击进行调查时，一位安全分析师发现，一位或多位员工遭遇到了网络钓鱼攻击，攻击者已经成功入侵并扩展到了一个内部服务器主机上。这种攻击模式与 X-Force 识别到的一种模式相匹配，已知的情况是它会注入很难检测到的远程访问木马 (RAT)。

通过轻轻单击几下，QRadar 就恢复了与该事件相关的所有网络数据包，并重建了整个攻击过程，向安全分析师展示了 RAT 软件确切的安装地点和安装时间。取证工作流程可让分析师快速轻松地构建丰富的恶意软件概要信息，并通过链接分析拼接起整个感染路径，进而确定"第一感染源"和任何其他被感染方。因此，安全团队可以快速修复受损部位，帮助最大限度降低再次发生攻击的可能性。

IBM 提供切实可行的情报洞察，帮助实施主动出击，实现强有力的防护

信息安全是高层关注的重点议题，但是许多企业仍然依赖于许许多多的单点产品来获得实时洞察。训练有素的人员正在使用搜索引擎来梳理大量数据，但是攻击者越来越通过切换 Ip、协议、端口和应用来避免检测，以便在成功攻破之后占有、扩展和收集重要数据。

IBM QRadar 与众不同。无论网络的规模如何，它都可以快速部署，并在短短数小时内开始交付结果。它的认知功能和已储备的情报可以将来自同一来源或对应同一目标数据的相关攻击关联起来。QRadar 交付这些切实可行的洞察，以满足当前和未来的需求，这些需求包括高级威胁检测、内部威胁监控、欺诈检测、风险和漏洞关联、取证调查以及合规性报告。

安全领域的领军企业选择 QRadar 的主要原因包括：

- 简单易用的安全仪表板，突出显示最为重要的威胁，支持快速有效的调查和修补工作流程
- 近乎无限的扩展能力，X-Force 威胁情报和 IBM X-Force Exchange 的协作功能为之提供支持
- IBM Security App Exchange，包含 IBM 和业务合作伙伴开发的应用，无需增加复杂性即可扩展 QRadar 的功能
- 具备全局可视性的一站式集成平台，提供关于网络、应用和用户活动的洞察

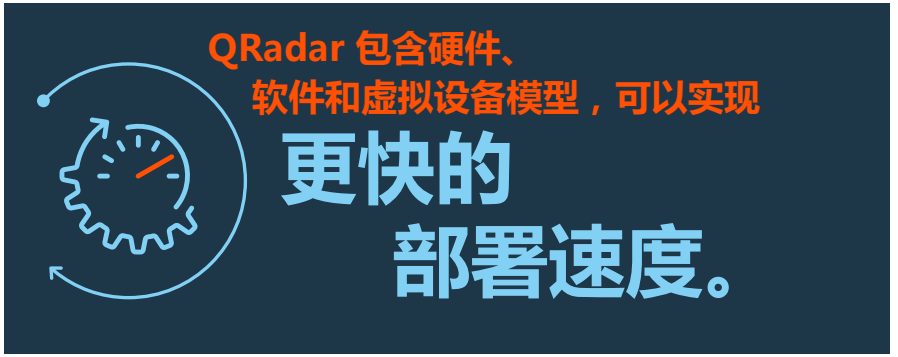
让最为重要的威胁无所遁形

一旦检测到威胁、攻击或违规，就是采取行动的时候。QRadar 为安全团队提供了基于 Web 的用户界面，该界面在整个平台中拥有统一的外观和风格。通过用户界面来监控日志活动、观察网络活动、浏览高度相关的攻击、运行风险和漏洞分析或执行取证分析时，安全团队可以在这些操作之间自如切换，只需单击选项卡就能显示信息丰富的仪表板屏幕。每个仪表板都有广泛的安全情报信息，而这些信息已被整理为高度可视化的最新活动视图，只需单击几下即可轻松完成调查。

安全团队只需花几分钟时间就能查看峰值事件或深入研究所报告的攻击背后的详细信息。安全团队可以快速了解突出问题的本质，被利用的任何漏洞，注入的任何僵尸网络、RAT 或其他恶意软件程序，以及数据丢失程度。现在是时候在造成任何实际破坏之前采取行动了。

获得大规模行动能力

借助更大的 QRadar 平台，安全团队可以清楚地了解已经发生什么事情以及如果他们不快速采取行动会面临哪些风险。威胁监控、风险和漏洞管理以及合规性报告等关键功能往往只需轻轻单击一下鼠标即可启动，还可以相互传递相关数据。此外，QRadar 可以 X-Force 威胁情报紧密集成，能够每小时更新一次全球攻击方法和恶意软件类型。



遇到入侵时，QRadar 搭载的取证技术可为 SOC 分析师提供相关攻击的所有数据，详细说明侵入者确切的操作步骤。对抗一些简单威胁只需阻止与外部 IP 地址的通信，但是其他威胁需要发动应急团队来隔离和重新配置主机，禁用恶意软件并修复漏洞。但是如果您的团队不知道具体应采取什么行动，那该怎么办？这时候就需要寻求帮助，与同行合作，寻求解决方案，甚至雇佣专业的服务团队了。

QRadar 开放框架以及 IBM Security App Exchange 可帮助促进 IBM 与第三方解决方案的更紧密集成。例如，站点上的一个应用可将 QRadar 攻击数据传递给灾备系统的事件响应平台，帮助即时采取行动。另一个应用可通过 Carbon Black Enterprise Response 终端管理解决方案提供类似的数据共享功能。

通过 IBM Security App Exchange 扩展平台功能

IBM Security App Exchange 可成倍提高 QRadar 的灵活性。这个高级的协作站点支持客户、开发人员和业务合作伙伴共享应用、安全应用扩展和 IBM ，Security 产品的增强功能。

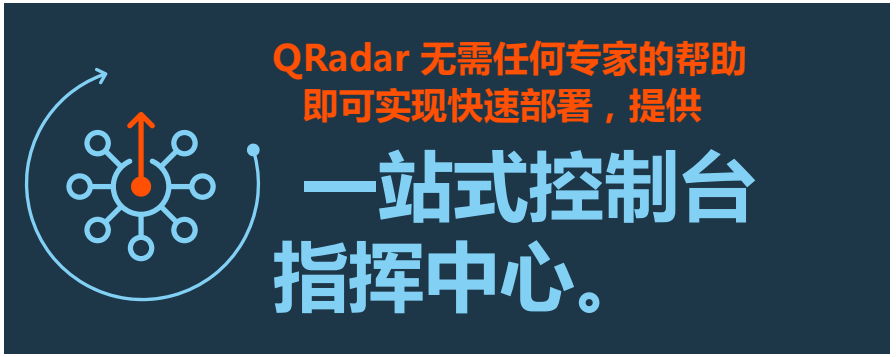
借助 IBM Security App Exchange，企业可以：

- 获得各种应用，扩展 IBM Security 解决方案的功能
- 共享最佳实践并向他人学习
- 找到丰富的解决方案和用例，增强安全运营战略价值

所有代码都由 IBM 根据设置标准进行审查，然后才会被发布到站点上。安全团队可以在官方产品发布周期以外独立下载和安装解决方案。这样，他们就可以应用最新的安全用例，而不会增加不必要的解决方案复杂性。

具体来讲，QRadar 用户可以从 IBM Security App Exchange 下载特定于行业、威胁、设备或供应商的内容。此外，他们还可以访问定制报告、仪表板、专业分析以及威胁信息。

部署一个平台，便可洞悉全局



当今的安全环境充满了复杂性，安全数据往往分布于不同供应商的多个产品中，所有产品都采用不同的界面和数据存储格式。要想有效检测现有威胁和新兴威胁，安全团队需要有关这些数据的统一视图，并结合使用全面的威胁检测分析和响应功能。QRadar 使用单个联合数据库来存储所有安全数据，这个数据库专门支持在内部环境和云系统中通过可扩展的方式收集数据，同时具备出色的存储、报告和快速调查搜索性能。此外，QRadar 针对实时和历史事件分析进行了优化，在事件发生几秒后就能检测出事件，而不会耗费数小时、数天或数周时间。

QRadar 还提供了一系列紧密整合的安全用例，并通过 IBM Security App Exchange 提供更多用例。安全团队可以使用基于仪表板的单一控制台来掌控所有功能，包括实时安全监控，主动风险和漏洞管理以及事件检测、取证和补救。这个安全运营和响应中心融合了来自 IBM 和第三方产品的智能智慧，由一个一致的用户界面和工作流程提供支持，可助力您的安全运营团队提升工作成效。

更多信息

如欲了解有关由 Sense Analytics 支持的 IBM QRadar 安全智能平台的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或者访问：**ibm.com**/security

关于 IBM Security

IBM Security 提供最先进最全面的企业安全产品与服务组合。该组合由世界知名的 X-Force 研究与开发团队支持，不仅提供深层的安全情报来帮助企业全面保护工作人员、基础架构、数据和应用，还提供各种解决方案来解决身份和访问管理、数据库安全、应用开发、风险管理、终端管理、网络安全等方面的需求。这些解决方案可支持企业有效地管理风险，跨移动、云计算、社交媒体以及其他企业业务架构实施全面安全防御。IBM 拥有世界上规模最大的安全研究、开发和交付组织，每天在 130 个国家或地区监控超过 150 亿个安全事件，拥有 3,000 多项安全专利。

IBM SecurityRoute 100
Somers, NY 10589

美国出品
2016 年 4 月

扫一扫，
关注 IBM 安全微信，
获取应对企业安全问题的全球资讯

致电垂询 IBM 安全专家
400 810 1818 转 2395
（工作日 9:00 – 17:00）

即刻访问 IBM 安全官方网站
https://www-03.ibm.com/security/cn-zh/?lnk=mpr_buse_cn-zh&lnk2=learnquick

WGW03211-CNZH-00