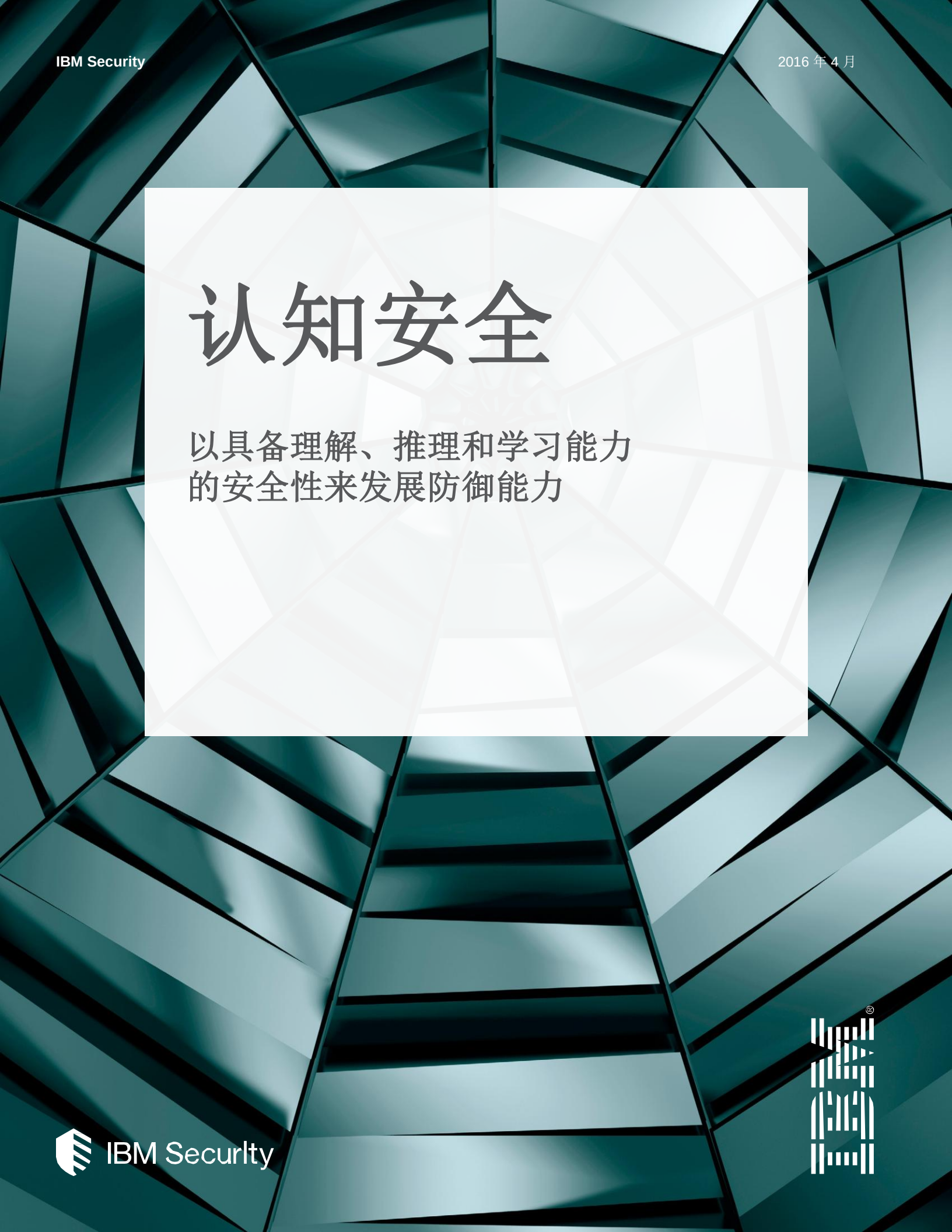
2016 年 4 月

认知安全

以具备理解、推理和学习能力的安全性来发展防御能力



IBM Security

目录

03 全新的必备能力

03 什么是认知安全？

04 从遵从到认知

06 认知安全的优势

07 挖掘越深，视角越广

10 缩小技术差距

08 使用案例：释放认知

09 未来：扭转网络犯罪经济

09 认知生态系统的集成和专业知识

10 IBM 如何为您助力

10 立即采取的 3 个步骤

全新的必备能力

近一个世纪以来，我们对计算机进行编程来帮助解决复杂的问题。我们现在可以模拟天气，对基因组排序，还可以即时在世界各地共享数据。但让计算机来完成人类每天做的工作，如辨识图像，读书或解释诗歌的含义，则另当别论了。传统系统无法做到这一点。

对安全性而言，情况如出一辙。数十年来，我们对计算机进行编程来识别病毒、恶意软件和攻击。我们不断对计算机进行优化使其变得更加准确，但这还不够。攻击者不断变换攻击方式，并寻找创新方式来突破防御。组织需要的是能够检测出活动中的细微变化，并尽可能多地结合上下文对其加以分析，以区分和消除新的威胁。

80%
的全球数据
一直是
隐形的。

如今则不然

组织需要持续进行监视并最大程度地使用数据来查找攻击和异常行为，以免造成损失。但全球每天会生成超过 2.5 艾字节的数据，其中 80% 是非结构化数据。这意味着数据是以自然语言（口头、书面或视觉语言）进行表达，人类可以很容易理解，但传统的安全系统却无法做到这点。事实上，成千上万的有关安全性的博客每天发布详细的威胁情报。但安全分析师无法了解其中的所有内容，传统的安全系统也无法像分析师那样分析和应用这些见解。

这就是为什么最具挑战性的安全问题仍需要人们来作出合理的决策：要针对哪些问题采取行动，哪些问题是虚假警报。事实上，最好的安全专业人士每天都在通过积累经验、与同事交流、参与会议、跟进最新研究报告来构建他们的知识体系。

IBM Security 正在训练新一代系统，来理解、推理和学习不断演变的安全威胁。我们正在开始将安全性的直觉和专业知识构建到新的防御中，它可以像安全专业人士那样每天分析研究报告、Web 文本、威胁数据和其他与安全性相关的结构化和非结构化数据，但其分析规模是我们前所未见的。这就是认知安全的本质。

结果：分析师将借助认知系统来帮助他们增强甚至自动化对威胁的理解，使分析师对最新的攻击更具判断力，以便腾出宝贵的时间着重处理其他紧迫问题。

什么是认知安全？

认知系统是自学习系统，可以使用数据挖掘、机器学习、自然语言处理和人机交互来模仿人脑的工作方式。

认知安全实现了两个广泛且相关的功能：

- 使用认知系统来分析安全趋势，将大量结构化和非结构化的数据提炼成信息，然后提炼成可执行的知识，以实现持续性的安全性和业务改进
- 使用自动化的数据驱动型安全技术、工艺和流程，支持认知系统享有最高级别的上下文和准确性

从遵从到认知

第一代网络出现后黑客便随之而来，从那时起，我们已经发展了安全技术以阻止攻击。到目前为止，我们经历过两个不同的网络安全时代：外围控制和安全情报。在此基础上，我们进入了第三个时代——认知安全。

外围控制：限制型安全（2005 年之前）

起初，我们采取静态防御，以防护或限制数据流，包括防火墙、防病毒软件和 Web 网关。企业内部信息安全的演变从遵从性活动开始。其目标是通过密码和一系列访问控制策略来锁定并限制对敏感信息的访问。成功意味着通过了审计。虽然外围防御仍在使用，但在当今环境中，仅使用外围防御已然不够。

安全情报：启发型安全（2005 年后）

随着时间的推移，我们发展为使用复杂的监视系统，可以收集和梳理大量的数据，以发现漏洞并优先处理潜在的攻击。这种转变更注重实时信息以检测可疑活动。如今，安全情报即实时采集、规范化和分析用户、应用程序和基础结构生成的结构化数据。

安全情报使用分析技术来检测与正常模式的偏差，发现网络流量的变化，并查找不同于规定水平的活动。在安全情报基础结构内，对大量的信息进行分析，努力在上下文中理解公司数据并优先处理日常活动。安全情报可以确定哪些偏差具有意义，这不仅有助于更快地检测漏洞，还可以减少误报，节省时间和资源。

认知安全：具备大规模理解、推理和学习能力的安全性（2015 年后）

认知安全以利用大数据分析的安全情报为基础，其技术特点是具备理解、推理和学习能力。现在可以使用认知系统来访问更大规模的相关安全数据，该系统可以处理和解读现今 80% 的非结构化数据，如书面语和口语。

认知安全系统摄取了专家设定的任何给定学科的大量知识，并通过输入一系列问答组合来进行训练。然后，安全专业人士会与系统进行互动，反馈系统响应是否准确，从而加强机器的“学识”。关键区别：认知系统理解和处理新信息的速度远超任何人类。现在，您每天都可以训练技术防御系统来分析数以千计的研究报告、会议材料、学术论文、新闻报道、博客文章和行业警报。

随着认知系统继续观察事件和行为（区分善意和恶意行为），它利用集成防御来阻止新威胁的能力会变得越来越强大。认知安全可以帮助安全分析师更有效地工作并加速对新出现威胁的响应速度，这将有助于缩小当前安全性技术方面的差距，带来高度的信心并提高风险控制水平。参见图 1。

安全性时间线历史

外围控制

2005 年之前

- 静态防御
- 密码保护
- 侧重于遵从性
- 成功 = 通过审计

安全情报

2005 年后

- 观察实时活动
- 重点关注与已知模式的偏离
- 优先处理潜在威胁的能力
- 应对型，基于规则

认知安全

2015 年后

- 模拟人类思维的推理
- 分析结构化和非结构化数据的能力，以理解行为和含义
- 根据持续的威胁情报自动进行学习
- 利用关系和建议主动关注

图 1

认知最终会纳入基于传统安全构建的框架中。安全情报不会消失；它是构建认知安全的重要基础。认知给我们提供了一个鉴别威胁情报和检测的途径，并以前所未有的速度和规模提供可操作的信息。

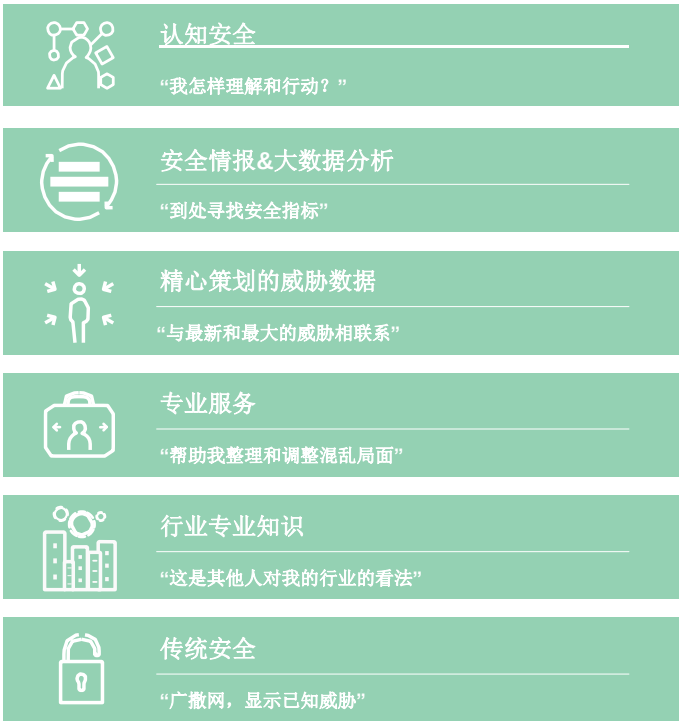


图 2

因为通常情况下安全情报和大数据分析是非结构化的，所以认知元素使我们可以进一步理解现状以及如何行动，这一点十分重要。凭借这些全套技术，您就可以为您的安全环境提供最大程度的保护。参见图 2。

认知安全的优势

传统的可编程安全系统会根据预定义的参数响应请求、作出判断和分析数据。认知系统则会解读数据，几乎每一次交互都会向其知识库中增加知识，基于深度洞察来权衡发生概率，并帮助您考虑相关变量而采取行动。

当前这一代系统是应对型系统（检测异常或攻击并作出响应），而认知安全是主动性系统。认知系统注重前瞻性并可持续进行多任务处理，它可以搜索漏洞、连接各点、检测差异并从数十亿次事件中进行筛选以构建可操作的知识库。

认知解决方案不仅会生成答案，还可以生成假设、基于证据的推理以及建议。现在，它能够解读 80% 非结构化数据（现有的系统无法访问这些数据），并将其与从无数来源和位置获得的结构化数据相集成。在信息越来越有价值的全球经济中，数据代表着世界上最丰富、最有价值和最复杂的原料之一。我们现在拥有了查找结构化和非结构化数据以及连续提取功能和模式的手段，可以提供实时的上下文来更好地制定决策。

认知安全的以下三个支柱在快速的模拟人类思维模式中发挥作用：

1. **理解**非结构化数据和自然语言文本。这包括通过“阅读”书籍、报告、博客和相关行业数据、“查看”图像和在上下文中“听取”自然语言来摄取和处理信息的能力。
2. **推理**，此能力可以解读和组织信息，提供含义的解释并给出结论的理由。
3. **学习**，随着数据的不断积累和从互动中获得的见解持续不断地进行学习。

挖掘越深，视角越广

只专注检测恶意软件、恶意威胁、异常值和异常状况往往导致过多的误报。这是认知系统运作的多维环境的优势。

在当今世界中，区分善意行为和恶意行为的能力仅是集成安全基础结构所需的专门知识的一个方面。还有越来越多的灰色地带，而这正是认知发挥作用之处。

认知系统增设了高度的直觉、理解力和洞察力，旨在不断利用数据进行强化，以帮助区分可接受行为与可能预示新威胁的细微变化。其结果是更广泛的视角，主动关注大局。

缩小技术差距

不只是我们的系统面临跟上当今安全环境的挑战，员工也面临同样的挑战。世界各地空缺的信息安全职位数预计为 208,000，并预期在 2020 年将增长到 150 万。认知安全可以提供帮助。

认知系统作为一个可扩展的资源助力人类，可作为经常人手不足的安全部门的特别补充。这个新维度至关重要，因为只密切关注您自己的系统内的状况已经远远不够。您需要监视全球范围内的威胁以便准备防御潜在的攻击。认知系统能够进入全球交换网络，该网络每秒分析几十万个安全事件，为全球几千位客户提供服务。

认知可以减轻安全分析师的工作，它提供以人为核心的通信，如先进的可视化、交互式漏洞分析、风险评估、修复和潜在原因分析。认知系统将能够发现异常状况和错误逻辑，并提供基于证据的推理。这可以让分析师权衡替代措施结果并提高决策水平。

使用案例：

释放认知

提升 SOC 分析师的能力

认知系统可以理解海量的结构化和非结构化数据，以迅速将初级分析师的价值从 1 级提升到 2 级或 3 级。认知系统可以自动摄取信息（如研究报告和最佳实践）以提供实时输入。以前，这种知识和洞察力只能通过多年的经验获得。

借助外部情报快速反应

当遭遇下一次“心脏出血”攻击时，人们将在博客上发布如何保护自己免受其害的博文。即使签名还不可用，在线自然语言仍可以帮助您解决问题。认知系统可以悄无声息地快速发现如何防御下一次的零日攻击。

借助高级分析识别威胁

认知系统可能使用各种分析方法来识别潜在的威胁，如机器学习、聚类、图形搜索和实体关系建模。它们可以帮助快速检测存在风险的用户行为、数据外泄和恶意软件，从而防患于未然。

加强应用程序安全性

认知系统可以理解分析和数据的语义上下文，同时探索代码和代码结构。它们可以分析数以千计的漏洞，并将结果精简为一组少量的可操作项目，并将您带到可以在该处修复漏洞的代码位置。

改进企业风险处境

在将来，认知系统可以分析大量的交互、交互的性质及其风险易感程度，为组织、企业行动、培训和再教育制定风险预测。认知系统可以使用自然语言处理功能来查找组织中的敏感数据并对其进行编辑。

未来：扭转网络犯罪经济

认知系统可以从大量的恶意软件中分析功能或特性，以便检测其细微的共性。这一点之所以重要，是因为恶意软件具有广泛的多样性，但网络犯罪群体会改进其代码，因此如今使用的许多恶意软件实际上与其他恶意软件相关。凭借认知系统，我们可以分析数以千计可疑的可执行文件的功能，并将它们聚集起来以发现其模式。甚至在无人了解这些功能、或者它们如何匹配或为何匹配的情况下，系统可以识别出一种模式来帮助发现新恶意软件变体并将其分类。

随着认知安全社区的增长和新攻击可行性的降低，网络犯罪将进入一个新的经济现实。开发逃避检测的恶意软件将变得越来越复杂且成本高昂。根据 Ponemon Institute 的 2015 Cost of Data Breach Study（2015 年数据泄露成本调查），组织检测高级持久性威胁所花费的平均时间为 256 天，美国数据泄露的平均成本是 650 万美元。认知安全将赋予安全分析师发现潜在攻击的早期预警的能力，大大加快了检测速度。网络罪犯会发现越来越难以实现收益。

认知计算正在驱动转型变革，它以闪电般的速度和广度利用数据以及意义、知识、流程和活动进展。对于拥抱认知功能的组织，其竞争优势将显而易见，影响深远。

认知生态系统的集成和专业知识

集成和专业知识对于正确的安全做法而言至关重要。过多的安全性做法都构建在许多尚未集成的单点产品之上，无法提供快速响应所需的可见性和可执行情报。

如果您的域功能不能跨混合 IT 环境彼此交互和通信，无法在整个生态系统中扩展到公司范围之外，这就不是彻底的集成。正确的集成有助于您获得所需的可见性，以便在发生安全事件时可以进行快速响应。集成使您事半功倍，这正是缩小安全技术差距的根本方法。

每天都会发现新威胁，这意味着安全专业知识和威胁情报共享至关重要。如果您的一系列解决方案和认知不具备顶级的专业知识，那么您将迅速落后。IBM X-Force Exchange 目前分类记录了超过 88,000 个漏洞的信息、多于 250 亿份网页以及 1 亿个端点的数据，可提供实时而全面的专业知识，以便立即采取行动。

IBM 如何为您助力

认知的旅程才刚刚开始，但 IBM 具备人才和财务实力去引领这场安全变革。每天，7500 多位 IBM Security 专业人士在全世界 36 个安全中心监控 133 个国家/地区的 350 亿次事件。IBM 在认知技术上的投资跨越了几十年，并在过去五年中取得了很大的进展——能够处理自然语言、声音和图像，还能将非结构化数据转变为知识图谱一样容易查询的工具。IBM 将拥抱认知，不断地增加安全使用案例，并将这些信息交给安全分析师。

现在，IBM Security 的解决方案中已具有认知功能。机器学习用来帮助提高检测漏洞的准确度并会优先处理这些漏洞，以便您可以更快地进行响应。行为学习用来主动预见并查找网络中正在发生的威胁周围的异常状况。

IBM Security 提供端到端的保护，以及涵盖深度分析、身份和访问、高级欺诈、数据、应用程序、网络、端点、云、移动和研究的免疫系统方法。上述每个平台都将受益于 IBM 的认知功能。如果您对认知安全的好处感兴趣，请考虑采用 IBM 将创新性地注入认知技术的平台。

立即采取的 3 个步骤

1. 了解有关利用认知功能智胜威胁的更多信息。
2. 制定提升安全成熟度的路线图，为认知做好准备。
3. 驱动安全基础结构的集成。

更多信息

请联系您的 IBM 代表或 IBM 业务合作伙伴，或者访问以下网站：ibm.biz/cognitivesec

关于 IBM Security

IBM Security 提供的企业安全产品和服务组合是所有产品中最高级和集成的产品之一。产品组合受世界知名的 IBM X-Force 研究和开发小组支持，可提供安全情报以帮助组织全面保护其员工、基础结构以及数据和应用程序，并提供针对身份和访问管理、数据库安全、应用程序开发、风险管理、端点管理以及网络安全等的解决方案。这些解决方案可让组织有效管理风险，并对移动设备、云、社交媒体和其他企业商务体系结构实施集成的安全性。IBM 运营着全球最广泛的安全研发和交付组织之一，每天在 133 个国家/地区监视 35 亿个安全性事件，并拥有 3,700 多项专利。

此外，IBM 全球融资部可以帮助您通过最具有成本效益和可行战略方式获得软件功能。我们可以与具有信用资格的客户合作，定制融资解决方案以满足您的业务和发展目标、实现有效的现金管理以及降低您的总体拥有成本。与 IBM 全球融资部合作，资助您的关键 IT 投资并推进业务发展。
有关更多信息，请访问 ibm.com/financing

创作于美利坚合众国，2016 年 4 月

SEW03134USEN-00