IBM Security

七个步骤
让 SOC 更安全，更现代

在采用网络安全认知解决方案之前先询问自己这七个问题

立即垂询 IBM Security
客服专线 400 665 7755

1

公司对于风险掌握与安全管控的平衡取舍是否让我放心？

首席信息安全官面临着技术领域最艰巨的任务：他们必须确保用户能够访问重要数据 - 同时还必须妥善保护数据，使其免遭内部威胁、认证滥用与人为失误的影响。他们的工作就是检测出并响应所有威胁 - 这是一项个无比艰巨的任务，因为仅能依赖于一个负担过重且人手不足的团队来完成。

更糟糕的是，市场对信息安全极为重视，其重视程度前所未有，没有丝毫余地。组织及其客户都需要确保安全性，监管机构也密切关注安全性。网络安全保险的保费飙升更是让情况雪上加霜。投资者们焦躁不安，律师们也束手无策。上至公司高层，下至普通员工，大家都需要确保绝对滴水不漏的安全性 - 同时他们本身也都有可能成为攻击者入侵漏洞的途径之一。

思考一下运筹管理清单上的这三个项目：

人才短缺

一线分析师往往都是业界新手。他们需要花费时间来培养调查威胁所需的技能、信心和技能成熟度。ESG Research 的相关报告显示，在 2108 年，51% 的组织表示其自身在网络安全技能方面存在“严重短缺”的问题，而在 2017 年，该比例只有 45%。网络安全工作疲劳是业界不争的事实；ESG 在相关报告中指出，38% 的网络安全专业人员认为技能不足会导致较高的员工倦怠率和流失率。

驻留时间太久 - 耗费大量成本

平均驻留时间因不同地区而异，大约从 50 天到 200 天不等。相比需要耗费 100 天以上才能识别出数据泄露事件的公司，在 100 天内识别出数据泄露事件的公司可节省超过 100 万美元的成本。

团队的洞察工作量超负荷 - 而您却帮不上忙

您的组织可能面临着网络安全工作疲劳这一难题（别紧张，您并不是唯一一家有此遭遇的组织）。重复性工作和繁琐的定义流程，早已让团队不堪重负。所有这些因素加起来，导致企业更容易错过真正重要的威胁指示器（IoC），而当您添加新的单点解决方案来应对最新的高级威胁时，只会让情况变得更糟：产生更多的数据孤岛，不但会增加集成的复杂性，还会增加分析师在洞察力分析方面的工作量。

SIEM 是运营不可或缺的要素之一，但 AI 的情况如何？哪个部分属于迷思？哪个部分才是真实？

2

AI 如何帮助我获得平衡?

您肯定听过 AI 宣讲者说起过 AI 的诸多优势，但如何能确保所投资的解决方案正是能够帮助您减轻工作负担的智能认知解决方案？抛开浮夸的观点，答案无外乎就是确保它能够学习且具备主动性。此外，它还要能实现可重复任务的自动化，以缓解工作疲劳，并解决您所面临的最大挑战 - 人。答案就是这么简单。

事实上，就算您的脚步再快，也不可能跟得上威胁范围的扩大步伐，尤其是您还需要忙于领导方面的事务、维护组织的安全态势、完成 SOC 的日常运营任务。因此，您需要一套一应俱全的工具来保护您的 SOC。

过去几年，AI 一直被大肆炒作，而且相关产品也卖得超好。这种情况我们都知道。但请您思考一下：如果能够在 SOC 中正确地运用 AI，就能够让 AI 成为一个高效工具，持续不断的自我学习、自行更新。AI 并非能治百病的万灵丹，但它肯定会成为您整套安全武器库中最重要的组件。

3

AI 实际上是以何种方式来强化我的安全武器库?

4

AI 是否会取代我的团队？基于 AI 的解决方案是否会威胁到员工生计?

AI 的目的在于与您的团队合作，而非与之对抗。AI 负责处理可重复的任务，协助您做出更明智的决策。AI 能够主动将来自各个来源的外部数据与您的原生环境结合，让您了解下一步应该采取的行动。不管在何种情况下，从非常耗时的任务到例行决策，AI 具体负担多少工作，完全都是由您决定的。简言之，AI 始终都在运行，也始终都在学习，而您则负责制定方向、掌控全局。

5

解决方案是 AI 还是机器学习？我是否了解两者的差别？

说起 AI 和“机器学习”之类的术语，人们经常会混用这些术语。更糟糕的是，大家还喜欢使用缩写词，例如喜欢说 ML 而不说“机器学习”、喜欢说 AI 而不说人工智能。不过千万不要被这些所混淆：AI（人工智能）和 ML（机器学习）并不一样，所以当您实际上想要部署 AI 时，千万不要误买到机器学习解决方案。机器学习着重于机器与数据之间的互动能力。它能够“学习”，甚至可以更改算法，因为它会接收更多的数据，但最终肯定会停止，毕竟机器学习只是 AI 的一个子集而已。

AI 则具备以算法为基础的认知能力，可以发展、学习和执行任务。它会通过持续充实知识的方式来增强您的 SOC，因为它能够从几乎无限多的来源收集数据 - 无论是整齐排列在数据库中可供搜寻的数据，还是由机器生成的数据（结构化数据）或者由社交媒体或杂志文章生成的数据（非结构化数据），它都能够收集。AI 不仅可以随时随地学习企业的内部数据，还可以学习来自博客、报告、研究与安全警报等的外部数据。这些就是 AI 与机器学习之间的区别。

通过在 SOC 中运用 AI，您可以访问机构记忆库，从中获得为您的组织量身定制的建议。AI 可帮助您实现安全运营与解决方案之间的平衡 - 因此确定您所购买的解决方案是否是真正的 AI 解决方案非常重要。

6 我可以通过 AI 获得哪些安全态势方面的增益?

自动链接不同的潜在事件。

AI 非常擅长根本原因分析流程的自动化和集成。AI 能捕捉关联，帮助您获得威胁与风险洞察力，而且永远不会疲倦。AI 还能够显示人员可能会因为员工流转、经验不足或时间推移而遗漏掉的相互关系。如果没有 AI，经验不足的分析师就可能会忽略一些很重要的警示，因为他们误认为这些只是单一的攻击事件而已。AI 能够使用认知推理来寻找事件之间的共同点，并提供可执行的反馈和情境 – 这些共同点可能是来自昨天刚刚处理完毕的服务票据，也可能是数个月前处理的服务票据。AI 还能够收集外部威胁情报，为分析添加更多情境信息，进而捕获其他人可能遗漏掉的内容。

解决人力问题。

AI 能够判断根本原因分析，还能够根据其针对威胁及组织的特定情况所构建的知识来统筹安排后续步骤。AI 不需要“休假”，也永远不会“离职”，而且您也不必担心会遗漏重要的 IoC。

每次都会推动一致且深入的调查。

AI 能够读取非结构化数据与结构化数据，而且其数量要远远超出人类可读取的数据量。除了具备学习能力之外，AI 还可通过一个更快、更具决策性的报告流程为您提供相应信息，帮助您缩短平均检测时间 (MTTD) 与平均响应时间 (MTTR)。此外，AI 能够提供高级分析，以检测已知威胁与未知威胁。AI 每次都会推动一致且深入的调查，让分析师能够作出数据驱动型决策，而不是光凭感觉行事。

具备跨人员、流程和技术的健全自动化事件响应工作流。

AI 通过由数据与证据驱动的快速、完整响应流程为安全分析师提供指导。它能够实现工作流与补救流程的完全自动化。它能够让 SOC 可以持续地评估并精简流程。

7

AI 在攻击之前、期间和之后三个阶段中分别以何种方式来改善 SOC?

在数据泄露之前、期间和之后，AI 能够让 SOC 更妥善地做好准备并快速完成恢复。IBM QRadar Security Intelligence Platform 采用了此项技术并将其集成到您的 SOC 中，进而提供了一款全方位的分析解决方案 - 所有这一切都是在单个平台上完成的。

攻击之前	攻击期间	攻击之后
IBM QRadar SIEM 可提供完整的可视性，且能够在攻击周期中及早识别威胁和异常。	**IBM QRadar SIEM** 能够不断收集持续证据，实现对取证数据的轻松访问。它能够根据业务影响对数据进行优先排序。	**IBM QRadar SIEM** 能够根据经验教训不断地调优检测机制。
IBM QRadar Advisor with Watson 能够自动调查所有异常并识别高风险的攻击行为。	**IBM QRadar Advisor with Watson** 能够实现根本原因分析流程的自动化，让团队的战力倍增，还能够帮助您了解威胁的全部范围。	**IBM QRadar Advisor with Watson** 能够不断调整响应模型，进而提升未来的威胁检测准确性。
IBM Resilient 能让 SOC 准备好跨人员、流程和技术的健全自动化工作流。	**IBM Resilient** 能够通过快速、完整的响应流程为安全分析师提供指导，而且可实现事件工作流程与补救流程的自动化。	**IBM Resilient** 让 SOC 能够持续地评估并精简流程。

关于 IBM QRadar Advisor with Watson

借助 AI，您可以优化 SOC 运营，同时成功阻止不断增多的网络威胁。IBM® QRadar® Advisor with Watson 可自动执行例行 SOC 任务、找出调查之间的共同点，并为分析师提供可执行的反馈意见，使分析师能够专注于调查更重要的元素，提高工作效率。

了解更多

立即垂询 IBM Security
客服专线 400 665 7755

参考文件

The State of Cyber Security Professional Careers, **ESG**

IBM Security