IBM QRadar Advisor with Watson

借助 AI 实现 SOC 自动化

亮点

- 解锁分析师与其技术之间的新伙伴关系
- 实现事件分析自动化并成本提升团队效率
- 推动一致的、更深入的调查
- 更快、更果断地提交事件
- 缩短驻留时间

当今 SOC 面临的挑战

无论您有一个两人组成的安全团队还是由 100 人组成的安全团队，目标都是确保业务蓬勃发展。这意味着您需要保护关键系统、用户和数据，检测和响应威胁，同时领先于网络犯罪。不过，当今 SOC 所面临的许多严峻挑战可能会阻碍您实现这些目标。

未处理的威胁

之所以有太多的信息被忽略，是因为您的分析师可能不知道信息的连接方式。分析师很难发现可执行的洞察力，然后他们可能会仅选择处理他们有信心解决的案例，如此一来就可能会导致缺少某些调查并使您的组织面临风险。

洞察力“超载”

需要分析的洞察力数量庞大、种类繁多且速度很快，因此很难对工作进行优先排序并找出根本原因。各种规模的公司都是如此。分析师不知道从何处着手将本地情境连为一体，以便他们快速确定当前问题。重复工作也使他们不堪重负，并且大多数分析师都为此感到疲倦，导致既定流程崩溃，进而很可能会错过重要的威胁指示器 (IoC)。93%[1] 的组织无法对所有相关威胁进行分类。近四分之一[2] 的组织认为他们足够幸运，能够在不调查这些警报的情况下避免相应的业务影响。

驻留时间越来越长

在衡量数据保护与防御是否成功方面，安全专业人员最常用的指标之一是驻留时间，该指标主要是指 MTTD (平均检测时间) 和 MTTR (平均响应时间)。驻留时间用于衡量威胁实施者在网络中拥有未被检测到的访问权限到此类访问权限被彻底删除之前所经过的持续时间。

尽管组织拥有比以往更多的解决方案和数据，但如今的平均驻留时间仍旧长达 50 天到 200 天。为什么该指标如此重要？Ponemon Institute 相关调研结果显示，相比需要耗费 100 天以上识别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。同样，与那些需要花费 30 天以上的时间才能遏制泄露的公司相比，那些可在 30 天内遏制泄露的公司可节省超过 100 万美元。[3] 缺乏一致、高质量且内容丰富的调查会导致现有流程崩溃，而且很可能会丢失关键洞察力，从而使您的组织面临风险。

缺乏网络安全人才和工作疲劳

像大多数安全分析师一样，您的团队也可能会面临工作过度、人员不足和不堪重负等问题，这些不是他们的错。我们不可能跟上不断扩大的威胁态势，尤其是在 SOC 团队需要处理日常繁忙的安全操作任务的情况下更是如此。

很多组织都像您一样，遇到国网络安全工作疲劳的情况。ESG Research 的相关报告显示，在 2018 年，51% 的组织宣称自身在网络安全技能方面存在“严重短缺”的问题。在 2017 年，该比例为 45%。[4] 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高的倦怠率和员工流失率。我们预计，情况只会随着数据量的持续增长、技能差距的不断扩大而恶化；到 2022 年，将会出现 180 万个安全岗位缺口。第 1 级或前线分析师通常都是行业和团队的新手。[5]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。

快速采用更多的单点解决方案

CISO 正在采用更多的单点解决方案来阻止不断发展的新威胁。无论使用哪种用例（保护关键数据、内部威胁、身份和访问管理、凭证滥用或其他原因），都一定会被繁杂的解决方案所淹没。因此，解决方案之间的集成、规模不足和难以使用也已成为组织所面临的严重问题。

风险创历史新高

抱怨解决不了任何问题，也不能帮助您重新获得烦恼客户的信任。Ponemon Institute 的相关数据显示，数据泄露的平均总成本已从 362 万美元增至 386 万美元，比 2017 年增长了 6.4%。[6] 安全领导者还面临着越来越多来自各种渠道的审查，包括行政领导、客户、员工、投资者、监管机构、保险公司和监管小组等等。面对前所未有的高风险，您的组织是否能够承受住不做准备而造成的后果?

解锁分析师与其技术之间的新伙伴关系

人工智能可以弥补这一差距，并解锁安全分析师与其技术之间的新协作方式人类与技术各有各的长处，比如说人类具有丰富的常识，而人工智能可以消除偏差、进行权衡分析。不过两者组成一个团队之后，便可以更好地阻止威胁并减少驻留时间。

AI 在 SOC 中的优势

实现事件分析自动化并让您的团队事半功倍

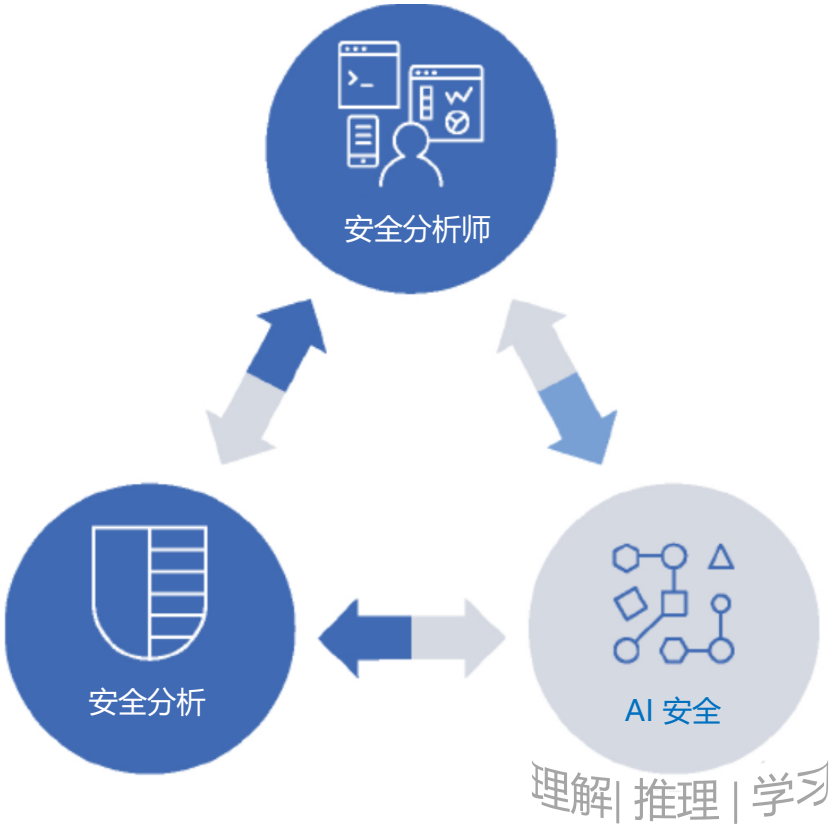
您不要在常规分析上浪费人力资本。取而代之的是，让 AI 自动执行重复的 SOC 任务，让分析师可以更好地专注于调查流程中更重要的元素，同时提高分析师的效率。

推动一致的、更深入的调查

您是否知道：分析师仅能应对完成工作所需信息中 8% 的数据。您可以让 AI 使用认知推理技术自动发现事件之间的共性，进而实现 SOC 升级，同时提供带有情境信息的可执行反馈。将 AI 视为您的私人顾问 - AI 应该走出去，收集外部威胁情报，为您的分析添加更多情境信息，而且应该将相关的不同潜在事件关联到一起，进而节省更多时间。无论是星期五的下午 4:30 还是星期一的下午 10:00，您的分析师每次都应该专注于进行一致而彻底的调查。

缩短驻留时间

通过更快、更果断的提交流程来降低 MTTD 和 MTTR。将攻击映射到您的动态运行手册（例如 MITER ATT&CK 模型），确定根本原因分析并充满信心地推进下一步。



AI 解锁了分析师与其技术之间的新伙伴关系

IBM QRadar Advisor with Watson - 基于 AI、面向一线安全分析师而构建

借助 IBM QRadar Advisor，安全分析师能够进行一致的调查，更快、更果断地提交事件，进而缩短驻留时间并提高分析师效率。

成倍提升团队效率

- 对风险最大的调查列表进行优先排序
- 根据关键程度更快地过滤和分类数据
- 使用内部和外部威胁情报提要来处理经增强的 IBM Watson 反馈

推动一致的、更深入的调查

- 借助交叉调查分析功能，通过关联的可观察对象自动关联调查，并扩展到当前潜在事件之外
- 避免重复劳动
- 在同一事件触发多次重复调查时，确定是否需要进行其他调整

缩短驻留时间

- 使用 MITRE 的 ATT&CK 模型实现攻击发生及发展方式、每个进展的置信度、发生的策略以及仍旧可能发生的策略的可视化
- 利用 Easy Incident Scoring 为分析师提供更快、更果断的提交流程
- 提高分析师效率并降低 MTTD 和 MTTR

不要只相信我们所说的。了解我们的客户借助 AI 所实现的优势。卢森堡 Sogeti 的分析师将调查时间从 2~3 个小时缩短到 2~3 分钟。分析师可以利用这些宝贵的时间，进一步调查实际威胁、为调查添加更多的情境信息。我们的许多其他客户也使用 AI 来提升团队的工作效率。借助 AI，他们能够让技能水平较低的人员来担任 1 级分析师，让当前的 1 级分析师专注于 2 级分析师的职责，进而提升整个团队的效率。

有关更多成功案例以及有关如何利用 AI 的更多信息，敬请访问 **ibm.biz/learnAI**

[1] McAfee Labs Threat Report，McAfee，2016 年。

(**https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/rp-quarterly-thre atsdec- 2016.pdf)**

[2] McAfee Labs Threat Report，McAfee，2016.

(**https://www.mcafee.com/content/dam/enterprise/en-us/assets/reports/rp-quarterly-thre atsdec- 2016.pdf**)

[3] Cost of a Data Breach，Ponemon，2018 年。

(**https://www.ibm.com/security/ data-breach**)

[4] Cybersecurity Realities and Priorities for 2018 and Beyond，Enterprise Strategy Group，2018 年。

(**https://www.thehaguesecuritydelta.com/media/com_hsd/report/213/document/ESG-Res earch-Insights-Paper- Spirent-2018.pdf**)

[5] Cybersecurity Realities and Priorities for 2018 and Beyond，Enterprise Strategy Group，2018 年。

(**https://www.thehaguesecuritydelta.com/media/com_hsd/report/213/document/ESG-Res earch-Insights-Paper- Spirent-2018.pdf**)

[6] Cost of a Data Breach，Ponemon，2018 年。

(**https://www.ibm.com/security/ data-breach**)

有关更多信息

有关 QRadar Advisor with Watson 的更多信息，请联系您的 IBM 代表或访问以下网站：**ibm.com/us-en/marketplace/cognitive-security-analytics**

有关 IBM 未来发展方向及意图的声明如有变更或撤销，恕不另行通知，且仅用于说明目标之用。