由 IBM Security 委托 Forrester
开展的“总体经济影响™”调研
2019 年 5 月

IBM QRadar Advisor With Watson 之总体经济影响分析报告

人工智能为企业安全团队带来的成本节省和业务收益

FORRESTER®

目录

概述

主要发现 **1**

TEI 框架与方法 1

IBM QRadar Advisor with Watson 客户之旅 4

受访企业 **5**

主要挑战 5

解决方案需求 5

主要成果 6

收益分析 6

SOC 分析人员生产力节省 **7**

避免的调查外包费用 7

企业安全状况改善 8

不可量化的收益 9

灵活性 11

成本分析 11

支付给 IBM Security 的费用 **12**

支付给外部威胁情报资源的费用 12

实施和培训的资源成本 12

财务摘要 14

IBM QRadar Advisor With Watson：概述 **16**

附录 A：总体经济影响 **17**

附录 B：尾注 **18**

19

项目总监：

Richard Cavallaro

Kathleen Byrne

关于 FORRESTER CONSULTING

Forrester Consulting 提供独立客观的研究咨询，助力企业领导取得成功。无论是简短的战略对话，还是定制项目，Forrester 的咨询服务都能让您直接体验到调研分析师的专家洞察，轻松应对特定的业务挑战。要了解详细信息，请访问：forrester.com/consulting。

FORRESTER®

主要收益

SOC 分析人员生产力节省

180 万美元

避免的调查外包费用

126,829 美元

企业安全状况改善

651,936 美元

概述

企业的安全职能部门迫切需要掌握适当技能的安全专业人员。在 Forrester Analytics 的 2018 年全球企业科技消费 (Global Business Technographics®) 安全调研中，决策者指出，安全运营 (39%) 和威胁情报 (26%) 是自己企业中最重要但严重缺乏的两项技能。[1] 即使企业拥有具备这些关键技能的安全员工，也需要采取适当的步骤，最大程度提高他们的工作效率，以便在日益复杂的威胁环境中，用更少的资源完成更多的工作。

IBM Security 为其 QRadar SIEM（安全信息与事件管理）平台提供了一个应用 — Advisor with Watson，旨在为安全分析人员提供 IBM Watson 人工智能功能，自动执行安全运营中心（SOC）的例行任务，提高威胁优先级划分、调查和最终上报的效率。

IBM Security 委托 Forrester Consulting 开展了“总体经济影响”(Total Economic Impact™, TEI) 调研，深入分析企业通过部署 QRadar Advisor with Watson 可能实现的投资回报 (ROI) 。本次调研旨在为读者提供一个框架，用于评估面向 QRadar 的 Advisor with Watson 应用对其组织的潜在财务影响。为了更好地了解与此项投资相关的收益、成本和风险，Forrester 采访了一家拥有多年 QRadar Advisor with Watson 使用经验的客户。

在采用 QRadar Advisor with Watson 之前，该受访企业为了应对警报中所指出的大量威胁而疲于奔命。他们的调查过程时间过长，而且缺少分析人员，使得许多可能导致严重后果的威胁未进行调查，更谈不上解决了。

而在部署 QRadar Advisor with Watson 之后，该组织的威胁调查过程从几小时缩短到了几分钟。因此，该组织可以开展更多的调查，而 SOC 分析人员则可以专注于主动出击，更好地保护组织免受威胁。

主要发现

可量化的收益。根据风险对现值（PV）进行调整之后，这家受访企业取得了以下可量化的收益：

- **SOC 分析人员生产力节省 180 万美元。**通过自动执行以前由人力完成的与威胁调查相关的繁琐任务，受访企业将威胁调查的平均时间从 4 小时缩短至 20 分钟以内。这节省了 SOC 分析人员将近 50% 的调查工作时间，使他们能够集中精力从事其他前瞻性的安全任务。通过将一级调查工作中多出的部分分配给网络运营中心（NOC）的分析人员，该组织还帮助 SOC 减少了未来的招聘工作。
- **避免了 126,829 美元的调查外包费用。**在使用 QRadar with Watson 之前，该受访企业将第二和第三级调查外包给管理服务提供商。随着 SOC 效率的提高，他们能够由内部的资深 SOC 分析人员完成这些工作。

ROI

收益现值
250 万美元

净现值
170 万美元

回报期
8 个月

> **企业安全状况改善收益为 651,936 美元。**由于平均威胁调查时间和 NOC 工作人员协助低级别调查的准备时间缩短，该受访企业每年的调查项目从大约 1800 项增加到 7000 多项。在将 Advisor with Watson 添加到 QRadar 之前，这些额外的威胁都没有经过调查，因此更谈不上解决。这些全新的调查使得严重安全漏洞的威胁降低了 8%。

不可量化的收益。这家受访企业还获得了以下本次调研未进行量化的收益：

> **安全及网络运营人员的专业发展。**生产力的提高使得安全运营和网络运营人员有时间专注于职业发展任务。受访企业指出，NOC 人员开始培养威胁发现技能，而 SOC 人员越来越善于进行较高级别的威胁调查。

成本。这家受访企业经过风险调整后的现值成本如下：

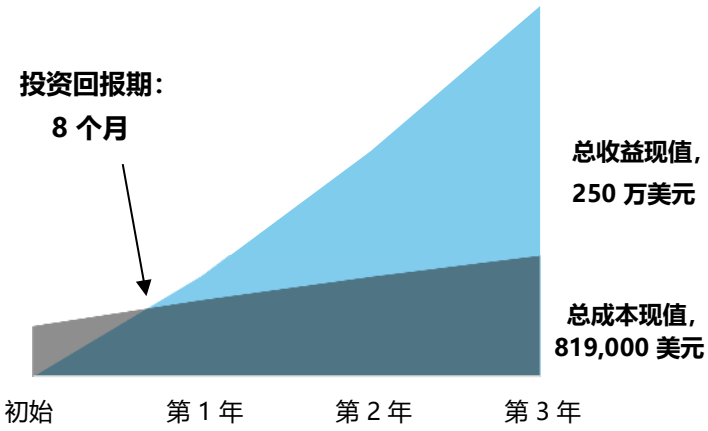
> **支付给 IBM Security 的费用。**该受访企业为 QRadar Advisor with Watson 支付了软件许可费用，三年期现值为 198,948 美元。

> **支付给外部威胁情报资源的费用。**该组织的 SOC 和 NOC 分析人员在使用 QRadar Advisor with Watson 的同时，还使用了几个外部威胁情报资源，为 Watson 提供了额外的学习循环。这使得他们能够从 Advisor with Watson 的机器学习能力中获得更多的收益。该组织在这些服务上投入的三年期现值成本为 273,554 美元。

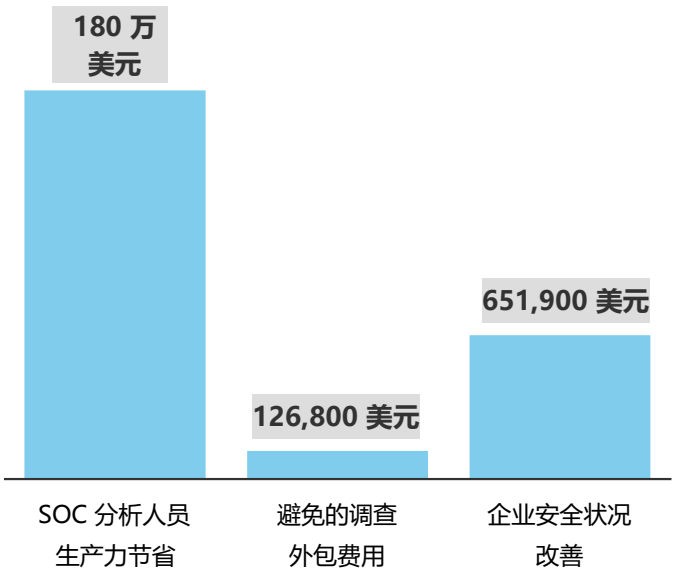
> **实施和培训的资源成本。**为了最大程度利用 QRadar Advisor with Watson 投资，在 12 个月的部署期间，该受访企业在 SOC 和 NOC 人员的配置、实施和培训方面投入了大量的工作时间。该组织在这些工作时间上投入的三年期现值成本为 346,785 美元。

通过开展访谈以及随后进行财务分析，Forrester 发现这家受访企业在三年内获得了 250 万美元的收益，而成本为 819,287 美元，净现值 (NPV) 等于 170 万美元，投资回报率为 210%。

财务摘要



收益（三年）



FORRESTER®

TEI 方法帮助企业向高级管理层和其他主要业务利益相关方展示、证明并实现 IT 计划的切实价值。

TEI 框架与方法

根据访谈中得到的信息，Forrester 为考虑实施 IBM QRadar Advisor with Watson 的企业构建了“总体经济分析”(Total Economic Impact™, TEI) 框架。

该框架旨在确定影响投资决策的成本、收益、灵活性和风险因素。Forrester 采用多步骤方法来评估 IBM QRadar Advisor with Watson 可能对企业造成的影响：

尽职调查

采访 IBM Security 利益相关方和 Forrester 分析师，以收集与 IBM QRadar Advisor with Watson 相关的数据。

客户访谈

采访了一家使用 IBM QRadar Advisor with Watson 的企业，以获取有关成本、收益和风险的数据。

财务模型框架

使用 TEI 方法，根据代表性的访谈构建财务模型，并根据受访企业的问题和关注点对财务模型进行风险调整。

成功案例

我们采用 TEI 的以下四个基本要素模拟 IBM QRadar Advisor with Watson 的影响：收益、成本、灵活性和风险。考虑到企业对 IT 投资开展相关的 ROI 分析变得越来越熟练，因此，Forrester 的 TEI 方法旨在帮助客户全面了解采购决策的总体经济影响。有关 TEI 方法的更多信息，请参阅附录 A。

IBM QRadar Advisor with Watson 客户之旅

IBM QRadar Advisor with Watson 投资前后

受访企业

在本次调研中，Forrester 采访了一家使用 IBM QRadar Advisor with Watson 的客户：

> Forrester 采访了该企业中安全团队的一名高级成员，他在安全团队中既负责运营，同时个人也从事具体安全工作。

> 该受访企业是总部位于美国的全球性技术解决方案提供商。在 2018 财年，该组织报告的收入超过 190 亿美元，在全球拥有超过 1.5 万名员工。

> 在添加 Advisor with Watson 功能之前，该组织多年来一直使用 IBM QRadar 作为安全事件和信息管理平台。IBM QRadar 目前的版本是 7.31，计划在本报告发布时更新到 7.32。

> 该组织在与 IBM Security 合作进行了 12 个月的 beta 测试项目后，部署了 QRadar Advisor with Watson。该受访企业目前使用的版本是 V1.16，计划升级至 V2.0。

> 使用 QRadar Advisor with Watson 的团队包括 SOC 和 NOC 的 24 名工作人员。

“我们希望有解决方案能够帮助我们缩短完成调查的时间，这样我们就可以推进到威胁补救和缓解周期。”

技术解决方案高级企业安全分析师

主要挑战

该受访企业表示，以下挑战促使他们决定实施 QRadar Advisor with Watson：

> **威胁调查过程冗长而繁琐。**日志审查和外部威胁研究等人工调查任务增加了分析人员用于调查每种威胁的平均时间。受访者告诉 Forrester：“每次威胁调查都需要耗费 4 小时到几周不等的时间。有几次调查的持续时间甚至要按月计。”这限制了分析人员寻找威胁或采取其他前瞻性措施以提高组织安全性的能力。

> **企业安全团队被过度利用。**该组织安全运营中心的分析人员在威胁调查方面花费了过多的时间。受访者估计，分析人员将大约 65% 的工作时间用于执行调查任务。

> **威胁补救措施往往为时已晚。**由于繁琐的调查过程，安全团队无法始终如一地及时从调查任务转向补救工作。这进一步让企业暴露在安全风险之下。

“鉴于我们团队的规模，威胁调查几乎占用了我们所有的时间。我们 65% 的时间都用在了调查上。”

技术解决方案高级企业安全分析师

- **安全威胁未得到解决。** 以该企业现有的威胁调查能力，完全无法应对所面临的威胁的数量。威胁的优先级划分也是 SOC 分析人员面临的一项挑战。

解决方案需求

受访企业所期望的解决方案必须：

- 能够与 QRadar 环境以及安全团队当前使用的其他安全工具进行交互。
- 要足够直观，适合初级安全人员使用并熟练掌握。

主要成果

采访揭示了 IBM QRadar Advisor with Watson 投资实现的几个主要成果：

- **实现了调查自动化。**借助 QRadar Advisor with Watson，原来与威胁优先级划分和调查相关的冗长而且重复的任务现在都可以自动完成，从而使平均调查时间从几个小时缩短到几分钟。
- **扩大了威胁调查的范围。**随着每项单独调查所花的时间显著缩短，该企业能够在相同的时间内调查更多以前来不及调查的威胁。
- **与网络运营中心（NOC）合作，应对超量的调查。**借助 QRadar Advisor with Watson 的直观功能，该企业网络运营中心内几乎没有接受过正规安全培训的工作人员能够轻松成为多面手，帮助进行一级威胁调查。由于获得了 NOC 的支持，因此 SOC 人员能够解放出来，专注于更高级别的调查，主动发现威胁。
- **赋能 SOC 分析人员，主动出击。**由于花费在调查低级别威胁上的时间减少，使得 SOC 分析人员能够主动去搜索更高级别的威胁。受访者表示，企业因此能够更有效地防范漏洞和威胁。

> “即便是最复杂的查询，Watson 也能在 3 到 4 分钟内返回结果。”
>
> *技术解决方案高级企业安全分析师*

收益分析

量化的收益数据

总收益

参考	收益	第 1 年	第 2 年	第 3 年	总计	现值
Atr	SOC 分析人员生产力节省	455,760 美元	725,760 美元	995,760 美元	2,177,280 美元	1,762,258 美元
Btr	避免的调查外包费用	51,000 美元	51,000 美元	51,000 美元	153,000 美元	126,829 美元
Ctr	企业安全状况改善	247,040 美元	262,851 美元	279,673 美元	789,564 美元	651,936 美元
	总收益（根据风险调整后）	753,800 美元	1,039,611 美元	1,326,433 美元	3,119,844 美元	2,541,023 美元

SOC 分析人员生产力节省

受访者告诉 Forrester，该企业希望通过 QRadar Advisor with Watson 解决的最大难点，是有效提高分析人员的生产力。每项调查都需要分析人员花费大量时间，消耗大量资源，导致他们根本无暇顾及前瞻性的活动。

鉴于安全人才短缺，企业亟需找到有效的方法，将 SOC 分析人员（尤其是较高级别的人员）从调查和优先级划分任务中解放出来，从而能够集中精力从事前瞻性的安全任务，改善企业的整体安全状况。受访者告诉 Forrester：

- 由于缺乏结构化的搜索和优先级划分流程，分析人员不得不在调查过程的前期花时间研究威胁。
- 每次威胁调查平均花费分析人员 4 个小时，还有一些则需要花费数周时间。
- SOC 分析人员每天投入 65% 的时间调查威胁，其中大部分是一级威胁。
- 冗长的调查周期延缓了威胁补救工作的实施，可能导致威胁或威胁制造者有更多的时间搞破坏。

为 QRadar 添加 Advisor with Watson，对于该企业 SOC 分析人员生产力的提高起到了立竿见影的作用。Watson for Cyber Security 直观的搜索功能可以帮助分析人员自动划分优先级，大大缩短了研究威胁和完成调查所需的时间。

最重要的好处之一，是能够灵活地让 NOC 工作人员参与进来，帮助调查超额的一级威胁。由于 Advisor with Watson 直观易用，该企业中很少或没有参加过正式安全培训的 NOC 工作人员也能够轻松承担 SOC 的大部分一级威胁调查工作。由于 NOC 能够分担调查工作，也使得该企业不必雇用更多的 SOC 人员。受访者告诉 Forrester：“是的，因为采用了 Advisor，所以我们无需再雇用更多的分析人员。”

上表显示了下列领域的所有收益总额，以及贴现 10% 之后的现值 (PV)。预计该受访企业根据风险调整后的三年总收益将超过 250 万美元。

受访企业的 SOC 分析人员节省了 50% 先前用于处理手动 SOC 任务的时间。

“我利用一个 NOC 中心，与 Watson 共同开展调查工作。虽然他们的网络运营人员，没有接受过安全培训，但我们的团队只需为他们编写一份快速操作指南就可以了。”

技术解决方案高级企业安全分析师

> 实施 QRadar Advisor with Watson 之后，平均调查时间从以前的 4 小时缩短到 10 分钟以内。

> SOC 分析人员用于调查的总时间从他们总工作时间的 65% 下降到了 15%。这使得接受过正规安全培训的 SOC 分析人员能够专注于更高级别的威胁调查和企业的前瞻性安全措施。

> 过去三年中，该企业通过将威胁调查任务分配给 NOC 员工，少雇用了 9 名分析师。

对于财务模型，Forrester 假设：

> 满负荷工作的 SOC 分析人员的薪资为 100,000 美元；满负荷工作的 NOC 分析人员的薪资为 62,000 美元。

> SOC 分析人员将节省下来的工作时间的 75% 用于执行 SOC 的其他增值任务。

> NOC 分析人员将他们总工作时间的 30% 用于执行威胁调查。

此收益因以下因素而异：

> 企业中 SOC 人员的技能和能力。

> 企业用于发挥 Advisor with Watson 全部潜能的 QRadar 环境的配置。

> 高质量威胁情报来源的可用性。

为了抵消这些风险，Forrester 将此项收益调低了 10%，根据风险调整后的三年总现值为 180 万美元。

"如果没有 QRadar Advisor 的帮助，我们的团队根本无法处理每天发生的大量安全警报。"

技术解决方案高级企业安全分析师

借助 QRadar Advisor with Watson，威胁调查的平均时间从 **4 小时**缩短到 **10 分钟。**

SOC 分析人员生产力节省：计算表

参考	指标	计算	第 1 年	第 2 年	第 3 年
A1	SOC 分析人员总数	访谈数据	6	6	6
A2	SOC 分析人员工作时间节省的百分比	(65%-15%)	50%	50%	50%
A3	生产力提高		75%	75%	75%
A4	SOC 少雇佣的人数	访谈数据	3	6	9
A5	SOC 分析人员年薪		100,000 美元	100,000 美元	100,000 美元
A6	NOC 分析人员年薪		62,000 美元	62,000 美元	62,000 美元
A7	NOC 分析人员每天花在调查上的时间百分比	访谈数据	30%	30%	30%
A8	调查工作人力节省	(A4*A5)-(A6*A7)	281.400	581.400	881.400
At	SOC 分析人员生产力节省	(A1*A2*A3*A5) + A8	506,400	806,400	1,106,400
	风险调整	↓10%			
At	因 SOC 分析人员生产力提高而节省的成本（根据风险调整后）		455,760	725,760	995,760

避免的调查外包费用

事实证明，更高级别的威胁调查对该企业而言是个挑战，因为他们缺少经验较为丰富的 SOC 人员。分析人员将大量时间花在了低层次的调查上，因此很多更高层次的威胁没时间调查。为了缓解这一问题，该企业考虑将较高级别的调查外包给安全管理服务提供商 (MSSP)，这和 Forrester 采访的面临类似挑战的其他企业的做法一样。[2] 然而，受访者承认，这是一个存在天生缺陷的解决方案，因为对威胁进行调查后，采取补救措施的责任仍由企业安全团队承担。受访者告诉 Forrester： “我们没有配备现场三级人员，而是将这方面的职责外包给一家安全管理服务提供商，由他们负责进行更高级别的调查。但是，调查之后的补救工作仍然由我们负责。” 该企业与 MSSP 进行沟通的过程还有可能造成调查与补救之间产生时间差。

对于财务模型，Forrester 假设：

> 该企业每年向管理服务提供商支付 660,000 美元，用于进行更高级别的威胁调查。

此收益因以下因素而异：

> 企业安全组织应对威胁调查的能力。

> 有能力调查更高级别威胁的熟练 SOC 分析人员的可用性。

为了抵消这些风险，Forrester 将此项收益调低了 15%，根据风险调整后的三年总现值为 126,829 美元。

影响风险是指可能因投资无法满足企业的业务或技术需求而降低总体效益的风险。不确定性越大，收益估算结果的潜在范围越大。

避免的调查外包费用：计算表

参考号	指标	计算	第 1 年	第 2 年	第 3 年
B1	避免 2 级和 3 级调查外包	访谈数据	60,000 美元	60,000 美元	60,000 美元
Bt	避免的调查外包费用		60,000 美元	60,000 美元	60,000 美元
	风险调整	↓15%			
Btr	避免的调查外包费用（根据风险调整后）		51,000 美元	51,000 美元	51,000 美元

企业安全状况改善

在实施 QRadar Advisor with Watson 之前，以该企业安全团队当时的威胁调查能力，完全无法应对所面临的威胁的数量。结果就是潜在的关键安全威胁没有得到调查和处理，使企业暴露在巨大的风险之中。

> 受访者告诉 Forrester，由于调查过程冗长，企业安全团队每天只能彻底调查 5 个威胁。

部署了 QRadar Advisor with Watson 之后，随着平均调查时间缩短，企业能够在相同时间内调查更多的威胁。由于 NOC 工作人员也能使用 Watson for Cyber Security，协助 SOC 工作人员进行更多调查，因此资深 SOC 分析人员就可以解放出来，专注于威胁捕获，从事更高级别的调查，为企业提供更高水平的主动保护。

通过使用 QRadar Advisor with Watson，每年可以多调查超过 7000 个威胁

受访者告诉 Forrester： “我们觉得，采用 Advisor [with Watson] 之后，发生数据泄露的风险已经显著降低。”

- 受访者告诉 Forrester，在实施了 QRadar Advisor with Watson 之后，该企业调查威胁的能力（从每天 5 个）提升至每天调查 25 到 50 个。
- 在一年的时间里，该企业能够调查超过 7000 个全新的威胁，而在以前这些调查可能会被忽视。
- 该组织因未调查威胁而造成重大泄露的风险降低了 8%。

对于财务模型，Forrester 假设：

- 根据 2018 年 Ponemon Institute 的调研，安全漏洞造成的平均损失为 386 万美元。[3]
- 数据泄露的平均成本每年增加 6.4%。

此收益因以下因素而异：

- 企业的 QRadar 威胁情报配置的调优和严格程度。
- 高质量威胁情报来源的可用性。
- 企业安全人员的技能和能力。

为了抵消这些风险，Forrester 将此项收益调低了 20%，根据风险调整后的三年总现值为 651,936 美元。

> “我们觉得，采用 Advisor [with Watson] 之后，发生数据泄露的风险已经显著降低。”
>
> *技术解决方案高级企业安全分析师*

企业安全状况改善：计算表

参考	指标	计算	第 1 年	第 2 年	第 3 年
C1	数据泄露的平均成本	每年增加 6.4%	3,860,000 美元	4,107,040 美元	4,369,891 美元
C2	借助 QRadar Advisor with Watson 减少的泄露可能性		8%	8%	8%
Ct	企业安全状况改善	C1*C2	308,800 美元	328,563 美元	349,591 美元
	风险调整	↓20%			
Ctr	企业安全状况改善（根据风险调整后）		247,040 美元	262,851 美元	279,673 美元

不可量化的收益

受访者提到了一项在本调研中无法量化的关键收益：

- **安全及网络运营人员的专业发展。**受访企业整体生产力的提高，使得安全运营和网络运营人员能够专注于职业发展任务，而如果没有实施 QRadar Advisor with Watson，这是不可能实现的。受访企业指出，NOC 人员能够专注于培养威胁发现技能，而 SOC 人员越来越善于进行较高级别的威胁调查。“我们计划扩大安全运营中心，开始培训工作人员成为二级和三级威胁猎手。”虽然受访者没有明确指出，但 Forrester 的研究注意到了员工工作满意度和员工留任之间的关系，这可能会在防止员工流失方面（招聘、培训）帮助企业节省成本。[4]

QRadar Advisor with Watson 可以帮助非安全背景的员工培养威胁调查技能。

灵活性

灵活性的价值显然因客户而异，价值衡量标准因组织而异。许多情况下，客户都是先行选择实施 QRadar Advisor with Watson，然后才意识到该产品的其他用途和商机，包括：

- **在 2.0 版本中扩展 QRadar Advisor with Watson 的功能。**受访者提到，该企业计划升级到 QRadar Advisor with Watson V2.0，以便利用这个版本提供的额外学习模型和网络犯罪行为战术手册。
- **随着时间的推移，从 Watson for Cyber Security 中获得更大价值。**借助 QRadar Advisor with Watson 的机器学习功能，企业部署应用的时间越长，就会经历越多的学习循环。这相当于获得更聪明的 AI，因此能够为使用该应用的分析人员带来更多利益。

如果作为特定项目的组成部分进行评估，灵活性也可被量化（附录 A 中有详细说明）。

根据 TEI 的定义，灵活性是指企业投资增加额外的容量或功能，可转化为商业利益，产生更多的投资价值。这使得企业有“权利”或能力规划未来投资，但并非强制。

成本分析

量化的成本数据

总成本

参考	成本	最初	第 1 年	第 2 年	第 3 年	总计	现值
Dt	支付给 IBM Security 的费用	0 美元	80,000 美元	80,000 美元	80,000 美元	240,000 美元	198,948 美元
Etr	支付给外部威胁情报资源的费用	0 美元	110,000 美元	110,000 美元	110,000 美元	330,000 美元	273,554 美元
Ftr	实施和培训的资源成本	343,200 美元	2,750 美元	688 美元	688 美元	347,325 美元	346,785 美元
	总成本（根据风险调整后）	343,200 美元	192,750 美元	190,688 美元	190,688 美元	917,325 美元	819,287 美元

支付给 IBM Security 的费用

除了核心 QRadar 平台的费用外，该企业还为 IBM QRadar Advisor with Watson 支付了一笔软件许可费用。对于 QRadar Advisor with Watson，受访企业目前为三年期合同支付 240,000 美元。

对于财务模型，Forrester 假设：

> 三年期许可费用为每年 8 万美元。

Forrester 没有对这项成本进行风险调整，因为它由受访企业直接提供，并得到 IBM Security 的确认。

上表显示了下列领域的所有收益总额，以及贴现 10% 之后的现值 (PV)。预计该受访企业根据风险调整后的三年总成本为 819,287 美元的现值。

支付给 IBM Security 的费用：计算表

参考号	指标	计算	最初	第 1 年	第 2 年	第 3 年
D1	为 IBM QRadar Advisor with Watson 支付的许可费用	访谈数据		80,000 美元	80,000 美元	80,000 美元
Dt	支付给 IBM Security 的费用			80,000 美元	80,000 美元	80,000 美元
	风险调整	0%				
Dtr	支付给 IBM Security 的费用（根据风险调整后）		0 美元	80,000 美元	80,000 美元	80,000 美元

支付给外部威胁情报资源的费用

QRadar Advisor with Watson 利用机器学习能力，越来越有效地帮助分析人员发现威胁并划分优先级。为了向 Watson for Cyber Security 提供额外的信息，以促进这些积极的学习循环，该企业订阅了几个额外的外部威胁情报源，以提高可以从 Advisor with Watson 中获得的价值。使用额外的威胁情报源不会影响分析人员的生产力，因为 Advisor with Watson 提高了企业分析人员审查订阅源的能力。

受访者表示，部署 QRadar Advisor with Watson 之后，外部威胁情报来源变得更有价值。

受访者告诉 Forrester：“Advisor with Watson 让我们能够更快地审查调查现场。这实际上是分析人员生产力提升的一方面。”

对于财务模型，Forrester 假设：

> 该企业订阅了两个全新的外部威胁情报数据源，年订阅费总计 100,000 美元。

此成本因以下因素而异：

> 企业当前订阅的外部威胁情报数据源的数量。

> 每个订阅的价格。

为了抵消这些风险，Forrester 将此项成本调高了 10%，根据风险调整后的三年总现值为 273,554 美元。

支付给外部威胁情报资源的费用：计算表

参考	指标	计算	最初	第 1 年	第 2 年	第 3 年
E1	订购外部威胁调查服务			100,000 美元	100,000 美元	100,000 美元
Et	支付给外部威胁情报资源的费用		0 美元	100,000 美元	100,000 美元	100,000 美元
	风险调整	↑10%				
Etr	支付给外部威胁情报资源的费用（根据风险调整后）		0 美元	110,000 美元	110,000 美元	110,000 美元

实施和培训的资源成本

受访者强调，正确配置 QRadar Advisor with Watson 部署，才能最大程度实现投资价值，这一点很重要。该企业参与了 IBM Security 的 QRadar Advisor with Watson beta 测试项目，作为自身实施流程的一部分。这涉及将企业安全团队人员专门分配给 QRadar Advisor with Watson 实施流程，并进行一些用户培训。

- 整个实施过程耗时 12 个月（包括 beta 测试），但受访者指出，如果该企业没有参与该测试项目，这个过程会快得多。受访者告诉 Forrester：“让 Advisor with Watson 启动并运行所需的时间非常短。你只需要安装程序，它就可以投入使用了。”
- 该企业为 QRadar Advisor with Watson 部署指派了六名全职员工，其中两名几乎是全职负责该项目，估计 85% 的时间都用在实施上。另外四人只是部分参与其中。
- 受访者花费了 40 个小时，对将要使用 QRadar Advisor with Watson 的 SOC 和 NOC 分析人员进行培训。在第一年，他进行了五次单独的短期培训。

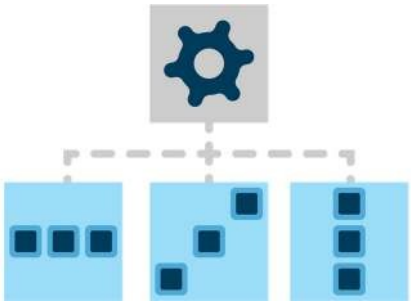
对于财务模型，Forrester 假设：

- 6 名全职员工平均将其总工作时间的 40% 用于实施。
- 每年还会举行 5 次两小时的培训，用于培训新分析人员或提升现有分析人员的技能。

此成本因以下因素而异：

- 企业的安全人员参与 QRadar Advisor with Watson 实施的程度及其资历。

为了抵消这些风险，Forrester 将此项成本调高了 10%，根据风险调整后的三年总现值为 346,785 美元。



典型实施

受访企业参与了 beta 测试项目，这可能导致实施周期延长。IBM Security 提供了以下数字，反映了目前 QRadar Advisor with Watson 典型实施的情况。

- **3 到 5 天（技术实施）**
- **1 到 2 名 IT 全职员工**
- **用不到 30 天的时间，培训分析人员使用 QRadar Advisor**

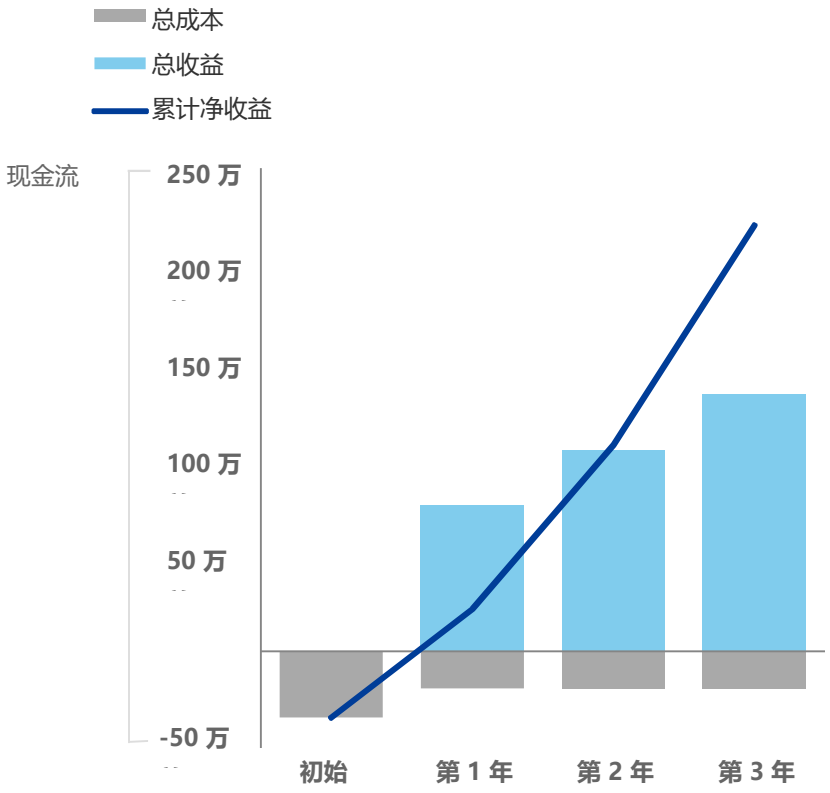
IBM Security 注意到，实施时间和所需的全职员工资源可能会因客户企业的成熟度、规模大小以及员工能力而有所不同。

实施和培训的资源成本：计算表						
参考号	**指标**	**计算**	**最初**	**第 1 年**	**第 2 年**	**第 3 年**
F1	参与 QRadar Advisor with Watson 实施的人员		6 名全职员工			
F2	用在实施上的工作时间的相对百分比		工作时间的 40%			
F3	用在实施上的时间		1 年			
F4	SOC 员工培训课程的开发			40 小时	10 小时	10 小时
F5	SOC 经理的时薪	130,000/2,080 美元		62.50 美元	62.50 美元	62.50 美元
Ft	实施和培训的资源成本	(F1*F2*F3* 130,000 美元) +(F4*F5)	312,000 美元	2,500 美元	625 美元	625 美元
	风险调整	↑10%				
Ftr	实施和培训的资源成本（根据风险调整后）		343,200 美元	2,750 美元	688 美元	688 美元

财务摘要

根据风险调整后的三年期综合指标

现金流图（根据风险调整后）



“收益”和“成本”部分所计算的财务结果可用于确定该受访企业的投资回报率、净现值和投资回收期。Forrester 假设此分析的年贴现率为 10%。

这些根据风险调整后的投资回报率、净现值和投资回报期是通过将风险调整因子应用于每个“收益”和“成本”部分中的未调整结果而算得的。

现金流表（根据风险调整后）

	最初	第 1 年	第 2 年	第 3 年	总计	当前价值
总成本	(343,200 美元)	(192,750 美元)	(190,688 美元)	(190,688 美元)	(917,325 美元)	(819,287 美元)
总收益	0 美元	753,800 美元	1,039,611 美元	1,326,433 美元	3,119,844 美元	2,541,023 美元
净收益	(343,200 美元)	561,050 美元	848,923 美元	1,135,745 美元	2,202,519 美元	1,721,736 美元
ROI						210%
回报期						8 个月

FORRESTER

IBM QRadar Advisor With Watson：概述

以下信息由 IBM Security 提供。Forrester 并未验证任何声明，也不为 IBM Security 或其产品背书。

关于 IBM QRadar Advisor with Watson

IBM® QRadar® Advisor with Watson™ 是对 IBM QRadar Intelligence 平台的补充，旨在帮助 SOC 分析人员更快、更一致地对事件进行分类和调查。QRadar Advisor with Watson 能够自动执行 SOC 日常任务，发现调查中的共性，并向 SOC 分析人员提供切实可行的反馈。Advisor 工具有助于显著缩短调查事件所需的时间，从几天或几周减少到几分钟或几小时。

主要收益

让团队工作成效成倍提高

Advisor 可以帮助您自动执行重复的 SOC 任务，从而使分析人员能够发现并专注于最重要的调查元素。

推动持续深入的调查

Advisor 不会有状态起伏，无论是周五下午 4:30 还是周一上午 10 点，都能够始终如一地增强人类智慧，使分析人员每次都能进行一致而彻底的调查。

缩短威胁停留时间

通过更快速、更果断的上报流程，缩短平均检测时间 (MTTD) 和平均响应时间 (MTTR)。

通过将攻击映射到 MITRE ATT&CK 模型，执行根本原因分析，并充满信心地推动实施下一步行动。

了解更多信息

附录 A：总体经济影响

“总体经济影响”(Total Economic Impact) 是 Forrester Research 开发的一种方法，旨在增强企业的技术决策流程，帮助供应商向客户传达其产品和服务的价值主张。TEI 方法帮助企业向高级管理层和其他主要业务利益相关方展示、证明并实现 IT 计划的切实价值。

“总体经济影响”方法

收益表示产品给企业带来的价值。 TEI 方法对收益和成本的评估给予同等的重视，旨在全面审视技术投资对整个企业的影响。

成本表示相关产品实现预期价值或收益所需的全部费用。TEI 方法中对成本的分类可捕捉现有环境中的增量成本，用于计算与解决方案相关的持续成本。

灵活性表示企业在现有初始投资的基础之上可以通过未来追加投资而获得的战略价值。如果具有实现此类收益的能力，就具备可估算的现值。

风险用于衡量收益和成本估算的不确定性，包括：1）估算符合最初预测的可能性；以及 2）估算可长期跟踪的可能性。TEI 风险因素基于“三角分布”。

“初始投资”列中包含“时间 0”或“第 1 年”开始时的未贴现成本。所有其他现金流均使用年底的贴现率进行贴现。计算每个总成本和收益估算的现值。汇总表中的净现值计算是初始投资及每年贴现现金流的总和。考虑到四舍五入，最终算得的总收益、总成本和现金流表的总和及现值可能不完全等于各项直接相加之和。

现值 (PV)

按利率（贴现率）给出的（贴现的）成本和收益估算的现值或当前值。成本和收益的现值是计算现金流总净现值的基础。

净现值 (NPV)

给定利率（贴现率）的（贴现）未来净现金流的现值或当前值。如果项目的净现值为正，通常表明应该进行投资，除非其他项目具有更高的净现值。

投资回报率 (ROI)

项目按百分比计算的预期回报。投资回报率的计算方法是将净收益（收益减去成本）除以成本。

贴现率

现金流分析中使用的利率，旨在将货币的时间价值考虑在内。企业通常使用 8% 到 16% 的贴现率。

投资回报期

投资的盈亏平衡点。是指净收益（收益减去成本）与初始投资或成本持平的时间点。

附录 B：尾注

[1] 来源：Forrester Analytics 全球企业科技消费安全调研，2018 年。
[2] 来源： “Why EX, Why Now?” Forrester Research, Inc.，2018 年 11 月 28 日。
[3] 来源： “2018 Cost of a Data Breach Study by Ponemon” ，Ponemon Institute，2018 年。
https://www.ibm.com/security/data-breach
[4] 来源：Forrester Analytics 全球企业科技消费基础架构调研，2018 年。