MITRE ATT&CK 评估

IBM Security ReaQta 展现出一流的能力

亮点

提高业务连续性，同时将安全团队从网络威胁人工分析任务中解放出来

通过生成最少数量的必要威胁警报，缓解警报疲劳，简化网络安全流程

获取有关终端的完整可视性，以便能够在每个阶段做出快速响应

关于本报告

ReaQta, an IBM 已成功完成 MITRE ATT&CK 评估。本报告[1]表明 ReaQta 完全覆盖各种狡猾的攻击，几乎不需要人为干预，并且能够生成最高质量的警报。

什么是 MITRE ATT&CK 评估?

MITRE ATT&CK 定义了网络攻击期间的一系列阶段，并评估有关其威胁检测能力的解决方案。列出的每个阶段都代表了“猎杀”链中的一种战术：

- 初始访问
- 执行
- 维持
- 特权提升
- 防御逃逸
- 凭证访问
- 发现
- 横向移动
- 收集
- 渗出
- 指挥控制

REAQTA
an IBM Company

IBM

MITRE 评估如何为组织提供帮助

评估并不是对解决方案进行评分或评级，而是旨在帮助组织确定最适合的解决方案，以应对其特定的安全挑战。组织需要注意，评估是在隔离的环境中进行的，存在一定的局限性。有时候，解决方案的某些功能是禁用的，因为它们不支持特定的实验室基础架构，例如在 ReaQta NanoOS 环境中，就无法使用旨在检测高级恶意行为的实时虚拟机管理器。但该平台即使没有核心组件也能正常运行。

MITRE 包含一系列确定的方法，每个都属于一个战术群组，这些群组基于为评估而选择的威胁实施者。对于本轮评估，MITRE 选择 APT29。

破坏

收集和逃逸

侦查跟踪

扩大访问范围

渗出

清除

提高业务连续性，同时将安全团队从网络威胁人工分析任务中解放出来

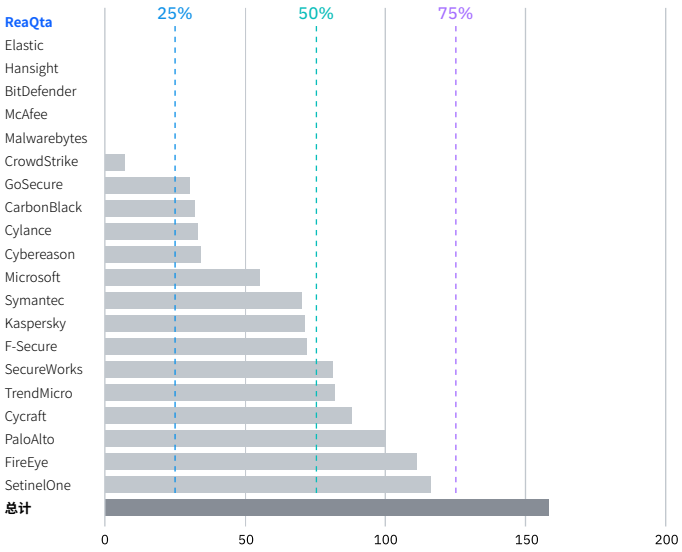
在开始评估之前，ReaQta 决定参与没有管理安全服务提供商 (MSSP) 的场景，也就是在攻击期间没有任何人员互动。MITRE 是一个技术评估框架，它似乎假装不知道评估循环中存在人类因素。最重要的是，MSSP 检测会对评估造成严重偏差。安全运营中心 (SOC) 团队知道正在发生的攻击以及攻击的确切位置和方法。

MSSP 方法无法为 ReaQta 的客户带来公平的技术评估。MITRE 认真倾听反馈意见，从第 3 轮开始，所有公司都将在没有人员参与循环的情况下进行评估。

MSSP 确实可以带来很大的价值，因此客户可以自由选择 MSSP 和独立部署。

如下图所示，人类执行的检测活动的数量对生成的检测产生巨大影响。在一些情况下，超过 50% 的检测（最高可达 73%）是人工创建的。只有 6 家公司决定在循环中没有人类活动的情况下参与评估。

MSSP 检测（人工生成）



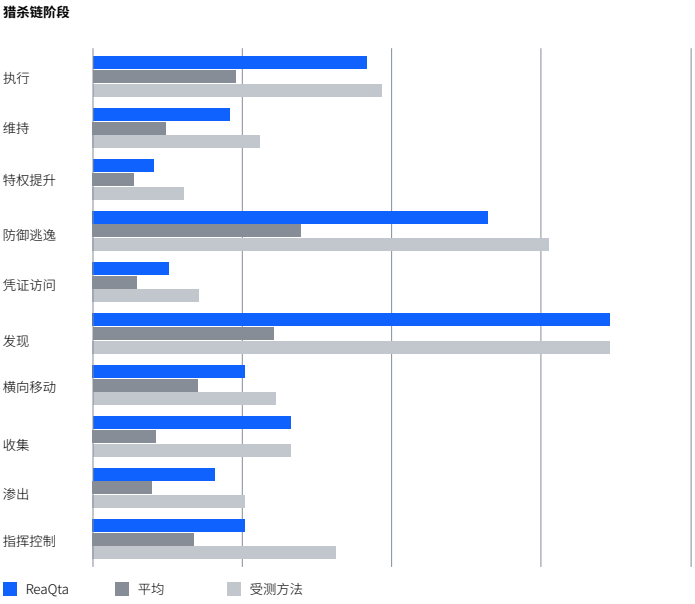
每个供应商生成的人工检测

MITRE 评估第 2 轮 - APT29

检验供应商检测 APT29（也称为 The Dukes、Cozy Bear 和 CozyDuke）所使用的战术和方法的能力，APT29 是因隐蔽攻击方法而闻名的一个老练的国家级黑客组织。APT29 被广泛认为是一些重大攻击行动的幕后黑手：2015 年对五角大楼的网络攻击、2016 年对民主党全国委员会的攻击以及 2017 年对挪威和荷兰政府的攻击。

与上一轮相比，变化很明显：APT 3（第一轮）是一个唯恐别人不知的威胁实施者，采用各种攻击工具，而且不太注意保持低调。而 APT29 是另一个极端，他们及其隐秘，非常低调地实施攻击，高度依赖于 LOLBins 和无文件恶意软件。

方法检测覆盖范围（自动）



ReaQta 自动化检测覆盖范围与平均水平的对比

ReaQta 评估结果

攻击在两天的时间里逐渐展开，攻击者在获得初始访问权限后逐渐向网络纵深渗透。绝大多数操作都使用 Microsoft PowerShell 进行，而不是使用自定义工具和恶意软件，以保持隐蔽，防止被检测到。评估目标是展现受测解决方案如何响应攻击，以及在整个猎杀链中提供怎样的可视性。

从评估结果摘要中可以看出，ReaQta 在整个猎杀链中提供完整的可视性。ReaQta 检测到了 90% 的受测战术和方法，能够在攻击的每个阶段响应和缓解威胁。

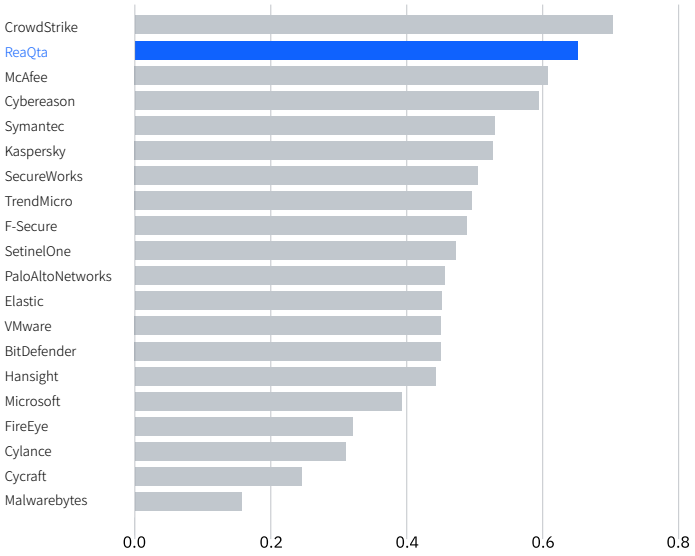
即使与依靠 MSSP 人工检测的供应商相比，ReaQta 也称得上世界上可操作性分数最高的解决方案之一。

通过生成最少数量的必要威胁警报，缓解警报疲劳，简化网络安全流程

该平台在执行、维持、特权提升和防御逃逸阶段检测和生成警报，帮助安全团队跟踪 APT29 及其行为。该平台在猎杀链后期阶段的警报是一致的，这包括横向移动、收集、渗出以及指挥控制，这表明 ReaQta 还能够在网络攻击的后期阶段做出响应和限制损失。

该平台的可操作性分数表明，它通过减少所生成警报的数量，有效减少噪声。该平台能够在几条相关的警报中捕获所有攻击战术和方法，这与每个战术和方法一条警报形成鲜明对比，后者会产生无法管理的大量警报，使得 SOC 团队根本无力一一研判和应对。

警报可操作性

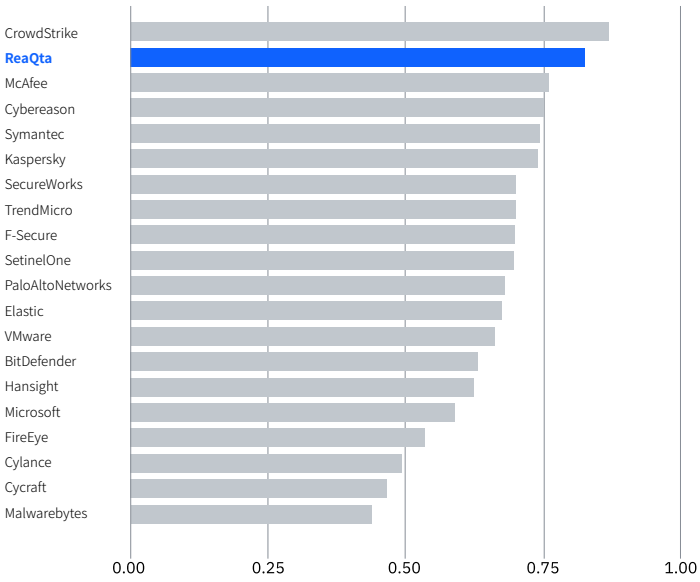


可操作性分数（数据包括依赖于 MSSP 的供应商的人工检测）

同样，ReaQta 能够在没有人为干预的情况下提供高质量的警报，而排名第一和第三的供应商在评估期间都依赖于人工分析。

ReaQta 提供的可视性水平使其能够过滤数据、关联数据并生成尽可能小的警报数量，每条警报都包含最大数量的相关信息。这就是 ReaQta 的 AI 引擎的用途：收集、关联和汇总遥测数据。以下图表中的 Forrester 分析也证实了警报质量。

警报质量



警报质量（数据包括依赖于 MSSP 的供应商的人工检测）

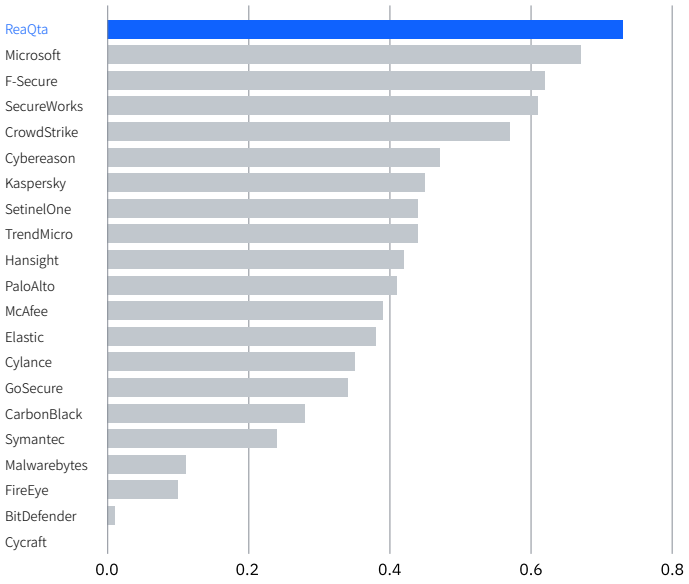
“可操作性是警报效率和警报质量的乘积[…] 警报的效率（警报不是太多）和警报的质量（帮助您了解情况的水平）相互关联，对于理解特定警报的“可操作”程度至关重要。”

Forrester[2]

能否提供高分辨率、全面的警报，是区分优秀平台与单纯的噪声制造者的标准。

下图显示了在移除人为检测的情况下，ReaQta 与其他解决方案的对比。每个条形都表示每条生成的报警所捕获的与事件相关的信息量。ReaQta 引擎捕获的信息量最大，因此能够显著减少实际环境中的工作量。

每条生成的警报的攻击覆盖范围（信噪比）



每条报警提供的攻击覆盖范围百分比

ReaQta 仅生成 25 条警报，并且正确收集了跟踪每个攻击者所需的全部信息，而不是创建 158 条警报（每个受测方法一条）。

提供统一的事件解决工作流程的能力对于降低警报疲劳至关重要。

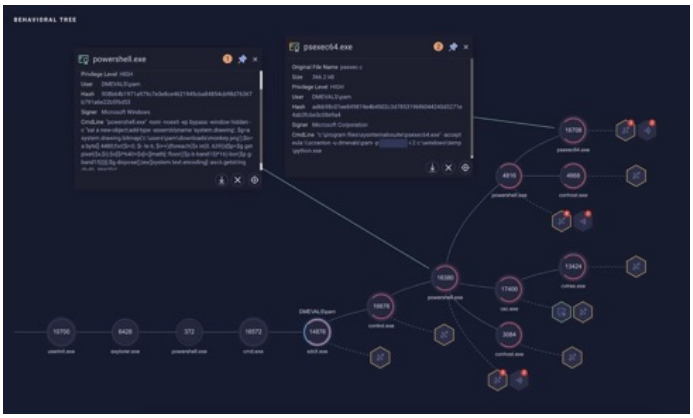
ReaQta 在 MITRE 评估期间能够关联攻击的“故事情节”。这使得分析人员能够轻松了解和研究活跃的攻击者，而不会为所生成的数以百计与原始事件没有直接关联的警报而分心。在实际分析中，这些警报“噪声”更难处理。

ReaQta 方法可使警报疲劳降低 85%，同时在整个攻击过程中保持完整的可视性。ReaQta 经过专门设计，旨在为每个事件生成最少数量的警报，打造顺畅、不间断的分析体验。分析人员能够一站式了解所有信息，从而可以更快地进行响应，而无需在多个屏幕视图中跳转以了解事件的全貌。

获取有关终端的完整可视性，以便能够在每个阶段做出快速响应

该平台能够将攻击猎杀链所有阶段中的行动关联起来。通过自动关联事件，有助于缩短将攻击者所实施的各种行动串联起来所需的时间，最终能够在实际发生攻击时加快响应速度。

行为树



ReaQta 在 MITRE 评估期间能够关联攻击的“故事情节”

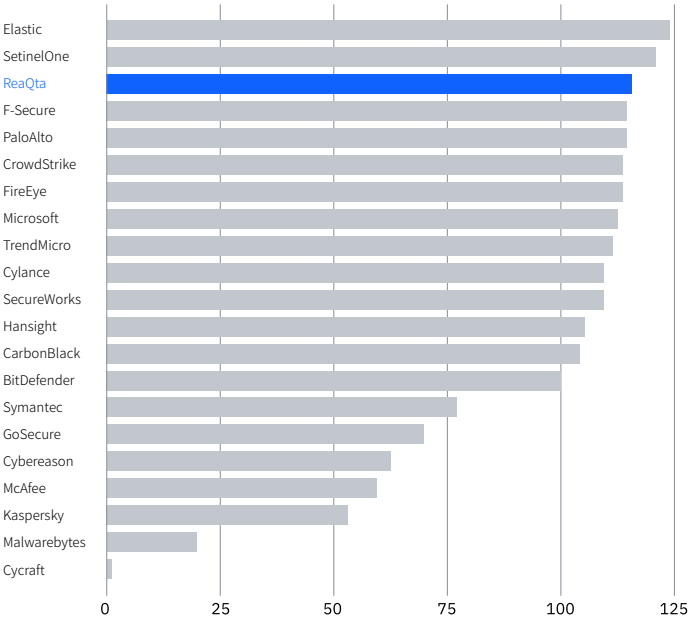
为了提供与评估相关的示例，上图显示了如何用一条警报捕获攻击的一个完整阶段。ReaQta 将所有信息关联到一个易于理解的“故事情节”中，从而为 SOC 团队提供及时分类所需的全部信息。不需要人员互动，能够清晰地解释攻击并评估其风险，无需任何人工活动。

通过近距离研究如何检测 APT29 的攻击战术和方法，我们发现，无论是在猎杀链的早期阶段还是在通常较难检测的更复杂阶段，ReaQta 都能提供出色的可视性。值得一提的是，该平台能够在每个阶段以统一方式检测威胁，从而使用户有机会在每个阶段做出响应和采取补救措施。

ReaQta 展现出最出色的遥测功能之一，它结合使用一个令人印象深刻的 AI 引擎，用于压缩信息和评估风险。事实证明，对于任何希望将时间花在威胁追踪而非持续管理警报的 SOC 团队而言，它是一种强大的工具。

ReaQta 展现出最出色的遥测功能之一。

遥测功能



ReaQta 提供的遥测数据量

结束语

ReaQta 的基于 AI 的平台为安全团队提供高级检测和快速响应能力，最大程度减少人为干预，简化整个安全流程，促进各种规模的组织的业务连续性。

这次评估验证了 ReaQta 检测复杂威胁实施者的方法。将来，ReaQta 将继续参与独立第三方的评测。

ReaQta 感激并赞赏 MITRE 的优异工作，他们通过这些评估，帮助组织做出明智决策。

要了解更多信息，请访问：

ibm.com/products/reaqta

国际商业机器中国有限公司
北京市朝阳区光华路10号
正大中心 南塔12 层；邮编: 100020

美国出品
2022 年 3 月

1 MITRE ATT&CK 评估，The MITRE Corporation and MITRE Engenuity，2020 年。
2 Further Down the Rabbit Hole With MITRE’ s ATT&CK Eval Data，Forrester 博客，2020 年 5 月 4 日。