elastic

公司高管见解：

生成式 AI

生成式 AI 几乎成为了众人瞩目的焦点。消费者渴望用它来提升自己的数字体验，组织则希望用它来削减成本并提高效率，而员工也在积极学习如何运用 AI 的功能来简化工作。随着生成式AI的飞速发展和日益成熟，我们既要勇于探索其广阔的应用前景，又要以务实态度，通过制定切实可行的战略来推进生成式 AI 的实施，从而加速实现业务目标。

当谈及生成式 AI 时，IT 领导者们会思考哪些内容呢？

我们综括了三位 IT 领导者的见解，一起探讨他们目前是如何运用生成式 AI 的，以及这一技术将如何为他们的组织带来最大的影响，并了解他们正在采取哪些措施来实施生成式 AI。

从愿景到现实：

利用生成式 AI 增强运营弹性

Matt Minetola
Elastic 首席信息官

作为企业 IT 领导者，您的团队需要投入大量时间来确保系统稳定运行，并实时监测和解决问题。很有可能，您的组织已经积累了海量的遥测数据，且随着组织不断寻求识别应用程序漏洞、检测用户错误，以及最为关键的是，在网络攻击影响业务之前便将其识别出来，这些数据量仍在持续增长。

将生成式 AI 用于增强运营弹性等商业用例的关键，在于要结合您特定的数据和信号向其寻求答案。诸如 ChatGPT 这样的生成式 AI 聊天机器人在回答问题方面非常有用。不过，这些聊天机器人所利用的大型语言模型 (LLM) 都是基于互联网上所有公开可用的数据来提供答案的。当您询问在自己环境中观察到的有关特定实例的问题时，您得到的答案将是基于可能与您的具体情况不相关的通用信息来生成的。

> 在现实场景中，生成式 AI 对组织的强大作用在于将组织的专有数据整合到您的 LLM 中。

您已经有了所需的数据

好消息是，您已经构建了内部数据存储库，这些数据可用于训练组织的可观测性和安全监测学习能力。借助这一基础架构，您可以将当前的自动化运营监测和响应能力转化为更稳健的 AIOps 功能。这将增强 Security 和 Observability 解决方案的工作流，并使您的团队能够更快地全面了解 IT 系统，从而快速解决事件，提升组织的运营弹性。

假设您是一家零售商，网站购物车出现故障，导致客户无法完成购买，销售额也因此下降。不同于以往只是针对事件做出反应并自动化响应以减轻业务影响，您现在可以将这些数据输入到生成式 AI 中，让 AI 学习其中的模式并自动化响应。这样做既能减少对客户体验的影响，又能增加销售额。

这只是生成式 AI 强大能力的冰山一角。

您或许想知道如何实现这一切

要使用生成式 AI 来获得增强运营弹性所需的见解，您首先需要实施一个一体化的数据平台，以便持续、实时地将所有数据无缝转化为结果，并将所有问题迅速转化为答案。

要实现这一点，您需要收集并整理自己的所有数据，确保这些数据能够进行搜索、分析、探索以及可视化呈现。同时，这个系统应构建在分布式架构之上，以便您的数据存储能够跨多个服务器和位置运行，从而提升性能，避免单点故障，并确保在发生中断时业务能够持续运行。

生成式 AI 将助力我们打破传统界限，开启广阔的应用前景。您可能已投入数年时间来优化流程，并找到了适合您团队的 Security 和 Observability 解决方案。现在，随着生成式 AI 的广泛普及，并且您能够灵活地创建与之集成的定制应用程序，您将能够显著提升这些工作流和解决方案的效能，快速找到答案，高效解决问题，并增强运营弹性。

以上内容摘自 CIO.com 上于 2023 年 7 月 27 日发布的一篇文章。单击此处阅读全文。

安全第一：

使用生成式 AI 减轻安全风险

Mandy Andress
Elastic 首席信息安全官

随着 ChatGPT 和 Bard 等这类工具向公众开放，大众都在积极探索将其融入日常工作和生活中。然而，这也为威胁行为者提供了可乘之机，他们现在也在使用生成式 AI 来识别并利用组织的安全漏洞，进而开发更为复杂精细的安全攻击。

如果不自动化您的 Security 解决方案的工作流，几乎无法实时抵御这些威胁。幸运的是，作为一名 IT 领导者，您早已致力于利用 AI 和 Machine Learning 的强大功能来保护您的组织。您很可能已经拥有了能够收集和匹配安全运营数据中模式的基础架构，因此您具备了利用生成式 AI 来自动化工作流的优势，这将使您能够更快地识别和应对威胁。

您在利用信息强化团队的能力

当您将生成式 AI 工具安全地集成到 Security 解决方案的工作流中时，您实际上是在为团队提供强大的武器，使他们能够实时发现安全漏洞和异常情况，从而更迅速、更便捷地抵御高级威胁。这样一来，团队就不需要花费宝贵的时间进行培训，也不必徒劳地尝试分析组织每秒都在产生的海量数据。

假设有一名员工不慎落入了网络钓鱼的陷阱。这一安全漏洞将使您的系统面临被攻击者入侵的风险。那么，攻击者是否已经潜入您的系统内部？您的敏感数据是否已得到妥善保护，以抵御此类威胁？在此情况下，您的团队能够迅速采取哪些有效措施，以阻止潜在的声誉和财务损失，并重新恢复一个安全无虞的环境？生成式 AI 能够实时为您提供关键信息和建议。

> 当我们谈论安全漏洞时，速度和规模都是至关重要的因素。

您需要相关的数据和安全的生成式 AI 工具

虽然您的团队可能会倾向于使用 ChatGPT 等工具来迅速了解如何解决问题，但这些工具所依赖的大型语言模型 (LLM) 往往都是基于自互联网诞生以来累积的（有时甚至是过时的）公开信息来生成答案的。这种影子 IT 可能会增加团队成员被生成式 AI 误导的风险，即生成式 AI 可能会产生“幻觉”，将错误信息误认为是准确信息提供出来。

如果您的团队将有限的上下文数据（如专有遥测数据）传输给一个安全的生成式 AI 工具，它便可以快速分析数据，并针对有关任何异常、现有问题或潜在问题提供有价值且相关的见解，同时给出解决这些问题的建议。您的团队提供的数据越详尽具体，所获得的答案就越具相关性和价值，从而能够更快地采取行动。

为了精准提取这些相关数据，您需要建立一个一体化的数据平台，以便持续、实时地将所有数据无缝转化为结果，并将所有问题迅速转化为答案。在此基础上，您的团队就可以利用生成式 AI，通过将应用和平台集成的方式，在关键时刻迅速获取所需的相关信息，以确保客户信息和关键业务数据的安全无虞。

以上内容摘自 Digital Nation 上于 2023 年 8 月 14 日发布的一篇文章。单击此处阅读全文。

如何使用生成式 AI 打造无缝客户体验之旅

Rick Laner
Elastic 首席客户官

在 ChatGPT 等生成式 AI 工具广泛普及之前，客户对各大品牌就已抱有极高的期待，并且这种期待至今依然强烈。消费者渴望从公司那里获得个性化的交互体验，一旦这种期待落空，他们往往会感到失望。显而易见，消费者想要的是那种既个性化又能够即时响应的服务体验。

现在，关键在于 IT 领导者需要投资于能够带来这些体验的技术。这正是生成式 AI 大展身手的地方。

简化客户（和员工）的使用体验

消费者已经习惯于使用 AI 驱动的应用来即时获取对话式的信息。如今，对于所有组织而言，在客户及员工需要的时候，以自然语言的形式提供高度相关的信息已成为一项基本要求 — 这正是生成式 AI 工具大放异彩的领域。

旅游公司可以在他们的数字体验中利用生成式 AI 聊天机器人，帮助客户规划出完美的度假行程，并直接通过该工具完成预订。同样，服装零售商也可以利用生成式 AI，帮助客户在几秒内找到适合任何场合的理想服饰，包括合适的尺寸、颜色、款式和版型。

同样，IT团队在监测基础架构和应用程序的同时，也可使用生成式 AI 来帮助识别和解决问题，从而确保在线应用程序的平稳运行。这一举措有助于提供可靠的数字体验，同时增强品牌信任。

 |

生成式 AI 的潜力无穷

当然，前提是您使用了正确的数据。生成式 AI 聊天机器人工具所依赖的大型语言模型 (LLM) 都是基于自互联网诞生以来整个网络累积的数据和信息中来生成回复的。这就意味着，它们很容易产生幻觉，将错误信息当作准确信息来提供。而您显然不能容忍向客户提供错误的信息。

> 作为 IT 领导者，您的首要任务是确保组织拥有强大的基础架构，以便客户每次都能迅速找到他们所需的内容。而这一切的基石，正是您的数据。

所以，如果您的组织正是前面提到的那家采用生成式 AI 聊天机器人进行预订的旅游公司，那么客户最终可能会

从互联网的各个角落获取行程建议，而不仅仅是您提供的方案。更糟糕的是，在您的聊天机器人的“帮助”下，他们可能最终会选择从竞争对手那里预订行程！

然而，如果您向生成式 AI 工具提供自己的数据供其拉取，那么客户就能够找到您提供的选项。这样，您就可以为客户提供量身定制、相关且安全的体验，并推动他们完成转化 — 在本例中，就是完成旅游行程预订。同样，如果您的 IT 团队利用生成式 AI 来获得可观测性，那么它就需要最相关、最准确的回复来消除中断，并为客户提供可靠的体验。

利用生成式 AI，您的 IT 团队可以获得相关的可观测性数据和告警，确保应用程序平稳运行；安全团队则能迅速发现安全漏洞并降低风险；而客户则能每次都轻松找到他们所需的品牌特定信息。这一切的结果便是：由生成式 AI 驱动的无缝客户体验。

以上内容摘自 CIO Dive 上于 2023 年 8 月 14 日发布的一篇文章。单击此处阅读全文。

准备好采取后续行动来迎接生成式 AI 了吗?

下载公司高管就生成式 AI 方面的见解集