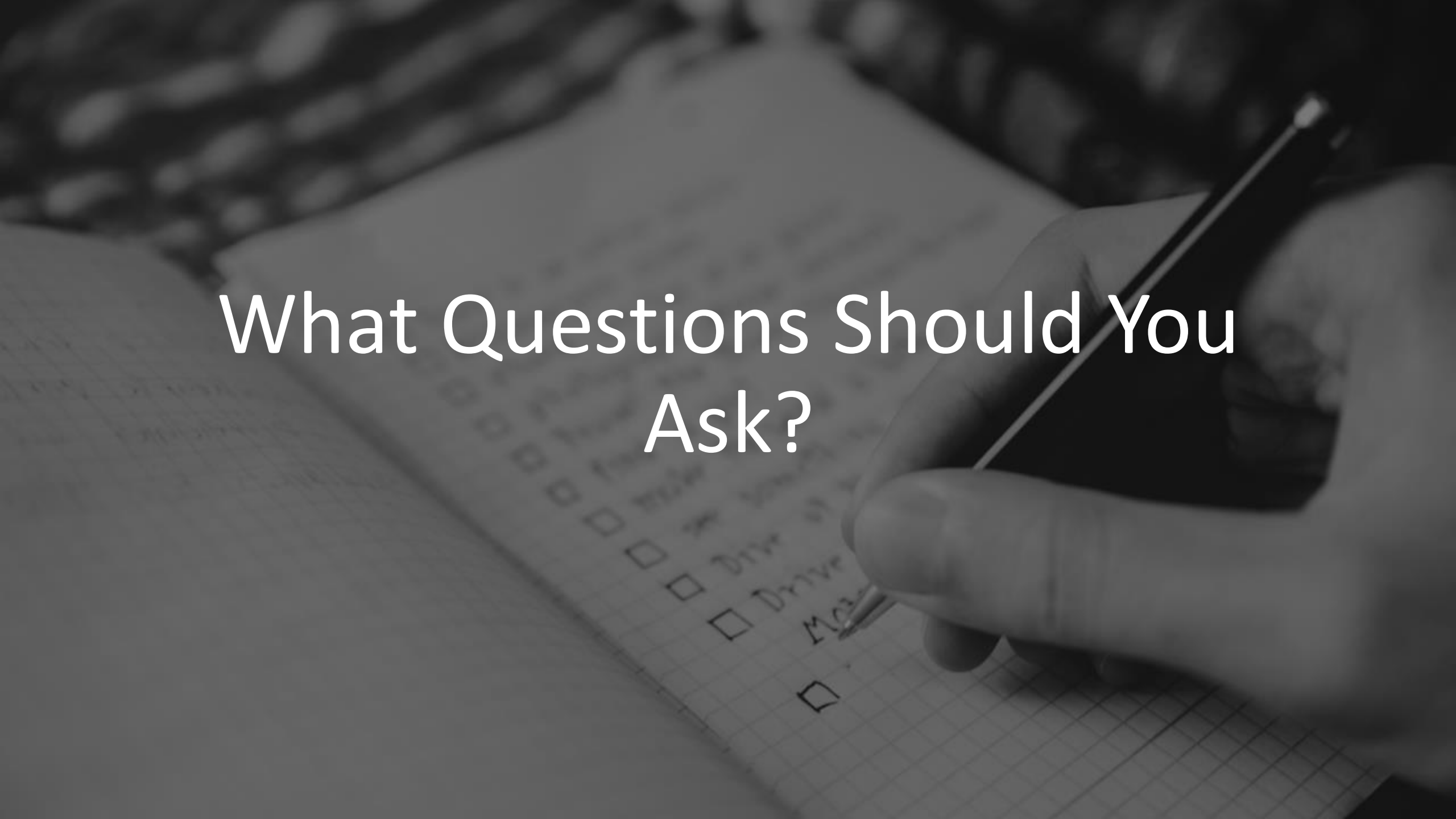
GAI Providers: What Questions Should You Ask?

When Leveraging GAI for Software Development Lifecycle

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Trac Bannon



What Questions Should You Ask?

GenAI Provider Questions – Set 1

1. How does the platform ensure the security and privacy of data used by the generative AI models?
   Importance: Understanding the data handling policies and practices of the vendor helps ensure that sensitive information is not inadvertently exposed or misused during the AI model's training or application.

2. What measures have been taken to prevent the AI model from generating malicious or vulnerable code?
   Importance: Ensuring that the AI model does not introduce new security vulnerabilities or promote insecure coding practices is crucial for maintaining the overall security of the applications built on the low-code platform.

3. How does the platform manage and control access to the generative AI models and their generated outputs?
   Importance: Proper access management is essential to prevent unauthorized access to the AI models, which could lead to unauthorized modifications, data breaches, or other security risks.

4. How does the vendor handle AI model updates, and what steps are taken to evaluate and maintain the security of the generative AI models over time?
   Importance: Regular updates and security assessments of the AI models are necessary to ensure that they continue to provide a secure and reliable foundation for low-code development as new vulnerabilities and security risks emerge.

MITRE

GenAI Provider Questions – Set 2

1. What are the pricing options and licensing terms for using the generative AI features?
2. Are there any hidden costs or usage limitations we should be aware of?
3. How does the tool handle edge cases or unexpected inputs?
4. Are there any built-in fail-safes to prevent the generative AI from producing harmful or problematic code?
5. Can the generative AI model be fine-tuned or customized to our organization's specific coding standards and practices?
6. Is it possible to extend the model's capabilities to address our unique requirements or use cases?

MITRE