Introduction to Security in the World of AI Review

Congratulations! You now have a basic understanding of AI security. This course summary is your review guide. Print it for a handy reference as you continue your AI security journey.

Three primary ways to engage with AI:

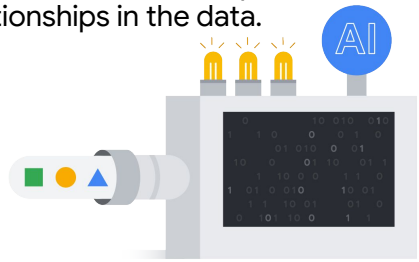
Built AI models.

Build applications or APIs the leverage AI models.

Use AI-powered applications or APIs.

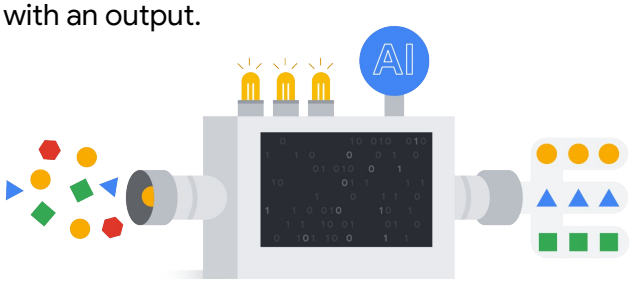
How AI models are created

Use an algorithm on your training data to train your AI model to learn patterns and relationships in the data.



How AI models are used

Provide an input to the AI system through an API or application. The then model provides you with an output.



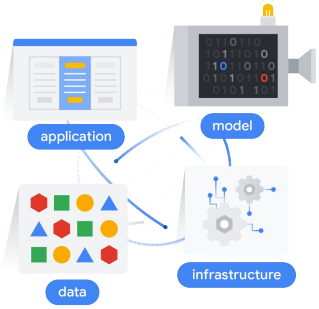
Understanding AI data collection

Like any application, some AI applications collect user data. Check terms and conditions to understand each individual application or license.

Three forms of AI security

1. Adding AI into security products.
2. Countering AI-powered cyberattacks.
3. Securing AI systems and services.

Components of a secure AI system



Google's Secure AI Framework (SAIF)

1. Understand the use.
2. Assemble the team.
3. Level set with an AI primer.
4. Apply the six elements of SAIF:

Build AI security into your processes. Assess AI risks, understand their business impact and adapt your security strategy accordingly.

Secure. Build a strong security foundation for all systems, and extend it to protect AI systems.

Detect and act. Adapt threat intelligence for AI-specific risks. Monitor AI for anomalies and leverage threat intelligence to predict attacks.

Automate defenses. Use AI for automation to enhance the scale and speed of security incident response.

Ensure consistency. Maintain consistent security controls across AI platforms for scalable and cost-efficient risk mitigation.

Continuously improve and stay ahead. Regularly test AI systems and stay informed on security practices to maintain strong defenses.