



---

# Anthropic's Claude Mythos Unveiled, Partners with Tech Giants

## Description

Experts have indicated that advancements in artificial intelligence (AI) could significantly alter the cybersecurity landscape. While numerous industry leaders have already integrated AI tools to mitigate hacking, data breaches, and cyberattacks, recent developments suggest a substantial escalation in the potential for sophisticated cyber intrusions.

The AI start-up Anthropic announced the release of Claude Mythos Preview, an advanced general-purpose AI model, claimed to be the most proficient to date for coding and agent-related tasks. Notably, this model has already identified thousands of zero-day vulnerabilities across critical infrastructure, vulnerabilities that hackers can exploit before they are known and resolved, necessitating immediate attention to safeguard users.

This announcement has reverberated throughout the cybersecurity sector, prompting a coalition of major technology companies to address these vulnerabilities proactively in a bid to prevent significant incidents.

In a move to enhance security, Anthropic introduced Project Glasswing, an initiative aiming to "secure the world's most critical infrastructure" against AI-driven attacks. This collaboration includes leading tech firms alongside cybersecurity specialists to rectify the vulnerabilities identified by Claude Mythos.

Prominent partners in this effort comprise Nvidia, Amazon Web Services (AWS), Apple, Alphabet's Google, Broadcom, Microsoft, and Cisco, along with cybersecurity entities like CrowdStrike and Palo Alto Networks. Furthermore, JPMorgan Chase and the Linux Foundation have also joined this alliance.

Anthropic highlighted that its AI model had detected numerous high-severity vulnerabilities, including those affecting all major operating systems and web browsers. The company asserts that Glasswing is a critical initiative to employ these findings for protective measures. Access to the initiative is being expanded to 40 additional organisations engaged in maintaining essential software infrastructure, with Anthropic contributing \$100 million in usage credits and \$4 million in donations to enhance open-source security.

This unprecedented collaboration among historically competing firms emphasises the urgency and seriousness of the emerging challenges presented by AI in cybersecurity.

---

## Vocabulary List:

1. **cybersecurity** //saɪbərseɪ'kjʊərɪti// (noun): work to protect computers and networks
2. **vulnerabilities** //vʌlnərə'bilətɪz// (noun): weak parts that can be attacked or harmed
3. **infrastructure** //ɪnfrə'strʌktʃə// (noun): important systems and services for a country or company
4. **exploit** //ɪk'splɔɪt// (verb): use something in a harmful or unfair way
5. **mitigate** //'mɪtɪ,geɪt// (verb): make something less bad or serious



---

6. **escalation** //,ɛskə'leɪʃən// (noun): a situation becoming bigger or more serious

## Comprehension Questions

### Multiple Choice

1. What is the name of the AI model released by Anthropic?

- Option: Claude Mythos Preview
- Option: Project Glasswing
- Option: Cyber Sentinel
- Option: Zero-Day Detector

2. Which company introduced an initiative to secure critical infrastructure against AI-driven attacks?

- Option: Nvidia
- Option: Anthropic
- Option: Microsoft
- Option: Amazon

3. How much money did Anthropic contribute in usage credits to enhance open-source security?

- Option: \$50 million
- Option: \$100 million
- Option: \$200 million
- Option: \$10 million

4. Which company is NOT mentioned as a partner in the Glasswing initiative?

- Option: Amazon Web Services
- Option: CrowdStrike
- Option: IBM
- Option: Apple

5. What type of vulnerabilities has Claude Mythos identified?

- Option: User-related
- Option: Operational
- Option: Zero-day
- Option: Compliance

6. Which operating systems are affected by the vulnerabilities detected by Anthropic's model?



- Option: Only Windows
- Option: Only macOS
- Option: All major operating systems
- Option: Only Linux

**True-False**

- 7. Anthropic's model has identified zero-day vulnerabilities across critical infrastructure.
- 8. Project Glasswing aims to secure infrastructure against traditional cyber threats.
- 9. The AI start-up mentioned is involved in an initiative with several major technology companies.
- 10. JPMorgan Chase is not part of the alliance working with Anthropic.
- 11. The collaboration among the firms is regarded as routine within the industry.
- 12. The vulnerabilities identified by Claude Mythos can be exploited by hackers before they are known.

**Gap-Fill**

- 13. Advancements in artificial intelligence (AI) could significantly alter the \_\_\_\_\_ landscape.
- 14. The AI model is claimed to be the most proficient to date for coding and agent-related tasks, named \_\_\_\_\_.
- 15. Anthropic introduced \_\_\_\_\_, an initiative aiming to secure critical infrastructure against AI-driven attacks.
- 16. The coalition includes firms like Nvidia, Apple, and \_\_\_\_\_ to address vulnerabilities.
- 17. Anthropic has committed to contribute \$100 million in usage credits and \$4 million in \_\_\_\_\_.



18. The collaboration emphasizes the urgency of challenges presented by AI in \_\_\_\_\_.

## Answer

**Multiple Choice:** 1. Claude Mythos Preview 2. Anthropic 3. \$100 million 4. IBM 5. Zero-day 6. All major operating systems

**True-False:** 7. True 8. False 9. True 10. False 11. False 12. True

**Gap-Fill:** 13. cybersecurity 14. Claude Mythos Preview 15. Project Glasswing 16. Google 17. donations

## CATEGORY

1. Business - LEVEL6

## POST TAG

1. anthropic
2. artificial intelligence
3. cybersecurity
4. esl news
5. Level 6

## Tags

1. anthropic
2. artificial intelligence
3. cybersecurity
4. esl news
5. Level 6

## Date Created

2026/04/09

## Author

aimeeyoung99

ESL-NEWS.COM