



---

# Anthropic's Claude Mythos Sparks Cybersecurity Shift with Tech Giants

## Description

Experts believe that artificial intelligence (AI) will greatly impact cybersecurity. Recently, a start-up called Anthropic introduced an AI model named Claude Mythos Preview. This model is very good at coding and identifying problems in software. It has already found many serious issues called "zero-day vulnerabilities." These vulnerabilities are ways that hackers can attack software suddenly and without warning.

The news about these vulnerabilities surprised many in the technology and cybersecurity fields. In response, major tech companies formed a group to fix these problems. This group is named Project Glasswing, and it aims to protect important systems from AI-driven attacks.

Companies involved include Nvidia, Amazon Web Services, Apple, Google, Microsoft, and Cisco, as well as cybersecurity experts like CrowdStrike and Palo Alto Networks. Anthropic noted that many of the vulnerabilities discovered affect major operating systems and web browsers.

To help secure the software, Anthropic is also supporting the project with \$100 million in usage credits. They aim to bring in more organisations that help build important software systems. This partnership shows how seriously companies take the risks posed by AI in cybersecurity.

---

## Vocabulary List:

1. **cybersecurity** //saɪbərseɪ'kjʊərəti// (noun): protecting computers and networks from harm
2. **vulnerabilities** //vʌlnərə'bɪlətɪz// (noun): weak parts in systems that can be attacked
3. **identifying** //aɪ'dentə'faɪɪŋ// (verb): finding and saying what something is
4. **response** //rɪ'spɑns// (noun): an answer or action after something happens
5. **partnership** //'pɑ:t.nəʃ.ʃɪp// (noun): two or more groups working together
6. **affect** //ə'fekt// (verb): to make a change to something

## Comprehension Questions

### Multiple Choice

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

Option: Claude Mythos Preview

---



- Option: AI Security Model
- Option: CyberProtect AI
- Option: Nvidia AI Model

2. What kind of vulnerabilities does the Claude Mythos Preview model identify?

- Option: Zero-day vulnerabilities
- Option: Artificial vulnerabilities
- Option: Day-one vulnerabilities
- Option: Phishing vulnerabilities

3. What is the name of the group formed by major tech companies to address vulnerabilities?

- Option: Cybersecurity Alliance
- Option: Project Glasswing
- Option: AI Defense Group
- Option: Tech Safety Coalition

4. Which company is NOT mentioned as being involved in Project Glasswing?

- Option: Nvidia
- Option: Sony
- Option: Apple
- Option: Microsoft

5. How much funding is Anthropic providing in usage credits to support the project?

- Option: \$50 million
- Option: \$100 million
- Option: \$150 million
- Option: \$200 million

6. What is the primary aim of Project Glasswing?

- Option: Increase software sales
- Option: Protect systems from AI-driven attacks
- Option: Create new operating systems
- Option: Develop new web browsers

### True-False

7. Anthropic's AI model is not effective at coding.



- 
8. Zero-day vulnerabilities allow hackers to attack software without warning.
  9. Project Glasswing includes participation from cybersecurity experts.
  10. The funding provided by Anthropic is aimed at improving hardware systems.
  11. AI will have no impact on cybersecurity according to experts.
  12. Major tech companies have proactively formed a group to address cybersecurity vulnerabilities.

### Gap-Fill

13. Anthropic introduced an AI model named Claude Mythos \_\_\_\_\_
14. The vulnerabilities discovered are called \_\_\_\_\_ vulnerabilities.
15. Project Glasswing aims to protect important systems from AI-driven \_\_\_\_\_
16. Anthropic is supporting the project with \$100 million in usage \_\_\_\_\_
17. Companies involved in Project Glasswing include Amazon, Apple, and \_\_\_\_\_
18. The news about zero-day vulnerabilities surprised many in the technology and \_\_\_\_\_  
fields.

### Answer

**Multiple Choice:** 1. Claude Mythos Preview 2. Zero-day vulnerabilities 3. Project Glasswing 4. Sony 5. \$100 million 6. Protect systems from AI-driven attacks

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

**Gap-Fill:** 13. Preview 14. zero-day 15. attacks 16. credits 17. Microsoft 18. cybersecurity

### Vocabulary quizzes

**Multiple Choice ( Select the Correct answer for each question. )**



- 
1. What is the primary focus of cybersecurity?
    - Option: Preventing physical theft
    - Option: Protecting computer systems and networks from damage
    - Option: Enhancing user experience
    - Option: Increasing internet speed
  
  2. Which term refers to weaknesses in a system that can be exploited by threats?
    - Option: Defenses
    - Option: Vulnerabilities
    - Option: Firewalls
    - Option: Protocols
  
  3. What is often required to stay ahead of new cybersecurity threats?
    - Option: Budget cuts
    - Option: Technical advancements
    - Option: Less training
    - Option: Fewer regulations
  
  4. Who are professionals that specialize in identifying and responding to cybersecurity issues?
    - Option: Novices
    - Option: Analysts
    - Option: Experts
    - Option: Amateurs
  
  5. What is the term for the actions taken to address a cybersecurity incident?
    - Option: Response
    - Option: Detection
    - Option: Prevention
    - Option: Analysis
  
  6. What can enhance the effectiveness of cybersecurity measures?
    - Option: Isolation
    - Option: Partnership
    - Option: Competition
    - Option: Confidentiality
  
  7. What do harmful activities targeting computer systems and networks refer to?
    - Option: Opportunities
    - Option: Creates
    - Option: Threats
    - Option: Rewards



8. What do organizations usually set to ensure cybersecurity projects are completed on time?

- Option: Timeline
- Option: Deadline
- Option: Schedule
- Option: Benchmark

9. What can result from a significant cybersecurity breach?

- Option: Order
- Option: Chaos
- Option: Stability
- Option: Growth

10. What situation does a major cybersecurity incident often trigger?

- Option: Normal operations
- Option: Emergency
- Option: Maintenance
- Option: Planning

**Gap-Fill ( Fill in the blanks with the correct word from the vocabulary list. )**

11. The potential misuse of technology is a serious concern in the field of \_\_\_\_\_.

12. There is often a lot of hype surrounding new advancements in technology, particularly in \_\_\_\_\_.

13. Analysts play a crucial role in identifying potential \_\_\_\_\_ before they can be exploited.

14. The latest gadgets are often priced based on their quality and technological \_\_\_\_\_.

15. Keeping up with rapid technical \_\_\_\_\_ is essential for cybersecurity professionals.

16. Many brands offer discounts on gadgets to attract customers during sales \_\_\_\_\_.

17. Failure to address cybersecurity threats can lead to significant \_\_\_\_\_ for businesses.



18. Customers were furious when their data was compromised, leading to a major public \_\_\_\_\_.
19. Innovative gadgets are continuously being released, enhancing our daily \_\_\_\_\_.
20. In times of a ceasefire, focus on cybersecurity can often be \_\_\_\_\_ as resources are redirected.

**Matching Sentences ( Match each definition to the correct word from the vocabulary list. )**

21. Technology companies often celebrate the release of new devices with grand events.
22. Analysts play a vital role in interpreting data trends and providing insights.
23. Cyber attacks during holiday sales can create chaos for online retailers.
24. The system was freezing due to an overload of requests during the promotion.
25. A strong partnership between organizations can improve their cybersecurity stance.
26. Many brands are offering discounts to entice consumers during the holiday season.
27. The hype surrounding the new smartphone model drove its initial sales.
28. Having the right expertise in cybersecurity is crucial to protecting sensitive information.
29. Identifying vulnerabilities before they are exploited is a key aspect of cybersecurity.
30. Ignoring cybersecurity measures can lead to devastating consequences for companies.

**Answer**

- Multiple Choice:** 1. Protecting computer systems and networks from damage 2. Vulnerabilities 3. Technical advancements 4. Experts 5. Response 6. Partnership 7. Threats 8. Deadline 9. Chaos 10. Emergency
- Gap-Fill:** 11. cybersecurity 12. cybersecurity 13. vulnerabilities 14. advancements 15. advancements 16. events 17. consequences 18. backlash 19. lives 20. disrupted
- Matching sentence:** 1. release 2. analysts 3. chaos 4. freezing 5. partnership 6. discounts 7. hype 8. expertise 9. vulnerabilities 10. consequences



---

## CATEGORY

1. Business - LEVEL2

## POST TAG

1. A2
2. amazon
3. Apple
4. Claude Mythos
5. cybersecurity
6. ESL learning
7. esl news
8. google
9. L2
10. Level 2
11. microsoft
12. Nvidia

## Tags

1. A2
2. amazon
3. Apple
4. Claude Mythos
5. cybersecurity
6. ESL learning
7. esl news
8. google
9. L2
10. Level 2
11. microsoft
12. Nvidia

## Date Created

2026/04/09

## Author

aimeeyoung99

ESL-NEWS.COM