



APP WAR

DIGITAL DETECTIVE

SET 3

LEVEL 1

Scenario: The Data Theft at CyberGuard Inc.

- At CyberGuard Inc., a cybersecurity company, a substantial amount of sensitive client data has been stolen from their secure servers. As a digital detective, your mission is to investigate this breach.

SUSPECTS

Dr. Emily Wong - Lead Cybersecurity Analyst: Dr. Wong oversees the company's security measures and has access to critical client databases. She's known for her expertise in data encryption.

Mark Thompson - Systems Administrator: Mark manages the company's server infrastructure and holds extensive knowledge of security protocols. He's been experiencing personal issues lately.

Sophie Rodriguez - Junior Software Engineer: Sophie has limited access to specific server configurations and has been working on optimizing database performance.

CLUES

Altered Access Logs: Examination of server logs reveals altered access logs related to the data theft. Suspicious log entries point to unauthorized access during non-office hours, traced back to Mark Thompson's administrative credentials.

LEVEL 2

Scenario: The Social Media Data Breach at NetConnect Inc.

- At NetConnect Inc., a prominent social media platform, a significant data breach has occurred, compromising user information. Your task as a digital detective is to investigate this cybercrime.

SUSPECTS

Dr. Emily Wong - Chief Security Officer: Dr. Wong oversees the company's security protocols and has access to user data. She's known for her expertise in encryption technologies.

Mark Thompson - Lead Developer: Mark is responsible for implementing new features and maintaining the platform's codebase. He has extensive knowledge of the system's architecture.

Sophie Rodriguez - Data Analyst: Sophie handles user data analytics and has been seen accessing sensitive user profiles more frequently than usual.

Ethan Carter - IT Administrator: Ethan manages server configurations and access controls. He has recently expressed dissatisfaction with the company's security protocols.

Liam Patel - Customer Support Representative: Liam interacts with users daily and has access to user profiles to resolve issues. He's been seeking ways to gain access to more user data for support purposes.

CLUES

Anomalous Login Activity: Analysis of server logs reveals unusual login attempts from multiple locations using Dr. Emily Wong's administrative credentials during off-hours.

Unauthorized Data Export: Investigation shows that a significant amount of user data was exported from the platform's database, coinciding with Sophie Rodriguez's user credentials.

LEVEL 3

Scenario: The Corporate Espionage at TechGenius Corp

- At TechGenius Corp, a leading technology company specializing in AI research, suspicions of corporate espionage have arisen after a substantial amount of proprietary code was stolen. As a digital detective, your mission is to investigate this breach.

SUSPECTS

- Dr. Emily Wong – Chief Scientist: Dr. Wong leads the AI research division and has access to the proprietary code. She's known for her breakthroughs in AI algorithms.
- Mark Thompson – Lead Developer: Mark is responsible for coding AI algorithms and has been under pressure due to project deadlines. He has extensive knowledge of the stolen code.
- Sophie Rodriguez – Data Analyst: Sophie works with AI datasets and has been seen accessing the code repository more frequently than usual.
- Ethan Carter – Security Analyst: Ethan oversees system security and has expressed concerns about vulnerabilities in the code repository.
- Liam Patel – Junior Programmer: Liam has access to the code repository and has recently shown an unusual interest in algorithms similar to the stolen ones.
- Natalie Rivera – AI Researcher: Natalie collaborates closely with Dr. Wong and has expressed dissatisfaction with limited access to specific code segments.
- Michael Johnson – Outsourced IT Consultant: Michael was involved in a recent system upgrade and had temporary access to the code repository.

CLUES

- Unusual Data Transfer: Investigation reveals a large data transfer from the code repository to an external server, coinciding with Sophie Rodriguez's user login.
- Altered Access Logs: Examination of server logs indicates tampering, with unauthorized access to the code repository during non-office hours, traced back to Liam Patel's credentials.
- Email Trail: Intercepted emails discuss the sale of proprietary code to a competitor. The email chain involves Dr. Emily Wong's email account and mentions potential collaboration with a developer.

ANSWER-LEVEL 1

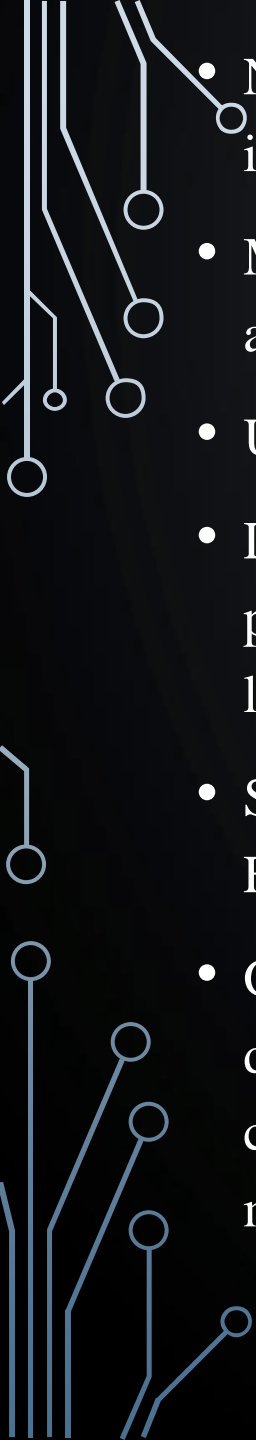
- Analyzing the evidence and suspects:
- Dr. Emily Wong: Oversees security measures and has access to critical databases, but there's no direct evidence linking her to the altered access logs or the data theft.
- Mark Thompson: The altered access logs traced back to his administrative credentials raise suspicions. His personal issues might suggest a motive, but further investigation into his actions during non-office hours is necessary.
- Sophie Rodriguez: Limited access to server configurations, but no direct evidence ties her to the altered logs or the data theft.
- Upon examination:
- Mark Thompson stands out due to the altered access logs linked to his administrative credentials. However, further investigation into his motives and actions during non-office hours is crucial to confirm his involvement in the data theft.
- Dr. Emily Wong and Sophie Rodriguez lack direct evidence connecting them to the data theft or the altered access logs.
- Given the evidence, Mark Thompson appears as the primary suspect due to the altered access logs linked to his credentials. However, further investigation into motives and potential collaborations among the suspects is necessary to confirm the perpetrator of the data theft.

ANSWER LEVEL 2

- Analyzing the evidence and suspects:
- Dr. Emily Wong: Unusual login attempts using her administrative credentials during off-hours raise suspicions. However, further investigation into potential motives or if her credentials were compromised is necessary.
- Mark Thompson: No direct evidence ties him to the breach. His extensive knowledge of the system doesn't link him to the unauthorized login or data export.
- Sophie Rodriguez: Exporting user data with her credentials raises suspicion. Her increased access to sensitive profiles needs further investigation to determine if it was legitimate or unauthorized.
- Ethan Carter: Expressing dissatisfaction with security protocols doesn't directly implicate him. No direct evidence connects him to the unauthorized activities.
- Liam Patel: Seeking more user data for support purposes is suspicious. However, no direct evidence ties him to the breach.
- Upon examination:
- Dr. Emily Wong stands out due to the unusual login attempts using her administrative credentials during off-hours. Further investigation is crucial to determine if she acted independently, if her credentials were compromised, or if there's a different explanation for this activity.
- Sophie Rodriguez also raises suspicion due to the unauthorized data export using her credentials. However, additional investigation is required to understand the context behind her increased access and determine if it was legitimate or malicious.

ANSWER LEVEL 3

- Upon examining the evidence and suspects:
- Dr. Emily Wong: Involvement in an intercepted email discussing the sale of proprietary code raises suspicions. However, direct involvement in the unusual data transfer or altered access logs isn't evident.
- Mark Thompson: No direct evidence links him to the data transfer or altered access logs. His stress due to project deadlines might suggest a motive, but more evidence is needed.
- Sophie Rodriguez: The large data transfer coinciding with her user login is suspicious. Further investigation into her motives for accessing the code repository extensively is required.
- Ethan Carter: Concerns about vulnerabilities but lacks direct evidence tying him to the data transfer or altered logs.
- Liam Patel: Unauthorized access using his credentials during non-office hours

- 
- A decorative graphic consisting of white and light blue lines resembling a circuit board or a stylized tree, located on the left and right edges of the slide.
- Natalie Rivera: Dissatisfaction with limited access to specific code segments doesn't directly implicate her in the data breach.
 - Michael Johnson: Had temporary access but lacks direct evidence tying him to the suspicious activities.
 - Upon examination:
 - Dr. Emily Wong stands out due to involvement in the intercepted email discussing the sale of proprietary code. However, direct evidence tying her to the data transfer or altered access logs is lacking.
 - Sophie Rodriguez is suspicious due to the large data transfer coinciding with her user login. Further investigation into her motives for accessing the code repository extensively is necessary.
 - Given the evidence, Dr. Emily Wong emerges as a primary suspect due to her involvement in discussing the sale of proprietary code. However, a deeper investigation into motives, collaborations among suspects, and the extent of their involvement is necessary to confirm the main perpetrator behind the corporate espionage.