APP WAR

DIGITAL DETECTIVE

SET 1

LEVEL 1

Scenario: **The Data Theft at Tech Innovations Inc.**

- At Tech Innovations Inc., a leading technology research company, a substantial amount of proprietary research data has been stolen from their secure servers. As a digital detective, your mission is to unravel this mystery.

SUSPECTS

- **Dr. Emily Johnson - Chief Research Scientist:** Dr. Johnson oversees the research department and has access to all proprietary data. She's known for her groundbreaking work but has been under pressure due to recent budget cuts affecting her projects.
- **Maxwell Chen - Lead Systems Administrator:** Maxwell manages the company's server infrastructure and has intricate knowledge of security protocols. He's been advocating for system upgrades but faced resistance from management due to budget constraints.
- **Sophie Patel - Junior Research Assistant:** Sophie is a talented researcher who had limited access to specific project data. She's ambitious and has expressed frustration about the slow career progression at the company.

CLUES

- **Unauthorized Access Log:** Investigation of the server logs reveals an unauthorized login during non-office hours, accessing the proprietary research database. The access was made using Maxwell's administrative credentials.

LEVEL 2

Scenario: **The Insider Trading Breach**

- At a prominent financial firm specializing in stock trading, a breach has occurred, leading to suspicions of insider trading. Your task as a digital detective is to investigate this complex breach.

SUSPECTS

- **Dr. Emily Wong - Senior Analyst:** Dr. Wong has been analyzing market trends and had access to confidential reports regarding upcoming company mergers. She's known for her accuracy in predicting market movements.
- **Mark Thompson - IT Specialist:** Mark manages the firm's network and servers. He's recently been advocating for system upgrades but faced pushback from management due to budget constraints.
- **Sophie Rodriguez - Junior Trader:** Sophie has been making unexpected profitable trades aligned with confidential information. Her recent extravagant lifestyle changes have raised eyebrows.
- **Ethan Carter - Compliance Officer:** Ethan is responsible for overseeing regulatory compliance within the firm. He's been vocal about stricter security protocols but faced resistance from traders.
- **Liam Patel - Financial Advisor:** Liam advises high-net-worth clients and has access to sensitive market forecasts. He's known for his strategic advice, but recent discrepancies have emerged in his trading patterns.

CLUES

- **Unusual Trading Patterns:** Analysis of trading records shows a series of unusually profitable trades made shortly before major market shifts. These trades were executed using Sophie's trading account.
- **Altered Security Logs:** Investigation of the security logs reveals deliberate tampering, with access logs related to the confidential reports being deleted. Some deleted logs point to activities conducted by Dr. Emily Wong's workstation.

LEVEL 3

Scenario: **The Ransomware Attack at TechTech Corp**

- At TechTech Corp, a leading technology company, a severe ransomware attack has occurred, causing a major data breach. As a digital detective, your task is to investigate this sophisticated cybercrime.

SUSPECTS

- **Dr. Emily Wong - Chief Technology Officer (CTO):** Dr. Wong oversees the company's technology infrastructure and had been advocating for enhanced cybersecurity measures. She has access to critical systems.
- **Mark Thompson - Lead Software Engineer:** Mark is responsible for developing security patches and maintaining the company's software. He's been dealing with stress due to recent project delays and resource constraints.
- **Sophie Rodriguez - Network Administrator:** Sophie manages the network configurations and had access to privileged accounts. She has been exhibiting unusual behavior, coming to the office outside her regular hours.
- **Ethan Carter - Security Analyst:** Ethan specializes in monitoring security threats and had flagged potential vulnerabilities in the system. He has been critical of the company's lax approach to security.

- **Liam Patel - IT Support Specialist:** Liam provides technical support and has extensive knowledge of the company's systems. He's been facing personal financial difficulties lately.
- **Natalie Rivera - Data Analyst:** Natalie handles sensitive customer data and has been working on a project involving encryption protocols. She's expressed frustration with the slow progress of her project.
- **Michael Johnson - Outsourced IT Consultant:** Michael was brought in for a recent system audit and had temporary access to various network configurations. He has been seeking a permanent role within the company.

CLUES

- **Altered System Logs:** Examination of the system logs indicates deliberate tampering, with access logs related to the ransomware attack being altered. Some logs show unauthorized access during non-office hours traced back to Sophie's workstation.
- **Email Trail:** An email exchange discussing system vulnerabilities and encryption weaknesses was found in Natalie's inbox. The email chain suggests potential exploitation of these weaknesses.
- **Unusual Financial Transactions:** Financial records reveal unexpected transactions involving large sums of money transferred from Liam's account to an offshore destination around the time of the attack.

ANSWER-LEVEL 1

- In this scenario, the unauthorized access log showing entry into the proprietary research database using Maxwell Chen's administrative credentials is a crucial clue. Considering the evidence and the suspects:
- Dr. Emily Johnson: Although she has access to all proprietary data, there's no direct indication or motive presented for her involvement in the breach. Her frustrations due to budget cuts don't directly tie her to this specific action.
- Sophie Patel: While Sophie is ambitious, her limited access to specific project data might not align with the ability to gain entry using administrative credentials. There's no apparent motive established linking her to the breach.
- Maxwell Chen: The unauthorized access using his administrative credentials is highly suspicious. His advocacy for system upgrades might suggest a motive related to highlighting security vulnerabilities, but it's essential to determine if this was a deliberate act or if his credentials were compromised.
- Upon careful examination, Maxwell Chen stands as the primary suspect due to the unauthorized access using his administrative credentials. However, further investigation is crucial to ascertain whether Maxwell was involved intentionally or if his credentials were misused or stolen, potentially implicating someone else.

ANSWER LEVEL 2

- Examining the evidence and suspects:
- Dr. Emily Wong: The deleted logs associated with confidential reports raise suspicions. However, there's no direct link between her and the trades made using Sophie's account, and her position might grant access but doesn’t necessarily align with trading activities.
- Mark Thompson: While advocating for system upgrades, there's no direct link between his actions and the trades or deleted logs. His role might involve network management, but it doesn't directly tie him to trading activities or the altered security logs.
- Sophie Rodriguez: Her account being used for unusual trades is a significant clue. However, it's necessary to determine if she acted alone, was coerced, or if her account was compromised.

- Ethan Carter: He oversees compliance but doesn't have direct access to trading accounts or confidential reports. His advocacy for tighter security doesn’t connect him to the altered logs or the trades.
- Liam Patel: While having access to sensitive forecasts, there's no direct evidence linking him to the altered logs or trades. His advisory role might not directly translate to executing trades on Sophie's account or deleting security logs.
- Upon careful examination, Sophie Rodriguez emerges as the primary suspect due to the trades made using her account. However, further investigation is necessary to understand if she acted independently, was manipulated, or if there's a larger conspiracy involving others among the suspects. The altered security logs connected to Dr. Emily Wong also indicate potential involvement, warranting deeper scrutiny into her motives and potential collaboration with Sophie or others.

ANSWER LEVEL 3

- In this intricate scenario with multiple suspects and clues:
- Dr. Emily Wong: Advocating for cybersecurity measures, she has access to critical systems. However, there's no direct evidence linking her to the altered logs, the email chain, or financial transactions.
- Mark Thompson: Dealing with stress due to project delays, but there's no direct evidence tying him to the altered logs, email chain, or financial transactions. His role in software maintenance doesn’t directly link him to the suspicious activities.
- Liam Patel: Financial difficulties and unexpected transactions are suspicious, but there's no direct link between his actions and the ransomware attack or other clues.

- Sophie Rodriguez: Suspicion arises due to unauthorized access from her workstation during non-office hours. This aligns with the altered system logs. However, more investigation is needed to determine her motives and if she acted alone.
- Ethan Carter: Critical of the lax security approach, but no direct evidence ties him to the altered logs, email chain, or financial transactions. His role in security monitoring doesn’t directly link him to the suspicious activities.
- Natalie Rivera: Involved in a project related to encryption weaknesses, suggesting a potential motive. However, more evidence is required to establish her involvement in the attack.

- Michael Johnson: As an outsider involved in a system audit, his temporary access might raise suspicion, but there's no direct evidence tying him to the altered logs, email chain, or financial transactions.
- Upon examining the evidence: Sophie Rodriguez stands out due to the unauthorized access from her workstation aligning with the altered logs. However, further investigation is needed to establish her motives and determine if she acted alone or in collaboration with others.
- Natalie Rivera also raises suspicion due to involvement in a project related to encryption weaknesses, suggesting potential exploitation. However, more evidence is required to link her directly to the attack.
- The investigation indicates that Sophie Rodriguez appears to be the primary suspect due to the unauthorized access aligned with the altered logs. However, the involvement of multiple suspects and the complexity of the cybercrime require further scrutiny to establish the full extent of involvement and potential collaborations among the suspects.