1. What is one thing that makes cybersecurity threats so challenging to deal with?   **1 point**

   ○ Most organizations are faced with too few attacks to study effectively or dedicate full-time specialists to investigate

   ● There is a big shortage in cyber security skills and many job openings unfilled

   ○ 'There are too few cybersecurity tools available from too few vendors

   ○ The large majority of "breaches" are inadvertent mistakes by employees which distracts from investigating the few that are from real cyber criminals

2. The level 3 and 4 cybersecurity analysts working in a Security Operations Center (SOC) combat cyber crime by performing which type of activity?   **1 point**

   ● Cyber forensic investigations

   ○ Penetration testing

   ○ Cyber threat hunting

   ○ Cyber data mining

3. True or False. If you have no better place to start hunting threats, start with a view of your own organization then work your way up to an industry view and then a regional view, a national view and finally a global view of the threat landscape.   **1 point**

   ○ True

   ● False

4. Your enemy uses a cyber kill chain to plan and execute his attack against your organization. Which three (3) of these are steps in a cyber kill chain?   **1 point**

   ☑ Exploitation

   ☑ Installation

   ☑ Delivery

   ☐ Recovery

5. True or False. A cyber threat hunting team generally sits outside the SOC command center.   **1 point**

   ● True

   ○ False

6. There is value brought by each of the IBM i2 EIA use cases. Which one of these identifies net new money chain transfers?   **1 point**

   ○ VIP Protection

   ● Fraud Investigations

   ○ Cyber Threat Hunting

   ○ Insider Threat

Submit   Save draft

👍 Like   👎 Dislike   🚩 Report an issue