IT认证电子书

质量更高　服务更好

半年免费升级服务

http://www.itrenzheng.com

Exam : P2150-870

Title : Technical Sales Foundations for IBM Security Intelligence and Analytics V1

Version : DEMO

1.Which QRadar Apps integrate with the User Behaviour Analytics App to enhance its detection capabilities?
A. QRadar Risk Manager and QRadar Network Security
B. QRadar Machine Learning App and Reference Data Import - LDAP
C. QRadar Asset Profiler App and Palo Alto Networks App for QRadar
D. QRadar Incident Remediation App and QRadar Artificial Analysis App
Answer: C

2.How can assets be used to help in investigations?
A. As valuable data sources.
B. Make searching for offenses easier.
C. Help connect an offense to a device.
D. Provide external threat intelligence.
Answer: D

3.An attacker, who has physical access to the premises, has connected a personal laptop to the network in an attempt to sniff traffic and record any clear text passwords.
This scenario would be classified as which type of attack?
A. Fabrication
B. Interception
C. Modification
D. Interruption
Answer: D

4.What does QRadar Network Insight (QNI) create?
A. An Offense from Events.
B. A demilitarized zone from Apple Airport data.
C. OSI Layer 7 packet from OSI Layer 3 flow information.
D. IPFIX records with deep security content from SPAN or TAN port data.
Answer: C

5.Which subjects should be covered when first demonstrating QRadar?
A. 1. The devices QRadar supports.
2. How to write rules to detect spear-fishing attacks.
3. How much EPS QRadar can handle on a single box.
4. Why QRadar should be chosen.
B. 1. The QRadar add-ons. and what problems they solve.
2. How QRadar add-ons work.
3. How to create a custom extracted property from a custom log source.
4. A use case involving different geographies, and its integration to a physical security system (badge reader).
C. 1. The problem QRadar solves.
2. How QRadar works (i.e.. data integration, correlation and offenses).
3. Use cases that apply to the client's business.

4. QRadar's competitive advantages
D. 1. The programming languages used to build QRadar.
2. The cost per EPS and FPM
3. Building a use case in QRadar's rule wizard.
4. A POC so client can personally test the product.
Answer: A