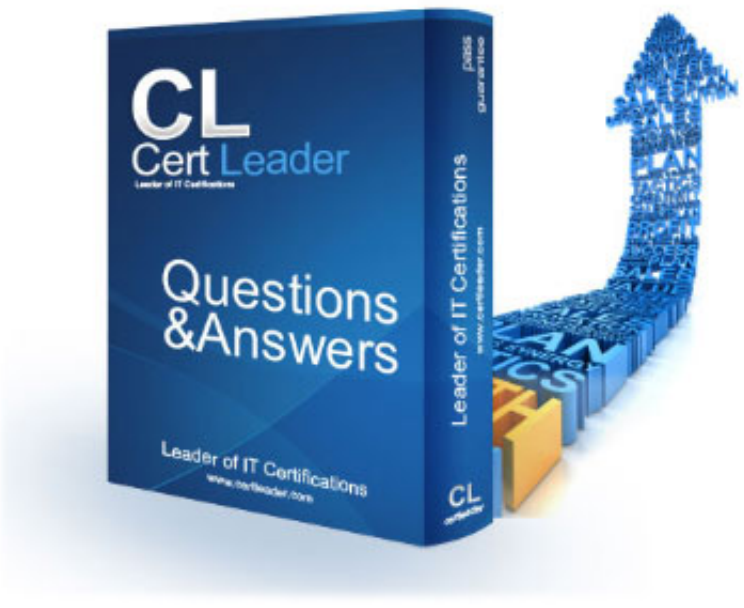
# P2150-870 Dumps

# Technical Sales Foundations for IBM Security Intelligence and Analytics V1

**https://www.certleader.com/P2150-870-dumps.html**



**NEW QUESTION 1**
What type of appliance is a 3105?

A. Flow Collector
B. Event Collector
C. Event Processor
D. All in One OR Console

**Answer:** A

**NEW QUESTION 2**
Where do reports get their data from?

A. Backups
B. Dashboards
C. Saved searches
D. Real-time event data

**Answer:** C

**NEW QUESTION 3**
Besides a QRadar Console, which additional types of appliance does a typical QRadar Incident Forensics deployment contain?
One or more QRadar Incident Forensics appliances, and:

A. one or more QRadar Event Collector appliances.
B. one or more QRadar QFlow Collector appliances.
C. one or more QRadar Vulnerability Scanner appliances
D. one or more QRadar Network Packet Capture appliances

**Answer:** A

**NEW QUESTION 4**
What do prospects typically care about for high level cyber use cases?

A. 1. Advanced Threats2. Insider Threats3. Securing the cloud4. Critical Data Protection
B. 1. Best price for performance2. Outside Threats3. Patching ALL vulnerabilities found as soon as they are reported4. Running a clean data center
C. 1. Having a proper time management system2. Evacuation rule compliance3. Making the sales target for the week4. Speed of deployment and Time to value
D. 1. Having a good password change policy2. Erasing documents which describe a recent data breach3. keeping up to date with Windows patch updates4. cleaning the BGP routing tables regularly

**Answer:** C

**NEW QUESTION 5**
Which is the most common formatused to send event data to a SIEM?

A. JSON
B. LEEF
C. Syslog
D. NetFlow

**Answer:** D

**NEW QUESTION 6**
How does QRadar Advisor with Watson help security analysts investigate security incidents?

A. It analyzes flow data.
B. It analyzes and investigates an offense.
C. It scans systems for vulnerabilities.
D. It extracts packet data for security investigations.

**Answer:** D

**NEW QUESTION 7**
Which metrics are defined for the three virtual appliance system specification (Minimum/Medium/High). (select 4)

A. NICs
B. IOPS
C. Memory
D. Storage
E. CPU cores/speed
F. Maximum Latency
G. Virtual Networks

**Answer:** ACEG

**NEW QUESTION 8**
Which set of items will be checked by IBM before an App is published in the QRadar App Exchange?

A. * Review the App name, version and description* Ensure there is a C&C channel to the App developer.* Run the App to see if it does anything useful.* Change the code so it will function in newer versions of QRadar.
B. * Create a Java version of the App* Check for collisions between App page_scripts and QRadar functions.* Verify that the App does not log any information.* Change the code so it will function in newer versions of QRadar.
C. * Review all APIcalls.* Ensure that there are no hard-coded values.* Run static analysis on any Python and Javascript code* Execute security tests
D. * Automatically deploy/upgrade the App in all QRadar installations* Review the screen-shots and icons in the App.* minimize any App storage usage* Verify the App will create a dashboard widget.

**Answer:** B

**NEW QUESTION 9**
What is the QRadar 14xx Data Node used for? It is used to:

A. offload Offense management tasks from a multi-tenant 31 xx appliance.
B. provide a long term data backup store for 16xx, 17xx, 18xx and 31 xx appliances.
C. provide additional storage and processing for 16x
D. 17xx, 18xx and 31 xx appliances.
E. run complex 'Machine Learning' style applications in the QRadar application framework.

**Answer:** B

**NEW QUESTION 10**
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

**NEW QUESTION 10**
Which types of software appliance are involved of an events is received by an Event Collector, and the event is then to an Event Processor and causes an Offense to be updated on the Console?

A. 13xx to 17xx to 31xx
B. 13xx to 18xxt o 21xx
C. 13xx to 16xx to 31xx
D. 15xx to 17xx to 21xx

**Answer:** C

**NEW QUESTION 11**
Which is NOT an option for the deployment of the QRader sopftware?

A. Cloud
B. Virtual
C. Live CD/DVD
D. 3rdParty Appliance

**Answer:** A

**NEW QUESTION 13**
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

**NEW QUESTION 15**
Which IBM artificial intelligence service can be used to speed up analysis of external threats?

A. QRadar Incident Overview
B. QRadar Advisor with Watson
C. QRadar Machine Learning Analytics
D. QRadar Artificial Intelligence toolbox

**Answer:** D

**NEW QUESTION 19**
What are thesystems called which send events to QRadar?

A. Assets
B. Firewalls
C. Log Sources
D. Data Backups

**Answer:** D

**NEW QUESTION 21**
.....

# Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

## 100% Pass Your P2150-870 Exam with Our Prep Materials Via below:

https://www.certleader.com/P2150-870-dumps.html