

## 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 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 2**

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 3**

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**

**NEW QUESTION 4**

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 5**

What is a benefit of having QRadar on Cloud? IBM is responsible for:

- A. generating new use cases.
- B. alerting the user regarding offenses.
- C. providing 24 hour
- D. 7 days a week health monitoring and system management of the QRadar Deployment.
- E. providing health monitoring and system management of the QRadar Deployment during normal business hours only.

**Answer: D**

**NEW QUESTION 6**

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 7**

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 8

What does QRadar Incident Forensics do? QRadar Incident Forensics:

- A. analyzes event data for an incident that is discovered by QRadar SI EM.
- B. analyzes flow data for an incident that is discovered by a QRadar SI EM.
- C. brings in the vulnerability data relevant for an incident that is discovered by QRadar SIEM.
- D. aggregates the relevant network data for an incident that is discovered by QRadar SIEM.

**Answer:** A

#### NEW QUESTION 9

Assuming relevant indexing is enabled, which is the fastest way to search recent data in an ad-hoc manner?

- A. AQL
- B. Quick Filters
- C. Quick Searches
- D. Saved Searches

**Answer:** C

#### NEW QUESTION 10

Which categorizes a threat to a type of attack?

- A. Sniffin
- B. Interruption
- C. SQL injection, Interception
- D. Man in the middle, Fabrication
- E. Denial of Service, Modification

**Answer:** B

#### NEW QUESTION 10

How can QRadar Network Security improve security posture for companies? By using QRadar Network Security, companies can:

- A. implement an application firewall.
- B. perform event monitoring.
- C. perform vulnerability scanning to detect vulnerabilities.
- D. perform application contro
- E. SSL inspection, and disrupt advanced malware

**Answer:** A

#### NEW QUESTION 12

Which question(s) can QRadar help customers answer concerning the security of their network?

- A. Who is attacking?
- B. What is being attacked?
- C. What is the security impact?
- D. When are the attacks taking place?
- E. All the above

**Answer:** D

#### NEW QUESTION 15

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 19

Which is standard on a QRadar on Cloud deployment?

- A. High Availability
- B. Packet analysis
- C. Vulnerability Management
- D. Custom log source development

**Answer:** B

**NEW QUESTION 24**

Which attributes would contribute to an effective demonstration of QRadar?

- A. Bring a whiteboard since prospect might not have on
- B. Show what each tab of the QRadar interface does.
- C. Show all analysis features on flow dat
- D. Focus on the functions that the prospect asked for
- E. Explain all extension options for add-ons to the prospec
- F. Explain QRadar's architecture and scalability.
- G. Tell a story on how QRadar solves an issue that is relevant to the prospec
- H. Talk about the benefits of QRadar in relation to the prospect's situation.

**Answer:** C

**NEW QUESTION 29**

What is a difference between rules and building blocks?

- A. Rules have responses and Building Blocks do not.
- B. Rules can be used for reporting and Building Blocks cannot.
- C. Building Blocks have responses and Rules do not.
- D. Building Blocks only use flows and Rules only use events.

**Answer:** A

**NEW QUESTION 31**

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 32**

Which TCP/IP protocols are at layer 4 of the OSI model (Select 2)

- A. TCP
- B. UDP
- C. ARP
- D. ICMP
- E. IGMP

**Answer:** AB

**NEW QUESTION 36**

What would be relevant questions to ask for scoping the environment? (Select 3)

- A. How many data centers do you have?
- B. How many users will be using QRadar?
- C. How many storage networks to you have?
- D. How many QRadar appliances do you want to acquire?
- E. How many log sources do you want to add to the project?
- F. In how many countries do you want to deploy QRadar?
- G. Which compliance extensions do you need to deploy?

**Answer:** CFG

**NEW QUESTION 39**

To view flow data in QRadar, which tab should a user navigate to?

- A. Assets
- B. Log Activity
- C. User Analytics
- D. Network Activity

**Answer:** A

**NEW QUESTION 41**

.....

## 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>