incertain

certain

**An organization is continually scanning their business application source code for vulnerabilities before releasing them into production. Using the maturity categories of the integration quadrant model, what state would this implementation be characteristic of for an organization and its evolving approach to IT security?**

1. proficient
2. basic
3. optimized
4. reactive

**What is the primary consequence of not detecting malware once it has infected its 'first' machine within your network?**

1. It becomes the new launch point in order to attain deeper penetration within the network.
2. It conducts port scans of your network to discover vulnerabilities within your firewall.
3. It exfiltrates as many valuable assets within your network as possible before detection.
4. It attacks and attempts to neutralize any and all endpoint protection on the device.

**What are two architectural components of the Architecture discipline when discussing the the O-ESA Enterprise Security Program? (Select two.)**

1. application architecture
2. network architecture
3. facilities architecture
4. logical architecture
5. conceptual architecture

**Which statement describes the process of Vulnerability Management within the Operations discipline of the O-ESA Enterprise Security Architecture?**

1. The process of protecting operational digital assets against accidental or unauthorized modification.
2. The process for identifying high-risk infrastructure components, assessing their vulnerabilities, and taking the appropriate actions to control the level of risk to the operational environment.
3. The process of ensuring that the deployed technology conforms to the organization's policies.
4. The process of responding to security-related events that may violate the organization's security policies.

**Which two search criteria are required to add a custom Dashboard Item? Select all that apply :**

1. compiled
2. grouped
3. time series based
4. fixed time period

**When can users change their account passwords in the User Preferences interface of QRadar SIEM?**

1. when the account utilizes LDAP authentication
2. when the account utilizes local system authentication
3. when the account utilizes RADIUS authentication
4. when the account utilizes Active Directory authentication

**Which PCI-DSS regulation can be addressed by a Security Intelligence platform in order to ensure compliance?**

1. data transmission encrypting
2. security policy for employees and contractors
3. restricting physical access
4. firewall protection of cardholder data

**Passive network flow analytics provides what benefit?**

1. building asset profiles and classifying hosts
2. imposing network data flow limits
3. resolving network traffic issues
4. protecting against 0-day attacks

**What functionality is provided by the Flow Processor?**

1. provides temporary storage of normalized log events and payload
2. processes third-party network and QFlow through the CRE and stores the flows
3. receives third-party network flows and packages
4. receives log records, normalizes and forwards them to an event processor

**How can a MAC address be entered for an asset? (Select three.)**

1. by an active scanner
2. by manually editing
3. by the asset profile
4. by the Flow Collector
5. by a system log scan
6. by the QFlow software

**In order to add new assets, which field can be included in a CSV file when importing it into QRadar SIEM?**

1. Operating System
2. IP address
3. MAC address
4. Vulnerabilities

**Which type of object does an asset profile describe?**

1. Service
2. Operating System
3. Network
4. Host

**How does QRadar SIEM determine which services are running on an asset?**

1. by probing the asset's network ports
2. by scanning system log files on the asset
3. by processing the asset's running task list
4. by observing network flows to/from the asset

**Which data source can add and update information about currently-running software products to an asset profile?**

1. VPN lease files
2. flow data
3. firewall logs
4. system logs

**If a system uses multiple network adapters on multiple networks but a user can only view one of the networks, how will the system appear in the QRadar Dashboard for that user?**

1. A yellow exclamation mark will appear next to the system.
2. A 'Hidden Data' message box will appear when reviewing results.
3. The user will not see the system asset profile at all.
4. The system will not have all its networks displayed.

**Which of the following is not a valid Offense Type?**

1. Destination IP
2. Source IP
3. Username
4. Vulnerability (CVE)

**Which offense weighted Magnitude parameter indicates how valid the information from the source is?**

1. Credibility
2. Severity
3. Status
4. Relevance

**Where can a user add custom notes? (Select two.)**

1. Rules
2. Log Activity
3. Dashboard
4. Offenses Summary

**Which type of offense originates from only one source IP address?**

1. source mac address
2. source ip identity
3. source port
4. source ip

**What is the prime benefit of QRadar SIEM for security analysts?**

1. It provides advanced filters to examine specific activities in your environment.
2. It stores security-relevant information about systems in your network.
3. It correlates data to detect suspicious activities, based on tests, and combines them together into offenses.
4. it automatically creates and updates asset profiles for systems.

**How does QRadar SIEM select the Top 5 Source IP addresses on the Offense Summary page?**

1. It selects the top 5 source IP addresses with the highest magnitude.
2. It selects the top 5 source IP addresses with the highest weight.
3. it selects the top 5 source IP addresses with the most severe vulnerabilities.
4. it selects the top 5 source IP addresses with the highest event count.

**Which anomaly detection rule type should be used to look for seasonal traffic trends?**

1. anomaly
2. offense
3. threshold
4. behavioral

**What can a custom 'common rule' test?**

1. flows only
2. events and flows
3. events only
4. offenses only

**Which two statements are true regarding compliance and control within today's organizations' IT structures? (Select two.)**

1. It is possible to be in compliance and not be in control.
2. It is possible to be in control and not be in compliance.
3. Being in compliance is more important than being in control.
4. Being in compliance demonstrates evidence of control

**What is the goal of a real-time Security Intelligence solution?**

1. make it harder for attackers to exfiltrate data by applying data-in-transit encryption
2. route all database activity monitoring data to a centralized console
3. implement proper privileged identity management to restrict access to high value assets
4. inform security analysts about a breach the moment an attacker penetrates the perimeter

**Which IBM QRadar platform product can compile reports to assist in HIPAA or PCI-DSS regulatory compliance?**

1. IBM Security QRadar Vulnerability Manager
2. IBM Security QRadar Data Node
3. IBM Security QRadar SIEM
4. IBM Security QRadar Log Manager

**Which method is used to correlate and accumulate historical data for report generation?**

1. Rule
2. Property filters
3. Compiled Search
4. Relational database table

**What is the data source for reports that are being run on raw data?**

1. data collected from previous reports
2. indexed data queue
3. data collected only within last 7 days
4. stored data

**Which two free vulnerability data sources are used by QRadar SIEM? (Select two.)**

1. Open Source Vulnerability Database (OSVDB)
2. Vulnerability process results from a network scanner outside the firewall.
3. Internal references from the active scanners inside the firewall.
4. national Vulnerability Database (NVDB)

**What is the definition of an event?**

1. An event is a record from a device that describes an action on a network or host.
2. An event represents log messages from a wide variety of external log sources.
3. An event represents a suspected attack or policy breach.
4. An event is used to map information to common field names.

**How are offenses created?**

1. Each data node uses Event Processors to create offenses.
2. Event collectors normalize the events and create the offense.
3. Device Support Modules (DSMs) parse events to create the offense.
4. The Magistrate correlates data from Event Processors to create offenses.

**Which QRadar SIEM component tracks services on assets that are listening on open network ports?**

1. Flow Collector
2. Asset Profiles
3. Magistrate
4. Event Collector

**What benefit does IBM Security QRadar Vulnerability Manager provide to QRadar SIEM?**

1. It processes results from a hosted scanner to see a view from inside the firewall boundaries.
2. It provides investigation capabilities to assess the collected raw data from assets.
3. it provides an active scanner that is present on all event and flow collectors.
4. It provides advanced filters to examine specific activities on the network.

**What is an IBM QRadar 'offense'?**

1. a correlated set of incidents triggering a rule or rules
2. a bidirectional sequence aggregated into sessions
3. raw network data related to a security incident
4. context to identify key vulnerabilities and reduce false positives

**You are the security officer of your company. You suspect that someone in your organization is leaking information to competitors by copying restricted files onto external cloud storage. You need to identify the culprit, retrieve and rebuild any incriminating information. Which IBM QRadar platform product would be ideal for performing this task?**

1. IBM Security QRadar Vulnerability Manager
2. IBM Security QRadar Incident Forensics
3. IBM Security QRadar SIEM
4. IBM Security QRadar Risk Manager

**How does an event collector support automating the parsing of collected log data?**

1. pushing logging settings to new machines
2. periodic server scanning and log configuration
3. autodiscovery of newly detected log sources
4. extraction of log message from network flows

**What type of database is used to store event data on the IBM QRadar Event Processor?**

1. Ariel
2. PostgreSQL
3. Oracle
4. MySQL

**Which type of network flow will be converted into a type B superflow (for example, DDoS) in an IBM QRadar flow collector?**

1. single source, single destination, changing ports
2. multiple source, multiple destination
3. multiple source, single destination
4. single source, multiple destination

## 

**Which statement is true when it comes to integrating BYOD into the network of a company organization?**

1. By its very nature, mobile technology is outside of an organization's physical network perimeter and control.
2. Companies no longer have to worry about the separation between work and personal data.
3. It allows users greater choice while reducing security risks to the network itself.
4. Asset management is no longer a concern since the company does not own the devices.

**Which statement represents a characteristic of today's social media as it relates to IT?**

1. It consists of structured data.
2. It utilizes predefined data models.
3. The data it contains is easy to work with.
4. It consists of unstructured data.

**How does QRadar SIEM capture time-series data in order to reduce storage needs?**

1. by generating hourly log files only of violations
2. by storing all network activity in a database
3. by aggregating data for time periods
4. by keeping data only for a day

**What is a unique feature of AQL filtering?**

1. It can use pre-defined category definitions.
2. It uses a graphical interface to build queries.
3. It allows an SQL-like syntax for filtering.
4. It can adjust what the network scanners catch.

**What is a negative implication of enabling time series data?**

1. QFlow cannot be utilized to analyze network traffic.
2. Flows that contain time series data cannot be grouped
3. It can negatively affect the performance of QRadar SIEM.
4. Events that contain time series data cannot be grouped.

**Which three types of information are included in the default 'List of Events' page? (Select three.)**

1. QID
2. Source IP
3. Protocol
4. Log Source
5. Event Name

**What does the 'Log Source' field record?**

1. the database where the raw entry is stored
2. the network segment of the offense
3. the original device sending the raw payload
4. the source IP of the raw event

**What does a 'false positive' designation do to a log or flow event?**

1. reduces the severity of the event by half
2. automatically hides future events that match the event
3. permanently disables any filter in all future scans
4. prevents the event from contributing to an offense

**What must be done first in order to define storage requirements for a Security Intelligence system?**

1. Configure the IT systems in scope to meet the logging requirements in accordance with the IT security policy.
2. Verify that logging does not affect service-level requirements of individual IT systems or the overall IT solution in scope.
3. Increase the storage needs by twenty percent to provide a buffer based on the user manuals of the Security Intelligence solution.
4. Monitor log generation for seven days to get a baseline in storage capacity planning.

**You are viewing a list of events within the 'List of Events' display. You are currently highlighting a firewall event with an IP address of 172.16.56.3, involving a potentially malicious host. In exact order, which two steps should you take in order to monitor the designated malicious source IP?**

1. Add a filter on the IP address, and then delete the offense filter with the Clear Filter option.
2. Clear the offense filter, and then add filter on the IP address.
3. Identify the IP address as a false positive, and then clear the offense filter.
4. Set the IP address as a normalized event, and then filter on the IP address.

**How is the raw payload of an event or flow stored by QRadar SIEM?**

1. QRadar adds a header describing the sending host.
2. It is stored in its original and un-parsed format.
3. Only the first 256 bytes of the message are saved.
4. QRadar highlights only the relevant parts of the message.

**One of the functional requirements of the Security Intelligence solution focuses on reporting. Which task associated with defining the reporting requirements has to be executed first?**

1. Define the types and use cases of reports needed.
2. Define the frequency of the reports needed.
3. Define the amount of data processed per report
4. Define the maximum number of users running reports simultaneously.

**Which Superflow attack type is profiled by the following characteristics: single source IP address over many ports to a single destination IP address?**

1. Type A : network sweep
2. Type B : distributed denial of service
3. Type C : port scan
4. Type A : broadcast

**By default, how many bytes of Layer 7 payload does QRadar SIEM capture?**

1. 64 bytes
2. 1024 bytes
3. the total bytes sent by the source
4. the total bytes received by the destination

**You are creating a false positive flow using QRadar SIEM and selecting the traffic direction of the flow. Why would you rarely, if ever, designate the traffic direction as being 'Any Source to any Destination?'**

1. It would only capture broadcast traffic.
2. It would create too much traffic on the local network.
3. It would eliminate all correlation of the flow with offenses.
4. It would utilize too much processing power.

**You are reviewing events listed under the Network Activity tab. Some of the events have a 'C' listed after the number of Source Bytes. What does this mean?**

1. The captured bytes have a high severity rating.
2. The captured bytes are part of a saved search.
3. The captured bytes are contained in a cache file.
4. The captured bytes contain Layer 7 payload.

**Which statement is true concerning false positive flows?**

1. QFlow collectors will ignore them.
2. They still contribute to offenses.
3. They are processed, displayed under Network Activity, and stored by QRadar SIEM.
4. They do not contribute to reports.

**What is a benefit of configuring a superflow in QRadar SIEM?**

1. There is reduced processing on the QRadar SIEM host machine.
2. Traffic from the QFlow collectors is encrypted and secure.
3. There is reduced traffic from the network QFlow collectors.
4. Reporting traffic is only captured on an hourly basis.

**Which activity would be performed during the data collection phase of a Security Intelligence design?**

1. Gather security intelligence requirements about the network topology.
2. Define the micro system design model.
3. Define functional requirements for event collection.
4. Update the component model for asset classification.

**Which functional requirement discipline of an IT security framework includes reporting on security logs?**

1. auditing
2. response
3. configuration
4. detection

**When designing a Security Intelligence solution design, you cannot simply collect and archive every audit and log record that is generated in your organization. What fact should be used to prioritize what data is collected from assets?**

1. The number of asset users.
2. Focus on the important and valuable assets that need protection.
3. The location of the assets.
4. The asset's level of integration.

**What is the first high-level step in creating a Security Intelligence solution design?**

1. Implement and deploy the Security Intelligence solution.
2. Design operational processes to support the Security Intelligence design.
3. Design the IT security architecture for the Security Intelligence design.
4. Identify the IT security framework and procedures used by the organization.

**When designing a Security Intelligence solution design, you cannot simply collect and archive every audit and log record that is generated in your organization. What fact should be used to prioritize what data is collected from assets?**

1. The location of the assets.
2. Focus on the important and valuable assets that need protection.
3. The number of asset users.
4. The asset's level of integration.

## 

## **What must be done first in order to define storage requirements for a Security Intelligence system?**

1. Configure the IT systems in scope to meet the logging requirements in accordance with the IT security policy
2. Verify that logging does not affect service-level requirements of individual IT systems or the overall IT solution in scope
3. Monitor log generation for seven days to get a baseline in storage capacity planning
4. Increase the storage needs by twenty percent to provide a buffer based on the user manuals of the Security Intelligence solution

## **One of the functional requirements of the Security Intelligence solution focuses on reporting. Which task associated with defining the reporting requirements has to be executed first?**

## 

|  |
| --- |
| A. Define the maximum number of users running reports simultaneously.  B. Define the types and use cases of reports needed  C. Define the amount of data processed per report  D. Define the frequency of the reports needed. |

## 

## 

## 

## 

## 

|  |  |
| --- | --- |
|  | |
|  |  |
|  |  |
|  |  |
|  |  |