1. True or False. SIEMs can be available on premises and in a cloud environment. **1 point**

- (•) True
- ( ) False

2. For a SIEM, what are logs of specific actions such as user logins referred to? **1 point**

- ( ) Logs
- ( ) Actions
- ( ) Flows
- (•) Events

3. Which of these describes the process of data normalization in a SIEM? **1 point**

- ( ) Removes duplicate records from incoming data
- ( ) Encrypts incoming data
- (•) Indexes data records for fast searching and sorting
- ( ) Compresses incoming

4. When a data stream entering a SIEM exceeds the volume it is licensed to handle, what are three (3) ways the excess data is commonly handled, depending upon the terms of the license agreement? (Select 3) **1 point**

- [x] The excess data is dropped
- [ ] The data is processed and the license is automatically bumped up to the next tier.
- [x] The excess data is stored in a queue until it can be processed
- [x] The data stream is throttled to accept only the amount allowed by the license

5. Which five (5) event properties must match before the event will be coalesced with other events? (Select 5) **1 point**

- [x] Source IP
- [x] Username
- [x] Destination Port
- [ ] Source Port
- [x] Destination IP
- [x] QID

6. What is the goal of SIEM tuning? **1 point**

- (•) To get the SIEM to sort out all false-positive offenses so only those that need to be investigated are presented to the investigators
- ( ) To get the SIEM to present all recognized offenses to the investigators
- ( ) To increase the speed and efficency of the data processing so license caps are never exceeded.
- ( ) To automatically resolve as many offenses as possible with automated actions

7. True or False. QRadar event collectors send all raw event data to the central event processor for all data handling such as data normalization and event coalescence. **1 point**

- ( ) True
- (•) False

8. The triad of a security operations centers (SOC) is people, process and technology. Which part of the triad would containment belong? **1 point**

- ( ) People
- (•) Process
- ( ) Technology
- ( ) None of the above

9. True or False. There is a natural tendency for security analysts to choose to work on cases that they are familiar with and to ignore those that may be important but for which they have no experience. **1 point**

- (•) True
- ( ) False

10. The partnership between security analysts and technology can be said to be grouped into 3 domains, human expertise, security analytics and artificial intelligence. The security analytics domain contains which three (3) of these topics? **1 point**

- [x] Anomaly detection
- [x] Data correlation
- [ ] Common sense
- [x] Pattern identification
- [ ] Natural language
- [ ] Generalization

11. A robust cybersecurity defense includes contributions from 3 areas, human expertise, security analytics and artificial intelligence. Which of these areas would contain the ability for data visualization? **1 point**

- ( ) Artificial intelligence
- ( ) Human expertise
- (•) Security analytics

Coursera Honor Code Learn more

[x] I, **Giang Pham**, understand that submitting work that isn't my own may result in permanent failure of this course or deactivation of my Coursera account.

Submit Save draft