Formative assessment preparation

Part 1: 4 Network and System logs monitoring in accordance

1. **What is the primary purpose of log monitoring?**
   - A. Identifying security incidents
   - B. Ensuring compliance
   - C. Optimizing system performance
   - D. All of the above
   - **Answer: D. All of the above**
2. **Which of the following is included in network logs?**
   - A. Operating system logs
   - B. Firewall logs
   - C. Application server logs
   - D. Database logs
   - **Answer: B. Firewall logs**
3. **What is the role of a SIEM (Security Information and Event Management) system?**
   - A. To manage user accounts
   - B. To centralize and analyze log data
   - C. To backup data
   - D. To develop applications
   - **Answer: B. To centralize and analyze log data**
4. **What does PCI DSS require in terms of log retention?**
   - A. Logs must be retained for six months
   - B. Logs must be retained for one year
   - C. Logs must be retained indefinitely
   - D. Logs must be retained for five years
   - **Answer: B. Logs must be retained for one year**

5. **Which tool is known for its powerful search, monitoring, and analysis of machine-generated data?**
    - A. ELK Stack
    - B. Graylog
    - C. Splunk
    - D. IBM QRadar
    - **Answer: C. Splunk**
6. **What is the function of Logstash in the ELK Stack?**
    - A. Visualization
    - B. Data storage
    - C. Data processing pipeline
    - D. Machine learning
    - **Answer: C. Data processing pipeline**
7. **Which logging tool supports advanced features like log filtering, classification, and encryption?**
    - A. rsyslog
    - B. Fluentd
    - C. Syslog-ng
    - D. NXLog
    - **Answer: C. Syslog-ng**
8. **What type of activities does Sysmon log?**
    - A. User login attempts
    - B. Network configurations
    - C. System activities such as process creations and network connections
    - D. Software installations
    - **Answer: C. System activities such as process creations and network connections**

9. **What is the first step in the log monitoring workflow?**
   - A. Data aggregation
   - B. Data collection
   - C. Real-time analysis
   - D. Alerting
   - **Answer: B. Data collection**
10. **What does UEBA stand for in log monitoring?**
    - A. User and Event Behavior Analytics
    - B. User and Entity Behavior Analytics
    - C. User and Endpoint Behavior Analytics
    - D. User and External Behavior Analytics
    - **Answer: B. User and Entity Behavior Analytics**
11. **Which of the following is a critical component of centralized logging?**
    - A. Individual log files on each server
    - B. A unified logging solution
    - C. Manual log analysis
    - D. Decentralized log storage
    - **Answer: B. A unified logging solution**
12. **What is an important aspect of log normalization?**
    - A. Compressing log data
    - B. Converting logs into a consistent format
    - C. Deleting old logs
    - D. Distributing logs across multiple servers
    - **Answer: B. Converting logs into a consistent format**

13. **Which tool is specifically known for endpoint log collection and processing?**
    - A. Fluentd
    - B. NXLog
    - C. Logstash
    - D. Splunk
    - **Answer: B. NXLog**
14. **What should be included in a detailed report after a security scan?**
    - A. Only the executive summary
    - B. Only detailed findings
    - C. Executive summary, detailed findings, and remediation plan
    - D. Only remediation plan
    - **Answer: C. Executive summary, detailed findings, and remediation plan**
15. **Which cybersecurity principle ensures that users operate with the minimum privileges necessary?**
    - A. Defense in Depth
    - B. Least Privilege
    - C. Regular Updates and Patching
    - D. User Awareness and Training
    - **Answer: B. Least Privilege**
16. **What is the purpose of log retention policies?**
    - A. To delete logs as soon as possible
    - B. To define how long logs should be kept based on regulatory and business needs
    - C. To ensure logs are available to all users
    - D. To prevent logs from being generated
    - **Answer: B. To define how long logs should be kept based on regulatory and business needs**

17. **What type of logs should be included from critical applications?**

- A. Network logs
- B. Application logs
- C. System logs
- D. Security tools logs
- **Answer: B. Application logs**

18. **What should be done to ensure secure log storage?**

- A. Storing logs in plain text files
- B. Using encryption and access controls
- C. Allowing all users access to log data
- D. Storing logs on local hard drives only
- **Answer: B. Using encryption and access controls**

19. **What is the purpose of real-time log analysis?**

- A. To archive old logs
- B. To detect anomalies and suspicious activities as they occur
- C. To back up logs
- D. To generate monthly reports
- **Answer: B. To detect anomalies and suspicious activities as they occur**

20. **What should be the focus of daily log reviews?**

- A. Identifying any unusual or suspicious activities
- B. Generating backups
- C. Updating log monitoring tools
- D. Deleting old logs
- **Answer: A. Identifying any unusual or suspicious activities**

21. **Which standard provides guidelines for log management?**

- A. ISO/IEC 27001
- B. NIST SP 800-92
- C. PCI DSS
- D. All of the above
- **Answer: D. All of the above**

22. **What type of alerts should be set up in log monitoring?**

- A. Alerts for all events
- B. Actionable alerts for critical events
- C. Alerts only for successful logins
- D. Alerts for file modifications only
- **Answer: B. Actionable alerts for critical events**

23. **Which log management tool is described as an open-source data collector?**

- A. Splunk
- B. Fluentd
- C. Graylog
- D. IBM QRadar
- **Answer: B. Fluentd**

24. **What is a key feature of IBM QRadar?**

- A. Simplified user interface
- B. Advanced analytics for threat detection
- C. Limited data sources
- D. Lack of real-time alerts
- **Answer: B. Advanced analytics for threat detection**

25. **Which principle involves using multiple layers of security controls?**

- A. Least Privilege
- B. Defense in Depth
- C. User Awareness and Training
- D. Continuous Monitoring
- **Answer: B. Defense in Depth**

26. **What is an example of a network logging tool?**

- A. Syslog-ng
- B. LogRhythm
- C. SolarWinds Log & Event Manager
- D. Splunk
- **Answer: C. SolarWinds Log & Event Manager**

27. **What is the main objective of vulnerability scanning?**

- A. Identifying open ports only
- B. Identifying potential security issues
- C. Creating user accounts
- D. Deleting old files
- **Answer: B. Identifying potential security issues**

28. **Which process should be used to validate the findings of automated tools?**

- A. Automated verification
- B. Manual verification
- C. Deletion of false positives
- D. Scheduling weekly backups
- **Answer: B. Manual verification**

29. **What is the benefit of user awareness and training in cybersecurity?**

    - A. Reduces the need for technical controls
    - B. Educates users on security best practices
    - C. Increases the number of security incidents
    - D. Makes systems less user-friendly
    - **Answer: B. Educates users on security best practices**

30. **Which tool provides real-time log analysis and correlation for network devices, systems, and applications?**

    - A. Sysmon
    - B. NXLog
    - C. SolarWinds Log & Event Manager
    - D. Fluentd
    - **Answer: C. SolarWinds Log & Event Manager**

Part 2: Monitoring Tools (IDS) & (SIEM) Selection in Line with Industry Best Practices

1. **What does IDS stand for in cybersecurity?**

    - A. Intrusion Detection System
    - B. Information Defense System
    - C. Internal Data Security
    - D. Internet Defense Service
    - **Answer: A. Intrusion Detection System**

2. **What does SIEM stand for?**

    - A. Security Information and Event Management
    - B. Security Incident and Event Monitoring
    - C. System Information and Event Management
    - D. System Incident and Event Monitoring
    - **Answer: A. Security Information and Event Management**

3. **Which method is used by IDS for detecting threats?**
    - A. Signature-based detection
    - B. Anomaly-based detection
    - C. Both A and B
    - D. None of the above
    - **Answer: C. Both A and B**
4. **Which deployment model does not belong to IDS?**
    - A. Network-based
    - B. Host-based
    - C. Cloud-based
    - D. User-based
    - **Answer: D. User-based**
5. **What is a critical feature to consider when selecting a SIEM solution?**
    - A. Incident detection and response workflows
    - B. Support for only one type of log source
    - C. Limited scalability
    - D. No integration with threat intelligence
    - **Answer: A. Incident detection and response workflows**
6. **Which of the following is a deployment option for SIEM?**
    - A. On-premises
    - B. Cloud-based
    - C. Hybrid
    - D. All of the above
    - **Answer: D. All of the above**

7. **What is the main purpose of compliance and reporting features in SIEM?**
    - A. To delete unnecessary logs
    - B. To align with regulatory requirements and support incident response
    - C. To limit log storage
    - D. To prevent log generation
    - **Answer: B. To align with regulatory requirements and support incident response**
8. **Which tool is known for collecting and analyzing log data from various sources like firewalls and endpoints?**
    - A. SIEM
    - B. IDS
    - C. Firewall
    - D. Antivirus
    - **Answer: A. SIEM**
9. **What does a SIEM system do with detected threats?**
    - A. Ignores them
    - B. Logs them only
    - C. Generates alerts for investigation
    - D. Deletes them immediately
    - **Answer: C. Generates alerts for investigation**
10. **What is a benefit of using automated responses in SIEM?**
    - A. Reduces human intervention time
    - B. Eliminates the need for security analysts
    - C. Increases manual workload
    - D. Slows down response times
    - **Answer: A. Reduces human intervention time**

11. **Which integration is important for enhancing SIEM functionality?**

    - A. Integration with threat intelligence feeds
    - B. Integration with social media
    - C. Integration with email marketing tools
    - D. Integration with office productivity software
    - **Answer: A. Integration with threat intelligence feeds**

12. **What does threat intelligence provide to SIEM systems?**

    - A. Indicators of compromise (IOCs)
    - B. Hardware specifications
    - C. User preferences
    - D. Marketing data
    - **Answer: A. Indicators of compromise (IOCs)**

13. **What is a playbook in the context of SIEM?**

    - A. A collection of video games
    - B. Step-by-step instructions for handling security incidents
    - C. A list of company policies
    - D. A software development guide
    - **Answer: B. Step-by-step instructions for handling security incidents**

14. **What is a benefit of incorporating threat intelligence into monitoring systems?**

    - A. Slower response times
    - B. Improved threat detection
    - C. Increased data redundancy
    - D. Lower detection accuracy
    - **Answer: B. Improved threat detection**

15. **Which monitoring technique involves analyzing anomalous behavior based on threat intelligence insights?**
    - A. Signature-based monitoring
    - B. Behavior-based monitoring
    - C. Manual monitoring
    - D. Static monitoring
    - **Answer: B. Behavior-based monitoring**
16. **What is a key advantage of using a distributed architecture in SIEM systems?**
    - A. Limited scalability
    - B. Efficient handling of large volumes of data
    - C. Centralized log storage
    - D. Reduced data redundancy
    - **Answer: B. Efficient handling of large volumes of data**
17. **What type of deployment model is hybrid in the context of IDS?**
    - A. Combination of on-premises and cloud-based
    - B. Network-based only
    - C. Host-based only
    - D. User-based only
    - **Answer: A. Combination of on-premises and cloud-based**
18. **Why is it important to integrate threat intelligence feeds with SIEM?**
    - A. To automate security tasks and improve response times
    - B. To increase manual workload
    - C. To reduce the number of alerts
    - D. To store data indefinitely
    - **Answer: A. To automate security tasks and improve response times**

19. **What is a tactical threat intelligence feed?**

- A. High-level threat actor insights
- B. Specific indicators of compromise (IOCs)
- C. Marketing data
- D. User preferences
- **Answer: B. Specific indicators of compromise (IOCs)**

20. **Which factor is NOT important for SIEM performance?**

- A. Handling large data volumes
- B. Distributed architecture
- C. Limited log sources
- D. Efficient data processing
- **Answer: C. Limited log sources**

21. **What should a comprehensive SIEM solution support?**

- A. Only firewall logs
- B. Diverse log sources including firewalls, endpoints, and applications
- C. Limited log storage
- D. Manual data entry
- **Answer: B. Diverse log sources including firewalls, endpoints, and applications**

22. **How do playbooks improve incident response in SIEM systems?**

- A. By providing unstructured data
- B. By automating response actions based on predefined steps
- C. By increasing manual investigation time
- D. By reducing alert accuracy
- **Answer: B. By automating response actions based on predefined steps**

23. **What does the term 'real-time monitoring' in IDS refer to?**

- A. Analyzing historical data only
- B. Monitoring and analyzing events as they occur
- C. Periodic data snapshots
- D. Ignoring current data
- **Answer: B. Monitoring and analyzing events as they occur**

24. **Which IDS type focuses on monitoring individual hosts or devices?**

- A. Network-based IDS
- B. Host-based IDS
- C. Cloud-based IDS
- D. Hybrid IDS
- **Answer: B. Host-based IDS**

25. **What is an example of a compliance regulation that IDS and SIEM help meet?**

- A. GDPR
- B. HIPAA
- C. PCI DSS
- D. All of the above
- **Answer: D. All of the above**

26. **Which of the following is a methodical approach to threat hunting?**

- A. Define objectives and scope
- B. Random log analysis
- C. Ignoring threat intelligence
- D. Arbitrary data collection
- **Answer: A. Define objectives and scope**

27. **What is a key component of incident detection in SIEM?**
    - A. Log collection
    - B. Hardware specifications
    - C. User preferences
    - D. Marketing data
    - **Answer: A. Log collection**
28. **Why is scalability important for SIEM systems?**
    - A. To handle increasing volumes of security data
    - B. To reduce storage capacity
    - C. To limit log sources
    - D. To minimize system updates
    - **Answer: A. To handle increasing volumes of security data**
29. **Which factor is crucial for effective IDS deployment?**
    - A. Real-time monitoring capabilities
    - B. Manual data entry
    - C. Limiting log storage
    - D. Reducing detection methods
    - **Answer: A. Real-time monitoring capabilities**
30. **How does integrating threat intelligence with monitoring systems benefit an organization?**
    - A. By automating threat detection and response
    - B. By reducing the accuracy of detections
    - C. By limiting log sources
    - D. By increasing manual workload
    - **Answer: A. By automating threat detection and response**

<<>> The end <<>>