**Q&A**

1.Are the logs accurate, timely and contextual data?

1. **True**
2. False

2.Does Logging as a term means management of logs?

**a. True**

b. False

3.Log management Log management is the collective processes and policies used to

a. Administer and facilitate the generation

b.Transmission

c.Analysis

d.Storage

e.Archiving

f.Disposal of the large volumes of log data

**g.All of the above**

4.What logs provide and what can we identify by that?

A: They provide a metric that can be used to identify any issue that could cause problems in a system.

5.What logs can be as an action preformed on the web service?

**a. A user’s connection to the platform**

**b. An HTTP error generation**

**c. An access to a resource on the server**

d. None of the above

6.Whith what we contexualize events(log enrichment)

**a. IP address that generated the logs**

**b. User concerned**

**c. Error detail**

d. None of the above

7.Structured logs are?

**a. Actionable**

b. Unactionable

8.What are the levels of severity of logs?

**a. Debug**

**b. Info**

**c. Warning**

**d. Error**

**e.Critical**

f. There are no levels of severity of logs

9.As a critical event weaponization means?

A: An intrusion within your environment where adversaries have decided to take action against your network and IT systems.

10.What is the difference between Logging and Monitoring?

A: Monitoring helps you manage application performance and Logging is all about managing the data inside logs.

11.What is monitoring?

A: Monitoring provides feedback from production and delivers information about an application’s performance and usage patterns.

12.What functionalities should a Monitoring tool provide?

a. Dashboards

b. Diagnostics

c. Data Collector

d. Data Retention

e. Notifications

f. Reports

g. REST API

h. Machine Learning

**i. All of the above**

13.What types of monitoring exist?

**a. Infrastructure Monitoring**

**b. Application Monitoring**

**c. Network Monitoring**

14.What should monitoring tools measure?

**a. Availability**

**b. CPU usage**

**c. Disk usage**

**d. Uptime**

**e. Response time**

**f. Databases**

g. None of the above

15.What are popular monitoring tools?

a. Prometheus

b. Nagios

c. Sensu

d. Monit

e. Collectl

**f. All of the above**

16.What is Prometheus?

A: Prometheus is an open-source monitoring solution, built primarily for gathering and analyzing time-series data. It uses SNMP to collect performance data from devices across the network.

17.What is Grafana?

A: Grafana is an open-source analytics and monitoring solution that effectively queries, visualizes, and processes the metrics collected from Prometheus.