1. Which two types of availability monitoring of assets are provided through the USM Appliance web interface? (Choose 2)
   A. Host Monitoring
   B. Process Monitoring
   C. Interface Monitoring
   D. Services Monitoring

2. What is the definition of Event Type ID?
   A. A unique number that indicates the relative priority of a data source
   B. A unique number that identifies a data source that generates events
   C. A human-readable descriptor of the data source that is generating events
   D. A unique number that identifies different events that a data source is able to generate

3. Which Linux command could be used to filter for error messages in the agent log file?
   A. ls
   B. scp
   C. ntop
   D. grep

4. Where can you set up default forwarding of alarms to a different USM Appliance in the web interface?
   A. Assets
   B. Deployment
   C. Administration
   D. Threat Intelligence

5. Which two methods can be used to prevent events received by the sensor from being sent to the server? (Choose 2)
   A. ossim-db
   B. plugin regex
   C. rsyslog rules
   D. ossim-server rules

6. You have to modify a plugin to add some new signatures that match a known signature ID. Which agent plugin function would be used in this situation?
   A. Resolv
   B. Convert
   C. Sanitize
   D. Translate

7. Which data collection method only requires inbound connections to AlienVault?
   A. SDEE
   B. syslog
   C. logrotate
   D. OPSEC LEA

8. Which two benefits are gained when Network flow data is being collected from multiple sources? (Choose 2)
   A. Traffic mapping to Risk Maps
   B. Compare network flow sources
   C. Additional granularity for query options
   D. NetFlow Graphs become available per source