Exam Code: 2B0-102

Exam Name: Enterasys Security Systems Engineer-Defense.

Vendor: Enterasys Networks

Version: DEMO

Part: A

1: Which of the following Dragon Agents sends notifications when the sensors detect an event that match a rule?
A.Real Time Console
B.MD5 Sum
C.Alarm Tool
D.Database
Correct Answers: C

2: Which of the following techniques is not a viable way for a Device Support Module (DSM) to receive event data?
A.OPSEC
B.SSH
C.SYSLOG
D.SNMP V3 Inform
Correct Answers: B

3: Dynamic Collection controls
A.The number of packets to analyze
B.The number of times to execute the signature in a flow
C.The number of follow on packets to capture for forensics
D.The number of bytes to search for a match
Correct Answers: C

4: Network policies and signatures are associated with the?
A.Managed node
B.Network sensor
C.Virtual sensor
D.Agent
Correct Answers: C

5: Traffic direction refers to traffic flows in relation to the
A.Server
B.Protected network
C.Client
D.DMZ
Correct Answers: B

6: The virtual sensor name?
A.Must match the license name
B.Is included in all events reported by the virtual sensor
C.Must include the node name
D.Applies only to the device view

Correct Answers: B

7: In a signature the service direction refers to
A.Ports
B.Networks
C.VLANS
D.Protocols
Correct Answers: A

8: When using the Report Wizard within the Dragon Security Command Console all but one of the following formats can be chosen for output?
A.HTML
B.DOC
C.RTF
D.PDF
Correct Answers: B

9: The net-config-client.xml file is associated with?
A.The Enterprise Management Server (EMS)
B.Managed node client
C.Enterprise Management Server (EMS) Management Client
D.Reporting server
Correct Answers: B

10: The license key file for Dragon Security Command Console must be?
A.pulled automatically from the Dragon EMS Server in the /usr/dragon/policymgr/keys directory
B.manually copied to each of the remote Behavioral Flow Sensors before flows are collected
C.must be carefully entered into the license field of the Dragon Administration Console because it is tied to the hostname of the server and may have an extra carriage return at the end of the file
D.None of the above
Correct Answers: D

11: In a standalone deployment the system will have?
A.A net-config-client.xml file
B.A net-config-server.xml file
C.A net-config-server.xml and a net-con fig-client.xml file
D.A net-config-server.xml, a net-con fig-client.xml and a net-config-reports.xml file
Correct Answers: C

12: Narrowing the timeframe displayed in any Network Surveillance graph can be accomplished by?
A.selecting an alternative value of time (measured in minutes) within the Select Time field positioned just below the right hand side of each network graph
B.altering the time displayed in the WEB Browsers URL field for the particular network graph

being displayed

C.placing the mouse cursor on the lower portion of the network graph at the center of a new window in time and then performing a single left click

D.Both A and C

Correct Answers: D

13: Which of the following is NOT a possible response to a rule match within the Custom Rule Editor?

A.Set the severity, credibility, and relevance of the event to a desired value

B.Save the event as a building block

C.Ensure the detected event is part of an offense

D.Dispatch a new event

Correct Answers: B

14: The host sensor name

A.Must match the license key

B.Is for display purposes only

C.Is included in events generated by the sensor

D.Must include the managed node name

Correct Answers: C

15: Dpmmwctl controls what?

A.Remote sensor processes

B.The connections that make up the configuration channel

C.The connections that make up the Event channel

D.Database updates

Correct Answers: B

16: Virtual sensor names?

A.Are included in events they generate

B.Must match the sensor key

C.Must include the device name

D.Require separate keys

Correct Answers: A

17: A Bare Bones Event Flow Processor (EFP) has?

A.Only event channels

B.Event channels and agents

C.Only Agents and Sensors

D.Event channels and sensors

Correct Answers: A

18: A networks sensor can have ______ virtual sensors?

A.1

B.2
C.3
D.4
Correct Answers: D

19: The Windows host sensor key
A.Is added to the /usr/keys directory
B.Is pushed from the Enterprise Management Server (EMS) when the managed node is deployed
C.Is installed manually on the Windows system
D.Is pushed from the Enterprise Management Server (EMS) when the sensor is deployed
Correct Answers: C

20: Signature OS
A.Applies signature to network traffic originating from the specified OS
B.Is used for writing Host signatures
C.Applies signature to network traffic destined for from the specified OS
D.Applies signature to network traffic between hosts running the specified OS
Correct Answers: B