Enterasys

2B0-018

ES Dragon IDS

Answer: C

QUESTION: 45
Which Dragon analysis and reporting tool is recommended as the first tool to use for quickly viewing recent event data?

A. Dragon Forensics Console
B. Dragon Executive Level Reporting
C. Dragon Trending Console
D. Dragon RealTime Console

Answer: D

QUESTION: 46
By default, the Alarmtool application reads event data from what source?

A. dragon.db
B. Ring Buffer
C. driders.cfg
D. SNMP E. SMTP

Answer: B

QUESTION: 47
Which analysis tool allows for the reconstruction of the TCP or UDP datagrams associated with a specified event?

A. sum_event
B. mkalarm
C. mklog
D. mktime
E. mksession

Answer: E

QUESTION: 48
Which of the following Dragon analysis and reporting tools allows for event correlation over more than one day?

A. CLI Analysis Tools
B. Forensics Console
C. Alarmtool
D. Executive Level Reporting

Answer: D

QUESTION: 49
The Dragon CLI Analysis Tools analyze events:

A. for a user-defined date range
B. for a single dragon.db file
C. for Dragon Host Sensors only
D. for Dragon Network Sensors only

Answer: B

QUESTION: 50
Which of the following is NOT configurable through Alarmtool?

A. SNMP trap notification
B. SMTP emailing
C. Invoking commands with arguments based on parameters of the IDS event
D. Syslog notification
E. RMON notification

Answer: E