B. Contain the intrusion.
C. Determine to what extent systems and data are compromised.
D. Communicate with relevant parties.

**Correct Answer: B**

**QUESTION 534**
After an intrusion has been contained and the compromised systems having been reinstalled, which of the following need not be reviewed before bringing the systems back to service?

A. Access control lists
B. System services and their configuration
C. Audit trails
D. User accounts

**Correct Answer: C**

**QUESTION 535**
Which of the following includes notifying the appropriate parties to take action in order to determine the extent of the severity of an incident and to remediate the incident's effects?

A. Intrusion Evaluation (IE) and Response
B. Intrusion Recognition (IR) and Response
C. Intrusion Protection (IP) and Response
D. Intrusion Detection (ID) and Response

**Correct Answer: D**

**QUESTION 536**
Which of the following is used to monitor network traffic or to monitor host audit logs in order to determine violations of security policy that have taken place?

A. Intrusion Detection System
B. Compliance Validation System
C. Intrusion Management System
D. Compliance Monitoring System

**Correct Answer: A**

**QUESTION 537**
Which of the following is not a technique used for monitoring?

A. Penetration testing
B. Intrusion detection
C. Violation processing (using clipping levels)
D. Countermeasures testing

**Correct Answer: D**

**QUESTION 538**
Which one of the following is NOT a characteristic of an Intrusion Detection System? (IDS)

A. Determines the source of incoming packets.
B. Detects intruders attempting unauthorized activities.
C. Recognizes and report alterations to data files.
D. Alerts to known intrusion patterns.

**Correct Answer: C**

**QUESTION 539**
An IDS detects an attack using which of the following?

A. an event-based ID or a statistical anomaly-based ID
B. a discrete anomaly-based ID or a signature-based ID
C. a signature-based ID or a statistical anomaly-based ID
D. a signature-based ID or an event-based ID

**Correct Answer: C**

**QUESTION 540**
Which of the following monitor's network traffic in real time?

A. network-based IDS
B. host-based IDS
C. application-based IDS
D. firewall-based IDS

**Correct Answer: A**

**QUESTION 541**
What technology is being used to detect anomalies?

A. IDS
B. FRR
C. Sniffing
D. Capturing

**Correct Answer: A**

**QUESTION 542**
IDSs verify, itemize, and characterize threats from:

A. Inside your organization's network.
B. Outside your organization's network.
C. Outside and inside your organization's network.
D. The Internet.

**Correct Answer: C**

**QUESTION 543**
IDS can be described in terms of what fundamental functional components?

A. Response
B. Information Sources
C. Analysis
D. All of the choices

**Correct Answer: D**

**QUESTION 544**
What are the primary goals of intrusion detection systems? (Select all that apply.)

A. Accountability
B. Availability
C. Response
D. All of the choices

**Correct Answer: AC**

**QUESTION 545**
What is the most common way to classify IDSs?

A. Group them by information source.
B. Group them by network packets.
C. Group them by attackers.
D. Group them by signs of intrusion.

**Correct Answer: A**

**QUESTION 546**
The majority of commercial intrusion detection systems are:

A. Identity-based
B. Network-based
C. Host-based
D. Signature-based

**Correct Answer: B**

**QUESTION 547**
Which of the following is a drawback of Network-based IDSs?

A. It cannot analyze encrypted information.
B. It is very costly to setup.
C. It is very costly to manage.
D. It is not effective.

**Correct Answer: A**

**QUESTION 548**
Host-based IDSs normally utilize information from which of the following sources?

A. Operating system audit trails and system logs.
B. Operating system audit trails and network packets.
C. Network packets and system logs.
D. Operating system alarms and system logs.

**Correct Answer: A**

**QUESTION 549**

When comparing host based IDS with network based ID, which of the following is an obvious advantage?

A. It is unaffected by switched networks.
B. It cannot analyze encrypted information.
C. It is not costly to setup.
D. It is not costly to manage.

**Correct Answer: A**

**QUESTION 550**

You are comparing host based IDS with network based ID. Which of the following will you consider as an obvious disadvantage of host based IDS?

A. It cannot analyze encrypted information.
B. It is costly to remove.
C. It is affected by switched networks.
D. It is costly to manage.

**Correct Answer: D**

**QUESTION 551**

Which of the following IDS inflict a higher performance cost on the monitored systems?

A. Encryption based
B. Host based
C. Network based
D. Trusted based

**Correct Answer: B**

**QUESTION 552**

Application-based IDSs normally utilize information from which of the following sources?

A. Network packets and system logs.
B. Operating system audit trails and network packets.
C. Operating system audit trails and system logs.
D. Application's transaction log files.

**Correct Answer: D**