shall act in good faith, with the care an ordinarily prudent person in a like position would exercise under similar circumstances and in a manner he reasonably believes is in the best interest of the enterprise. The notion of profit would tend to go against the due care principle.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 10: Law, Investigation, and Ethics (page 186).

QUESTION 427
What ensures that the control mechanisms correctly implement the security policy for the entire life cycle of an information system?

A. Accountability controls
B. Mandatory access controls
C. Assurance procedures
D. Administrative controls

Correct Answer: C
Explanation:
Controls provide accountability for individuals accessing information. Assurance procedures ensure that access control mechanisms correctly implement the security policy for the entire life cycle of an information system.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

QUESTION 428
The viewing of recorded events after the fact using a closed-circuit TV camera is considered a

A. Preventative control.
B. Detective control
C. Compensating control
D. Corrective control

Correct Answer: B
Explanation:
Detective security controls are like a burglar alarm. They detect and report an unauthorized or undesired event (or an attempted undesired event). Detective security controls are invoked after the undesirable event has occurred. Example detective security controls are log monitoring and review, system audit, file integrity checkers, and motion detection.

Visual surveillance or recording devices such as closed circuit television are used in conjunction with guards in order to enhance their surveillance ability and to record events for future analysis or prosecution.

When events are monitored, it is considered preventative whereas recording of events is considered detective in nature.

Below you have explanations of other types of security controls from a nice guide produce by James Purcell (see reference below):

Preventive security controls are put into place to prevent intentional or unintentional disclosure, alteration, or destruction (D.A.D.) of sensitive information. Some example preventive controls follow:

Policy - Unauthorized network connections are prohibited.
Firewall - Blocks unauthorized network connections.
Locked wiring closet - Prevents unauthorized equipment from being physically plugged into a network switch.

Notice in the preceding examples that preventive controls crossed administrative, technical, and physical categories discussed previously. The same is true for any of the controls discussed in this section.

Corrective security controls are used to respond to and fix a security incident. Corrective security controls also limit or reduce further damage from an attack. Examples follow:

Procedure to clean a virus from an infected system
A guard checking and locking a door left unlocked by a careless employee Updating firewall rules to block an attacking IP address

Note that in many cases the corrective security control is triggered by a detective security control. Recovery security controls are those controls that put a system back into production after an incident. Most Disaster Recovery activities fall into this category. For example, after a disk failure, data is restored from a backup tape.

Directive security controls are the equivalent of administrative controls. Directive controls direct that some action be taken to protect sensitive organizational information. The directive can be in the form of a policy, procedure, or guideline.

Deterrent security controls are controls that discourage security violations. For instance, "Unauthorized Access Prohibited" signage may deter a trespasser from entering an area. The presence of security cameras might deter an employee from stealing equipment. A policy that states access to servers is monitored could deter unauthorized access.

Compensating security controls are controls that provide an alternative to normal controls that cannot be used for some reason. For instance, a certain server cannot have antivirus software installed because it interferes with a critical application. A compensating control would be to increase monitoring of that server or isolate that server on its own network segment.

Note that there is a third popular taxonomy developed by NIST and described in NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems." NIST categorizes security controls into 3 classes and then further categorizes the controls within the classes into 17 families. Within each security control family are dozens of specific controls. The NIST taxonomy is not covered on the CISSP exam but is one the CISSP should be aware of if you are employed within the US federal workforce.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical security (page 340).
CISSP Study Guide By Eric Conrad, Seth Misenar, Joshua Feldman, page 50-52
Security Control Types and Operational Security, James E.Purcell, http://www.giac.org/cissp-papers/207.pdf

QUESTION 429

Which of the following usually provides reliable, real-time information without consuming network or host resources?

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

Correct Answer: A
Explanation:
A network-based IDS usually provides reliable, real-time information without consuming network or host resources.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

QUESTION 430
Which of the following are the two MOST common implementations of Intrusion Detection Systems?

A. Server-based and Host-based.
B. Network-based and Guest-based.
C. Network-based and Client-based.
D. Network-based and Host-based.

Correct Answer: D
Explanation:
The two most common implementations of Intrusion Detection are Network- based and Host-based.

IDS can be implemented as a network device, such as a router, switch, firewall, or dedicated device monitoring traffic, typically referred to as network IDS (NIDS).

The" (IDS) "technology can also be incorporated into a host system (HIDS) to monitor a single system for undesirable activities. "

A network intrusion detection system (NIDS) is a network device .... that monitors traffic traversing the network segment for which it is integrated." Remember that NIDS are usually passive in nature.

HIDS is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3649-3652). Auerbach Publications. Kindle Edition.

QUESTION 431

Attributes that characterize an attack are stored for reference using which of the following Intrusion Detection System (IDS) ?

A. signature-based IDS
B. statistical anomaly-based IDS
C. event-based IDS
D. inferent-based IDS

Correct Answer: A
Explanation:
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

QUESTION 432
In what way can violation clipping levels assist in violation tracking and analysis?

A. Clipping levels set a baseline for acceptable normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred.
B. Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant.
C. Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status.
D. Clipping levels enable a security administrator to view all reductions in security levels which have been made to user accounts which have incurred violations.

Correct Answer: A
Explanation:
Companies can set predefined thresholds for the number of certain types of errors that will be allowed before the activity is considered suspicious. The threshold is a baseline for violation activities that may be normal for a user to commit before alarms are raised. This baseline is referred to as a clipping level.

The following are incorrect answers:
Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant. This is not the best answer, you would not record ONLY security relevant violations, all violations would be recorded as well as all actions performed by authorized users which may not trigger a violation. This could allow you to indentify abnormal activities or fraud after the fact.

Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to user accounts with a privileged status. It could record all security violations whether the user is a normal user or a privileged user.

Clipping levels enable a security administrator to view all reductions in security levels which have been made to user accounts which have incurred violations. The keyword "ALL" makes this question wrong. It may detect SOME but not all of violations. For example, application level attacks may not be detected.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1239). McGraw- Hill. Kindle Edition.
And TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
QUESTION 433

Which of the following is NOT a characteristic of a host-based intrusion detection system?

A. A HIDS does not consume large amounts of system resources
B. A HIDS can analyse system logs, processes and resources
C. A HIDS looks for unauthorized changes to the system
D. A HIDS can notify system administrators when unusual events are identified

Correct Answer: A
Explanation:
A HIDS does not consume large amounts of system resources is the correct choice. HIDS can consume inordinate amounts of CPU and system resources in order to function effectively, especially during an event.

All the other answers are characteristics of HIDSes

A HIDS can:

scrutinize event logs, critical system files, and other auditable system resources; look for unauthorized change or suspicious patterns of behavior or activity can send alerts when unusual events are discovered

Reference:
Official guide to the CISSP CBK. Pages 197 to 198.

QUESTION 434
Knowledge-based Intrusion Detection Systems (IDS) are more common than:

A. Network-based IDS
B. Host-based IDS
C. Behavior-based IDS
D. Application-Based IDS

Correct Answer: C
Explanation:
Knowledge-based IDS are more common than behavior-based ID systems.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 63.

Application-Based IDS - "a subset of HIDS that analyze what's going on in an application using the transaction log files of the application." Source: Official ISC2 CISSP CBK Review Seminar Student Manual Version 7.0 p. 87

Host-Based IDS - "an implementation of IDS capabilities at the host level. Its most significant difference from NIDS is intrusion detection analysis, and related processes are limited to the boundaries of the host." Source: Official ISC2 Guide to the CISSP CBK - p.197

Network-Based IDS - "a network device, or dedicated system attached to the network, that monitors traffic traversing the network segment for which it is integrated." Source: Official ISC2 Guide to the CISSP CBK - p. 196

CISSP for dummies a book that we recommend for a quick overview of the 10 domains has nice and concise coverage of the subject:
Intrusion detection is defined as real-time monitoring and analysis of network activity and data for