ST0-095

Symantec Technical Foundations: Security Solutions 1.0 (STS)

Version 4.1

ST0-095

Topic 1, Volume A

QUESTION NO: 1

Which statement reflects a risk-based security program?

A. We are in the process of identifying the effectiveness of the security in our PCI environment.

B. We are in the process of identifying the business impact related to our PCI environment.

C. We are in the process of identifying the appropriate controls related to our PCI environment.

D. We are in the process of identifying the systems impacted by PCI regulations.

Answer: B

QUESTION NO: 2

How can a security professional within an organization become viewed as a business partner to an executive?

A. by speaking to security roles and processes

B. by articulating risk in terms of financial value

C. by speaking to the fundamentals of security

D. by ensuring that compliance is the top priority

Answer: B

QUESTION NO: 3

What drives consultative conversations and establishes credibility with an organization?

A. establishing a security policy

B. providing industry insight

C. providing regulatory information

D. establishing technical controls

Answer: B

QUESTION NO: 4

What is one of the common security concerns among organizations today, according to the Global State of Information Security survey 2010?

A. quality of service

B. PCI compliance

C. data protection

D. asset management

Answer: C

QUESTION NO: 5

Which two process types form the basis for the development of a workflow solution? (Select two.)

A. production processes

B.security processes

C.business processes

D.monitoring processes

E.automation processes

Answer: C, E

QUESTION NO: 6

What is the benefit that a workflow solution provides for the security of an environment?

A. It allows the ability to react to security events in a timely and automated fashion.

B. It allows the ability to reduce the number of people being managed in an environment.

C. It allows the ability to hire more people to manage the automation of an environment.

D. It allows the ability to transform security data that can be acted on within an environment.

Answer: A

QUESTION NO: 7

What drives policies and procedures, according to the Security Solutions 1.0 course?

A. industry regulations and order

B. business goals and objectives

C. company security and awareness

D. business growth and efficiency

Answer: B

QUESTION NO: 8

How does a workflow solution work with collaborative applications?

A. It helps monitor system utilization between applications.

B. It streamlines tasks and connects independent business applications.

C. It helps monitor configuration changes between applications.

D. It streamlines tasks and applies configuration changes to each application.

Answer: B

QUESTION NO: 9

A customer is experiencing image-based spam and phishing attacks that are negatively impacting messaging flow. Which Symantec solution should be recommended to this customer?

A. Brightmail Gateway

B. Endpoint Protection

C. Network Access Control

D. Backup Exec System Recovery

Answer: A

QUESTION NO: 10

Which strategy is an appropriate means of defending against social engineering attacks?

A. endpoint security

B. security awareness

C. data loss prevention

D. web security

Answer: B

QUESTION NO: 11

Which information does an organization need to analyze in order to apply a risk-based approach to their security and compliance practices, according to the Security Solutions 1.0 course?

A. which hardware is most costly to replace

B. which data is being backed-up

C. which employees have remote access

D. which servers contain critical data

Answer: D

QUESTION NO: 12

Last year a company had an incident where several notebooks belonging to executives were stolen from their cars. These notebooks could have contained information that, if put into the wrong hands, would have presented a large risk. Which two solutions can reduce the risk associated with this scenario? (Select two.)

A.Data Loss Prevention

B.Endpoint Protection

C.Control Compliance Suite

D.Endpoint Encryption

E.Critical System Protection

Answer: A, D

QUESTION NO: 13

What does the Control Objectives for Information and Related Technology (CobiT) framework focus on, according to the Security Solutions 1.0 course?

A. IT implementation lifecycle

B. computer security concepts

C. international security procedures for audit

D. confidentiality, integrity, and availability

Answer: A

QUESTION NO: 14

Which method did the MetaFisher bot use to extract data from a system?

A. RSS

B. FTP

C. peer to peer

D. IRC

Answer: B

QUESTION NO: 15

What are the three types of scans used to identify systems?

A. port, network, and vulnerability

B. protocol, hardware, and services

C. port, subnet, and client

D. hardware, vulnerability, and virus

Answer: A

QUESTION NO: 16

Which method would a cybercriminal most likely use in a drive-by download?

A. spam with an attachment

B. whaling with a link to click on

C. SQL injection

D. cross-site request forgery

Answer: D

QUESTION NO: 17

The security team of a major government agency discovers a breach involving employee data that has been leaked outside the agency. They discover that a software developer for the agency transferred employee data from a secure primary system to a secondary system, for the purpose of software development and testing. This secondary system was the target of a hacker. Which type of breach source(s) is this?

A. cybercriminal only

B. malicious insider and cybercriminal

C. cybercriminal and well-meaning insider

D. well-meaning insider only

Answer: C

QUESTION NO: 18

Which global trade does the United States Federal Bureau of Investigation (FBI) say is smaller than the global market for illegally-obtained information, according to the Security Solutions 1.0 course?

A. illegal drug trade

B. arms trafficking trade

C. human trafficking trade

D. money laundering trade

Answer: A

QUESTION NO: 19

Malware that contains a backdoor is placed on a system that will later be used by the cybercriminal to gain access to the system. The cybercriminal was successful in which phase of the breach?

A. capture

B. discovery

C. incursion

D. exfiltration

Answer: C

QUESTION NO: 20

According to the Symantec research shared in the Security Solutions 1.0 course, which group is the number one source of IT security attacks?

A. corporate competitors

B. organized criminals

C. well-meaning insiders

D. malicious insiders

Answer: B

QUESTION NO: 21

What is the leading root cause for successful malicious attacks?

A. improper system utilization

B. default system configurations

C. exposed network configurations

D. ineffective security software

Answer: B

QUESTION NO: 22

What is the goal of a denial of service attack?

A. to capture files from a remote system

B. to incapacitate a system or network

C. to exploit a weakness in the TCP/IP stack

D. to execute a trojan using the hidden shares