**Learning Tips for Chapter 12**

Chapter 12 considers the three innermost layers of defense in depth (DiD): endpoints, applications, and data.t

In older DiD depictions, the endpoint layer is called the host or platform layer. Today, it is usually called the endpoint layer. As noted throughout the book, there are many types of endpoints.

Malware is a common endpoint threat, but there are many types of malware. This provides the book’s most comprehensive overview of malware, and it is valuable for you to be aware of its major types, especially those that are most difficult to detect or combat.

Vulnerability assessment and management is a common aspect of endpoint security, and it is important for you to be aware of what it encompasses. It is also valuable for you to have a general understanding of how/why browser isolation, sandboxing, and application control contributes to endpoint security.

Endpoint security platforms that combine various security defenses, such as EPP, EDR, and XDR, warrant some attention, but it is more valuable to develop a general understanding of their differences than detailed knowledge of how they work.

The endpoint security best practices identified in this chapter deserve some attention, especially since they provide an overview of endpoint security defenses.

Because applications process and support network users, it is important to secure them, especially mission-critical systems such as enterprise systems (ESs). Businesses often classify/categorize applications on their security risks. Like other network assets, risk values and levels may be assigned to applications via processes like those described in Chapter 11. Whitelisting, blacklisting, and application controls are common in enterprise networks, and it is valuable for you to have a general understanding of each.

The performance and security of ESs and other mission-critical applications are prioritized in enterprise networks, and it is valuable for you to understand the major reasons why this happens.

Some ES products, including SAP products include specialized technologies to secure them. SAProuter, SAP Web Dispatcher, and Secure Network Communications (SNC) are examples of specialized security technologies for SAP products.

ESs often use a combination of RBAC and ABAC to protect their integrity and use. This, and their use in zero trust architectures make it important for you to understand the major characteristics of RBAC and ABAC.

Secure coding practices and best practices can decrease application vulnerabilities and increase their immunity to cybersecurity attacks. Hence, it is valuable for you to be aware of what they include.

When considering data security, you are encouraged to review Chapter 2’s description and discussion of sensitive data before diving into the various types of data threats and attacks.

It is important to recognize data exfiltration as a type of data theft and to understand how it differs from both data modification and data destruction attacks. It is also valuable for you to have a general understanding of data in use (DIU) threats and defenses.

A wide range of data at rest (DAR) security controls are identified and briefly described in this chapter and it is valuable for you to have a general understanding of these, especially database access controls.

It is also valuable for you to have a general understanding of data masking, column-based encryption, and hashing as data security controls.

Do not ignore the Key Concepts in Chapter 12 Presentation.

You are also encouraged to leverage the supplement videos and readings for this chapter.

Use the Chapter 12 Problems and Exercises tips to assist with any problems and exercises that you may be assigned.

**Especially Important Sections**

Section 12.0

Section 12.1.1 and each of its subsections

Section 12.1.2 and each of its subsections

Section 12.1.3

Section 12.2.2

Section 12.2.4 and each of its subsections

Section 12.2.5

Section 12.3.1 and each of its subsections

Section 12.3.2 and each of its subsections

**Especially Important Figures and Tables**

*Note:* It is important to read/study the discussion related to each figure and table that is identified.

Figure 12-1

Figure 12-3 and Table 12-1

Table 12-2

Figure 12-5

Table 12-3

Figure 12-7

Table 12-4

Tables 12-5 and 12-6

Table 12-7

Figures 12-14 and 12-15

Figures 12-16 and 12-17

Table 12-8

Figure 12-18

Tables 12-11 and 12-12

Tables 12-13, 12-14, and 12-15

Figure 12-19

Figures 12-20, 12-21, and 12-22

**Especially Important Key Terms**

Attribute-based access control (ABAC)

Column-based encryption

Database access control

Data destruction attack

Data exfiltration

Data masking

Data medication attack

Data redaction

Endpoint detection and response (EDR)

Endpoint protection platform (EPP)

Extended detection and response (XDR)

Fileless malware

Hashing

Host-based IDS (HIDS)

Role-based access control (RBAC)

Sandboxing

Zero-day vulnerability

**Especially Important Review Questions**

Questions 3-5, 7-16, 18-23, 25-27, 29, 30

**Especially Valuable Problems and Exercises**

Exercises 12-3, 12-4