PEARSON IT CERTIFICATION

Save 10% on Exam Voucher
See Inside

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

CompTIA®

Cybersecurity Analyst (CySA+)

CS0-002

TROY McMILLAN

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

CompTIA Cybersecurity Analyst (CySA+) CS0-002 Cert Guide

Troy McMillan

CompTIA Cybersecurity Analyst (CySA+) CS0-002 Cert Guide

ISBN-13: 978-0-13-674716-1

ISBN-10: 0-13-674716-7

Library of Congress Control Number: 2020941742

ScoutAutomatedPrintCode

Editor-in-Chief
Mark Taub

Product Line Manager
Brett Bartow

Executive Editor
Nancy Davis

Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Bill McManus

Indexer
Erika Millen

Proofreader
Abigail Manheim

Technical Editor
Chris Crayton

Editorial Assistant
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Contents at a Glance

Table of Contents

Online Elements:

About the Author

Troy McMillan is a product developer and technical editor for Kaplan IT as well as a full-time trainer. He became a professional trainer 20 years ago, teaching Cisco, Microsoft, CompTIA, and wireless classes. He has written or contributed to more than a dozen projects, including the following recent ones:

- Contributing subject matter expert for *CCNA Cisco Certified Network Associate Certification Exam Preparation Guide* (Kaplan)
- Author of *CISSP Cert Guide* (Pearson)
- Prep test question writer for *CCNA Wireless 640-722 Official Cert Guide* (Cisco Press)
- Author of *CompTIA Advanced Security Practitioner (CASP) Cert Guide* (Pearson)

Troy has also appeared in the following training videos for OnCourse Learning: Security+; Network+; Microsoft 70-410, 411, and 412 exam prep; ICND1; and ICND2.

He delivers CISSP training classes for CyberVista, and is an authorized online training provider for (ISC)2.

Troy also creates certification practice tests and study guides for CyberVista. He lives in Asheville, North Carolina, with his wife, Heike.

Dedication

I dedicate this book to my wife, Heike, who has supported me when I needed it most.

Acknowledgments

I must thank everyone on the Pearson team for all of their help in making this book better than it would have been without their help. That includes Chris Cleveland, Nancy Davis, Chris Crayton, Tonya Simpson, and Mudita Sonar.

About the Technical Reviewer

Chris Crayton (MCSE) is an author, technical consultant, and trainer. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional teaching awards, and has served as a state-level SkillsUSA competition judge.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Introduction

CompTIA CySA+ bridges the skills gap between CompTIA Security+ and CompTIA Advanced Security Practitioner (CASP+). Building on CySA+, IT professionals can pursue CASP+ to prove their mastery of the hands-on cybersecurity skills required at the 5- to 10-year experience level. Earn the CySA+ certification to grow your career within the CompTIA recommended cybersecurity career pathway.

CompTIA CySA+ certification is designed to be a "vendor-neutral" exam that measures your knowledge of industry-standard technology.

Goals and Methods

The number-one goal of this book is a simple one: to help you pass the 2020 version of the CompTIA CySA+ certification exam, CS0-002.

Because the CompTIA CySA+ certification exam stresses problem-solving abilities and reasoning more than memorization of terms and facts, this book is designed to help you master and understand the required objectives for each exam.

To aid you in mastering and understanding the CySA+ certification objectives, this book uses the following methods:

- The beginning of each chapter identifies the CompTIA CySA+ objective addressed in the chapter and defines the related topics covered in the chapter.
- The body of the chapter explains the topics from a hands-on and theory-based standpoint. This includes in-depth descriptions, tables, and figures that are geared toward building your knowledge so that you can pass the exam. The structure of each chapter generally follows the outline of the corresponding exam objective, which not only enables you to study the exam objectives methodically but also enables you to easily locate coverage of specific exam objectives that you think you need to review further.
- Key Topic icons identify important figures, tables, and lists of information that you should know for the exam. Key topics are interspersed throughout the chapter and are listed in a table at the end of the chapter.
- Key terms in each chapter are emphasized in ***bold italic*** and are listed without definitions at the end of each chapter. Write down the definition of each term and check your work against the complete key terms in the glossary.

Strategies for Exam Preparation

Strategies for exam preparation vary depending on your existing skills, knowledge, and equipment available. Of course, the ideal exam preparation would consist of three or four years of hands-on security or related experience followed by rigorous study of the exam objectives.

Before and after you have read through the book, have a look at the current exam objectives for the CompTIA CySA+ Certification Exam, listed at https://www.comptia.org/certifications/cybersecurity-analyst#examdetails. If there are any areas shown in the certification exam outline that you would still like to study, find those sections in the book and review them.

When you feel confident in your skills, attempt the practice exams found on the website that accompanies this book. As you work through the practice exams, note the areas where you lack confidence and review those concepts or configurations in the book. After you have reviewed those areas, work through the practice exams a second time and rate your skills. Keep in mind that the more you work through the practice exams, the more familiar the questions will become.

After you have worked through the practice exams a second time and feel confident in your skills, schedule the CompTIA CySA+ CS0-002 exam through Pearson Vue (https://home.pearsonvue.com). To prevent the information from evaporating out of your mind, you should typically take the exam within a week of when you consider yourself ready to take it.

The CompTIA CySA+ certification credential for those passing the certification exams is now valid for three years. To renew your certification without retaking the exam, you need to participate in continuing education (CE) activities and pay an annual maintenance fee of $50 (that is, $150 for three years). See https://www.comptia.org/continuing-education/learn/ce-program-fees for fee details. To learn more about the certification renewal policy, see https://certification.comptia.org/continuing-education.

How the Book Is Organized

Table I-1 outlines where each of the CySA+ exam objectives is covered in the book. For a full dissection of what is covered in each objective, you should download the most recent set of objectives from https://www.comptia.org/certifications/cybersecurity-analyst#examdetails.

Table I-1 CySA+ CS0-002 Exam Objectives: Coverage by Chapter

Exam Objective	Chapter Where This Objective Is Covered
Domain 1.0 Threat and Vulnerability Management (accounts for 22% of the exam)	
1.1 Explain the importance of threat data and intelligence	Chapter 1
1.2 Given a scenario, utilize threat intelligence to support organizational security	Chapter 2
1.3 Given a scenario, perform vulnerability management activities	Chapter 3
1.4 Given a scenario, analyze the output from common vulnerability assessment tools	Chapter 4
1.5 Explain the threats and vulnerabilities associated with specialized technology	Chapter 5
1.6 Explain the threats and vulnerabilities associated with operating in the cloud	Chapter 6
1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities	Chapter 7
Domain 2.0 Software and Systems Security (accounts for 18% of the exam)	
2.1 Given a scenario, apply security solutions for infrastructure management	Chapter 8
2.2 Explain software assurance best practices	Chapter 9
2.3 Explain hardware assurance best practices	Chapter 10

Exam Objective	Chapter Where This Objective Is Covered
Domain 3.0 Security Operations and Monitoring (accounts for 25% of the exam)	
3.1 Given a scenario, analyze data as part of security monitoring activities	Chapter 11
3.2 Given a scenario, implement configuration changes to existing controls to improve security	Chapter 12
3.3 Explain the importance of proactive threat hunting	Chapter 13
3.4 Compare and contrast automation concepts and technologies	Chapter 14
Domain 4.0 Incident Response (accounts for 22% of the exam)	
4.1 Explain the importance of the incident response process	Chapter 15
4.2 Given a scenario, apply the appropriate incident response procedure	Chapter 16
4.3 Given an incident, analyze potential indicators of compromise	Chapter 17
4.4 Given a scenario, utilize basic digital forensics techniques	Chapter 18
Domain 5.0 Compliance and Assessment (accounts for 13% of the exam)	
5.1 Understand the importance of data privacy and protection	Chapter 19
5.2 Given a scenario, apply security concepts in support of organizational risk mitigation	Chapter 20
5.3 Explain the importance of frameworks, policies, procedures, and controls	Chapter 21

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **Foundation Topics:** These are the core sections of each chapter. They explain the concepts for the topics in that chapter.
- **Exam Preparation Tasks:** After the "Foundation Topics" section of each chapter, the "Exam Preparation Tasks" section provides the following study activities that you should do to prepare for the exam:
  - **Review All Key Topics:** As previously mentioned, the Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The Review All Key Topics activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.

- **Define Key Terms:** Although the CySA+ exam might be unlikely to ask a question such as "Define this term," the exam does require that you learn and know a lot of cybersecurity-related terminology. This section lists the most important terms from the chapter, asking you to write a short definition of each and compare your answer to the glossary entry at the end of the book.

- **Review Questions:** Confirm that you understand the content that you just covered by answering these questions and reading the answer explanations.
- **Web-based practice exam:** The companion website includes the Pearson Test Prep practice test software that enables you to take practice exam questions. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

What's New?

With every exam update, changes in the relative emphasis on certain topics can change. Here is an overview of some of the most important changes:

- Increased content on the importance of threat data and intelligence
- Increased emphasis on regulatory compliance
- Increased emphasis on the options and combinations available for any given command
- Increased emphasis on identifying attacks through log analysis
- Increased coverage of cloud security
- Increased coverage of forming and using queries

The Companion Website for Online Content Review

All the electronic review elements, as well as other electronic components of the book, exist on this book's companion website.

To access the companion website, which gives you access to the electronic content with this book, start by establishing a login at www.pearsonITcertification.com and register your book.

To do so, simply go to www.pearsonitcertification.com/register and enter the ISBN of the print book: 9780136747161. After you have registered your book, go to your account page and click the **Registered Products** tab. From there, click the **Access Bonus Content** link to get access to the book's companion website.

Note that if you buy the *Premium Edition eBook and Practice Test* version of this book from Pearson, your book will automatically be registered on your account page. Simply go to your account page, click the **Registered Products** tab, and select **Access Bonus Content** to access the book's companion website.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the steps at left, please visit www.pearsonITcertification.com/contact and select the **Site Problems/ Comments** option. Our customer service representatives will assist you.

How to Access the Pearson Test Prep Practice Test Software

You have two options for installing and using the Pearson Test Prep practice test software: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- **Print book:** Look in the cardboard sleeve in the back of the book for a piece of paper with your book's unique PTP code.
- **Premium Edition:** If you purchase the Premium Edition eBook and Practice Test directly from the www.pearsonITcertification.com website, the code will be populated on your account page after purchase. Just log in to www.pearsonITcertification.com, click **Account** to see details of your account, and click the **Digital Purchases** tab.
- **Amazon Kindle:** For those who purchase a Kindle edition from Amazon, the access code will be supplied directly from Amazon.
- **Other bookseller e-books:** Note that if you purchase an e-book version from any other source, the practice test is not included because other vendors to date have not chosen to vend the required unique access code.

NOTE Do not lose the activation code because it is the only means with which you can access the QA content with the book.

Once you have the access code, to find instructions about both the PTP web app and the desktop app, follow these steps:

Step 1. Open this book's companion website.

Step 2. Click the **Practice Exams** button.

Step 3. Follow the instructions listed there both for installing the desktop app and for using the web app.

Note that if you want to use the web app only at this point, just navigate to www.pearsontestprep.com, establish a free login if you do not already have one, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

NOTE Amazon eBook (Kindle) customers: It is easy to miss Amazon's e-mail that lists your PTP access code. Soon after you purchase the Kindle eBook, Amazon should send an e-mail. However, the e-mail uses very generic text, and makes no specific mention of PTP or practice exams. To find your code, read every e-mail from Amazon after you purchase the book. Also do the usual checks for ensuring your e-mail arrives, like checking your spam folder.

NOTE Other eBook customers: As of the time of publication, only the publisher and Amazon supply PTP access codes when you purchase their eBook editions of this book.

Customizing Your Exams

Once you are in the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** Enables you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all test banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software while connected to the Internet, it checks if there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software.

Sometimes, due to many factors, the exam data might not fully download when you activate your exam. If you find that figures or exhibits are missing, you might need to manually update your exams. To update a particular exam you have already activated and downloaded, simply click the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply click the **Tools** tab and click the **Update Application** button. This ensures that you are running the latest version of the software engine.

Credits

Cover image: New Africa/Shutterstock
Chapter opener image: Charlie Edwards/Photodisc/Getty Images
Figure 3-1 © Greenbone Networks GmbH
Figure 3-2 © Greenbone Networks GmbH
Figure 3-3 © 2020 Tenable, Inc
Figure 3-4 © 2020 Tenable, Inc
Figure 3-5 © 2020 Tenable, Inc
Figure 4-1 © Sarosys LLC 2010-2017
Figure 4-4 © Greenbone Networks GmbH
Figure 4-5 © Greenbone Networks GmbH

Quote, “the process of analyzing a subject system to identify the system’s components and their interrelationships, and to create representations of the system in another form or at a higher level of abstraction” © Institute of Electrical and Electronics Engineers (IEEE)

Figure 4-7 © Insecure.Com LLC

Figure 4-8 © Insecure.Com LLC

Figure 4-9 © Insecure.Com LLC

Figure 4-10 © Insecure.Com LLC

Figure 4-12 © 2020 KSEC

Figure 4-13 © 2009-2020 Aircrack-ng

Figure 4-14 © hashcat

Figure 4-15 © 2020 HACKING LAND

Figure 5-5 © U.S. Department of Health and Human Services

Figure 11-1 © 2020 Zoho Corp

Figure 11-5 © Microsoft 2020

Figure 11-8 © 2020 SolarWinds Worldwide, LLC

Figure 11-9 © Microsoft 2020

Figure 11-10 © 2020 SolarWinds Worldwide, LLC

Figure 11-11 © Microsoft 2020

Figure 11-13 © 2020 Cloudflare, Inc

Figure 11-14 © Microsoft 2020

Figure 11-15 © 2004-2018 Zentyal S.L.

Figure 11-17 © 1992-2020 Cisco

Figure 11-18 © 1992-2020 Cisco

Figure 11-19 © 2020 Apple Inc

Figure 11-20 © 2020 AT&T CYBERSECURITY

Figure 11-21 © 2005-2020 Splunk Inc.

Figure 13-3 © Microsoft 2020

Figure 13-4 © Microsoft 2020

Figure 17-1 © 2004-2020 Rob Dawson

Figure 17-4 © Microsoft 2020

Figure 17-5 © Microsoft 2020

Figure 18-1 © wireshark

Figure 18-2 © wireshark

Figure 18-3 © wireshark

Figure 18-4 © 2001-2014 Massimiliano Montoro

Figure 18-7 © Microsoft 2020

Figure 19-1 courtesy of Wikipedia

Threats and Vulnerabilities Associated with Operating in the Cloud

Placing resources in a cloud environment has many benefits, but also introduces a host of new security considerations. This chapter discusses these vulnerabilities and some measures that you can take to mitigate them.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read the entire chapter. If you miss no more than one of these eight self-assessment questions, you might want to skip ahead to the "Exam Preparation Tasks" section. Table 6-1 lists the major headings in this chapter and the "Do I Know This Already?" quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the "Do I Know This Already?" quiz appear in Appendix A.

Table 6-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Question
Cloud Deployment Models	1
Cloud Service Models	2
Function as a Service (FaaS)/Serverless Architecture	3
Infrastructure as Code (IaC)	4
Insecure Application Programming Interface (API)	5
Improper Key Management	6
Unprotected Storage	7
Logging and Monitoring	8

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. In which cloud deployment model does an organization provide and manage some resources in-house and has other resources provided externally via a public cloud?
   a. Private
   b. Public
   c. Community
   d. Hybrid

2. Which of the following cloud service models is typically used as a software development environment?
   a. SaaS
   b. PaaS
   c. IaaS
   d. FaaS

3. Which of the following is an extension of the PaaS model?
   a. FaaS
   b. IaC
   c. SaaS
   d. IaaS

4. Which of the following manages and provisions computer data centers through machine-readable definition files?
   a. IaC
   b. PaaS
   c. SaaS
   d. IaaS

5. Which of the following can enhance security of APIs?
   a. DPAPI
   b. SGX
   c. SOAP
   d. REST

6. Which of the following contains recommendations for key management?
   a. NIST SP 800-57 REV. 5
   b. PCI-DSS
   c. OWASP
   d. FIPS

7. Which of the following is the most exposed part of a cloud deployment?
   a. Cryptographic functions
   b. APIs
   c. VMs
   d. Containers

8. Which of the following is lost with improper auditing? (Choose the best answer.)
   a. Cryptographic security
   b. Accountability
   c. Data security
   d. Visibility

Foundation Topics

Cloud Deployment Models

Cloud computing is all the rage these days, and it comes in many forms. The basic idea of cloud computing is to make resources available in a web-based data center so the resources can be accessed from anywhere. When a company pays another company to host and manage this type of environment, it is considered to be a public cloud solution. If the company hosts this environment itself, it is considered to be a private cloud solution. The different cloud deployment models are as follows:

Key Topic

- **Public:** A ***public cloud*** is the standard cloud deployment model, in which a service provider makes resources available to the public over the Internet. Public cloud services may be free or may be offered on a pay-per-use model. An organization needs to have a business or technical liaison responsible for managing the vendor relationship but does not necessarily need a specialist in cloud deployment. Vendors of public cloud solutions include Amazon, IBM, Google, Microsoft, and many more. In a public cloud deployment model, subscribers can add and remove resources as needed, based on their subscription.
- **Private:** A ***private cloud*** is a cloud deployment model in which a private organization implements a cloud in its internal enterprise, and that cloud is used by the organization's employees and partners. Private cloud services require an organization to employ a specialist in cloud deployment to manage the private cloud.
- **Community:** A ***community cloud*** is a cloud deployment model in which the cloud infrastructure is shared among several organizations from a specific group with common computing needs. In this model, agreements should explicitly define the security controls that will be in place to protect the data of each organization involved in the community cloud and how the cloud will be administered and managed.
- **Hybrid:** A ***hybrid cloud*** is a cloud deployment model in which an organization provides and manages some resources in-house and has others provided externally via a public cloud. This model requires a relationship with the service provider as well as an in-house cloud deployment specialist. Rules need to be defined to ensure that a hybrid cloud is deployed properly. Confidential and private information should be limited to the private cloud.

Cloud Service Models

There is trade-off to consider when a decision must be made between cloud architectures. A private solution provides the most control over the safety of your data but also requires the staff and the knowledge to deploy, manage, and secure the solution. A public cloud puts your data's safety in the hands of a third party, but that party is more capable and knowledgeable about protecting data in such an environment and managing the cloud environment. With a public solution, various cloud service models can be purchased. Some of these models include the following:

Key Topic

- ***Software as a Service (SaaS)*:** With SaaS, the vendor provides the entire solution, including the operating system, the infrastructure software, and the application. The vendor may provide an email system, for example, in which it hosts and manages everything for the customer. An example of this is a company that contracts to use Salesforce or Intuit QuickBooks using a browser rather than installing the application on every machine. This frees the customer company from performing updates and other maintenance of the applications.
- ***Platform as a Service (PaaS)*:** With PaaS, the vendor provides the hardware platform or data center and the software running on the platform, including the operating systems and infrastructure software. The customer is still involved in managing the system. An example of this is a company that engages a third party to provide a development platform for internal developers to use for development and testing.
- ***Infrastructure as a Service (IaaS)*:** With IaaS, the vendor provides the hardware platform or data center, and the customer installs and manages its own operating systems and application systems. The vendor simply provides access to the data center and maintains that access. An example of this is a company hosting all its web servers with a third party that provides the infrastructure. With IaaS, customers can benefit from the dynamic allocation of additional resources in times of high activity, while those same resources are scaled back when not needed, which saves money.

Figure 6-1 illustrates the relationship of these services to one another.

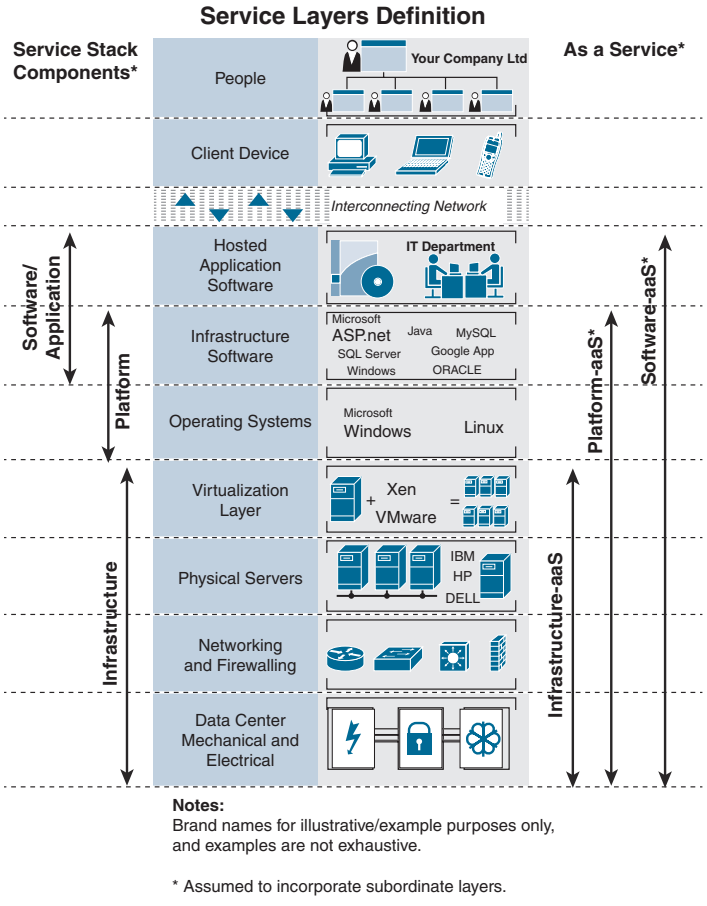

FIGURE 6-1 Cloud Service Models

Function as a Service (FaaS)/Serverless Architecture

Function as a Service (FaaS) is an extension of PaaS that goes further and completely abstracts the virtual server from the developers. In fact, charges are based not on server instance sizes but on consumption and executions. This is why it is sometimes also called *serverless architecture*. In this architecture, the focus is on a function, operation, or piece of code that is executed as a function. These services are event-driven in nature.

Although FaaS is not perfect for every workload, for transactions that happen hundreds of times per second, there is a lot of value in isolating that logic to a function that can be scaled. Additional advantages include the following:

Key Topic

- **Ideal for dynamic or burstable workloads:** If you run something only once a day or month, there's no need to pay for a server 24/7/365.
- **Ideal for scheduled tasks:** FaaS is a perfect way to run a certain piece of code on a schedule.

Figure 6-2 shows a useful car analogy for comparing traditional computing (own a car), cloud computing (rent a car), and FaaS/serverless computing (car sharing). VPS in the rent-a-car analogy stands for virtual private server and refers to provisioning a virtual server from a cloud service provider.

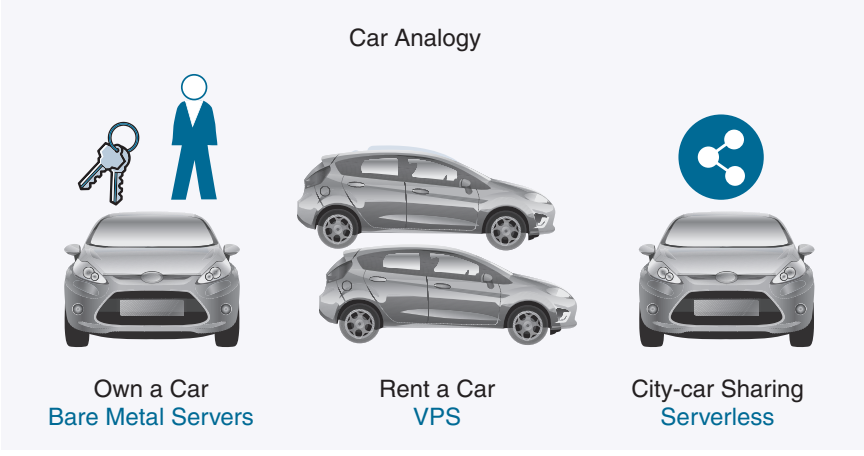

FIGURE 6-2 Car Analogy for Serverless Computing

The following are top security issues with serverless computing:

Key Topic

- **Function event data injection:** Triggered through untrusted input such as through a web API call
- **Broken authentication:** Coding issues ripe for exploit and attacks, which lead to unauthorized authentication
- **Insecure serverless deployment configuration:** Human error in setup
- **Over-privileged function permissions and roles:** Failure to implement the least privilege concept

Infrastructure as Code (IaC)

In another reordering of the way data centers are handled, ***Infrastructure as Code (IaC)*** manages and provisions computer data centers through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools. IaC can use either scripts or declarative definitions, rather than manual processes, but the term more often is used to promote declarative approaches.

Naturally, there are advantages to this approach:

Key Topic

- Lower cost
- Faster speed
- Risk reduction (remove errors and security violations)

Figure 6-3 illustrates an example of how some code might be capable of making changes on its own without manual intervention. As you can see in Figure 6-3, these code changes can be made to the actual state of the configurations in the cloud without manual intervention.

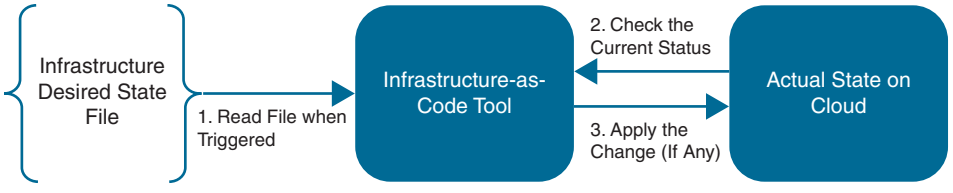

FIGURE 6-3 IaC in Action

Security issues with Infrastructure as Code (IaC) include

Key Topic

- **Compliance violations:** Policy guardrails based on standards are not enforced
- **Data exposures:** Lack of encryption
- **Hardcoded secrets:** Storing plain text credentials, such as SSH keys or account secrets, within source code
- **Disabled audit logs:** Failure to utilize audit logging services like AWS CloudTrail and Amazon CloudWatch
- **Untrusted image sources:** Templates may inadvertently refer to OS or container images from untrusted sources

Insecure Application Programming Interface (API)

Interfaces and APIs tend to be the most exposed parts of a system because they're usually accessible from the open Internet. APIs are used extensively in cloud environments. With respect to APIs, a host of approaches—including Simple Object Access Protocol (SOAP), REpresentational State Transfer (REST), and JavaScript Object Notation (JSON)—are available, and many enterprises find themselves using all of them.

The use of diverse protocols and APIs is also a challenge to interoperability. With networking, storage, and authentication protocols, support and understanding of the protocols in use is required of both endpoints. It should be a goal to reduce the number of protocols in use in order to reduce the attack surface. Each protocol has its own history of weaknesses to mitigate.

One API that can enhance cloud security is the ***Data Protection API (DPAPI)*** offered by Windows. Let's look at what it offers. Among other features, DPAPI supports in-memory processing, an approach in which all data in a set is processed from memory rather than from the hard drive. In-memory processing assumes that all the data is available in memory rather than just the most recently used data, as is usually the case when using RAM or cache memory. This results in faster reporting and decision making in business. Securing in-memory processing requires encrypting the data in RAM. DPAPI lets you encrypt data using the user's login credentials. One of the key questions is where to store the key, because storing it in the same location as the data typically is not a good idea (the next section discusses key management). Intel's Software Guard Extensions (SGX), shipping with Skylake and newer CPUs, allows you to load a program into your processor, verify that its state is correct (remotely), and protect its execution. The CPU automatically encrypts everything leaving the processor (that is, everything that is offloaded to RAM) and thereby ensures security.

Even the most secure devices have some sort of API that is used to perform tasks. Unfortunately, untrustworthy people use those same APIs to perform unscrupulous tasks. APIs are used in the Internet of Things (IoT) so that devices can speak to each other without users even knowing they are there. APIs are used to control and monitor things we use every day, including fitness bands, home thermostats, lighting, and automobiles. Comprehensive security must protect the entire spectrum of devices in the digital workplace, including apps and APIs. API security is critical for an organization that is exposing digital assets.

Guidelines for providing API security include the following:

- Use the same security controls for APIs as for any web application in the enterprise.
- Use Hash-based Message Authentication Code (HMAC).
- Use encryption when passing static keys.

- Use a framework or an existing library to implement security solutions for APIs.
- Implement password encryption instead of single key-based authentication.

Improper Key Management

Key management is essential to ensure that the cryptography provides confidentiality, integrity, and authentication in cloud environments. If a key is compromised, it can have serious consequences throughout an organization.

Key management involves the entire process of ensuring that keys are protected during creation, distribution, transmission, and storage. As part of this process, keys must also be destroyed properly. When you consider the vast number of networks over which the key is transmitted and the different types of systems on which a key is stored, the enormity of this issue really comes to light.

As the most demanding and critical aspect of cryptography, it is important that security professionals understand key management principles.

Keys should always be stored in ciphertext when stored on a noncryptographic device. Key distribution, storage, and maintenance should be automatic by integrating the processes into the application.

Because keys can be lost, backup copies should be made and stored in a secure location. A designated individual should have control of the backup copies, and other individuals should be designated to serve as emergency backups. The key recovery process should also require more than one operator, to ensure that only valid key recovery requests are completed. In some cases, keys are even broken into parts and deposited with trusted agents, who provide their part of the key to a central authority when authorized to do so. Although other methods of distributing parts of a key are used, all the solutions involve the use of trustee agents entrusted with part of the key and a central authority tasked with assembling the key from its parts. Also, key recovery personnel should span across the entire organization and not just be members of the IT department.

Organizations should also limit the number of keys that are used. The more keys that you have, the more keys you must ensure are protected. Although a valid reason for issuing a key should never be ignored, limiting the number of keys issued and used reduces the potential damage.

When designing the key management process, you should consider how to do the following:

- Securely store and transmit the keys
- Use random keys

- Issue keys of sufficient length to ensure protection
- Properly destroy keys when no longer needed
- Back up the keys to ensure that they can be recovered

Systems that process valuable information require controls in order to protect the information from unauthorized disclosure and modification. Cryptographic systems that contain keys and other cryptographic information are especially critical. Security professionals should work to ensure that the protection of keying material provides accountability, audit, and survivability.

Accountability involves the identification of entities that have access to, or control of, cryptographic keys throughout their life cycles. Accountability can be an effective tool to help prevent key compromises and to reduce the impact of compromises when they are detected. Although it is preferred that no humans be able to view keys, as a minimum, the key management system should account for all individuals who are able to view plaintext cryptographic keys. In addition, more sophisticated key management systems may account for all individuals authorized to access or control any cryptographic keys, whether in plaintext or ciphertext form.

Two types of audits should be performed on key management systems:

Key Topic

- **Security:** The security plan and the procedures that are developed to support the plan should be periodically audited to ensure that they continue to support the key management policy.
- **Protective:** The protective mechanisms employed should be periodically reassessed with respect to the level of security they currently provide and are expected to provide in the future. They should also be assessed to determine whether the mechanisms correctly and effectively support the appropriate policies. New technology developments and attacks should be considered as part of a protective audit.

Key management survivability entails backing up or archiving copies of all keys used. Key backup and recovery procedures must be established to ensure that keys are not lost. System redundancy and contingency planning should also be properly assessed to ensure that all the systems involved in key management are fault tolerant.

Key Escrow

Key escrow is the process of storing keys with a third party to ensure that decryption can occur. This is most often used to collect evidence during investigations. Key recovery is the process whereby a key is archived in a safe place by the administrator.

Key Stretching

Key stretching, also referred to as key strengthening, is a cryptographic technique that involves making a weak key stronger by increasing the time it takes to test each possible key. In key stretching, the original key is fed into an algorithm to produce an enhanced key, which should be at least 128 bits for effectiveness. If key stretching is used, an attacker would need to either try every possible combination of the enhanced key or try likely combinations of the initial key. Key stretching slows down the attacker because the attacker must compute the stretching function for every guess in the attack. Systems that use key stretching include Pretty Good Privacy (PGP), GNU Privacy Guard (GPG), Wi-Fi Protected Access (WPA), and WPA2. Widely used password key-stretching algorithms include Password-Based Key Derivation Function 2 (PBKDF2), bcrypt, and scrypt.

Unprotected Storage

While cloud storage may seem like a great idea, it presents many unique issues. Among them are the following:

- **Data breaches:** Although cloud providers may include safeguards in service-level agreements (SLAs), ultimately the organization is responsible for protecting its own data, regardless of where it is located. When this data is not in your hands—and you may not even know where it is physically located at any point in time—protecting your data is difficult.
- **Authentication system failures:** These failures allow malicious individuals into the cloud. This issue sometimes is made worse by the organization itself when developers embed credentials and cryptographic keys in source code and leave them in public-facing repositories.
- **Weak interfaces and APIs:** Interfaces and APIs tend to be the most exposed parts of a system because they're usually accessible from the open Internet.

Transfer/Back Up Data to Uncontrolled Storage

In some cases, users store sensitive data in cloud storage that is outside the control of the organization, using sites such as Dropbox. These storage providers have had their share of data loss issues as well. Policies should address and forbid this type of storage of data from mobile devices.

Cloud services give end users more accessibility to their data. However, this also means that end users can take advantage of cloud storage to access and share company data from any location. At that point, the IT team no longer controls the data. This is the case with both public and private clouds.

With private clouds, organizations can ensure the following:

Key Topic

- That the data is stored only on internal resources
- That the data is owned by the organization
- That only authorized individuals are allowed to access the data
- That data is always available

However, a private cloud is only protected by the organization's internal resources, and this protection can often be affected by the knowledge level of the security professionals responsible for managing the cloud security.

With public clouds, organizations can ensure the following:

- That data is protected by enterprise-class firewalls and within a secured facility
- That attackers and disgruntled employees are unsure of where the data actually resides
- That the cloud vendor provides security expertise and maintains the level of service detailed in the contract

However, public clouds can grant access to any location, and data is transmitted over the Internet. Also, the organization depends on the vendor for all services provided. End users must be educated about cloud usage and limitations as part of their security awareness training. In addition, security policies should clearly state where data can be stored, and ACLs should be configured properly to ensure that only authorized personnel can access data. The policies should also spell out consequences for storing organizational data in cloud locations that are not authorized.

Big Data

Big data is a term for sets of data so large or complex that they cannot be analyzed by using traditional data processing applications. These data sets are often stored in the cloud to take advantage of the immense processing power available there. Specialized applications have been designed to help organizations with their big data. The big data challenges that may be encountered include data analysis, data capture, data search, data sharing, data storage, and data privacy.

While big data is used to determine the causes of failures, generate coupons at checkout, recalculate risk portfolios, and find fraudulent activity before it ever has a chance to affect the organization, its existence creates security issues. The first issue is its unstructured nature. Traditional data warehouses process structured data and can store large amounts of it, but there is still a requirement for structure.

Big data typically uses Hadoop, which requires no structure. Hadoop is an open source framework used for running applications and storing data. With the Hadoop Distributed File System, individual servers that are working in a cluster can fail without aborting the entire computation process. There are no restrictions on the data that this system can store. While big data is enticing because of the advantages it offers, it presents a number of issues when deployed in the cloud.

Key Topic

- Organizations still do not understand it very well, and unexpected vulnerabilities can easily be introduced.
- Open source codes are typically found in big data, which can result in unrecognized backdoors. It can contain default credentials.
- Attack surfaces of the nodes may not have been reviewed, and servers may not have been hardened sufficiently.

Logging and Monitoring

Without proper auditing, you have no accountability. You also have no way of knowing what is going on in your environment. While the next two chapters include ample discussion of logging and monitoring and its application, this section briefly addresses the topic with respect to cloud environments.

Insufficient Logging and Monitoring

Unfortunately, although most technicians agree with and support the notion that proper auditing is necessary, in the case of cloud deployments, the logging and monitoring can leave much to be desired. "Insufficient Logging and Monitoring" is one of the categories in the Open Web Application Security Project's (OWASP) Top 10 list and covers the list of best practices that should be in place to prevent or limit the damage of security breaches.

Security professionals should work to ensure that cloud SLAs include access to logging and monitoring tools that give the organization visibility into the cloud system in which their data is held.

Inability to Access

One of the issue with utilizing standard logging and monitoring tools in a cloud environment is the inability to access the environment in a way that renders visibility into the environment. In some cases, the vendor will resist allowing access to its environment. The time to demand such access is when the SLA is in the process of being negotiated.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have several choices for exam preparation: the exercises here, Chapter 22, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 6-2 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 6-2 Key Topics in Chapter 6

Key Topic Element	Description	Page Number
Bulleted list	Cloud deployment models	126
Bulleted list	Cloud service models	127
Bulleted list	Advantages of FaaS	129
Bulleted list	Top security issues with serverless computing	129
Bulleted list	Advantages of IaC	130
Bulleted list	Security issues with Infrastructure as Code (IaC)	130
Bulleted list	Guidelines for providing API security	131
Bulleted list	Designing the key management process	132
Bulleted list	Types of audit that should be performed on key management systems	133
Bulleted list	Security issues with cloud storage	134
Bulleted list	Capabilities with private and public clouds	135
Bulleted list	Issues with big data	136

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), public cloud, private cloud, community cloud, hybrid cloud, Function as a Service (FaaS), Infrastructure as Code (IaC), Data Protection API (DPAPI), NIST SP 800-57 REV. 5, key escrow, key stretching, big data

Review Questions

1. With _____, the vendor provides the entire solution, including the operating system, the infrastructure software, and the application.
2. Match the terms on the left with their definitions on the right.

Terms	Definitions
FaaS	Manages and provisions computer data centers through machine-readable definition files.
IaC	The vendor provides the hardware platform or data center, and the customer installs and manages its own operating systems and application systems.
PaaS	The vendor provides the hardware platform or data center and the software running on the platform, including the operating systems and infrastructure software.
IaaS	Completely abstracts the virtual server from the developers.

3. List at least one advantage of IaC.
4. _____ tend to be the most exposed parts of a cloud system because they're usually accessible from the open Internet.
5. APIs are used in the _____ so that devices can speak to each other without users even knowing the APIs are there.
6. List at least one of the security issues with serverless computing in the cloud.
7. Match the key state on the left with its definition on the right.

Terms	Definitions
Pre-activation state	Temporarily inactive
Suspended state	Keys may be used to cryptographically protect information
Deactivated state	Discovered by an unauthorized entity
Active state	Key has been generated but has not been authorized for use
Compromised state	Keys are not used to apply cryptographic protection, but in some cases, they may be used to process cryptographically protected information

8. In the _____ phase of a key, the keying material is not yet available for normal cryptographic operations.
9. List at least one security issue with cloud storage.
10. _____ is a term for sets of data so large or complex that they cannot be analyzed by using traditional data processing applications.

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y-Z