CompTIA®

CySA+

PRACTICE TESTS

Third Edition

EXAM CS0-003

Provides 1,000 practice questions covering all the exam objectives.

Complements the *CompTIA CySA+ Study Guide: Exam CS0-003, Third Edition*.

MIKE CHAPPLE
DAVID SEIDL

SYBEX®
A Wiley Brand

CompTIA® CySA+ Practice Tests

Exam CS0-003

Third Edition

CompTIA®

CySA+ Practice Tests

Exam CS0-003

Third Edition

Mike Chapple

David Seidl

SYBEX®
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394182930 (paperback), 9781394182954 (ePDF), 9781394182947 (ePub)

Limit of Liability/Disclaimer of Warranty: While the publisher and authors have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Control Number: 2023939017

Cover image: © Jeremy Woodhouse/Getty Images, Inc.
Cover design: Wiley

For Renee, the most patient and caring person I know. Thank you for being the heart of our family.
—MJC

This book is dedicated to my longtime friend Amanda Hanover, who always combined unlimited curiosity with an equally infinite number of questions about security topics. In 2019, Amanda lost her fight with mental health struggles. But you, our readers, should know that there is support out there. Mental health challenges are a struggle that many in the security community face, and community support exists for those who need it. Visit `www.mentalhealthhackers.org` *to find mental health activities at security conferences in your area, as well as resources and links to other resources. You are not alone.*
And Amanda—here are a thousand more security questions for you. Your friend, David.
—DAS

Acknowledgments

Books like this involve work from many people, and as authors, we truly appreciate the hard work and dedication that the team at Wiley shows. We would especially like to thank senior acquisitions editor Kenyon Brown. We have worked with Ken on multiple projects and consistently enjoy our work with him.

We also greatly appreciate the editing and production team for the book, including Lily Miller, our project editor, who brought years of experience and great talent to the project; Chris Crayton, our technical editor, who provided insightful advice and gave wonderful feedback throughout the book; Magesh Elangovan, our production editor, who guided us through layouts, formatting, and final cleanup to produce a great book; and Kim Wimpsett, our copy editor, who helped the text flow well. We would also like to thank the many behind-the-scenes contributors, including the graphics, production, and technical teams who make the book and companion materials into a finished product.

Our agent, Carole Jelen of Waterside Productions, continues to provide us with wonderful opportunities, advice, and assistance throughout our writing careers.

Finally, we would like to thank our families and significant others who support us through the late evenings, busy weekends, and long hours that a book like this requires to write, edit, and get to press.

About the Authors

Mike Chapple, Ph.D., Security+, CySA+, CISSP, is author of more than 50 books, including the best-selling *CISSP (ISC)^2 Certified Information Systems Security Professional Official Study Guide* (Sybex, 2021) and the *CISSP (ISC)^2 Official Practice Tests* (Sybex, 2021). He is an information security professional with two decades of experience in higher education, the private sector, and government.

Mike currently serves as Teaching Professor in the IT, Analytics, and Operations Department at the University of Notre Dame's Mendoza College of Business, where he teaches undergraduate and graduate courses on cybersecurity, data management, and business analytics.

Before returning to Notre Dame, Mike served as executive vice president and chief information officer of the Brand Institute, a Miami-based marketing consultancy. Mike also spent four years in the information security research group at the National Security Agency and served as an active duty intelligence officer in the U.S. Air Force.

Mike earned both his BS and PhD degrees from Notre Dame in computer science and engineering, and also holds an MS in computer science from the University of Idaho and an MBA from Auburn University. Mike holds certifications in Cybersecurity Analyst+ (CySA+), Security+, Certified Information Security Manager (CISM), Certified Cloud Security Professional (CCSP), and Certified Information Systems Security Professional (CISSP). He provides security certification resources on his website at `CertMike.com`.

David Seidl, CySA+, CISSP, PenTest+, is Vice President for Information Technology and CIO at Miami University. During his IT career, he has served in a variety of technical and information security roles, including serving as the Senior Director for Campus Technology Services at the University of Notre Dame where he co-led Notre Dame's move to the cloud and oversaw cloud operations, ERP, databases, identity management, and a broad range of other technologies and service. He also served as Notre Dame's Director of Information Security and led Notre Dame's information security program. He has taught information security and networking undergraduate courses as an instructor for Notre Dame's Mendoza College of Business, and he has written books on security certification and cyberwarfare, including co-authoring *CISSP (ISC)^2 Official Practice Tests* (Sybex, 2021) as well as the previous editions of both this book and the companion *CompTIA CySA+ Practice Tests* (Sybex, 2020, 2018).

David holds a bachelor's degree in communication technology and a master's degree in information security from Eastern Michigan University, as well as certifications in CISSP, CySA+, Pentest+, GPEN, and GCIH.

About the Technical Editor

Chris Crayton, MCSE, CISSP, CASP+, CySA+, A+, N+, S+, is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He has also been recognized with many professional and teaching awards.

Contents

Introduction

CompTIA® CySA+ (Cybersecurity Analyst) Practice Tests: Exam CS0-003, Third Edition is a companion volume to the *CompTIA CySA+ Study Guide, Third Edition* (Sybex, 2023, Chapple/Seidl). If you're looking to test your knowledge before you take the CySA+ exam, this book will help you by providing a combination of 1,000 questions that cover the CySA+ domains and easy-to-understand explanations of both right and wrong answers.

If you're just starting to prepare for the CySA+ exam, we highly recommend that you use the *Cybersecurity Analyst+ (CySA+) Study Guide, Third Edition* to help you learn about each of the domains covered by the CySA+ exam. Once you're ready to test your knowledge, use this book to help find places where you may need to study more or to practice for the exam itself.

Since this is a companion to the *CySA+ Study Guide*, this book is designed to be similar to taking the CySA+ exam. It contains multipart scenarios as well as standard multiple-choice questions similar to those you may encounter in the certification exam itself. The book is broken up into six chapters: four domain-centric chapters with questions about each domain, and two chapters that contain 85-question practice tests to simulate taking the CySA+ exam itself.

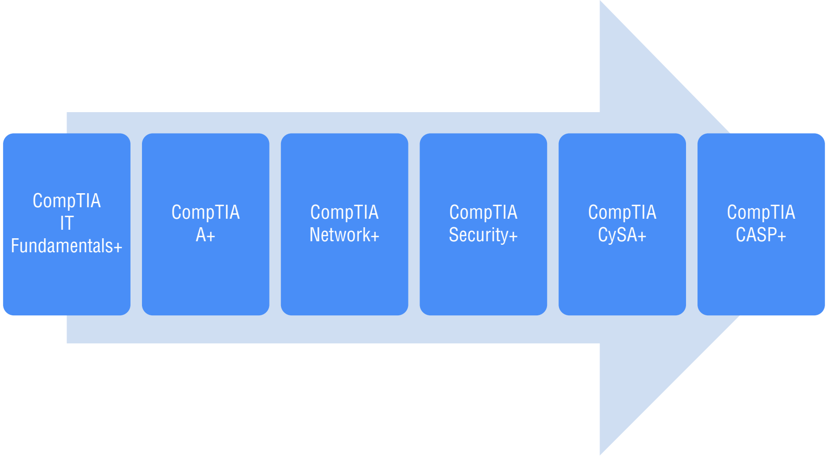
CompTIA

CompTIA is a nonprofit trade organization that offers certification in a variety of IT areas, ranging from the skills that a PC support technician needs, which are covered in the A+ exam, to advanced certifications such as the CompTIA Advanced Security Practitioner (CASP+) certification.

CompTIA recommends that practitioners follow a cybersecurity career path, as shown here:

The Cybersecurity Analyst+ exam is a more advanced exam, intended for professionals with hands-on experience and who possess the knowledge covered by the prior exams.

CompTIA certifications are ISO and ANSI accredited, and they are used throughout multiple industries as a measure of technical skill and knowledge. In addition, CompTIA certifications, including the CySA+, the Security+, and the CASP+ certifications, have been approved by the U.S. government as Information Assurance baseline certifications and are included in the State Department's Skills Incentive Program.



The Cybersecurity Analyst+ Exam

The Cybersecurity Analyst+ exam, which CompTIA refers to as CySA+, is designed to be a vendor-neutral certification for cybersecurity, threat, and vulnerability analysts. The CySA+ certification is designed for security analysts and engineers as well as security operations center (SOC) staff, vulnerability analysts, and threat intelligence analysts. It focuses on security analytics and practical use of security tools in real-world scenarios. It covers four major domains: Security Operations, Vulnerability Management, Incident Response and Management, and Reporting and Communications. These four areas include a range of topics, from reconnaissance to incident response and forensics, while focusing heavily on scenario-based learning.

The CySA+ exam fits between the entry-level Security+ exam and the CompTIA Advanced Security Practitioner (CASP+) certification, providing a mid-career certification for those who are seeking the next step in their certification and career path.

The CySA+ exam is conducted in a format that CompTIA calls *performance-based assessment*. This means that the exam uses hands-on simulations using actual security tools and scenarios to perform tasks that match those found in the daily work of a security practitioner. Exam questions may include multiple types of questions such as multiple-choice, fill-in-the-blank, multiple-response, drag-and-drop, and image-based problems.

CompTIA recommends that test takers have four years of information security–related experience before taking this exam. The exam costs $392 in the United States, with roughly equivalent prices in other locations around the globe. More details about the CySA+ exam and how to take it can be found at `https://certification.comptia.org/certifications/cybersecurity-analyst`.

NOTE For up- to- the- minute updates covering additions or modifications to the CompTIA certification exams, visit the CompTIA website at `www.comptia.org`.

Study and Exam Preparation Tips

A test preparation book like this cannot teach you every possible security software package, scenario, or specific technology that may appear on the exam. Instead, you should focus on whether you are familiar with the type or category of technology, tool, process, or scenario as you read the book. If you identify a gap, you may want to find additional tools to help you learn more about those topics.

CompTIA recommends the use of NetWars-style simulations, penetration testing and defensive cybersecurity simulations, and incident response training to prepare for the CySA+.

Additional resources for hands-on exercises include the following:

- Hacking-Lab provides capture-the-flag (CTF) exercises in a variety of fields at `https://hacking-lab.com`.
- PentesterLab provides a subscription-based access to penetration testing exercises at `https://pentesterlab.com/exercises/`.

Since the exam uses scenario-based learning, expect the questions to involve analysis and thought, rather than relying on simple memorization. As you might expect, it is impossible to replicate that experience in a book, so the questions here are intended to help you be confident that you know the topic well enough to think through hands-on exercises.

Taking the Exam

Once you are fully prepared to take the exam, you can visit the CompTIA website to purchase your exam voucher:

`https://store.comptia.org`

Currently, CompTIA offers two options for taking the exam: an in-person exam at a testing center and an at-home exam that you take on your own computer.

TIP This book includes a coupon that you may use to save 10 percent on your CompTIA exam registration.

In-Person Exams

CompTIA partners with Pearson VUE's testing centers, so your next step will be to locate a testing center near you. In the United States, you can do this based on your address or your ZIP code, while non-U.S. test takers may find it easier to enter their city and country. You can search for a test center near you at the Pearson VUE website, where you will need to navigate to "Find a test center."

`https://home.pearsonvue.com/comptia`

Now that you know where you'd like to take the exam, simply set up a Pearson VUE testing account and schedule an exam on their site.

On the day of the test, take two forms of identification, and make sure to show up with plenty of time before the exam starts. Remember that you will not be able to take your notes, electronic devices (including smartphones and watches), or other materials in with you.

At-Home Exams

CompTIA also offers an at-home testing option that uses the Pearson VUE remote proctoring service. Candidates using this approach will take the exam at their home or office and be proctored over a webcam by a remote proctor.

You can learn more about the at-home testing experience by visiting this site:

`www.comptia.org/testing/testing-options/take-online-exam`

After the Cybersecurity Analyst+ Exam

Once you have taken the exam, you will be notified of your score immediately, so you'll know if you passed the test right away. You should keep track of your score report with your exam registration records and the email address you used to register for the exam.

Maintaining Your Certification

CompTIA certifications must be renewed on a periodic basis. To renew your certification, you can either pass the most current version of the exam, earn a qualifying higher-level CompTIA or industry certification, or complete sufficient continuing education activities to earn enough continuing education units (CEUs) to renew it.

CompTIA provides information on renewals via its website at `www.comptia.org/continuing-education`.

When you sign up to renew your certification, you will be asked to agree to the CE program's Code of Ethics, pay a renewal fee, and submit the materials required for your chosen renewal method.

A full list of the industry certifications you can use to acquire CEUs toward renewing the CySA+ can be found at `www.comptia.org/continuing-education/choose/renew-with-a-single-activity/earn-a-higher-level-comptia-certification`.

Like all exams, the Exam CS0-003: CompTIA® CySA+ is updated periodically and may eventually be retired or replaced. At some point after CompTIA is no longer offering this exam, the old editions of our books and online tools will be retired. If you have purchased this book after the exam was retired or are attempting to register in the Sybex online learning environment after the exam was retired, please know that we make no guarantees that this exam's online Sybex tools will be available once the exam is no longer available.

Using This Book to Practice

This book consists of six chapters. Each of the first four chapters covers a domain, with a variety of questions that can help you test your knowledge of real-world, scenario, and best practices–based security knowledge. The final two chapters are complete practice exams that can serve as timed practice tests to help determine whether you're ready for the CySA+ exam.

We recommend taking the first practice exam to help identify where you may need to spend more study time and then using the domain-specific chapters to test your domain knowledge where it is weak. Once you're ready, take the second practice exam to make sure you've covered all the material and are ready to attempt the CySA+ exam.

As you work through questions in this book, you will encounter tools and technology that you may not be familiar with. If you find that you are facing a consistent gap or that a domain is particularly challenging, we recommend spending some time with books and materials that tackle that domain in depth. This can help you fill in gaps and help you be more prepared for the exam.

Interactive Online Learning Environment and Test Bank

The interactive online learning environment that accompanies CompTIA CySA+ Practice Tests: Exam CS0-003 provides a test bank and study tools to help you prepare for the exam. By using these tools you can dramatically increase your chances of passing the exam on your first try.

The online test bank includes over 1000 practice questions. Use all these practice questions to test your knowledge of the exam objectives. The online test bank runs on multiple devices.

NOTE Go to `www.wiley.com/go/sybextestprep` to register and gain access to the interactive online learning environment and test bank with study tools.

Objectives Map for CompTIA CySA+ (Cybersecurity Analyst) Exam CS0-003

The following objective map for the CompTIA CySA+ (Cybersecurity Analyst) certification exam will enable you to find where each objective is covered in the book.

Objectives Map

Objective	**Chapter(s)**
1.0 Security Operations	
1.1 Explain the importance of system and network architecture concepts in security operations	Chapter 1
1.2 Given a scenario, analyze indicators of potentially malicious activity	Chapter 1

Objective	Chapter(s)
1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity	Chapter 1
1.4 Compare and contrast threat intelligence and threat hunting concepts	Chapter 1
1.5 Explain the importance of efficiency and process improvement in security operations	Chapter 1
2.0 Vulnerability Management	
2.1 Given a scenario, implement vulnerability scanning methods and concepts	Chapter 2
2.2 Given a scenario, analyze output from vulnerability assessment tools	Chapter 2
2.3 Given a scenario, analyze data to prioritize vulnerabilities	Chapter 2
2.4 Given a scenario, recommend controls to mitigate attacks and software vulnerabilities	Chapter 2
2.5 Explain concepts related to vulnerability response, handling, and management	Chapter 2
3.0 Incident Response and Management	
3.1 Explain concepts related to attack methodology frameworks	Chapter 3
3.2 Given a scenario, perform incident response activities	Chapter 3
3.3 Explain the preparation and post-incident activity phases of the incident management life cycle	Chapter 3
4.0 Reporting and Communication	
4.1 Explain the importance of vulnerability management reporting and communication	Chapter 4
4.2 Explain the importance of incident response reporting and communication	Chapter 4

How to Contact the Publisher

If you believe you've found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

To submit your possible errata, please email it to our Customer Service Team at `wileysupport@wiley.com` with the subject line "Possible Book Errata Submission."

Domain 1.0: Security Operations

EXAM OBJECTIVES COVERED IN THIS CHAPTER:

✓ **1.1 Explain the importance of system and network architecture concepts in security operations**

- Log ingestion
- Operating system (OS) concepts
- Infrastructure concepts
- Network architecture
- Identity and access management
- Encryption
- Sensitive data protection

✓ **1.2 Given a scenario, analyze indicators of potentially malicious activity**

- Network-related
- Host-related
- Application-related
- Other

✓ **1.3. Given a scenario, use appropriate tools or techniques to determine malicious activity**

- Tools
- Common techniques
- Programming languages/scripting

✓ **1.4. Compare and contrast threat-intelligence and threat-hunting concepts**

- Threat actors
- Tactics, techniques, and procedures (TTP)

- Confidence levels
- Collection methods and sources
- Threat intelligence sharing
- Threat hunting

✓ **1.5. Explain the importance of efficiency and process improvement in security operations**

- Standardize processes
- Streamline operations
- Technology and tool integration
- Single pane of glass

1. Olivia is considering potential sources for threat intelligence information that she might incorporate into her security program. Which one of the following sources is most likely to be available without a subscription fee?

   A. Vulnerability feeds

   B. Open source

   C. Closed source

   D. Proprietary

2. Roger is evaluating threat intelligence information sources and finds that one source results in quite a few false positive alerts. This lowers his confidence level in the source. What criteria for intelligence is not being met by this source?

   A. Timeliness

   B. Expense

   C. Relevance

   D. Accuracy

3. Brad is working on a threat classification exercise, analyzing known threats and assessing the possibility of unknown threats. Which one of the following threat actors is most likely to be associated with an advanced persistent threat (APT)?

   A. Hacktivist

   B. Nation-state

   C. Insider

   D. Organized crime

4. What term is used to describe the groups of related organizations that pool resources to share cybersecurity threat information and analyses?

   A. SOC

   B. ISAC

   C. CERT

   D. CIRT

5. Singh incorporated the Cisco Talos tool into his organization's threat intelligence program. He uses it to automatically look up information about the past activity of IP addresses sending email to his mail servers. What term best describes this intelligence source?

   A. Open source

   B. Behavioral

   C. Reputational

   D. Indicator of compromise

6. Jamal is assessing the risk to his organization from their planned use of AWS Lambda, a serverless computing service that allows developers to write code and execute functions directly on the cloud platform. What cloud tier best describes this service?

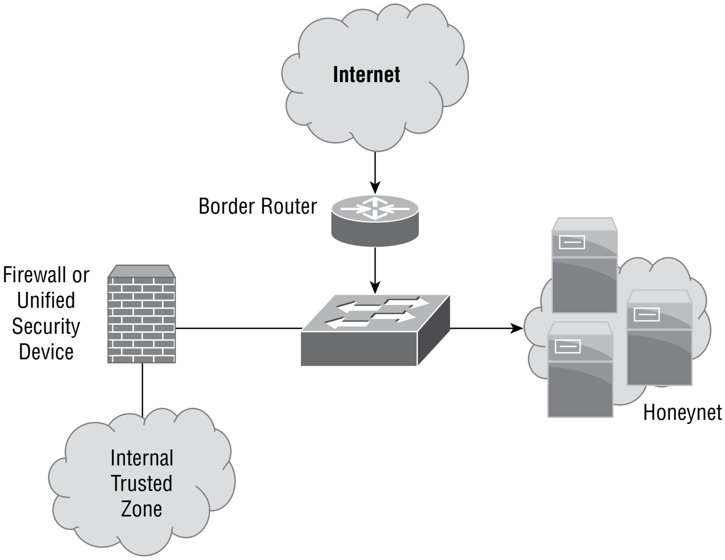
   A. SaaS

   B. PaaS

   C. IaaS

   D. FaaS

7. Lauren's honeynet, shown here, is configured to use a segment of unused network space that has no legitimate servers in it. This design is particularly useful for detecting what types of threats?



   A. Zero-day attacks

   B. SQL injection

   C. Network scans

   D. DDoS attacks

8. Fred believes that the malware he is tracking uses a fast flux DNS network, which associates many IP addresses with a single fully qualified domain name as well as using multiple download hosts. How many distinct hosts should he review based on the NetFlow shown here?

```
Date flow start   Duration     Proto    Src      IP Addr:Port  Dst IP Addr:Port
Packets   Bytes   Flows
2020-07-11        14:39:30.606 0.448    TCP      192.168.2.1:1451->10.2.3.1:443
10        1510    1
```

```
2020-07-11        14:39:30.826 0.448    TCP      10.2.3.1:443->192.168.2.1:1451
7         360     1
2020-07-11        14:45:32.495 18.492   TCP      10.6.2.4:443->192.168.2.1:1496
5         1107    1
2020-07-11        14:45:32.255 18.888   TCP      192.168.2.1:1496->10.6.2.4:443
11        1840    1
2020-07-11        14:46:54.983 0.000    TCP      192.168.2.1:1496->10.6.2.4:443
1         49      1
2020-07-11        16:45:34.764 0.362    TCP      10.6.2.4:443->192.168.2.1:4292
4         1392    1
2020-07-11        16:45:37.516 0.676    TCP      192.168.2.1:4292->10.6.2.4:443
4         462     1
2020-07-11        16:46:38.028 0.000    TCP      192.168.2.1:4292->10.6.2.4:443
2         89      1
2020-07-11        14:45:23.811 0.454    TCP      192.168.2.1:1515->10.6.2.5:443
4         263     1
2020-07-11        14:45:28.879 1.638    TCP      192.168.2.1:1505->10.6.2.5:443
18        2932    1
2020-07-11        14:45:29.087 2.288    TCP      10.6.2.5:443->192.168.2.1:1505
37        48125   1
2020-07-11        14:45:54.027 0.224    TCP      10.6.2.5:443->192.168.2.1:1515
2         1256    1
2020-07-11        14:45:58.551 4.328    TCP      192.168.2.1:1525->10.6.2.5:443
10        648     1
2020-07-11        14:45:58.759 0.920    TCP      10.6.2.5:443->192.168.2.1:1525
12        15792   1
2020-07-11        14:46:32.227 14.796   TCP      192.168.2.1:1525->10.8.2.5:443
31        1700    1
2020-07-11        14:46:52.983 0.000    TCP      192.168.2.1:1505->10.8.2.5:443
1         40      1
```

A. 1

B. 3

C. 4

D. 5

9. Which one of the following functions is not a common recipient of threat intelligence information?

A. Legal counsel

B. Risk management

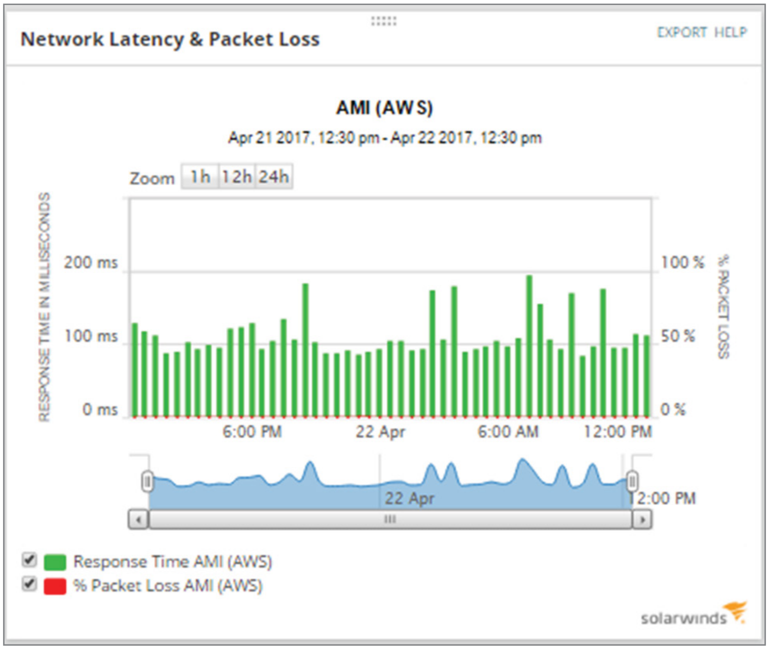
C. Security engineering

D. Detection and monitoring

10. Alfonzo is an IT professional at a Portuguese university who is creating a cloud environment for use only by other Portuguese universities. What type of cloud deployment model is he using?

- **A.** Public cloud
- **B.** Private cloud
- **C.** Hybrid cloud
- **D.** Community cloud

11. As a member of a blue team, Lukas observed the following behavior during an external penetration test. What should he report to his managers at the conclusion of the test?


Network Latency & Packet Loss
EXPORT HELP
AMI (AWS)
Apr 21 2017, 12:30 pm - Apr 22 2017, 12:30 pm
Zoom 1h 12h 24h
RESPONSE TIME IN MILLISECONDS
200 ms
100 ms
0 ms
100 %
50 %
0 %
% PACKET LOSS
6:00 PM
22 Apr
6:00 AM
12:00 PM
22 Apr
12:00 PM
☑ 🟩 Response Time AMI (AWS)
☑ 🟥 % Packet Loss AMI (AWS)
solarwinds

- **A.** A significant increase in latency.
- **B.** A significant increase in packet loss.
- **C.** Latency and packet loss both increased.
- **D.** No significant issues were observed.

12. The company that Maria works for is making significant investments in infrastructure-as-a-service hosting to replace its traditional datacenter. Members of her organization's management have Maria's concerns about data remanence when Lauren's team moves from