

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

Special Offers

Save 80% on Premium Edition eBook and Practice Test

The *CompTIA Cybersecurity Analyst (CySA+) CS0-002 Premium Edition eBook and Practice Test* provides three eBook files (PDF, EPUB, and MOBI/Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You also receive two additional practice exams with links for every question mapped to the PDF eBook.

See the card insert in the back of the book for your Pearson Test Prep activation code and special offers.

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

Table of Contents

Cover

Title Page

Copyright Page

Contents at a Glance

Table of Contents

Introduction

Chapter 1 The Importance of Threat Data and Intelligence

Do I Know This Already? Quiz

Foundation Topics

Intelligence Sources

Open-Source Intelligence

Proprietary/Closed-Source Intelligence

Timeliness

Relevancy

Confidence Levels

Accuracy

Indicator Management

Structured Threat Information eXpression (STIX)

Trusted Automated eXchange of Indicator Information (TAXII)

OpenIOC

Threat Classification

Known Threat vs. Unknown Threat

Table of Contents

Zero-day

Advanced Persistent Threat

Threat Actors

Nation-state

Organized Crime

Terrorist Groups

Hacktivist

Insider Threat

Intentional

Unintentional

Intelligence Cycle

Commodity Malware

Information Sharing and Analysis Communities

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 2 Utilizing Threat Intelligence to Support Organizational Security

Do I Know This Already? Quiz

Foundation Topics

Attack Frameworks

MITRE ATT&CK

The Diamond Model of Intrusion Analysis

Kill Chain

Threat Research

Reputational

Behavioral

Table of Contents

Indicator of Compromise (IoC)

Common Vulnerability Scoring System (CVSS)

Threat Modeling Methodologies

Adversary Capability

Total Attack Surface

Attack Vector

Impact

Probability

Threat Intelligence Sharing with Supported Functions

Incident Response

Vulnerability Management

Risk Management

Security Engineering

Detection and Monitoring

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 3 Vulnerability Management Activities

Do I Know This Already? Quiz

Foundation Topics

Vulnerability Identification

Asset Criticality

Active vs. Passive Scanning

Mapping/Enumeration

Validation

Remediation/Mitigation

Configuration Baseline

Table of Contents

Patching

Hardening

Compensating Controls

Risk Acceptance

Verification of Mitigation

Scanning Parameters and Criteria

Risks Associated with Scanning Activities

Vulnerability Feed

Scope

Credentialed vs. Non-credentialed

Server-based vs. Agent-based

Internal vs. External

Special Considerations

Types of Data

Technical Constraints

Workflow

Sensitivity Levels

Regulatory Requirements

Segmentation

Intrusion Prevention System (IPS), Intrusion Detection System (IDS), and Firewall
Settings

Firewall

Inhibitors to Remediation

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 4 Analyzing Assessment Output

Do I Know This Already? Quiz

Table of Contents

Foundation Topics

Web Application Scanner

- Burp Suite

- OWASP Zed Attack Proxy (ZAP)

- Nikto

- Arachni

Infrastructure Vulnerability Scanner

- Nessus

- OpenVAS

Software Assessment Tools and Techniques

- Static Analysis

- Dynamic Analysis

- Reverse Engineering

- Fuzzing

Enumeration

- Nmap

- Host Scanning

- hping

- Active vs. Passive

- Responder

Wireless Assessment Tools

- Aircrack-ng

- Reaver

- oclHashcat

Cloud Infrastructure Assessment Tools

- ScoutSuite

- Prowler

- Pacu

Exam Preparation Tasks

Table of Contents

Review All Key Topics

Define Key Terms

Review Questions

Chapter 5 Threats and Vulnerabilities Associated with Specialized Technology

Do I Know This Already? Quiz

Foundation Topics

Mobile

- Unsigned Apps/System Apps

- Security Implications/Privacy Concerns

- Data Storage

- Nonremovable Storage

- Removable Storage

- Transfer/Back Up Data to Uncontrolled Storage

- USB OTG

- Device Loss/Theft

- Rooting/Jailbreaking

- Push Notification Services

- Geotagging

- OEM/Carrier Android Fragmentation

- Mobile Payment

- NFC Enabled

- Inductance Enabled

- Mobile Wallet

- Peripheral-Enabled Payments (Credit Card Reader)

- USB

- Malware

- Unauthorized Domain Bridging

- SMS/MMS/Messaging

Table of Contents

Internet of Things (IoT)

- IoT Examples

- Methods of Securing IoT Devices

Embedded Systems

- Real-Time Operating System (RTOS)

- System-on-Chip (SoC)

- Field Programmable Gate Array (FPGA)

Physical Access Control

- Systems

- Devices

- Facilities

Building Automation Systems

- IP Video

- HVAC Controllers

- Sensors

Vehicles and Drones

- CAN Bus

- Drones

Workflow and Process Automation Systems

- Incident Command System (ICS)

- Supervisory Control and Data Acquisition (SCADA)

- Modbus

Exam Preparation Tasks

- Review All Key Topics

- Define Key Terms

- Review Questions

Chapter 6 Threats and Vulnerabilities Associated with Operating

Table of Contents

in the Cloud

Do I Know This Already? Quiz

Foundation Topics

Cloud Deployment Models

Cloud Service Models

Function as a Service (FaaS)/Serverless Architecture

Infrastructure as Code (IaC)

Insecure Application Programming Interface (API)

Improper Key Management

- Key Escrow

- Key Stretching

Unprotected Storage

- Transfer/Back Up Data to Uncontrolled Storage

- Big Data

Logging and Monitoring

- Insufficient Logging and Monitoring

- Inability to Access

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 7 Implementing Controls to Mitigate Attacks and Software Vulnerabilities

Do I Know This Already? Quiz

Foundation Topics

Attack Types

- Extensible Markup Language (XML) Attack

Table of Contents

Structured Query Language (SQL) Injection

Overflow Attacks

Buffer

Integer Overflow

Heap

Remote Code Execution

Directory Traversal

Privilege Escalation

Password Spraying

Credential Stuffing

Impersonation

Man-in-the-Middle Attack

VLAN-based Attacks

Session Hijacking

Rootkit

Cross-Site Scripting

Reflected

Persistent

Document Object Model (DOM)

Vulnerabilities

Improper Error Handling

Dereferencing

Insecure Object Reference

Race Condition

Broken Authentication

Sensitive Data Exposure

Insecure Components

Code Reuse

Insufficient Logging and Monitoring

Weak or Default Configurations

Table of Contents

Use of Insecure Functions

strcpy

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 8 Security Solutions for Infrastructure Management

Do I Know This Already? Quiz

Foundation Topics

Cloud vs. On-premises

Cloud Mitigations

Asset Management

Asset Tagging

Device-Tracking Technologies

Geolocation/GPS Location

Object-Tracking and Object-Containment Technologies

Geotagging/Geofencing

RFID

Segmentation

Physical

LAN

Intranet

Extranet

DMZ

Virtual

Jumpbox

System Isolation

Air Gap

Table of Contents

Network Architecture

- Physical
- Firewall Architecture
- Software-Defined Networking
- Virtual SAN
- Virtual Private Cloud (VPC)
- Virtual Private Network (VPN)
- IPsec
- SSL/TLS
- Serverless

Change Management

Virtualization

- Security Advantages and Disadvantages of Virtualization
- Type 1 vs. Type 2 Hypervisors
- Virtualization Attacks and Vulnerabilities
- Virtual Networks
- Management Interface
- Vulnerabilities Associated with a Single Physical Server Hosting Multiple Companies
Virtual Machines
- Vulnerabilities Associated with a Single Platform Hosting Multiple Companies Virtual
Machines
- Virtual Desktop Infrastructure (VDI)
- Terminal Services/Application Delivery Services

Containerization

Identity and Access Management

- Identify Resources
- Identify Users
- Identify Relationships Between Resources and Users
- Privilege Management

Table of Contents

Multifactor Authentication (MFA)

Authentication

Authentication Factors

Knowledge Factors

Ownership Factors

Characteristic Factors

Single Sign-On (SSO)

Kerberos

Active Directory

SESAME

Federation

XACML

SPML

SAML

OpenID

Shibboleth

Role-Based Access Control

Attribute-Based Access Control

Mandatory Access Control

Manual Review

Cloud Access Security Broker (CASB)

Honeypot

Monitoring and Logging

Log Management

Audit Reduction Tools

NIST SP 800-137

Encryption

Cryptographic Types

Symmetric Algorithms

Table of Contents

Asymmetric Algorithms

Hybrid Encryption

Hashing Functions

One-way Hash

Message Digest Algorithm

Secure Hash Algorithm

Transport Encryption

SSL/TLS

HTTP/HTTPS/SHTTP

SSH

IPsec

Certificate Management

Certificate Authority and Registration Authority

Certificates

Certificate Revocation List

OCSP

PKI Steps

Cross-Certification

Digital Signatures

Active Defense

Hunt Teaming

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 9 Software Assurance Best Practices

Do I Know This Already? Quiz

Foundation Topics

Table of Contents

Platforms

- Mobile
- Containerization
- Configuration Profiles and Payloads
- Personally Owned, Corporate Enabled
- Corporate-Owned, Personally Enabled
- Application Wrapping
- Application, Content, and Data Management
- Remote Wiping
- SCEP
- NIST SP 800-163 Rev 1
- Web Application
- Maintenance Hooks
- Time-of-Check/Time-of-Use Attacks
- Cross-Site Request Forgery (CSRF)
- Click-Jacking
- Client/Server
- Embedded
- Hardware/Embedded Device Analysis
- System-on-Chip (SoC)
- Secure Booting
- Central Security Breach Response
- Firmware

Software Development Life Cycle (SDLC) Integration

- Step 1: Plan/Initiate Project
- Step 2: Gather Requirements
- Step 3: Design
- Step 4: Develop
- Step 5: Test/Validate
- Step 6: Release/Maintain

Table of Contents

Step 7: Certify/Accredit

Step 8: Change Management and Configuration Management/ Replacement

DevSecOps

DevOps

Software Assessment Methods

User Acceptance Testing

Stress Test Application

Security Regression Testing

Code Review

Security Testing

Code Review Process

Secure Coding Best Practices

Input Validation

Output Encoding

Session Management

Authentication

Context-based Authentication

Network Authentication Methods

IEEE 802.1X

Biometric Considerations

Certificate-Based Authentication

Data Protection

Parameterized Queries

Static Analysis Tools

Dynamic Analysis Tools

Formal Methods for Verification of Critical Software

Service-Oriented Architecture

Security Assertions Markup Language (SAML)

Simple Object Access Protocol (SOAP)

Table of Contents

Representational State Transfer (REST)

Microservices

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 10 Hardware Assurance Best Practices

Do I Know This Already? Quiz

Foundation Topics

Hardware Root of Trust

Trusted Platform Module (TPM)

Virtual TPM

Hardware Security Module (HSM)

MicroSD HSM

eFuse

Unified Extensible Firmware Interface (UEFI)

Trusted Foundry

Secure Processing

Trusted Execution

Secure Enclave

Processor Security Extensions

Atomic Execution

Anti-Tamper

Self-Encrypting Drives

Trusted Firmware Updates

Measured Boot and Attestation

Measured Launch

Integrity Measurement Architecture

Table of Contents

Bus Encryption

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 11 Analyzing Data as Part of Security Monitoring Activities

Do I Know This Already? Quiz

Foundation Topics

Heuristics

Trend Analysis

Endpoint

Malware

Virus

Worm

Trojan Horse

Logic Bomb

Spyware/Adware

Botnet

Rootkit

Ransomware

Reverse Engineering

Memory

Memory Protection

Secured Memory

Runtime Data Integrity Check

Memory Dumping, Runtime Debugging

System and Application Behavior

Known-good Behavior

Table of Contents

Anomalous Behavior

Exploit Techniques

File System

File Integrity Monitoring

User and Entity Behavior Analytics (UEBA)

Network

Uniform Resource Locator (URL) and Domain Name System (DNS) Analysis

DNS Analysis

Domain Generation Algorithm

Flow Analysis

NetFlow Analysis

Packet and Protocol Analysis

Packet Analysis

Protocol Analysis

Malware

Log Review

Event Logs

Syslog

Kiwi Syslog Server

Firewall Logs

Windows Defender

Cisco Check Point

Web Application Firewall (WAF)

Proxy

Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)

Sourcefire

Snort

Zeek

HIPS

Table of Contents

Impact Analysis

- Organization Impact vs. Localized Impact

- Immediate Impact vs. Total Impact

Security Information and Event Management (SIEM) Review

- Rule Writing

- Known-Bad Internet Protocol (IP)

- Dashboard

Query Writing

- String Search

- Script

- Piping

E-mail Analysis

- E-mail Spoofing

- Malicious Payload

- DomainKeys Identified Mail (DKIM)

- Sender Policy Framework (SPF)

- Domain-based Message Authentication, Reporting, and Conformance (DMARC)

- Phishing

- Spear Phishing

- Whaling

- Forwarding

- Digital Signature

- E-mail Signature Block

- Embedded Links

- Impersonation

Exam Preparation Tasks

- Review All Key Topics

- Define Key Terms

- Review Questions

Table of Contents

Chapter 12 Implementing Configuration Changes to Existing Controls to Improve Security

Do I Know This Already? Quiz

Foundation Topics

Permissions

Whitelisting and Blacklisting

- Application Whitelisting and Blacklisting

- Input Validation

Firewall

- NextGen Firewalls

- Host-Based Firewalls

Intrusion Prevention System (IPS) Rules

Data Loss Prevention (DLP)

Endpoint Detection and Response (EDR)

Network Access Control (NAC)

- Quarantine/Remediation

- Agent-Based vs. Agentless NAC

- 802.1X

Sinkholing

Malware Signatures

- Development/Rule Writing

Sandboxing

Port Security

- Limiting MAC Addresses

- Implementing Sticky MAC

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Table of Contents

Review Questions

Chapter 13 The Importance of Proactive Threat Hunting

Do I Know This Already? Quiz

Foundation Topics

Establishing a Hypothesis

Profiling Threat Actors and Activities

Threat Hunting Tactics

Hunt Teaming

Threat Model

Executable Process Analysis

Memory Consumption

Reducing the Attack Surface Area

System Hardening

Configuration Lockdown

Bundling Critical Assets

Commercial Business Classifications

Military and Government Classifications

Distribution of Critical Assets

Attack Vectors

Integrated Intelligence

Improving Detection Capabilities

Continuous Improvement

Continuous Monitoring

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 14 Automation Concepts and Technologies

Table of Contents

Do I Know This Already? Quiz

Foundation Topics

Workflow Orchestration

Scripting

Application Programming Interface (API) Integration

Automated Malware Signature Creation

Data Enrichment

Threat Feed Combination

Machine Learning

Use of Automation Protocols and Standards

- Security Content Automation Protocol (SCAP)

Continuous Integration

Continuous Deployment/Delivery

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 15 The Incident Response Process

Do I Know This Already? Quiz

Foundation Topics

Communication Plan

- Limiting Communication to Trusted Parties

- Disclosing Based on Regulatory/Legislative Requirements

- Preventing Inadvertent Release of Information

- Using a Secure Method of Communication

- Reporting Requirements

Response Coordination with Relevant Entities

Table of Contents

- Legal
- Human Resources
- Public Relations
- Internal and External
- Law Enforcement
- Senior Leadership
- Regulatory Bodies

Factors Contributing to Data Criticality

- Personally Identifiable Information (PII)
- Personal Health Information (PHI)
- Sensitive Personal Information (SPI)
- High Value Assets
- Financial Information
- Intellectual Property
- Patent
- Trade Secret
- Trademark
- Copyright
- Securing Intellectual Property
- Corporate Information

Exam Preparation Tasks

- Review All Key Topics
- Define Key Terms
- Review Questions

Chapter 16 Applying the Appropriate Incident Response Procedure

- Do I Know This Already? Quiz
- Foundation Topics

Table of Contents

Preparation

- Training

- Testing

- Documentation of Procedures

Detection and Analysis

- Characteristics Contributing to Severity Level Classification

- Downtime and Recovery Time

- Data Integrity

- Economic

- System Process Criticality

- Reverse Engineering

- Data Correlation

Containment

- Segmentation

- Isolation

Eradication and Recovery

- Vulnerability Mitigation

- Sanitization

- Reconstruction/Reimaging

- Secure Disposal

- Patching

- Restoration of Permissions

- Reconstitution of Resources

- Restoration of Capabilities and Services

- Verification of Logging/Communication to Security Monitoring

Post-Incident Activities

- Evidence Retention

- Lessons Learned Report

- Change Control Process

Table of Contents

- Incident Response Plan Update
- Incident Summary Report
- Indicator of Compromise (IoC) Generation
- Monitoring

Exam Preparation Tasks

- Review All Key Topics

- Define Key Terms

- Review Questions

Chapter 17 Analyzing Potential Indicators of Compromise

- Do I Know This Already? Quiz

- Foundation Topics

Network-Related Indicators of Compromise

- Bandwidth Consumption
- Beaconing
- Irregular Peer-to-Peer Communication
- Rogue Device on the Network
- Scan/Sweep
- Unusual Traffic Spike
- Common Protocol over Non-standard Port

Host-Related Indicators of Compromise

- Processor Consumption
- Memory Consumption
- Drive Capacity Consumption
- Unauthorized Software
- Malicious Process
- Unauthorized Change
- Unauthorized Privilege
- Data Exfiltration

Table of Contents

Abnormal OS Process Behavior

File System Change or Anomaly

Registry Change or Anomaly

Unauthorized Scheduled Task

Application-Related Indicators of Compromise

Anomalous Activity

Introduction of New Accounts

Unexpected Output

Unexpected Outbound Communication

Service Interruption

Application Log

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 18 Utilizing Basic Digital Forensics Techniques

Do I Know This Already? Quiz

Foundation Topics

Network

Wireshark

tcpdump

Endpoint

Disk

FTK

Helix3

Password Cracking

Imaging

Memory

Table of Contents

Mobile

Cloud

Virtualization

Legal Hold

Procedures

- EnCase Forensic

- Sysinternals

- Forensic Investigation Suite

Hashing

- Hashing Utilities

- Changes to Binaries

Carving

Data Acquisition

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 19 The Importance of Data Privacy and Protection

Do I Know This Already? Quiz

Foundation Topics

Privacy vs. Security

Non-technical Controls

- Classification

- Ownership

- Retention

- Data Types

- Personally Identifiable Information (PII)

- Personal Health Information (PHI)

Table of Contents

Payment Card Information

Retention Standards

Confidentiality

Legal Requirements

Data Sovereignty

Data Minimization

Purpose Limitation

Non-disclosure agreement (NDA)

Technical Controls

Encryption

Data Loss Prevention (DLP)

Data Masking

Deidentification

Tokenization

Digital Rights Management (DRM)

Document DRM

Music DRM

Movie DRM

Video Game DRM

E-Book DRM

Watermarking

Geographic Access Requirements

Access Controls

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Chapter 20 Applying Security Concepts in Support of Organizational Risk Mitigation

Table of Contents

Do I Know This Already? Quiz

Foundation Topics

Business Impact Analysis

- Identify Critical Processes and Resources
- Identify Outage Impacts and Estimate Downtime
- Identify Resource Requirements
- Identify Recovery Priorities
- Recoverability
- Fault Tolerance

Risk Identification Process

- Make Risk Determination Based upon Known Metrics
- Qualitative Risk Analysis
- Quantitative Risk Analysis

Risk Calculation

- Probability
- Magnitude

Communication of Risk Factors

Risk Prioritization

- Security Controls
- Engineering Tradeoffs
- MOUs
- SLAs
- Organizational Governance
- Business Process Interruption
- Degrading Functionality

Systems Assessment

- ISO/IEC 27001
- ISO/IEC 27002

Documented Compensating Controls

Table of Contents

Training and Exercises

- Red Team

- Blue Team

- White Team

- Tabletop Exercise

Supply Chain Assessment

- Vendor Due Diligence

- OEM Documentation

- Hardware Source Authenticity

- Trusted Foundry

Exam Preparation Tasks

- Review All Key Topics

- Define Key Terms

- Review Questions

Chapter 21 The Importance of Frameworks, Policies, Procedures, and Controls

- Do I Know This Already? Quiz

- Foundation Topics

- Frameworks

 - Risk-Based Frameworks

 - National Institute of Standards and Technology (NIST)

 - COBIT

 - The Open Group Architecture Framework (TOGAF)

 - Prescriptive Frameworks

 - NIST Cybersecurity Framework Version 1.1

 - ISO 27000 Series

 - SABSA

 - ITIL

Table of Contents

Maternity Models

ISO/IEC 27001

Policies and Procedures

Code of Conduct/Ethics

Acceptable Use Policy (AUP)

Password Policy

Data Ownership

Data Retention

Account Management

Continuous Monitoring

Work Product Retention

Category

Managerial

Operational

Technical

Control Type

Preventative

Detective

Corrective

Deterrent

Directive

Physical

Audits and Assessments

Regulatory

Compliance

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

Table of Contents

Chapter 22 Final Preparation

Exam Information

Getting Ready

Tools for Final Preparation

Pearson Test Prep Practice Test Software and Questions on the Website

Memory Tables

Chapter-Ending Review Tools

Suggested Plan for Final Review/Study

Summary

Appendix A: Answers to the Do I Know This Already?

Quizzes and Review Questions

Appendix B: CompTIA Cybersecurity Analyst (CySA+) CS0-002

Cert Guide Exam Updates

Glossary of Key Terms

A

B

C

D

E

F

G

H

I

J

K

L

Table of Contents

M

N

O

P

Q

R

S

T

U

V

W

X-Z

Index

APPENDIX C: Memory Tables

APPENDIX D: Memory Tables Answer Key

APPENDIX E: Study Planner

Glossary of Key Terms