Pearson

Name: mazen oreilly

Run Date: March 4, 2025

Product: Pearson Practice Test: CompTIA Cybersecurity Analyst CySA+ CS0-002

Exam: CompTIA Cybersecurity Analyst (CySA+) CS0-002 Exam 2, CompTIA Cybersecurity Analyst (CySA+) CS0-002 Exam 3, CompTIA Cybersecurity Analyst (CySA+) CS0-002 Exam 1, CompTIA Cybersecurity Analyst (CySA+) CS0-002 Exam 4

Mode: Study Mode

Objective Name	Percentage %	Possible Points	Your Points
Chapter 01 - The Importance of Threat Data and Intelligence	100	4	4
Chapter 02 - Utilizing Threat Intelligence to Support Organizational Security	100	4	4
Chapter 03 - Vulnerability Management Activities	100	4	4
Chapter 04 - Analyzing Assessment Output	100	4	4
Chapter 05 - Threats and Vulnerabilities Associated with Specialized Technology	100	4	4
Chapter 06 - Threats and Vulnerabilities Associated with Operating in the Cloud	100	4	4
Chapter 07 - Implementing Controls to Mitigate Attacks and Software Vulnerabilities	100	4	4
Chapter 08 - Security Solutions for Infrastructure Management	75	4	3
Chapter 09 - Software Assurance Best Practices	100	4	4
Chapter 10 - Hardware Assurance Best Practices	100	4	4
Chapter 11 - Analyzing Data as Part of Security Monitoring Activities	100	4	4
Chapter 12 - Implementing Configuration Changes to Existing Controls to Improve Security	100	4	4
Chapter 13 - The Importance of Proactive Threat Hunting	100	4	4
Chapter 14 - Automation Concepts and Technologies	100	4	4
Chapter 15 - The Incident Response Process	100	4	4
Chapter 16 - Applying the Appropriate Incident Response Procedure	100	4	4
Chapter 17 - Analyzing Potential Indicators of Compromise	100	4	4
Chapter 18 - Utilizing Basic Digital Forensics Techniques	100	3	3
Chapter 19 - The Importance of Data Privacy and Protection	100	3	3
Chapter 20 - Applying Security Concepts in Support of Organizational Risk Mitigation	100	3	3
Chapter 21 - The Importance of Frameworks, Policies, Procedures, and Controls	100	3	3