

CERTIFICATE NUMBER: CERT20240210386



Muhammad Rohmattullah Joyonegoro

Has completed a 40 hours program of Comptia Security+ (Include Exam) Training at the IDN.ID Training Center, Jakarta, on 4, 5, 6, 7, 8 Maret 2024 The student was able to obtain proficiency:

- 1. Threats, Attcks, and Vulnerabilities
- 1.1 Compare and Contrast different types of social engineering techniques.
- 1.2 Given a scenario, analyze potential indicators to determine the type of attacks
- 1.3 given a scenario, analyze potential indicators associated with application attacks
- 1.4 Given a scenario, analyze potential indicators associated with network attacks
- 1.5 Explain differenct threat actors, vectors and intellifence sources
- 1.6 Explain the security concenrns associated with various types of vulnerabilties
- 1.7 Summarize the techniques used in security assessments
- 1.8 Explain the techniques used in penetration testing

- 2. Architecture and Design
- 2.1 Explain the importance of security concepts in an enterprise environment
- 2.2 Summarize virtualization and cloud computing concepts
- 2.3 Summarize secure application development, deployment, and automation concets
- 2.4 Summarize authentication and authorization design concepts
- 2.5 Given a scenarion, implement cybesecuriyt resilence
- 2.6 Explain the security implications of embedded and specialzed systems
- 2.7 Explain the importance of physical security controls
- 2.8 summarize the basics of cryptographic concepts

- 3. Implementation
- 3.1 Given a scenario, implement secure protocols
- 3.2 Given a scenario, implement host or application security solutions3.3 Given a scenario, implement secure
- network designs

 3.4 Given a scenario, install and configure
- wireless security settings

 2.5 Given a scenario, install and configure
- 3.5 Given a scenario, implement secure mobile solutions3.6 Given a scenario, apply cybersecurity
- solutions to the cloud

 3.7 Given a scenario, implement identity
- and account management controls

 3.8 Given a scenario, implement
- authentication and authorization solutions
- 3.9 Given a scenario, implement public key infrastructure

- 4. Operations and Incident Response
- 4.1 Given a scenario, use the appropriate tool to asses organizational security
- 4.2 Summarize the importance of policies, processes, and procedures for incident response
- 4.3 Given an incident, utilize approporiate data sources to support an investigation
- 4.4 Given an incident, apply mitigation techniques or controls to secure an environment
- 4.5 Explain the key aspects of digital forensics

- 5. Governance, Risk, and complicance
- 5.1 Compare and contrast various types of controls
- 5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture
- 5.3 Explain the importanc of policies to organizational security
- 5.4 Summarize risk management processes and concepts
- 5.5 Explain privacy and sensitive data concepts in reletaion to security

8 Maret 2024¹



CIDALID Tacining C

CEO of IDN.ID Training Center