The Certified Cybersecurity Operations Analyst™ (CCOA™)

Table of Contents

20% DOMAIN 2 – CYBERSECURITY PRINCIPLES AND RISK

A–CYBERSECURITY PRINCIPLES

Compliance

Cybersecurity Objectives

Governance

Risk Management

Roles and Responsibilities

Cybersecurity Models

B–CYBERSECURITY RISK

Application Risk

Cloud Technology Risk

Data Risk

Network Risk

Supply Chain Risk

System/Endpoint Risk

Web Application Risk

10% DOMAIN 3 – ADVERSARIAL TACTICS, TECHNIQUES, AND PROCEDURES

A–THREAT LANDSCAPE

Attack Vectors

Threat Actors/Agents

Threat Intelligence Sources

B–MEANS AND METHODS

Attack Types

Cyber Attack Stages

Exploit Techniques

Penetration Testing

34% DOMAIN 4 – INCIDENT DETECTION AND RESPONSE

A–INCIDENT DETECTION

Data Analytics

Detection Use Cases

Indicators of Compromise and/or Attack

Logs and Alerts

Monitoring Tools and Technologies

B–INCIDENT RESPONSE

Incident Containment

Incident Handling

Forensic Analysis

Malware Analysis

Network Traffic Analysis

Packet Analysis

Threat Analysis

11% DOMAIN 5 – SECURING ASSETS

A–CONTROLS

Contingency Planning

Controls and Techniques

Identity and Access Management

Industry Best Practices, Guidance, Frameworks, and Standards

B–VULNERABILITY MANAGEMENT

Vulnerability Assessment

Vulnerability Identification

Vulnerability Remediation

Vulnerability Tracking