Certaining Cybersecurity Practitioner

Exam Code- CCYP™

Table of Contents

Introduction

The CCYP certified professional possesses knowledge of the foundation of cybersecurity and can apply the skills learned to protect the digital infrastructure of an organization. The candidates are tested for their ability to work on and configure systems, and monitor systems.

CCYP is formulated according to the international standards such as NIST Cybersecurity Framework (CSF 2.0), ISO/IEC 27002: 2022, and CIS Critical Security Controls v8. Domains covered are– Security Operations (SOC), Threat Hunting, Advanced IAM, and Incident Response.

CCYP is the link that connects the Base Literacy (CCYF) and the Mastery of Enterprise-Scale Security (CCYL). It equips candidates with the necessary knowledge and skills for such positions as SOC analyst, security engineer, and incident responder.

Core Competencies

- Deploy IAM (Identity and Access Management) methods to protect the digital infrastructure.
- Security Information and Event Management (SIEM) tools are combined with monitoring strategies to investigate suspicious activities.
- Practice incident response and digital forensics activities with the industry standards and frameworks.
- Use risk management and compliance execution that are consistent with ISO/IEC 27002 and NIST CSF.
- Identify vulnerabilities and carry out system hardening to ensure security by design.
- Secure network and application security measures should be taken, such as cloud-based systems.

Suitable Professionals for the CCYP Certification

- SOC Analysts (Tier-1 & Tier-2).
- Cybersecurity Engineers.
- Cloud Security Professionals.
- IT Risk & Compliance Specialists.
- Career professionals looking to switch from the basic roles to technical security operations.

Exam Information

Field	Details
Exam Code	CCYP
Delivery Mode	Online Proctored (Certaining Test Platform) / Authorized Test Center
Exam Format	Multiple Choice (MCQ) and Multiple Response (MR)
No. of Questions	75
Duration	90 minutes
Passing Score	700/1000
Language	English
Validity	Lifetime

EXAMINATION DOMAINS & WEIGHTAGE

S.No.	Domain Name	Weightage
1	Security Operations & Monitoring	30%
2	Threat Detection & Analysis	25%
3	Incident Response & Handling	20%
4	Vulnerability & Risk Management	15%
5	Security Automation & Orchestration	10%

1. SECURITY OPERATIONS & MONITORING

This domain focuses on the core functions, workflows, and analytical skills essential for effective Security Operations Center (SOC) performance. Candidates learn the **operational models and structures** of SOCs—centralized, distributed, and hybrid—and understand the full **security monitoring lifecycle**, including data collection, correlation, alerting, and response. The course outlines the **roles and responsibilities** of Tier 1, Tier 2, and Tier 3 analysts, emphasizing collaboration, escalation handling, and effective shift handovers. Learners also study key **SOC metrics and KPIs** such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). Practical focus areas include **alert management**, documentation best practices, and strategies to reduce **alert fatigue** while maintaining high operational efficiency and incident readiness.

1.1. Security Monitoring Fundamentals & SOC Operations
1.2. SIEM Architecture, Deployment & Administration
1.3. Log Analysis & Correlation
1.4. Alert Triage & Prioritization
1.5. EDR/XDR Platform Operations
1.6. Network Security Monitoring
1.7. Cloud Security Monitoring

2. THREAT DETECTION & ANALYSIS

This domain equips candidates with the skills to detect, analyze, and respond to cybersecurity threats effectively. Learners explore **threat intelligence fundamentals**, including strategic, operational, and tactical intelligence, and understand how to consume and validate **Indicators of Compromise (IOCs)**. The course covers integration of threat intelligence into **SIEM and security tools**, enabling prioritization of alerts and investigation workflows. Candidates also study frameworks such as the **Cyber Kill Chain** and the **Diamond Model of Intrusion Analysis** to systematically analyze attack patterns. Emphasis is placed on assessing the reliability and relevance of threat intelligence sources and applying them to strengthen **threat detection, incident response, and proactive hunting capabilities** within organizational environments.

- **2.1. Threat Intelligence Fundamentals**
- **2.2. IOC Identification & Validation**
- **2.3. MITRE ATT&CK Framework Application**
- **2.4. Threat Actor TTPs & Kill Chain Analysis**
- **2.5. Behavioral Analytics & Anomaly Detection**
- **2.6. Network Traffic & Packet Analysis**
- **2.7. Endpoint Behavior Analysis**
- **2.8. Threat Hunting Methodologies**

3. INCIDENT RESPONSE & HANDLING

This domain focuses on the structured approach to managing and resolving security incidents effectively. Candidates learn the **Incident Response Lifecycle (PICERL)**, encompassing preparation, identification, containment, eradication, recovery, and lessons learned. The course emphasizes **incident detection and validation**, helping analysts recognize genuine threats from false positives. Participants study **triage and analysis** techniques to prioritize and investigate incidents efficiently. Core skills include **containment strategies**, **evidence collection**, and **system recovery and restoration** while maintaining integrity for potential forensic investigation. Learners also explore **incident documentation and reporting**, ensuring compliance and transparency. Finally, **post-incident activities** are highlighted to derive lessons learned, enhance defenses, and continuously improve organizational incident response capabilities.

3.1. Incident Response Lifecycle (PICERL)
3.2. Incident Detection & Validation
3.3. Incident Triage & Analysis
3.4. Containment Strategies
3.5. Eradication & Evidence Collection
3.6. Recovery & Restoration
3.7. Incident Documentation & Reporting
3.8. Post-Incident Activities & Lessons Learned

4. VULNERABILITY & RISK MANAGEMENT

This domain focuses on identifying, assessing, and mitigating vulnerabilities to reduce organizational risk. Candidates learn the **vulnerability management lifecycle**, including discovery, assessment, prioritization, remediation, and reporting. The course covers **vulnerability scanning techniques** and frameworks, along with **CVSS scoring** to evaluate and prioritize risks effectively. Learners explore **attack surface management**, understanding exposed assets and potential entry points, and develop strategies for **patch management and remediation** to address identified weaknesses. Emphasis is placed on modern environments, including **cloud and containerized infrastructure**, ensuring that vulnerabilities are managed across diverse platforms. By mastering these concepts, candidates are prepared to proactively minimize risk, maintain system integrity, and enhance organizational resilience against evolving cyber threats.

- **4.1. Vulnerability Management Lifecycle**
- **4.2. Vulnerability Scanning & Assessment**
- **4.3. CVSS Scoring & Prioritization**
- **4.4. Attack Surface Management**
- **4.5. Patch Management & Remediation**
- **4.6. Cloud & Container Vulnerability Management**

5. SECURITY AUTOMATION & ORCHESTRATION

This domain focuses on leveraging automation to enhance the efficiency and effectiveness of security operations. Candidates learn **SOAR (Security Orchestration, Automation, and Response) fundamentals**, including the design and implementation of structured **playbooks** for incident handling. The course covers **automated response actions**, integration with security tools via **APIs**, and the use of **scripting** to streamline repetitive tasks. Learners also explore **workflow automation**, **case management**, and **automated reporting and metrics**, ensuring timely and consistent handling of security events. By mastering these techniques, candidates can reduce manual effort, minimize response times, and improve overall operational efficiency while maintaining rigorous security standards and accurate documentation for compliance and continuous improvement.

- **5.1. SOAR Fundamentals**
- **5.2. Playbook Concepts & Structures**
- **5.3. Automated Response Actions**
- **5.4. API Integration for Security**
- **5.5. Scripting for Security Automation**
- **5.6. Automated Reporting & Metrics**
- **5.7. Workflow Automation & Case Management**