CompTIA SecAI+ Certification Exam Objectives

EXAM NUMBER: CY0-001 V1

CompTIA SecAI+ CY0-001 V1 Certification Exam
Exam Objectives Document Version 4.0

About the Exam

The CompTIA SecAI+ CY0-001 V1 certification exam will certify the successful candidate has the knowledge and skills required to:

- Understand important AI concepts.
- Secure AI systems using various technical controls.
- Leverage AI to enhance corporate security posture while automating security tasks.
- Understand how governance, risk, and compliance (GRC) impacts AI technologies on a global scale.

This is equivalent to 3–4 years of IT experience and approximately 2 years of hands-on cybersecurity experience.

These content examples are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

EXAM ACCREDITATION

TBD

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

CompTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka “brain dumps”). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka “brain dumps”), they should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	SecAI+ CY0-001 V1
Number of questions	Maximum of 60
Types of questions	Multiple-choice and performance-based
Length of test	60 minutes
Recommended experience	3–4 years of IT experience and approximately 2 years of hands-on cybersecurity experience.
Passing score	600 (on a scale of 100–900)

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Basic AI Concepts Related to Cybersecurity	17%
2.0	Securing AI Systems	40%
3.0	AI-assisted Security	24%
4.0	AI Governance, Risk, and Compliance	19%
Total		**100%**

1.0 Basic AI Concepts Related to Cybersecurity

1.1 Compare and contrast various AI types and techniques used in cybersecurity.

- Types of AI
    - Generative AI
    - Machine learning
    - Statistical learning
    - Transformers
    - Deep learning
    - Generative adversarial networks (GANs)
    - Natural language processing (NLP)
        - Large language models (LLMs)
        - Small language models (SLMs)
- Model training techniques
    - Model validation
    - Supervised learning
    - Unsupervised learning
    - Reinforcement learning
    - Federated learning
    - Fine-tuning
        - Epoch
        - Pruning
        - Quantization
- Prompt engineering
    - System prompts
    - User prompts
    - One-shot prompting
    - Multi-shot prompting
    - Zero-shot prompting
    - System roles
    - Templates

1.2 Explain the importance of data security in relation to AI.

- Data processing
    - Data cleansing
    - Data verification
    - Data lineage
    - Data integrity
    - Data provenance
    - Data augmentation
    - Data balancing
- Data types
    - Structured data
    - Semi-structured data
    - Unstructured data
- Watermarking
- Retrieval-augmented generation (RAG)
    - Vector storage
    - Embeddings

1.3 Explain the importance of security throughout the life cycle of AI.

- Business use case
  - Alignment with corporate objectives
- Data collection
  - Trustworthiness
  - Authenticity
- Data preparation
- Model development/selection
- Model evaluation
- Deployment
- Validation
- Monitoring and maintenance
- Feedback and iteration
- Human-centric AI design principles
  - Human-in-the-loop
  - Human oversight
  - Human validation

2.0 Securing AI Systems

2.1 Given a scenario, use AI threat-modeling resources.

- Open Worldwide Application Security Project (OWASP) Top 10
    - LLM Top 10
    - Machine Learning (ML) Security Top 10
- Massachusetts Institute of Technology (MIT) AI Risk Repository
- MITRE Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS)
- Common Vulnerabilities and Exposures (CVE) AI Working Group
- Threat-modeling frameworks

2.2 Given a set of requirements, implement security controls for AI systems.

- Model controls
    - Model evaluation
    - Model guardrails
        - Prompt templates
- Gateway controls
    - Prompt firewalls
    - Rate limits
    - Token limits
    - Input quotas
        - Data size
        - Quantity
    - Modality limits
    - Endpoint access controls
- Guardrail testing and validation

2.3 Given a scenario, implement appropriate access controls for AI systems.

- Model access
- Data access
- Agent access
- Network/application programming interface (API) access

2.4 Given a scenario, implement data security controls for AI systems.

- Encryption requirements
    - In transit
    - At rest
    - In use
- Data safety
    - Data anonymization
    - Data classification labels
    - Data redaction
    - Data masking
    - Data minimization

2.5 Given a scenario, implement monitoring and auditing for AI systems.

- Prompt monitoring
  - Query
  - Response
- Log monitoring
- Log sanitization
- Log protection
- Response confidence level
- Rate monitoring
- AI cost monitoring
  - Prompts
  - Storage
  - Response
  - Processing
- Auditing for quality and compliance
  - Hallucinations
  - Accuracy
  - Bias and fairness
  - Access

2.6 Given a scenario, analyze the evidence of an attack and suggest compensating controls for AI systems.

- Attacks
  - Backdoor attacks
  - Trojan attacks
  - Prompt injection
  - Poisoning
    - Model poisoning
    - Data poisoning
  - Jailbreaking
  - Input manipulation
  - Introducing biases
  - Circumventing AI guardrails
  - Manipulating application integrations
  - Model inversion
  - Model theft
  - AI supply chain attacks
  - Transfer learning attacks
  - Model skewing
  - Output integrity attacks
  - Membership inference
  - Insecure output handling
  - Model denial of service (DoS)
  - Sensitive information disclosure
  - Insecure plug-in design
  - Excessive agency
  - Overreliance
- Compensating controls
  - Prompt firewalls
  - Model guardrails
  - Access controls
  - Data integrity controls
  - Encryption
  - Prompt templates
  - Rate limiting
  - Least privilege

3.0 AI-assisted Security

3.1 Given a scenario, use AI-enabled tools to facilitate security tasks.

- Tools/applications
  - Integrated development environment (IDE) plug-ins
  - Browser plug-ins
  - Command-line interface (CLI) plug-ins
  - Chatbots
  - Personal assistants
  - Model Context Protocol (MCP) server
- Use cases
  - Signature matching
  - Code quality and linting
  - Vulnerability analysis
  - Automated penetration testing
  - Anomaly detection
  - Pattern recognition
  - Incident management
  - Threat modeling
  - Fraud detection
  - Translation
  - Summarization

3.2 Explain how AI enables or enhances attack vectors.

- AI-generated content (deepfake)
  - Impersonation
  - Misinformation
  - Disinformation
- Adversarial networks
- Reconnaissance
- Social engineering
- Obfuscation
- Automated data correlation
- Automated attack generation
  - Attack vector discovery
  - Payloads
  - Malware
  - Honeypot
  - Distributed denial of service (DDoS)

3.3 Given a scenario, use AI to automate security tasks.

- Scripting tools
    - Low-code
    - No-code
- Document synthesis and summarization
- Incident response ticket management
- Change management
    - AI-assisted approvals
    - Automated deployment/rollback
- AI agents
- Continuous integration and continuous deployment (CI/CD)
    - Code scanning
    - Software composition analysis
    - Unit testing
    - Regression testing
    - Model testing
    - Automated deployment/rollback

4.0 AI Governance, Risk, and Compliance

4.1 Explain organizational governance structures that support AI.

- Organizational structures
  - AI Center of Excellence
  - AI policies and procedures
- AI-related roles
  - Data scientist
  - AI architect
  - Machine learning engineer
  - Platform engineer
  - MLOps engineer
  - AI security architect
  - AI governance engineer
  - AI risk analyst
  - AI auditor
  - Data engineer

4.2 Explain risks associated with AI.

- Responsible AI
  - Fairness
  - Reliability and safety
  - Transparency
  - Privacy and security
  - Differential privacy
  - Explainability
  - Inclusiveness
  - Accountability
  - Consistency
  - Awareness training
- Risks
  - Introduction of bias
  - Accidental data leakage
  - Reputational loss
  - Accuracy and performance of the model
  - Intellectual Property (IP)-related risks
  - Autonomous systems
- Shadow IT
  - Shadow AI

4.3 Summarize the impact of compliance on business use and development of AI.

- European Union (EU) AI Act
- Organisation for Economic Co-operation and Development (OECD) standards
- International Organization for Standardization (ISO) AI standards
- National Institute of Standards and Technology (NIST) AI Risk Management Framework (AIRMF)
- Corporate policies
  - Sanctioned vs. unsanctioned
  - Private vs. public models
  - Sensitive data governance
- Third-party compliance evaluations
- Data sovereignty

CompTIA SecAI+ Acronym List

The following is a list of acronyms that appear on the CompTIA SecAI+ CY0-001 V1 exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	DEFINITION
AI	Artificial Intelligence
AIRMF	AI Risk Management Framework
API	Application Programming Interface
ATLAS	Adversarial Threat Landscape for Artificial Intelligence Systems
CDN	Content Delivery Network
CI/CD	Continuous Integration and Continuous Deployment
CLI	Command-line Interface
CPU	Central Processing Unit
CRM	Customer Relationship Management
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DAST	Dynamic Application Security Testing
DDoS	Distributed Denial of Service
DoS	Denial of Service
EDR	Endpoint Detection and Response
ETL	Extract, Transform, Load
EU	European Union
GAN	Generative Adversarial Network
GDPR	General Data Protection Regulation
GPU	Graphics Processing Unit
GRC	Governance, Risk, and Compliance
HTTPS	Hypertext Transfer Protocol Secure
IaC	Infrastructure as Code
IAM	Identity and Access Management
IDE	Integrated Development Environment
IdP	Identity Provider
IDS	Intrusion Detection System
IP	Intellectual Property
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LLM	Large Language Model
MCP	Model Context Protocol
MDLC	Model Development Life Cycle

ACRONYM	DEFINITION
MFA	Multifactor Authentication
MIT	Massachusetts Institute of Technology
ML	Machine Learning
MLOps	Machine Learning Operations
MSSP	Managed Security Service Provider
NACL	Network Access Control List
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
OECD	Organisation for Economic Co-operation and Development
OAuth	Open Authorization
OWASP	Open Worldwide Application Security Project
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
RAG	Retrieval-augmented Generation
RMF	Risk Management Framework
SCA	Software Composition Analysis
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management
SLM	Small Language Model
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SOC 2	System and Organization Controls 2
SQL	Structured Query Language
SSH	Secure Shell
TLS	Transport Layer Security
VPC	Virtual Private Cloud
WAF	Web Application Firewall

CompTIA SecAI+
Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the SecAI+ CY0-001 V1 certification exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

EQUIPMENT

- Laptops
- Cloud VMs
- Graphics processing units (GPUs)
- NVidia Jetson Nano Orin
- Mobile devices
- Sandbox environment
- Local area network (LAN)

SOFTWARE

- Virtual containers
- Large data sets
- Test data sets
- Python environment
- R environment
- IDE
- Jupyter environment
- Chatbots
- LLMs
- Open-source tools
    - GitHub
    - Ollama
- Cloud-based environment
- Cloud-based AI studios
- Vector database
- NoSQL Database
- Neo4j Graph Database