CompTIA SecAI+

Certification Exam
Pre-draft Exam Objectives
Exam Number: CY0-001

- Pre-draft Exam Objectives summarize the tasks and skills identified in the Job Task Analysis (JTA) workshop that provide directional information about the upcoming exam version.
- The Draft Exam Objectives will replace the Pre-draft Exam Objectives after approximately two months when the skills have been peer-evaluated and validated through a JTA survey of job role practitioners.
- Pre-draft Exam Objectives may contain typos and errata that will be corrected during the development process.
- CompTIA will not accept feedback on the Pre-draft Exam Objectives document. If errors are found, please wait until the Draft Exam Objectives are posted, and then provide feedback using the Draft Exam Objectives Feedback form.

1.0 Basic AI Concepts Related to Cybersecurity

1.1 Compare and contrast various AI types and techniques within the context of cybersecurity.

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

1.2 Explain the importance of data security related 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.

- OWASP Top 10
  - LLM Top 10
  - ML Top 10
- MIT AI Risk Repository
- MITRE Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS)
- 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 Analyze the evidence of an attack and suggest compensating controls for AI systems.

- Attacks
    - Prompt injection
    - Poisoning
        - Model poisoning
        - Data poisoning
    - Jailbreaking
    - Hallucinations
    - 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
    - Sensitive information disclosure

  - Unsecure 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 assistant
- 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
- AI agents
- Continuous integration/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 policy 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
  - Explainability
  - Inclusiveness
  - Accountability
  - Consistency
- Risks
  - Introduction of bias
  - Accidental data leakage
  - Reputational loss
  - Accuracy and performance of the model
  - IP-related risks

  - Autonomous systems

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

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