Dell AI Security Achievement

D-AIS-F-A-00

Exam Description:

The Dell AI Security exam validates a candidate's foundational understanding of core concepts, terminology, and considerations involved in securing AI systems throughout their lifecycle. This includes everything from data collection and model training to deployment, monitoring, and recovery. Candidates will have a solid understanding of how sensitive data is used in AI, the importance of privacy-by-design principles, what AI security controls are and standard methods for mitigating risks and threats.

The exam also covers common AI-specific threats, such as adversarial attacks, model inversion, prompt injection, data poisoning, and model manipulation. In addition, candidates gain awareness of the safeguards that help protect AI environments, including access management, threat detection, and incident response practices. By earning this achievement, professionals prove they have the foundational knowledge to be able to identify the importance AI security for their company, maintain system integrity, and understand the evolving landscape AI-driven security.

Target Audience:

This certification is designed for a broad range of technological and business professionals who engage with AI systems or cybersecurity practices. Ideal candidates include IT professionals with experience in cybersecurity, systems administration, software development, or AI workflows, as well as technical sellers, product managers, product marketers, and service delivery teams seeking deeper security understanding. AI developers, product analysts, business analysts, and startup founders exploring secure AI adoption will also find significant value. Additionally, cybersecurity specialists, cyber-resilience experts, and AI enthusiasts looking to strengthen foundational AI security competencies are well-suited for this certification.

Exam Details:

Duration: 90 mins

# of Questions: 50

Available Languages: English, French, Japanese, Chinese Simplified, Korean and Portuguese Brazilian

Recommended Training:

Course Title	Course Number	Modality	Duration
AI Security Foundations	ESDTFD08593	OnDemand	60 mins

Exam Blueprint:

Introduction to AI Security (26%):

- Understand AI & Security Terminology
- Understand fundamental data security and privacy requirements for AI systems
- Describe security concerns with AI
- Understand the companies' data and application classification
- Understand the difference in securing AI and any other applications
- Explain basic principles of AI ethics and their impact on security practices.
- Understand types of AI security threats based on provided examples or scenarios.
- Identify the appropriate course of action to mitigate security threats

Reduce the Attack Surface (i.e., identifying threats and protecting application) (26%):

- Planning and strategies for reducing the attacks
- Identify the key security risks and privacy concerns associated with AI workflow/Ecosystem- Data, model, infrastructure/pipelines
- Identify the common model behavior/vulnerabilities that exist within the models
- Identify essential AI security controls to protect AI applications
- Describe standard methods for mitigating risks/privacy issues for AI environments

Detect and Respond to Cyber Threats (24%):

- Planning and strategies for detecting and responding
- Detect common AI-specific threats that target AI applications
- How to detect common AI specific threats
- Respond to AI-specific security incidents
- Monitor and Detect AI System Misuse

Recover from the Cyberattack (24%):

- Planning and strategies for recovering the cyberattack
- Leverage their Incident Management Plans
- Isolate/quarantine
- Incident Recovery and Troubleshooting
- Perform forensic investigation to identify root cause
- Recommendations