



# Dell Security Foundations Achievement v2

D-SF-A-01

## Exam Description:

The exam is designed for anyone who needs to demonstrate a solid grasp of fundamental security concepts, terminology, and best practices, particularly those working directly with IT systems, code, or sensitive data, or those beginning their journey into dedicated security roles. It establishes a baseline understanding upon which more specialized knowledge can be built.

## Exam Details:

Duration: 90 mins    # of Questions: 50    Available Languages: English, French

## Recommended Training:

Course Title	Course Number	Modality	Duration
Cybersecurity Threats and Business Impacts	ESDTFD04731	On-Demand	1 hour
Introduction to Cybersecurity Frameworks	ESDTFD04729	On-Demand	1 hour
IT and Cybersecurity Risk	ESDTFD04737	On-Demand	1 hour
Understanding Ransomware	ESDTFD04735	On-Demand	1 hour
Cybersecurity Tools and Processes	ESDTFD04730	On-Demand	1 hour
Zero Trust Overview	ESDTFD04732	On-Demand	1 hour
Security Hardening Concepts	ESDTFD04738	On-Demand	1 hour
Identity and Access Management	ESDTFD04736	On-Demand	1 hour
Security in the Cloud	ESDTFD04739	On-Demand	1 hour
Security at the Edge	ESDTFD04740	On-Demand	1 hour

## Exam Blueprint:

### Understanding the Security Landscape and Assets (18%)

- Identify the importance of Cybersecurity Frameworks
- Identify security measures for different network/environments
- Understand the threat entry point

### Implementing Security Controls and Access Management (20%)

- Manage user access and permissions
- Apply security controls to reduce security risks in the organization with a security-first approach

### Security Monitoring and Threat Identification (16%)

- Monitor security events and logs
- Identify risks, threats, vulnerabilities, and events

### Security Incident Handling and Preparedness (10%)

- Respond to security event
- Contribute to security incident exercises

### Post-Incident Remediation and Continual Improvement (12%)

- Perform Lessons Learned and After-Action Report
- Implement remediation efforts and corrective actions
- Update Recovery Strategies

### Cybersecurity Program Management and Compliance (24%)

- Apply knowledge of common security principles
- Reduce security risks in the organization with a security-first approach
- Implement escalation matrix/RACI
- Apply different laws and regulations