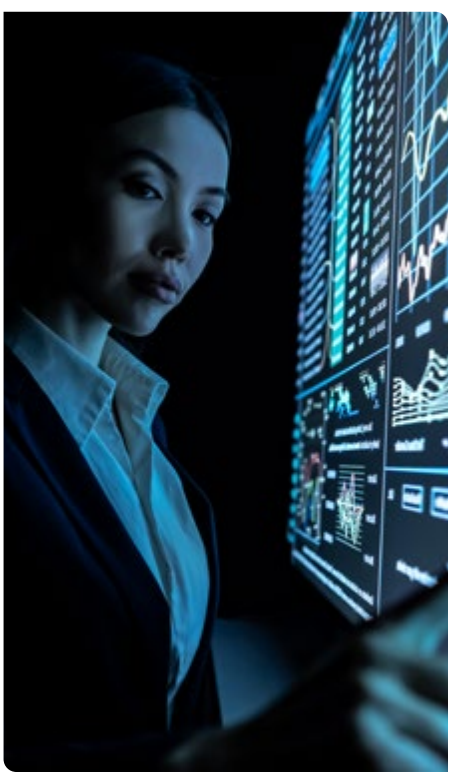
ThriveDX

Cloud Security Course



Cloud Security Course

Learning Method
Live (Online), Instructor-Led

Difficulty
Essentials

Duration
40 Hours

Pricing
$4,950

In an era where cloud computing is at the forefront of technology, securing cloud environments has become imperative for organizations worldwide. This course is designed to empower professionals with the knowledge and skills necessary to navigate the complexities of cloud security. From foundational aspects of cloud computing and identity management to more advanced topics such as virtualization, containers, and compute management. Participants will delve deep into securing cloud data, networks, and compliance with regulatory standards, all while exploring the advanced tools and practices for cloud security hardening. This course features tailored content for both AWS and Azure.

This course goes beyond theory with hands-on exercises that simulate real-world situations. By completing AWS and Azure labs, you'll gain the practical skills to secure cloud environments effectively.

Who Should Attend:

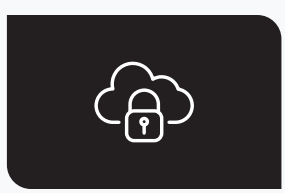
- IT professionals
- Security practitioners
- Cloud engineers and architects

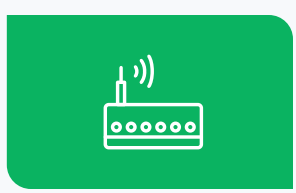
Prerequisites:

- Familiarity with IT and security concepts, including a basic understanding of networking.
- Prior exposure to or experience with information security principles and practices.
- Work experience with operating systems.

Relevant for the Following Work Paths:

- Cloud Engineer
- Cloud Security Architect
- DevOps
- IT Specialist





Upon Completion, Participants Will Emerge With:

1. **Enhanced Cloud Security Knowledge:** Understanding of cloud security principles and the significance of Identity and Access Management (IAM).

2. **Effective IAM Strategies**: Skills to implement robust IAM strategies for safeguarding cloud environments.

3. **Secure Compute Resources**: Knowledge of deploying secure and manageable computing resources in the cloud.

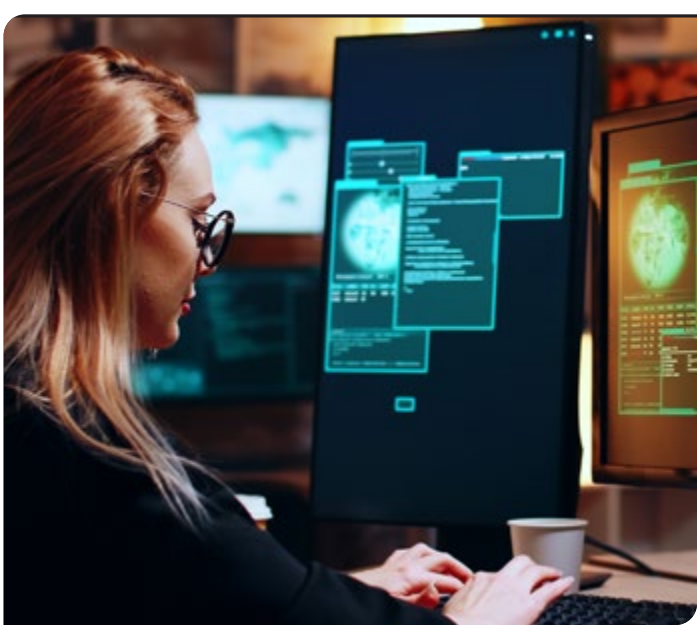
4. **Risk Identification and Mitigation**: Ability to identify and address cloud security challenges.

5. **Data Protection Techniques**: Implementation strategies for data protection in cloud environments.

6. **Cloud Networking Insight**: Understanding of cloud networking complexities and logging practices.

7. **Advanced Cloud Services Understanding:** Familiarity with advanced cloud service offerings.

8. **Threat Management Services:** Ability to anticipate and manage security threats in cloud environments.



Program Structure

Module 1

Cloud Fundamentals & Identity Management

- Cloud Computing Fundamentals
- Shared Responsibility Model
- Cloud Security Fundamentals
- Identity and Access Management (IAM)
  - IAM Best Practices and Tools
  - Hands-On IAM Analysis Exercises
  - Least Privilege Access

Module 2

Virtualization, Containers, and Compute Management

- Virtualization in Cloud Computing
- Compute Virtualization
- Cloud Network Virtualization
- Virtual Appliance
- Containers and Compute and Configuration Management
  - Intro to Docker
  - Secure Instance Deployment and Lifecycle Management
  - Image Creation and Hardening
  - Host Configuration Management
- Cloud Infrastructure Automation
- Secure Deployment in the Cloud
- Vulnerability Scanning

Module 3

Securing the Cloud With Data Protection and Networking

- Security Challenges in the Cloud
- Securing Cloud Networking and Remote Access
- Software-Defined Perimeter
- Securing Data in the Cloud
- Networking and Logging
  - Log Management for Security
  - Network Visibility and Threat Detection

Module 4

Advanced Cloud Computing & Compliance

- Benefits and Concerns of SeCaaS
  - Factors for Choosing a SeCaaS Provider
  - Security Event Management
  - Intrusion Detection
  - Configuration Auditing
- Data Protection and Automation
  - Data Classification and Encryption (Rest and Transit)
  - CASBs, CWPPs, and CSPMs Tools
- Compliance Frameworks and Audit Reports

Module 5

Securing and Hardening the Cloud

- CIS Benchmark
- Cloud-Native Security Tools and Best Practices
  - Integrating Dedicated Native Tools Into Security Workflows
  - Cloud-Native vs. Traditional Security Tools
- Vulnerability Management and Patching in Cloud Environments
  - Vulnerability Scanning Tools
  - Patch Management Strategies
  - Automation for Patching
- Monitoring
- Incident Response in the Cloud
- Reports and Automation

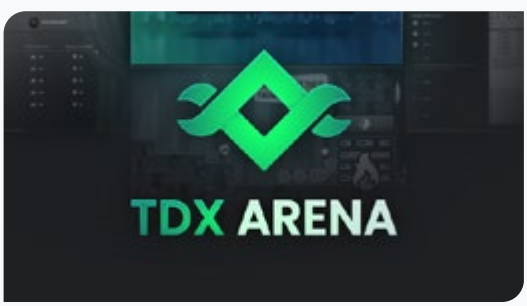
TDX

Certification Readiness

All participants who complete the course will receive a **ThriveDX Course Completion Certification**, and participants who complete the final accreditation exam will receive a ThriveDX Cloud Security Practitioner certification.

This course also aligns with the required knowledge expected for the GIAC Cloud Security Essentials (GCLD) certification.

Note: Specific materials and focus areas for the GCLD certification exam are subject to change by the certifying organization. Additional study and research may be necessary to meet certification requirements.



Embedded Labs and Challenges

The course includes our state-of-the-art proprietary cloud-based digital education platform, **TDX Arena**, in which real-life scenarios and advanced tech teaching meet in a gamified environment.

TDX