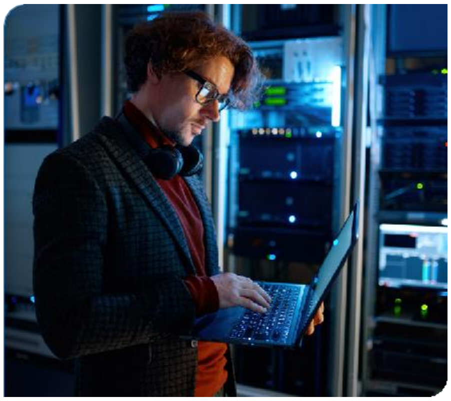
ThriveDX™

ThriveDX Cloud Security

# TDXCS-3



ThriveDX Cloud Security Course

Time Commitment	Skill Level	Format	Course Category
40 hours	Essentials	Online (Live), Instructor-Led,	Cloud Security

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 understanding the foundational aspects of cloud computing and identity management to mastering the intricacies of virtualization, containers, and compute management, this program offers a comprehensive curriculum that addresses every facet of cloud security. 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.

The curriculum incorporates hands-on exercises and real-world scenarios, ensuring that learners not only grasp theoretical concepts but also gain the practical skills needed to protect cloud environments effectively by interacting with AWS and Azure lab environments.

Who Should Attend:

- IT professionals looking to specialize in cloud security.
- Security practitioners looking to enhance their skill set in cloud environments.
- Cloud engineers and architects looking to implement security best practices within their cloud deployments.
- Teams and organizations looking to improve their cloud security readiness and response capabilities.

Relevant For The Following Work Paths:

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

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.

Upon Completion, Participants will Emerge with:

1

Thorough understanding of cloud security principles and the importance of Identity and Access Management (IAM)

2 Box 2

Robust IAM strategies to safeguard cloud environments

3

Deploying secure and manageable compute resources

4

Identifying and mitigating cloud security challenges

5

Implementing data protection strategies

6

Understanding the complexities of cloud networking and logging

7

Thorough understanding of cloud security principles and the importance of Identity and Access Management (IAM)

8

Anticipating and managing security threats

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 Appliances
- Containers & 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 & 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 automations

Certification Readiness

All participants completing the course will receive a **ThriveDX Course Completion Certification**. Participants completing 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 and 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.