

# Team Details

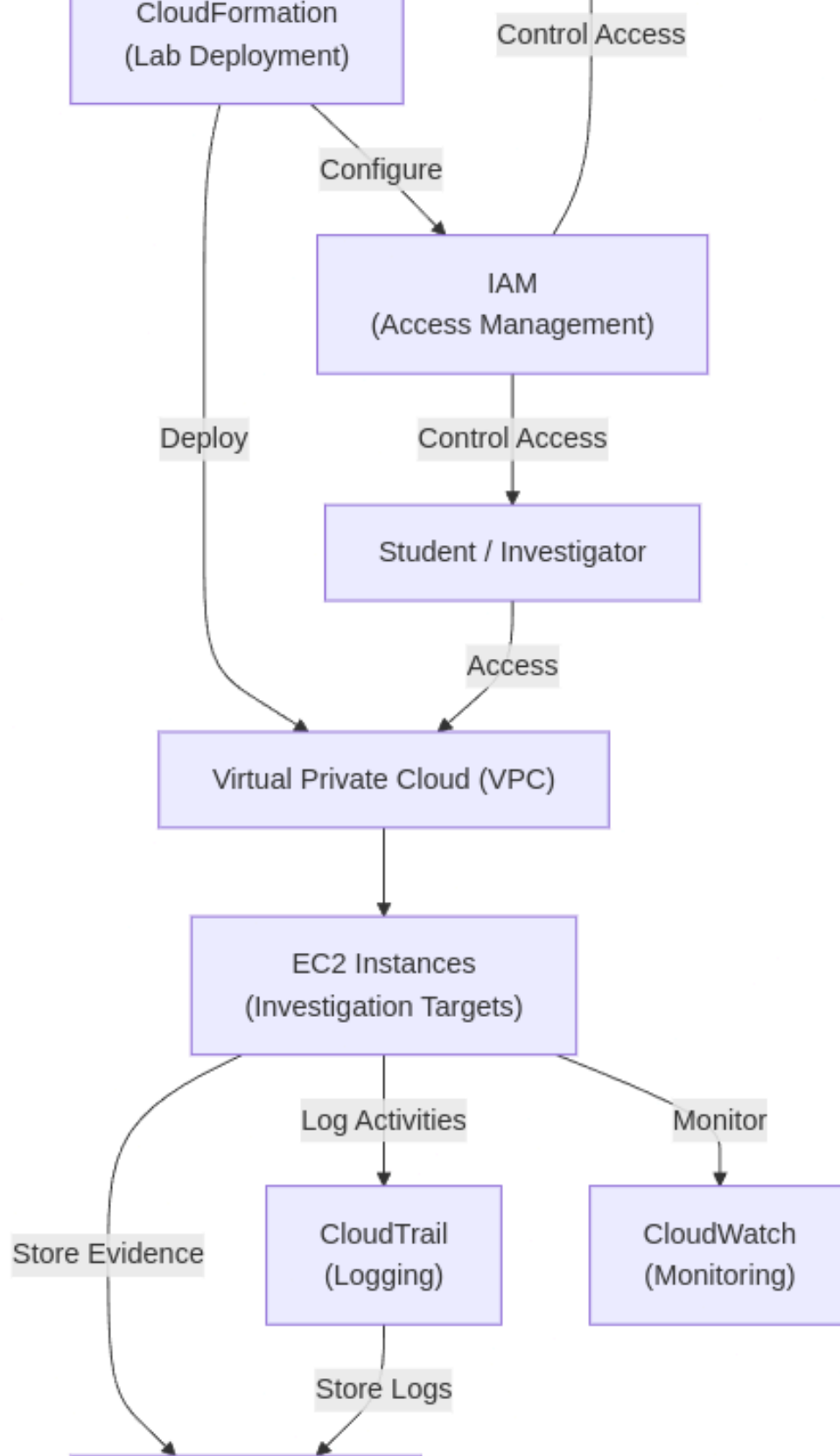
## TEAM TECHIEZ

- Team Leader – ASHISH BAGHEL
- Member 1 – YUVRAJ ANAND
- Member 2 – YASH VERMA

# Diagram

The diagram illustrates a security breach in a cloud environment. The flow is as follows:

- Attacker** (hacker icon) sends traffic to a **Load Balancer**.
- The **Load Balancer** directs traffic to **EC2 Auto Scaling**.
- EC2 Auto Scaling** provisions **EC2** instances.
- One **EC2** instance runs an **ECS** container with **PHP** and **Docker**.
- The attacker exploits a **Docker Breakout** to gain access to the **EC2** instance's **Command Execution (Interactive Shell)**.
- From the shell, the attacker performs a **File Upload**.
- The **File Upload** leads to a **Permissions Boundary** (key icon).
- The **Permissions Boundary** is associated with an **EC2 Role** (key icon).
- The **EC2 Role** is linked to an **Overly Permissive Policy** (crown icon with checkmarks and an X).
- The **Overly Permissive Policy** allows the attacker to access **Secrets Manager** (crown icon with a key).
- Secrets Manager** is connected to **RDS DB** (blue database icon).
- The **EC2** instance also has an **ECS Container Role** (key icon) that provides access to **Secrets Manager**.
- The **EC2** instance also has a **Docker Breakout** (blue whale icon) that leads to a **Command Execution (Interactive Shell)**.
- The **Command Execution (Interactive Shell)** is connected to a **File Upload** (document icon).





## Enhanced Interactivity

- Unlike traditional static textual training resources, our lab offers real-time simulations that engage users actively in a gamified learning process.

## Integrated Command Line Interface

- Combines command execution with instructional materials in one platform, reducing cognitive load and improving workflow efficiency.

## Realistic Scenario Development

- Focused on complex, real-world cloud forensics challenges, ensuring that students encounter relevant issues they will face in the field.

## Offline Accessibility

- Provides downloadable VM labs for uninterrupted practice, overcoming the limitations of online-only training platforms.

## Detailed Post-Challenge Feedback

- Offers comprehensive solutions and explanations after challenges, promoting deeper understanding and reinforcing learning.

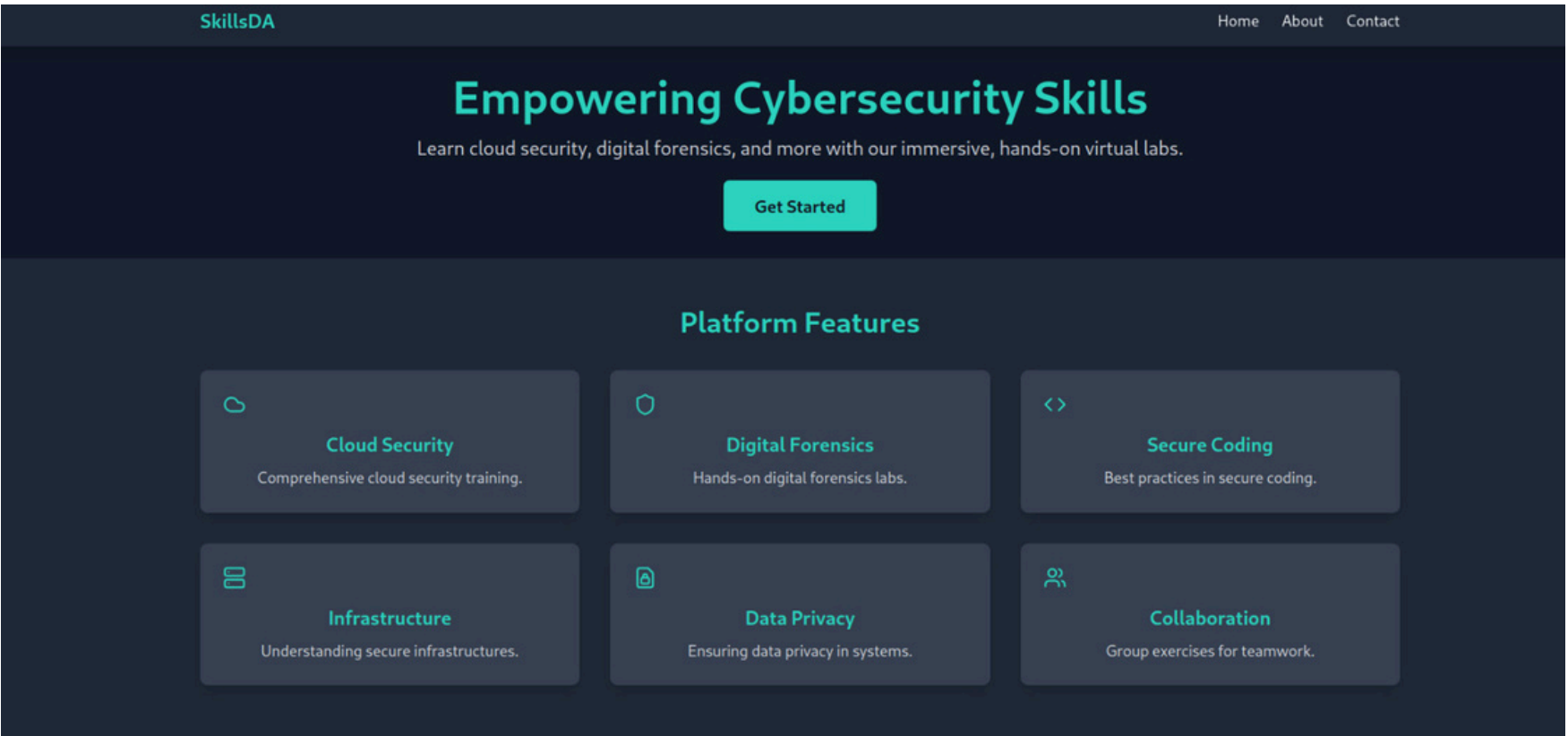
## Focus on Modern Technologies

- Incorporates cutting-edge tools and methodologies that address the latest trends in cloud forensics.

## Comprehensive Training Materials

- A well-structured lab manual that combines theory and practical application, ensuring a holistic approach to cyber investigation training.

# Improvement Over Existing Solutions



## Platform Landing Page

## 1. Comprehensive Hands-On Experience

- Simulates complex, real-world cloud-based digital forensics scenarios.
- Focus on essential AWS services: EC2 instances, S3 buckets, and more.

## 2. Integrated Learning Platform

- Unified interface for executing commands and referencing the lab manual.
- Reduces the need to switch between multiple resources, enhancing user efficiency.

## 3. Step-by-Step Guidance

- Detailed lab manual with clear objectives & procedures.
- Structured learning approach facilitates better understanding and retention.

## 4. Post-Challenge Solutions

- Comprehensive solutions provided after attempts to reinforce learning.
- Aids in concept clarification and skill enhancement through feedback.

## 5. Offline Capabilities

- Provides offline VM labs for local practice with VirtualBox and other software.
- Ensures continuous learning without reliance on internet connectivity.

## 6. Real-World Relevance

- Scenarios designed to reflect current trends and challenges in cloud forensics.
- Prepares users for actual investigative roles in evolving cyber landscapes.

U

S

P