Test Plan - CyberRange Cybersecurity Training Platform

1. Introduction

The purpose of this Test Plan is to define the testing strategy, resources, and schedule for the CyberRange platform. This document outlines the scope of testing, the methodologies to be used, and the criteria for success for the current release cycle (January 2026).

2. Test Items

Testing will be performed on the latest build of the CyberRange platform, which includes:

- **Frontend**: Next.js 14 based administrative and student dashboards.
- **Backend**: NestJS microservices (Auth, Scenario, Simulation, User).
- **Infrastructure**: Kubernetes cluster orchestration for simulation containers.

3. Scope

3.1 Features to be Tested

Based on the `Comprehensive_Test_Cases.md`, the following modules are in scope:

1. **Authentication**: Signup, Login, JWT Validation, and Role-Based Access (Admin vs. Student).
2. **User Profile & Progress**: Profile updates, password resets, account deletion, and progress tracking.
3. **Scenarios & Simulation**: Scenario listing, questionnaires, and Kubernetes simulation launch/stop lifecycle.
4. **Admin Dashboard**: Cluster health monitoring (Pods), user management, audit logs, and administrative security constraints.
5. **General & Navigation**: Responsiveness and 404 error handling.

3.2 Features Not to be Tested

- Direct cloud provider infrastructure (e.g., AWS/GCP control planes).
- Third-party browser internals.
- Physical network security of the hosting environment.

4. Approach

Testing follows a **Hybrid Testing Approach**:

- **Automated Testing**: Using **Katalon Studio** for high-priority regression paths (Auth and Admin Dashboard).
- **Manual Testing**: Black-box testing for UX-heavy features and edge-case validation.
- **Traceability**: All tests map back to `Comprehensive_Test_Scenarios.md` for stakeholder visibility.

5. Item Pass/Fail Criteria

- **Pass**: The actual behavior exactly matches the "Expected Behavior" defined in the test cases without functional errors.
- **Fail**: Any deviation from expected behavior, UI crashes, or security bypasses.
- **Critical Fail**: Any failure that prevents a user from completing a core learning workflow (e.g., simulation fails to launch).

6. Suspension & Resumption Criteria

- **Suspension**: Testing will be suspended if the Kubernetes cluster or API Gateway is inaccessible for more than 4 hours.
- **Resumption**: Testing will resume once the DevOps team confirms environment stability.

7. Test Deliverables

1. **Test Plan** (This document)
2. **Comprehensive Test Cases** (`Comprehensive_Test_Cases.md`)
3. **Comprehensive Test Scenarios** (`Comprehensive_Test_Scenarios.md`)
4. **Katalon Test Scripts** (Located in `/New folder/Tests/Scripts/`)
5. **Bug Reports** (`BUG_REPORTS.md`)

8. Test Tasks & Automation Status (as of 2026-01-08)

Module	Total Cases	Automated	Manual	Completion
Authentication	11	10	1	100%
User Profile & Progress	10	0	10	100%
Scenarios &				

Module	Total Cases	Automated	Manual	Completion
Simulation	8	8	0	100%
Admin Dashboard	12	10	2	100%
General & Navigation	2	0	2	100%
Total	**43**	**28**	**15**	**100%**

9. Environmental Needs

- **Test Environment**: Local Node.js server (Port 3000) and API Gateway.
- **Cluster**: Minikube or Docker Desktop (with Kubernetes enabled).
- **Database**: MongoDB (Isolated test instance).
- **Tools**: Katalon Studio 9.x, Chrome Browser, Postman.

10. Risks and Mitigations

Risk	Probability	Impact	Mitigation
Kubernetes Resource Limits	Medium	High	Monitor RAM/CPU usage during concurrent simulations.
Test Data Pollution	High	Medium	implement reset scripts for the MongoDB test collection.
Browser Compatibility	Low	Medium	Test primary flows on Chrome, Firefox, and Edge.

11. Approvals

Role	Signature	Date
Project Manager	_____	2026-01-08
QA Lead	_____	2026-01-08
Lead Developer	_____	2026-01-08
DevOps Engineer	_____	2026-01-08