

AmCham Bulgaria Hackathon 2026

March 20 – April 30, 2026

Social Engineering Resilience Training for Enterprise Messaging Channels

by Syscom Engineering



ASSIGNMENT CONTENT

1/2

Develop a chat-based security awareness training game that simulates real-world social engineering attacks (Teams/WhatsApp/Slack style) and measures user behaviour through risk scoring, policy compliance, and resistance to manipulation.

The goal of this project is to build an interactive training prototype that helps employees recognize and stop social engineering attempts in chat channels - where urgency, authority, and informal tone often lead to costly mistakes (e.g., CEO fraud, supplier bank change, MFA reset scams). The solution should train practical “muscle memory”: verify out-of-band, refuse unsafe requests, and report suspicious conversations quickly and correctly. The system will evaluate user choices in realistic chat scenarios and provide immediate feedback, explanations, and a personal weakness profile (e.g., “falls for urgency” or “falls for authority”).

ASSIGNMENT CONTENT

2/2

Students will work through all phases of development, including designing scenario content and a consistent scoring model, implementing a chat-like user interface, and building analytics to track performance and learning outcomes. A key focus will be delivering measurable improvements via replayability, adaptive difficulty, and clear reporting workflows. The prototype should include a mandatory “Report” feature that generates a structured incident report template, reinforcing correct escalation and response behaviour.

By the end of the project, students will present a functional prototype demonstrating at least 15 complete scenarios, interactive decision points, scoring and feedback, reporting workflow, and a dashboard/scoreboard with analytics - along with a brief plan for how the training could be rolled out and maintained at scale in a real organization.



MENTOR: Anzhela Damyanova, Presales Engineer Cybersecurity

Angela Damyanova has more than five years of experience in the field of cybersecurity, with a focus on technical consulting and developing client solutions.

She is part of the Syscom Engineering team, where she works on projects related to the implementation and support of information security solutions. Angela holds professional certifications from leading companies such as Fortinet, WithSecure, TeamViewer, NAKIVO, IBM, Lenovo, and Trend Micro, and is currently advancing her cybersecurity education in Germany. She is also a member of Women4Cyber Bulgaria, where she supports the development of women in the sector. In her professional role, Angela supports organizations in selecting and implementing effective information security solutions, conducts product demonstrations and consultations, and contributes to the preparation of technical specifications in the field of cybersecurity.



TECHNICAL REQUIREMENTS:

- **Web development (front-end):** build a responsive, chat-like UI and consume data from an API.
- **Back-end / API:** implement a simple server with endpoints for scenarios, choices, scores, and reports.
- **Data structuring:** model scenarios and user results in JSON and/or a database and store them cleanly.
- **Scoring logic:** implement basic scoring (risk / policy compliance / resistance) and a simple results dashboard.

SKILLS TO BE DEVELOPED

- **Front-end skills**
- **Back-end skills**
- **Cybersecurity fundamentals:** understanding social engineering tactics and safe response procedures (verify out-of-band, report, escalation).
- **Data skills:** modeling scenarios and results, querying and structuring data cleanly.
- **Scoring & logic skills:** implementing rules/algorithms for risk, policy compliance, resistance, and weakness profiling.
- **Analytics skills:** calculating KPIs (accuracy, time-to-report, common mistakes) and presenting them in a dashboard.
- **Content engineering:** writing/structuring realistic scenarios with clear explanations and consistent tagging.