PURPOSE OF THE COMPETITION

Cyex Camp's University Decision Simulation (CTF+TTX) aims to provide a simulation environment in which students in higher education can learn about the technical and strategic challenges associated with cybersecurity, especially cyber incidents and try out related practical solutions. Cyex Camp contributes to the professional development of students and also serves as a forum for networking. Accordingly, participants will have the opportunity to meet other teams, mentors, jury members, and experts working in various parts of cybersecurity and other related fields.

The task of the competing teams is to develop solution proposals for different areas of cybersecurity (situation analysis, strategy development, incident management) based on a fictional scenario. In responding, teams need to consider the implications and contexts for the public and private sectors, even as they affect physical reality.

In the first part of the competition, the teams develop the necessary skills remotely (in their institution, at home, etc.) with the help of the team's coach and prepare for the competition. In the oral round of the competition, based on the professional feedback of the jury members, all participants will have the opportunity to improve their knowledge and develop their professional relationships. The final order between the teams is determined by the quality of the written operative and strategic responses as well as the decision-making proposals, the technical task solved, and the quality of the oral presentation.

SIGNIFICANCE OF THE COMPETITION RULES

All applicants must be familiar with the rules before entering the competition. As participants are assessed based on written qualification and subsequent oral assignments, a thorough knowledge of the rules is essential for successful participation.

CONTACT OF THE COMPETITION ORGANISERS

If you have any questions about the competition, please contact the organisers at the following contact details:

hello@cyex.camp

+3620/549 0816

RULES

Rule 1: Conditions of participation

All university student teams (higher vocational education, BSc, BA, MSc, MA, PhD, DLA), postgraduate, and postdoctoral program participants can apply to the competition. It is not mandatory to be involved in any specific cybersecurity training to participate in the competition. However, the organisers remind the competitors that knowledge of everyday issues and problems in this field increases the success of the participation in the competition; therefore, it is recommended that at least one member of the team have such knowledge, skills, and interests.

The organisers do not check compliance with the conditions of participation at Registration. However, proof of student status can be verified at any point.

The organisers do not provide financial support for the competitors to travel to the venue of the final round of the competition (except for V4 and Western Balkan countries). It is suggested that, if required, sending institutions to be asked to provide the necessary financial resources.

The competition is held in English, so knowledge of it is mandatory to participate.

By submitting the application form, each applicant automatically consents to the production of audio, images, and video during the competition and to the organisers sharing their data with the organiser partners for a maximum of one year to send job offers.

Rule 2: Ways of organising the competition

Due to the COVID 19 pandemic situation, the following two options are available for the competition:

- **Hybrid way:** The qualifying round (see Section 6.1) will be held online, while the live round will be held in person in Budapest. If a team is unable to attend in person due to current pandemic regulations, they will have the opportunity to join in the form of a video conference call as well. (Due to the nature of the competition, this has neither an advantage nor a disadvantage.) For remote joining, team members must submit a separate request. It is necessary to detail the current rules in the explanatory memorandum (referring to English). The request should be sent to **hello@cyex.camp** to the organisers. The Clerk of the Competition will consider absence. If the application does not stand, the team will be disqualified, and the next team in consolation will be entered into the live round.
- **Online**: The entire event (the qualifying and the live round) will be held online.

Along with notifying the advancing teams, the organisers will indicate how the event will be held based on current pandemic rules. However, they point out that they have no influence on the current national and international situation and accordingly reserve the right to change the method of organisation at any time. This includes the possibility that the live-action round of the competition will be held Online even though the Hybrid event has been announced at the qualification announcement. (This is not true backwards, that is, if the Online way was announced, the Hybrid version will certainly not be applied at a later date.)

Rule 3: Composition of teams

Each team consists of 3 students. There are no restrictions on the qualifications and experience of team members or the composition of the team. However, the organisers draw attention to the fact that in addition to the decision-making simulation during the competition, Capture the Flag (CTF) type Blue Team tasks must also be solved. Accordingly, it is recommended that at least one team member should be able to perform such tasks.

Team members do not have to study in the same institution. The organisers encourage participants to bring together students from different fields (e.g., technical, legal, policy, etc.) to think together about cyber security, as a collaboration between disciplines is paramount in real life.

Members do not have to come from the same country but must indicate a home country they represent. If a team comprises two members from the same country and the third member has a different home country, the given team's home country must indicate where the more members come from. If all three members represent different countries, they can decide which one to choose for their team's home country.

In addition, each team must provide a team coach (preferably selected from the sending institutions). The coach cannot be a member of the team or any other team. Although the coach's participation in the live round of the competition is not mandatory, their personal presence may be necessary for the team to receive all the help they need to perform successfully.

Each team must have a team name.

Rule 4: Registration

Students interested in the competition can register via the following link: **https://forms.gle/HFtXoYA84U8dYgrv5**

The application deadline is **October 1, 2021**, although the Clerk of the Competition may consider an application beyond the registration deadline.

Rule 5: Progress and notification

Successful registration and entry into the qualifying round are conditional on compliance with the rules for participation under *Rule 1:*. The Cybersecurity Report received from the teams in the qualification round will be evaluated by the jury based on a pre-defined, identical set of criteria.

A total of 16 teams can advance to the live semi-finals, proceed as follows:

- The best performing team from each nominated home country will advance.
- If the number of nominated home countries is less than 16, the remaining places will be filled. It no longer matters what home country the teams represent. In this case, only the scores will be taken into account by the organisers. The teams with the most points get into the top 16.

- If the number of nominated home countries exceeds 16, the organisers will rank the best performing teams from each country based on the score. The 16 best-performing teams will advance to the live semi-finals.
- In the case of point identity, the passage shall be as described in Rule 12:.
- Non-eligible teams will be comforted by the above set of rules due to the uncertainty of the pandemic situation. All teams will be notified of their placement in the consolation.

Each team will be notified via e-mail about their score in the qualifying round. For the advancing teams, the organisers will send an e-mail invitation to the oral round and other information related to the semi-final (e.g. modified scenario, technical tasks, etc.).

The four teams with the highest scores from the semi-finals will advance to the finals. In the case of equal scores, the passage shall be as described in Rule 12:. The organisers will announce the results at the competition venue or on the applied platform in case of the online organisation/participation. After the competition, each team will be informed about the results (scores given by the jury members, comments).

Rule 6: Rounds of the competition

A Cyex Camp's University Decision Simulation is based on a fictitious scenario published after the deadline of the Registration. According to the scenario, the teams act as a group of experts and advisers who prepare various written and oral reports for the decision-making management of the hypothetical organisation represented by the jury.

Based on the scenario, the teams must first react in writing to the situation (Qualification Round). In the later rounds, they have to adapt their proposals or perform new tasks to the changed, escalating scenario in the meantime to act successfully. The later rounds consist of a semi-final and a final. The tasks of the given round must be solved, taking into account the results achieved earlier.

The competition aims for teams to find the best course of action for the cybersecurity situation and present it to decision-makers. In developing the responses, the teams should rely strictly on the scenario published by the organisers and the documents appearing in the scenario (foreign and intelligence reports, articles, social network entries, etc.).

6.1. Qualification Round (written)

Teams are qualified based on a written Cybersecurity Report.

The organisers will present each team with the scenario and related documents containing the background. The scenario requires situation analysis and strategy-making tasks for an international company, for which teams must prepare a cybersecurity report. The report must be sent to the organisers by **9 October 2021** at **hello@cyex.camp**. Based on the scores obtained, as described in Rule 5:, 16 teams will be placed in the oral round of the competition. The organisers will notify the teams about the advance by **October 13, 2021**.

6.1.1. Cybersecurity Report

In the first round of the competition, the teams make a short note in a report that fulfils the tasks. The report should include a SWOT analysis and formulate a strategy. The report's length should not exceed **two pages** (A/4 format) using normal line spacing, Times New Roman font, size 12. It should include the name of the team, the members, and the coach.

The organisers encourage the teams to develop proposals for the current cybersecurity situation in addition to what is required. The aim of the competition is not to discuss a specific issue but rather to analyse and explain the proposals of the teams. Organisers encourage teams to come up with creative and unique solutions.

The use of graphs, figures, tables, and other graphical solutions is permitted, but must be included in the two-page size limit. Exceeding the size limit will result in a point deduction.

6.1.2. Technical Task

There is no technical (CTF) Blue Team task in the Qualification Round.

6.2.Semi-final (oral)

Following the announcement of the teams advancing from the Qualification Round, the original scenario will be supplemented and continued. It is up to the teams to react to the modified scenario and prepare for the oral round accordingly. Advancing teams will receive the new documents along with the notification. In addition, the organisers will give them technical (CTF) Blue Team tasks, which will provide additional information to the teams besides injects of the scenario. Using the information from the two sources (scenario + CTF results), teams should review previously produced outcome products and prepare a decision document and oral presentation for incident management.

At least the following questions must be answered related to the incident (if any): What happened? What data could be at risk? Is it necessary to notify customers and authorities?

In addition, threat intelligence needs to be implemented in connection with the incident.

The semi-final will take place on **November 12, 2021**. The teams that advance will be drawn into two sections (8-8 teams).

6.2.1. Decision-making Document

For the Semi-final round, the teams must prepare a Decision-making Document. The content should be adapted to the oral presentation. The document summarises the response alternatives, the related issues, the decision-making process, and suggestions.

The Decision-making Document should not exceed one page (A/4 format), but there is no other formal requirement. The use of graphs, figures, tables, and other graphical solutions is permitted but must be included in the scope limit. Exceeding the one page A/4 limit cannot be accepted and will result in automatic disqualification.

The Decision-making Document must send in **PDF format** to the organisers **by midnight (CET) on November 10, 2021** at hello@cyex.io.

6.2.2. Oral Report

The teams will give the Oral Report in a separate room in front of the jury.

Teams must present their solution proposals to the jury. The presentation should contain the discovered data and correlations and the solution that the given team expects as the best one. Teams should explain why the chosen solution is considered the best and detail the countermeasures required. Anything can be used in the oral round, except for presenting (e.g., PPT projection).

The procession of the presentation is as follows:

- The organisers give the Decision-making Document to the jury.
- The jury has 1 minute to study it.
- The team presents orally (without PPT or similar) without interrupting by the jury. (Max. 10 minutes)
- The team answers the jury's direct questions. (Max. 10 minutes)
- The jury will evaluate the performance of the team using the criteria at **Error! Reference source not found.**. In the case of a personal presence, the teams must leave the auditorium by the time of scoring. (Max 5 minutes)
- After scoring, the jury members give feedback to the teams. (Max. 7 minutes)

The teams that advance to the final will be selected based on the points achieved. The two teams from the two sections with the **most joint scores from the Qualification Round and the Semi-final** will advance to the final. The organisers will inform the teams on the spot about the fact of the advance.

6.3.Final (Oral round)

The Final will be held on the second day of the competition in front of the jury and the audience.

During the final, the events described in the original scenario escalate. Teams must respond to new information. The new injects will be delivered to the advanced teams at 7 pm (CET) on the day of the semi-finals. Based on the new information, the teams should continue to roll out the previous incident or respond to the new one(s), explicitly answering what happened and whether additional assets or persons involved are at risk. The implementation of threat intelligence is also required in the context of incident management.

During this time, an Oral Report should be prepared for the (new) jury. The team should present what happened about the incident(s) as well as the implementation of the incident(s) remediation. They should select the best solution and describe the exact steps proposed.

The teams that make it to the Final will be given extra technical (CTF) Blue Team tasks on the night between the two days of the live competition, which will help them get valuable information about the next day's Final.

The procession of the presentation is as follows:

- The team present orally (without PPT or similar) without interrupting by the jury. (Max. 10 minutes)
- The team answers the jury's direct questions. (Max. 10 minutes)
- The jury will evaluate the performance of the team using the criteria at **Error! Reference source not found.**. In the case of a personal presence, the teams must leave the auditorium by the time of scoring. (Max. 5 minutes)

Rule 7: Scenario-based competition

The competition focuses on cybersecurity incident(s) related to the operation of a fictitious organisation composed of several sources. In line with the purpose of the competition, teams must respond in writing and orally to the business, economic, social, environmental, and safety issues included in the scenario. In each round of the competition, the scenario and related tasks are published in such a way that all teams have an equal chance to prepare.

Rule 8: Authorised devices and cheating

During the presentation and jury questions, teams are not allowed to seek outside help; however, they may use any means (if they have time), e.g., to read their notes. The use of PPT or other similar presentations is not allowed in this round either.

Cheating (e.g., outside help) during the competition is not allowed, resulting in immediate disqualification. The organisers will notify the sending institutions of the teams excluded from the competition in all cases.

Rule 9: Jury

Each round of the competition will be evaluated by a jury of cybersecurity professionals (4-5 individuals) with expertise in different areas of cybersecurity and relevant knowledge of the scenario. The scoring is standardised to ensure equal opportunities, with judges evaluating teams' performance using pre-prepared criteria in **Error! Reference source not found.**. The members of the jury may vary from round to round.

Rule 10: Observers, media, and broadcasting

A limited number of observers may take part in the oral round of the semi-finals. During the competition, observers must not disturb or assist the competing teams, which the organisers pay special attention to.

The final is public to everyone, except finalist teams who have not yet finished their Oral Report. Coaches can decide whether or not to stick with their team when announcing the promotion. If so, they cannot stay at the final venue until it is their turn. Teams can join the Final's audience after presenting their report.

In the case of online participation/organisation, the participants of the waiting teams can join the competition only after the signal of the organisers.

The organisers of Cyex Camp reserve the right to broadcast a traditional or online program about the event, and media representatives may be present at the event. Ethical, responsible, and professional behaviour is expected of all participants (teams, observers, etc.). The organisers also reserve the right to record the entire competition when organising Online.

Rule 11: Timing

The organisers will ensure that the same timeframe available to each team and the judges are strictly adhered to during the competition. Teams are assisted by three signs during the oral presentation. The teams get the first sign at five, the second one at nine and the third at ten minutes. At the last signal, the team must finish the presentation even if it has not reached the end. Otherwise, exceeding the time limit will result in a point deduction. Adherence to the timeframe during the direct questions of the jury will be signalled in a similar way by the organisers.

Rule 12: Evaluation and scoring

Each team is evaluated equally by the jury in the Qualification Round based on five critical criteria:

- Interpretation of cybersecurity standards,
- Key issue recognition,
- Analysis of alternatives for responses,
- Structure and organisation,
- Originality and creativity.

In the Semi-final and the Final, in addition to the existing five points, the following sixth criteria will be taken into account:

- Use of information obtained from technical (CTF) tasks.

Judges may only use guidance on these aspects and the standard scorecard (**Error! Reference source not found.**) during the evaluation. The teams that advance will be determined by summing up the points.

In the event of equal scores, the teams' points will be evaluated and compared in the order indicated on the score sheet. The team that scores the first point in the doubles comparison by category will advance. For example, suppose Team A and B score 20-20 points and 6-6 points in the first category (Interpretation of cybersecurity standards) but in the second criteria (Key issue recognition Team A scores 4 points, and Team B scores only 3, then Team A will be ranked better.

The order between the teams in the Semi-final is formed by summing up the points obtained in the Qualification Round and the score obtained in the Semi-final.

After summing up the scores, the team with the 2-2 highest scores per section will advance to the Final. The ranking between the teams that made it to the finals is only based on the oral report presented in the Final round. There may be a tie between the four teams in the final. In this case, the final order will be decided by the jury members by secret ballot.

Each team receives unique, detailed feedback on their performance in the oral rounds, covering both the decision-making document and the oral presentation.

The jury will vote on the special prizes in several categories. These are made based on the results achieved in the Semi-final. Performance in the Final is not included in the evaluation of special prizes.

Rule 13: Participation as an observer after dropout

As the competition is open, all teams eliminated during the qualifiers have the opportunity to be present as observers in the oral rounds (Semi-final, Final). The organisers must be informed of the intention to participate by e-mail (hello@cyex.io) by **November 2, 2021**. The organisers encourage both eliminated and competing teams to take advantage of the networking opportunities offered by the competition.

Rule 14: Prizes

There is a prize pool of more than 3000€ to be distributed among the top three teams. The prizes that can be awarded to the winners can be extended after the announcement of the competition until the day before the final round. The organizers will always provide information about this through the official communication channels of the competition.

The organisers will issue a diploma to the teams participating in person at the oral rounds.

Rule 15: Notification of rule change and other information

The previous rules are for design purposes only. The organisers of Cyex Camp reserve the right to change competition rules depending on the current logistical and technical conditions. In case of a rule change, the organisers will notify the participating teams of the change and publish the updated rules on the official communication channels.

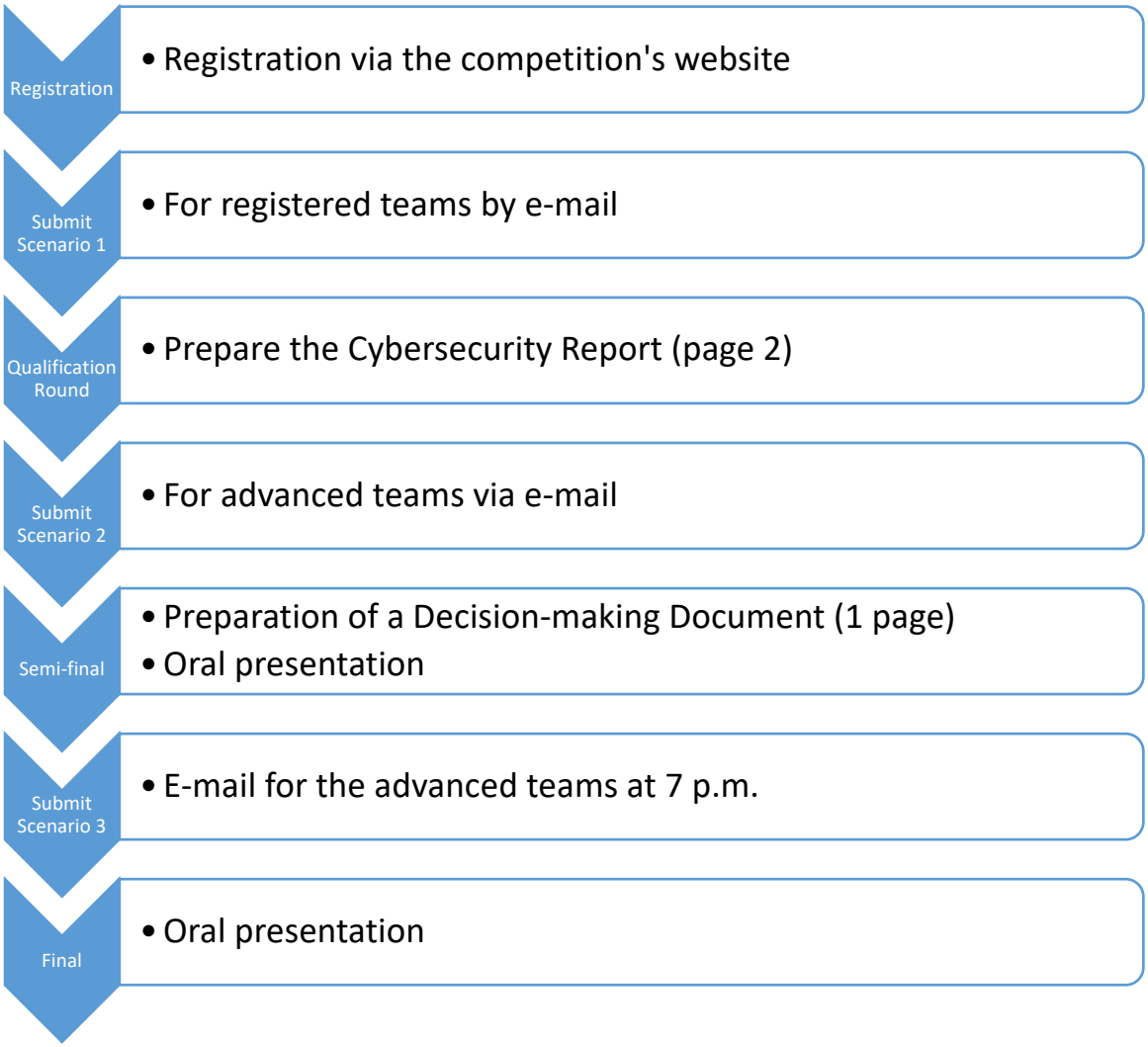
The teams are constantly informed about all the information and knowledge about the competition on the competition's Facebook page.

COMPETITION SUMMARY, IMPORTANT DATES

Important dates

Application deadline (Registration)	October 1, 2021 at midnight (CET)
Publish the Qualification Round scenario	October 1, 2021
Deadline for submission of qualification assignment	October 9, 2021
Semi-final notice	October 13, 2021
Observer application of teams that did not make it to the semi-finals but want to participate in the competition	November 2, 2021
Deadline for sending a Decision-making Document	November 10, 2021 at midnight (CET)
Semi-final	November 12, 2021
Final	November 13, 2021

Summary of the course of the competition



APPENDIX 1: PREPARATION AND SCORING CRITERIAS

Teams should consider the following during the preparation:

- **Do not fight against the scenario.** The information published must be considered accurate. The organisers call the teams' attention to focus their energy on the conclusions drawn from the scenario and not on considering the acceptability of the information.
- **Multi-dimensional approach.** When analysing the scenario, it is worth considering the different approaches of different organisations (e.g., private, military, diplomatic sector), and disciplines (e.g., legal, public policy, IT, cybersecurity).
- **Creativity.** Strategic decisions affecting cybersecurity result from an ongoing dialogue between actors in different sectors, so there is no proper response to the crisis situation in the scenario. There are a number of ideas to try out when designing responses.
- **Analysis of the issues is inevitable.** Teams need to address complex issues and find the best responses in decision-making by weighing the pros and cons of often conflicting interests.
- **Effectiveness.** In addition to analysing the situation, the goal is to develop and present an incident response with strategic alternatives to be implemented in a real cybersecurity incident.

Judging criteria

The jury will evaluate the written and oral performance of the teams based on the five plus one categories in the table below. In case of a question related to the judging criteria, the organisers of the competition are available.

Criterias	Guidelines
Interpretation of cybersecurity standards	**[7 points]** The team has an outstanding knowledge of cybersecurity norms (standards, best practices, etc.) and can identify all the actors involved and the tools that can be applied in detail.
	[4 points] The team has a general knowledge of cybersecurity norms (standards, best practices, etc.), and has identified, but not entirely, the appropriate actors and tools.
	[1 point] The team's knowledge of cybersecurity-related norms (standards, best practices, etc.) is limited.
Key issue recognition	**[7 points]** The team successfully identified and responded to the critical cybersecurity issues raised by the scenario.
	[4 points] The team recognised only a few conspicuous cybersecurity issues, or although it did recognise most of them, although it did not formulate responses to all of them.
	[1 point] The team drew attention to some general cybersecurity issues *and/or* focused on issues unrelated to the scenario.

Analysis of alternatives for responses	**[7 points]** The strategic alternatives proposed by the team actually respond to the scenario. The differences and trade-offs between the individual alternatives have been thoroughly analysed.
	[4 points] The strategic alternatives proposed by the team are only partially responsive or irrelevant to the scenario, *and/or* the analysis of each part is missing or not sufficiently substantiated.
	[1 point] The strategic alternatives proposed by the team are not relevant to the scenario or are not supported by adequate analysis, *and/or* the team failed to analyse the response alternatives.
Structure and organisation	**[7 points]** The team presented the responses effectively, clearly, and concisely and comprehensively communicated the analysis to help select the proposed alternative.
	[4 points] The team properly presented the proposed responses, but the presentation lacked a coherent analysis of the alternatives *and/or* lacked justification for the proposed alternative.
	[1 point] The team's presentation lacked coherence and conciseness, which hindered the effective presentation of alternatives.
Originality and creativity	**[7 points]** The team has developed an original, creative, and innovative solution proposal beyond established practices and literature.
	[4 points] The team approached the cybersecurity situation individually but relied too heavily on well-known solutions.
	[1 point] The team's efforts regarding the scenario came to a halt with the preparation materials provided by the organisers, conveying little originality.

Extra aspect in the semi-finals and finals:

Use of information obtained from technical (CTF) tasks	**[7 points]** The team made full use of the information contained in the technical (CTF) tasks in developing and presenting the alternatives.
	[4 points] The team partially used the information in the technical (CTF) tasks to develop and present the alternatives.
	[1 point] The team lacked the information in the technical (CTF) tasks when developing and presenting the alternatives.