The European Cyber Security Challenge: Lessons Learned report

VERSION 1.0
DECEMBER 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For media enquires about this paper, please use press@enisa.europa.eu.

Table of Contents

Executive Summary 4
1. Purpose of this document 5
2. Methodology 6
3. ECSC editions 7
3.1 ECSC 2014 7
3.2 ECSC 2015 8
3.3 ECSC 2016 8
4. Lessons Learned 9
4.1 Public relations and communication strategy 9
4.2 Budget and sponsorship 9
4.3 Challenge 9
1.1 Logistics 10
1.2 Conferences, job fair and social event 11
1.3 Jury and Steering Committee 11
1.4 Scalability 11
5. Recommendations 12
6. Suggested work packages 15

Executive Summary

Both the growing need for IT security professionals and skills shortage are widely acknowledged. To help solve this, multiple countries have initiated national cybersecurity competitions for students, security professionals and even non-IT professionals, all with a common goal: find cyber talents and encourage all of them to pursue a career in cybersecurity. The European Cyber Security Challenge (ECSC) builds upon these competitions adding a pan-European layer.

The ECSC is an initiative of multiple European countries supported by the European Union Agency for Network and Information Security (ENISA) that aims at engaging cybersecurity talent across Europe and connecting high potentials.

This report contains a detailed list of the lessons learned from previous ECSCs, of which the key takeaways are:

- The **quality of the ECSC** is crucial in meeting the participants' expectations. The scenario, stability and complexity of the platform used during the ECSC are key success factors in order to provide a challenging competition that attracts top cyber talent from all over Europe.
- **Public relations and communication activities** are key in order to meet the objectives on participation and sponsorship.
- The **event agenda should be tailored to the participants** needs and expectations, and include activities that relate to their interests and subject matter expertise.
- Given the current growth objectives of the ECSC (plus five countries per year), **solid back-office processes** regarding the organisation of the event are necessary to meet the rising quality expectations from stakeholders. This includes, amongst others, a proper governance structure with clear roles, responsibilities, decision-making, agreed-upon principles and rules with regard to fair play and transparency.
- **Sharing lessons learned and recommendations** between organisers and participating states is crucial in order to improve the quality of the event and implement best practices.

1. Purpose of this document

The European Cyber Security Challenge is gaining momentum and increasing in scale. In order to meet the rising quality expectations of all stakeholders, including participants, organisers and sponsors, the capacity and maturity of the ECSC organisation should increase accordingly.

In order to achieve the target maturity, exchanging lessons learned and recommendations is crucial. This document aims at listing the observations and improvement areas as captured during previous ECSCs and at providing guidance for future editions.

2. Methodology

Representative feedback has been captured from both organisers and participants by means of an online survey and stakeholder interviews. The objective of capturing this feedback was **to assess the overall experience** of the attendees and to identify strengths and opportunities for improvement.

The online survey contained both open and closed questions. Open questions encouraged the respondents to provide **qualitative feedback**, while the closed questions were included to obtain **quantitative feedback** that enabled comparison and statistical analysis.

Stakeholder interviews were held on behalf of ENISA prior to and during the ECSC2017 event. Multiple conference calls have been set up between previous ECSC organising States to discover key success factors and best practices. During the ECSC2017 event, **stakeholder interviews** were held to **grasp the overall experience** of the event and to capture any potential issues or improvement areas.

3. ECSC editions

The ECSC has been strongly influenced by an ENISA study on the status of cyber security competitions in the EU in November 2014[1]. This study assessed the current state with regard to objectives, mission and vision, and maturity of existing cyber security challenges.

Pre-existing national competitions (Austrian, Swiss, Spanish, Romanian, United Kingdom), and private challenges were part of the study. The feedback of multiple stakeholders from both private and public domains were captured and included in the report, resulting in a document that includes guidelines for "a pan-European cyber challenge competition".

The main conclusion of the study was that there was a fertile ground for the emergence of a European level challenge:

> ***"the importance of the European Commission's active involvement in getting on board policymakers in Member States, the expertise of the EU's cybersecurity agency, ENISA, in involving the best experts in the field and the responsibility of public and private stakeholders in understanding that the target is set very high and that they should engage to the best of their ability."***

The emergence of the ECSC was thus the result of private and public stakeholders committing to a common goal: to place cybersecurity at the service of humankind, with a view to promoting a peaceful society concerned with the preservation of democratic values, freedom of taught, dignity and critical thinking.

The abovementioned is one of the principles of the European Cyber Security Charter.

The following section gives an overview of all ECSC events until 2016.

3.1 ECSC 2014

The ECSC2014 event was the first of its kind and the initial pilot event; it took place from **3rd to 5th November 2014 in Fürstenfeld, Austria**. The finals took the form of a competition between teams from Austria, Germany and Switzerland, who competed against each other in different live challenges. After the event, the teams travelled to an awards ceremony at the **Museum of Military History in Vienna**, in the presence of politicians, economists and representatives of government bodies.

Figure 1 - ECSC 2014 Team Austria

The ECSC 2014 platform and challenges included several challenges such as an APT Network Forensic Challenge, Java Hash Collisions, HQL injections and License Key Circumventions.

[1] Cybersecurity competitions – the status in Europe, ENISA, November 2014. Retrieved from: here

3.2 ECSC 2015

The ECSC2015 event took place on 21 October in Switzerland. Six teams from six different countries (Austria, Germany, Spain, Romania, UK and Switzerland) attended the event. This edition marked also the involvement of ENISA in the project.

This year's competition saw a new format in which teams had to **fix security holes in software** applications while attacking other teams' assets.

Figure 2 - ECSC 2015 finalists

3.3 ECSC 2016

One hundred European cyber security talents, representing 10 EU Member States and EFTA countries, met in Düsseldorf for the ECSC2016 event from the 7th to the 9th of November.

All teams had to protect their own infrastructure while attacking that of the opposing teams, while deciphering hidden messages and solving hacking challenges.

Participants were able to meet and talk with representatives of academia

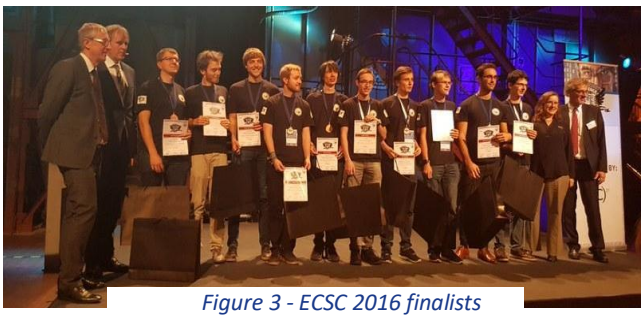

Figure 3 - ECSC 2016 finalists

4. Lessons Learned

The following lessons learned serve as guidelines for maintaining and increasing the quality of the ECSC with regard to logistics, technical challenges, communication, scalability, accommodation and budget.

4.1 Public relations and communication strategy

- Since **creating awareness about the event is ke**y to stimulate the scaling of the Challenge, national organisers, participating teams and ENISA should define and execute a consistent and optimised communication strategy in order to meet its full potential.
- The **potential of social media should be leveraged** to obtain maximum exposure amongst the target audience and the cybersecurity community.
- A **PR timeline** supports this objective by defining dates, channels and messages. The timeline implies a consistent timing of the publication of posts across multiple channels.
- A cross-country PR timeline should be established in collaboration with all participating States and ENISA to maximise exposure and visibility by **maintaining coherence in the communication strategy**.

4.2 Budget and sponsorship

- The national organisers of the previous ECSCs and the ECSC Steering Committee stress that **external sponsorship is key to funding the event**.
- The national organisers of previous challenges have received significant funding from both private and public partners. The organisations experienced a very proactive attitude from private organisations towards offering funding. This is the result of **proactive communication** about the challenge and informing the industry of **the benefits of a potential sponsorship**.
- In order to establish an attractive climate for investors, the national organisers established a sponsorship scheme that results in different benefits according to the funding amount. For example:
- **Gold sponsorship** (full exposure, access to talent, additional marketing and advertising opportunities)
- **Silver sponsorship** (medium exposure, access to talent)
- **Bronze sponsorship** (limited exposure)
- Sponsors that obtain access to talent should tailor their presence to the expectations of the audience. **Traditional "HR booths" do not appeal to cyber security talent.** The sponsors should be encouraged to **explore innovative and non-conventional ways** to interact with participants. This will result in a high return-on-investment from the sponsors' perspective, and a high satisfaction rate from the participants' perspective.
- Sponsors that provide conferences or presentations should tailor the content to the target audience.

4.3 Challenge

Design

- Participants expect a challenge that is encouraging them to push their limits and expect to face situations that involve multiple aspects of cybersecurity such as capture-the-flags (CTF) and jeopardy.
- The design of the technical challenges should **reflect a reasonable learning curve in accordance with the level of the participants**. The design should anticipate a divergent level of expertise by involving self-contained steps and real-time feedback in order to support contestants to reach the next steps.
- **The challenges should reflect real-life scenarios** that prepare the participants for their future career.

- The technical **infrastructure of the challenge should be secure and resilient** in order to guarantee availability during the competition. A loss of availability of the challenge platform drastically affects the overall experience.
- The **scoring mechanism should be transparent** with regard to attribution and distribution of points over the challenge.
- The challenge design should aim at **maximizing the interaction between the teams** in order to stimulate the competitive aspect of the challenge.
- The design of the challenges should also take into account the continuous growth of the competition.

Service providers

- The service providers should guarantee the functionality and security of the challenge platforms and supporting systems.
- The service providers should foresee measures in order to prevent, detect and respond to any incidents that could impact the availability and integrity of their systems. This includes, but is not limited to testing of infrastructure and platform and setting up back-up infrastructure.
- The service providers should provide adequate support during the competition to participants and organisers in case of incidents in order to safeguard the continuity of the competition.
- The host and the ECSC Steering Committee should closely follow-up with the service providers on the progress of the platform development and deployment in order to detect, prevent and respond to events that might affect the delivery of the platform.

Rules

- The **rules should be clear**, unambiguous and agreed-upon by all participating countries.
- **Clear communication about the rules** to the teams is key to ensure the fairness of the competition.
- **Compliance to the rules should be monitored** and taken into account in order to avoid malicious activities such as cheating or unfair competition.
- **Amendments to the rules should be backed-up by reasonable argumentation** and discussed during the Steering Committee meetings at the earliest convenience.

Presentations

- **The presentations held by the participants as part of the Challenge should be aligned with the objectives of the challenge with regard to building expertise.**
- **Clear guidelines on the practicalities** such as the submission should be provided from the Jury and organisers to the participants.

4.4 Logistics

- The **location should be determined taking into account the overall connectivity and infrastructural capacity**. The selected venue and city should be able to provide accommodation capacity, reliable and qualitative infrastructure, as well as efficient accessibility for participating teams from all over Europe.
- Selecting the accommodation and **location of events should reflect – and be tailored to – the preferences of the participants**.
- Taking into account the satisfaction of the sponsors in terms of exposure to talent, the **location should also consider the student and talent population within the region**. Having multiple universities is an asset that positively influences the exposure of private organisations towards students, and stimulates the attendance rate to the side conference and job fair.
- Should a national organiser believe the ECSC date should be rescheduled, this should be formally brought up in a timely manner to the complete ECSC group to avoid overlap or conflicts with other national initiatives.

- In general, **the earliest time to organise the ECSC event is October**. Any deviation from the original planning should be discussed and decided upon with the formal input of all the members of the ECSC organisation.
- **When unforeseen logistical problems arise, the participants and organisers should be informed immediately.**

4.5 Conferences, job fair and social event

- Although cybersecurity puzzles are the focus of the event, activities such as the conferences, job fair and social event add value to the ECSC. **The link between these events and the actual challenge should be established and these activities should be embedded in the event**.
- The ECSC should not be seen as another traditional cyber security conference, but rather focuses on the potential added value of the challenge where **top cyber security talent from Europe are invited to compete**, collaborate, meet and network with private sector organisations.
- **The social event agenda and activities should reflect the interests of the participants.**
- The **conferences should be tailored to the target audience** and add value to the development of technical knowledge.
- **The job fair and recruiting activities should be embedded and aligned with the actual conference.** Traditional "booth job fairs" should be reconsidered as they have limited effect on participants. The involved private organisations should be encouraged to propose innovative and non–conventional recruiting activities.

4.6 Jury and Steering Committee

- **The Steering Committee should focus on its main function of being a decision making body that serves the improvement of the ECSC**. The efficiency of the Steering Committee is crucial in order to implement recommendations and increase the maturity and capacity of the event.
- **The Steering Committee meetings should be highly effective and have a clear and agreed-upon agenda** that is strictly followed to ensure all topics are covered and timing is respected.
- **Decisions taken by the Steering Committee should be logged in a decision-making register** that allows for reference in following meetings. This logbook will contain information about decisions, owners and actions.
- **The Steering Committee meetings should not reflect upon already taken decisions.** Should certain points require further discussion, this should be communicated to the Secretariat in advance.
- **The Jury should be transparent about its decision towards participants and organisers**.
- The role of an independent jury and referees should be considered.

4.7 Scalability

- When organising the European Cyber Security Challenge, **national organisers should consider the scalability aspects of the event**. The ultimate goal of the ECSC is to grow and expand every year with regard to quantity and quality.
- **Establishing a robust framework that includes a clear governance structure, marketing and communications plan, and other organisational, planning and logistic support is necessary to enable the ECSC to scale towards the future.**
- The goal is to **formalise the key decisions in a structured way**, leading to a framework that reduces the organisational efforts in the planning and organising of future ECSC events.

5. Recommendations

The following recommendations serve as guidelines for maintaining and increasing the quality of the ECSC based on the lessons learned as described in the previous chapter[4].

Organisation team (ECSC hosting country)

- **The national organiser should establish a dedicated team to organise the ECSC.** The team should describe clear roles and responsibilities in order to facilitate the correct ownership of tasks and project management. The team can consist of members of the national organisation body and external consultants or volunteers.
- **The organisation team should be in close contact with the pan-European ECSC community** to ensure the implementation of best practices and a coherent communication strategy.
- The host should be in close contact with the ECSC Steering Committee and ENISA during the implementation of the project. **Transparent status reporting is crucial**.

Attending countries

- The **hosts for future editions should be established well in advance** in order to facilitate proper planning and budgeting.
- **Countries interested in attending the challenge should be given the opportunity to announce their intention at least one year prior to the event.**
- **The scope of the challenge in terms of attending countries should be defined** (European vs EU+EFTA).
- All countries should ensure that in addition to their team's players a number of additional (or backup) team members are chosen and also trained in order to take care of unforeseen events.

Public relations and communication strategy

- **Establish a common public relations and communications strategy**, including social media, to ensure a consistent approach across all participating States and achieve maximum exposure and visibility.
- **Encourage and incentivise participants' social media engagement** with the #ECSC20XX tag.
- **Capture, analyse and share online communication statistics** in order to strengthen the ECSC business case and attract sponsors.

Budget and sponsorship

- **Establish an attractive sponsoring scheme for private organisations.** The sponsoring scheme should ideally provide multiple levels of sponsorship based on the amount of funding to stimulate substantial contributions.
- **Reach out to national government and public organisations** to promote the event and potentially obtain sponsorship and leadership commitment.
- **Consider the potential of entry fees** for non-participants for the conference, job fair and spectating.

Challenge

- **Ensure the stability and security of the platform during the challenge** and take into account any unforeseen circumstances that might affect the continuity of the event. This includes regular and adequate testing by the service provider to build capacity to prevent, detect and respond to incidents.

- **Achieve a challenge design that meets the requirements** as set out in the ECSC curricula that takes the expectations of the participants into account.
- **Be transparent about any decisions made by the Steering Committee** or organisers that could affect the course of the challenge.
- **Clearly communicate the rules and agreements to participants on beforehand to avoid any ambiguity or misunderstanding.**
- **Clearly communicate the agreements and expectations with regard to the presentations**. The content of the presentations should meet the expectations of the participants.
- **Perform a capacity and quality assessment of the platform service provider** in order to ensure the ability to meet the requirements and expectations of the ECSC.

Logistics

- **Determine the challenge venue by taking into account the overall connectivity**, mobility and infrastructural capacity. The selected venue should be accessible in a comfortable manner by the participating teams all over Europe.
- **Decorate the venue to reflect the activity of the event and meet the participants' interests**.
- **Transparently communicate unforeseen events with regard to logistics to the participants and organisers.**

Conferences, job fair and social event

- Identify and engage with speakers and panellists for the conferences that reflect the interests of the participants. **The conferences should be tailored to the target audience** and relate to their interests.
- **Integrate the conferences in the ECSC** so it is not perceived as a necessary side event but rather an integral part of the overall experience. The conferences should add value to the technical expertise of the participants rather than promote products, services or organisations.
- **Ensure a clear link between the cybersecurity challenge and the content of the conferences** and social event. These activities should appeal to the participants.
- **Encourage private organisations to propose innovative and non-conventional job fair formats** that appeal to the participants. Focus on the mutual benefit for both organisations and students.

Jury and Steering Committee

- **Define a clear agenda for every Steering Committee** and avoid any deviation from the foreseen timeframe in order to avoid delays and maintain efficient decision-making.
- **Capture and document all decisions made during the Steering Committee meetings, including decisions, actions and owners, in a decision-making log.**
- **Transparently communicate the decisions made by the Steering Committee** to all relevant stakeholders including participants and organisers.
- **Appoint a single point of contact (SPOC) of the platform and service providers to represent the provider during the ECSC event**. This SPOC could join the Steering Committee in case an incident occurs or a representative of the service provider is required.

Scalability

- **The national organiser should adequately document the activities related to the organisation of the European Cyber Security Challenge** in order to optimise the process for the following editions.
- In order to scale the event, improving the maturity of the organisation process is crucial. The first step in improving the maturity is to **document all steps leading to a successful event**. This documentation stimulates a debate between national organisers, and the exchange of best practices.
- **All relevant working documents and project management tools should be shared amongst the national organisers to optimise the process.** The intention is to formalise the key decisions in structured way, leading to a framework that reduces the organisational efforts in the planning and organising of future ECSC events.

6. Suggested work packages

The abovementioned lessons learned describe critical success factors and areas of improvement are translated into suggested work packages in this section. The work packages indicate the recommendations, implementation actions, owner and timeframe. These packages enable a clear view on open action points in order to increase the maturity of ECSC.

Title	
Organisation team	
Number	**Owner**
1	ECSC National organiser
Recommendations	

- The national organiser should establish a dedicated team to organise the ECSC. The team should describe clear roles and responsibilities in order to facilitate the correct ownership of tasks and project management. The team can consist of members of the national organisation body and external consultants or volunteers.
- The organisation team should be in close contact with the pan-European ECSC community to ensure the implementation of best practices and a coherent communication strategy.

Timeframe	**Implementation actions**
1 year before next ECSC	• Establish an ECSC project governance model including clear roles and responsibilities. • Assess the need for external human resources. • Engage with pan-European ECSC community.

Title	
Attending countries	
Number	**Owner**
2	ECSC National organiser
Recommendations	

- The hosts for future editions should be established well in advance in order to facilitate proper planning and budgeting.
- Countries interested in attending the challenge should be given the opportunity to announce their intention at least one year prior to the event.
- The scope of the challenge in terms of attending countries should be defined (European vs EU+EFTA).

Timeframe	**Implementation actions**
1 year before next ECSC	• Establish a formal ECSC project plan. • Assess potential participating Member States. • Establish a ECSC attendance scope

Title	
Rules	
Number	**Owner**
3	ECSC National organiser
Recommendations	

- Rules concerning the content of the challenge should be established prior to each edition. Any changes to these rules should be made by the Steering Committee and should enter into force as of the next edition.

Timeframe	Implementation actions
1 year before next ECSC	• Establish an ECSC project governance model including clear roles and responsibilities. • Assess the need for external human resources. • Engage with pan-European ECSC community.

Title	
Budget and sponsorship	
Number	**Owner**
4	ECSC National organiser
Recommendations	

- The national organisers of the previous ECSCs and Steering Committee stress that external sponsorship is key to funding the event.
- The national organisers of previous challenges have received significant funding from both private and public partners. The organisations experienced a very reactive attitude from private organisations towards offering funding. This is the result of proactive communication about the challenge and informing the industry of the benefits of a potential sponsorship.
- In order to establish an attractive climate for investors, the national organisers established a sponsorship scheme that results in different benefits according to the funding amount. For example:
    1) **Gold sponsorship** (full exposure, access to talent, additional marketing and advertising opportunities)
    2) **Silver sponsorship** (medium exposure, access to talent)
    3) **Bronze sponsorship** (limited exposure)
- Sponsors that obtain access to talent should tailor their presence to the expectations of the audience. Traditional "HR boots" do not appeal to cyber security talent. The sponsors should be encouraged to explore innovative and non-conventional ways to interact with the talent. This will result in a high return-on-investment from the sponsors' perspective, and a high satisfaction rate from the participants' perspective.
- Sponsors that provide conferences or presentations should tailor the content to the target audience.

Timeframe	Implementation actions
1 year before next ECSC	• Establish an attractive sponsoring scheme for private organisations. The sponsoring scheme should ideally provide multiple levels of sponsorship based on the amount of funding to stimulate substantial contributions. • Reach out to national government and public organisations to promote the event and potentially obtain sponsorship and leadership commitment. • Consider the potential of entry fees for non-participants for the conference, job fair and spectating.

Title	
Challenge	
Number	**Owner**
5	ECSC National organiser
Recommendations	

- Ensure the stability and security of the platform during the challenge and take into account any unforeseen circumstances that might affect the continuity of the event. This includes regular and adequate testing by the service provider to build capacity to prevent, detect and respond to incidents.
- Achieve a challenge design that meets the requirements as set out in the ECSC curricula that takes the expectations of the participants into account.
- Be transparent about any decisions made by the Steering Committee or organisers that could affect the course of the challenge.
- Clearly communicate the rules and agreements to participants on beforehand to avoid any ambiguity or misunderstanding.
- Clearly communicate the agreements and expectations with regard to the presentations. The content of the presentations should meet the expectations of the participants.
- Perform a capacity and quality assessment of the platform service provider in order to ensure the ability to meet the requirements and expectations of the ECSC.

Timeframe	Implementation actions
1 year before next ECSC	• Assess the features and properties of the ECSC challenge platform according to the ECSC Curriculum. • Identify and contact ECSC challenge (CTF) platform providers. • Ensure the platform provider can meet the quality standards of ECSC in order to guarantee the continuity and security of the platform. • Closely follow-up with the platform provider during the platform deployment. • Establish a scoring scheme. • Raise the scoring scheme to the Steering Committee for approval.

Title	
Scalability	
Number	**Owner**
6	ECSC National organiser
Recommendations	

- The national organiser should adequately document the activities related to the organisation of the European Cyber Security Challenge in order to optimise the process for the following editions.
- In order to scale the event, improving the maturity of the organisation process is crucial. The first step in improving the maturity is to document all steps leading to a successful event. This documentation stimulates a debate between national organisers, and the exchange of best practices.
- All relevant working documents and project management tools should be shared amongst the national organisers to optimise the process. The intention is to formalise the key decisions in structured way, leading to a framework that reduces the organisational efforts in the planning and organising of future ECSC events.

Timeframe	Implementation actions
1 year before next ECSC	• Assess lessons learned from previous ECSC challenges. • Establish a knowledge management team collaboration environment to store ECSC documentation. • Identify and document ECSC organising processes. • Document lessons learned and opportunities for improvement. • Share lessons learned and opportunities for improvement with the ECSC stakeholder group.

Title	
Public relations and communication strategy	
Number	**Owner**
7	ECSC National organiser
Recommendations	

- Since creating awareness about the event is key to stimulate the scaling of the Challenge, national organisers, participating teams and ENISA should execute a consistent and optimised communication strategy in order to meet its full potential.
- The potential of social media should be leveraged to obtain maximum exposure amongst the target audience and the cybersecurity community.
- A PR timeline supports this objective by defining dates, channels and messages. The timeline implies a consistent timing of the publication of posts across multiple channels.
- A cross-Country PR timeline should be established in collaboration with all participating States and ENISA to maximise exposure and visibility by maintaining coherence in the communication strategy.

Timeframe	Implementation actions
1 year before next ECSC	• Establish a common public relations and communications strategy, including social media, to ensure a consistent approach across all participating States and achieve maximum exposure and visibility. • Encourage and incentivise participants' social media engagement with the #ECSC20XX-tag. • Capture, analyse and share online communication statistics in order to strengthen the ECSC business case and attract sponsors.

Title	
Conferences, job fair and social event	
Number	**Owner**
8	ECSC National organiser

Recommendations

- Although cybersecurity puzzles are the focus of the event, activities such as the conferences, job fair and social event add value to the ECSC. The link between these events and the actual challenge should be established and these activities should be embedded in the event.
- The ECSC should not be seen as another traditional cyber security conference, but rather focuses on the potential added value of the challenge where top cyber security talent from Europe are invited to compete, collaborate, meet and network with private sector organisations.
- The social event agenda and activities should reflect the interests of the participants.
- The conferences should be tailored to the target audience and add value to the development of technical knowledge.
- The job fair and recruiting activities should be embedded and aligned with the actual conference. Traditional "booth job fairs" should be reconsidered as they have limited effect on participants. The involved private organisations should be encouraged to propose innovative and non–conventional recruiting activities.

Timeframe	Implementation actions
1 year before next ECSC	• Identify and engage with speakers and panellists for the conferences that reflect the interests of the participants. The conferences should be tailored to the target audience and relate to their interests. • Integrate the conferences in the ECSC so it is not perceived as a necessary side event but rather an integral part of the overall experience. The conferences should add value to the technical expertise of the participants rather than promote products, services or organisations. • Ensure a clear link between the cybersecurity challenge and the content of the conferences and social event. These activities should appeal to the participants. • Encourage private organisations to propose innovative and non-conventional job fair formats that appeal to the participants. Focus on the mutual benefit for both organisations and students.

Title	
Jury and Steering Committee	
Number	**Owner**
9	ECSC National organiser

Recommendations

- The Steering Committee should focus on its main function of being a decision making that serves the improvement of the ECSC. The efficiency of the Steering Committee is crucial in order to implement recommendations and increase the maturity and capacity of the event.
- The Steering Committee meetings should be highly effective and have a clear and agreed-upon agenda that is strictly followed to ensure all topics are covered and timing is respected.
- Decisions taken by the Steering Committee should be logged in a decision-making register that allows for reference in following meetings. This logbook will contain information about decisions, owners and actions.
- The Steering Committee meetings should not reflect upon already taken decisions. Should certain points require further discussion, this should be communicated to the Secretariat in advance.
- The Jury should be transparent about its decision towards participants and organisers.

Timeframe	Implementation actions
1 year before next ECSC	• Define a clear agenda for every Steering Committee and avoid any deviation from the foreseen timeframe in order to avoid delays and maintain efficient decision-making. • Capture and document all decisions made during the Steering Committee meetings, including decisions, actions and owners, in a decision-making log. • Transparently communicate the decisions made by the Steering Committee to all relevant stakeholders including participants and organisers. • Appoint a single point of contact (SPOC) of the platform provider to represent the provider during the ECSC event. This SPOC could join the Steering Committee in case an incident occurs or a representative of the service provider is required.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu