enisa

EUROPEAN CYBER SECURITY CHALLENGE

LONDON, UNITED KINGDOM 2018

ECSC 2018 Analysis Report

DECEMBER 2018

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 queries in relation to this paper, please use ecsc@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

We would like to thank our colleagues at Cyber Security challenge UK for taking care of all local logistics for the organisation of ECSC'2018 and in particular Ms. Debbie Tunstall and the colleagues at BT that provided the technical support throughout the event.

Our gratitude is also extended to our colleagues Razvan Gavrila and Adrien Ogee for their contributions to the success of the European Cyber Security Challenge. Finally, we would to thank all our colleagues' responsible for the national competitions and the preparation of the teams that participate at the ECSC. Without their untiring efforts this competition will not be possible.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Table of Contents

Executive Summary

The 5th Edition of the European Cyber Security Challenge, ECSC2018 was hosted in London during 14th to 17th October. The event was organised by the Cyber Security Challenge UK at the Tobacco Dock, an iconic grade one listed building which has a rich history. The event was hosted together with the job fair Cyber Re:coded.

Each country was represented at the ECSC final by a team of 10 contestants, comprised of the winners of the national competition. Half of the team members are within the range of ages of 14-20 years old and half in the 21-25 range. In total, 200 people (contestants, coaches and judges) representing 17 EU and EFTA countries (Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Greece, Italy, Liechtenstein, Norway, Romania, Spain, Switzerland, and United Kingdom) competed in the ECSC final in London. The participants investigated vulnerabilities in web applications, binaries and document files, solved crypto puzzles and hacked hardware systems. However, technical skills are just one part of the whole story. Teamwork and presentation skills were also evaluated. The complete skillset which is important for working in an IT security team, is thus tested. The finalists of ECSC 2018 were the teams from Germany, France and UK.

ENISA is currently hosting different platforms and performing different activities to support the European Cyber Security Challenge hosting country and the evolution of the project, this includes among others: ECSC main website, ECSC planning platform, public affairs strategy, challenges creation, governance framework of the competition, secretariat support, etc…

In order to ensure appropriate and transparent reporting to the Steering Committee ENISA, the following key observations were made by independent third-party observers that have attended the ECSC planning meetings and the actual event. These observations have been produced based on the feedback collected from participants, members of the ECSC Jury, members of the ECSC Steering Committee, and attendees to the event. In addition, these observations reflect the feedback provided by organisers and participants collected by an online evaluation survey:

- The venue, accommodation and logistics provided by Cyberchallenge UK has been very well received by participants. The venue was very well aligned with the theme of the challenge and provided for adequate facilities to support the event.
- The technical infrastructure supporting the challenge has significantly improved as compared to ECSC2017. The service providers contracted by Cyberchallenge UK delivered a relatively stable, state-of-the-art and reliable infrastructure. Some opportunities for improvement have been noted, but overall the user experience was positive. Some infrastructure challenges have affected the course of specific individual challenges (e.g. King of the hill, Capture The Flag), which is a key lesson learned to take into account in future editions.
- The platform developed by ENISA to support the challenges in the format of contracts was received well by the participants and organisers as it facilitates a real-time scoreboard that is also accessible to the public over the ECSC website (www.ecsc.eu).
- The Public Affairs activities conducted by the national teams, the organisers and ENISA have gained significantly in exposure, reach and engagement. To put things in perspective: #ECSC2017 had a total estimated social media reach of 199 913, compared to 5 062 457 for #ECSC2018.
- Exposure towards traditional press and media, as well as potential sponsors, national representatives, and private entities has significantly increased. ECSC2018 welcomed several political representatives of EU Member States thereby supporting the objective of bringing

nationalities together and foster a pan-European spirit in the realm of the European Cyber Security Challenge.

The 2019 edition of the European Cyber Security Challenge will take place in Bucharest Romania, in October 2019.

1. Introduction

The growing need for IT security professionals is widely acknowledged at European level. To help mitigate this shortage of skills, many countries launched national cyber security competitions addressed towards students, university graduates or even non-ICT professionals with a clear aim:

'Identify new and young cyber talents and encourage young people to pursue a career in cyber security.'

The European Cyber Security Challenge (ECSC) https://www.europeancybersecuritychallenge.eu/ leverages on these competitions by adding a pan-European layer. Top cyber talents from each participating country meet to network and collaborate and finally compete against each other. Contestants are challenged in solving security related tasks from domains such as web security, mobile security, crypto puzzles, reverse engineering and forensics and in the process collect points for solving them.

In a nutshell, ECSC is the annual European event that brings together young talent from across Europe to have fun and compete in cyber security. Its main aim is to highlight the importance of the national competition.

1.1 ECSC Background

The project was initiated under the umbrella of the EU Cyber Security Strategy (Feb 2013):

'The European Commission will organise, with the support of ENISA, a cybersecurity Championship in 2014, where university students will compete in proposing NIS solutions.'

As of 2014, ENISA has been supporting the organisation of the ECSC. ENISA is actively organising the meetings of the governance structures, supporting the development of the competition rules and games and it is also part of the ECSC Jury. As of 2016, ENISA is the acting secretariat of the ESCS Steering Committee.

In 2017, 15 countries attended (Austria, Cyprus, Czech Republic, Denmark, Estonia, Germany, Greece, Ireland, Italy, Liechtenstein, Norway, Romania, Spain, Switzerland and United Kingdom). The ECSC2017 took place between the 31st and 2nd November in Malaga, Spain. The winner of the final was Spain.

In the edition of 2018, held during 15-17 October 2018, 200 people (contestants, coaches and judges) representing 17 EU and EFTA countries (Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Greece, Italy, Liechtenstein, Norway, Romania, Spain, Switzerland, and United Kingdom) competed in the ECSC final at London. The participants investigated vulnerabilities in web applications, binaries and document files, solved crypto puzzles and hack hardware systems. However, technical skills are just one part of the whole story. As time and resources were limited, teamwork and presentation skills were also evaluated. The complete skillset which is important for working in an IT security team, is thus tested. The finalist of ECSC 2018 were the teams from Germany, France and UK. By 2020, ENISA expects to have more than 25 countries involved in the ECSC.

The 2019 edition of the European Cyber Security Challenge will take place Bucharest Romania, in October 2019.

1.2 ECSC Setup

Each country is represented at the ECSC final by a team of 10 contestants, comprised by the winners of the national round. Half of them are within the range of ages of 14-20 years old and half in the 21-25 range.

Two preparatory pilot phases of ECSC have been held in 2014 (in Austria) and 2015 (in Switzerland) with attendance by 3 and 6 countries, respectively. Since 2015, ENISA is lending its experience and position to coordinate and organise the ECSC effort to reach its full maturity by 2020.

The activities of the ECSC are supervised by a Steering Committee, composed of representatives of the attending countries. ENISA facilitates the meetings of this group and provides strategic guidance. The decision making processes are described in the ECSC Charter, which is approved every year.

ENISA is currently hosting different platforms and performing different activities to support the European Cyber Security Challenge hosting country and the evolution of the project, this includes among others: the ECSC main website, the ECSC planning platform, the public affairs strategy, challenges creation, etc…

In addition, ENISA is working closely with the host of each edition, in order to ensure appropriate and transparent reporting to the Steering Committee.

During the year, two Steering Committee meetings are held prior the execution of the event:

- Initial Planning Conference (IPC) was held in Brussels, 1st of March in DG Connect
- Main Planning Conference (MPC), held in Athens (ENISA premises) during 19th-20th June

ENISA organised these preparatory events and was overall responsible for the efficient running of the project, including meetings minutes and the follow-up of the proposed actions.

2. ECSC Attendance Evolution

From the first edition of the ECSC in 2014 the evolution of the attendant's countries has been the following:

- 2014 [3]: Austria, Germany, Switzerland
- 2015 [6]: Austria, Germany, Switzerland, Spain, Romania, United Kingdom
- 2016 [10]: Austria, Estonia, Germany, Greece, Ireland, Liechtenstein, Romania, Spain, Switzerland, United Kingdom
- 2017 [15]: Austria, Cyprus, Czech Republic, Denmark, Estonia, Germany, Greece, Ireland, Italy, Liechtenstein, Norway, Romania, Spain, Switzerland, United Kingdom
- 2018 [17]: Austria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Italy, Liechtenstein, Norway, Poland, Romania, Spain, Switzerland, United Kingdom

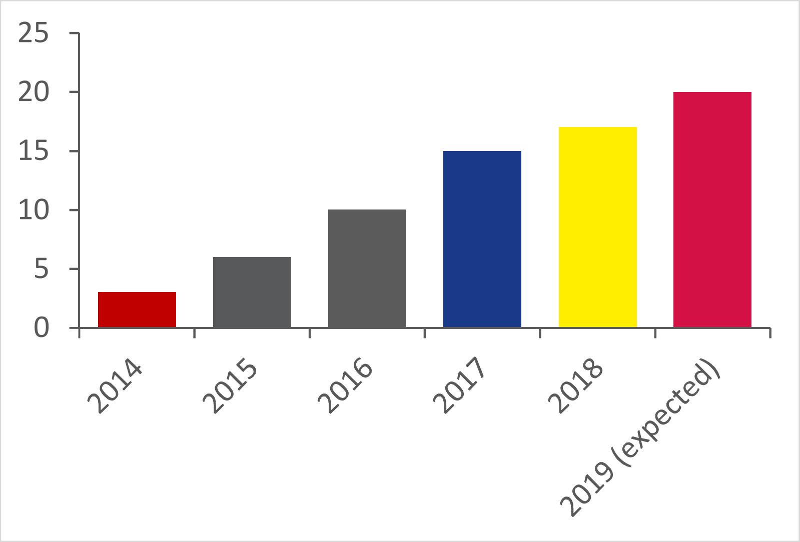


Figure 1: ECSC Attendance evolution

3. ECSC 2018 hosting country

The 5th Edition of the European Cyber Security Challenge, ECSC2018 was hosted in London during 14th to 17th October. The event was organised by the Cyber Security Challenge UK at the Tobacco Dock, an iconic grade one listed building which has a rich history. The event was hosted together with the job fair Cyber Re:coded.

The organization provided different useful information about how to get to the event from the selected hotel and the different facilities provided during the execution of the competition. Also, different activities were performed for the participants:

- Sunday 14th Oct : Welcome dinner and presentation of the teams
- Monday 15th Oct: Dinner in London with some of the teams
- Tuesday 16th Oct: ECSC Competition Closing Party at London's newest rooftop bar
- Wednesday 17th Oct: Awards Dinner and Presentations on the River Thames, aboard Riverboat

EUROPEAN CYBER SECURITY CHALLENGE 2018
CONGRATULATIONS TO TEAM GERMANY

Figure 2 ECSC 2018 Winning team - Award ceremony

4. ENISA Contribution to ECSC2018

4.1 Steering Committee Management

The activities of the ECSC are supervised by a Steering Committee, made out of representatives of the attending countries. ENISA facilitates the meetings of this groups and provides strategic guidance. The decision making processes are described in the ECSC Charter, which is approved every year.

During the preparation of ECSC 2018, ENISA was responsible for the following activities related with the management of the Steering Committee:

- Planning Platform maintenance and update
- Mail list management
- Organization of the IPC in Brussels
- Organization of the MPC in Athens
- Hot wash meeting after the execution of the competition in London
- Feedback collection: Lessons learnt report and surveys to the participants

4.2 Jury Management

A jury body was established during the competition: A jury member is appointed from each of the members of the ECSC's Steering Committee, once this is set, it will resolve any dispute during the competition.

The following improvements were implemented this year:

1. A "Jury guidelines" document was created, summing up the most important points to take in to account. The Jury members and captains from all teams could use this document as a reference.
2. Jury meetings were scheduled at regular intervals in order to improve the efficiency of the competition: Jury members meet at predefined times during the competition to discuss and resolve complaints and queries received during the period in between two jury meetings. Also, a framework was created in the case an "extraordinary jury meeting" was necessary for issues that may affect severely the running of the competition.
3. Creation of a Jury coordinator role: In charge of acting as a PoC, receiving and collecting complains from participants, captains and jury members.
4. Definition of a clear workflow in case of complaints. The workflow is depicted in Fig. 3.

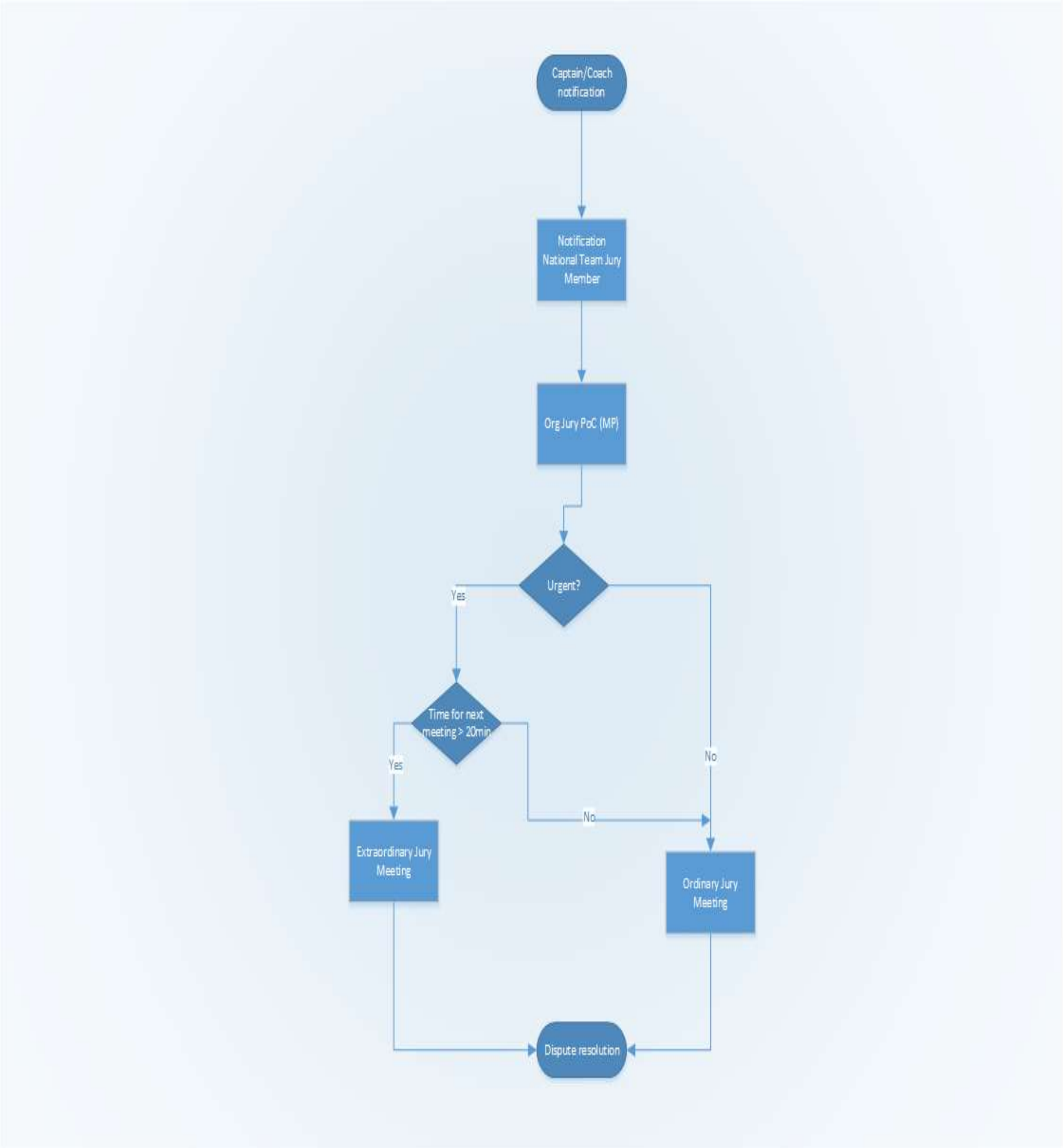

Captain/Coach notification
Notification National Team Jury Member
Org Jury PoC (MP)
Urgent?
Yes
No
Time for next meeting > 20min
Yes
No
Extraordinary Jury Meeting
Ordinary Jury Meeting
Dispute resolution

Figure 3 Jury Workflow

In general, during the competition the role of the jury was:

- Attend jury meetings
- Resolve disputes with impartiality
- Attend and evaluate presentations
- Attend to any other issue that may need the expertise of the jury.

4.3 Presentation management

For ECSC 21018, ENISA proposed new guidelines and rules for the presentation of the contracts ("ECSC contract presentations guidelines"). During the event, the teams had the chance to present a contract of their choice, earning additional cash rewards.

The final grade varied between:

- Good (extra 40% cash reward of the selected contract)
- Very good (extra 50% cash reward of the selected contract)
- Excellent (extra 60% cash reward of the selected contract)

All the 17 teams presented during the competition with the following grades:

GRADE	NUMBER OF TEAMS
Excellent	13
Very good	3
Good	1

Table 1 Presentation grades

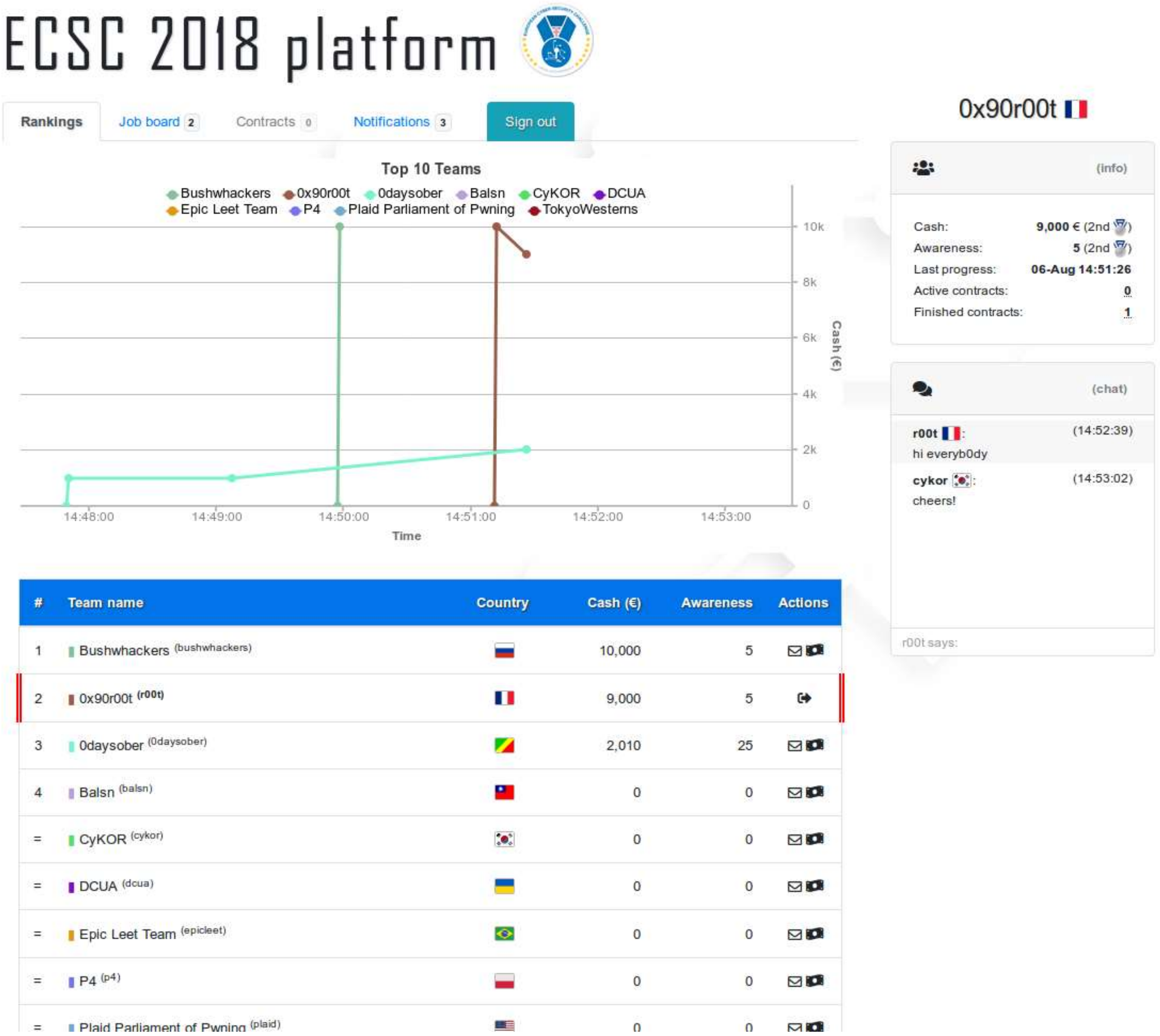
4.4 Deployed Platforms

For the planning, testing and execution of the ECSC, ENISA supported the development of the competition by deploying different platforms:

- Planning portal: https://ecsc.enisa.europa.eu.
- Test Scoreboard and contracts platform: https://board.ecsc.eu
- File Sharing platform (owncloud): Used for information sharing and contingency mechanism: https://storage.ecsc.eu/
- ECSC 2018 Website: Promotion of the event. Real time scoring information was provided during the challenge to externals interested parties: https://www.europeancybersecuritychallenge.eu/

4.5 Scoring Platform (Score board)

In order to manage the scores and the contract resolution, ENISA coordinated the development of a new game board platform:



ECSC 2018 platform

#	Team name	Country	Cash (€)	Awareness	Actions
1	Bushwhackers (bushwhackers)		10,000	5	✉
2	0x90r00t (r00t)		9,000	5	
3	0daysober (0daysober)		2,010	25	✉
4	Balsn (balsn)		0	0	✉
=	CyKOR (cykor)		0	0	✉
=	DCUA (dcua)		0	0	✉
=	Epic Leet Team (epicleet)		0	0	✉
=	P4 (p4)		0	0	✉
=	Plaid Parliament of Pwning (plaid)		0	0	✉

0x90r00t

(info)

Cash:	9,000 € (2nd)
Awareness:	5 (2nd)
Last progress:	06-Aug 14:51:26
Active contracts:	0
Finished contracts:	1

(chat)

r00t: (14:52:39)
hi everyb0dy

cykor: (14:53:02)
cheers!

r00t says:

Figure 4 Scoreboard and contract management platform

Also, onsite support by the main developer was provided during the challenge.

The code of the platform was released to the community under EUPL licensing and can be found on Github (https://github.com/enisaeu/ecsc-gameboard). For ECSC 2019 is expected that this platform will be further improved and many changes requested and identified during the challenge will be implemented.

4.6 Competition Challenges

For ECSC 2018, 36 challenges or "contracts" were provided to participants during the two days of the competition divided in 110 different tasks, these includes activities involving different skills like Crypto, forensics, malware and artefacts analysis, reverse engineering, network forensics, hardware, mobile, steganography, and Capture the flag (CTF) challenges.

Challenges were provided by BT and ENISA. The final selection of challenges was done by the organisers. The Final list of challenges executed in the event was the following:

REF	PROPOSED TITLE	CHALLENGE TYPE	ESTIMATED TIME TO COMPLETE	ESTIMATED DIFFICULTY
BT1	Following the Trail	Unix privilege escalation	4 hours	Hard
BT3	Image Intelligence - Scenario #1	Forensic Image Analysis	1 hour	Easy
BT4	Do Androids Dream?	Android mobile	4 hours	Medium
BT7	Beneath the Waves	Password attack / Hash stealing	4 hours	Hard
BT9	Unscrambling the Message #1 - Source	Crypto	3 hours	Medium
BT10	Unscrambling the Message #2 - Binary	Crypto	3 hours	Medium
BT11	Proving your Skills #1 - Smashing the Stack	Exploit development	3 hours	Medium
BT13	Vigenère Cipher Cracking	Crypto	3 hours	Medium
BT15	Hardware Manipulation #1	Hardware	3 hours	Medium
BT18	Curious Service	Combination network / reversing	3 hours	Hard
BT20	Image Intelligence - Scenario #2	Forensic Image Analysis	1 hour	Easy
Enterprise1	KnowYourBrand - Forensic Analysis	Forensic	4 hours	Medium
Enterprise2	KnowYourBrand - Traffic Analysis	Forensic Traffic Analysis	2 hours	Easy
Enterprise3	KnowYourBrand - Blockchain Analysis	Memory Dump Analysis	3 hours	Medium
Enterprise5	KnowYourBrand - TreasurePro	Packet capture analysis.	2 hours	Easy

Enterprise6	KnowYourBrand - Data Leakage	Packet capture analysis, steganography.	2 hours	Easy
Enterprise7	KnowYourBrand - RSA Analysis	Packet capture analysis, cryptanalysis.	3 hours	Medium
ENISA1	Game of Dorms	Password attack / bruteforcing	1h (Easy)	Easy
ENISA2	Forest for the Trees	Node analysis	2h (Easy)	Easy
ENISA3	Lost in Transmission	Packet capture analysis.	3h (Medium)	Medium
ENISA4	Ma Baker	Cryptanalysis.	3h (Medium)	Medium
ENISA5	Ma Baker Returns	Cryptanalysis.	3h (Hard)	Hard
ENISA6	Byte Queen	Cryptanalysis	2h (Easy)	Easy
ENISAForensics1a	Abyssinium Forensics - Linux	Post-incident forensics on Linux	6 hours	Hard
ENISAForensics1b	Abyssinium Forensics - Windows	Post-incident forensics on Windows	6 hours	Hard
ENISACrypto1	Bob's Encrypted Email	Cryptanalysis	1 hour	Easy
ENISACrypto2	Analysing BC4	Cryptanalysis	1 hour	Easy
ENISACrypto3	Online Banking OTP Token	Cryptanalysis	2 hour	Medium
ENISACrypto7	Old Cryptogram	Cryptanalysis	1 hour	Easy
ENISAHaris1	CTF - Congo	CTF	3h (Medium)	Medium
ENISAHaris2	CTF - Domotica	CTF	1h (Easy)	Easy
ENISAHaris3	CTF - Irony	CTF	2h (Easy)	Easy
ENISAHaris4	CTF - Patient0	CTF	3h (Medium)	Medium
ENISAHaris5	CTF - Untrackable	CTF	2h (Easy)	Easy
ENISAHaris6	CTF - VelvetTrail	CTF	4h (Hard)	Hard
The Device	Hardware Challenge	Hardware	3h (Medium)	Medium

Table 2 Final list of challenges

The teams managed to resolve more than the 95% of the tasks

4.7 Bandstand

As a novelty, an exterior bandstand challenge with an escape-room approach was introduced this year with a very positive feedback. The bandstand was set-up by BT and consisted in a physical challenge with 5 different associated tasks which the teams can choose to do but is not compulsory.

1. Bypass electronic access control
2. Disarm an intruder alarm using a number sequence challenge
3. Bypass some combination locks
4. Solve some hidden riddles which will be exposed by use of a UV torch
5. Using teamwork, disarm a device (wire cutting challenge)

This challenge was located just outside the main competition area and was manned by BT personnel.

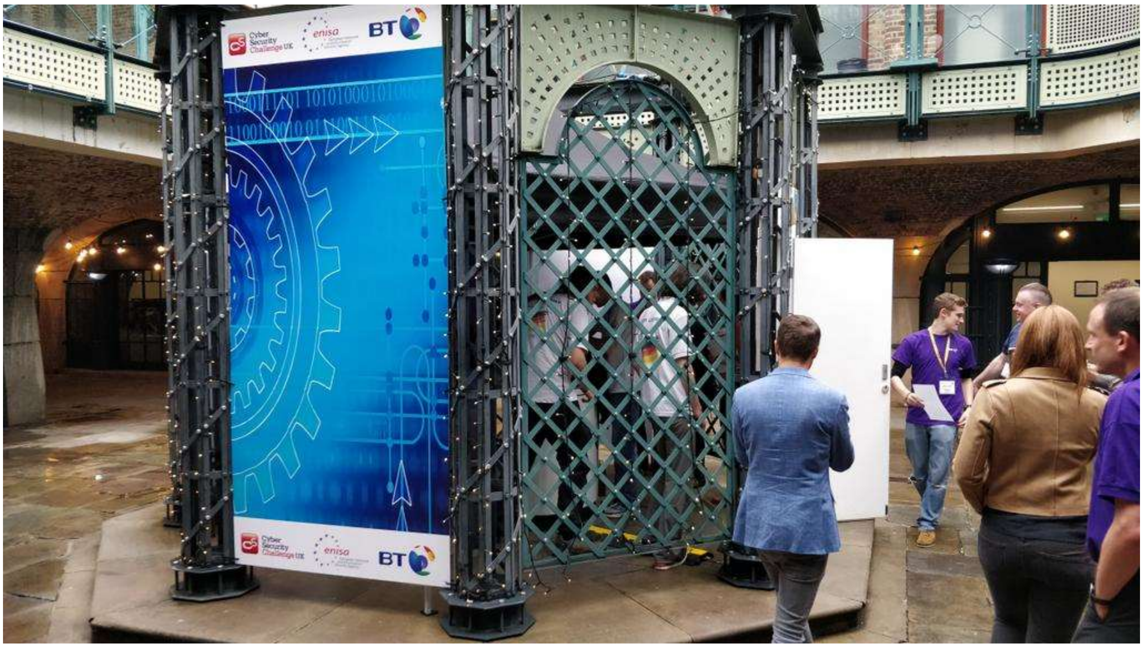


Figure 5 Bandstand

4.8 Public affairs Strategy

The European Cyber Security Challenge (ECSC) Steering Committee decided per ECSC Charter to develop a Public Affairs Strategy for every edition. The main objective of this Public Affairs strategy is to create, distribute and manage a coherent information flow to inform relevant audiences and participating countries about the ECSC final. Moreover, the Strategy provides the input for the Dissemination plan that ensures coherent and synchronised communication.

These documents will contribute to the maturity enhancement of the European Cyber Security Challenge and increase brand exposure. This will draw interested parties from the private sector in context of sponsor opportunities and attract more countries and participants to enrol in future ECSC editions.

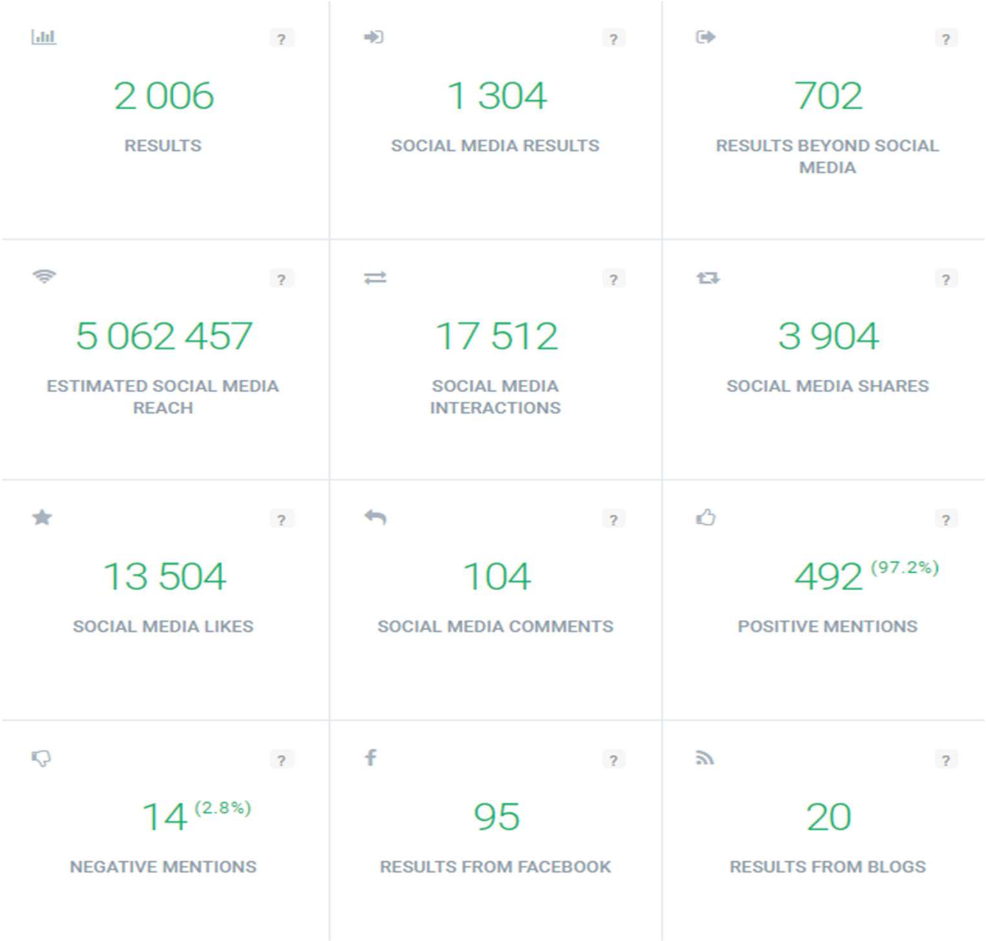
The hosting country and ENISA implemented the strategy for the first year and the participants were provided with an official media pack which included the **lines to take**, **brand identity information** and **press release**s. In addition, ENISA will provide a **Dissemination Plan** that facilitates timely and coordinated implementation of the strategy amongst all participants and ECSC stakeholders.

4.9 Social media impact

Together with the public affair strategy a social media report was created, collecting the reactions during the event, according to the report, some of the most remarkable facts regarding to social media impact were the following:

- Estimated social media reach over the 5 million
- Over 17 thousands direct social media interactions
- 97,2% of positive mentions.

The complete list of collected indicators is the following:



2 006 RESULTS	1 304 SOCIAL MEDIA RESULTS	702 RESULTS BEYOND SOCIAL MEDIA
5 062 457 ESTIMATED SOCIAL MEDIA REACH	17 512 SOCIAL MEDIA INTERACTIONS	3 904 SOCIAL MEDIA SHARES
13 504 SOCIAL MEDIA LIKES	104 SOCIAL MEDIA COMMENTS	492 (97.2%) POSITIVE MENTIONS
14 (2.8%) NEGATIVE MENTIONS	95 RESULTS FROM FACEBOOK	20 RESULTS FROM BLOGS

Figure 6 Social Media Impact

4.10 VIP program support

A program for VIP visits was supported by ECSC 2018 organization. In this context, the following VIP visits were received during the execution of the competition:

- Raffaele Trombetta, Italy's ambassador in the UK
- His Excellency Lars Thuesen, Danish Ambassador to the UK
- Brigadier Lars Christian Hedemark, Defence Attaché, Danish Embassy UK
- Jakob Holm, Press Attaché at the Royal Danish Embassy in the UK
- Guillaume POUPARD, Director general ANSSI

4.11 International Engagement

The head of the USA cyber challenge, Douglas Logan, attended as observer in order to find synergies for future collaborations and leverage the event to a more international scale.

5. Final results

The final results were the following:

POSITION	COUNTRY	POINTS
1	Germany	179350
2	France	177050
3	United Kingdom	169950
4	Poland	169250
5	Greece	166940
6	Italy	166450
7	Estonia	156450
8	Belgium	153450
9	Romania	149950
10	Austria	147690
11	Spain	147550
12	Norway	147250
13	Denmark	146250

14	Switzerland	135490
15	Czech Republic	134650
16	Liechtenstein	71640
17	Cyprus	57800

Table 3 ECSC 2018 Final results

5.1 Post event activities

As post event activity and, in order to promote the competition and the work that is done at national level, representatives of the winning team of ECSC 2018 were invited by the European Commission as VIP guests to the ICT 2018 event held in Vienna on 4th- 6th of December. The ICT conference and fair is the largest event of DG CONNECT taking place every three years. This year is organised under the auspices of the Austrian Presidency to the EU Council.

The representation of the team had the chance to take part in the following activities:

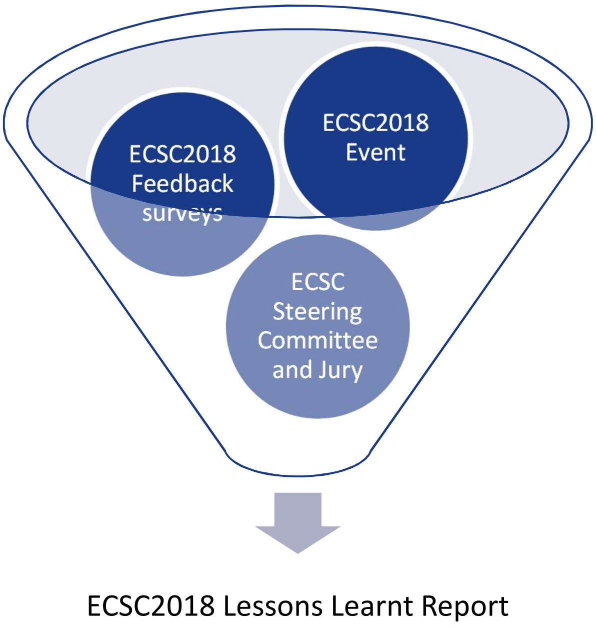
- VIP tour on the exhibition area together with key EU officials
- Attend to different ICT conferences and participate in the Innovation and Startups forum
- Meet with key cybersecurity stakeholders but also MEPs and other EU officials
- Participation in the social event of the conference
- Participation at a Facebook LIVE chat interview

Table 4 Meeting with MEP Eva Kaili

6. Lessons learnt

A lessons learnt report has been developed by an external observer on behalf of ENISA. It takes into account the feedback provided by ECSC organisers, the ECSC Steering Committee, the Jury, and participants regarding to the following domains:

1. Governance and decision-making aspects
2. Public Affairs: Improvements on the social media communication strategy
3. Challenge: Aspects of the competition to be improved related to the development and setup of the challenge and exercises
4. Logistics: Aspects of the competition related with venue, catering, hotel, transportation, etc.
5. Side Events: Aspects of the competition related with social events and networking meetings
6. Compliance: Aspects of the competition to be improved related with compliance with laws and standards


ECSC2018 Event
ECSC2018 Feedback surveys
ECSC Steering Committee and Jury
ECSC2018 Lessons Learnt Report

6.1 Governance and decision-making

PARAMETER	RECOMMENDATION
Roles and responsibilities	• The ECSC project team should consider creating a playbook with pictures of the national teams ("Who is who") to be made available to the other ECSC stakeholders digitally and via hard copies during the event in order to enable the ECSC stakeholders (participants, facilitators, watch dogs…) to distinguish the team captains and coaches of the national teams and the ECSC Jury members. • Clearly define and communicate the internal roles (team captains, coaches, ECSC Jury members, watch dogs…) to the ECSC stakeholders. • Consider creating visual indications for the different roles, for example, by providing stickers, polos and lanyards in different colours for each role.
Decision-making of the Steering Committee and Jury	• Consider foreseeing specific time slots for Jury meetings during the competition. • Capture and document all decisions made during the ECSC Steering Committee and Jury meetings, including decisions, actions and owners, in a decision-making log. • Track the implementation of decisions made by the ECSC Steering Committee and Jury in a central register. • Ensure fair and equal representation of the different national teams with equal voting power in the ECSC Steering Committee and Jury meetings.
Transparency	• Communicate all decisions made during the ECSC Steering Committee and Jury meetings in a transparent manner via official communication channels to the ECSC stakeholders (participants, organisers, facilitators, watch dogs…). • Avoid any last-minute changes to the ECSC game rules, in order to avoid confusion and ambiguity within the teams and unfair outcomes during the challenge. • Consider putting in place a screen within the ECSC gaming area via which any relevant communication towards the ECSC participants about the Jury meetings can be displayed.

Table 5 Governance and decision-making lessons learnt

6.2 Public Affairs

PARAMETER	RECOMMENDATION
Public Affairs Strategy adoption by national teams	• Consider incentivising the transposition of the Public Affairs Strategy on a national level. Improve the communication between the national teams and coordination on social media in order to ensure an even intenser and more valuable collaboration between the Member States on approaching social media for ECSC2019.

Table 6 Public affairs lessons learnt

6.3 Challenge

PARAMETER	RECOMMENDATION
Design	• Consider developing a few real challenges to be tested by the participants in order to assess whether the level of complexity is adequate to their skill. Request participant's feedback on complexity for individual test challenges and take these into account for development of the final challenges.

	• Consult with ECSC alumni and other active CTF players to ensure a level of complexity and challenge proportionate to the level of skill of participants. • Consider implementing a feature on the platform to report and provide feedback on challenges from a complexity point of view.
Service Providers	• Fixed position for service provider representative in jury. • Additional HR capacity for service provider for trouble shooting.
Rules	• Consider a process for enforcement of rules and define standard consequences based on the type of violation. For example the use of red and yellow cards could be used by analogy with football games, where significant violations are penalised by a red card. Consider the following enforcement scheme: ○ Red card. First red card: half hour time-out, second red card: disqualification ○ Yellow card. First yellow card: warning, second yellow card: 15 minutes time-out, third yellow card constitutes first red card. • Consider assigning the role of Referee to an individual that monitors compliance with the rules. Upon unclarity, the Referee can escalate to the Jury for final decision.
Enforcement	• Mandatory communication channels (between coaches and teams, and jury members). • Consider establishing an enforcement scheme that discourages malicious participants to spoil the fun for others. I.e. consider assessing ethical behaviour and incentivise fairplay. It is up the Steering Committee to develop and apply these rules. • Consider detailing specific responsibilities for the watchdog function and communicate clearly their role to all stakeholders, including participants and organisers in order to avoid confusion about their mandate. • Consider installing a technical monitoring capability that enables identification of technical rule infringement by participating teams or specific individuals.
Presentations	• Reconsider incentives for presentations in order to make them more strategically fitting with the challenges and encourage participants to do it. • Consider enlarging the driver for presentations. Incentivising presentations by providing points that will be taken into account for the challenge could be an option, but it has to be aligned with the overall philosophy of combining soft skills with technical skills.
Platform	• Consider implementing access controls to prevent users access the platform before it is intended to be used.
Infrastructure	• Perform adequate capacity testing beforehand (i.e. simulation testing/stress test). • Consider cloud / hybrid setup for hosting the challenge platform -> given high-bandwith and speed internet uplink.
Complexity	• Consider involving ECSC alumni into designing the challenges in order to reflect the groups' level of expertise. • Consider involving CTF community – that is, actively involving seasoned CTF players into the process - in designing challenges.
Scoring	• Consider implementing a scoring system that indicates scores for different phases in the challenge progress (indicate completion of milestones, overall progress for specific individual challenges, etc.).

Table 7 Challenge lessons learnt

6.4 Logistics

PARAMETER	RECOMMENDATION
Venue	• When determining the location of the challenge venue and hotel accommodations, take into account the distance and transportation options between both places. Ensure that participants, organisers, facilitators and other relevant ECSC stakeholders can easily reach the challenge venue under any weather conditions.
Catering	• Ensure that sufficient water and food supplies are foreseen at the challenge venue. • Consider foreseeing a variety of meal options (including several vegan/vegetarian meal options, gluten-free…) for the participants and other ECSC stakeholders during the challenge.
In-event communication	• Consider putting in place a big, central screen at the challenge venue, which displays all relevant communication regarding the outcome of the Jury meetings, lunch time, end time of the competition… towards the ECSC participants and other stakeholders. • Consider establishing a central WhatsApp group or other communication platform for the ECSC Jury members and organisers before the start of the challenge, in order to make it possible for the members to communicate during the competition and inform each other of decisions taken during the Jury meetings. • Consider sharing an updated program schedule with the ECSC participants and other stakeholder throughout the competition to create the right expectations. • Consider using other means than microphones to communicate updates to the ECSC participants and other stakeholders during the competition.
Accomodation	• Consider the climate and weather context of the hosting country in order to foresee alternate transport options from the accommodations to the actual event venue (e.g. in case of heavy rain).

Table 8 Logistics lessons learnt

6.5 Side Events

PARAMETER	RECOMMENDATION
Social event	• Consider facilitating the social events in spacious locations, which are adequate and sufficiently large to accommodate the amount of people present at the ECSC. • Consider organising social events which trigger more interaction between the national teams (e.g. by placing name tags on the tables during dinner and ensuring that at least 4 countries are represented at each table).
Schedule/timing	• Ensure that the ECSC program schedule is aligned with the agendas of the side event (e.g. job fair) in order to enable participants to attend the side event.

Table 9 Side events lessons learnt

6.6 Compliance

PARAMETER	RECOMMENDATION
Data protection	• Ensure that the privacy preferences of all ECSC attendees are visible and respected. Privacy preferences could be expressed, for example, by providing coloured bracelets, polos or badges, which indicate whether or not the attendee wants to be captured in pictures, movies or other images which will be shared on social media (choice principle). • Ensure that all ECSC attendees are aware of the possible processing activities (e.g. being part of a group picture that will be shared on social media) by providing a general transparency notice at the event, for example via a banner at the entrance of the event, stating that pictures could be taken and shared with a wider audience) (transparency principle). • Ensure that all individuals have the option to opt-out of some of the processing activities (e.g. enable them to express they do not want to be in pictures published on the internet etc.) (choice principle).

Table 10 Compliance lessons learnt

7. Maturity assessment results

In order to measure the current status of the ECSC project, a maturity assessment on different areas was developed by an external contractor, the results on the report are the following:

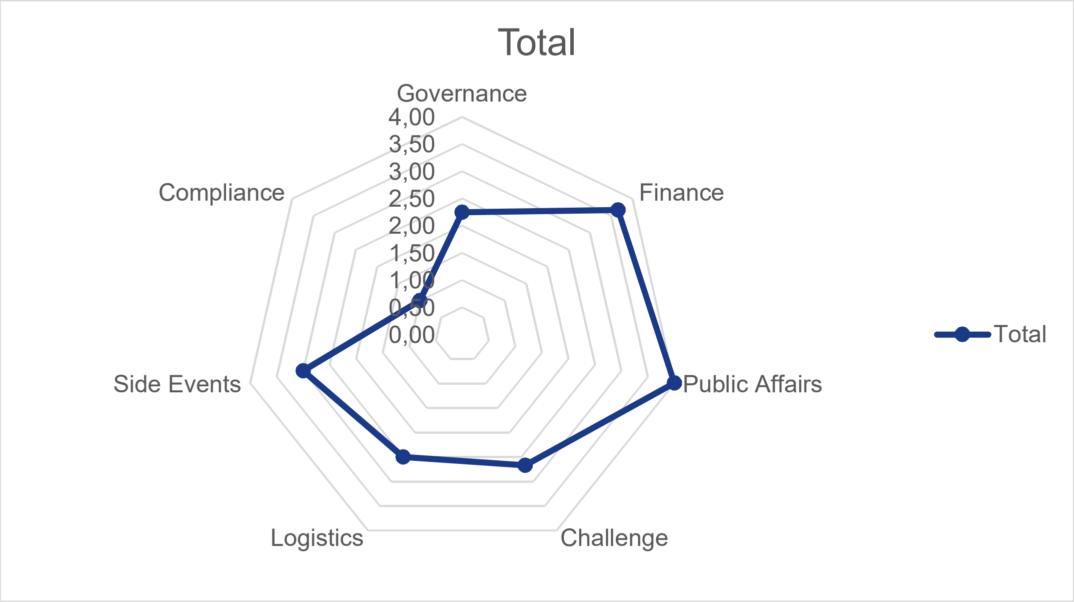


Figure 7 Maturity assessment results chart

8. ECSC 2019

The final of the 2019 edition of the European Cyber Security Challenge 2019 will take place at Bucharest in October 2019 where, at least, 20 countries are expected to participate. The latest updates will be published on ECSC 2019 website: https://www.europeancybersecuritychallenge.eu/

ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu