The New Global Challenges in Cyber Security
October 30-31|2017
Bucharest, Romania

Conference report

Contents

- Summary
- Session Insights
- Participants’ feedback
- Attendance stats

Dear partners, supporters and guests,

First of all, thank you all for your participation at this years' edition of our annual event, ***#certcon7***!

This year has been very dynamic for cyber security from many perspectives. We have seen the largest cyber-attacks yet in terms of scale of impact and number of affected entities. Threats have multiplied and increased in sophistication. There are more and more devices coming on the internet worldwide and vendors, researchers and developers are racing on developing new products.
Looking forward, there are important initiatives that will start producing effects in 2018. GDPR regulation and NIS Directive are coming into force, a new mandate for ENISA is being discussed and the current European strategic framework that includes all three pillars (defense, cybercrime and cybersecurity) is being updated. Moreover, cooperation on a global scale between public and private actors is intensifying. Please read the full report for insights on all these issues from the most relevant institutions present at the event.

This edition has been the largest yet, having around 300 attendees during the two days. Moreover, the event achieved the global reach that we had hoped for, accommodating guests from 18 countries this year and proving that Romania can become an important regional actor on cyber.

We plan to have at least the same global impact with the 2018 edition and we hereby extend the invitation to have you as partners, supporters and / or guests both for the event and throughout the year!

Respectfully,
The CERT-RO Team

278
Total participants

1524
Website visits in October

CERT.RO

6
National televisions covered the event

2
Live streaming sources during the event

18
nationalities among attendees

lots of sleepless nights

9
Institutional partners

16
Private partners

74
Companies present

1000+
Participants at certcon '12 - '17

54
Speakers

8
Sessions

Summary

Every year, “The New Global Challenges in Cyber Security” conference tackles the most pressing cyber security issues on the public agenda and looks at both the latest challenges in this field and ways to overcome them together with cyber security experts from private companies across all sectors and industries, government officials, policy-makers, NGOs and Academia.

This year we were honored by the presence of the EU Commissioner for Digital Economy and Society, the Romanian Minister for Communication and Information Society and the Romanian Minister for European Affairs, who addressed in their speeches the most pressing challenges from a regulatory and strategic perspective at both European and national level. Other key institutions, such as NATO, UN's International Telecommunications Union, US Embassy and EU's Cyber Security Agency, ENISA, have also been represented at the highest level and joined the discussion with their own perspective.

In the context of increased efforts at European and International level in the area of capacity building, resilience and cooperation, particularly EU-wide ongoing efforts to transpose and implement the NIS Directive and
the EU General Data Protection Regulation, as well as with a view to address other regulatory and policy challenges, the first day of the event was dedicated to discussions between representatives from European institutions, industry stakeholders and other international organizations.

Mariya Gabriel, EU Commissioner for Digital Economy and Society

The EU deploys a cybersecurity strategy since 2013, but today the number, complexity and amplitude of attacks and their societal impact prove that we need to be more reactive"

Lucian Șova, Minister for Communications and Information Society

“Romania should become a generator of expertise and good practices in Europe and beyond.”

Debates in parallel meeting rooms provided an opportunity to share ideas and best practices with other EU Member States and various stakeholders on ensuring cyber security through stronger regulations, sharing NIS implementation challenges, balancing cyber security and privacy and building on the development of a strong cyber security industry.

Moreover, the parallel tracks dedicated to solutions and technologies for operators of essential services in the banking and energy sectors, two of the sectors regulated by the NIS Directive, have shifted towards industry-specific needs.

The agenda for the second day was dedicated to plenary sessions where leading experts from the public and private sector and industry leaders presented the latest challenges to cyber security, trends as well as updates on the industry overall.

“We need a cyber security reform that is in line with local and national demands.”

Victor Negrescu, Minister for EU affairs

Both public and private institutions covered the latest developments: the private sector perspective was covered by leading companies that play an important role in the global cyber security market, launching new technologies and having a global view of the cyber threat landscape, while key public actors such as Europol, FBI, European External Action Service, Rotative Presidency of the Council of the European Union, Council of Europe, Romanian Police and Romanian Intelligence Service have provided their view on the challenges of today and tomorrow.

Session Insights

Plenary Session – Strategy and policy outlook

This panel provided an overview of the current strategic context for NATO, ENISA, ITU and CERT-RO. Representatives of these key-institutions detailed upon the latest developments in the area of capacity building, developing cyber resilience and building confidence and security in the use of ICT at EU and international level. The US Embassy in Bucharest has also shared its strategic positioning and reinforced the close and successful collaboration with the above-mentioned institutions.

Within the Trans-Atlantic community, NATO has been actively engaged in cyber defence since its involvement in the 1999 Western Balkans operations.

The Alliance built a network of CERT-like bodies following the 2002 cyber-attacks on its IT infrastructure, which ultimately provided centralised protection over its system, following the Lisbon Summit.

However, on the backdrop of other geopolitical crises, NATO's approach has shifted more into cybersecurity governance. Since the 2008 Estonian cyber-attacks the Alliance has included policy and strategic elements into its defence framework. Furthermore, the 2015 hybrid campaign against Ukraine prompted the Organisation to prioritize cyber defence at an intergovernmental level, to establish guidelines toward protecting critical infrastructure and to escalate cyberspace as an operational domain (along air, land and sea).

Other notable developments include the 2014 commitment to an Enhanced Cyber Defence Policy and the 2016 pledges during the Warsaw Summit.

Sorin Ducaru, NATO

"We must bridge the cognitive gap between addressing cyber at technical level and at a policy and strategic level."

#certcon7
Cooperation – the best way to engage
other stakeholders (different approaches)
• CERTs/CSIRTs – mitigation and rapid response
• LEA – attribution and prosecution
• Military and Intelligence – diplomatic response
Capacity building and maturity
to have the right tools to provide the best possible
response in the shortest amount of time
CERT-RO is now one of the few CERTs in the world that
provides automated response to alerts and incidents
www.cert.ro/certcon7

Presently, NATO coordinates numerous cyber defence programmes aimed at consolidating its Member States’ preparedness and resilience in the face of an evolving threat landscape. The Alliance uses real time tools for analysis, assessment and information exchange in order to mitigate advanced persistent threats. Finally, its partnership programmes with International Organisations and key cyber industry actors provide a valuable platform for information exchange, intelligence analysis and good governance norm dissemination.

While the Alliance remains at the forefront of cyber defence, there is still room for improvement. Firstly, Members States should strive to bridge the cognitive gap between addressing cyber issues at technical and at policy or strategic level. Another action is consolidating ties between NATO, law enforcement and civilian agencies such as Europol, Interpol and ENISA at the crossroads of critical infrastructure protection. NATO should enforce its potential as a clearinghouse which can centralise and leverage information and intelligence across various sectors and industries.

The civilian angle echoes similar challenges and paths for improvement. Clearly, cybersecurity is not an issue that can be addressed solely by one country, one industry or one organisation. Therefore, cooperation is essential among states and industry sectors alike, under clear and coherent guidelines and national cybersecurity strategies.

Rosheen Awotar-Mauree, ITU

“We need a better dialogue with the shapers of cyberspace.”

The UN’s specialized agency for information and communication technologies, ITU promotes a multi stakeholder approach to cybersecurity governance under five pillars of activity: legal, technical, organisational, capacity building and cooperation.

Among the challenges identified, cybersecurity capacity building comes to the fore. The Union cooperates closely with government, academic and private sector partners through its Sustainable Development Goals framework. It provides counselling for numerous digital initiatives with considerable success in human/societal security related topics such as online child protection, privacy and also the promotion of open data.

Another issue on the agenda is bridging the cybersecurity divide, namely the lack of coherent cybersecurity strategies and comprehensive metrics to measure the level of cyber preparedness at national level. Therefore, the aims is to create a harmonized reference point through a Reference Guide for National Cybersecurity Strategy and to provide methodological counselling to soliciting countries for establishing national CERTs and relevant policies.

Jean-Baptiste Demaison, ENISA Management Board

In the context of EU efforts in cyber policy development, there are four main strategic directions: to provide Member states with expertise and harmonise practices; to support the development and implementation of coherent cyber policies to engage in capacity building by providing dedicated, on-site experience in establishing CERTs and national strategies for Member States; and to build European network and information security expert fora to achieve enhanced operational cooperation.

To this end, the EU policy makers have tabled some key policy initiatives including the EU Cybersecurity strategy, the NIS Directive and the Cyber Security package, which aims, among other points, to enhance the centralised capabilities of European authorities. Other notable initiatives such as the Cyber Europe Exercises and the EU Cybersecurity Month promote trans-sector cooperation and facilitate the establishment of NIS professional communities.

Transposing the NIS Directive

The panel dedicated to the NIS Directive discussed the challenges met by France, Slovakia and Romania, as well as ENISA, in boosting the overall level of cybersecurity and the development of a unified cybersecurity incidents response mechanism in the EU: the implementation of the NIS directive.

The speakers shared best practices and challenges met along the way in this complex process such as: establishing competent national NIS authorities, increasing member states preparedness by appropriately equipping their Computer Security Incident Response Teams (CSIRT), identifying the essential services as well as the operators of essential services and promoting a culture of security across sectors. All these topics are vital for the economy and society and rely heavily on ICTs in key industries, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Harmonizing practice at Union level poses challenges for member states and for the Commission. However, close cooperation between stakeholders helps in defining priorities and implementation schedules.

Rastislav Janota,
Security Council of Slovak Republic

Supporting the cybersecurity industry - best practices, public-private partnerships and ways forward

Although it is, least to say, hard to replicate a Silicon Valley or Tel Aviv model, smaller, focused clusters can be efficiently developed. The discussion within this panel focused on good practices from other countries, having the case study of Israel in mind, following up with the success stories of private companies and start-ups and ending up with what can be better done in terms of market development: enhanced government support, better marketing and awareness and more education.

The panel covered the initiatives the different speakers undergo for the creation of added value inside the cybersecurity industry in Romania. The panel included most of the stakeholders in the industry: government, academia, business incubation, researchers, technology vendors and integrators.

In terms of regulation and government support, there are a few initiatives worth mentioning, such as the Start-up Nation, the new PPP law that is about to come out or the new project of a dedicated authority for government cloud in order to integrate life services into one platform and digitize operations. Moreover, the government should try to integrate innovation more and more in order to support the market. However, one take-away from the panel is that innovation comes in a heavily regulated industry and without government support it is next to impossible to create a viable ecosystem.

Dorin Pena, CISCO

Yanir Laubshtein
Former Manager of Israel's National C-SOC for Critical Infrastructure

Another highly debated topic was access to information for start-ups, a vital part of their success. One example was the laboratory created in Israel, the Cyber Gym, where different companies could test their products on existing technology. Another one is creating an ecosystem through business incubators and accelerators to catalyze development and bring products closer to customers, giving entrepreneurs a much needed marketing boost. There is a good example in the ecosystem on cyber security created around Beersheba University in Israel, but there are promising programs in Romania as well, such as Innovation Labs or Orange Fab. European research projects are another way of adding value, through programs such as Horizon 2020, where research is done in cooperation with other European counterparts.

Last but not least, the formation of specialists is mandatory, not only in Romania, but worldwide. Universities should be heavily involved, but education should come from high school as soon as possible in order reduce the granularity in the Romanian education system.

All in all, Romania has great knowledge on technologies, well trained specialists and has a great chance of becoming an important player in the global industry. However, without a clear strategy, good marketing and access to information it will be hard to have a competitive industry.

Cybersecurity and data protection (the privacy challenge)

Over the past years, online privacy has slowly glided into public discourse. Our increasingly digitalized world brought significant advantages to how we communicate, conduct business and govern. However, it has also eroded the thin red line between personal and public, causing ripples across the political spectrum. Today, talks of major data breaches and privacy infringements arising from data monetization or transnational transfers have become the norm.

Key government and industry representatives joined us in addressing these challenges. The panelists covered all the main stakeholders in this field – public authorities, providers of technical solutions to secure data, consultancy and companies that will be affected by recent regulatory developments.

Panagiotis Sotiriou, Symantec

As the GDPR entry into force is drawing near, three key challenges were identified concerning implementation, the mandated measures and compliance.

Indeed, Data Protection Authorities (DPAs) will benefit from an enhanced mandate. Traditionally, DPAs have three lines of activities: monitoring, enforcement and raising awareness. The regulation switches the roles between data processors and data controllers, who will be able to make their own assessments. Furthermore, companies may solicit an impact assessment from their DPA and benefit from a wide array of white papers and guidelines in what regards the process of alignment. Some of those mentioned were Article 29's Data Breach Notification Guidelines and ENISA's Guide to Cryptographic practices.

Bogdan Manolea, APTI

Pseudonymization and encryption were recurrent themes of compliance practices mentioned during the discussion. The former is a new concept in European law and defines a process which renders data neither anonymous nor directly identifying. Pseudonymization is the separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately.

Companies can achieve better security by going back to the basics, namely data protection training for their staff, which was identified as one of the main bottlenecks and regular data breach and incident response simulations. Another key aspect is integrating data protection and security components in business practices.

George Dragusin, Romanian Bank Association

Challenges and solutions for the Banking sector

For 2017, many risk managers from the banking sector have identified cyber threats as top priority. Taking into account the data breaches from the last 2 years globally, but also the accelerated pace of digitalization in the sector, information security officers have a lot on their plate for the upcoming years, especially in assessing the gaps in cybersecurity, learning from past incidents and steering the mindset of top management towards security.

One of the challenges discussed within the sector is information sharing, impeded by the silo approach and lack of mechanisms for information sharing. Possible solutions include voluntary information sharing protocols for the purpose of better detection, prevention and response to cyber crime.

Challenges and solutions for energy operators

Recent years revealed a series of incidents in the energy sector, be it external attack or incidents coming from inside the company, highlighting the need to ramp up security measures. Many systems are now protected because they are legacy systems, but with each network upgraded to IP, new threats arise and energy stakeholders should be prepared.

The panel discussed the main challenges to tackle in the Energy industry today. The sector has some well-known incidents, such as 2014 and 2016 attacks on the grid in Ukraine or espionage campaigns, therefore the threat exists.

But how important is it today? Technology wise, it depends on how much of the process network is on IP. Having obsolete systems today is actually a positive thing in regard to cyber security, as these systems act as islands and are not online. This in not only the case of Romania, it is a worldwide fact, as industrial control systems are usually designed to have a 20-25 year old life span. However, those networks that already started to migrate partially or totally to IP technologies or start to bring the network to the internet one way or another should update As-Built blueprints in order to precisely map their network. Although many of the installations, if compromised, could lead to catastrophe, the major risk is losing control or having data manipulated.

In terms of best practices, mapping the network, aligning roles and responsibilities with the main business functions, well documented information security policies and management involvement are the main directions agreed upon.

However, one bottleneck discussed was the lack of C-Level involvement in the matter. Are managers aware of future legislation and potential losses due to attacks or fines? The Information Security or Cyber Security Officers should talk more about cyber risks and how these quantify in losses in order to have the full attention of management. If the industry manages to bring them to the table, budgets will open. It is especially difficult in public companies, where employees are not empowered by management.

As most of the cyber security industry pointed out, the lack of skilled people is the biggest setback of the industry. In the end, the most notorious cyber-attacks in energy or industry in general started from a USB stick or a spear phishing e-mail. This can happen only through raising awareness, both to attract new talents and to combat social engineering. For this we need media, large organizations and public institutions to work together in order to increase awareness.

A private sector perspective on the new global challenges in cybersecurity

There are probably only a few areas where public-private cooperation is as important as it is for ensuring cybersecurity. Cyber security spending is driven by cyber crime and it is rapidly growing – predictions on global spending on cyber security products and services place the value at over 1 trillion dollars over the next five years (from 2017 to 2021).

Most of the companies represented in this panel play an important role in the global cyber security market, being leaders in launching new technologies and having a global view of the cyber threat landscape.

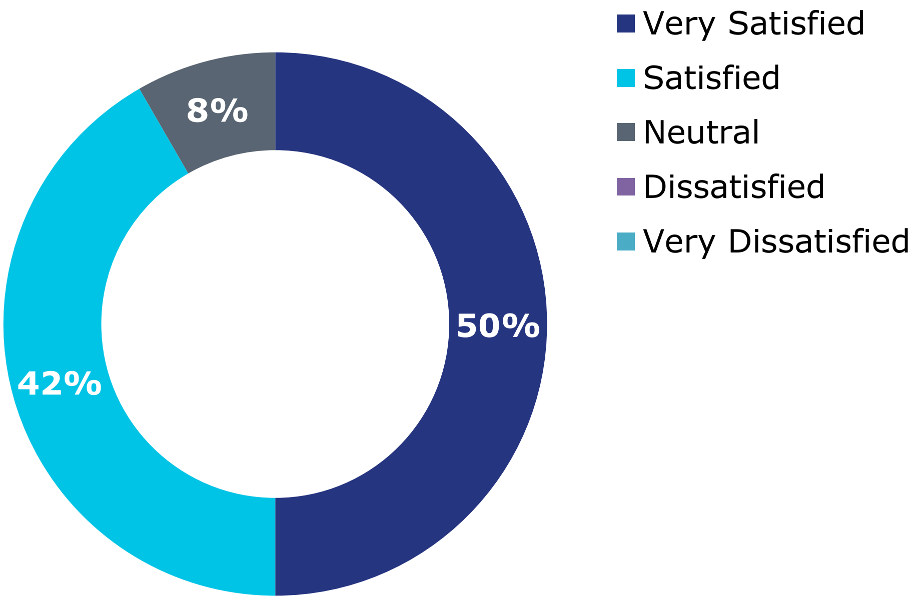
They had the challenge to present their view on the most stringent challenges to cyber security today and also the solutions and technologies that they are developing to overcome these challenges.

A public sector perspective on the new global challenges in cybersecurity

Incidents involving ransomware and phishing attacks have tripled and doubled, respectively, since 2015; their projected market impact at the turn the decade is expected to reach as much as $6 trillion annually. These developments confirm the increasing importance of state agencies in the digital realm. While the private sphere leads in technological innovation, governments worldwide are seeking better ways to enforce and improve relevant countermeasures. One clear message encompasses their initiatives : cooperation is essential. We discussed with representatives from FBI, Europol, European External Action Service, Estonian Presidency of the Council, the Council of Europe, Romanian Police and Romanian Intelligence Service the intricacies of cybercrime response initiatives and each institutions' take on the most pressing challenges in cyber security as well as the latest sets of measures adopted by public institutions at EU / national level to overcome those respective challenges

Participants’ feedback

Overall satisfaction with the conference



General Comments

“ From my point of view it was a success and I do not know what would be improved. I want you to keep the same level.“

“You should invite CIO from other countries, especially from USA, from the public and private domain. “

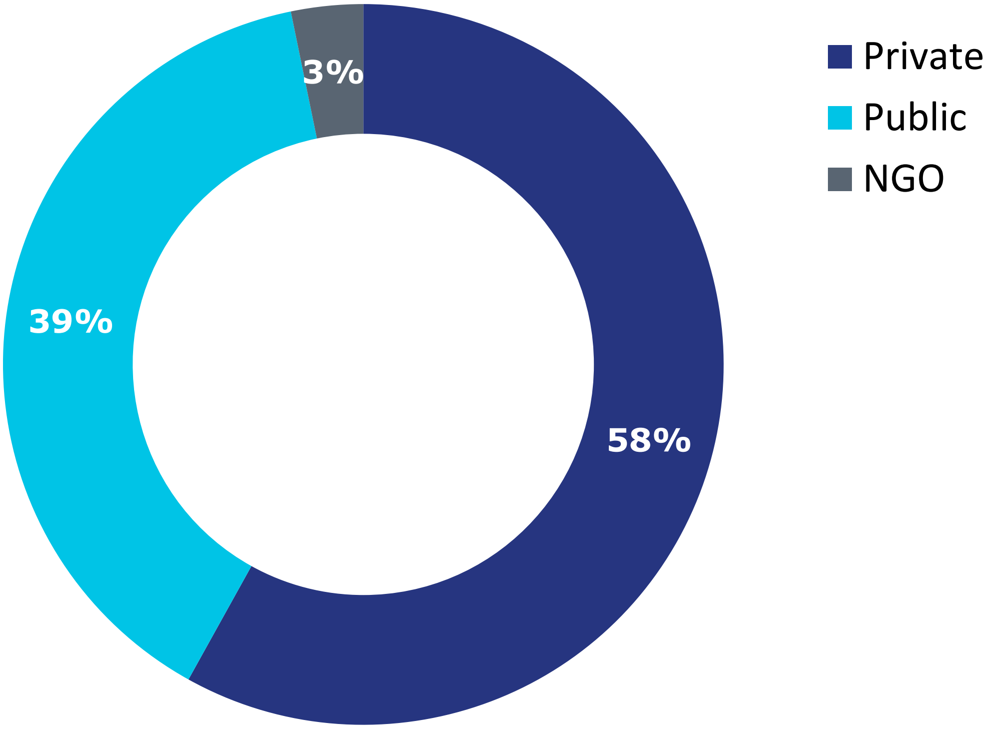
“Organize debates regarding what should be the Romanian strategy of leveraging technology to improve the efficiency and effectiveness of the activities in the public sector (central and local administrations).“

“Overall a very interesting, actual event which is mandatory to be continued and upgraded. Very good organization.“

If you haven’t got the chance, we’re still accepting feedback at:
https://docs.google.com/forms/d/e/1FAIpQLScCTTUiH16_Y0-fjWSHKCy83xzKBYtjvGYVlEMziQiG8xKaNA/viewform?c=0&w=1

Attendance stats

Sector Overview

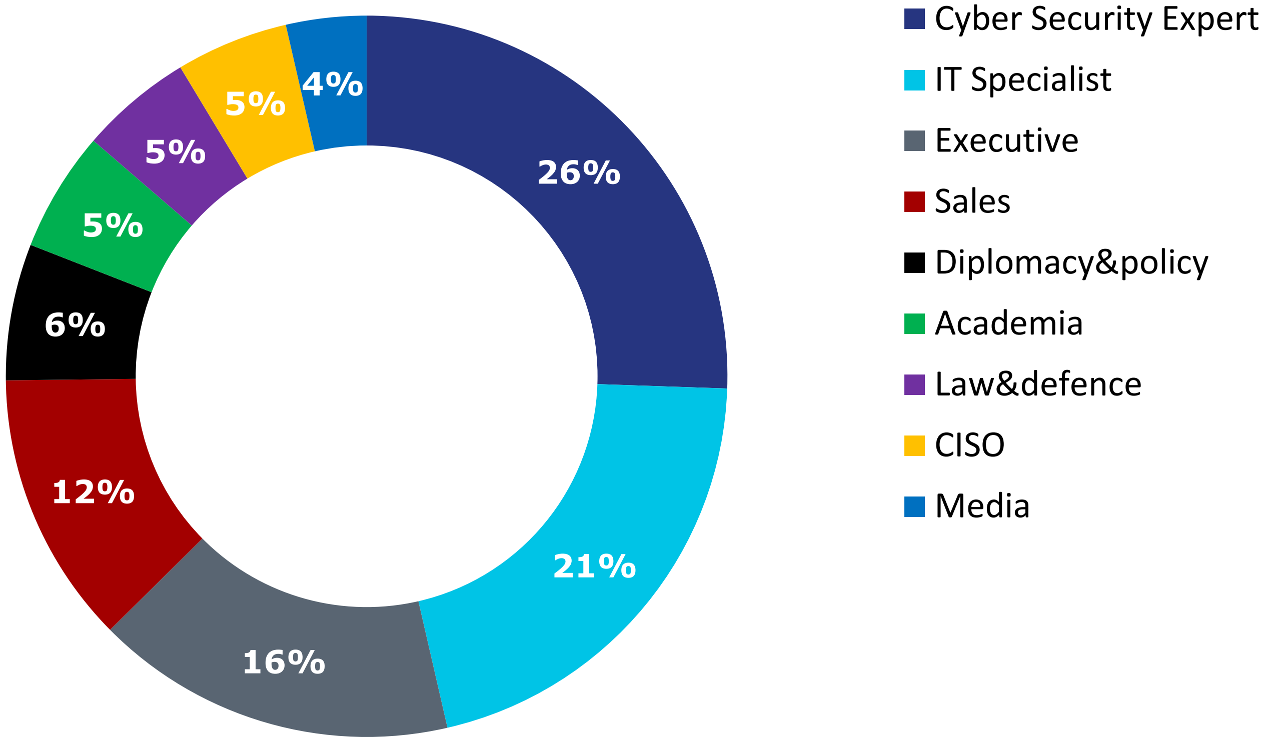


Key stats

Participants	278
Speakers	54
Partners	16
Support of	9

Sector	**Number**
Private	162
Public	108
NGO	9
TOTAL	**278**

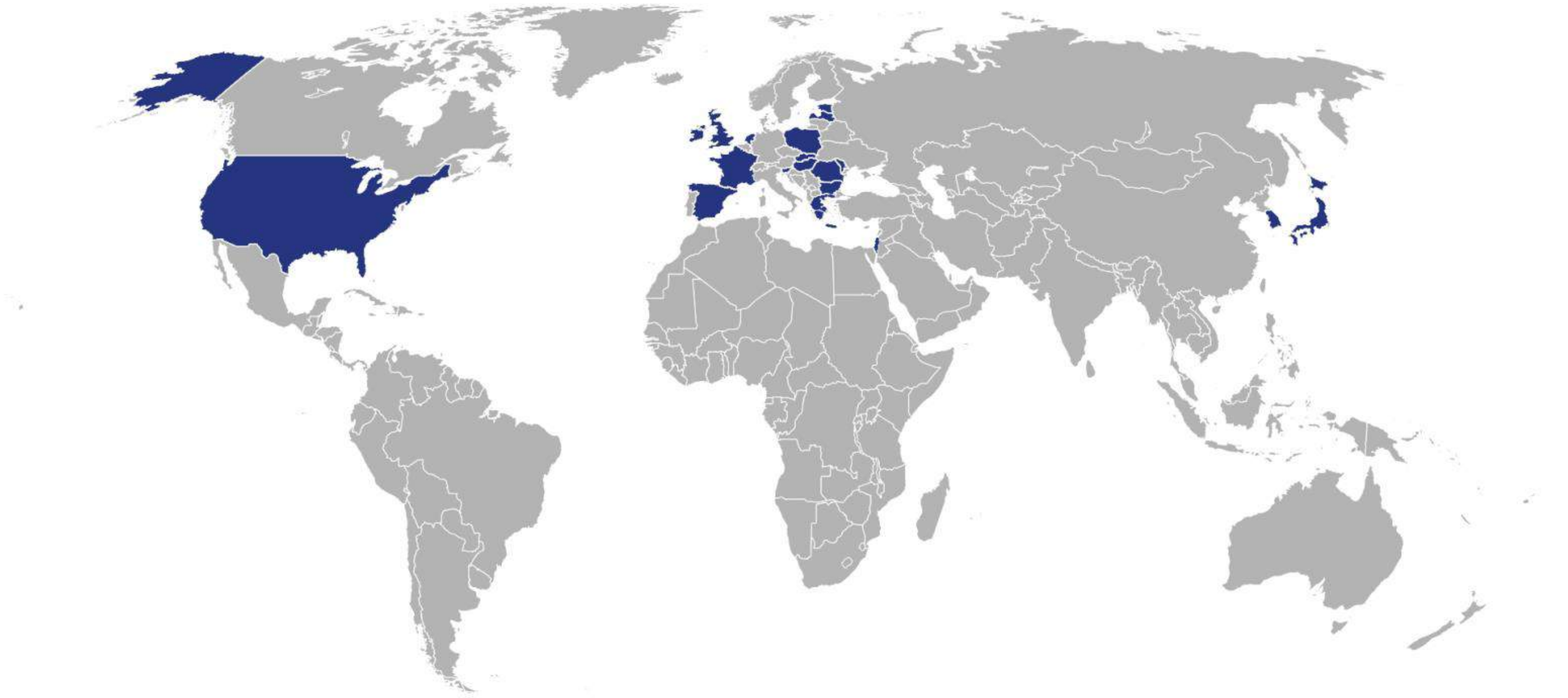
Participants by expertise



Expertise by individual	Number	Percentage
Cyber Security Expert	71	25.5
IT Specialist	58	20.9
Executive	45	16.2
Sales	34	12.2
Diplomacy & Policy	17	6.1
Academia	15	5.4
Law & Defence	14	5.0
CISO	14	5.0
Media	10	3.6
TOTAL	**278**	

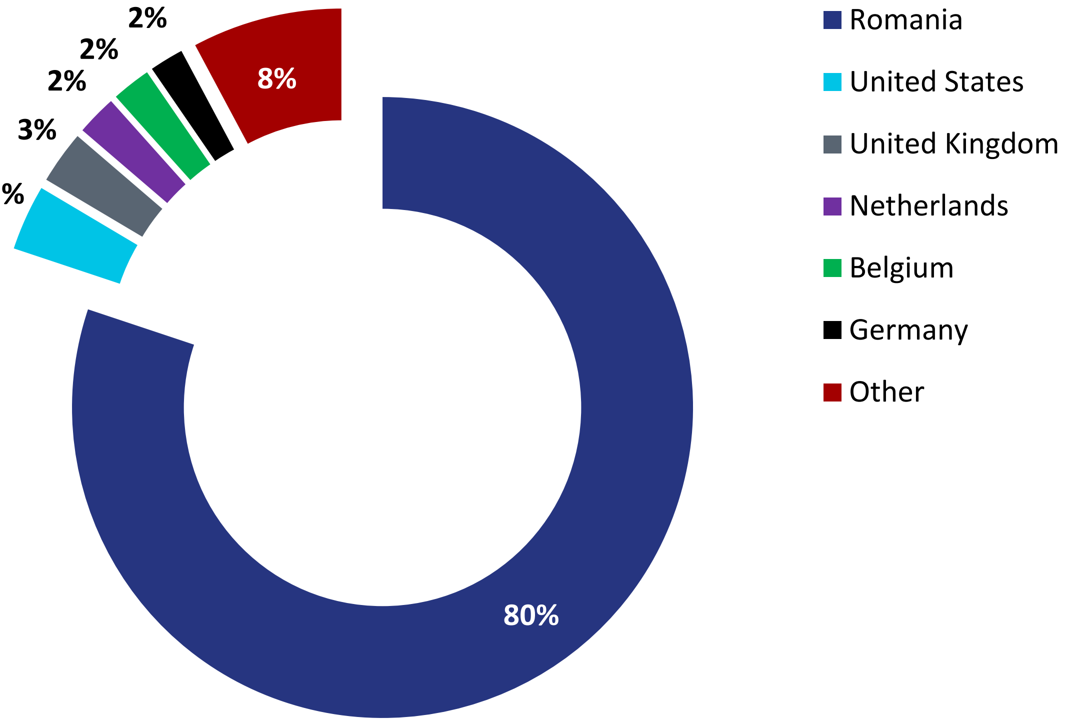
Participants by country

Attendants at the event included representatives of public institutions, companies and C-SIRT representatives from 18 countries: United Kingdom, France, the Netherlands, Slovakia, Latvia, South Korea, Japan, Estonia, United States, Ireland, Spain, Slovenia, Israel, Poland, Greece, Republic of Moldavia, Bulgaria, Hungary.



CERT.RO

Website visits - October



Acquisition type	Unique visitors
Direct	1108
Referral	156
Social	127
Organic Search	103

Country	Unique Visitors
Romania	1221
United States	52
United Kingdom	42
Netherlands	32
Belgium	31
Germany	27
Other	119
TOTAL	**1524**

Our partners

certSIGN®

Check Point® SOFTWARE TECHNOLOGIES LTD.

CISCO™

ENEVO GROUP

FORTINET®

Microsoft

Q-EAST SOFTWARE Smart Systems Management

yellowcube

TREND MICRO™

Combridge Deutsche Telekom Group

provision® protect your business

orange™

CLICO

Bitdefender®

KASPERSKY lab

Deloitte.

With the support of

GUVERNUL ROMÂNIEI MINISTERUL COMUNICAȚIILOR ȘI SOCIETĂȚII INFORMAȚIONALE

UNITED STATES OF AMERICA EMBASSY

ANSSI ASOCIATIA NATIONALA PENTRU SECURITATEA SISTEMELOR INFORMATICE

CIO COUNCIL Romania

ISACA® Trust in, and value from, information systems

AGENȚIA NAȚIONALĂ DE PRESĂ AGERPRES Actualizează lumea.

energynomics.ro

PQB communication designers

UBER

CERT.RO

🌐 www.cert.ro

📱 +4031-6202187

✉ cooperation@cert.ro

🏠 8-10 Mareșal Averescu Blvd., 011455 Bucharest, Romania