Cyber Polygon

International online training
for raising global cyber resilience

cyberpolygon.com

2020

Contents

Mikhail Mishustin, Prime Minister of the Russian Federation

'I am pleased to see at this event the leaders of large international organisations and CEOs of global corporations from a wide range of industries and countries. The training is another step in creating a trusted digital environment and fostering an open dialogue to discuss even the most challenging cybersecurity issues. Today, the participants of Cyber Polygon are making a contribution to building a more secure digital world and a safer future for all of us'.

Klaus Schwab, Founder and Executive Chairman, World Economic Forum

'Technology and cybersecurity are of crucial importance in this COVID era. One of the most striking and exciting transformations caused by the pandemic has been our transition to the digital 'everything', both in our professional and also in our personal lives.

I am glad that Cyber Polygon has proved itself as one of those brilliant initiatives that address the need for developing and enhancing global cyber resilience in the fight against cybercrime and cyberattacks'.

The 2020 pandemic has further accelerated digital transformation. With electronic services gaining traction and the adoption of disruptive telecom technologies, many businesses that have switched to remote operations might not return to their former work patterns.

The global digital transformation is opening truly unlimited opportunities for humanity, but, likewise, cybercriminals benefit from technology and universal interconnectivity. They coalesce in gangs on the Darknet, exchange data and create large-scale attacks, taking full advantage of people's curiosity and fear.

According to the World Economic Forum, cyberattacks and data theft are the 9th most likely fallout to the world. The damage caused by these factors continues to increase and, in 2030, is projected to reach $90 trillion.

Cybercriminals are using the global instability to their advantage — the number of cyberattacks rose dramatically because of the pandemic, with most of them exploiting the coronavirus turmoil. In Q1 2020, Palo Alto Networks detected a 569% growth in COVID-19-themed malicious registrations, including malware and phishing.

This year has demonstrated that a crisis can occur unexpectedly. Our research reveals that 83% of companies have no recovery plans in place. In times of crisis, they find it most challenging to restore business operations and maintain their efficiency. A robust response plan and effective teamwork help to avoid such scenarios and minimise losses. Therefore, the increasing importance of regular training and education across all levels must not be overlooked.

This is the reason behind Cyber Polygon — an annual international exercise aimed at strengthening global cyber resilience through raising public awareness in cybersecurity and developing the competencies of technical specialists.

In addition to the technical training, where teams practise their skills in repelling cyberattacks, Cyber Polygon also features an online conference. The key topics for discussion this year covered the emerging technologies that will shape the digital future, the role of cybersecurity given the fast-paced digitalisation, and measures that organisations and the international community as a whole need to take to protect the digital space.

This report summarises the key takeaways from the lectures and interviews as well as the results of the technical training and practical recommendations based on these results.

Executive Summary

About Cyber Polygon

Cyber Polygon is a unique event that combines the world's largest cybersecurity exercise for corporate technical teams and an online conference featuring high-profile speakers.

Goals:

- develop the teams' competencies in repelling cyberattacks
- engage global organisations and corporations, namely management, in a cybersecurity dialogue
- raise public awareness in cybersecurity

Hence, the exercise is aimed at enhancing cybersecurity on all levels.

The ultimate idea behind Cyber Polygon is to ensure global cyber resilience and active intersectoral cooperation.

In 2020, it was the second time the event took place, again with the support of the World Economic Forum and INTERPOL.

The partners and participants involved in Cyber Polygon were tech companies, international organisations as well as state and law enforcement agencies coming from all corners of the globe.

Concept 2020

With the digital world being as interconnected as it is, all its participants expose themselves to a number of safety risks. A single data breach across the ocean could trigger a chain reaction and spark a 'digital pandemic' across the globe. People, organisations and entire states may fall victim to the catastrophe.

The central theme for the Cyber Polygon 2020 online stream was the **prevention of a 'digital pandemic'**. The year has demonstrated that a crisis may hit unexpectedly and we must be prepared for an emergency — to protect ourselves and entire corporations.

Information and money remain the main target of cybercriminals. In 2019–2020, the world witnessed a wave of massive data leaks — even technologically advanced companies were not always immune. This is why, for the technical part of our training, we developed an attack scenario which in real life would jeopardise company reputation and data. The teams could hone their skills in countering this type of attack in real time and investigate the incident.

Structure

Cyber Polygon featured two parallel tracks:

1. online stream for a wide audience
2. technical exercise for cybersecurity teams from organisations

Live Stream

The live stream featured top officials from international organisations and tech corporations who met online to analyse the current cybersecurity trends and risks, and discuss how to avoid a ‘digital pandemic’.

The event was launched with opening statements from the honorary guests: Mikhail Mishustin, Prime Minister of the Russian Federation, and Klaus Schwab, Founder and Executive Chairman, World Economic Forum.

The live stream also featured Herman Gref, CEO, Chairman of the Executive Board, Sberbank; the Rt. Hon. Tony Blair, Prime Minister, Great Britain and Northern Ireland (1997–2007); Jürgen Stock, Secretary General, INTERPOL; Troels Oerting, Chairman of the Advisory Board, the World Economic Forum Centre for Cybersecurity; Nik Gowing, BBC World News main presenter (1996–2014); Founder and Director, Thinking the Unthinkable; Vladimir Pozner, Journalist and broadcaster; as well as senior officials from ICANN, Visa, IBM and other global corporations.

The broadcast at Cyber Polygon 2020 gathered 5 million viewers from 57 states. Such a broad outreach is indicative of the global community beginning to recognise cybersecurity as a global issue that can only be combated through joint efforts.

5 million spectators
from **57 countries**

Technical Training

The technical exercise attracted 120 of the largest Russian and international organisations from 29 countries. These included banks, telecom companies, energy suppliers, healthcare institutions, universities as well as state and law enforcement agencies.

The teams practised response actions at the moment of a targeted attack that aimed to steal confidential data and undermine the company reputation.

The participants took the side of the **Blue Team** and worked on protecting their segments of the training infrastructure. The organisers from BI.ZONE represented the **Red Team** and simulated the attacks.

120 organisations
from **29 countries**

The exercise included two scenarios:

1. Defence

In the first scenario, the participants practised repelling a massive cyberattack in real time.

They had to manage the attack as fast as possible and minimise the amount of information stolen while maintaining availability of the infrastructure.

2. Response

The second scenario involved investigating the identified incident by applying traditional forensics as well as **Threat Hunting** — a method whereby specialists continuously hunt for threats by manually analysing security events from various sources, rather than waiting for security alerts to go off.

The teams also practised collaboration with law enforcement agencies: based on the information gathered, they composed a dossier for INTERPOL that in real life would help law enforcement to locate the criminals.

Cyber Polygon became the first international event for corporate teams of such format and scale.

How Did It Go

This year, we made our technical training scenarios as close to real-life situations as possible. To achieve this, we implemented a complex technical infrastructure, with over 400 virtual machines rolled out. Further, preliminary load testing was conducted to ensure smooth operation of all systems during the event.

In the run-up to the exercise, we released a series of technical articles. The publications helped the participants improve their knowledge of the topics covered in the scenarios and prepare better for the training. This laid the foundation of our public knowledge library, which is being enriched on a continuous basis.

The event featured the world's first public exercise for corporate teams where the Threat Hunting method was applied. We are especially pleased to realise that for many teams Cyber Polygon became the first opportunity to master this technique and thereby gain new practical experience. We strongly believe that such initiatives are an effective tool in enhancing cyber resilience through knowledge sharing.

What Is Next?

With the accelerated rate of digitalisation, the level of cybercrime will also continue to rise. In order to withstand a large-scale cyber threat, the global community needs to unite its efforts and establish collaboration at all levels: practise joint mitigation of cyberattacks, expand technical skills, and engage in open dialogue on key global cybersecurity issues.

Such events as Cyber Polygon are instrumental in achieving these goals, as they already allow experts from participating organisations to increase their skills and draw the attention of a wider audience to the issues of cybersecurity.

We continue to develop training opportunities to strengthen global cybersecurity and ensure a secure digital world and we invite you to join the next Cyber Polygon in 2021.

We hope that the results and conclusions of this year's training presented in the report as well as the knowledge of invited experts, will benefit the entire community and enable us to develop practical measures to improve global interaction in the fight against cybercrime.

Participants and Partners

Cyber Polygon 2020 attracted a variety of organisations from a range of industries: global corporations, small and medium businesses, international organisations and government structures, law enforcement agencies and healthcare institutions.

This diversity has further highlighted the global scale of cybersecurity issues and the importance of such exercises across the board.

Partners

IBM

A global technology and innovation company and the largest technology employer in the world, delivering services in 170 countries. IBM's cognitive solutions and cloud platforms help transform institutions, communities and the quality of life. It is a leading provider of high-value solutions and services to clients in a variety of industries, including government, telecommunications, healthcare, finance, retail, oil and gas.

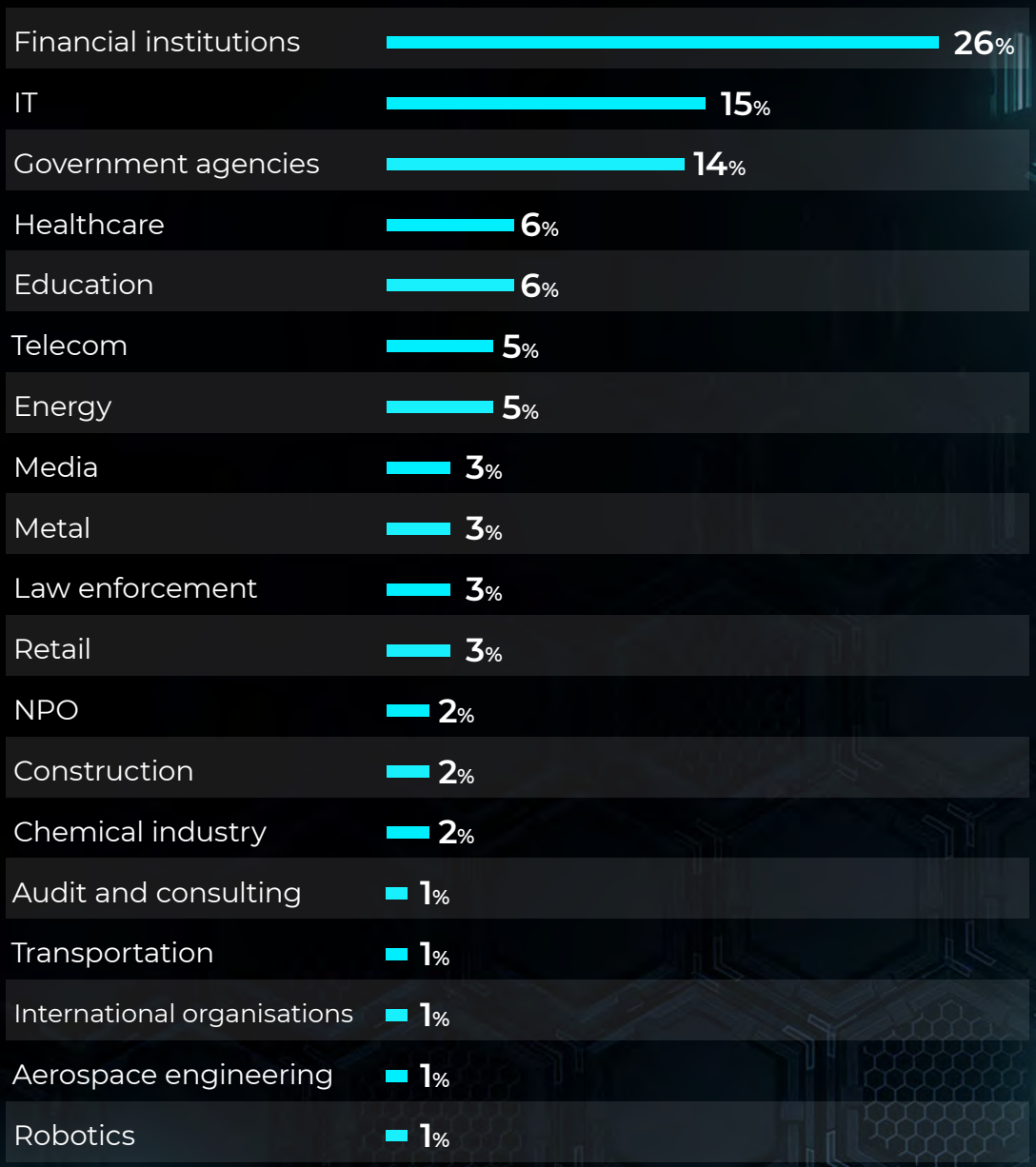
ICANN

A not-for-profit public-benefit corporation and a global community. ICANN's mission is to ensure a stable, secure, and unified global Internet. The company oversees unique identifiers that allow computers on the Internet to locate one another. ICANN ensures universal resolvability — users receive the same predictable results when they access the network from anywhere in the world.

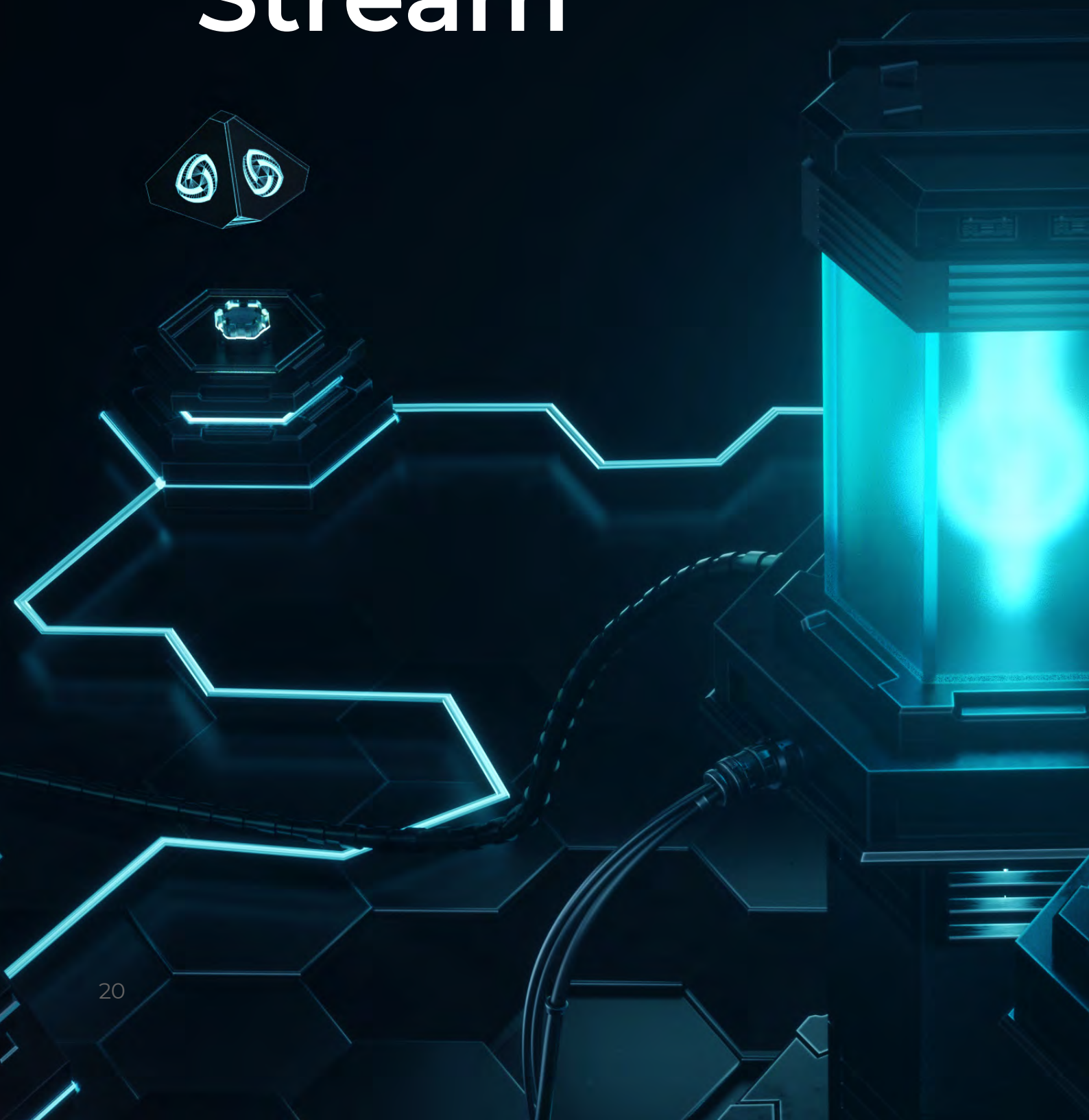
Participants

Cyber Polygon brought together participants from all continents, except Antarctica. The technical training attracted 120 organisations from 29 countries, and the live stream gathered 5 million spectators from 57 states.

The teams represented organisations from both the public and private sectors.



Live Stream



Technology and New Reality

The world won't be the same again

The pandemic has spurred digitalisation: many people have transitioned to remote work and are more and more reliant on electronic services. Effective interaction demands new communication methods and faster data transmission. Such changes pose not only additional risks and challenges to businesses, but affect people's way of life. In a dynamic technological environment and an increasingly interconnected world, cybersecurity has become and will continue to be the main focus.

'COVID-19 has accelerated various processes. Before the pandemic, we had been rather critical of digitalisation because of all the problems brought about by the new technologies. Now, everybody is beginning to understand that this process is inevitable, we need to move forward and cybersecurity plays a great role in tech innovation'.

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

'We will probably never go back to the times we had before — we will not go back to the offices. I think that more people will work from home, we will have a more flexible work relationship, which also means that the challenges we are dealing with now will remain, and we need to be ready to face them'.

Troels Oerting, Chairman of the Advisory Board,
the World Economic Forum Centre for Cybersecurity

'5G will be the platform for the society, for hospitals, for public transport, for everything that is to be connected. You need to have absolute trust in the underlying infrastructure, hence there is a high demand for security. Today, we cannot even imagine what capabilities the new 5G network will enable, and artificial intelligence will obviously be one of the key features of our technologies and tools in the development of new application services. AI can be used for predictive analytics to improve performance, maintenance and security of the network'.

Sebastian Tolstoy, Head of Eastern Europe & Central Asia
and General Director Ericsson Russia, Ericsson

'I believe the Internet of Things will be one of the biggest game changers. Industrial automation will bring the most added value globally over the next 10 years and that will be based very much on the Internet of Things'.

Alexey Kornya, President, CEO,
Chairman of the Management Board, MTS

State structures to embrace technological revolution

Governments need to adapt more quickly to the ongoing changes: not only to search for new tools and ways of interacting with people and businesses, but also to ensure the safety of such interaction. A digital identity can become one of the effective ways of communication between the state and individual citizens. However, this is only possible provided that privacy and data protection is properly regulated.

'If Clement Attlee, who served as Prime Minister in the UK from 1945 to 1951, came back to Britain today, he would see a country completely transformed in the way we work, in the way we live, in technology, in living standards, in its class structure. But then, when he went back into government, he would find himself completely at home, as everything would be familiar. The government is always the last to change, and the problem with cyber threats is that we cannot afford the government to take 10 years to catch up because at that time the damage will be too great'.

The Rt. Hon. Tony Blair, Prime Minister,
Great Britain and Northern Ireland (1997–2007)

Threats and Risks

Cybercriminals taking advantage of new digital reality

Since early 2020, the number of data breaches, phishing attacks and registrations of malicious sources has increased, and the trend is predicted to grow.

'Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19. We have seen a steep increase of new narratives in online scams, phishing approaches and targeting of critical infrastructures: health service ransomware, attacks on hospitals, exploiting the need for personal protective material and medical research'.

Jürgen Stock, Secretary General, INTERPOL

'Whenever there is a global crisis or an event of public significance, there is always an uptick in criminal activity related to such events. Therefore, it is understandable that people out there are clicking on emails or website links or report downloads that promise to provide updates on such events and thereby being lured into certain situations, and COVID-19 is no exception'.

Dhanya Thakkar, Vice President AMEA, Trend Micro

6,000% — global growth in COVID-19 related spam in March–May 2020[1]

[1] W. Whitmore, source: IBM X-Force

Critical infrastructure companies exposed to highest risk

Healthcare, the financial industry, government agencies, manufacturing, IT and telecom are at greatest risk. Being the most frequent targets of attacks, such organisations incur enormous losses. However, healthcare and manufacturing are the least protected due to the use of outdated equipment. Further, their IT infrastructure is often unable to quickly detect an intrusion as well as manage its consequences.

> *'What we are seeing now is cases of attackers squatting within organisations undetected for months, if not longer, and they have really taken their time and patience to understand the lay of the land and determine when and where they can wage a ransomware attack, how to deploy the software, and then demand money. In some recent cases, we have seen as much as $25 million being sought as ransom'.*
>
> **Wendi Whitmore**, Vice President of IBM X-Force Threat Intelligence, IBM

> *'Calculation shows that a six-hour blackout in mainland France could cost $1.5 billion. The electrical utilities, the hospital systems were not designed for the era that we are in today, so we need direct collaborations with industry leaders in different sectors — electricity, energy, healthcare, aviation — to help them strengthen their cyber posture, to increase awareness of the underlying threats'.*
>
> **Jeremy Jurgens**, Chief Business Officer and Member of the Managing Board, World Economic Forum

260% — increase in malicious COVID-related URLs in February–March 2020[2]

[2] D. Thakkar, source: Trend Micro

Fake news poses a major challenge for society

Information spreads through digital communication channels at record speeds. However, data on the web is not always trustworthy. In the era of digitisation, fake news has become a dangerous weapon being used by cybercriminals to attack people and organisations.

> *'The speed with which the digital reality is changing is far faster than any regulations can ever be constructive'.*

Nik Gowing, BBC World News main presenter (1996–2014); Founder and Director, Thinking the Unthinkable

> *'We should rely on ourselves when trying to protect against fake news: we need a good education, critical outlook, we need to compare the facts and analyse the incoming information'.*

Vladimir Pozner, Journalist and broadcaster

How to Prepare for a Cyber Crisis?

Having an emergency plan is essential

A crisis does not care for time or place. An emergency can befall any industry or company, whether now or in the future – cyber space being no exception. One of the effective ways for organisations and the entire global community to be prepared for such situations is to develop and implement an emergency plan.

> *'A cyber incident or attack can turn into a crisis if you have little capability or capacity to deal with it. If you are well-prepared, you can be more resilient and effective in responding and mitigating such events'.*

Craig Jones, Cybercrime Director, INTERPOL

Training and awareness across all levels

Businesses should take measures to enhance their cyber resilience: implement best practices in risk management and conduct regular security audits of their systems. They need to create strong teams to ensure secure operations as well as develop, test and implement crisis management and business continuity plans.

'Risk management is everyone's responsibility. Every person within an organisation is responsible for identifying and reporting risks and/or breaches to security protocol. This, of course, must be supplemented by a resilient security infrastructure and robust tools and capabilities to spot and mitigate accidental incidents, which can be caused by only one click on the wrong link'.

Hector Rodriguez, Senior Vice President, Regional Risk Officer for Central and Eastern Europe, Middle East and Africa, Visa

'I do not believe that we can put the expectation for security on each individual. I think we need to make them aware of what the risks and the challenges are, but we actually also have to move towards models that are not dependent on single individuals who can be manipulated or perhaps fail to understand the implications and therefore put entire organisations and institutions at risk'.

Jeremy Jurgens, Chief Business Officer and Member of the Managing Board, World Economic Forum

'In this negative picture of the increase in attacks there is a good thing: we have rarely seen anything so new and so novel that we are not really ready to defend against them. Many organisations are doing that very successfully and, in particular, those that have threat intelligence tailored towards their industry. They have a good understanding of what their particular attack surface looks like'.

Wendi Whitmore, Vice President of IBM X-Force Threat Intelligence, IBM

Training, education and preparation of every employee, regardless of their competencies and roles, should be recognised by businesses as a strategic priority. Each staff member at their respective level must understand security policies and procedures and know in advance how to act in an emergency.

'Regular phishing and awareness training is really important, as is analysing the results of the training to help understand how many employees click through. However, it is really easy to run the same old phishing simulations week-on-week, so it is important to think of new ways to test employees and make them think. There does not have to be a penalty around it that makes everybody upset or worried about the training, but you do need to think about how to challenge the organisation'.

Jacqueline Kernot, Partner in Cybersecurity, Ernst & Young

'We need to continue with the pace of introducing cyber hygiene rules as criminals do not want to invest 1 dollar to steal 50 cents, they want it automated, so if it is too difficult, they will move on to somebody else'.

Troels Oerting, Chairman of the Advisory Board, the World Economic Forum Centre for Cybersecurity

Effective protection builds on trust and collaboration

A critical situation cannot be tackled by an organisation or a lone individual. In a highly interconnected world, a single cyber attack can spread exponentially across the global community. This situation can be prevented by promoting collaboration between the public and private sectors and law enforcement agencies. Furthermore, efficient interaction requires the implementation and regulation of a range of standards, the exchange of information and establishing trustworthy relationships.

'As for a global community, awareness, education and prevention are vital. As the head of an organisation that unites law enforcement worldwide, I can say that we need even greater cooperation and information exchange in tackling the threat of cybercrime'.

Jürgen Stock, Secretary General, INTERPOL

'We should find new mechanisms for cooperation to combat cybercrime — this could be international conventions or international treaties'.

Petr Gorodov, Head of the General Directorate for International Relations and Legal Assistance of the Prosecutor General's Office of the Russian Federation

'Regulatory frameworks and government intervention in the cybersecurity space are important. I have certainly had clients tell me that it is government intervention or regulation that has made them change the way that they operate'.

Jacqueline Kernot, Partner in Cybersecurity, Ernst & Young

'We at ICANN understand the domain name system and the DNS industry probably as much or better than anybody else out there. So one of the things we can do, is to work with those who combat criminality to help them understand the effects of their actions and to make sure that they get the results they intend'.

John Crain, Chief Security, Stability & Resiliency Officer, ICANN

60% — share of cloud attacks that used previously exploited data and vulnerabilities[3]

[3] W. Whitmore, source: IBM X-Force

'We want to have a world that is collaborative, so we are now building a network of cyber volunteers out of the capable and the willing in order to work collectively to achieve cyber peace'.

Stéphane Duguin, CEO, CyberPeace Institute

Technical Training

Scenarios

The training was essentially a challenge between two opposing sides: the **Red Team** (the attacker) vs the **Blue Team** (defence teams).

The participants acted as the Blue Team. They had to perform a variety of tasks: assess infrastructure security of a fictional organisation CyberCorp, search for and remediate potential vulnerabilities as well as identify and respond to security incidents.

The organisers (BI.ZONE) assumed the role of the Red Team seeking to compromise the secured systems by identifying and exploiting weaknesses in CyberCorp's infrastructure.

Each participating team was given access to their own dedicated IT infrastructure under the guise of CyberCorp. The infrastructure was created specifically for the training and was deployed on an IBM cloud.

The training had a range of distinctive features:

- It was targeted at corporate teams, rather than individuals, for the participants to practise collaborative teamwork.
- Given that the attack was carried out by the organisers themselves, all the teams were on an equal playing field and had the opportunity to objectively assess their capabilities.
- The companies did not risk their reputation: the teams were assigned numbers to disguise the real names of their organisations.
- The participants' own business IT infrastructure was not involved.

Scenario 1. Defence — the teams developed their skills in repelling a large-scale attack in real time.

Scenario 2: Response — the participants investigated the incident using traditional computer forensics and Threat Hunting techniques.

Scenario 1. Defence

According to the first scenario, CyberCorp's infrastructure included a public service, which processed confidential client information. This service became the subject of interest to an APT group. Cybercriminals were going to steal confidential user data in order to receive financial benefits and cause damage to company reputation. The APT group studied the target system in advance, discovered a number of critical vulnerabilities and carried out an attack.

The participants had to confront the actions of cybercriminals at the moment of the attack. They were expected to find and eliminate the vulnerabilities in the service as fast as possible and thus minimise the amount of stolen information while maintaining service availability.

The amount of leaked data was assessed by the number of **flags** that the APT group was able to steal. The teams had to analyse the service code, the attackers' network activity and determine which vectors were used to conduct the attack and seize the flags.

Flag — a string with a strictly defined format, which is used in CTF (Capture the Flag) cybersecurity competitions. The players' main goal is to locate the hidden string, i.e. 'capture the flag'.

They were allowed to apply any methods to defend their infrastructure, provided that they did not disrupt service operations.

The first scenario accumulated some of the best ideas found in modern training activities **(Attack-Defence CTF, Red Teaming)** as well as cybersecurity courses.

Selecting the data breach attack scenario, where a web application vulnerability is exploited, was done for good reason: web applications remain one of the most popular attack vectors. According to the Verizon Data Breach Investigations Report 2020, they account for 43% of attacks against organisations.

Attack-Defence CTF — a CTF competition where teams are required to defend their services (i.e. prevent them from being attacked by other participants) and, at the same time, attack opposing teams' services by taking advantage of their vulnerabilities. To win points, players must 'capture' the opponent's flag, which proves that the vulnerability has been exploited successfully.

Red Teaming — a cybersecurity exercise that simulates an attack on the existing corporate infrastructure by imitating real-life conditions and methods applied by hacker groups.

43% of data leaks in 2020 featured attacks on web applications

Scenario 2. Response

The second scenario consisted of two rounds, each of which included tasks aimed at practising response actions to the identified cybersecurity incident, though, with different approaches applied.

According to the **first-round** legend, CyberCorp discovered that its infrastructure had been compromised given the number of anomalies in the outbound traffic. The character of those anomalies suggested that the attack might be associated with a widely known APT1337 group. CyberCorp's cybersecurity team isolated one of the suspicious hosts from the corporate network and collected artifacts for investigation.

The participants had to analyse the artifacts and solve the tasks by applying any tools available.

During the first round, the participants were encouraged to apply and develop classic forensics skills, when all the necessary artifacts are collected after the attack and the response team is trying to trace the incident. This is what is known as the **reactive** approach.

According to the **second-round** legend, following a cybersecurity incident, CyberCorp purchased and rolled out an **EDR (Endpoint Detection and Response)** solution in its infrastructure, with agents installed on all the workstations and servers. The extended telemetry gathered by such endpoints was sent to the centralised Threat Hunting platform for proactive threat detection. The company also invited a team of expert analysts to build a detection process based on the Threat Hunting approach.

Endpoint Detection and Response (EDR) — a solution designed to detect and respond to cybersecurity incidents at endpoints (workstations and servers). EDR collects, processes and analyses extended telemetry from endpoints with the purpose of detecting abnormal activity; and provides a variety of tools to respond to such activity (both automatically and upon request).

There was some information published on the web about a new technique used by attackers to gain a foothold in the system — better known as Persistence. One of the experts decided to check whether this method was employed in the CyberCorp attack. The hypothesis proved true: one host in the infrastructure was found affected by this technique.

This discovery became the starting point of the investigation. By analysing the telemetry collected on the Threat Hunting platform, the teams had to understand how the threat actor had infiltrated the infrastructure and piece together the sequence of their actions.

While Threat Hunting is not an alternative to traditional forensics, **proactive** collection of security events as well as the ability to quickly obtain artifacts from the EDR agents, can speed up, simplify and improve incident response and investigation.

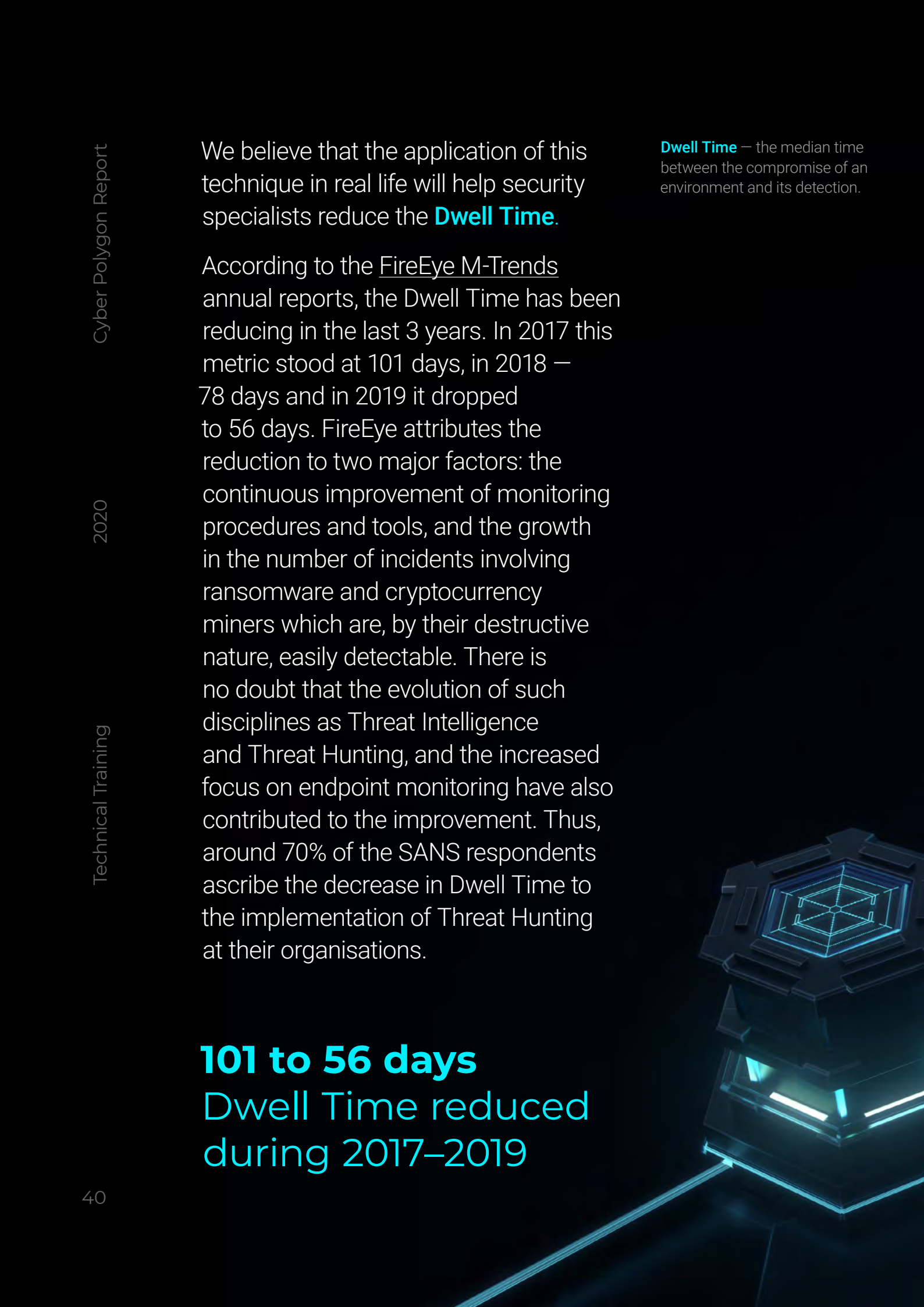
According to the SANS 2019 Threat Hunting survey, many organisations have not yet realised the essence of proactive detection of vulnerabilities and what benefits they get with this technology. Therefore, when developing the second scenario, we hoped that practising Threat Hunting and applying the hypothesis-based method will help the participants gain the required experience and enhance their trust in this approach.

We believe that the application of this technique in real life will help security specialists reduce the **Dwell Time**.

Dwell Time — the median time between the compromise of an environment and its detection.

According to the FireEye M-Trends annual reports, the Dwell Time has been reducing in the last 3 years. In 2017 this metric stood at 101 days, in 2018 — 78 days and in 2019 it dropped to 56 days. FireEye attributes the reduction to two major factors: the continuous improvement of monitoring procedures and tools, and the growth in the number of incidents involving ransomware and cryptocurrency miners which are, by their destructive nature, easily detectable. There is no doubt that the evolution of such disciplines as Threat Intelligence and Threat Hunting, and the increased focus on endpoint monitoring have also contributed to the improvement. Thus, around 70% of the SANS respondents ascribe the decrease in Dwell Time to the implementation of Threat Hunting at their organisations.

101 to 56 days
Dwell Time reduced during 2017–2019



Results

We intentionally avoided using real names of the organisations so as not to set off a competition between the participants and keep their results confidential. However, the teams could compare their progress with the others using the scoreboard. The table below shows 10 teams (out of a total of 120) with the highest score.

Rating	Team	Industry	Total Score	Scenario 1. Defence	Scenario 2. Response (Round 1)	Scenario 2. Response (Round 2)
			max: 2700	max: 900	max: 900	max: 900
1	Team 29	Financial institutions	1329	207	552	570
2	Team 67	IT	1261	331	750	180
3	Team 53	IT	1213	223	600	390
4	Team 14	Education	1158	480	303	375
5	Team 41	Financial institutions	857	227	495	135
6	Team 33	Financial institutions	753	243	480	30
7	Team 6	IT	677	95	252	330
8	Team 3	Audit and consulting	633	0	351	282
9	Team 11	Robotics	620	200	330	90
10	Team 16	IT	595	205	300	90

Conclusions

The following conclusions can be drawn based on the final results achieved by the participants:

Participants could assess their capabilities

It was not clear until the end of the exercise who would take the first place. Different teams were leading at different stages, which means that none of them could fully utilise the techniques at their disposal.

The exercise allowed the participants to identify their strengths and weaknesses. We hope that the received information will help them create plans for developing the necessary competencies and improve their results in the future.

Financial institutions and IT delivered the best results

Banks and companies from the IT industry demonstrated the highest resilience. Security assessment expertise in these sectors is quite well developed, with classic forensics and Threat Hunting widely applied.

Specialists are better prepared for investigation than defence

27% of the teams had difficulties earning points for the first scenario, which allows us to conclude that some of the team members lack or have insufficient expertise in security assessment and protection of web applications.

At the same time, all the participants were awarded points for the first round of the second scenario, which is indicative of each team having at least one expert who is competent in traditional forensics.

The Threat Hunting approach is uncharted for most organisations

21% of the teams could not earn a single point for the second round of the second scenario. We attribute this to Threat Hunting being a relatively novel approach and the majority of organisations lacking experience of applying its techniques in practice. This creates the potential for developing teams and tools within the companies. Threat Hunting is not an alternative to classic forensics and cannot replace it, but we showed how this approach can supplement conventional methods.

More effort in preparation — better result

The best results were predictably achieved by the teams who had asked many questions during the preparation and familiarised themselves with the new techniques and defences beforehand. We hope that our Cyber Polygon publications as well as other hosted events, will increase future participants' chances of succeeding and effectively countering cyberattacks.


cyberpolygon.com