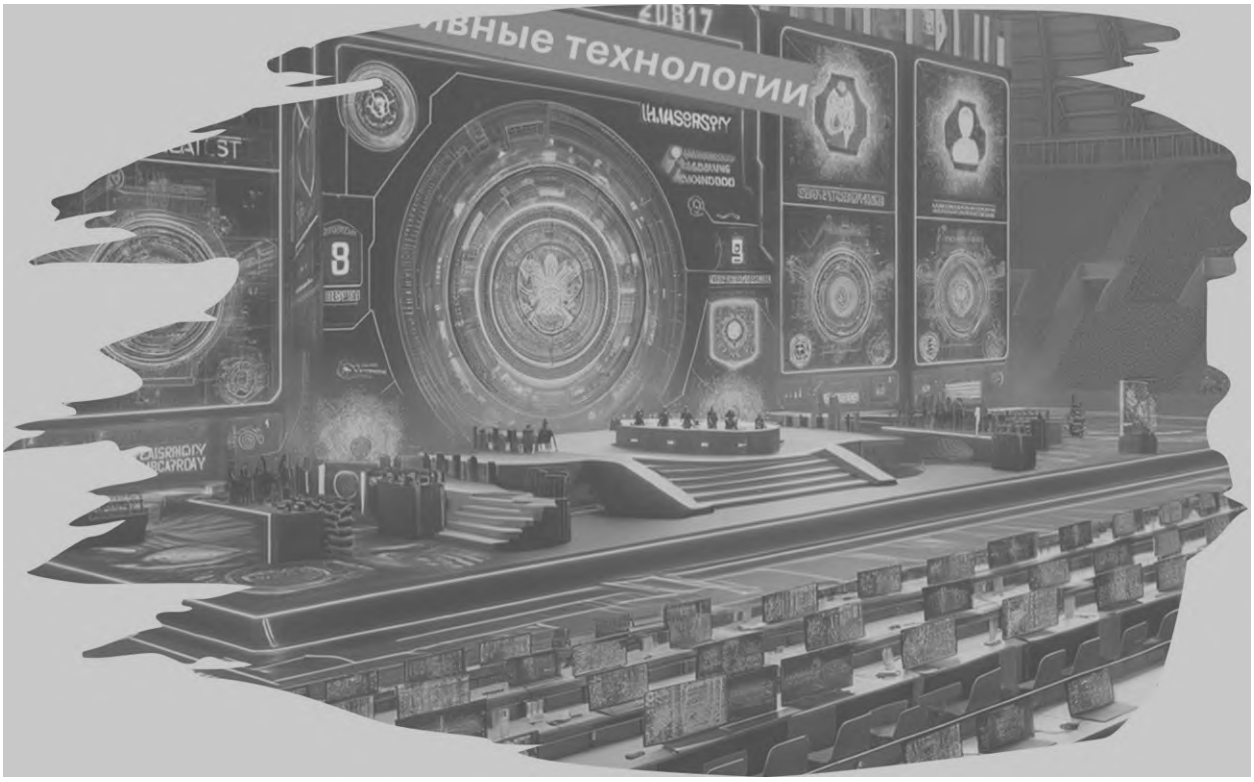
PH Days Moscow Sanctioned Organizations – Likely Outcomes

Treadstone 71



Contents

Intro

The US-sanctioned Ravin Academy, an Iranian cybersecurity training institute supported by Iran's MOIS and IRGC, recently attended Positive Hack Days (PHDays) alongside Positive Technologies and Kaspersky in Moscow. Each is known for its cybersecurity expertise and presents significant concerns under US sanctions or bans. The training and collaboration at PHDays could enhance Ravin Academy's malware development skills, potentially leading to sophisticated cyber-attacks on US, Israeli, and NATO targets. Continuous monitoring and intelligence gathering are essential to mitigate these emerging threats and ensure robust cybersecurity defenses.[1]

The Brief

The advanced training and collaboration at Positive Hack Days (PHDays) among Ravin Academy, Positive Technologies, and Kaspersky pose significant cybersecurity threats, leading to new sophisticated cyber-attacks on US, Israeli, and NATO targets, necessitating enhanced vigilance and strategic countermeasures. Continuous monitoring and intelligence gathering are critical to anticipating and mitigating these threats.

- Ravin Academy- An Iranian cybersecurity training institute sanctioned by the US for supporting Iran's MOIS and IRGC.
- Positive Technologies- A Russian cybersecurity firm sanctioned by the US for activities against US national security interests, highly likely integrated with Russian intelligence.
- Kaspersky- A Russian cybersecurity company banned from the US government and NATO systems due to alleged ties with Russian intelligence.

--

- Training at PHDays- Ravin Academy members are likely undergoing advanced malware development training.
- Collaboration- Interaction between these entities at PHDays, sharing knowledge and tools.

[1] Note- There are many other Russia and non-Russia companies (China, -Syrian, Pakistani, etc.) other than what is covered in this report. There is a picture list of all speakers in Appendix A below with their listed country.

--

- Enhanced Malware Skills- The training enhances Ravin Academy's offensive capabilities, potentially leading to more sophisticated cyber-attacks.
- Increased Collaboration- Sharing advanced cyber tools and techniques amplifies collective cyber threat capabilities.
- Knowledge Transfer- Ravin Academy disseminates newly learned skills and techniques, expanding Iran's offensive cyber workforce.

--

- Recent Attendance- Ravin Academy attended PHDays, held from May 23 to 26, 2024, at the Luzhniki sports complex in Moscow, engaging in activities that enhance their cyber capabilities.

--

- Potential for Sophisticated Attacks- Enhanced skills and collaboration could result in more complex cyber-attacks that are harder to detect and mitigate.

--

- Increased Cyber Attacks- Expect a rise in sophisticated attacks on US, Israeli, and NATO targets involving advanced malware.
- Collaboration and Tool Sharing- Enhanced capabilities due to shared knowledge and tools.
- Knowledge Transfer- Training programs in Iran could increase the number of skilled cyber operatives, leading to coordinated attacks.

--

Defensive Perspective

- Enhanced Monitoring- Implement advanced threat detection and response systems.
- Strategic Countermeasures- Develop and deploy strategic measures to counteract sophisticated malware.
- International Cooperation- Strengthen cooperation and information sharing among global cybersecurity agencies.

Offensive Perspective

- Proactive Measures- Conduct offensive cyber operations to disrupt potential threats.
- Intelligence Operations- Increase intelligence operations to infiltrate and disrupt the activities of these cyber units.

--

- Detection Capabilities- Existing detection methods may not be sufficient against advanced evasion techniques.
- Resource Allocation- Potential lack of resources dedicated to continuous monitoring and intelligence gathering.

Expanded Analysis of Ravin Academy's Malware Development Training and Collaboration at PHDays by Positive Technologies with Kaspersky

Ravin Academy, an Iranian cybersecurity training institute, was sanctioned by the US Department of Treasury for its support of Iran's Ministry of Intelligence and Security (MOIS) and the Islamic Revolutionary Guard Corps (IRGC). The Academy offers non-inclusive defensive and offensive cybersecurity training, including hacking skills associated with activities that disrupt communications during Iranian protests.

Recently, members of Ravin Academy attended Positive Technologies' Positive Hack Days (PHDays) event in Moscow alongside Kaspersky. The gathering of sanctioned entities, known for their expertise in cybersecurity, raises significant concerns about the potential for collaboration and the enhancement of their cyber capabilities.

Positive Technologies, a Russian cybersecurity firm, has also been sanctioned by the US for activities against US national security interests, is known for sophisticated security solutions such as MaxPatrol 10 and PT Network Attack Discovery, designed for managing vulnerabilities, detecting hidden threats, and enhancing the effectiveness of Security Operations Centers (SOCs).

Kaspersky, another participant, has faced bans from use on US government and NATO systems due to alleged ties with Russian intelligence. The involvement of Kaspersky at

PHDays suggests a potential for knowledge exchange that could bolster the cyber capabilities of Ravin Academy and other sanctioned entities.

PHDays is a prominent cybersecurity event held annually in Moscow and organized by Positive Technologies. The event features various activities, including hacking competitions, technical talks, and workshops. The year's event, scheduled from May 23 to 26, 2024, at the Luzhniki sports complex, promises to be a significant convergence of cyber expertise. Notable activities include "The Standoff," a high-profile hacking contest simulating real-world cyber-attack and defense scenarios. Technical talks and presentations cover the latest developments in cybersecurity, including malware detection, rootkit evolution, and advanced persistent threats (APTs).

Potential Malware Development Training

Given the context of PHDays and the expertise of Positive Technologies and Kaspersky, it is likely that Ravin Academy members are undergoing advanced malware development training. The training encompasses sophisticated areas crucial for enhancing offensive cyber capabilities.[2]

Rootkit Development and Evolution

Rootkits are among the most insidious forms of malware, designed to gain unauthorized access and maintain persistent control over a computer system while concealing their presence. Training in rootkit development at PHDays would involve understanding their historical development and the techniques used to embed them deeply within operating systems.

Scenario- Ravin Academy members might be learning how to create kernel-mode rootkits, which operate at the lowest level of the operating system, making them extremely difficult to detect and remove. They might explore using advanced hooking techniques to intercept system calls and API functions, ensuring the rootkit remains hidden while allowing malicious activities to continue undetected.

Evolution of Rootkits- The training likely covers the progression from early user-mode rootkits, which were relatively more straightforward to detect, to more sophisticated kernel-mode rootkits and firmware-level rootkits that can persist through system reboots and even OS reinstalls. Participants may also learn about bootkits, a rootkit

[2] See Appendix A – Malware Table

that infects the master boot record (MBR) or UEFI, gaining control before the OS loads.

Advanced Persistent Threat (APT) Techniques

Advanced Persistent Threats are a form of cyberattack where unauthorized users gain prolonged access to a network to steal sensitive data. Managing APTs involves mastering techniques for maintaining long-term access to systems without detection.

Scenario- Ravin Academy trainees could learn to use a multi-stage attack approach, starting with spear-phishing or zero-day exploits to gain initial access. They might then move on to lateral movement techniques within the network, using legitimate credentials and tools to avoid detection. The goal is to understand how to set up a command-and-control infrastructure that allows continuous data exfiltration.

Management of APTs- Training would also include strategies for data exfiltration that minimize the risk of detection, such as encoding stolen data to blend with regular traffic or using steganography to hide data within images. The focus would be maintaining persistence by creating multiple backdoors, leveraging legitimate software, and using living-off-the-land (LotL) techniques.

Malware Detection Evasion

Evading modern detection methods is crucial for any successful malware operation. Training would cover various techniques to bypass antivirus software, endpoint detection and response (EDR) systems, and network security tools.

Scenario- Attendees may learn about polymorphic and metamorphic malware techniques, which constantly change the malware's code to evade signature-based detection. They might also explore using obfuscation methods, such as packing and encryption, to hide the true nature of the malware from static analysis tools.

Advanced Techniques- Other evasion techniques include anti-debugging and anti-virtualization checks to prevent malware from analysis in sandbox environments. They may also learn about advanced evasion tactics like fileless malware, which resides in the system's memory and does not leave a footprint on the disk, making it harder to detect with traditional file-based scanning methods.

Ransomware Development

Ransomware has become one of the most lucrative forms of cybercrime. Training in ransomware development would focus on creating malware capable of encrypting a victim's data and demanding a ransom for decryption.

Scenario- Ravin Academy participants may learn how to design ransomware that uses robust encryption algorithms, ensuring that the decrypting of encrypted data is unlikely without the corresponding key. They would learn to implement secure critical management systems that prevent recovery without paying the ransom.

Ensuring Persistence- Training would also cover methods to ensure that the ransomware remains on the victim's system until the ransom is paid, involving techniques such as deleting or disabling system recovery options, spreading across the network to infect backup systems, and using time-delayed payloads to evade initial detection.

Exploiting Zero-Day Vulnerabilities

Zero-day vulnerabilities are undisclosed software flaws that attackers exploit before developers can issue patches. Training in this area would involve identifying and exploiting these vulnerabilities to deploy malware.

Scenario- Attendees could learn to perform detailed code analysis and fuzz testing to discover new vulnerabilities. They might also explore exploit development frameworks that automate the creation of exploits for discovered vulnerabilities.

Deployment Techniques- Once identified, zero-day training would likely cover strategies for deploying malware using these exploits, such as delivering payloads through various vectors such as malicious email attachments, compromised websites, or drive-by downloads and ensuring that the malware can execute successfully without detection by security measures.

The advanced malware development training that Ravin Academy members are likely undergoing at PHDays covers a broad spectrum of sophisticated cyber-attack techniques. These individuals enhance their capabilities by mastering rootkit development, APT management, malware detection evasion, ransomware development, and zero-day exploitation, posing a substantial risk to global cybersecurity, particularly for US, Israeli, and NATO targets, necessitating proactive and comprehensive countermeasures. Understanding the full scope and potential impact of this training is critical for anticipating and mitigating future cyber threats.

Hypotheses and Scenarios

Enhanced capabilities from training at PHDays could lead to an uptick in sophisticated cyber-attacks against US, Israeli, and NATO targets. These attacks might involve advanced malware that is harder to detect and mitigate.

Scenario- Following their training at PHDays, Ravin Academy members could develop and deploy new strains of malware that incorporate advanced evasion techniques learned from Positive Technologies and Kaspersky. For instance, they might create polymorphic or metamorphic malware that frequently changes its code signature, making it difficult for traditional antivirus software to detect. They could also utilize rootkits and fileless malware to maintain persistent access to targeted systems.

Example Attack- Imagine a scenario where a new malware strain targets critical infrastructure in the US, such as power grids or water treatment facilities. The malware could exploit zero-day vulnerabilities in industrial control systems (ICS) to gain initial access. Once inside, it could deploy rootkits to hide its presence and use advanced persistent threat (APT) techniques to exfiltrate sensitive data over an extended period. The malware's ability to evade detection and its persistent nature would make it a formidable threat, requiring sophisticated detection and response strategies.

--

Ravin Academy might share newly acquired tools and techniques with other Iranian cyber units, amplifying their collective cyber threat capabilities.

Scenario- After attending PHDays, Ravin Academy members return to Iran with new tools and techniques. They collaborate with other Iranian cyber units, such as those within the MOIS or IRGC, to integrate these advanced capabilities into their existing cyber arsenals. The collaboration could involve sharing malware source code, attack methodologies, and defensive evasion tactics.

Example Collaboration- Suppose Ravin Academy obtains a sophisticated rootkit from Positive Technologies that is highly effective at evading detection. They could modify this rootkit to suit the needs of different Iranian cyber units. For instance, one unit might target financial institutions for espionage, while another uses it to disrupt communication networks in adversary countries. The shared knowledge and resource pooling would significantly enhance Iran's cyber capabilities.

--

The knowledge and techniques learned from Positive Technologies and Kaspersky help train additional cyber operatives in Iran, expanding their offensive cyber workforce.

After gaining advanced knowledge at PHDays, Scenario- Ravin Academy members could return to Iran and establish new training programs to disseminate this knowledge to a broader group of cyber operatives. These programs might include hands-on workshops, simulated attack scenarios, and detailed lectures on malware development and evasion techniques.

Example Training Program- Imagine a comprehensive training program where experienced Ravin Academy members teach recruits about advanced malware development. The curriculum could cover topics like constructing polymorphic viruses, using steganography to hide malicious payloads within images, and implementing secure command-and-control (C2) infrastructures for APT operations. By training more cyber operatives, Iran could increase its capacity to conduct widespread and coordinated cyber-attacks on global targets.

The advanced training and collaboration observed at Positive Hack Days (PHDays) among Ravin Academy, Positive Technologies, and Kaspersky pose significant cybersecurity threats. The potential enhancement of malware development skills, increased collaboration among these entities, and expanded training efforts could result in more sophisticated and widespread cyber-attacks targeting US, Israeli, and NATO assets.

Enhanced Malware Development Skills

Training at PHDays provides Ravin Academy members access to innovative malware development techniques, such as understanding the intricacies of rootkits, advanced persistent threats (APTs), malware detection evasion, ransomware development, and zero-day vulnerability exploitation. The acquisition of such advanced skills enables the creation of highly sophisticated malware that is more difficult to detect and mitigate, posing a severe risk to critical infrastructure and national security.

Example Scenario- An attack could involve a newly developed rootkit that uses advanced evasion techniques learned at PHDays. Without detection, the rootkit could infiltrate and maintain access to critical systems, such as power grids or

financial networks. The resulting disruption could lead to significant economic and operational impacts.

Increased Collaboration

The collaboration between Ravin Academy, Positive Technologies, and Kaspersky at PHDays suggests a pooling of resources and expertise. The partnership leads to the development and sharing of advanced cyber tools and techniques. Ravin Academy, known for supporting Iranian intelligence operations, could integrate these advanced capabilities into its cyber arsenal, enhancing its offensive operations.

Example Collaboration- Suppose Ravin Academy acquires a sophisticated malware toolkit from Positive Technologies. They could modify and adapt this toolkit to suit various cyber operations, from espionage to disruption of critical services. By sharing these tools with other Iranian cyber units, they amplify their collective threat capabilities, posing a heightened risk to adversaries.

Expanded Training Efforts

The knowledge and techniques learned at PHDays will be disseminated through structured training programs within Iran. These programs could expand the offensive cyber workforce by equipping recruits with advanced skills in malware development, network infiltration, and data exfiltration. The broader base of trained operatives increases the capacity for large-scale, coordinated cyber-attacks.

Example Training Program- A comprehensive cyber training program where seasoned Ravin Academy members train new operatives in advanced cyber tactics, something they are already in process. The program might include hands-on labs, simulated cyber-attacks, and detailed instructions on evading modern security measures. The result is a more robust and capable cyber force ready to conduct sophisticated operations against high-value targets.

Monitoring and Strategic Countermeasures

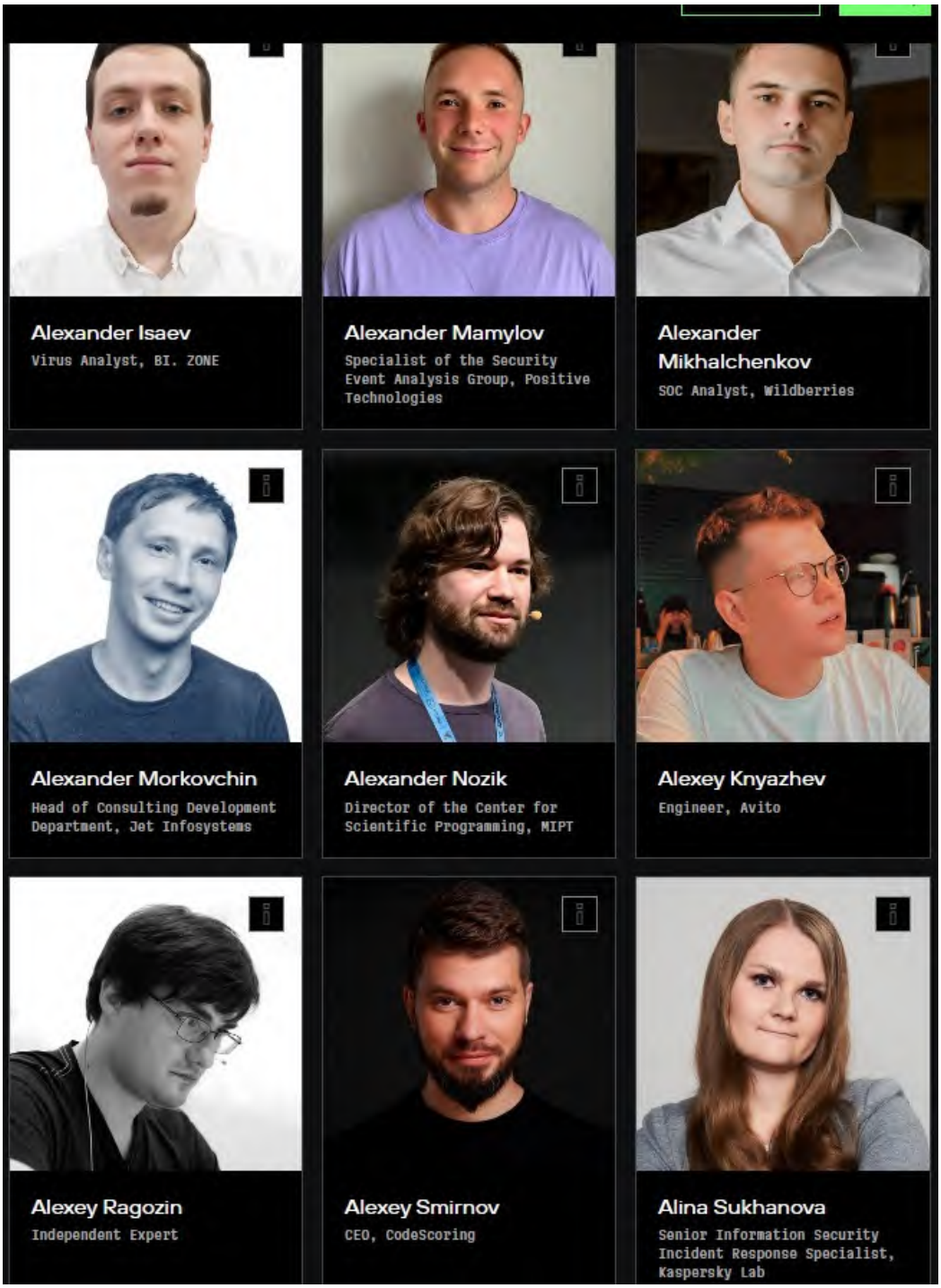
Given these developments, continuous monitoring and intelligence gathering at Ravin Academy, Positive Technologies, and Kaspersky are critical. Understanding the nature and scope of their activities enables the anticipation and mitigation of emerging cyber threats. Develop strategic countermeasures to address the enhanced capabilities resulting from this collaboration.

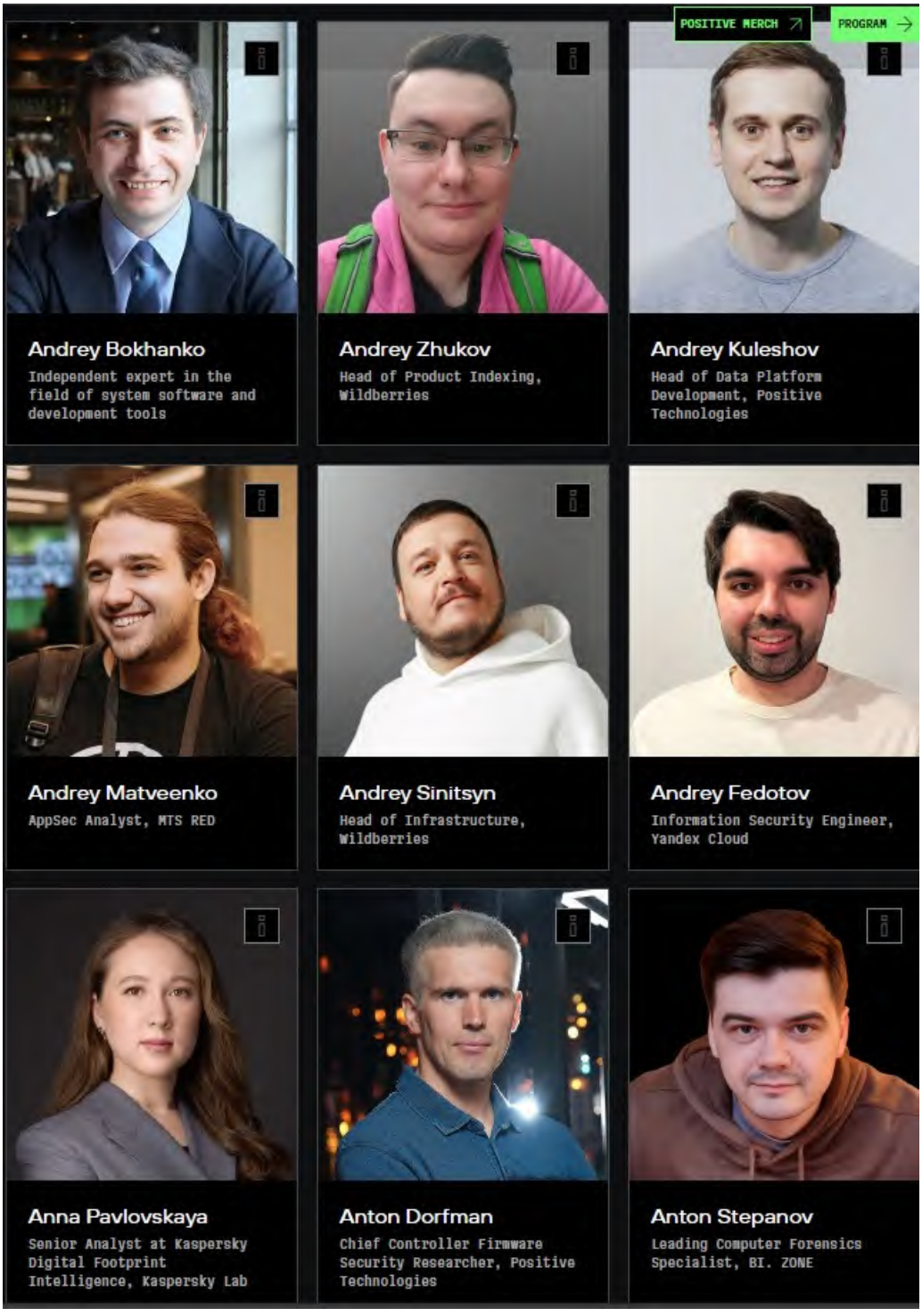
Governments and organizations should invest in advanced threat detection and response systems to counter the sophisticated malware likely to emerge from this collaboration. Enhanced cooperation and information sharing among international cybersecurity agencies can help identify and neutralize threats more effectively. Regularly updating and patching systems to address vulnerabilities is also crucial in mitigating the risk of advanced cyber threats.

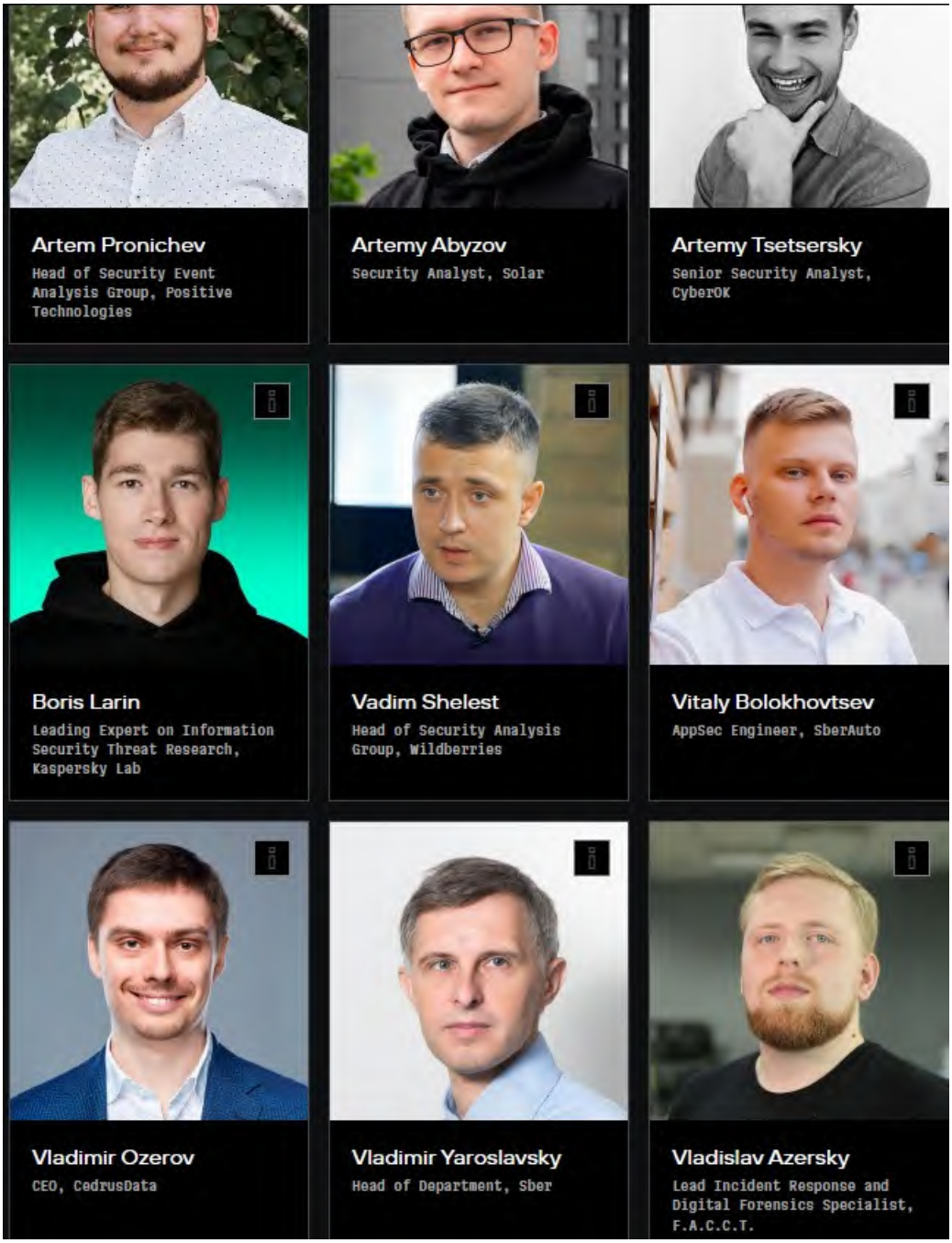
The collaboration and training facilitated at PHDays among Ravin Academy, Positive Technologies, and Kaspersky present a significant cybersecurity concern. The enhanced capabilities in malware development, increased collaboration, and expanded training efforts underscore the need for heightened vigilance and strategic countermeasures. Continuous monitoring and intelligence gathering on these entities and their activities are crucial for anticipating and mitigating emerging cyber threats, thereby ensuring robust cybersecurity defenses and protecting critical infrastructure.

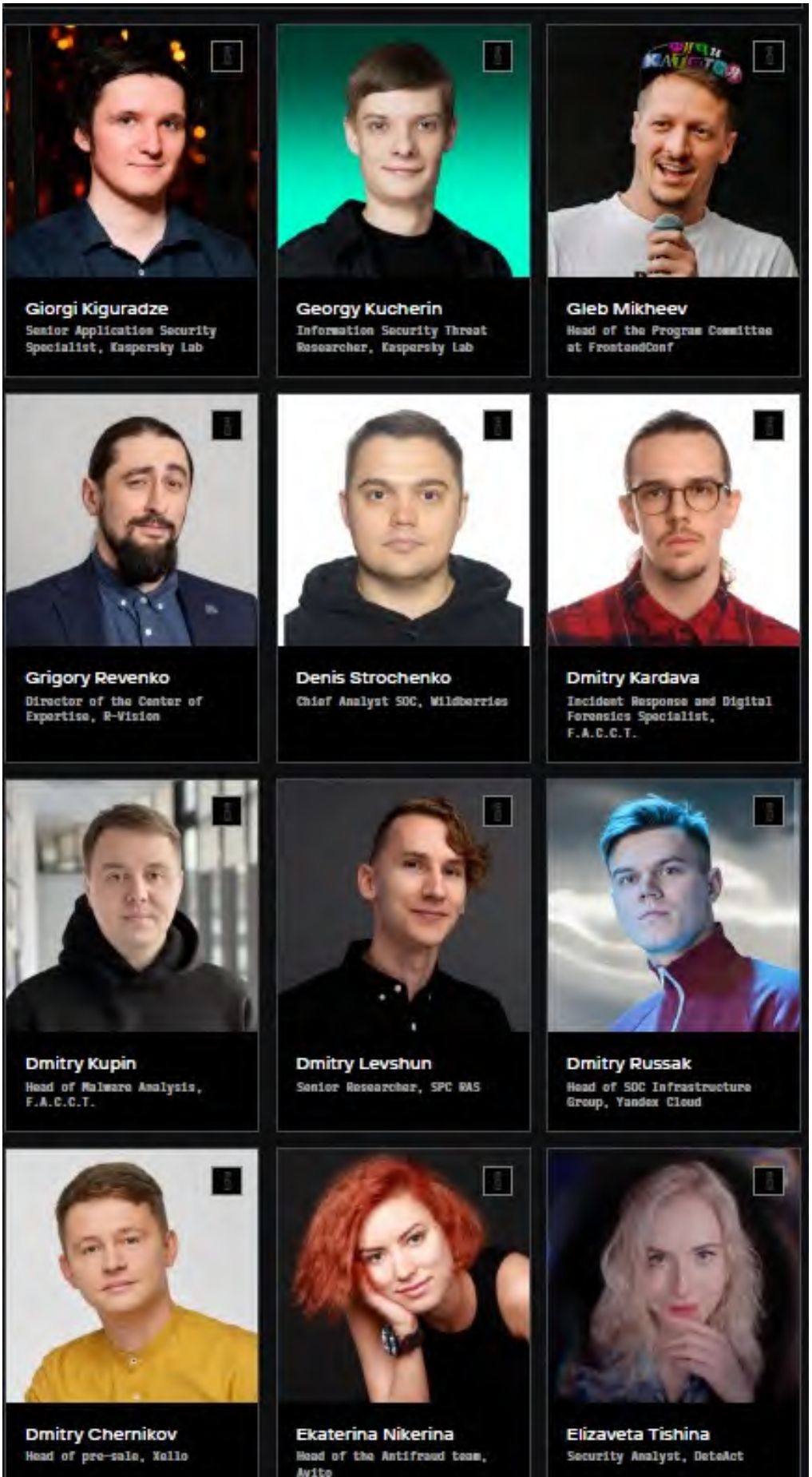
Appendix A

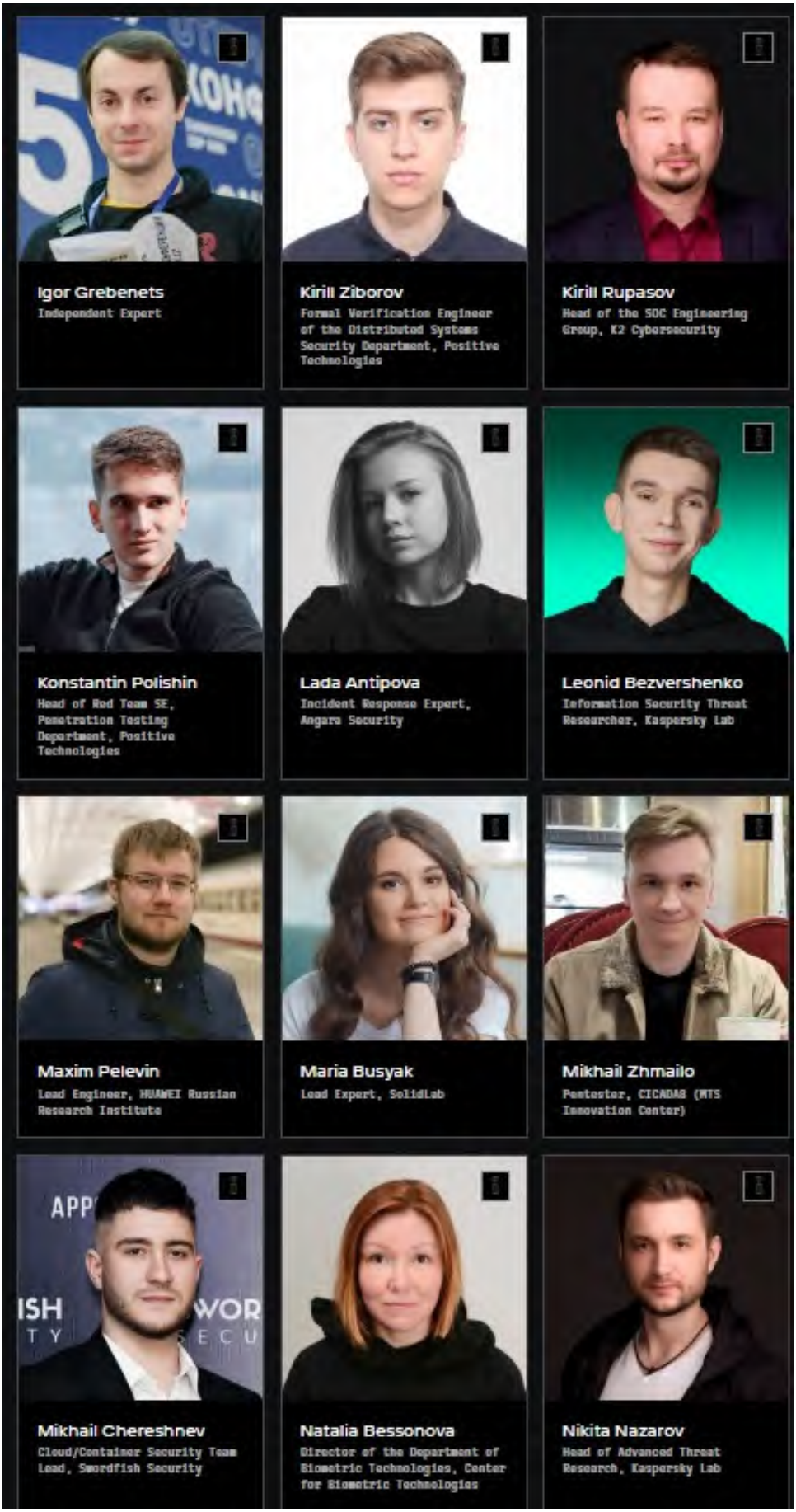
PHDays








Giorgi Kiguradze
Senior Application Security Specialist, Kaspersky Lab
Georgy Kucherin
Information Security Threat Researcher, Kaspersky Lab
Gleb Mikheev
Head of the Program Committee at FrontendConf
Grigory Revenko
Director of the Center of Expertise, R-Vision
Denis Strochenko
Chief Analyst SOC, Wildberries
Dmitry Kardava
Incident Response and Digital Forensics Specialist, F.A.C.C.T.
Dmitry Kupin
Head of Malware Analysis, F.A.C.C.T.
Dmitry Levshun
Senior Researcher, SPC RAS
Dmitry Russak
Head of SOC Infrastructure Group, Yandex Cloud
Dmitry Chernikov
Head of pre-sale, Xello
Ekaterina Nikerina
Head of the Antifraud team, Avito
Elizaveta Tishina
Security Analyst, DataAct



Igor Grebenets
Independent Expert

Kirill Ziborov
Formal Verification Engineer of the Distributed Systems Security Department, Positive Technologies

Kirill Rupasov
Head of the SOC Engineering Group, K2 Cybersecurity

Konstantin Polishin
Head of Red Team SE, Penetration Testing Department, Positive Technologies

Lada Antipova
Incident Response Expert, Angara Security

Leonid Bezvershenko
Information Security Threat Researcher, Kaspersky Lab

Maxim Pelevin
Lead Engineer, HUAWEI Russian Research Institute

Maria Busyak
Lead Expert, SolidLab

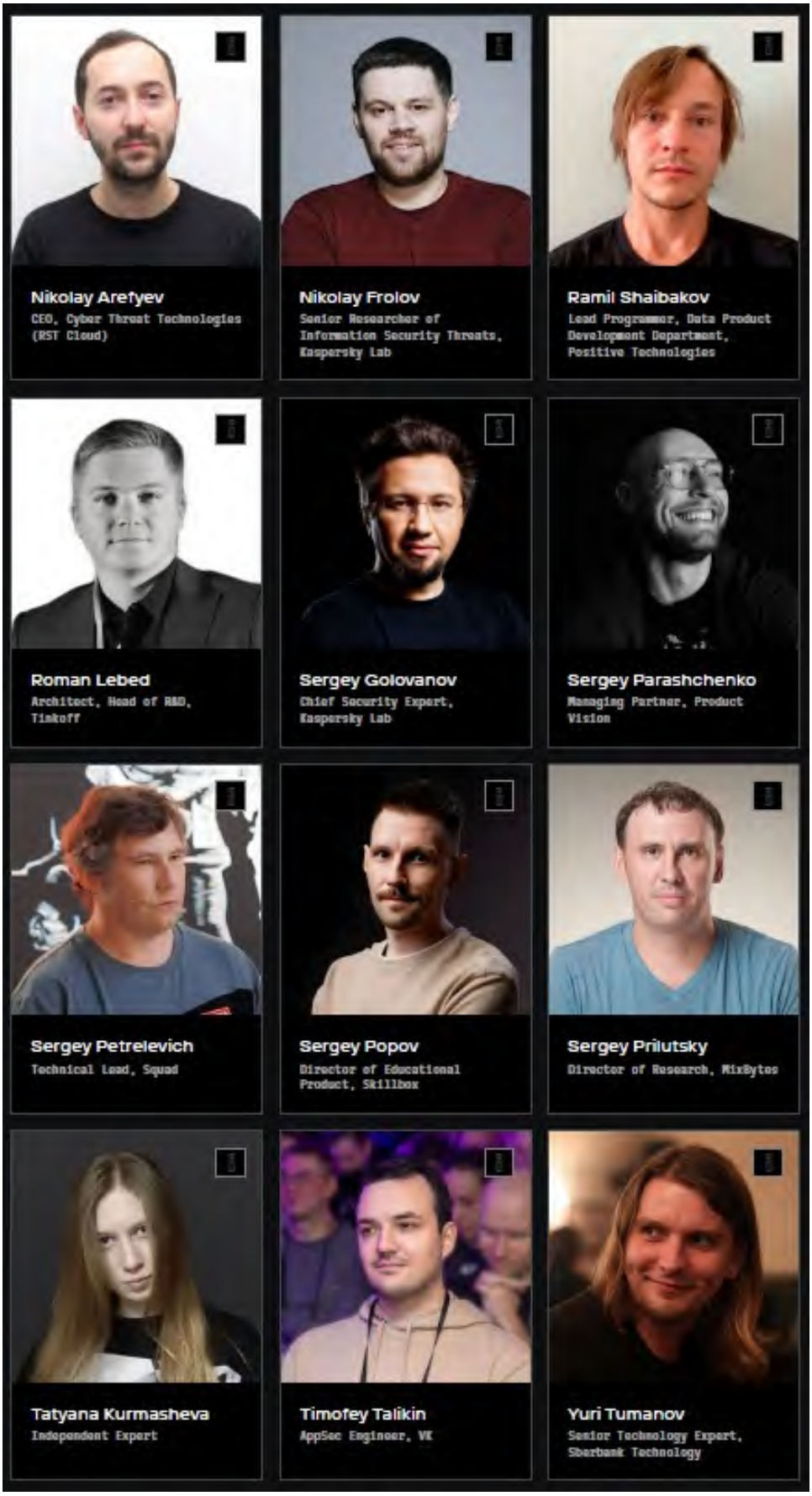
Mikhail Zhmailo
Pentester, CICADA8 (MTS Innovation Center)

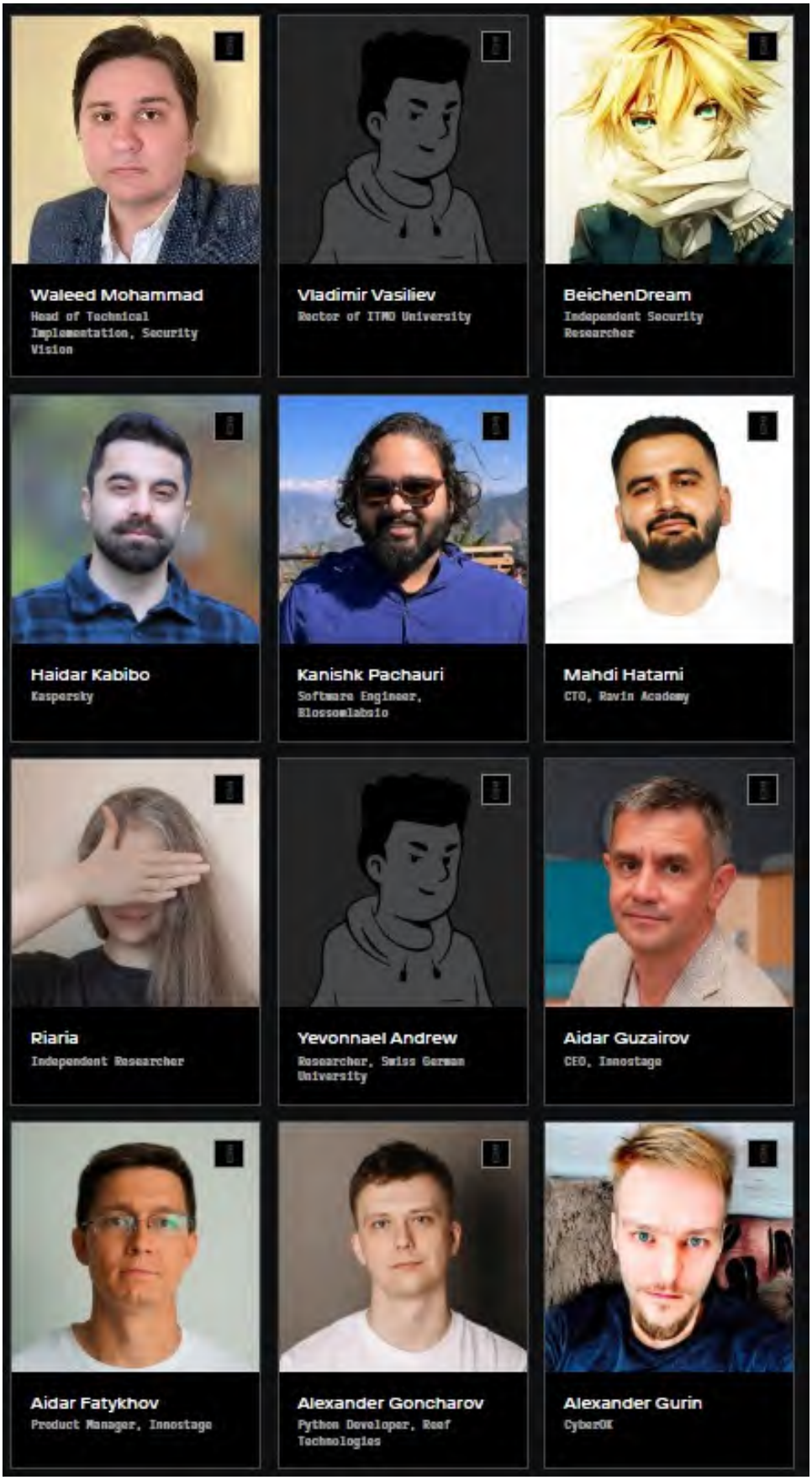
Mikhail Chereshnev
Cloud/Container Security Team Lead, Swordfish Security

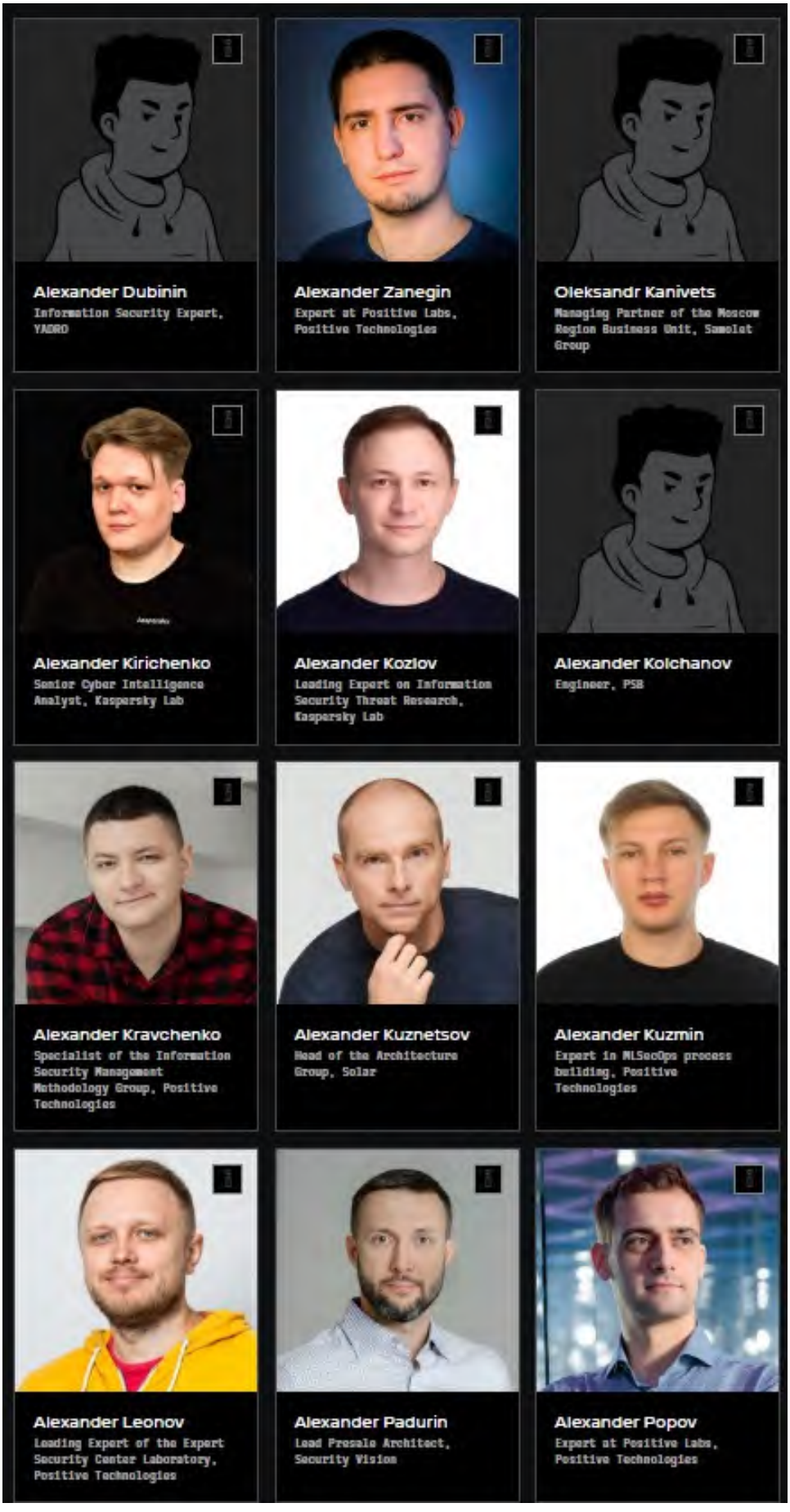
Natalia Bessonova
Director of the Department of Biometric Technologies, Center for Biometric Technologies

Nikita Nazarov
Head of Advanced Threat Research, Kaspersky Lab

Treadstone 71




Waleed Mohammad
Head of Technical Implementation, Security Vision
Vladimir Vasiliev
Rector of ITMO University
BeichenDream
Independent Security Researcher
Haidar Kabibo
Kaspersky
Kanishk Pachauri
Software Engineer, Blossomlabsio
Mahdi Hatami
CTO, Ravin Academy
Riaria
Independent Researcher
Yevonnael Andrew
Researcher, Swiss German University
Aidar Guzairov
CEO, Innostage
Aidar Fatykhov
Product Manager, Innostage
Alexander Goncharov
Python Developer, Reef Technologies
Alexander Gurin
CyberOK



Alexander Dubinin
Information Security Expert, YADRO

Alexander Zanegin
Expert at Positive Labs, Positive Technologies

Oleksandr Kanivets
Managing Partner of the Moscow Region Business Unit, Samolet Group

Alexander Kirichenko
Senior Cyber Intelligence Analyst, Kaspersky Lab

Alexander Kozlov
Leading Expert on Information Security Threat Research, Kaspersky Lab

Alexander Kolchanov
Engineer, PSB

Alexander Kravchenko
Specialist of the Information Security Management Methodology Group, Positive Technologies

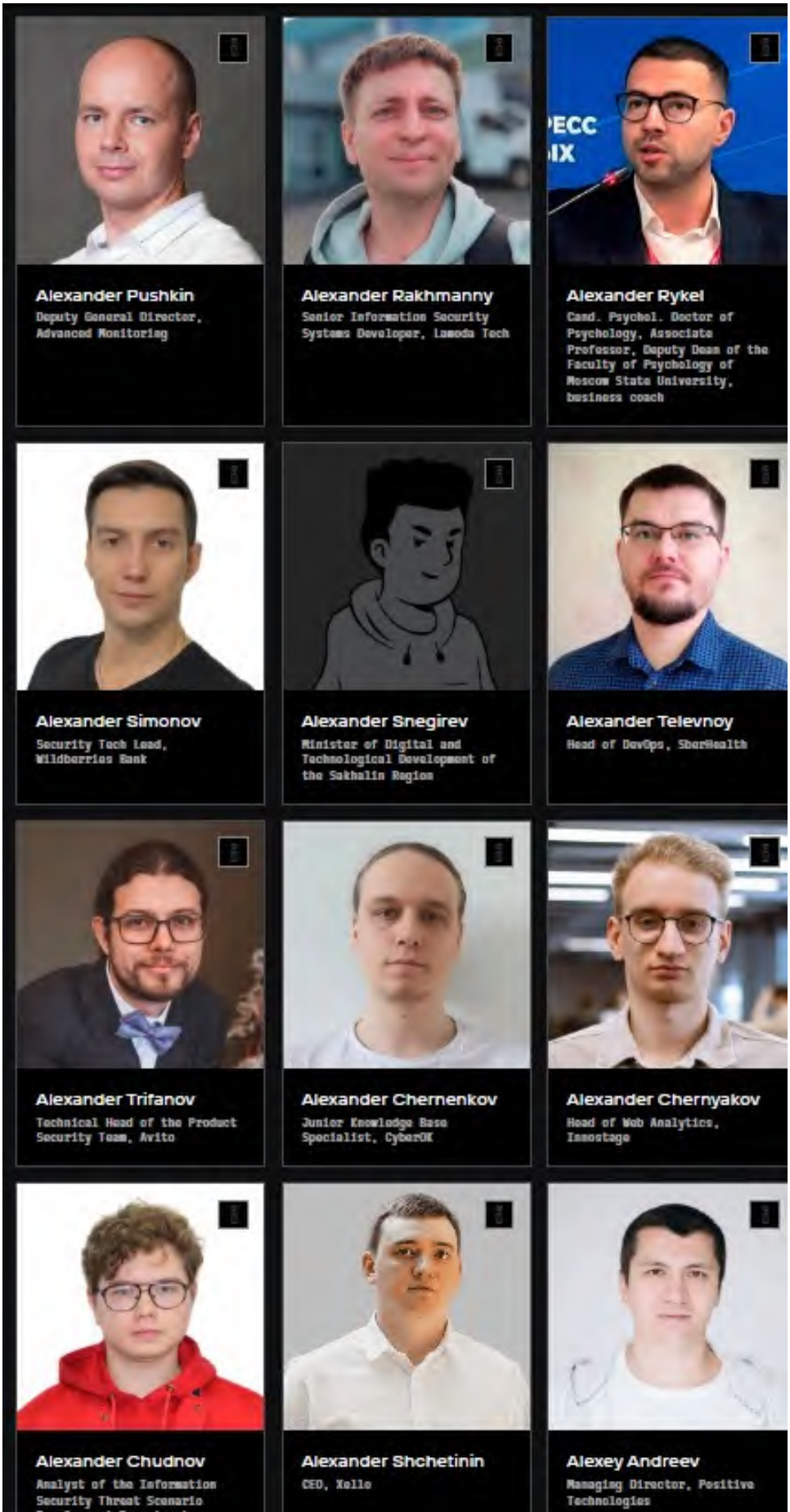
Alexander Kuznetsov
Head of the Architecture Group, Solar

Alexander Kuzmin
Expert in NLSecOps process building, Positive Technologies

Alexander Leonov
Leading Expert of the Expert Security Center Laboratory, Positive Technologies

Alexander Padurin
Lead Presale Architect, Security Vision

Alexander Popov
Expert at Positive Labs, Positive Technologies



Alexander Pushkin
Deputy General Director, Advanced Monitoring

Alexander Rakhmanny
Senior Information Security Systems Developer, Lamoda Tech

Alexander Rykel
Cand. Psychol. Doctor of Psychology, Associate Professor, Deputy Dean of the Faculty of Psychology of Moscow State University, business coach

Alexander Simonov
Security Tech Lead, Wildberries Bank

Alexander Snegirev
Minister of Digital and Technological Development of the Sakhalin Region

Alexander Televnoy
Head of DevOps, SberHealth

Alexander Trifanov
Technical Head of the Product Security Team, Avito

Alexander Chernenkov
Junior Knowledge Base Specialist, CyberOK

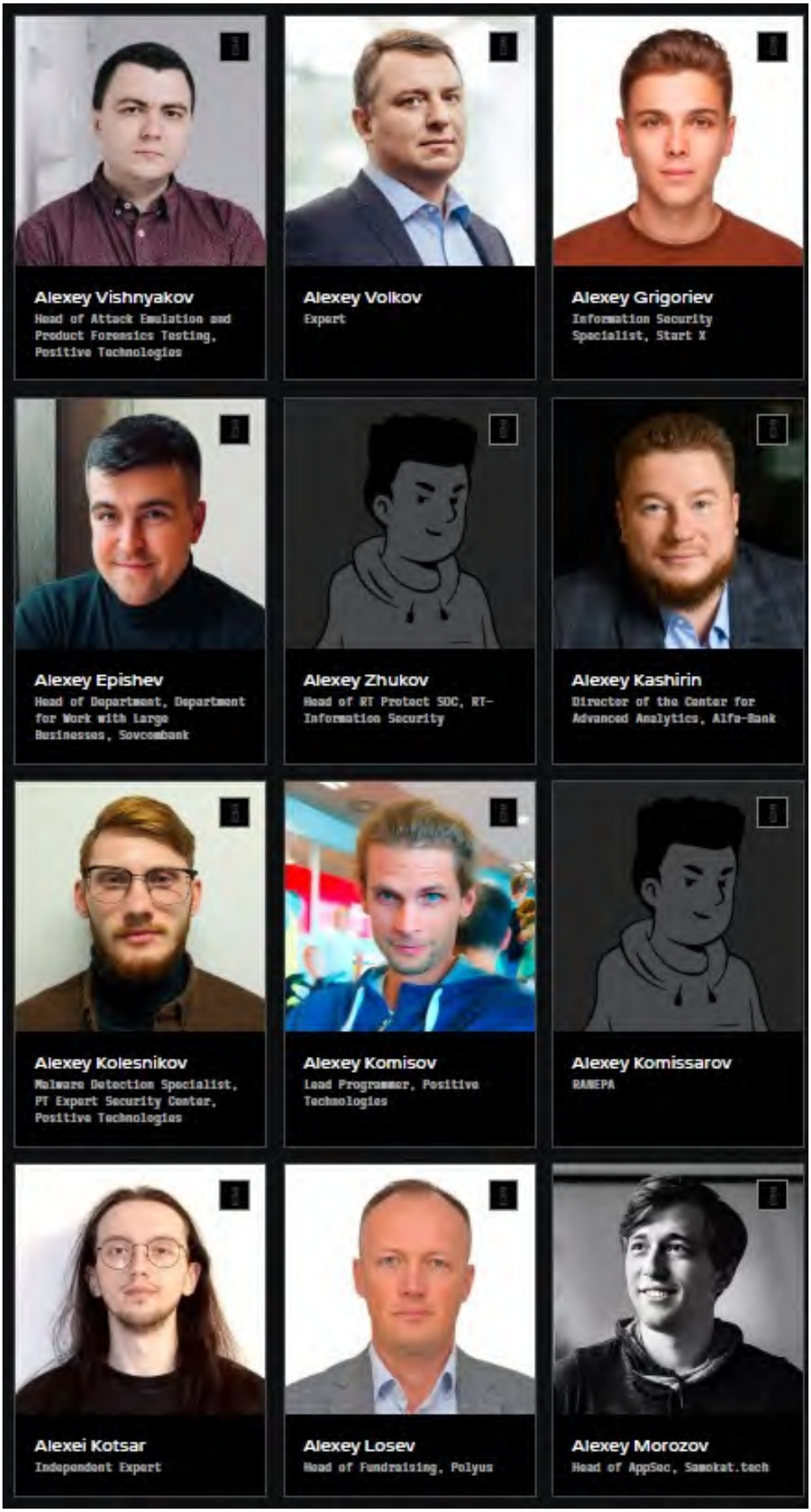
Alexander Chernyakov
Head of Web Analytics, Insostage

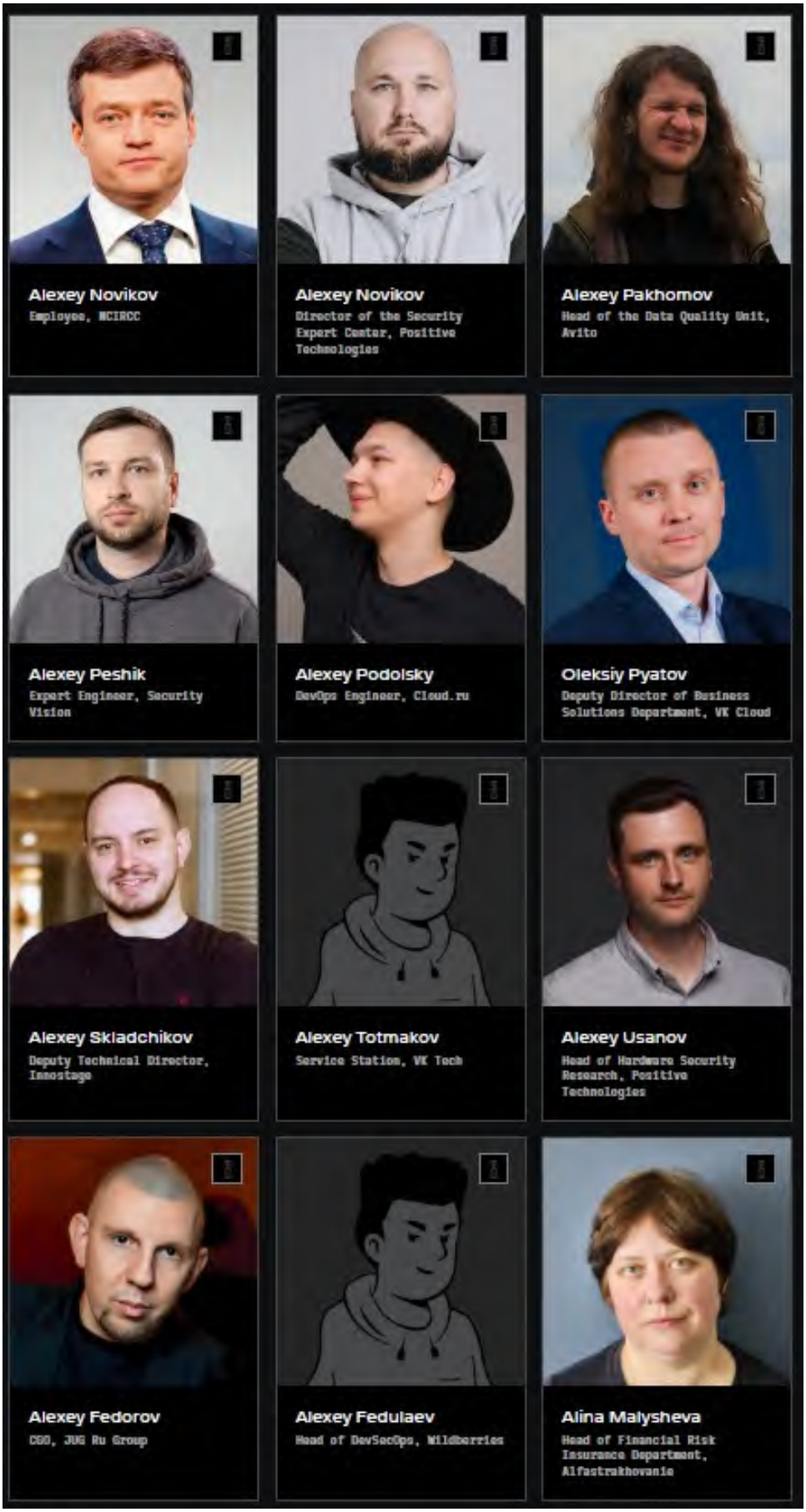
Alexander Chudnov
Analyst of the Information Security Threat Scenario

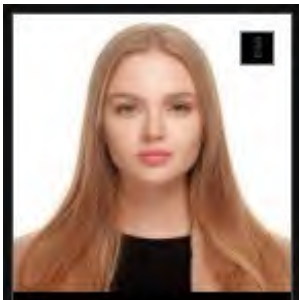
Alexander Shchetinin
CEO, Xello

Alexey Andreev
Managing Director, Positive Technologies

Treadstone 71

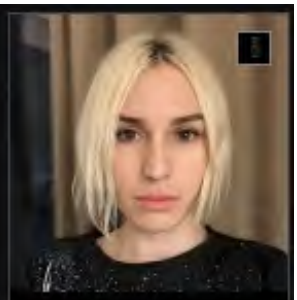



Alexey Novikov
Employee, NCIRCC
Alexey Novikov
Director of the Security Expert Center, Positive Technologies
Alexey Pakhomov
Head of the Data Quality Unit, Avito
Alexey Peshik
Expert Engineer, Security Vision
Alexey Podolsky
DevOps Engineer, Cloud.ru
Oleksiy Pyatov
Deputy Director of Business Solutions Department, VK Cloud
Alexey Skladchikov
Deputy Technical Director, Innostage
Alexey Totmakov
Service Station, VK Tech
Alexey Usanov
Head of Hardware Security Research, Positive Technologies
Alexey Fedorov
CSO, JUG Ru Group
Alexey Fedulaev
Head of DevSecOps, Wildberries
Alina Malysheva
Head of Financial Risk Insurance Department, Alfastrakhovanie



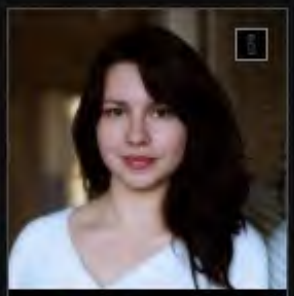
Alina Petrova
Head of the State Information Systems Expertise Division of the Department of Digital Transformation and Coordination of Budget Expenditures, Ministry of Digital Development, Communications and Mass Media

Alisa Kulishenko
Digital Footprint Analyst, Kaspersky Lab



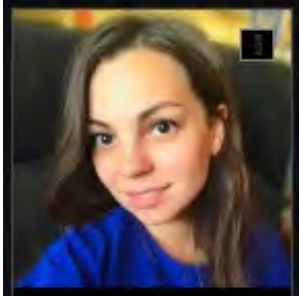
Alice Esage
Founder, ZeroDay Engineering

Alla Khrapunova
Deputy Director of the Foundation "For the Rights of Borrowers", curator of the MOSHELOVKA.RF platform



Almira Fatikhova
Design Engineer, Innostage

Anar Bakhshaliyev
Executive Director, SOGAZ



Anastasia Volynskaya
Information Security Specialist, VK

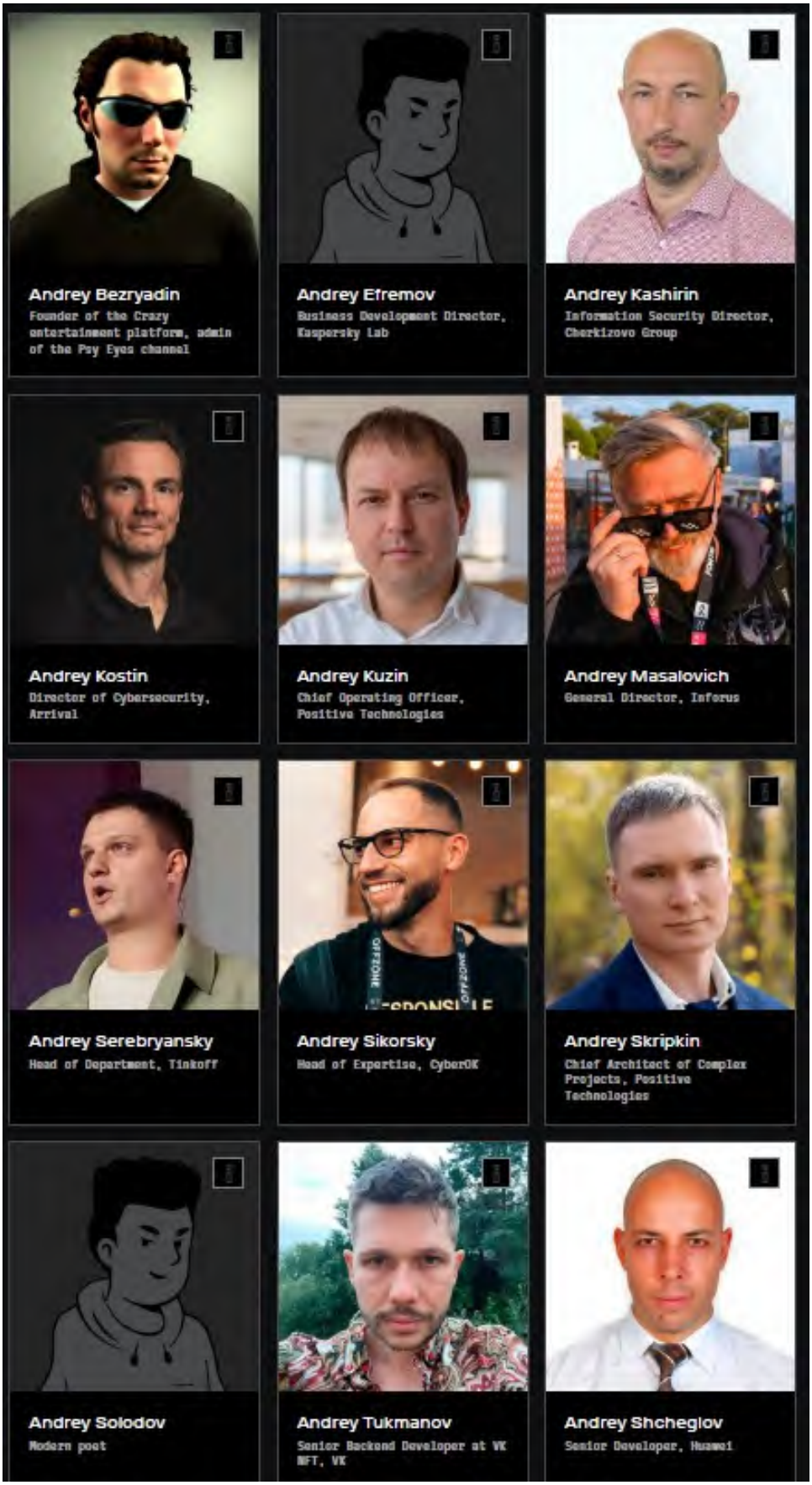
Anastasia Gainetdinova
Information Security Analyst, Whoosh

Anastasia Dogadkina
Head of Financial Planning, Reporting, and Business Support, Positive Technologies

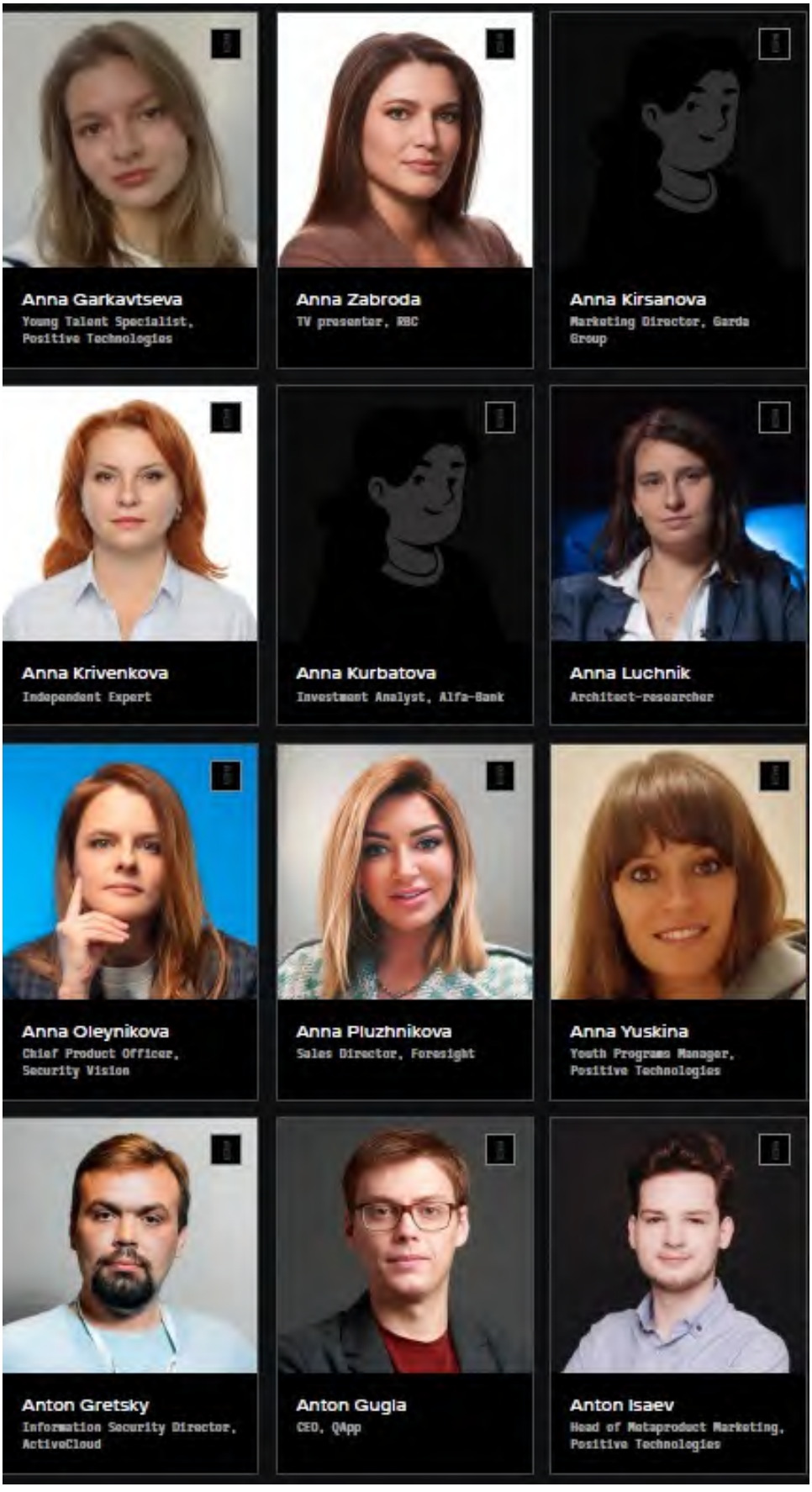
Anastasia Petrova
Head of SOC, Biocad

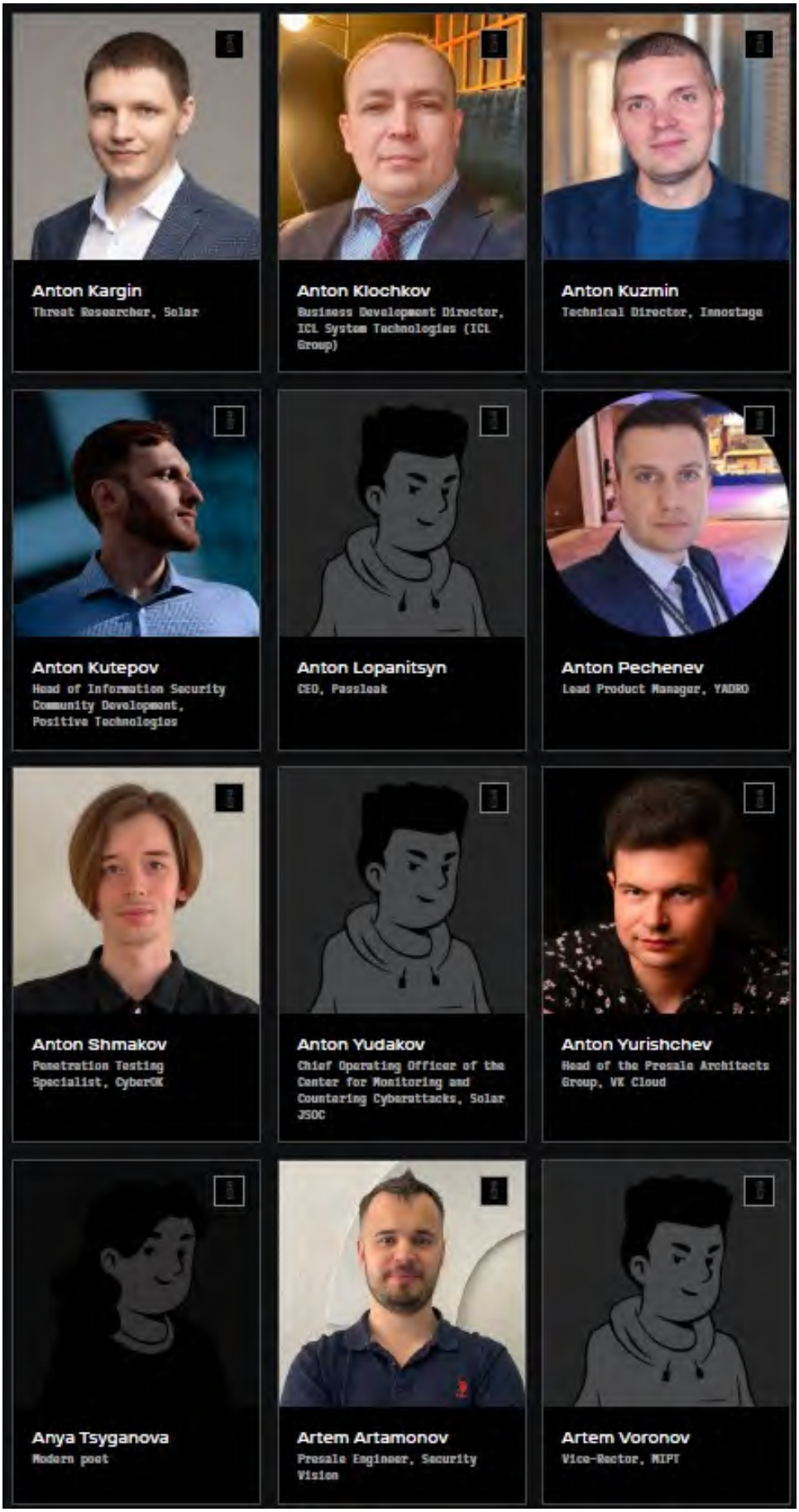
Anastasia Fedorova
Development Director of the Cybersecurity Monitoring Center, K2 Cybersecurity

Anatoly Smirnov
CFO, Arenadata Software


Andrey Bezryadin
Founder of the Crazy entertainment platform, admin of the Psy Eyes channel
Andrey Efremov
Business Development Director, Kaspersky Lab
Andrey Kashirin
Information Security Director, Cherkizovo Group
Andrey Kostin
Director of Cybersecurity, Arrival
Andrey Kuzin
Chief Operating Officer, Positive Technologies
Andrey Masalovich
General Director, Inforus
Andrey Serebryansky
Head of Department, Tinkoff
Andrey Sikorsky
Head of Expertise, CyberOK
Andrey Skripkin
Chief Architect of Complex Projects, Positive Technologies
Andrey Solodov
Modern poet
Andrey Tukmanov
Senior Backend Developer at VK NFT, VK
Andrey Shcheglov
Senior Developer, Huawei

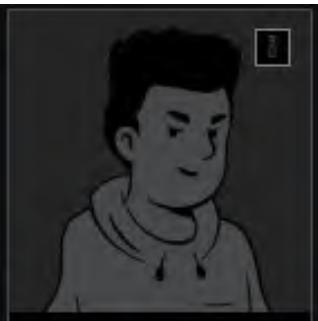
Treadstone 71



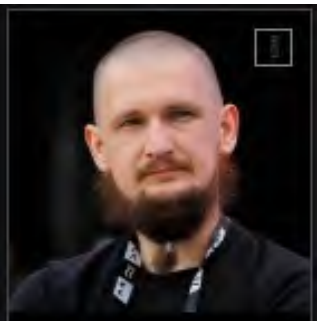

Anton Kargin
Threat Researcher, Solar
Anton Klochkov
Business Development Director, ICL System Technologies (ICL Group)
Anton Kuzmin
Technical Director, Innostage
Anton Kutepov
Head of Information Security Community Development, Positive Technologies
Anton Lopanitsyn
CEO, Passleak
Anton Pechenev
Lead Product Manager, YADRO
Anton Shmakov
Penetration Testing Specialist, CyberOK
Anton Yudakov
Chief Operating Officer of the Center for Monitoring and Countering Cyberattacks, Solar JSOC
Anton Yurishchev
Head of the Presale Architects Group, VK Cloud
Anya Tsyganova
Modern poet
Artem Artamonov
Presale Engineer, Security Vision
Artem Voronov
Vice-Rector, MIPT

Treadstone 71

Artem Goriov
Independent expert on internal audit and risk management



Artem Karmazin
Leading expert in the implementation of secure development processes, Positive Technologies



Artem Kulakov
Security Researcher, Positive Technologies

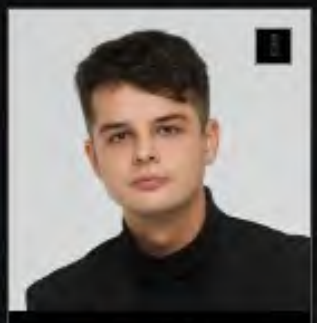
Artem Medvedev
Chief Executive Officer, Intalpro

Artem Muradyan
Engineer, Swordfish Security

Artem Puzankov
Head of Secure Development Practices Implementation Group, Positive Technologies

Artem Sychev
First Deputy General Director, RT-Information Security

Artem Sychev
Advisor to the CEO for Public Sector Relations, Positive Technologies

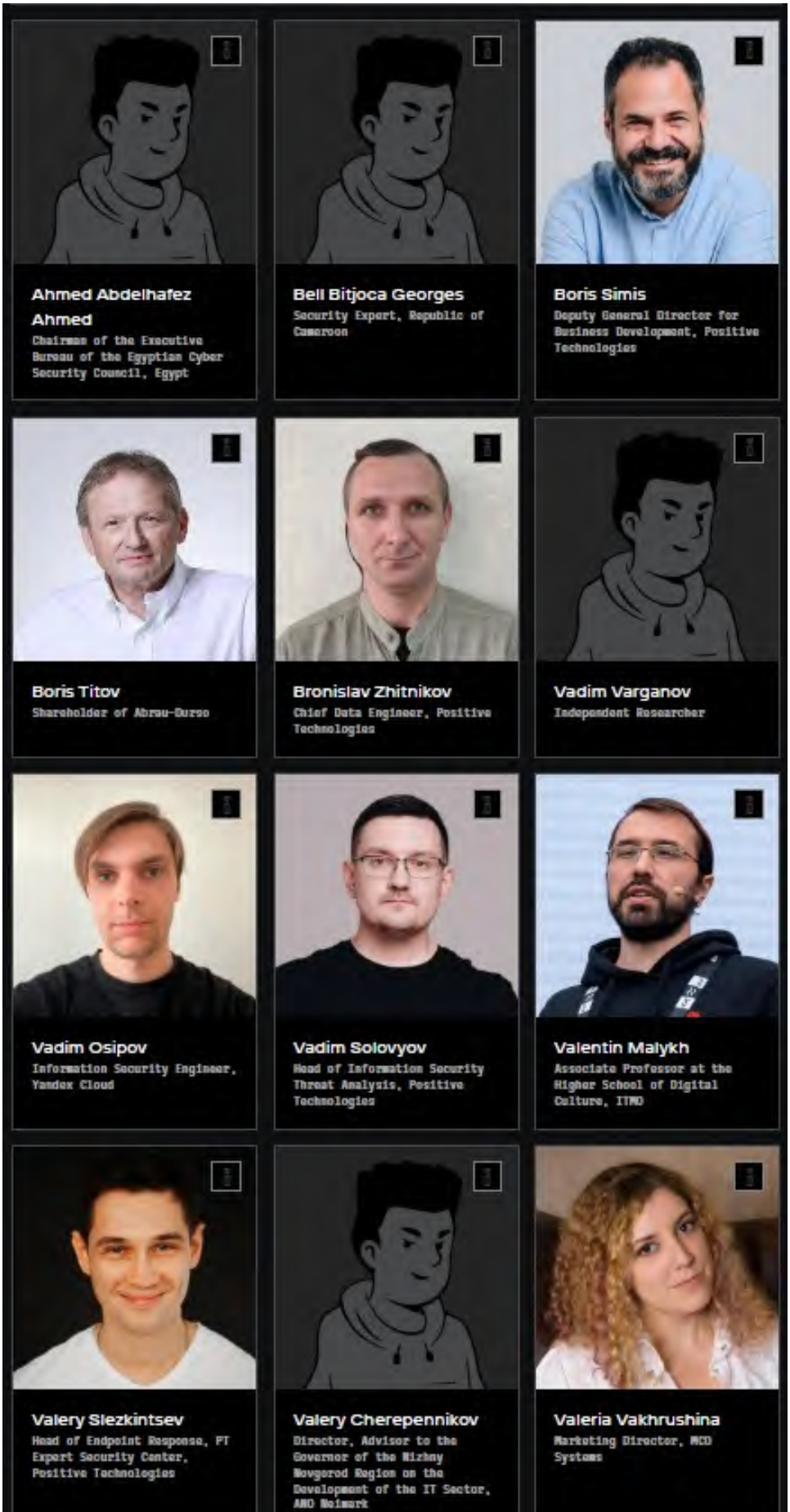


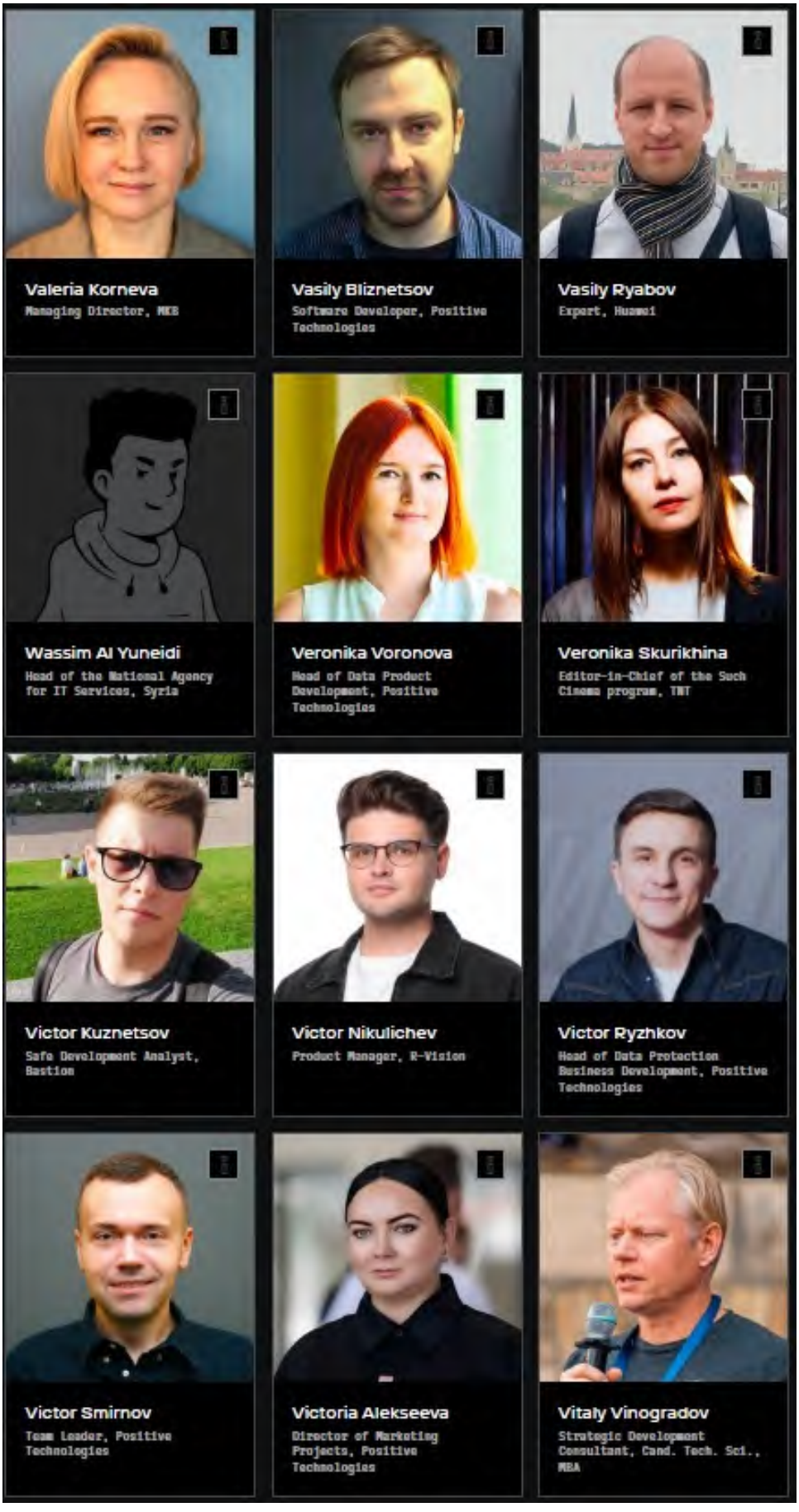
Artem Tolmachev
Computer Incident Response Specialist, NCCCI

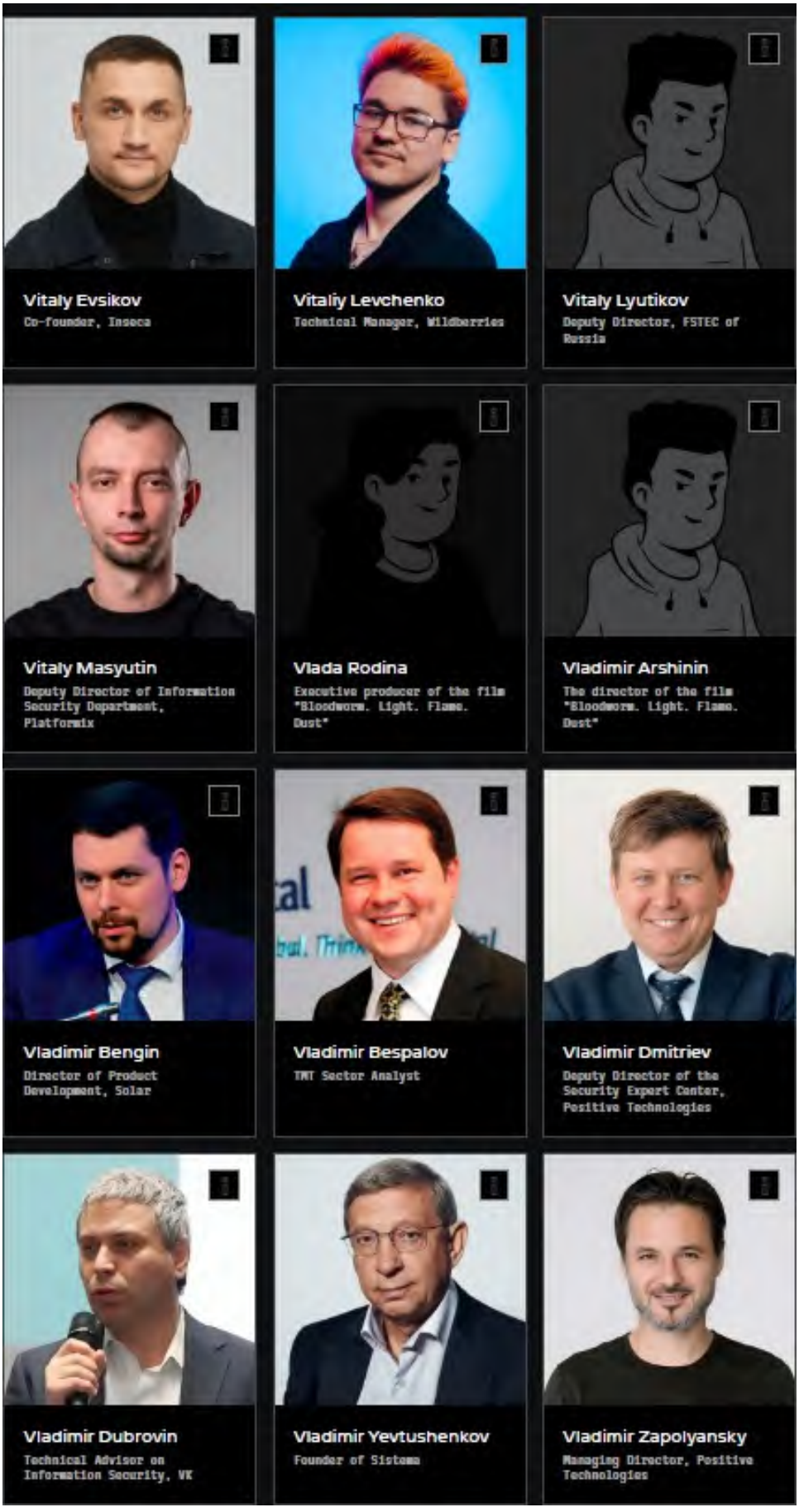
Artemy Yuriev
Head of Security Analysis, Gazprombank

Artur Saprykin
Lead data scientist, Entrepreneur

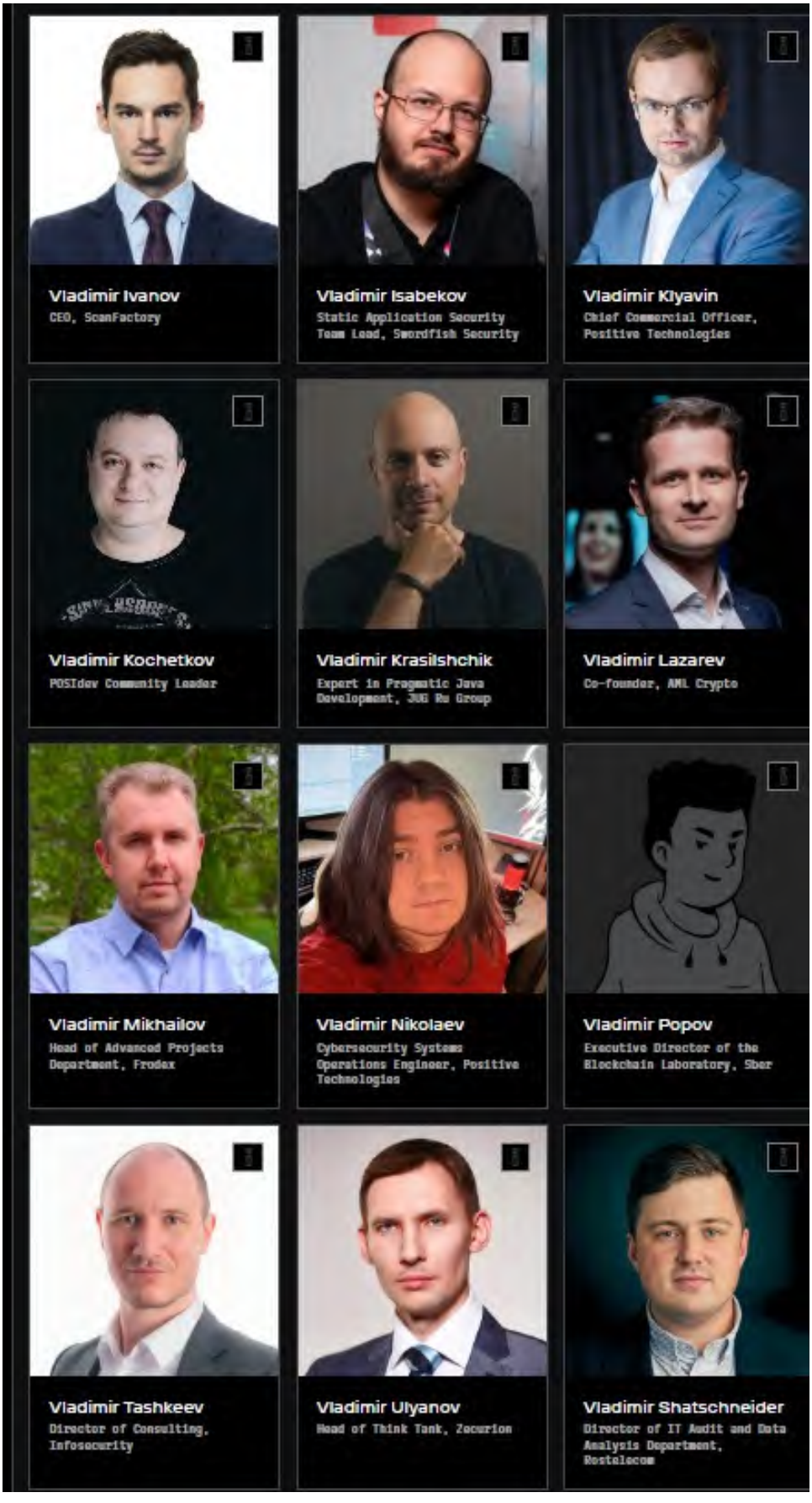
Artur Khanov
Developer, Hackerdom

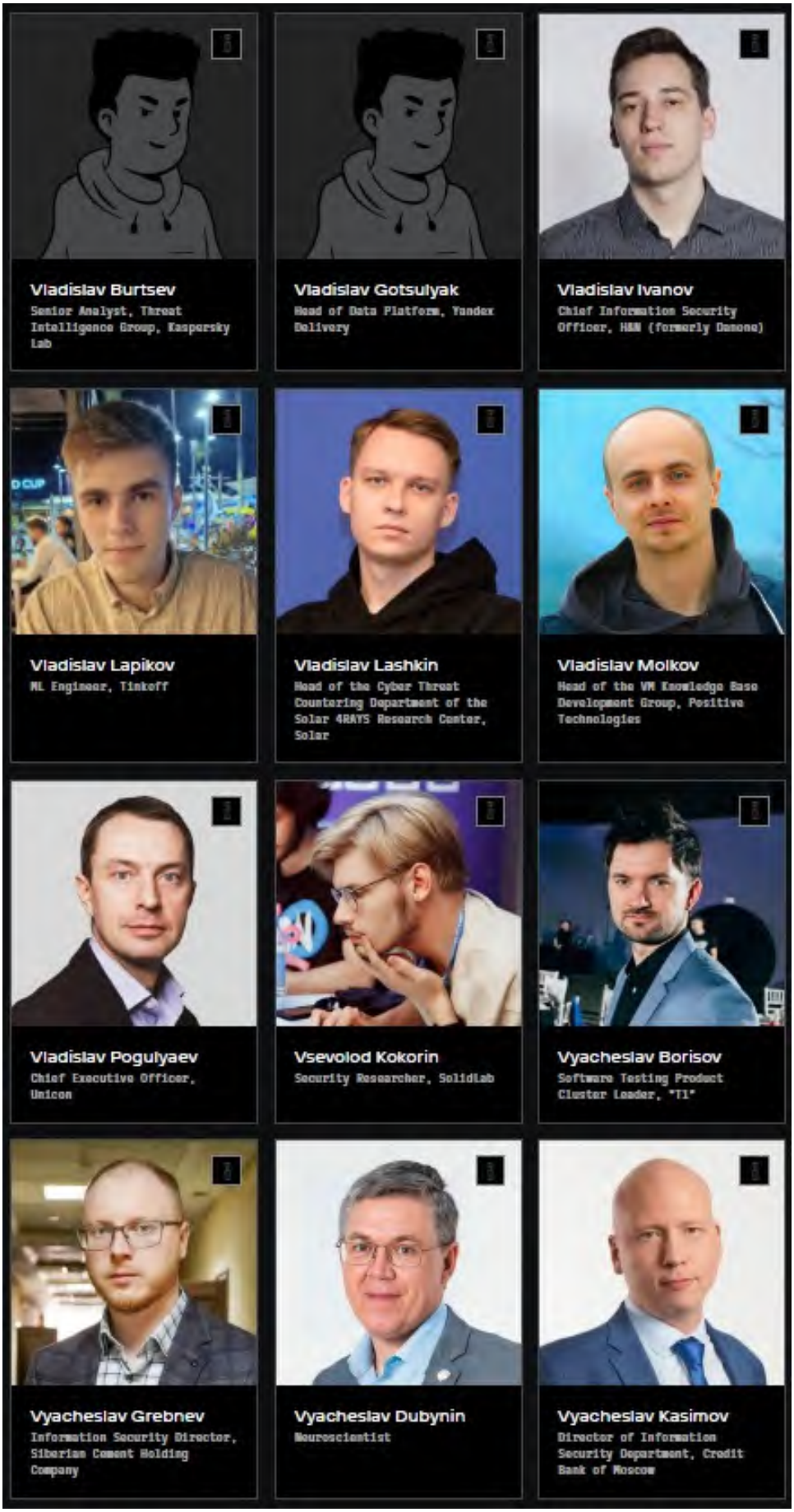

Ahmed Abdelhafez Ahmed
Chairman of the Executive Bureau of the Egyptian Cyber Security Council, Egypt
Bell Bitjoca Georges
Security Expert, Republic of Cameroon
Boris Simis
Deputy General Director for Business Development, Positive Technologies
Boris Titov
Shareholder of Abrau-Durso
Bronislav Zhitnikov
Chief Data Engineer, Positive Technologies
Vadim Varganov
Independent Researcher
Vadim Osipov
Information Security Engineer, Yandex Cloud
Vadim Solovyov
Head of Information Security Threat Analysis, Positive Technologies
Valentin Malykh
Associate Professor at the Higher School of Digital Culture, ITMO
Valery Slezkintsev
Head of Endpoint Response, PT Expert Security Center, Positive Technologies
Valery Cherepennikov
Director, Advisor to the Governor of the Nizhny Novgorod Region on the Development of the IT Sector, ANO Neimark
Valeria Vakhrushina
Marketing Director, MCD Systems


Valeria Korneva
Managing Director, MKB
Vasily Bliznetsov
Software Developer, Positive Technologies
Vasily Ryabov
Expert, Huawei
Wassim Al Yuneidi
Head of the National Agency for IT Services, Syria
Veronika Voronova
Head of Data Product Development, Positive Technologies
Veronika Skurikhina
Editor-in-Chief of the Such Cinema program, TNT
Victor Kuznetsov
Safe Development Analyst, Bastion
Victor Nikulichev
Product Manager, R-Vision
Victor Ryzhkov
Head of Data Protection Business Development, Positive Technologies
Victor Smirnov
Team Leader, Positive Technologies
Victoria Alekseeva
Director of Marketing Projects, Positive Technologies
Vitaly Vinogradov
Strategic Development Consultant, Cand. Tech. Sci., MBA


Vitaly Evsikov
Co-founder, Inseca
Vitaliy Levchenko
Technical Manager, Wildberries
Vitaly Lyutikov
Deputy Director, FSTEC of Russia
Vitaly Masyutin
Deputy Director of Information Security Department, Platformix
Vlada Rodina
Executive producer of the film "Bloodworm. Light. Flame. Dust"
Vladimir Arshinin
The director of the film "Bloodworm. Light. Flame. Dust"
Vladimir Bengin
Director of Product Development, Solar
Vladimir Bespalov
TMT Sector Analyst
Vladimir Dmitriev
Deputy Director of the Security Expert Center, Positive Technologies
Vladimir Dubrovin
Technical Advisor on Information Security, VK
Vladimir Yevtushenkov
Founder of Sistema
Vladimir Zapolyansky
Managing Director, Positive Technologies

Treadstone 71





Vladislav Burtsev
Senior Analyst, Threat Intelligence Group, Kaspersky Lab

Vladislav Gotsulyak
Head of Data Platform, Yandex Delivery

Vladislav Ivanov
Chief Information Security Officer, H&N (formerly Danone)

Vladislav Lapikov
ML Engineer, Tinkoff

Vladislav Lashkin
Head of the Cyber Threat Countering Department of the Solar 4RAYS Research Center, Solar

Vladislav Molkov
Head of the VM Knowledge Base Development Group, Positive Technologies

Vladislav Pogulyaev
Chief Executive Officer, Unicon

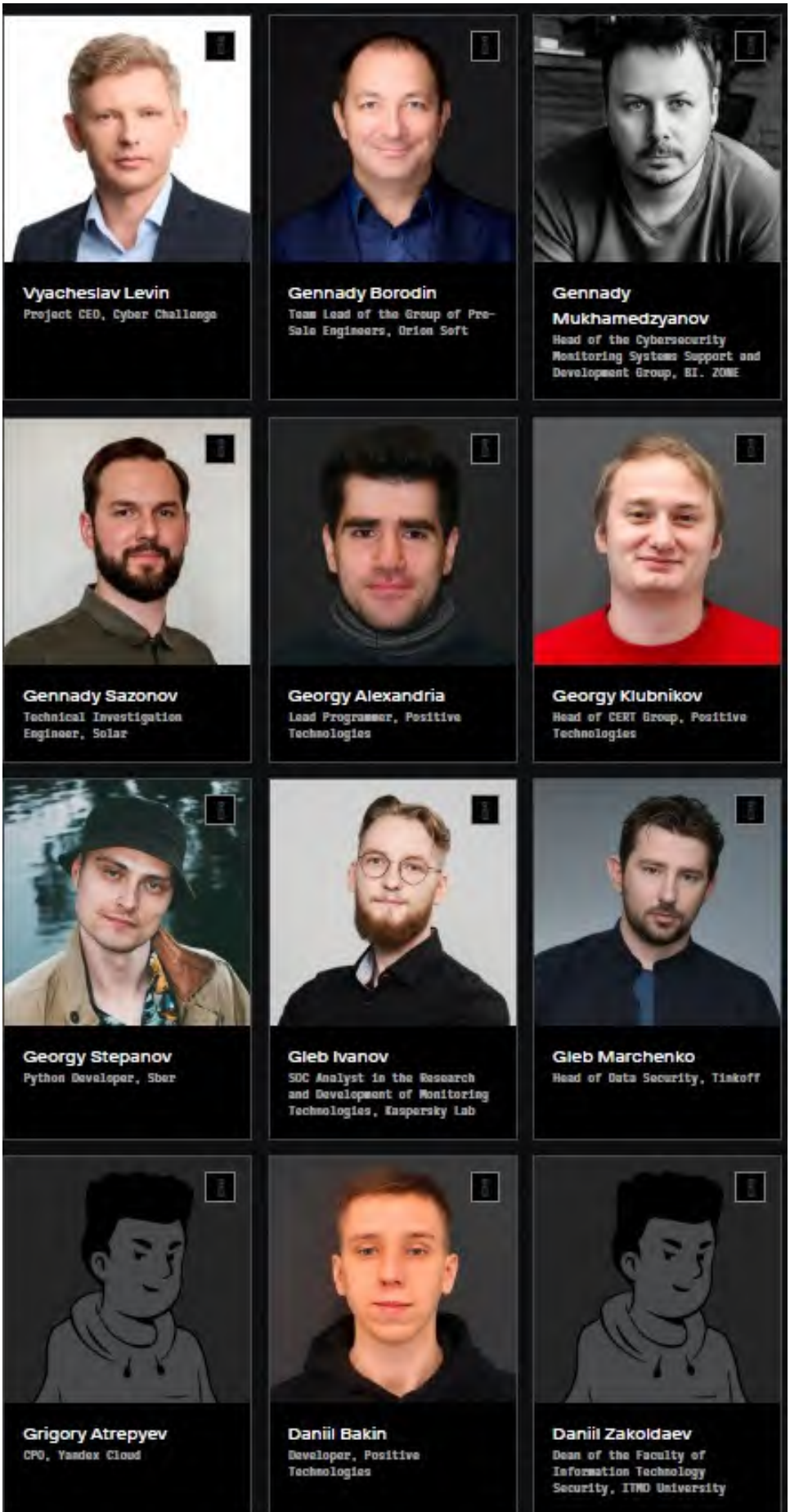
Vsevolod Kokorin
Security Researcher, SolidLab

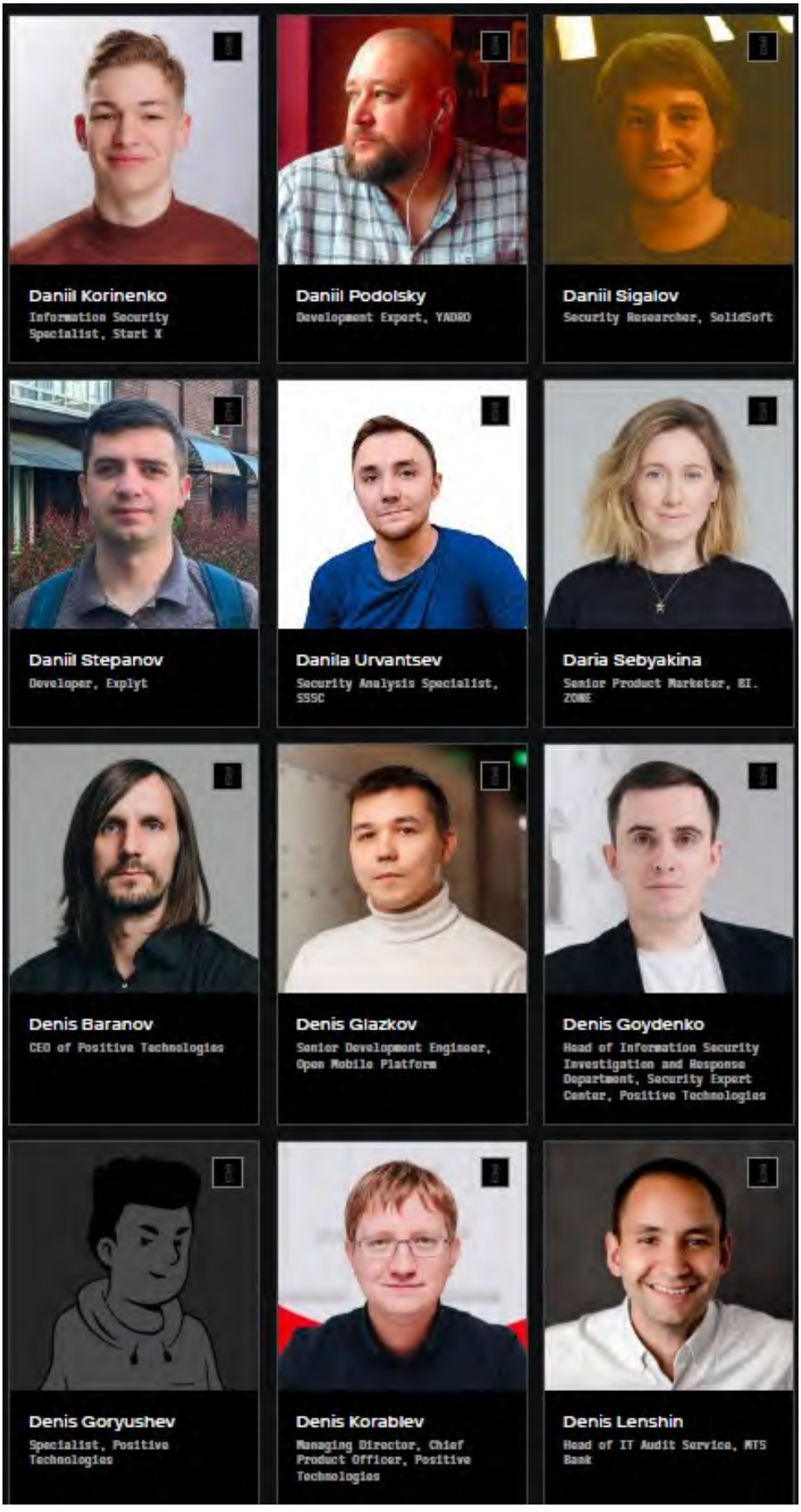
Vyacheslav Borisov
Software Testing Product Cluster Leader, "TI"

Vyacheslav Grebnev
Information Security Director, Siberian Cement Holding Company

Vyacheslav Dubynin
Neuroscientist

Vyacheslav Kasimov
Director of Information Security Department, Credit Bank of Moscow


Vyacheslav Levin
Project CEO, Cyber Challenge
Gennady Borodin
Team Lead of the Group of Pre-Sale Engineers, Orion Soft
Gennady Mukhamedzyanov
Head of the Cybersecurity Monitoring Systems Support and Development Group, BI. ZONE
Gennady Sazonov
Technical Investigation Engineer, Solar
Georgy Alexandria
Lead Programmer, Positive Technologies
Georgy Klubnikov
Head of CERT Group, Positive Technologies
Georgy Stepanov
Python Developer, Sber
Gleb Ivanov
SOC Analyst in the Research and Development of Monitoring Technologies, Kaspersky Lab
Gleb Marchenko
Head of Data Security, Tinkoff
Grigory Atrepyev
CPO, Yandex Cloud
Daniil Bakin
Developer, Positive Technologies
Daniil Zakoldaev
Dean of the Faculty of Information Technology Security, ITMO University



Daniil Korinenko
Information Security Specialist, Start X

Daniil Podolsky
Development Expert, YADRO

Daniil Sigalov
Security Researcher, SolidSoft

Daniil Stepanov
Developer, Explyt

Danila Urvantsev
Security Analysis Specialist, SSSC

Daria Sebyakina
Senior Product Marketer, EI. ZONE

Denis Baranov
CEO of Positive Technologies

Denis Glazkov
Senior Development Engineer, Open Mobile Platform

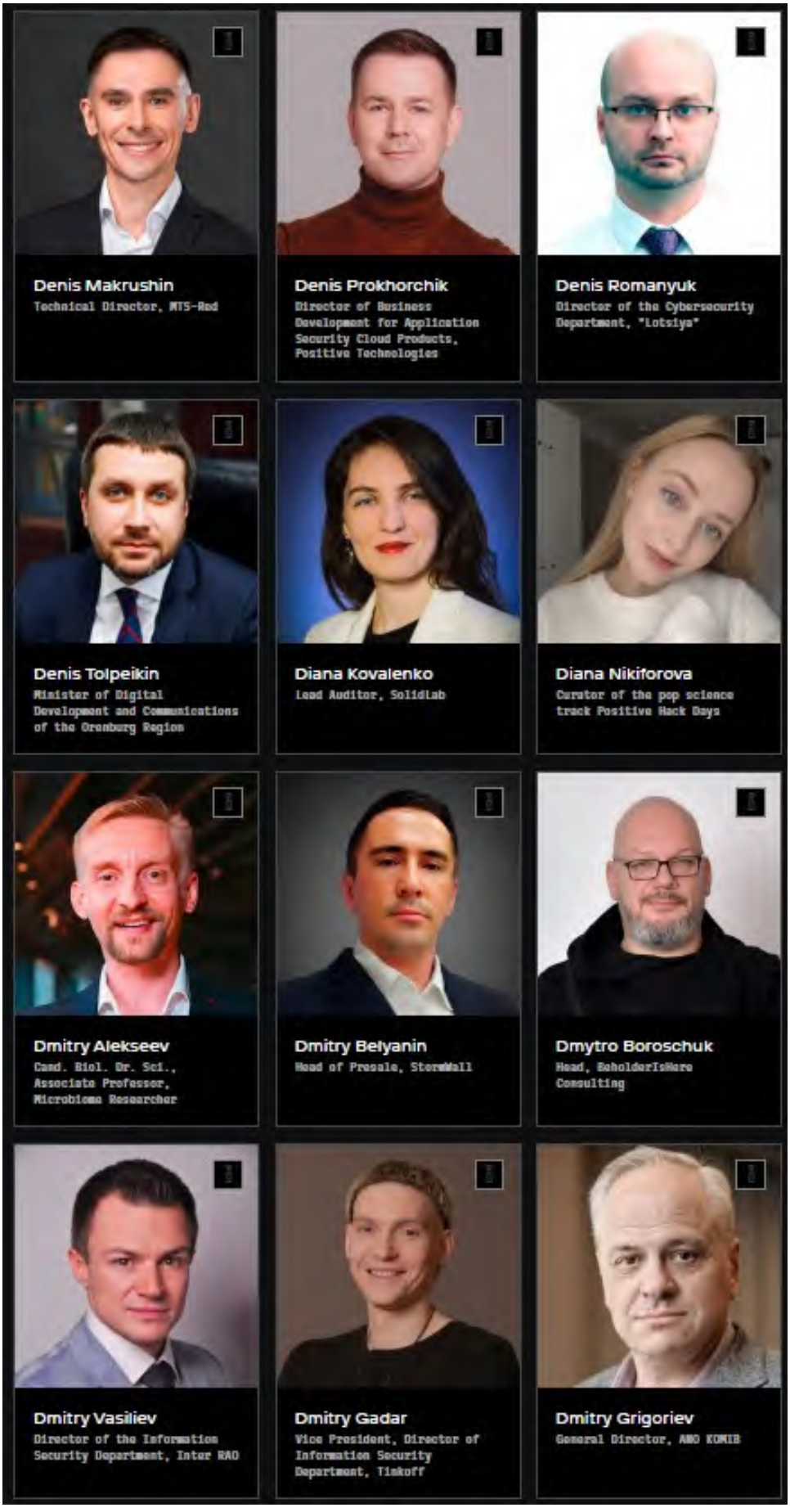
Denis Goydenko
Head of Information Security Investigation and Response Department, Security Expert Center, Positive Technologies

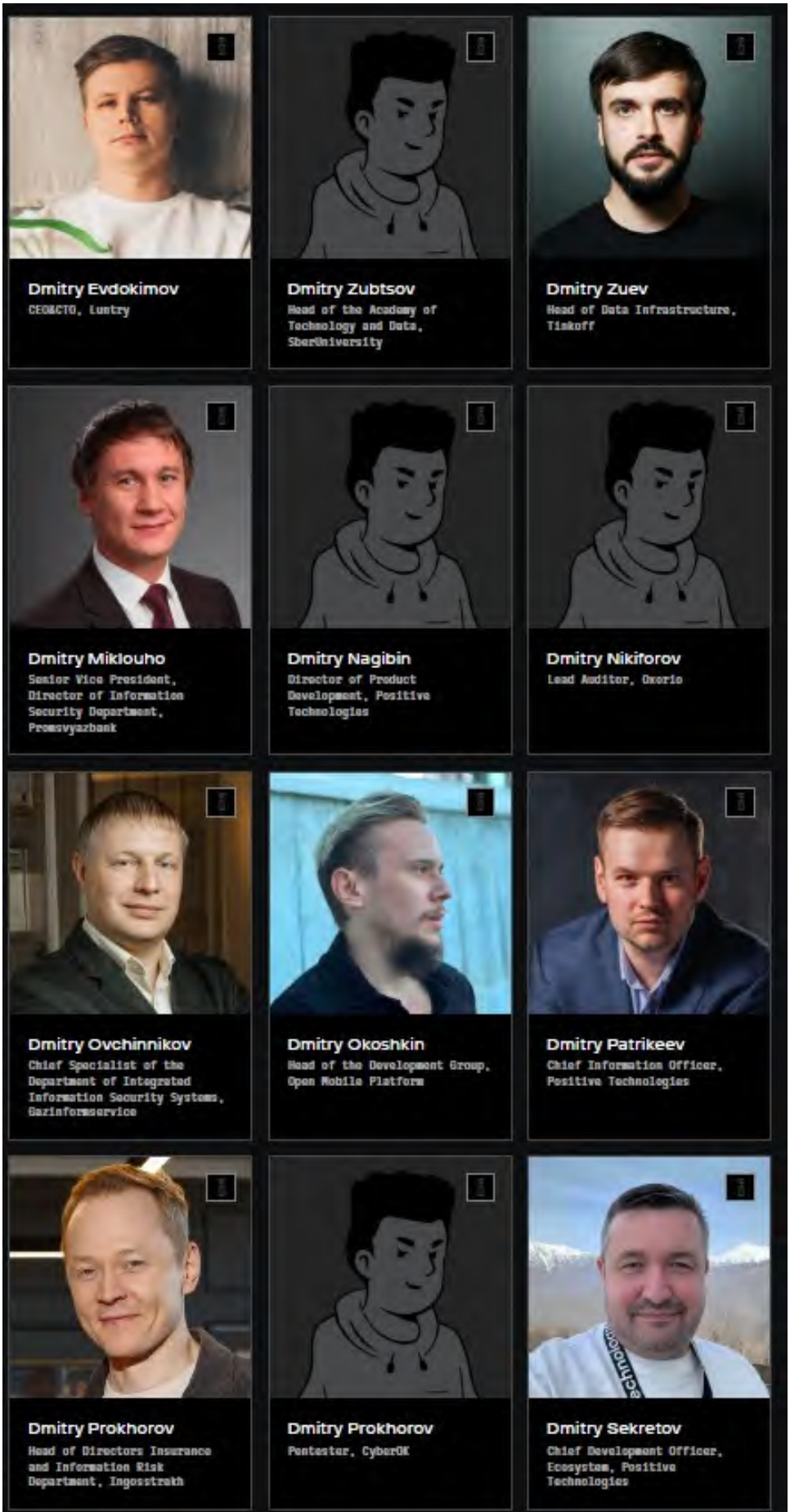
Denis Goryushev
Specialist, Positive Technologies

Denis Korablev
Managing Director, Chief Product Officer, Positive Technologies

Denis Lenshin
Head of IT Audit Service, MTS Bank

Treadstone 71




Dmitry Evdokimov
CEO&CTO, Luntry
Dmitry Zubtsov
Head of the Academy of Technology and Data, SberUniversity
Dmitry Zuev
Head of Data Infrastructure, Tinkoff
Dmitry Miklouho
Senior Vice President, Director of Information Security Department, Promsvyazbank
Dmitry Nagibin
Director of Product Development, Positive Technologies
Dmitry Nikiforov
Lead Auditor, Oxeria
Dmitry Ovchinnikov
Chief Specialist of the Department of Integrated Information Security Systems, Gazinformservice
Dmitry Okoshkin
Head of the Development Group, Open Mobile Platform
Dmitry Patrikeev
Chief Information Officer, Positive Technologies
Dmitry Prokhorov
Head of Directors Insurance and Information Risk Department, Ingosstrakh
Dmitry Prokhorov
Pentester, CyberOK
Dmitry Sekretov
Chief Development Officer, Ecosystem, Positive Technologies

Treadstone 71

Dmitry Serebryannikov
Director of Security Analysis, Positive Technologies

Dmitry Smirnov
Head of Information Security Department, Sports Lotteries

Dmitry Taranenko
CISO, SberHealth

Dmitry Tishkin
Head of Application Protection, Tele2

Dmitry Fedorov
Head of University Relations Projects, Positive Technologies

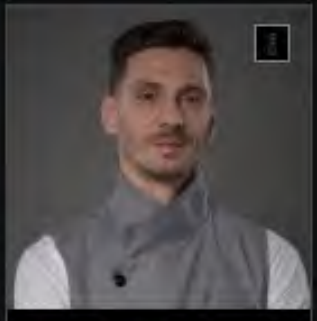
Dmitry Tsarev
Head of Cloud Cybersecurity Solutions Department, BI. ZONE

Dmitry Tseluyko
Director of Information Systems Development Department, Positive Technologies

Dmitry Chebotarev
Product Development Manager, UserGate

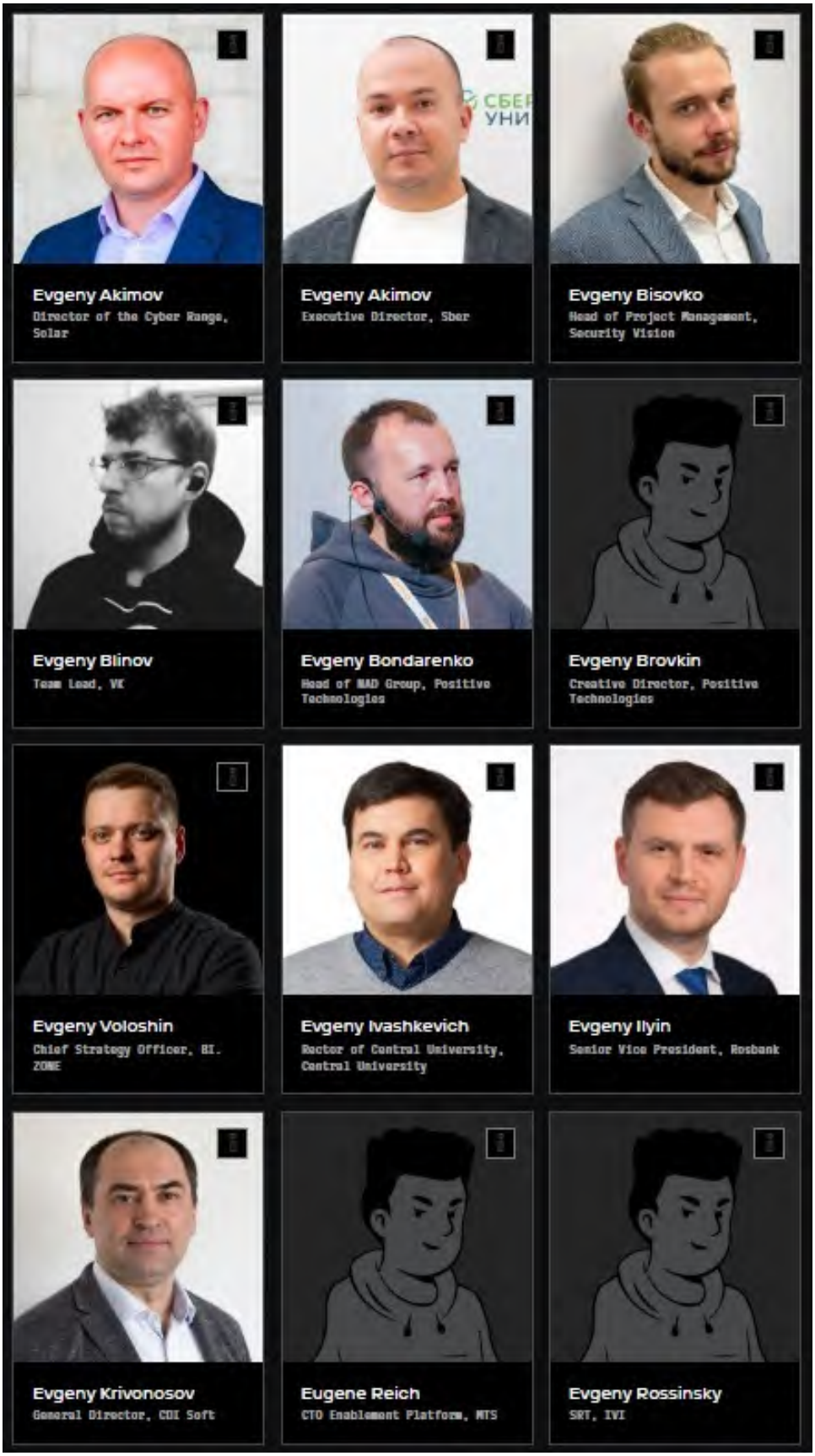
Dmitry Chemeris
Founder, GENVED

Dmitry Shmoylov
Head of Software Security, Kaspersky Lab



Dmitry Shulinin
Head of the Information Security Management Situation Center, UserGate

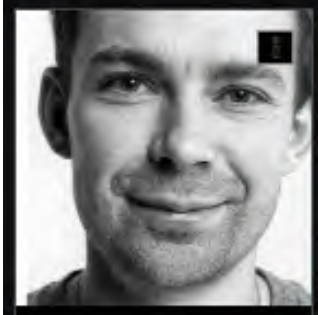
Eva Belyaeva
Head of Development, Security Vision



Evgeny Surkov
Product Manager, Innostage

Evgeny Khasin
Deputy Director of the Department of Cybersecurity, Ministry of Digital Development, Communications and Mass Media

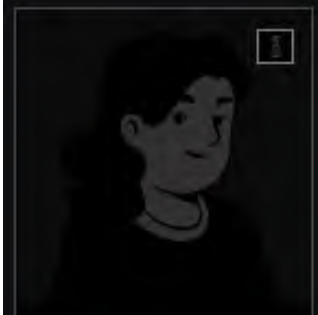
Evgeniya Lukiyan
Deputy Manager of the Northern Branch of Srednerussky Bank, Sberbank



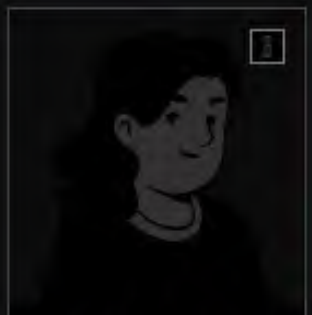
Yegor Appolonov
Marketer, founder of the neurocreative agency "Synthetics"

Yegor Bayandin
CIO and co-founder of the kicksharing service Whoosh

Egor Bogomolov
CEO, CyberED



Ezhova Es
Modern poet



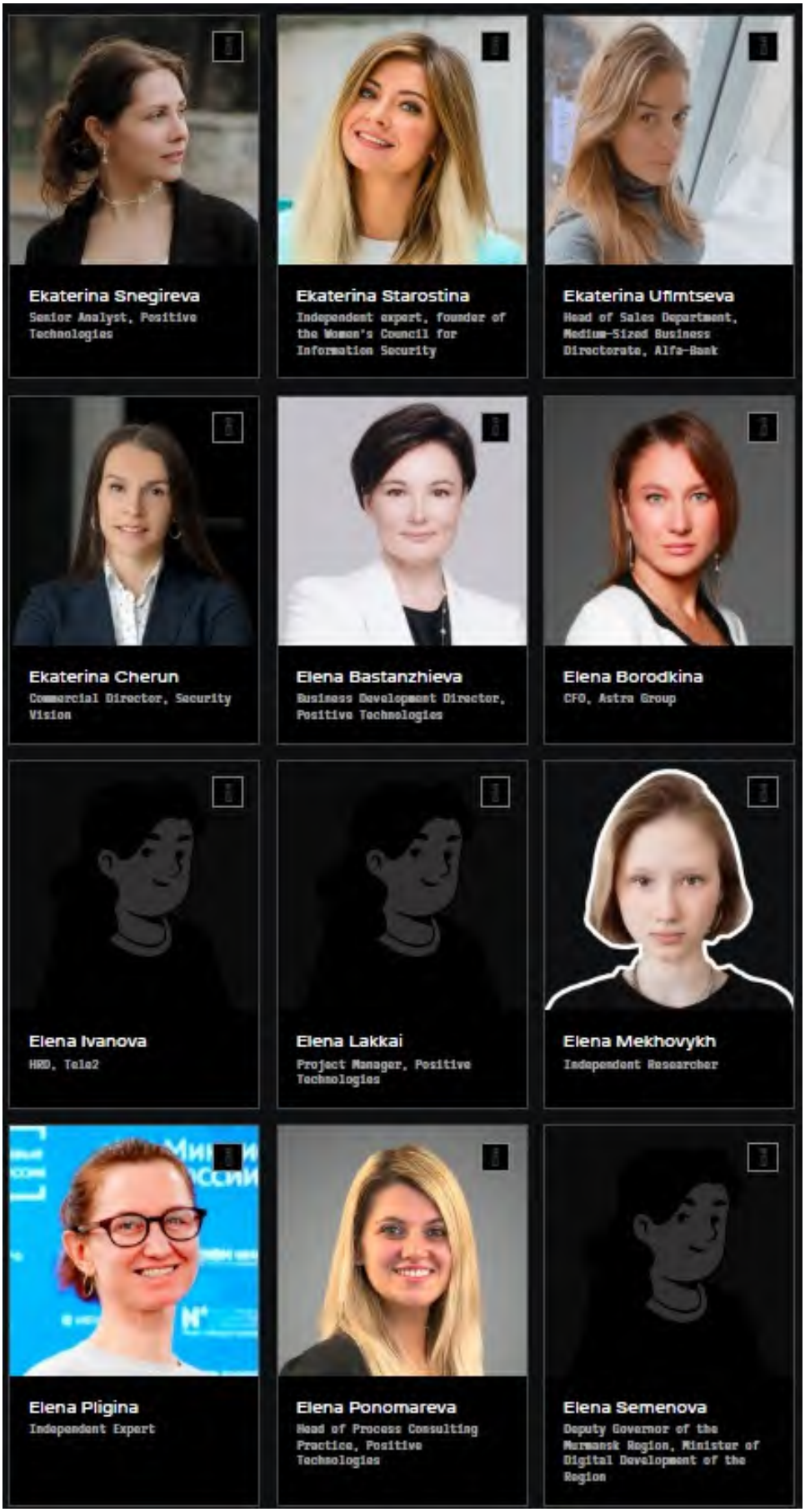
Ekaterina Barabanova
HR Development Director, Rostelecom

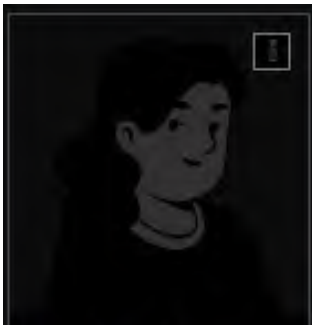
Ekaterina Isaykina
Director of Development and Marketing, S-Terra

Ekaterina Kononenko
Co-founder of the production studio Versus Pictures

Ekaterina Nikulina
Senior Specialist of Information Security Monitoring Department, Positive Technologies

Ekaterina Rudaya
Jet CyberCamp Product Manager, Jet Infosystems


Ekaterina Snegireva
Senior Analyst, Positive Technologies
Ekaterina Starostina
Independent expert, founder of the Women's Council for Information Security
Ekaterina Ufimtseva
Head of Sales Department, Medium-Sized Business Directorate, Alfa-Bank
Ekaterina Cherun
Commercial Director, Security Vision
Elena Bastanzhieva
Business Development Director, Positive Technologies
Elena Borodkina
CFO, Astra Group
Elena Ivanova
HRD, Tele2
Elena Lakkai
Project Manager, Positive Technologies
Elena Mekhovykh
Independent Researcher
Elena Pligina
Independent Expert
Elena Ponomareva
Head of Process Consulting Practice, Positive Technologies
Elena Semenova
Deputy Governor of the Murmansk Region, Minister of Digital Development of the Region



Elena Chernikova
PhD, Entrepreneur, CEO, Invisible Force (formerly Culture of Innovation)

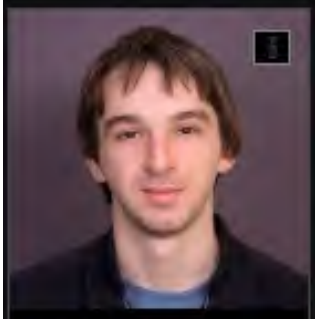
Elena Shedova
Vice President for Marketing, Kaspersky Lab

Elena Shmeleva
Chairman of the Council of the Sirius Federal Territory, Head of the Talent and Success Foundation

Zhan Prosyanov
Editor-in-Chief, General Director of Kino-Teatr.Ru, Development Director of CHILL, Producer

Ivan Balagurov
Senior Data Engineer, Kaspersky Lab

Ivan Koreshkov
Product Manager, Gazinformservice



Ivan Krivosheev
Lead Programmer, Positive Technologies

Ivan Stelmakh
Professor, New Economic School, Central University CFO

Ivan Chernov
Development Manager, UserGate

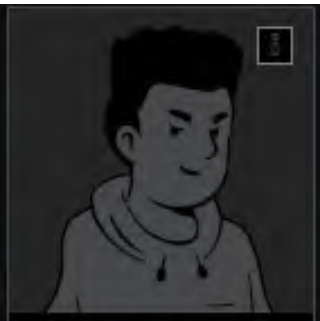
Igor Anokhin
PaaS Team Lead, K2 Cloud

Igor Verbitsky
Head of Information Security, Lamoda Tech

Igor Gots
Information Security Engineer, Yandex

Treadstone 71

Igor Panarin
Senior Developer, Tinkoff



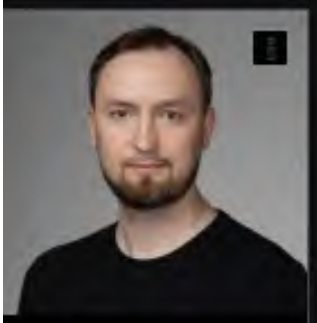
Igor Pervushin
Head of Knowledge Base Creation, CyberOK

Igor Serikov
Expert on the development of blockchain products, Idea Research Center

Ildar Sadykov
Head of Expert Training, Positive Technologies

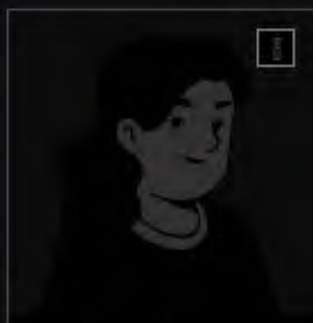
Ilya Borisov
Director of the Information Security Methodology Department, VK

Ilya Vikulov
Expert, Gazprombank



Ilya Zuev
Vice President for Information Security, MTS Bank

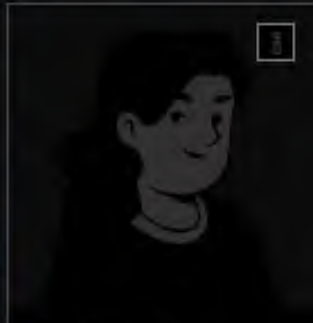
Ilya Kotsyuba
Expert, Bank GPB (JSC)



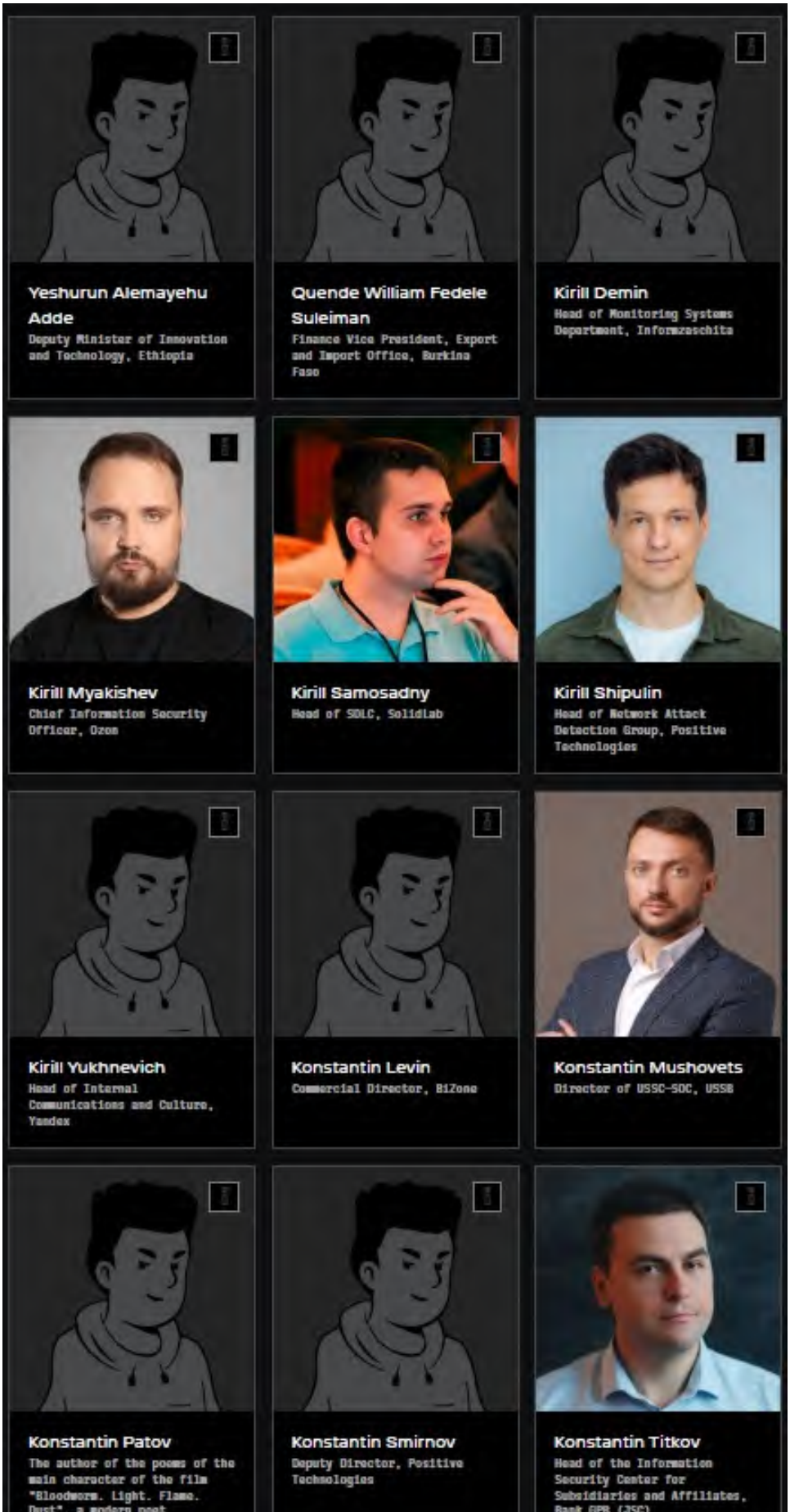
Irina Akopyan
Director of PTFS and Corporate Finance, Positive Technologies

Irina Zinovkina
Head of Research Group, Positive Technologies

Irina Levova
Director of Strategic Projects, Big Data Association



Irina Slonkina
Cryptographic Analyst, Positive Technologies



Yeshurun Alemayehu Adde
Deputy Minister of Innovation and Technology, Ethiopia

Quende William Fedele Suleiman
Finance Vice President, Export and Import Office, Burkina Faso

Kirill Demin
Head of Monitoring Systems Department, Informzaschita

Kirill Myakishev
Chief Information Security Officer, Ozon

Kirill Samosadny
Head of SDLC, SolidLab

Kirill Shipulin
Head of Network Attack Detection Group, Positive Technologies

Kirill Yukhnevich
Head of Internal Communications and Culture, Yandex

Konstantin Levin
Commercial Director, BiZone

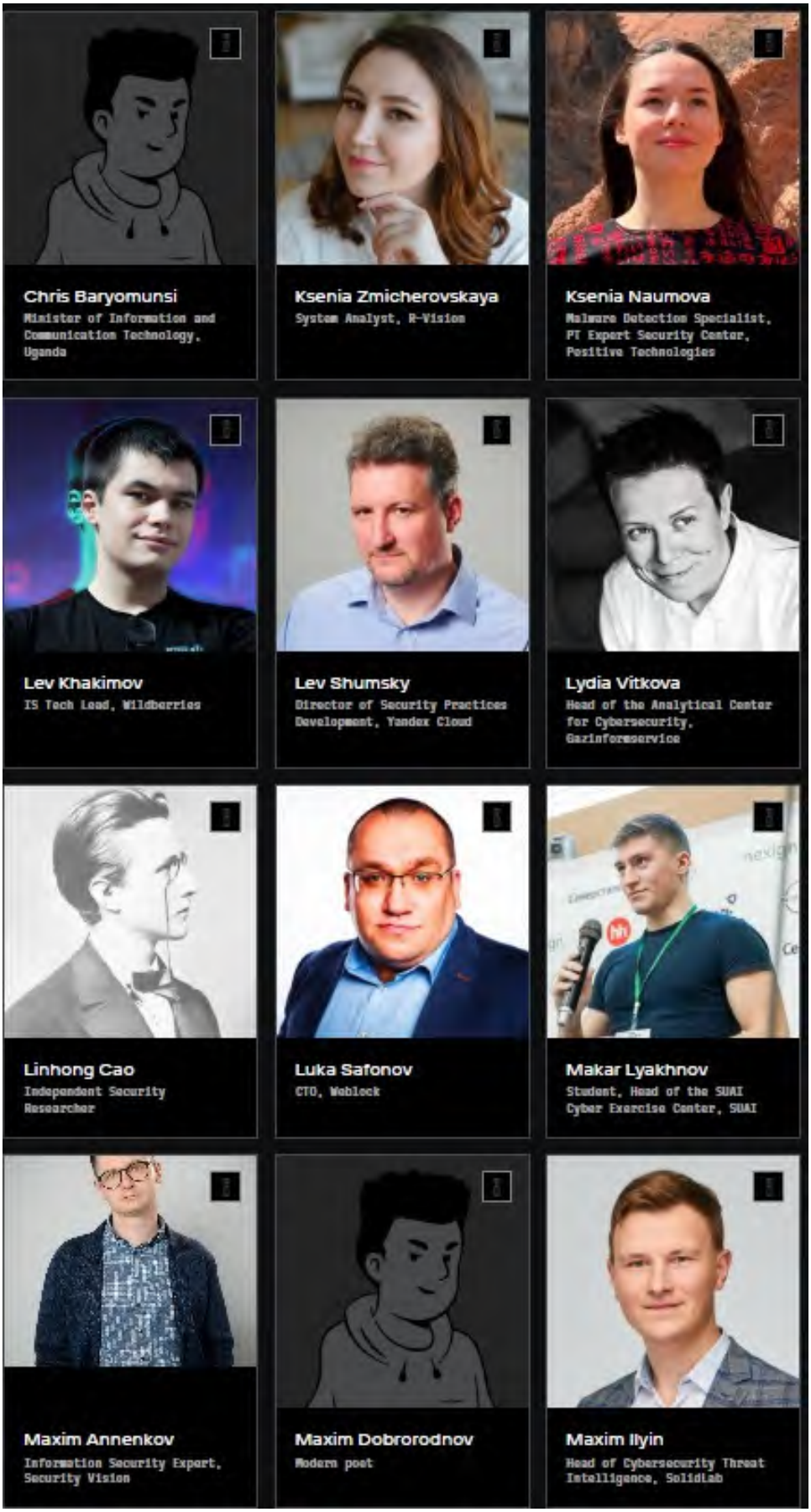
Konstantin Mushovets
Director of USSC-SOC, USSB

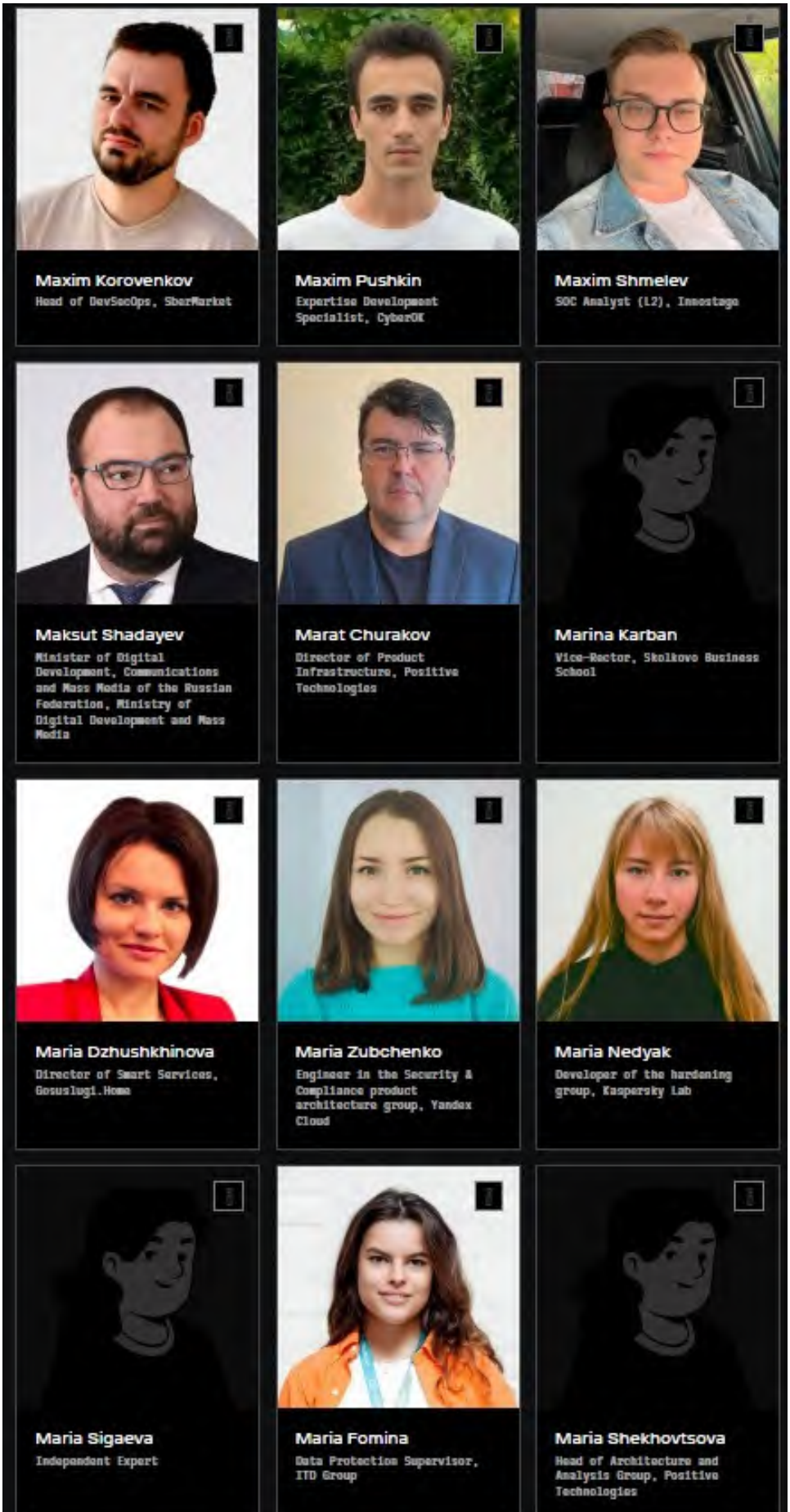
Konstantin Patov
The author of the poems of the main character of the film "Bloodworm. Light. Flame. Dust". a modern poet

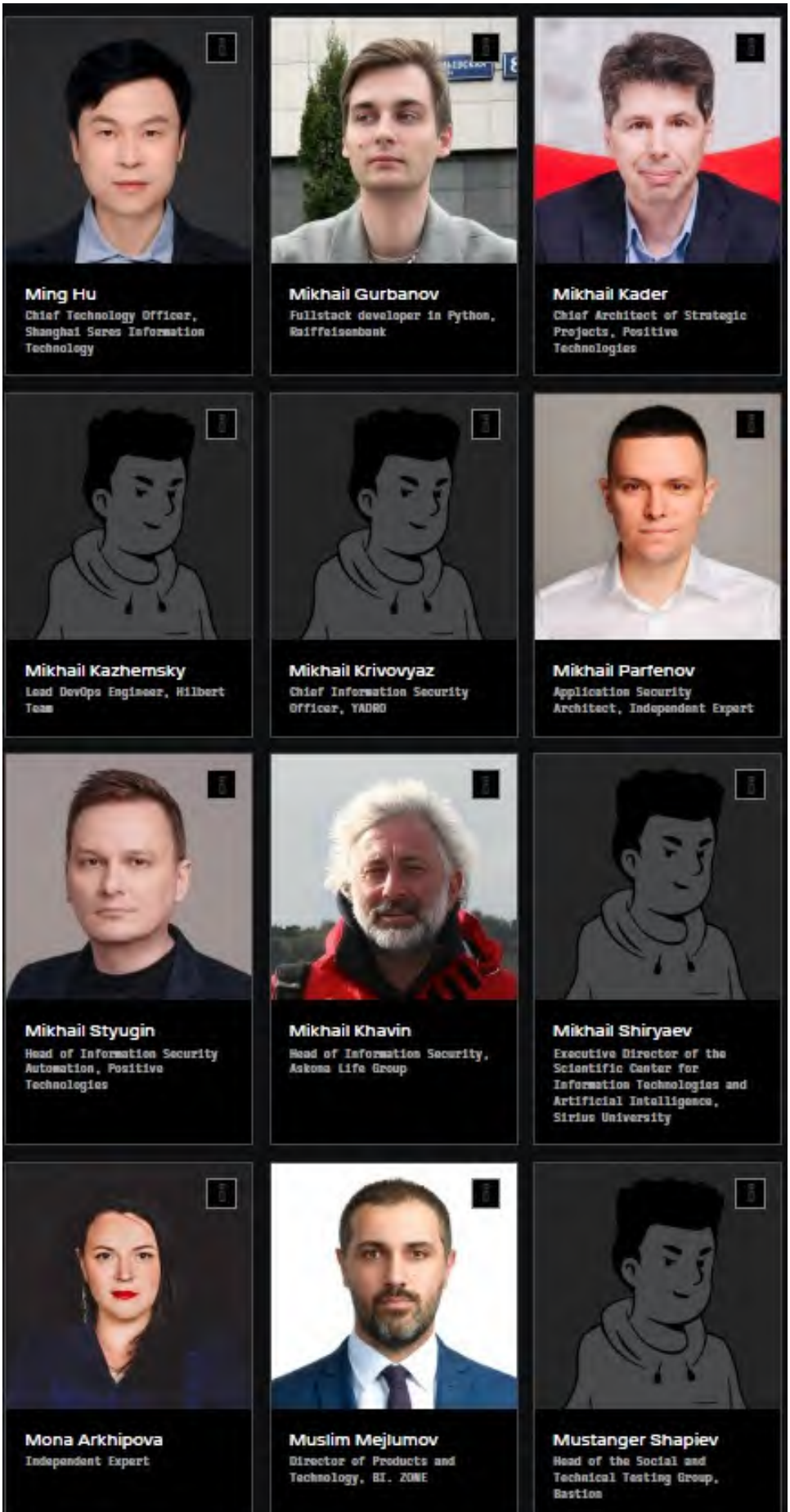
Konstantin Smirnov
Deputy Director, Positive Technologies

Konstantin Titkov
Head of the Information Security Center for Subsidiaries and Affiliates, Bank GPB (JSC)

Treadstone 71




Maxim Korovenkov
Head of DevSecOps, SberMarket
Maxim Pushkin
Expertise Development Specialist, CyberOK
Maxim Shmelev
SOC Analyst (L2), Innostage
Maksut Shadayev
Minister of Digital Development, Communications and Mass Media of the Russian Federation, Ministry of Digital Development and Mass Media
Marat Churakov
Director of Product Infrastructure, Positive Technologies
Marina Karban
Vice-Rector, Skolkovo Business School
Maria Dzhushkhinova
Director of Smart Services, Gosuslugi.Home
Maria Zubchenko
Engineer in the Security & Compliance product architecture group, Yandex Cloud
Maria Nedyak
Developer of the hardening group, Kaspersky Lab
Maria Sigaeva
Independent Expert
Maria Fomina
Data Protection Supervisor, ITD Group
Maria Shekhovtsova
Head of Architecture and Analysis Group, Positive Technologies



Ming Hu
Chief Technology Officer, Shanghai Sanes Information Technology

Mikhail Gurbanov
Fullstack developer in Python, Raiffeisenbank

Mikhail Kader
Chief Architect of Strategic Projects, Positive Technologies

Mikhail Kazhemsky
Lead DevOps Engineer, Hilbert Team

Mikhail Krivovyaz
Chief Information Security Officer, YADRO

Mikhail Parfenov
Application Security Architect, Independent Expert

Mikhail Styugin
Head of Information Security Automation, Positive Technologies

Mikhail Khavin
Head of Information Security, Askona Life Group

Mikhail Shiryaev
Executive Director of the Scientific Center for Information Technologies and Artificial Intelligence, Sirius University

Mona Arkhipova
Independent Expert

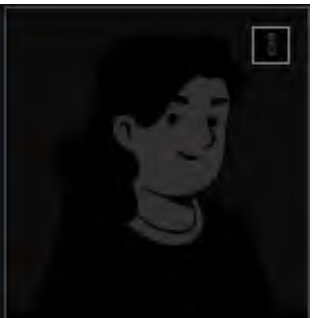
Muslim Mejlumov
Director of Products and Technology, BI. ZONE

Mustanger Shapiev
Head of the Social and Technical Testing Group, Bastion

Treadstone 71

Mustafa Salima Lotia
Head of Information Security Department, EasyPaisa Bank, Pakistan

Natalia Akimova
Head of Smart City, Rosatom



Natalia Voevodina
Independent Expert

Natalia Klishina
Founder of DE M.A.D.A. LLC

Natalia Seliverstova
Project Manager, ICL ST

Nikita Gergel
Head of Cloud Security & Compliance, Yandex Cloud

Nikita Zelinsky
Head of the MTS Big Data and ML Platforms Competence Center, MTS

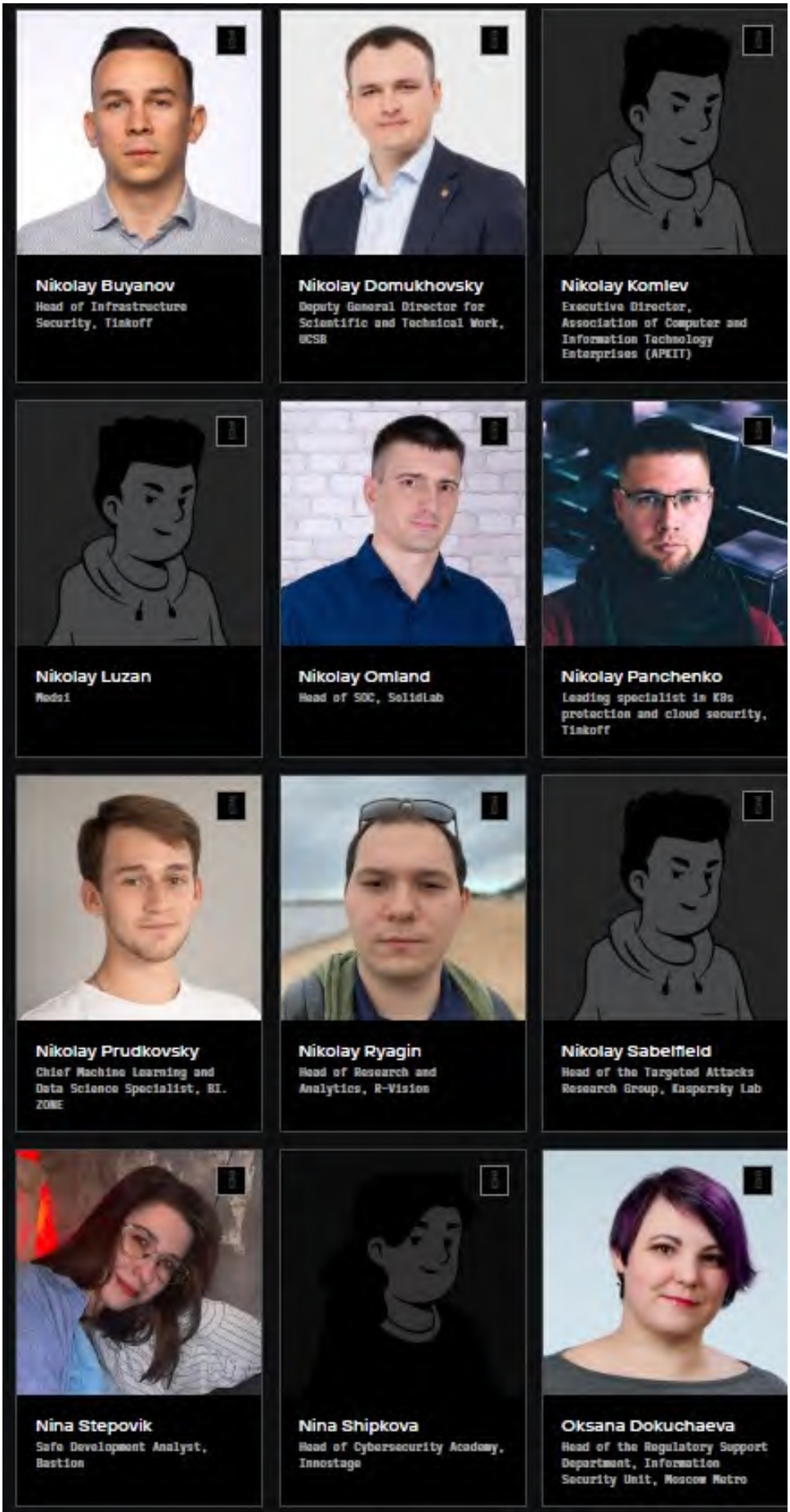
Nikita Ladoshkin
Head of Development at PT Container Security, Positive Technologies

Nikita Sinkevich
Head of Analysis and Response, Angara Security

Nikita Firsov
Expert at Positive Labs, Positive Technologies

Nikita Yudin
Product Marketing Manager, Positive Technologies

Nikolay Anisenya
Head of Advanced Technologies of the Security Analysis Department, Positive Technologies



Nikolay Buyanov
Head of Infrastructure Security, Tinkoff

Nikolay Domukhovsky
Deputy General Director for Scientific and Technical Work, UCSB

Nikolay Komlev
Executive Director, Association of Computer and Information Technology Enterprises (APKIT)

Nikolay Luzan
Modsi

Nikolay Omland
Head of SOC, SolidLab

Nikolay Panchenko
Leading specialist in K8s protection and cloud security, Tinkoff

Nikolay Prudkovsky
Chief Machine Learning and Data Science Specialist, BI.ZONE

Nikolay Ryagin
Head of Research and Analytics, R-Vision

Nikolay Sabelfield
Head of the Targeted Attacks Research Group, Kaspersky Lab

Nina Stepovik
Safe Development Analyst, Bastion

Nina Shipkova
Head of Cybersecurity Academy, Innostage

Oksana Dokuchaeva
Head of the Regulatory Support Department, Information Security Unit, Moscow Metro

Oleg Ignatov
Head of University Relations, Positive Technologies

Oleg Kolesnikov
Deputy General Director, Director for Product, Competitions, Broadcasting and Technology, Agency for the Development of Computer and Other Sports

Oleg Kochergin
Director of Data Management, Positive Technologies

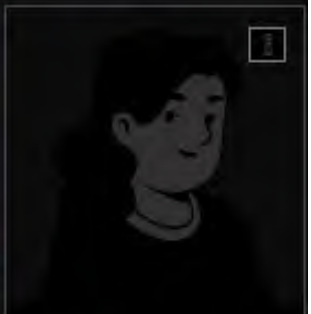
Oleg Kochetov
Head of Security Analysis Department, Astra Group

Oleg Kuzmin
Independent Expert

Oleg Skulkin
The head of BI. ZONE Threat Intelligence, BI. ZONE

Oleg Shakirov
Independent Researcher

Olga Pukhova
Information Security Consultant, Innostage

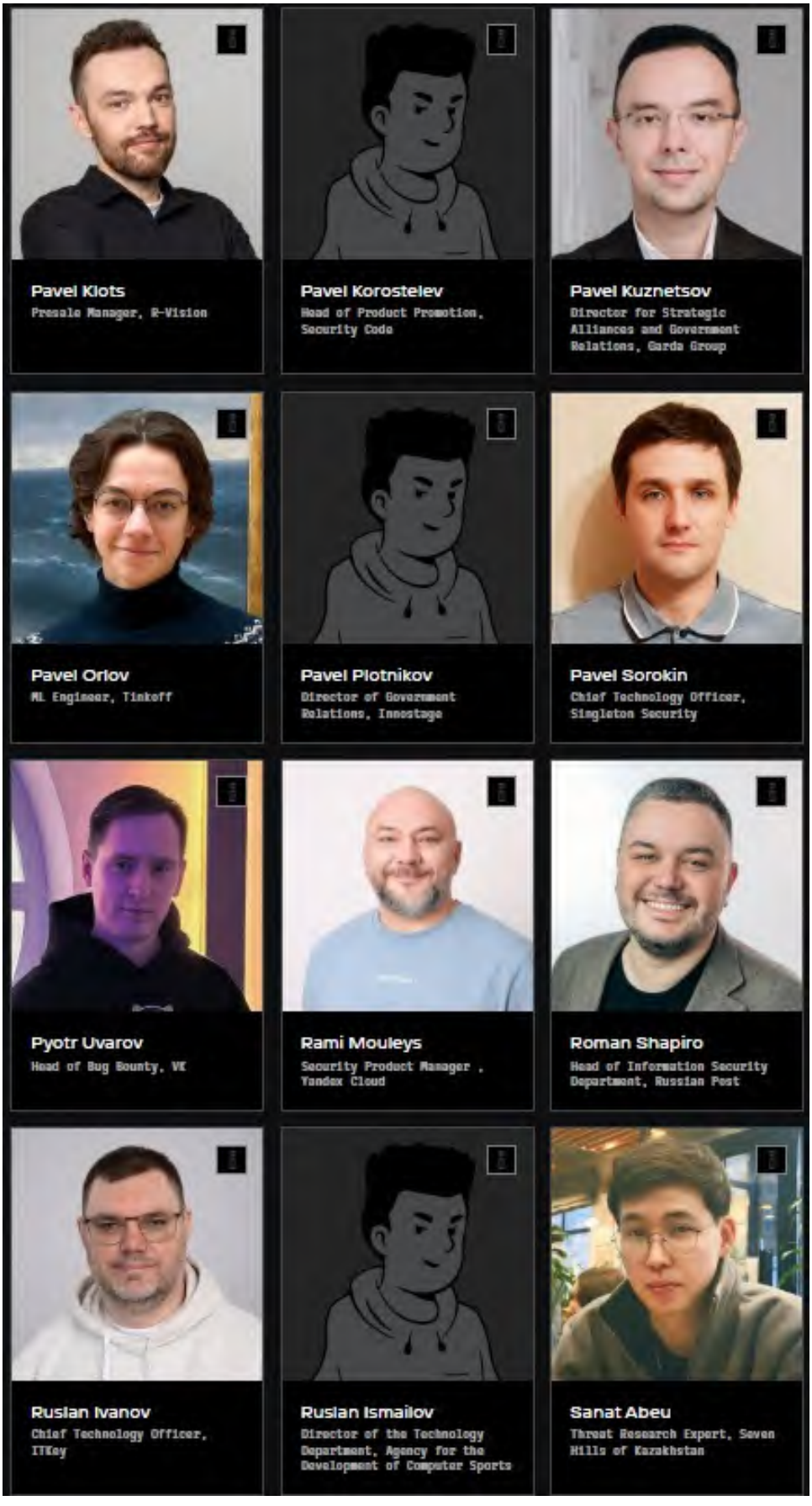


Olga Skorobogatova
First Deputy Chairman of the Central Bank of the Russian Federation, Central Bank of the Russian Federation

Oscar Gadyishin
Head of Information Technology and Cybersecurity Department, ICL System Technologies (ICL

Pavel Vorobyov
CEO, QRate, QSpace

Pavel Ivannikov
Expert at Positive Labs, Positive Technologies



Pavel Klots
Presale Manager, R-Vision

Pavel Korostelev
Head of Product Promotion, Security Code

Pavel Kuznetsov
Director for Strategic Alliances and Government Relations, Garda Group

Pavel Orlov
ML Engineer, Tinkoff

Pavel Plotnikov
Director of Government Relations, Innostage

Pavel Sorokin
Chief Technology Officer, Singleton Security

Pyotr Uvarov
Head of Bug Bounty, VK

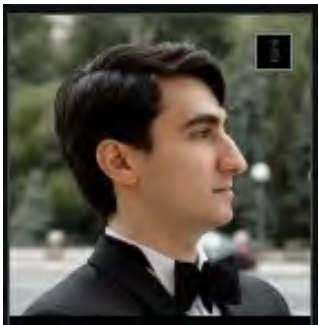
Rami Mouleys
Security Product Manager , Yandex Cloud

Roman Shapiro
Head of Information Security Department, Russian Post

Ruslan Ivanov
Chief Technology Officer, ITKey

Ruslan Ismailov
Director of the Technology Department, Agency for the Development of Computer Sports

Sanat Abeu
Threat Research Expert, Seven Hills of Kazakhstan



Sargis Nanyan
Head of Infrastructure Security, Ozon Tech

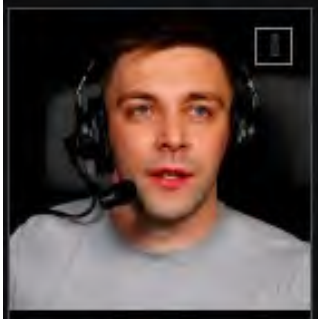
Sasha Maloy
Stand-up comedian

Svetlana Gazizova
Director of DevSecOps Process Building, Positive Technologies

Sec Maktar
Head of the Technology and Innovation Section of the United Nations Economic Commission for Africa, Senegal

Sergey Bogdasarov
Modern poet

Sergey Bychkov
Deputy Head for Information Security, CIT of the Krasnoyarsk Territory



Sergey Vasiliev
Developer, Positive Technologies

Sergey Voldokhin
Start X

Sergey Golyakov
Head of DevSecOps, Ingosstrakh

Sergey Gordeychik
CEO, CyberOK

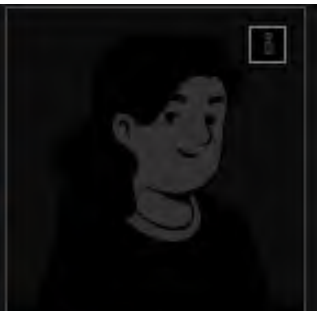
Sergey Danilov
Head of Information Security Department, Rosreestr

Sergey Demidov
Deputy Chairman of the Executive Board for Information Security, Moscow Exchange

Treadstone 71

Sergey Iskhakov
Head of the Department of Analysis and Automation of Computer Incident Response, PSB

Sergey Kalmykov
General Director, Cyberdom

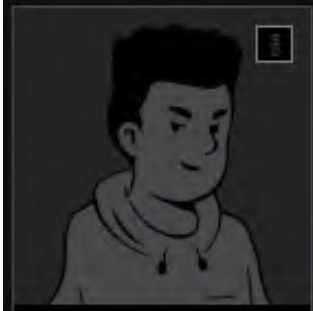


Sergey Libik
Invest Analyst, Gazprombank

Sergey Malozyomov
Leading

Sergey Nikitin
Head of Product Management Group, Gazinformservice

Sergey Plotko
Director of Analytics and Integration, Digital Solutions



Sergey Savchenko
Director of Information Security, Pulkovo

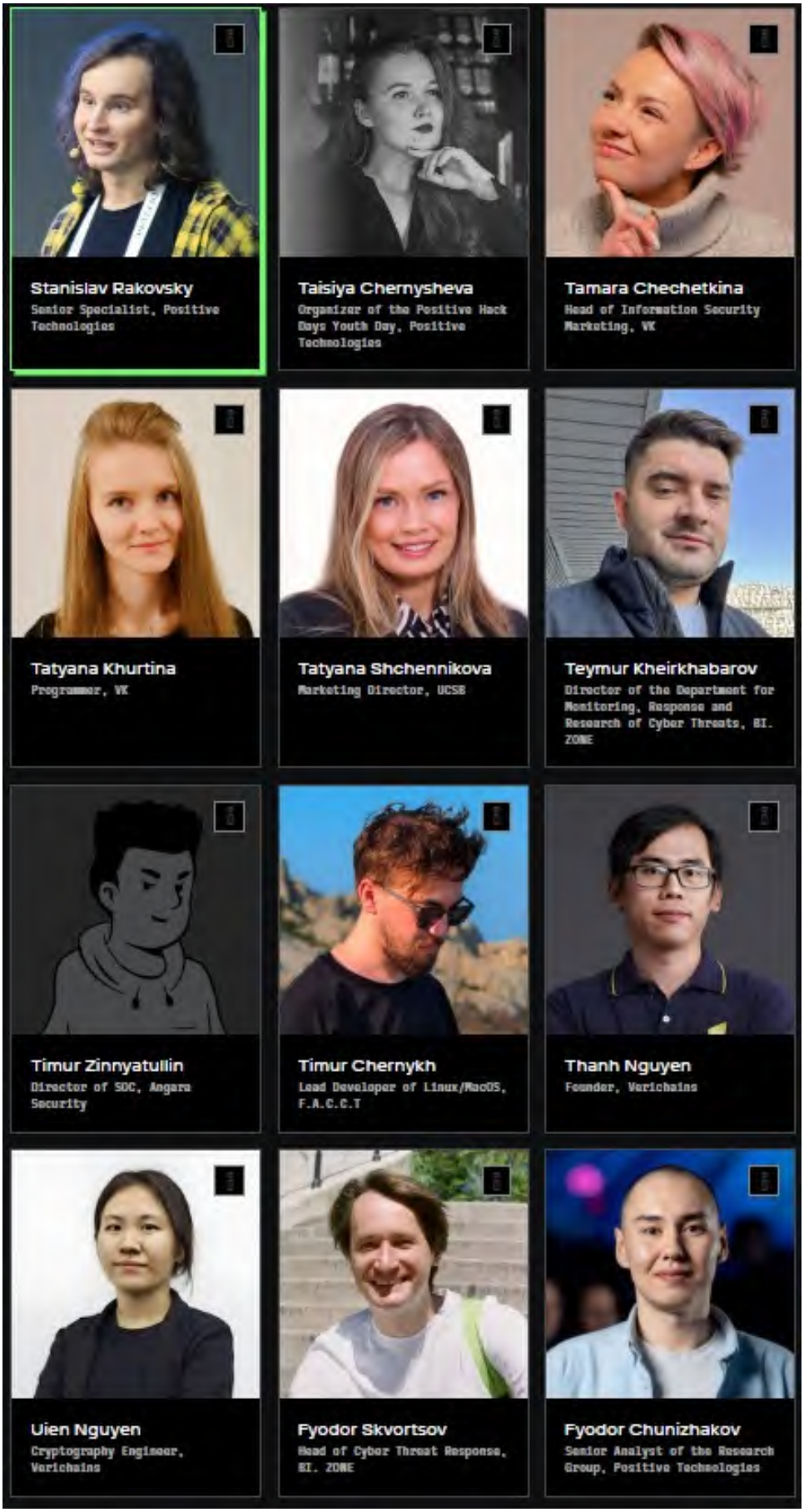
Sergey Sazhin
Independent Expert

Sergey Sobolev
Distributed Systems Security Specialist, Positive Technologies

Sergey Soldatov
Head of the Cybersecurity Monitoring Center, Kaspersky Lab

Sergey Sytin
Head of Department, Innostage

Stanislav Pyzhov
Senior Specialist of the Information Security Threat Research Department of PT Expert Security Center, Positive Technologies


Stanislav Rakovsky
Senior Specialist, Positive Technologies
Taisiya Chernysheva
Organizer of the Positive Hack Days Youth Day, Positive Technologies
Tamara Chechetkina
Head of Information Security Marketing, VK
Tatyana Khurtina
Programmer, VK
Tatyana Shchennikova
Marketing Director, UCSB
Teymur Kheirkhabarov
Director of the Department for Monitoring, Response and Research of Cyber Threats, GI. ZONE
Timur Zinnyatullin
Director of SOC, Angara Security
Timur Chernykh
Lead Developer of Linux/MacOS, F.A.C.C.T
Thanh Nguyen
Founder, Verichains
Uien Nguyen
Cryptography Engineer, Verichains
Fyodor Skvortsov
Head of Cyber Threat Response, GI. ZONE
Fyodor Chunizhakov
Senior Analyst of the Research Group, Positive Technologies

Philippe Delgyado
Architect, Lekton.io

Hussein Daher
CEO, Web Immunify

Charles Lim
Deputy Head of the Master of Information Technology, Swiss-German University

Jinyang Peng
Chief Architect and Chief Security Researcher, Sangfor

Edgar Sipki
Ozon Tech

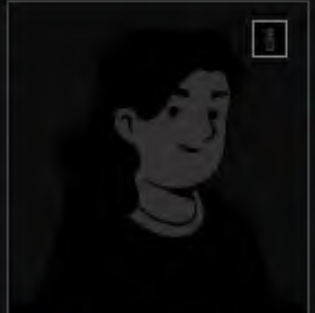
Elman Behbudov
Director of Product Business Development, Positive Technologies

Erika Lundmoen
Independent performer

Julia Voronova
Consulting Director, Positive Technologies

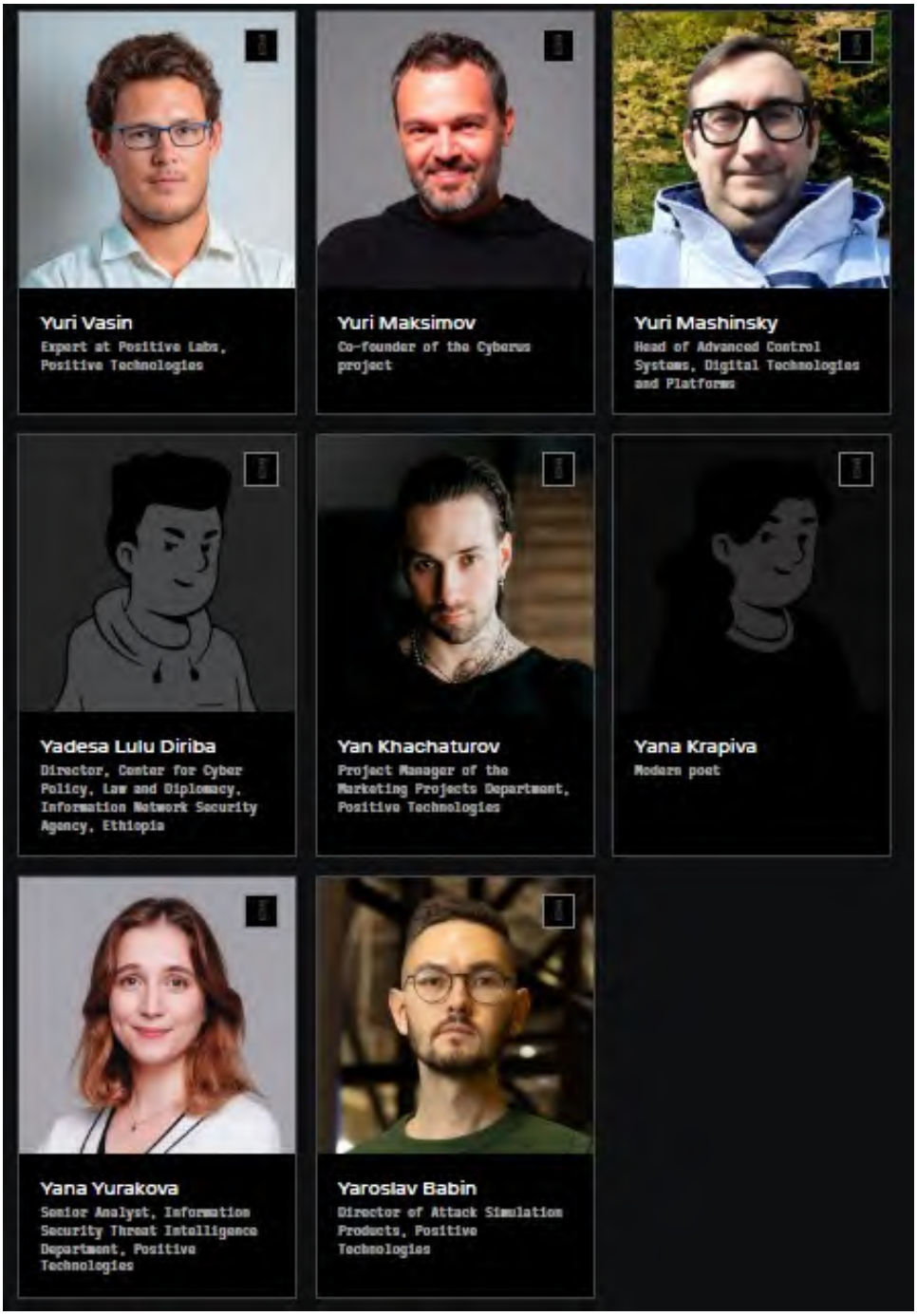
Yulia Goryachkina
Director of Human Resources for the Digital Economy, ANO Digital Economy

Yulia Danchina
Director of Customer and Partner Training, Positive Technologies



Yulia Sanzharevskaya
Modern poet

Yulia Fomina
Head of Metaproduct Expertise Group, Threat Detection Department, PT Expert Security Center, Positive Technologies



Innovative and Unusual Malicious Techniques from PHDays Collaboration

The collaboration at Positive Hack Days (PHDays) among Ravin Academy, Positive Technologies, and Kaspersky could lead to the development of novel and highly sophisticated cyberattack techniques. Here are several unique and innovative tactics that may emerge from this collaboration, distinct from previously discussed methods-

Quantum Computing Exploits

As quantum computing technology advances, breaking traditional encryption methods becomes more feasible. The collaboration could develop quantum algorithms capable of decrypting data encrypted with current standards. Quantum computers could solve problems currently intractable for classical computers, potentially rendering most of today's cryptographic defenses obsolete.

Scenario- A nation-state actor deploys quantum-powered decryption techniques to access sensitive data from government and military communication channels previously thought secure, allowing for real-time interception and decryption of encrypted messages, leading to significant intelligence gains.

AI-Driven Autonomous Malware

Leveraging advancements in artificial intelligence, attackers could develop autonomous malware capable of learning and adapting to its environment without human intervention. Such malware would use machine learning to identify and exploit vulnerabilities, adjust its behavior based on detection mechanisms it encounters, and continuously evolve.

Scenario- Releasing AI-driven malware into a corporate network, where it learns the network's defensive measures and adapts its tactics to remain undetected. Over time, it becomes increasingly effective at stealing data and avoiding mitigation efforts, requiring equally advanced AI to counteract.

Biological Computing Attacks

The intersection of biology and computing has given rise to biological computing, using biological materials to perform computational processes, leading to bio-hacked malware, which uses biological processes to interfere with or enhance traditional cyber attacks.

Scenario- Developing Bio-hacked malware to interact with biological systems in medical devices, potentially causing malfunctions or data corruption in health monitoring systems, leading to false readings or unauthorized control over medical treatments.

Cyber-Physical Fusion Attacks

Integrating cyber-attacks with physical processes, attackers could develop methods to exploit cyber-physical systems in ways not previously imagined, such as creating malware that interacts directly with physical devices in novel ways, leading to unexpected behaviors or damage.

Scenario- Design malware to infiltrate smart infrastructure systems, such as smart grids or smart cities, and cause coordinated disruptions. For example, altering traffic light patterns to cause congestion or manipulating energy distribution systems to create power outages.

Steganographic Malware

Use advanced steganographic techniques to embed malicious code within seemingly benign data files, such as images or audio files. These methods make detection exceedingly tricky, as the malware is hidden within non-executable data streams.

Scenario- Attackers distribute malware hidden within popular image files on social media platforms. When these images are downloaded and viewed, the embedded code executes, installing spyware on the victim's device without detection.

Bioinformatics Exploits

With the rise of bioinformatics, cyber attackers might exploit genetic data and other biological datasets, possibly involving the manipulation of biological data to create false research outcomes or tampering with genetic information to impact medical treatments.

Scenario- Hackers access and alter genetic research data, leading to incorrect scientific conclusions or compromised personalized medicine programs, having long-term impacts on health policies and medical research.

Neuromorphic Computing Attacks

Neuromorphic computing mimics the human brain's neural structure to create highly efficient and adaptive systems. Cyber attackers might develop malware leveraging neuromorphic chips, resulting in highly adaptive and energy-efficient attacks that are hard to detect using traditional methods.

Scenario- Introduce a neuromorphic chip-based malware into critical infrastructure systems, where it operates with minimal energy consumption and high adaptability, making it capable of continuous operation without detection.

Geo-Targeted Attacks Using Advanced Geofencing

Combined with advanced geographic information systems (GIS), geofencing could create highly targeted attacks based on the target's physical location, triggering attacks only when the target is within a specific geographic boundary.

Scenario- Design malware to activate only when a high-profile target travels to a specific location, such as a conference or meeting. This geofenced attack ensures that the malware remains dormant and undetectable until the precise conditions are met.

Implications and Countermeasures

Developing these advanced techniques highlights the need for continuous innovation in cybersecurity defenses. Organizations must invest in cutting-edge research and technology to anticipate and counteract these novel threats. Strategies should include-

- Enhanced Threat Intelligence- Proactively gather and analyze threat intelligence to anticipate new attack vectors and methodologies.
- Advanced AI and Machine Learning Defenses- Developing AI-driven security solutions capable of detecting and responding to autonomous and adaptive threats.
- Quantum-Resistant Cryptography- Investing in quantum-resistant encryption methods to prepare for the eventual rise of quantum computing exploits.
- Interdisciplinary Security Research- Combining biology, neurology, and computer science knowledge to develop comprehensive defenses against bio-hacked and neuromorphic attacks.

Organizations significantly enhance their cybersecurity defenses and reduce the risks associated with these innovative and potentially destructive techniques by proactively identifying and preparing for these emerging threats. Understanding the evolving threat landscape and implementing advanced defensive strategies allows organizations to stay ahead of malicious actors and protect their critical assets more effectively.

Malware Table

Malware Development Technique	Maliciousness	Intent	Targets	Country of Origin	Industry Targets	Likelihood of Use	Additional Considerations
Rootkit Development and Evolution	High	Espionage, Sabotage	Government, Military, Critical Infrastructure	Iran	Energy, Finance, Defense	High	Rootkits are difficult to detect and remove, posing a long-term threat.
Advanced Persistent Threat (APT) Techniques	High	Espionage, Data Theft	Government, Corporate Networks	Iran	Technology, Finance, Healthcare	High	APTs focus on prolonged, undetected presence in networks.
Malware Detection Evasion	High	Espionage, Sabotage	Government, Corporate Networks	Iran	Financial, Healthcare, Technology	High	Techniques evolve rapidly to stay ahead of detection tools.
Ransomware Development	High	Financial Gain, Sabotage	Corporate, Healthcare	Iran	Healthcare, Finance, Retail	High	Lucrative attacks with significant economic impact.
Exploiting Zero-Day Vulnerabilities	High	Espionage, Sabotage	Government, Corporate Networks	Iran	All sectors	High	Exploiting unknown vulnerabilities gives a significant advantage.
Quantum Computing Exploits	High	Espionage	Government, Military	Iran, Russia	All sectors	Medium	Emerging technology with potential to break current encryption.
AI-Driven Autonomous Malware	High	Espionage, Sabotage	Critical Infrastructure, Corporate Networks	Iran, Russia	Energy, Healthcare, Technology	High	AI-driven malware can adapt and evolve autonomously.
Biological Computing Attacks	Medium	Sabotage	Healthcare, Biotech	Iran, Russia	Biotech, Healthcare	Low	Novel attack vector with potential high impact.
Cyber-Physical Fusion Attacks	High	Sabotage	Critical Infrastructure, Smart Cities	Iran, Russia	Energy, Transportation, Utilities	High	Combines physical and cyber elements for impactful attacks.
Steganographic Malware	High	Espionage	Government, Corporate Networks	Iran, Russia	All sectors	High	Hidden within benign files, making detection difficult.
Bioinformatics Exploits	Medium	Espionage	Research Institutions, Healthcare	Iran, Russia	Healthcare, Research	Medium	Manipulates biological data for high-stakes espionage.
Neuromorphic Computing Attacks	High	Sabotage, Espionage	Military, Industrial Control Systems	Iran, Russia	Defense, Manufacturing	Medium	Highly efficient and adaptive, leveraging neuromorphic chips.
Geo-Targeted Attacks	High	Espionage, Sabotage	Political Figures, Military	Iran, Russia	Government, Defense	Medium	Attacks activate based on specific geographic locations.

Figure 1 Potential Malware Table

- Rootkit Development and Evolution- Rootkits allow unauthorized access and control, maintaining long-term stealth within systems. The likelihood of use is high due to their persistence and difficulty in detection.
- Advanced Persistent Threat (APT) Techniques- APTs enable prolonged espionage and data theft, targeting critical sectors with high-value data. The sophistication of these attacks makes them highly likely.
- Malware Detection Evasion- Techniques to evade detection are crucial for maintaining malware presence. Advanced evasion tactics increase the likelihood of successful attacks.
- Ransomware Development- Ransomware continues to be a lucrative form of cybercrime, significantly impacting targeted industries. Its profitability ensures a high likelihood of use.
- Exploiting Zero-Day Vulnerabilities- Zero-day exploits provide attackers with opportunities to breach systems before patches are available, making these highly valuable and likely to be used.
- Quantum Computing Exploits- While still emerging, quantum computing poses future threats to encryption. The potential impact is high, though the current likelihood remains medium.
- AI-Driven Autonomous Malware- AI-driven malware can independently adapt and evolve, presenting a significant threat to diverse sectors due to its high adaptability and intelligence.

- Biological Computing Attacks- Using biological processes in cyber attacks is novel and less likely but could significantly impact the biotech and healthcare sectors.
- Cyber-Physical Fusion Attacks- Integrating cyber and physical systems, these attacks can cause significant disruptions to critical infrastructure, making them highly likely and impactful.
- Steganographic Malware- By hiding within benign files, steganographic malware evades detection, posing a high risk to targeted sectors.
- Bioinformatics Exploits- Manipulating biological data for espionage is a medium-likelihood threat, potentially impacting healthcare and research.
- Neuromorphic Computing Attacks- Leveraging neuromorphic chips, these attacks are efficient and adaptive, posing medium likelihood but high potential impact.
- Geo-Targeted Attacks- Activating based on geographic location, these attacks can precisely target political and military figures, presenting a medium likelihood and high risk.

Program

ON THE TRACK | BY LOCATION

MAY 23 | MAY 24 | MAY 25 | MAY 26

Hide past reports

TRACKS

The time in the program is displayed according to your time zone

03:00–04:00

DEFENSE REPORT

Incident response errors in 2023-2024

Data theft and encryption are two of the most pressing issues of 2023. Each company that encountered them tried to use their own approaches to solving the problems that arose, and many managed to mess things up, given that they encountered such attacks for the first…

Sergey Golovanov
Kaspersky Lab

Titan Hall

LOOK

03:00–03:15

EVASION DISCUSSION

Introductory remarks about the track Evasion

Alexey Vishnyakov
Positive Technologies

Gravity Hall

LOOK ▷

03:00–04:00

OFFENSE REPORT

Small big boxes

We will focus on management, control and management, which breed passion in the hearts of hackers. Let's dig up a variety of small and large boxes – black and various shades of gray – that live in your nets, and we won't hurt them (but that's not certain). We will…

Artemy Tsetsersky
CyberOK

Andrey Sikorsky
CyberOK

Maxim Pushkin
CyberOK

Ganymede Hall

LOOK ▷

03:00–03:25

CYBERBEZ: WHERE TO START REPORT

Positive Hack Days festival. Discovery. Are Russian companies ready to resist cyberattacks?

We conducted a study to find out what measures Russian companies are taking to proactively protect against cyber threats. At the presentation, we will share the results, talk about the main problems in ensuring the company's cyber resilience, as well as give…

Anton Isaev
Positive Technologies

Fyodor Chunizhakov
Positive Technologies

Main Stage "Galaxy"

LOOK ▷

03:00–03:45

CISO SCHOOL REPORT

Do businesses still need you? Lessons from Russia's largest private bank

Attendees will learn about the world's leading digital bank's strategy to strengthen cybersecurity through a product-centric approach that transforms data-driven insights into results that demonstrate the value of security for the various business teams involved in…

Dmitry Gadar
Tinkoff

Meteor Hall

LOOK ▷

03:00–03:20

SECURE DEVELOPMENT REPORT

Opening a Track

Welcome speech from the organizers of the track

Vladimir Kochetkov
POSIdev Community Leader

Phobos Hall

LOOK ▷

03:20–04:00

SECURE DEVELOPMENT REPORT

Culture of secure by design

Let's talk about what the secure by design culture is, how it is born, and how we can all help it develop.

Denis Korablev

LOOK ▷

03:30–04:15

EVASION DISCUSSION

How to Avoid Missing a Hacker on a Client Machine, or Protection Technologies and Techniques to Bypass Antiviruses and EDR Systems

Technical experts of cybersecurity products and solutions will face off: they will analyze in detail the protection technologies that are used in SIEM, IDS, EDR, sandbox products, as well as in meta-products.

Valery Slezkintsev — Positive Technologies
Teymur Kheirkhabarov — BI. ZONE

Gravity Hall

LOOK ▷

03:35–04:35

CYBERBEZ: WHERE TO START ДИСКУССИЯ

Is it possible to provide information security without having billion-dollar budgets?

The discussion will focus on affordable and effective information security strategies for organizations with limited resources. We will consider the basic protection measures that allow you to achieve a high level of security of digital assets without requiring…

Denis Romanyuk — "Pilot"
Mona Arkhipova — Independent Expert
Marat Churakov — Positive Technologies
Mikhail Kader — Positive Technologies
Andrey Kashirin — Cherkizovo Group

Main Stage "Galaxy"

LOOK ▷

phd 2

ПРОГРАММА

DEFENSE REPORT

Operation Triangulation: Why You Shouldn't Attack Researchers

Imagine that you detected a zero-touch (0-click) attack targeting your colleagues' iOS devices, and you were able to detect and analyze all stages of this sophisticated attack. That's exactly what happened to us! This led to the elimination of four zero-day…

Leonid Bezvershenko
Kaspersky Lab

Boris Larin
Kaspersky Lab

Georgy Kucherin
Kaspersky Lab

Titan Hall

LOOK ▷

04:00–05:00

OFFENSE REPORT

Faceless: Present your quotation mark

Biometric readers offer a unique solution to provide a higher level of security and convenience. They allow you to identify a person based on his unique biological characteristics. However, like any technology, biometric readers have their own security…

Giorgi Kiguradze
Kaspersky Lab

Ganymede Hall

LOOK ▷

04:00–05:00

GENERAL DEVELOPMENT REPORT

Go There — I Don't Know Where: Features of Interaction in Distributed Systems

Whether you're designing a microservice, service-oriented, monolithic, or three-tier architecture, you'll have to decide how services interact. Popular books are distinguished by unreasonable categoricalness, which greatly increases the cognitive complexity of…

Philippe Delgyado

Deimos Hall

LOOK ▷

04:00–05:00

SECURE DEVELOPMENT REPORT

ASP.NET Core SCA

Recently, there has been a lot of talk about supply chain attacks. Let's dive deeper into this topic regarding the ASP.NET platform. We will consider popular vulnerable libraries, discuss the Nuget package manager, see examples of attacks and effective SCA solutions.

Alexey Morozov
Samokat.tech

Phobos Hall

LOOK ▷

04:00–04:45

AI TRACK REPORT

How to Analyze 2000 Threat Intelligence Reports a Year and Not Go Crazy

When building a defense or responding to an incident, it is important to understand who is attacking you and what they will do next. Where to get this knowledge? Every day, from 6 to 11 full-fledged multi-page threat-intelligence reports describing the work of groups…

Nikolay Arefyev
Cyber Threat Technologies (RST Cloud)

Orion Hall

LOOK ▷

04:00–04:45

CISO SCHOOL REPORT

The speaker will talk about how the economic efficiency of implementing secure development practices is calculated.

Svetlana Gazizova
Positive Technologies

Maria Shekhovtsova
Positive Technologies

Meteor Hall

LOOK ▷

04:00–04:30

AFFILIATE REPORT

Cyber Resilience Methodology and Multi-Vendor Ecosystem. Why Being Friends Is Better Than Cannibalizing

The talk will touch on the issues that arose when the company was faced with the need to turn a disparate product portfolio into a real ecosystem. How to avoid cannibalization inside the line and bloody competition outside? Highlight obvious weaknesses that you can…

Evgeny Surkov
Innostage

Hyperion Hall

LOOK ▷

04:00–12:00

STANDOFF

Standoff 13 Cyber Battle

Live from the heart of the cyber battle with a breakdown of cyber attacks and hot topics

Standoff

LOOK ▷

04:30–05:15

What Hackers Do to Avoid Detection on the Network, or Traffic Analysis Technologies and How to Bypass Them

Technical experts of cybersecurity products and solutions will face off: they will analyze in detail the protection technologies that are used in SIEM, IDS, EDR, sandbox products, as well as in meta-products.

Ksenia Naumova
Positive Technologies

Mustanger Shapiev
Bastion

Gravity Hall

LOOK ▷

04:30–05:00

AFFILIATE REPORT

NG SOAR: Next-Generation Response

In the talk, the speakers will present a new concept of a SOAR solution for managing the NIST incident handling process: from preparation for it to mitigation. Let's consider which features are necessary for investigating and responding to cybersecurity incidents,…

Eva Belyaeva
Security Vision

Alexey Peshik
Security Vision

Hyperion Hall

LOOK ▷

04:45–05:15

CYBERBEZ: WHERE TO START REPORT

PRINCIPIA. Fundamentals of information security of commercial organizations

Let's talk about what benefits a business receives from creating an information security service even in a non-large company, what are the goals and objectives of this service, as well as what basic principles and changes need to be implemented in the company to achiev…

Mikhail Khavin

Main Stage "Galaxy"

LOOK ▷

04:45–05:30

AI TRACK ДОКЛАД

Прогресс в обнаружении уязвимостей: векторизация кода с помощью трансформеров для надежного распознавания компонентов программного обеспечения и зависимостей

В докладе рассматривается проблематика распознавания уязвимых компонентов и зависимостей в ПО без метаданных. Авторы описывают метод векторизации кода с использованием моделей-трансформеров, основанный на графовом представлении без эвристических признаков. Изложены…

Роман Лебедь «Тинькофф»

Павел Орлов «Тинькофф»

Зал «Орион»

СМОТРЕТЬ ▷

05:00–06:00

GENERAL DEVELOPMENT REPORT

Прагматичная архитектура, или Проектируем ПО, руководствуясь алгоритмом и практическими соображениями

There is an opinion that the software architecture has nothing to do with the real program and that clever but incapable of writing real code entertains themselves with it, quoting Uncle Bob by heart. The architecture does require a different view of the problem than th…

Daniil Podolsky
YADRO

Deimos Hall

LOOK ▷

SECURE DEVELOPMENT REPORT

The Problem of Fathers and Sons: Analytics and Triage of Transitive Dependencies

According to statistics, vulnerabilities that get into our applications through transitive dependencies account for 85% of problems introduced from open source. Someone turns a blind eye to these problems due to the complexity of the triage, someone does not…

Alexey Smirnov
CodeScoring

Phobos Hall

LOOK ▷

05:00–06:00

DEFENSE REPORT

Hellhounds: Operation Lahat

The Decoy Dog malware first became publicly known in April 2023, but by the time the first research on the backdoor appeared, it had been actively used by threat actors since at least the end of 2021. At the same time, according to our research, the development of th…

Alexander Grigoryan Positive Technologies
Stanislav Pyzhov Positive Technologies

Titan Hall

LOOK ▷

05:00–05:45

CISO SCHOOL DISCUSSION

What is the result of the CISO's work: an increase in business indicators or a decrease in the number of incidents

Let's discuss the roles and goals of the chief security officer in the organization. The panelists will consider two opposing views on the performance of a CISO: the views of those who believe that the main measure of success is the growth of business indicators,…

Эксперт Банк ГПБ (АО) Московская биржа МТС Банк Yandex Cloud

Илья Борисов
VK

Алексей Лукацкий
Positive Technologies

Зал «Метеор»

СМОТРЕТЬ ▷

05:00–06:00

OFFENSE REPORT

Return of the zero session

The peak of zero-session attacks has passed more than 24 years ago, and today most companies monitor and prevent such activities using configured security policies. But is there a chance after such a long time to successfully use the zero session in modern…

Haidar Kabibo
Kaspersky

Ganymede Hall

LOOK ▷

05:00–06:00

AFFILIATE DISCUSSION

Quantum Technologies: When Is It Too Late?

At present, the field of quantum technologies is at a stage of development when, in addition to important advances in the field of scientific development and research, the first commercial products are also beginning to appear. However, there is still an opinio…

Anton Gugla
QApp

Pavel Vorobyov
QRate, QSpace

Pavel Korostelev
"Security Code"

Hyperion Hall

LOOK ▷

phd 2

ПРОГРАММА

POSITIVE LABS REPORT

Auto Root from the Celestial Empire

Cars are becoming smart. Sometimes even too much. Many modern cars have Bluetooth and Wi-Fi. The operating systems that users interact with in cars are quite familiar. Basically, all of them are based on Android. All this splendor appeared in modern cars relatively…

Artem Kulakov
Positive Technologies

Positive Labs

WITHOUT BROADCAST

05:25–06:25

CYBERBEZ: WHERE TO START DISCUSSION

How to Protect the Core Business Communication Channel

Let's talk about methods and strategies for ensuring email security as the main means of communication in modern organizations. Participants will discuss current threats and challenges and share best practices and innovative approaches to protection. Key question…

Yaroslav Babin
Positive Technologies

Vadim Shelest
Wildberries

Dmitry Tsarev
BI. ZONE

Sergey Iskhakov
PSB

Vladimir Dubrovin
VK

Nikolay Buyanov
Tinkoff

Main Stage "Galaxy"

LOOK ▷

05:30–06:15

EVASION DISCUSSION

How Many Problems Does Close Surveillance Isolation Bring to a Hacker, or Protection Technologies and Sandbox Circumvention Techniques

Technical experts of cybersecurity products and solutions will face off: they will analyze

Alexey Kolesnikov — Positive Technologies
Fyodor Skvortsov — BI. ZONE

Gravity Hall

LOOK ▷

05:30–06:15

AI TRACK REPORT

Categorizing cyber threats using artificial intelligence and graph data analysis

This research focuses on developing a comprehensive platform for analyzing and understanding cyberattacks that combines machine learning, natural language processing (NLP), and graph analysis techniques. The result of the study should be a detailed…

Yevonnael Andrew
Swiss German University

Orion Hall

LOOK ▷

06:00–07:00

OFFENSE REPORT

CI/CD unchained: looking for a weak link in the development infrastructure

The development infrastructure in large companies consists of a large number of components and even more integrations between them. And these integrations can contain many different security issues. The report will consider serious security problems encountered by the…

Pavel Sorokin
Singleton Security

Ganymede Hall

LOOK ▷

GENERAL DEVELOPMENT REPORT

You don't need queues

In backend development, queues are often used as a silver bullet that solves all the problems of failover handling, load growth, and service scaling. The speaker will talk about the reverse side of queues and the boundaries of their application. We will conside…

Vitaliy Levchenko
Wildberries

Deimos Hall

LOOK ▷

06:00–07:00

SECURE DEVELOPMENT REPORT

SLSA: Assessing the effectiveness of supply chain security in the cloud

We will tell you how to build a pipeline for secure development in a cloud infrastructure. We will talk about the importance of the SLSA framework for DevSecOps and what tools can be used to protect the supply chain, show an example of a secure development pipeline in…

Maria Zubchenko
Yandex Cloud

Phobos Hall

LOOK ▷

06:00–07:00

DEFENSE REPORT

Threat intelligence sharing platform with hacker traps

The project is to create a system that collects, categorizes, and disseminates cyber threat data, contributing to the strengthening of cybersecurity. With the help of hacker traps, the platform monitors and analyzes various actions of attackers, providing a…

Чарльз Лим

Зал «Титан»

СМОТРЕТЬ ▷

06:00–06:30

ПАРТНЕРСКИЙ ДОКЛАД

SIEM: как мы на нем собаку съели

Вендор расскажет, с какими сложностями сталкиваются пользователи при эксплуатации SIEM. Слушатели смогут принять участие в опросах и оценить эффективность мер для решения этих проблем.

Павел Клоц
R-Vision

Зал «Гиперион»

СМОТРЕТЬ ▷

06:00–06:45

ШКОЛА CISO ДОКЛАД

Жизненный цикл CISO

В докладе будут рассмотрены этапы жизненного цикла руководителя ИБ в организации – от начала переговоров о приеме на работу до увольнения по различным обстоятельствам. Обязательно с примерами из личного опыта спикера.

Алексей Волков
Expert

Зал «Метеор»

LOOK ▷

06:00–07:00

POSITIVE LABS REPORT

In his presentation, the speaker will share many years of experience in fuzzing to find vulnerabilities and try to organize a live discussion with the audience.

Alexander Popov
Positive Technologies

Positive Labs

WITHOUT BROADCAST

06:15–07:00

AI TRACK REPORT

Mythbusters: Three Experiments in Biometrics

In everyday life, we are surrounded by many legends, internet rumors and myths. And one of the most intriguing areas regarding our security and technology is biometrics. Sometimes myths deal with important technical details, sometimes these myths are so absurd that the…

Natalia Bessonova
JSC "Center for Biometric Technologies"

Orion Hall

LOOK ▷

06:30–07:00

AFFILIATE REPORT

YADRO - Russian hardware platforms. Product Creation from PCB to Microcode

A representative of the Russian engineering company YADRO will share his experience in the development and production of a reliable and secure infrastructure platform that meets the needs of the market and customers, meets the tasks of information security and regulatory…

Anton Pechenev
YADRO

Hyperion Hall

LOOK ▷

06:35–07:05

CYBERBEZ: WHERE TO START REPORT

About sand castles, comfort boxes and other delights of small companies

Let's talk about the points that you need to pay attention to before there are many disparate systems. What can be useful when a small company is already moving from manual to process management, when there is already an awareness that something needs to be done…

Anastasia Gainetdinova
Whoosh

Main Stage "Galaxy"

LOOK ▷

07:00–08:00

DEFENSE REPORT

Identity-Aware Proxy: How to Take a Significant Step Towards Zero Trust

In recent years, remote work has become very popular and in demand. This has led to more frequent use of VPNs in organizations – more and more employees can connect to the company's network from anywhere in the world. Even if the network is properly segmented…

Sargis Nanyan
Ozon Tech

Titan Hall

LOOK ▷

07:00–08:00

OFFENSE REPORT

Memory Regions, or How I Loaded the Shellcode in the Wrong Place

More and more information about in-memory code execution, shellcode injection, and BYOI methods is flashing on the Internet. It may seem that almost all antivirus problems can be solved if you find a way to put the load in memory. Indeed, it used to be a great panacea…

Mikhail Zhmailo
CICADA8 (MTS Innovation Center)

Ganymede Hall

LOOK ▷

07:00–08:00

GENERAL DEVELOPMENT REPORT

Fuzzing: Why Your API Should Suffer

We will tell you how to painlessly conduct fuzzing testing of web applications with only the API specification (but this is not accurate). We will discuss existing solutions, the choice of tools, and preparation for testing. Let's talk about problem solving and…

Vladimir Isabekov
Swordfish Security

Artem Muradyan
Swordfish Security

Deimos Hall

LOOK ▷

07:00–08:00

SECURE DEVELOPMENT ДОКЛАД

Why protect public cloud deployment pipelines and how to do it?

Let's talk about utilities and approaches to implementing the protection of public cloud deployment pipelines. Let's consider examples of cloud Terraform providers for domestic clouds, talk about the advantages and disadvantages of Checkov and OPA. Let's consider an…

Николай Панченко
«Тинькофф»

Рами Мулейс
Yandex Cloud

Зал «Фобос»

СМОТРЕТЬ ▷

07:00–07:45

Применение LLM в информационной безопасности: путь к AI-ассистенту

Одним из перспективных направлений в области информационной безопасности является использование больших языковых моделей (large language model, LLM). LLM – это генеративные модели, которые обучены на огромных объемах текстовых данных и имеют более миллиарда…

Артем Проничев
Positive Technologies

Александр Мамылов
Positive Technologies

Зал «Орион»

СМОТРЕТЬ ▷

07:00–07:30

ШКОЛА CISO ДОКЛАД

От стажера до CISO в крупной компании за шесть лет: что нужно знать и уметь молодому руководителю

Какие знания и умения должны быть у руководителя отдела ИБ? Что делать в первые месяцы в новой роли? Как соответствовать ожиданиям менеджмента? Ответами на эти и другие вопросы спикер поделится в презентации.

Vladislav Ivanov
H&N (formerly Danone)

Meteor Hall

LOOK ▷

07:00–07:30

AFFILIATE REPORT

How to Implement SOAR

At Security Vision, we implement dozens of SOAR solutions every year on a wide variety of industry infrastructures, taking into account the specifics of specific customers. But, as a rule, everyone has the same problems and pains during implementation – the rake is laid…

Evgeny Bisovko

Hyperion Hall

LOOK ▷

07:00–08:00

POP SCIENCE

DJ Andrew Addison

Sputnik Scene

LOOK ▷

07:15–08:15

CYBERBEZ: WHERE TO START DISCUSSION

How Web Attacks Can Bury Your Business

Let's talk about the protection of small and medium-sized businesses from attacks on web resources. Topics for discussion: Public attacks on small and medium-sized companies: how they happened, what were the consequences for business, how to protect yourself from them…

Denis Prokhorchik	Dmitry Smirnov	Anton Gretsky	Nikita Yudin
Positive Technologies	"Sports lotteries"	ActiveCloud	Positive Technologies

Dmitry Belyanin
StormWall

Main Stage "Galaxy"

LOOK ▷

07:30–08:15

EVASION DISCUSSION

Can a Hacker Fool the Heart of a SOC, or Security Technologies and SIEM Bypass Techniques

Technical experts of cybersecurity products and solutions will face off: they will analyze

Ekaterina Nikulina — Positive Technologies
Vladislav Lashkin — Solar

Gravity Hall

LOOK ▷

07:30–08:00

AFFILIATE REPORT

Ecosystems, feature factories and tech debt: how to be productive

The demand for information security products has increased significantly. Two fundamentally different approaches have formed in the market: to create a single-vendor ecosystem or to provide interfaces for integration with third-party solutions. What are…

Sergey Nikitin
Gazinformservice

Hyperion Hall

LOOK ▷

07:45–08:30

AI TRACK REPORT

MTS protects against phone scammers

During the talk, an anti-fraud system based on modern GNN and LLM models will be considered. It is designed to identify bank customers who are subject to telephone fraud.

Nikita Zelinsky
MTS

Orion Hall

LOOK ▷

CISO's Career Path: From Dawn to Dusk

Let's talk about the career development of the Chief Information Security Officer (CISO). Participants will discuss the key stages and challenges that CISOs face at different stages of their careers, as well as best practices and strategies for success in this…

Oleg Kuzmin	Evgeny Voloshin	Lev Shumsky	Alexey Volkov
Independent Expert	BI. ZONE	Yandex Cloud	Expert

Meteor Hall

LOOK ▷

08:00–09:00

DEFENSE ДОКЛАД

RCE vulnerability in Managed ClickHouse through the eyes of a SOC specialist in Yandex Cloud

Доклад посвящен обнаружению RCE-уязвимости в СУБД ClickHouse с помощью таких инструментов, как AppArmor и Osquery. Спикер также расскажет о том, как можно обнаружить дальнейшую эксплуатацию уязвимости.

Вадим Осипов	Дмитрий Руссак
Yandex Cloud	Yandex Cloud

Зал «Титан»

СМОТРЕТЬ ▷

08:00–09:00

OFFENSE ДОКЛАД

Вам письмо: старые новые атаки на почту

Доклад о том, как старые неразрешенные вопросы реализации и клеймо «легаси» повлияли на уязвимость современной электронной почты к внедрению кода. Разберем особенности работы почты и основных почтовых протоколов, рассмотрим виды внедрения кода в почтовую…

Елизавета Тишина	Всеволод Кокорин

Зал «Ганимед»

СМОТРЕТЬ ▷

08:00–09:00

GENERAL DEVELOPMENT REPORT

How we fuzzed the OS kernel with syzkaller and what came out of it

The story is about how we spent several months figuring out the features of the most popular operating system fuzzer syzkaller in order to teach it how to find bugs in the kernel of the microkernel operating system KasperskyOS. This is how we learned a lot abou…

Maria Nedyak
Kaspersky Lab

Deimos Hall

LOOK ▷

08:00–09:00

SECURE DEVELOPMENT REPORT

How secure development works in a cloud provider

For companies operating in the B2B sector, the issue of security is acute: choosing a secure partner – a technology supplier – is one of the main focuses of attention. Nowadays, certifications and compliance with requirements are no longer enough, you need…

Nikita Gergel
Yandex Cloud

Phobos Hall

LOOK ▷

08:00–09:00

POSITIVE LABS REPORT

The researcher set himself the goal not to detect any vulnerabilities, but to make quite standard protection technologies work. In the absence of documentation, this is a rather non-trivial task. The report contains a detailed description of all the stages of this…

Nikita Firsov
Positive Technologies

Positive Labs

WITHOUT BROADCAST

08:00–08:30

POP SCIENCE INTERVIEW

Honestly about technology. Interviews with representatives of cybersecurity and IT. Black Questions to White Hats

Popular presenter and blogger Kirill Didenok talks with IT representatives.

Konstantin Polishin
Positive Technologies

Kirill Didenok
DIDENOK TEAM

Sputnik Scene

LOOK

08:00–08:30

AFFILIATE REPORT

Scenarios for using UEBA to detect atypical attacks

The speaker will talk about practical experience in covering the blind spots of SIEM systems using automatically built models of the behavior of infrastructure facilities (UEBA system). The speaker will pay special attention to non-typical cases related to the…

Alexey Peshik
Security Vision

Hyperion Hall

08:25–09:25

CYBERBEZ: WHERE TO START DISCUSSION

Change People or Change People: How Training Programs Enable You to Achieve a Strategic Business Goal

The most important factors in ensuring cybersecurity are the interest of top management and the development of employees at all levels: from those who directly ensure the security of the infrastructure, are the customer for this activity, to ordinary employees…

Ekaterina Barabanova, Rostelecom
Yulia Danchina, Positive Technologies
Dmitry Zubtsov, SberUniversity
Aidar Guzairov, Innostage
Anastasia Fedorova, K2 Cybersecurity
Natalia Voevodina, Independent Expert

Main Stage "Galaxy"

LOOK ▷

08:30–09:15

AI TRACK REPORT

Reduce SOC analyst workload

Report on the development and implementation of a solution that helps optimize the work of analysts and reduce alert fatigue, as well as on the problems and pitfalls in the implementation of this solution.

Nikolay Prudkovsky
BI. ZONE

Orion Hall

LOOK ▷

08:30–09:15

EVASION DISCUSSION

When there is no hope left: meta-products on guard if a hacker has passed

Technical experts of cybersecurity products and solutions will face off: they will analyze in detail the protection technologies that are used in SIEM, IDS, EDR, sandbox products, as well as in meta-products.

Yulia Fomina
Positive Technologies

Gravity Hall

LOOK ▷

08:30–08:55

POP SCIENCE INTERVIEW

How a girl can succeed in IT and cybersecurity

Popular presenter and blogger Kirill Didenok talks with IT representatives.

Svetlana Gazizova
Positive Technologies

Kirill Didenok
DIDENOK TEAM

Sputnik Scene

LOOK ▷

08:30–09:00

AFFILIATE REPORT

Why AI is triumphant in all areas except information security

The talk will consider the main problems that ML and AI methods successfully solve today, as well as the methods that are in the arsenal of AI engineers. Let's talk about the mathematical essence of the problem and the method (without unnecessary immersion in…

Nikolay Domukhovsky
UCSB

Hyperion Hall

LOOK ▷

08:45–09:15

CISO SCHOOL REPORT

Life after the incident

A typical goal of a CISO is to prevent the negative impact of cyber threats on the organization, which is undoubtedly appreciated by top management. But when a real incident occurs, which entails catastrophic consequences and other types of damage, sooner or late…

Vladimir Tashkeev
Infosecurity

Meteor Hall

LOOK ▷

08:55–09:20

POP SCIENCE INTERVIEW

Scooter or flying saucer: what will be the transport of the future

Popular presenter and blogger Kirill Didenok talks with IT representatives.

Yegor Bayandin
CIO and co-founder of the kicksharing service Whoosh

Kirill Didenok
DIDENOK TEAM

Sputnik Scene

LOOK ▷

09:00–10:00

DEFENSE REPORT

What was yours is ours: what useful things can be found on the servers of intruders

Specialists of the DFIR department have to not only reconstruct information security incidents, but also work with images of the attackers' servers. The proposed talk will present a methodology for their analysis, as well as prepare scripts for converting logs…

Titan Hall

LOOK ▷

09:00–10:00

GENERAL DEVELOPMENT REPORT

Making noise: Implementing fuzzing

We will talk about the implementation of fuzzing from scratch into a complex software product that has been developed for several years, from a practical point of view. Students will be provided with information about this type of testing, information about…

Alexander Zanegin
Positive Technologies

Deimos Hall

LOOK ▷

09:00–10:00

SECURE DEVELOPMENT REPORT

You've implemented security scanners in your pipelines — that's it?

After conducting a sufficient number of technical interviews, the speaker came to the conclusion that most beginners (or not so beginners) DevSecOps specialists do not understand what should really be taken into account when implementing scanners in…

Maxim Korovenkov
SberMarket

Phobos Hall

LOOK ▷

09:00–10:00

Our research team evaluated the safety of a popular children's educational robot based on artificial intelligence. We were able to build a chain of attacks that allowed us to breach its security and gain unauthorized remote access to it without noticing. In this…

Alexander Kozlov
Kaspersky Lab

Nikolay Frolov
Kaspersky Lab

Ganymede Hall

LOOK ▷

09:00–09:30

AFFILIATE REPORT

Difficulties in choosing a Russian NGFW

During the talk, we will discuss: The situation in the NGFW market in 2023 and 2024. What difficulties do our customers face? Minimum number of must-have features. How to conduct a "pilot". How not to suffer when choosing a solution.

Ivan Chernov
UserGate

Hyperion Hall

LOOK ▷

09:00–10:00

POSITIVE LABS REPORT

Nutrition attacks, or Glitch in real life

During the talk, the authors will share their real experience of power supply attacks on microcontrollers, as well as tell how the most popular of them are detected. Most of the talk will be devoted to stories and examples from life, and, of course, the rake that you…

Yuri Vasin
Positive Technologies

Pavel Ivannikov
Positive Technologies

Positive Labs

WITHOUT BROADCAST

09:15–10:00

AI TRACK ДОКЛАД

Chatbot Attacks: Indirect Prompt Injection in a Real Application

Modern chatbots, such as ChatGPT, Microsoft Copilot, Google Gemini, are complex applications with a non-trivial internal structure, where the interaction of components is coordinated by a large language model (LLM). This complexity, combined with the…

Владислав Тушканов
«Лаборатория Касперского»

Зал «Орион»

СМОТРЕТЬ ▷

09:20–09:45

НАУЧПОП ИНТЕРВЬЮ

Кибербуллинг

Популярный ведущий и блогер Кирилл Диденок беседует с представителями ИТ.

Сцена «Спутник»

СМОТРЕТЬ ▷

09:30–10:00

EVASION ДИСКУССИЯ

Итоги дискуссий

Противостояние технических экспертов продуктов и решений кибербезопасности: они подробно разберут технологии защиты, которые применяются в продуктах классов SIEM, IDS, EDR, sandbox, а также в метапродуктах.

Alexey Vishnyakov
Positive Technologies

Gravity Hall

LOOK ▷

09:30–10:15

CISO SCHOOL DISCUSSION

Should the CISO be ashamed of missed incidents?

The discussion will touch on the issue of the Chief Information Security Officer's (CISO) sense of responsibility and shame in the event of cyber incidents in the organization. Participants will discuss whether CISOs should feel ashamed of incidents, how to properly…

Ilya Zuev	Artem Sychev	Oleg Kuzmin	Sergey Demidov	Alexey Volkov
MTS Bank	RT-Information Security	Independent Expert	Moscow Exchange	Expert

Ilya Borisov
VK

Meteor Hall

LOOK ▷

Beyond the password: new horizons in security awareness

In this talk, we will focus on the importance of developing and implementing programs to raise awareness of information security issues in modern organizations. We will discuss how such initiatives can reduce the risks associated with the human factor, and outline…

Anastasia Petrova
Biocad

Main Stage "Galaxy"

LOOK ▷

09:45–10:10

POP SCIENCE INTERVIEW

Burn IT out: Why IT professionals burn out so quickly

Popular presenter and blogger Kirill Didenok talks with IT representatives.

Almira Fatikhova
Innostage

Kirill Didenok
DIDENOK TEAM

Sputnik Scene

LOOK ▷

10:00–11:00

DEFENSE REPORT

Trusting is good, trusting too much is dangerous, or Trusted relationship attacks

The speaker will talk about attacks based on trust-based relationships between organizations, or trusted relationship attacks. You will learn how these attacks are carried out, what tactics, techniques, and procedures (TTPs) attackers use, and how you…

Alina Sukhanova
Kaspersky Lab

Titan Hall

LOOK ▷

10:00–11:00

OFFENSE REPORT

Bug Bounty: A View from the Other Side

A view from the other side is what a bug bounty vendor sees, not a hacker. The speaker will tell why businesses need bug bounty programs and what to do at the start so that it is not excruciatingly painful for either the company or the hacker later. Let's talk abou…

Pyotr Uvarov
VK

Ganymede Hall

LOOK ▷

10:00–11:00

SECURE DEVELOPMENT REPORT

The X-Files: The convenience of (safe) security

The report presents a study of popular secret vaults, attack vectors for secret vaults, and measures to ensure their security.

Victor Kuznetsov
Bastion

Nina Stepovik
Bastion

Phobos Hall

LOOK ▷

10:00–10:45

AI TRACK REPORT

Prediction of vulnerabilities in the configurations of information system devices

Attack graphs have long been a popular method for modeling multi-step attacks. They are used to assess the likelihood of network hosts being compromised and identify attack paths with the highest probability and risk. Typically, this analysis is based on vulnerability…

Dmitry Levshun
SPC RAS

Orion Hall

LOOK ▷

10:00–11:00

GENERAL DEVELOPMENT REPORT

API-First Security Strategy

The report discusses the main methods of API protection as one of the key components of modern infrastructure. The speaker will talk about the dangers of high visibility, the increase in the number of attacks on APIs, as well as talk about encryption and access…

Лука Сафонов
Weblock

Зал «Деймос»

СМОТРЕТЬ ▷

10:10–10:35

Популярный ведущий и блогер Кирилл Диденок беседует с представителями ИТ.

Жан Просянов
Главный редактор, генеральный директор «Кино-Театр.Ру», директор по развитию развитию CHILL, продюсер

Кирилл Диденок
DIDENOK TEAM

Сцена «Спутник»

СМОТРЕТЬ ▷

10:10–10:25

КИБЕРБЕЗ: С ЧЕГО НАЧАТЬ ДОКЛАД

Отрицание, оправдание, штраф: обзор административных дел за утечки персональных данных

На основе анализа судебных решений по делам об утечках персональных данных за 2022–2023 годы спикер расскажет, как регулятор узнает об утечках, из-за чего они происходят, а также как организации (безуспешно) пытаются избежать наказания.

Oleg Shakirov
Independent Researcher

Main Stage "Galaxy"

LOOK ▷

10:30–11:00

CISO SCHOOL REPORT

Chief Information Officer at 25: Ten Years Later

Experience as an information security director. Where to start? What is important? What doesn't matter? Content addressed to oneself 10 years ago.

Vyacheslav Grebnev
Siberian Cement Holding Company JSC

LOOK ▷

10:35–11:35

CYBERBEZ: WHERE TO START DISCUSSION

What needs to change to reduce leaks

The discussion will bring together representatives of companies that process personal data, developers of data protection tools and standards, as well as representatives of services that track information leaks. Participants will discuss the current situation,…

Gleb Marchenko	Anna Kirsanova	Victor Ryzhkov	Vyacheslav Kasimov
Tinkoff	Garda Group of Companies	Positive Technologies	Credit Bank of Moscow

Irina Levova
Big Data Association

Main Stage "Galaxy"

LOOK ▷

10:35–11:00

POP SCIENCE INTERVIEW

The Phygital World and Tools for Changing Thinking in It

Popular presenter and blogger Kirill Didenok talks with IT representatives.

Sergey Kalmykov	Kirill Didenok
Cyberdom	DIDENOK TEAM

Sputnik Scene

LOOK ▷

10:45–11:30

AI TRACK REPORT

In this talk, we will dive into the world of speech recognition technology, explore its application in our daily lives, and find out what kind of magic lies at the heart of its functionality. We'll also look at the security risks associated with it and analyze how…

Igor Grebenets
Independent Expert

Timofey Talikin
VK

Orion Hall

LOOK ▷

11:00–12:00

DEFENSE REPORT

Dark promotion: research of pricing, distribution models and promotion methods on shadow resources

Every day, new ads for the sale of malware, database samples, and access to corporate networks appear on shady resources. Often these messages are in demand among attackers attacking Russian companies. In addition to the quality of the content offered, sellers…

Daria Sebyakina
BI. ZONE

Titan Hall

LOOK ▷

11:00–13:00

POP SCIENCE

Model to build. Literary and musical program

Sputnik Scene

LOOK ▷

11:15–12:15

CISO SCHOOL DISCUSSION

The Q&A session invites conference participants to ask questions to experienced CISOs to get useful tips and life hacks on managing cybersecurity in organizations of different forms of ownership, different sizes and industry ties. This is a unique opportunity to…

Ilya Zuev	Evgeny Voloshin	Artem Sychev	Lev Shumsky	Alexey Lukatsky
MTS Bank	BI. ZONE	RT-Information Security	Yandex Cloud	Positive Technologies

Vladislav Ivanov
H&N (formerly Danone)

Meteor Hall

LOOK ▷

11:45–12:30

CYBERBEZ: WHERE TO START REPORT

Digging up archives of leaks from 2020: what else is available and what has not been removed for years

Today, data leaks are one of the most frequent news in the world of information security. But the journey from a problem in the service being used or a human error to a successful attack or the publication of news about a data breach is often longer than it seems. How…

Alexander Kolchanov
PSB

Main Stage "Galaxy"

LOOK ▷

13:00–13:15

POP SCIENCE

Day Finale

Sputnik Scene

WITHOUT BROADCAST

VK TG YTB

RU <> EN