May 18

🟠 Technical talk 🟣 Threat research ⚪ Development 🟢 AI Track 🔴 Fast track 🟡 Investor Day 🔵 Business talk

	Valdai Hall	Seliger Hall	Press hall	The Standoff hall	Amphitheater	
09:00	Registration					
10:00	Opening ceremony in The Standoff hall				**Cyberplenary** A tectonic shift of the Russian cybersecurity industry	10:00
10:30		Opening. POSIDev organizers' welcome speech **Vladimir Kochetkov**		**Contests:** • IDS Bypass • Payment Village • AI Track • Cyberart at risk		10:30
11:00	How to detect 95% of attacks covering 5% of threat actors' techniques **Oleg Skulkin**	Secure development in your IDE **Andrey Lyadusov**	Collaborative computing technologies. How companies can share data without actually sharing it **Petr Emelyanov**		**Panel discussion** Cybersecurity in the era of digital transformation	11:00
12:00	Modern rootkits and methods of their detection **Alexey Vishnyakov**	Analysis of the client JavaScript code for detecting HTTP endpoints **Daniil Sigalov**	Choosing an ML algorithm to search for anomalies in network traffic **Valentina Pugacheva**		**Panel discussion** Towards a technological independence	12:00
13:00	Another way attackers can use ACLs in AD **Pavel Shlyundin**	Swordfish Security's secure development framework **Svetlana Gazizova**	Detection of anomalies and signs of attacks in network traffic using the TCN autoencoder **Nikolay Zmitrovich**		**Section** The ploy won't work: protection against supply chain attacks	13:00
14:00	Zero days and sanctions: how to report a vulnerability to a vendor who does not want to hear about it **Vadim Solovyev**	Self-assessment of the AppSec process maturity **Ilya Sharov**			**Round table and talks by experts** A daily routine of IT specialists under the cyberstorm	14:00
15:00	Phishing on official websites: how victims hand over their passwords to hackers on legitimate resources **Aleksandr Kolchanov**	Security champions: a voice of security in a team **Pavel Kulikov**	Big data (in)security **Vadim Shelest**		**Partners' talks** • Assessing the maturity of SOC processes based on MITRE ATT&CK **Danila Lutsiv, Security Vision** • Sales considering the real needs of the customer **Alexander Paramonov, MONT**	15:00
16:00	Qualcomm BootROM: extraction, investigation, and exploitation of vulnerabilities **Dmitry Artamonov**	A new approach to automated generation of exploits for major web applications **Daniil Sadyrin**	The use of GAN models to generate attacks **Nikolay Lyfenko**		**Round table** Development of open-source security solutions for the corporate sector	16:00
17:00	How Zhui and Dindin spent their last year in Russia **Igor Zalevsky**		Testing biometric vitality detection algorithms for the Unified Biometric System **Natalya Bessonova**		**Investment track** Stock market reloaded. New opportunities for technology companies	17:00
18:00	MaxPatrol SIEM health check: we know your SIEM can do more **Vladimir Voloshin**					
18:30						
19:00					**Investment track** Positive Technologies presentation for investors	18:30
19:30						19:30

May 19

● Technical talk ● Threat research ● Development ● AI Track ● Fast track ● Investor Day ● Business talk

	Valdai Hall	Seliger Hall	Press hall	Hall A	Amphitheater	
09:00	Registration					**09:00**
10:00	Hunting for modern attacks on the Active Directory infrastructure **Teymur Kheirkhabarov**	Supply chain attacks **Eugeny Polonskiy**			**Partners' talks:** • Investigation of information security incidents caused by employees: how to detect and catch **Daniil Borislavsky, Atom Security**	**10:00**
11:00	Preprocessing is our everything **Anton Dorfman**	Software compositional analysis: current challenges **Alexey Smirnov**		Bypassing WAF signatures **Roman Romanov**		**11:00**
11:20				JavaScript in PDF **Anastasiya Pryadko**	• How to build a SOC by effectively combining SOAR and SIEM **Anzhelika Svoikina, Security Vision**	**11:20**
11:40				API keys storage **Ilsaf Nabiullin**	• K8S Hardening. (Non)obvious settings **Anton Gavrilov, Jet Infosystems**	**11:40**
12:00	A new face of OSINT. 20 useful ways to search information in the digital age **Andrey Masalovich**	Developing the best Linux kernel livepatch **Timur Chernykh**		A hardware solution to protect against USB attacks **Andrey Biryukov**	• On-premise SOC: how to build it without pain **Andrey Proshin, Rostelecom-Solar**	**12:00**
12:20				CVE-2021-40444: why it is important **Alexander Goncharov**	• Modern data center: what is it like? **Airat Mustafin, Liberum Navitas**	**12:20**
12:40				Domain admin blitzkrieg **Anton Bochkarev**	• Building an incident management process under the MSSP model **Roman Ovchinnikov, Security Vision**	**12:40**
13:00	A Kernel hacker meets Fuchsia OS **Alexander Popov**	Vulnerable Allsafe mobile application through the eyes of a source code analyst with examples for beginners **Tatyana Kutsovol**		Detection of phishing domain names and typosquatting by using a string similarity metric **Sergey Kolpinsky**	**Section** A big brouhaha over data breaches: how to minimize the risks of attacks	**13:00**
13:20				Correlation of events from information security sensors **Oleg Guzev**		**13:20**
13:40				Methods to access the Tuxera Reliance Nitro embedded file system and the FlashFX Tera flash memory manager of industrial devices **Sergey Vlasov**		**13:40**
14:00	How to not stop trusting a root of trust **Anton Belousov**	Security games people play **Alexey Babenko**		Reverse engineering of secure OS (TEE) using the AMD PSP TEE **Bulat Zagartdinov**	**Section: controversial topics** My friend once told me a story... or How to get your infosec article on the front page and not to mess it up	**14:00**
14:20				Methodology for assessing the risks of successful social engineering attacks against companies **Yuriy Drugach**		**14:20**
14:40				How to detect and counter backdoor attacks on neural networks **Artem Menisov**		**14:40**
15:00	What TI vendors do not say. IoC scoring **Nikolay Arefiev**	NetworkPolicy, a native Kubernetes firewall **Dmitriy Evdokimov**	**Open Source finals**	The new reality of information security and vulnerability management **Alexander Leonov**	**Section without press representatives** How to work with customers in a new reality	**15:00**
15:20				A new take on deception: catching an internal attacker **Kseniya Zmicherovskaya**		**15:20**
15:40						**15:40**
16:00	50 shades of Cobalt: a retrospective on targeted infrastructure attacks **Danila Lutsiv**	PT Application Inspector vs embedded malware **Dmitry Rassadin**	Tune against the machine. How we made PHDays' official soundtrack **Sergey Gordeychik**		**Round table and talks by experts** Bug bounty through the eyes of developers, users, and hackers	**16:00**
17:00	01111111day **Sergey Golovanov**		**HackerToon finals**			**17:00**
18:00						**18:00**