
phd
Positive
Hack
Days
DIGITAL BEE
MAY 15–16, 2018
FORUM AGENDA
phdays.com

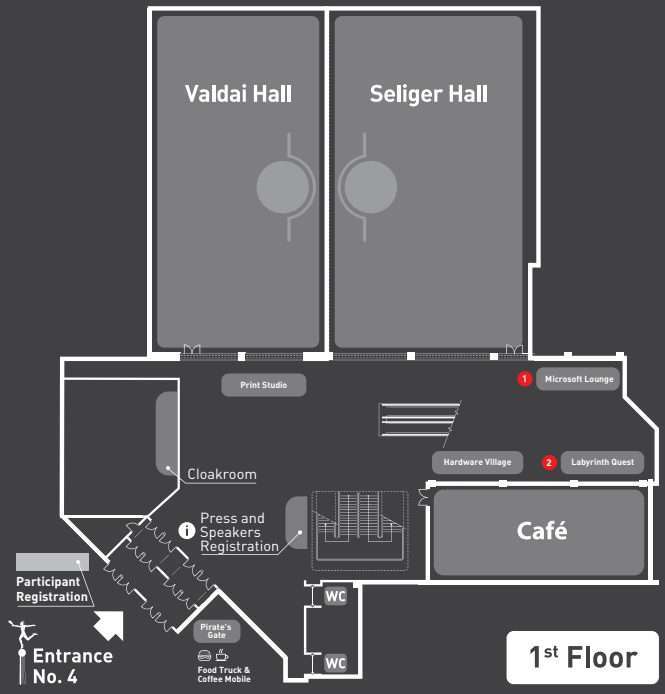
Positive Hack Days

DIGITAL BET

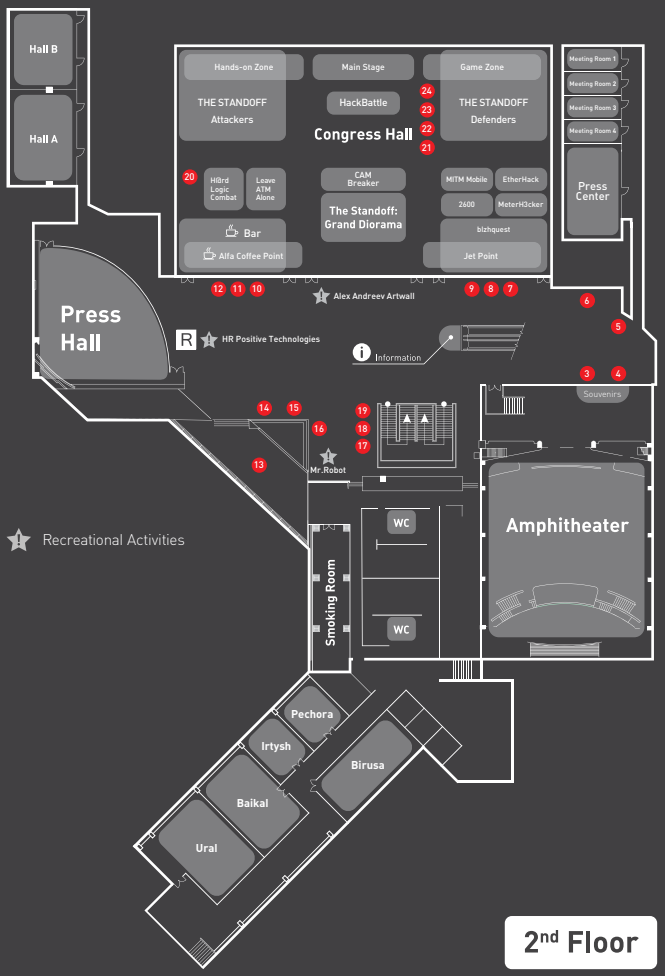
POSITIVE TECHNOLOGIES

Organizer: Positive Technologies

The international forum on practical information security



1st Floor



2nd Floor

WTC MOSCOW

1. Microsoft
2. Rostelecom
3. Axoft
4. IBM
5. Rostelecom
6. R-Vision
7. MOXA
8. Angara & Garda
9. Sberbank
10. Solar Security
11. Group-IB
12. Advantech
13. MONT
14. ICL
15. ARinteg
16. Kaspersky Lab
17. Softline
18. Phoenix Contact
19. Qrator Labs
20. Fizpribor
21. Servionica & Softprom
22. Advanced Monitoring
23. ASP Labs
24. Informzaschita

May 15

Tech · Business · Session · Hands-on lab · Fast track Young School · Development

	Amphitheater	Valdai Hall	Press Hall	Seliger Hall	Hands-on Zone		Hall A	Hall B	Ural
10:00	RE: search	Go ahead and hash without Google **Leonid Yuryev** Build your own cloud shell **German Namestnikov** Information security forensics **Evgeny Tsarev** Shodan for SOC **Andrey Dugin**	Exploiting vulnerabilities 4G Diameter interoperator network **Sergey Mashukov**	Put something on the internet—and get hacked **Noam Rathaus**	10:00	It's the end of security as we know it (and I feel fine!) **Jelle Niemantsverdriet**	Rocket jump from practical security to compliance **Dmitry Desyatkov and Yulia Omelyanenko**		**10:40** PDUG Opening
11:00		Automate that, if you can: How not to lose it while automating SDLC processes **Kirill Samosadny and Andrey Petukhov**	Turning SDR into a GSM mobile phone **Vadim Yanitskiy and Piotr Krysik**	The Shadow Brokers' unpublished implant **Andrey Dolgushev and Alexey Shulmin**	11:00		How to bypass an IDS using netcat and Linux **Kirill Shipulin**		Source code analyzers: how generalizable are they? **Ivan Kochurkin**
11:30	Six angry clients, or What else the information security industry needs **Boris Simis and Maxim Filippov**				11:30				
12:00		Workplace privacy **Mikhail Emeliyannikov**	Neurosurgery for industrial routers, Sarian OS security **Danila Parnishchev**	Decompiler internals: Microcode **Ilfak Guilfanov**	12:00			Handy security tools **Andrey Ivanov, Microsoft**	Myths and legends of secure development **Yury Shabalin**
13:00	CISO 2020: Challenges and opportunities **Eddie Schwartz**		Homebrew information security used in corporate environment **Danil Borodavkin**	IDA Pro processor modules: Nios II **Anton Dorfman**	13:00		Full automatic threat intelligence and incident response **Igor Smetanev and Andrey Chechetkin, R-Vision**		Security of integer types in C++ **Igor Sobinov**
13:30		Security of critical infrastructure: practical aspects **Muslim Medzhlumov, Rostelecom**			13:30				
14:00	Risk management in information security: just hype or an essential management tool? **Sergey Demidov, Roman Chaplygin, Dmitry Gadar, Andrey Pogodin**		Why EINSTEIN was wrong. An overview of state-level cybersecurity initiatives **Sergey Gordeychik**	Telecom security: getting better or worse? **Dmitry Kurbatov**	14:00	SELinux enforcing **Ivan Agarkov**		OSINT: tools and cases **Maxim Avdyunin, Advanced Monitoring**	Theory and practice of vulnerability detection. Why there is no ideal static analyzer? **Yaroslav Alexandrov, Alexander Chernov, Ekaterina Troshina**
14:30					14:30		SOC. Cyberexercise **Private session (Informzaschita)**		
15:00			Lie to me: analyzing hidden C2 channels **Denis Kolegov** Cloud with gaps: How IoT gets hacked **Andrey Birukov** HomeHack: How hackers could spy on you via LG home appliances **Roman Zaikin** Level up your recon: how to make money for sneakers with 700 bug hunters ahead **Igor Lyrchikov** Auditing corporate IT infrastructure **Ivan Piskunov**	Things attacked: Peek into an 18-month IoT honeypot **Tan Kean Siong**	15:00				Static analysis: striving for perfection **Vladimir Kochetkov**
15:30	Security of using biometric technologies **Denis Gorchakov**				15:30				
16:00		Do you need to protect blockchain?		Knocking down the big door, or Breaking authentication and segregation of production and non-production environments **Nahuel Grisolía**	16:00			Sandbox. Pressing questions to anti-APT developers **Nikita Durov, Check Point**	**Roundtable: SAST and its role in SDLC** Representatives from Positive Technologies, SolidLab, Mail.ru, Solar Security, PVS-Studio, Institute for System Programming of the RAS
16:30			Information security in Eastern Europe **Arman Abdrasilov, CAICA**		16:30		Secret tale of bug bounty **Sergey Belov, Mail.ru**		
17:00				Live smart, live longer. On modern intelligent cyberweapon **Andrei Masalovich**	17:00				
17:30		Blockchain security: technology vulnerabilities and a smart contract auditor's instruments **Marat Rakhimov**			17:30				

May 16

Tech · Business · Session · Hands-on lab · Fast track Young School · Development

	Amphitheater	Valdai Hall	Press Hall	Seliger Hall	Hands-on Zone	Hall A	Hall B	Ural
10:00	Digital economy: A threat or a chance? **Dmitry Finogenov**	Security serves evil **Sergey Golovanov**	Generating lists of attacking IP addresses **Evgeny Sagatov** IoT. How to protect it? What threat does it pose? **Andrey Dugin** Adopting a strict CSP **Vadim Gorbachev** Are viruses in Kazakhstan more dangerous? **Oleg Bil**	A spy in the house, or How to scare a cat via UDP **Leonid Krolle and Georgy Zaytsev**	10:00 Build your own threat hunting based on open-source tools **Teimur Kheirkhabarov**		Dynamic binary instrumentation in malware analysis **Artur Pakulov, HackerU**	
11:00		Mobile app security fails and how to survive them **Gustavo Sorondo**	Everything you always wanted to know about regulations and critical infrastructure (but were afraid to ask) **Dmitry Kuznetsov**	Big data in advanced security analytics **Igor Kotenko**	11:00	SAP security source code testing. Vendor approach **Vladislav Klimov, SAP**		LibProtection: 6 months later **Vladimir Kochetkov**
11:30	Antiplenary session **Alexey Kachalin**				11:30			
12:00		**IPv6 security: How did we get here?** **Fernando Gont**	Cryptographical algorithms for strengthening blockchains **Sergey Krendelev**	Secure cloud: what are the rules of the game? **Lev Shumsky (independent expert) and Andrey Akinin (Web Control)**	12:00	Full automatic threat intelligence and incident response **Igor Smetanev and Andrey Chechetkin, R-Vision**	New tendencies in information security **Grigory Galkin, MONT**	Security considerations for blockchain consensus algorithms **Evangelos Deirmentzoglou**
13:00	Code attribution in APT attacks **Costin Raiu**	**IP spoofing attacks exterminate the internet** **Evgeniy Bogomazov and Pavel Bragin**	FinSpy: Zero facts given **Sergey Tarasov and Nikita Proshin**		13:00	**Hacking tales from X-Force Red IBM** **Vladan Nikolic**		Predicting random numbers in Ethereum smart contracts **Arseny Reutov**
14:00	Securing the financial sector **Alexey Kachalin, Sberbank**	Vulnerability databases: extracting metals from ores **Alexander Leonov** Vulnerability management in a large infrastructure **Mikhail Parfenov** Gathering scanners under one roof **Mikhail Aksenov** To SIEM or not to SIEM **Emil Altynbaev** Attacks against and using ML/AI **Alexey Sizov and Evgeny Kolesnikov**	Industry 4.0: Unarmed march into the future? **Roman Krasnov, Positive Technologies**	Smart car forensics and vehicle weaponization **Stefan Tanase and Gabriel Cirlig**	14:00 Catching malware with custom sinkholes **Krassimir Tzvetanov**	New information security technologies **Dmitry Pudov, Angara Technologies Group**	Protection of privileges is the foundation for an integrated security platform **Andrey Akinin, Web Control**	Parameterization and object-oriented approaches: what developers should watch out for **Vladimir Koch**
15:00				Biometrics: Bypassing an enterprise-grade face authentication system **Matthias Deeg**	15:00			Method Hooking on Android **Alexander Guzenko**
15:30	How to make your SOC finally work **Vladimir Bengin**	Artificial security: How much and what kind of intellect is needed to build a security system?	How to launch bug bounty **Igor Bulatenko**		15:30			
16:00				Security of hardware wallets **Sergei Volokitin**	16:00	Forensic techniques against hackers evading the hook **Greg Tworek, Director of CQURE**	Sell your CISO technology in 7 minutes	How to create a fast WAF: building a high-performance system for analyzing network traffic **Mikhail Badin**
16:30			Flaws in telephone banking: client data disclosure and money stealing **Alexander Kolchanov**		16:30			
17:00				The obscure revealed, or Why IPMI can be dangerous **Alexey Morozov**	17:00			


Rostelecom


MCNT
GROUP OF COMPANIES


IBM


МОСКОВСКИЙ ЗАВОД
ФИЗПРИБОР


Microsoft


ICL
СИСТЕМНЫЕ
ТЕХНОЛОГИИ


СБЕРБАНК
Всегда рядом


Альфа-Банк


R-Vision
At the root of your security


Jet


AXXOFT


ANGARA
technologies group


ТАСС
ИНФОРМАЦИОННОЕ
АГЕНТСТВО РОССИИ


ЭЛАНЕР


SecurityLab.ru
by Positive Technologies


AM
ANTI-MALWARE


BIS JOURNAL
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ


COMNEWS
ЛЕТ


МУЖСКОЙ ЖУРНАЛ О ТЕХНОЛОГИЯХ
CHIP


InformationSecurity
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ


DIGITAL
SUBSTATION


RUSCADASEC