











# What The Hack 2018 - Agenda

	 Main Stage	 Red & Blue Teaming (Attack & Defence)	 Cybercrime & Cyberwar powered by WCY WAT	 Risk, audit, privacy & compliance	 Hardware hacking / IoT / ICS powered by WEITI PW	 Banking & Blockchain Security	 Malware	 Lightning Talks
	Aula 107	Aula 328	Aula 329	Aula 040	Aula 101	Aula 102	Aula 103	Aula 105
08:45 - 09:00	<b>Oficjalne otwarcie</b>							
09:00 - 09:20	CyberSec@PL – prawdziwy biznes czy hobby dla geek'ów? Artur Józefiak (Accenture)							
09:30 - 10:10	3 mity CYBERbezpieczeństwa Piotr Konieczny (Niebezpiecznik)	Jak zostać Panem Linuksa wykorzystując najczęstsze błędy konfiguracyjne i programistyczne Paweł Jankowski (Accenture)	Wykrywanie botnetów opartych na sieciach społecznościowych Ryszard Antkiewicz, Hubert Ostap (WCY WAT)	Jak ograniczyć ryzyko i zapewnić zgodność w czasie współpracy z dostawcami Jan Anisimowicz (AdaptiveGRC)	Rola sprzętu w cyberbezpieczeństwie Mariusz Rawski (Instytut Telekomunikacji, WEITI, Politechnika Warszawska)	Narzędzia analizy i wnioskowania stosowane w procesie identyfikacji i rozpoznawania schematów prania brudnych pieniędzy Piotr Stapor, Marcin Chmielewski (WCY WAT)	Malware - analiza dynamiczna złośliwego oprogramowania Marcin Strzałek (KPMG)	Lightning Talks: Fuckups, Use cases, How to get into security
10:25 - 11:05	Nie znam się na bezpieczeństwie Adam Haertle (Zaufana Trzecia Strona)	3xT: Threat Hunting, Threat Actor, Threat Intelligence ... czy wszyscy wiedzą o czym mówią Ireneusz Tarnowski	OSINT - techniki, narzędzia, zakres wykorzystania. Czyli 10 twarzy researchu. Monika Sadlok (XCaliber)	Analiza ryzyka w IT - jak tego nie robić Mateusz Borowski (Elit Partner)	Co mi lata w powietrzu w domu. Reverse engineering domowych urządzeń radiowych na przykładzie stacji pogodowej Marcin Jurczuk (Netia)	Praktyczne zastosowanie technologii blockchain - Trwały Nośnik Robert Przychodzień (Accenture)	Kiedy koń kwacze jak kaczką, czyli wprowadzenie do podobieństwa malware'u i czemu ma to znaczenie Maciej Kotowicz (MalwareLab.pl / Kaspersky GREAT)	# 15 minutowe wystąpienia  # Możliwość zgłoszenia wypowiedzi w trakcie konferencji, wpisując proponowany temat na rollupie przed salą
11:20 - 12:00	Rekonesans sieciowy na żywo Michał Sajdak (Sekurak)	Zapobieganie czy Reakcja na Incydent w typowej polskiej firmie. Tomasz Wodziński	Czym zajmuje się znany APT? Ireneusz Parafjańczuk (Team Cymru Inc)	Dyrektywa NIS - obciążenie czy szansa dla jednostek bezpieczeństwa Daniel Dyszlewski, Karol Chwastowski (Accenture)	Monitorowanie systemu TETRA za pomocą Telive Jacek Lipkowski (Pekao Financial Services)	Wielowarstwowe bezpieczeństwo w bankowości Grzegorz Sowa, Rafał Gołębowski (BNP Paribas)	Zagubione Ogniwo Przemysław Dęba (Orange), Adam Haertle (Zaufana Trzecia Strona)	# Wstęp wolny. Uczestnictwo bez konieczności posiadania rezerwacji miejsca
12:15 - 12:55	New emerging threats for 2019 - best practices to tackle them Sebastian Pawtowski Yoad M. Dvir (Microsoft)	Zero Trust Theorem Andrzej Dyjak (SIGSEGV)	Analiza behawioralna w informatyce śledczej Wojciech Piłszak, Edward Szczyпка (e-Detektywi)	Jak szacować ryzyko, aby spełnić wymagania RODO i KSC Janusz Cendrowski (Asseco)	Czy łatwo włamać się do sprzętu głosem? Artur Janicki (Instytut Telekomunikacji, WEITI, Politechnika Warszawska)	Czy blockchain ma sens w banku - panel dyskusyjny Tomasz Piłat, Cezary Piekarski, Adam Lange, prowadzi Adam Haertle	Co w OT piszczy - bezpieczeństwo sieci technologicznych z perspektywy różnych warstw modelu OSI Adam Bojarski, Dariusz Gońda (CERT ENEA)	
12:55 - 13:40	<b>Lunch (Uczestnicy Standard: Parter w Strefie Food &amp; Drink i na I piętrze / Uczestnicy VIP: Strefa Food &amp; Drink VIP na V piętrze)</b>							
13:40 - 14:20	Attacks of the Industry: A View to the Future of Cybersecurity Paula Januszkiewicz (CQure)	Aliens vs predators Patrik Czezczo Paweł Jacewicz Marcin Ludwizewski (Deloitte)	Przygotowania do cyberwojny – jak i dlaczego państwa budują zespoły hackerów Grzegorz Tworek (freelancer)	Co polskie prawo mówi o wykorzystaniu chmury. Najczęściej zadawane pytania. Michał Jaworski (Microsoft)	Zabezpieczanie infrastruktury krytycznej – lekcje z projektów wdrożeniowych i konsultingowych Michał Paulski, (Accenture)	 Cloud Security	Dlaczego mój komputer działa tak wolno? O potencjalnie niepożądanych aplikacjach stów kilka Kacper Szurek (ESET)	Lightning Talks: Fuckups, Use cases, How to get into security
14:35 - 15:15	Z gumkami przez świat Łukasz Jachowicz	Od serwera Quake do udanego pentestu Mateusz Kocielski (LogicalTrust)	Wyzwania w ściganiu cyberprzestępców Agnieszka Gryszczyńska (UKSiW, Prokuratura Regionalna w Warszawie)	Insecure by design Tomasz Konieczny (Boldare)	Hardware RE: hakujemy firmware zamka hotelowego i piszemy lepszy Michał Leszczyński, Marek Klimowicz (CERT Polska)	Chmura możliwości: bezpieczeństwo dzięki analizie chmurowej i automatyzacji Piotr Łakomski (Microsoft)	(Szybka) analiza dropperów z użyciem Wine Paweł Srokosz (CERT Polska)	# 15 minutowe wystąpienia  # Możliwość zgłoszenia wypowiedzi w trakcie konferencji, wpisując proponowany temat na rollupie przed salą
15:30 - 16:10	Wędkarstwo dla Myśliwych – z phishingiem przygody bezpiecznika Adam Lange	Powershell dla hakerów Paweł Maziarz (Immunity Systems)	Odpowiedź organów ścigania na migrację przestępczości do sieci Internet Dominik Rozdziałowski (Policja)	Catch a secret before an attacker: how to detect hardcoded secrets in big volumes of data Paweł Rzepa (SecuRing)	ICS z punktu widzenia atakującego – ataki na sterowniki PLC Marcin Dudek (PGNiG, NCBJ)	5 wskazówek, jak dostarczać wartość biznesową dzięki cyberbezpieczeństwu Piotr Pawlik (Microsoft)	Techniki Anti-VM Aleksandra Kwiecińska (ComCERT.pl)	# Wstęp wolny. Uczestnictwo bez konieczności posiadania rezerwacji miejsca
16:25 - 17:05	NonPetya i świątynia zagłady! Czego nie nauczyliśmy się wcześniej i czego nie nauczyliśmy nas incydent z NonPetya Tomasz Onyszko (Predica)	Długoterminowe operacje ofensywne Błażej Kantak (Sektor7)	Jak mam bronić kiedy ich jest więcej - panel dyskusyjny o ściganiu cyberprzestępców Agnieszka Gryszczyńska, Dominik Rozdziałowski prowadzi Adam Haertle	Czy przy tysiącu wdrożeń, nasze aplikacje nadal są bezpieczne? Wojciech Lesicki Paweł Czubachowski (Allegra)	IoT/IIoT a bezpieczeństwo aplikacji Michał Kurek (KPMG Cyber Security)	Microsoft Security – newest technology vs. cybercrime Jarostaw Wilk (Comparex Poland)	Wykrywanie fałszywych aplikacji w Google Play Łukasz Cepok	
17:20 - 18:00	Komedia pomyłek – częste porażki i rzadkie sukcesy programów typu crowd-hacking Cezary Piekarski (Bank Millennium)	Wybrane zagadnienia bezpieczeństwa L2 Łukasz Skibniewski (WCY WAT)	Kompresja na krzywych eliptycznych, nowe formuły na alternatywnych modelach krzywych Robert Dryto (Instytut Matematyki i Kryptologii, WCY WAT)	Podstawy Biometrii w bezpieczeństwie systemów Maciej Szymkowski (Wydział Informatyki, Politechnika Białostocka)	Printers hacking Krzysztof Bińkowski (NET COMPUTER)	Passwordless Azure Infrastructure Emil Wasilewski (Bystronic Laser AG)	Powershell - deobfuskacja Dawid Pachowski	
21:00 - ∞	 <b>Afterparty @ 6 Cocktails, Makotowska 57/6. (III piętro), Warszawa</b>							

Wystąpienie nie sprostato Twoim oczekiwaniom? Chcesz wejść do sali pomimo braku wcześniejszej rezerwacji na wybrany slot? Już 5 minut po rozpoczęciu – możesz wejść do auli, niezależnie od rezerwacji, jeśli jeszcze będą wolne miejsca siedzące zgodne z typem Twojego biletu.

Miejsce wydarzenia: Kampus Politechniki Warszawskiej, Budynek Wydziału Matematyki i Nauk Informatycznych (MINI PW), ul. Koszykowa 75, 00-662 Warszawa

