#WTH19 What The H@ck 2019 (Sobota, 14 grudnia) - Agenda

	Main Stage P1 (La Cantina)	Tomorrow Technologies P2L1 (Paryż 1)	Governance Risk and Compliance by ISACA and IIA P2R1 (Londyn 1)	Banking & Finance P2L5 (Warszawa)	Cloud, SysOps, DevOps P2R2 (Londyn 2)	Secure Software Development & Architecture P2L4 (Barcelona)	Red & Blue Teaming (Attack & Defence) P2R5 (Rzym)	Cybercrime & Forensics by WCY WAT P2R3 (Londyn 3)	Mobile & IoT Security P2L3 (Paryż 3)	Hardcore P2R4 (Amsterdam)	Off-Topic P2L2 (Paryż 2)	Round Tables P1RT
	13.12.2019 21:00 - ... PreParty											
08:45 - 09:15	Oficjalne otwarcie											
9:30 - 10:10	APT41 - grupa (trochę) inna niż wszystkie Marcin Siedlarz, Wojciech Ledzion (FireEye)	Privacy by Design Piotr Siemieniak (UPSecure)	Wybrane aspekty dostosowania operatorów usług kluczowych do przepisów UKSC Janusz Cendrowski (Asseco)	Idealne włamanie do bankomatu Adam Rafajeński (Bank Pekao SA)	DevSecOps: Bohater, którego potrzebujemy! Andrzej Dyjak	O tym jak mało jest Sec w Dev(Sec)Ops podczas testów aplikacji Grzegorz Siewruk (Orange)	Zatrute źródło, czyli cache poisoning w praktyce Łukasz Jachowicz (ISEC)	BitLocker z perspektywy informatyki śledczej(ang. BitLocker forensics) Krzysztof Bińkowski (NET COMPUTER)	Analiza wektorów ataków na urzadzenia mobilne Aleksander Goszczycki (RAW)	Uwazaj gdzie piszesz - sym link, oplock Windows exploitation Michał Bazyli (Afine)	Radio: trochę historii, trochę o krótkofalarstwie, jak zacząć i jak to się ma do security Jacek Lipkowski (Pekao Financial Services)	
10:25 - 11:05	Podatności z krypty. Martwe od wielu lat... czy aby na pewno? Michał Sajdak (Sekurak)	IoT - sojusznik czy pogromca cyberbezpieczeństwa i prywatności? Mariola Więckowska (Lex Digital)	Wielowarstwowe zarządzanie bezpieczeństwem informacji Jakub Syta (bezpiecznik.pl)	Getting (serious) things done (in secure way :-) Tomasz Bukowski (Standard Chartered)	Multi i Hybrydowa Chmura – Taktyczne i Praktyczne Bezpieczeństwo Marcin Motylski	Bezpieczeństwo dla paranoików cz. 1 - usługa email Dawid Pachowski	Active Directory - atak i obrona Wojciech Lesicki, Paweł Małkiewicz (Allegro)	Wykorzystanie telemetrii Windows 10 w informatyce śledczej Grzegorz Tworek (Standard Chartered)	Jak zbudować laboratorium do analiz "mobilnego" malware Łukasz Cepok (Santander Bank)	Wykrywanie botnetów na podstawie identyfikacji aktywności grupowej Ryszard Antkiewicz, Hubert Ostap (WCY WAT)	Poligraf. Mitologie i fake news'y Mieszko Dziebłowski	Cyberbezpieczeństwo w telemedycynie Mariusz Chmielewski (WCY WAT)
11:20 - 12:00	Najlepsze (lub najgorsze) porażki w bezpieczeństwie i prywatności (wybór subiektywny) Cezary Piekarski (Standard Chartered), Adam Haertle (Zaufana Trzecia Strona)	RODOBOT, czyli jak sztuczna inteligencja może pomóc wyszukać dane osobowe Jan Anisimowicz (C&F Sp. z o.o.)	Zarządzanie ryzykiem w łańcuchu dostaw Sebastian Burgemejster	Bezpieczeństwo banku - "od środka" Grzegorz Sowa (BNP Paribas)	Attacking AWS: the full cyber kill chain Paweł Rzepa (SecuRing)	Iceberg - zobacz to czego nie widać Kamil Olszówka (T-Systems Poland)	Z nożem kuchennym po konto Administratora Domeny Maciej Michałowski (KPMG)	Wykorzystanie stylometrii i uczenia maszynowego w informatyce śledczej do identyfikacji sprawców przestępstw Wojciech Pilszak, Edward Szczypka (e-Detektywi)	Cotopaxi - zestaw narzędzi do testów bezpieczeństwa IoT Jakub Botwicz (Samsung)	Introduction to side-channel attacks Adam Wysocki (GlobalLogic)	Odzyskiwanie "utraconych" danych. Paradoks informacji Radek Kaczorek (IMMUSEC)	
12:15 - 12:55	Detecting the undetectable in domain environment with Microsoft Security Stack Piotr Pawlik (Microsoft)	Peeking inside your brain. With an interface! Tomasz Mucha (Nokia)	... just one damn thing after another Piotr Filip Sawicki	Jak atakują hakerzy - budu wiedzę, procedury i ćwicz Ireneusz Tarnowski (Santander Bank Polska)	Jak z podejścia DevOps zrobić DevSecOps? Maciej Nogas (Accenture)	Co zrobić aby nie pojawić się na pierwszej stronie gazet? Kluczowe elementy architektury bezpieczeństwa w zmieniającym się otoczeniu zagrożeń Tomasz Sawiak (PwC)	Atakowanie środowisk opartych na Active Directory Patryk Czeczko, Paweł Kordos (Deloitte)	SW czyli o co pytać reagując na incydent bezpieczeństwa. Filip Rejch (T-Mobile)	Bezpieczeństwo sieci 5G - analiza przypadku wieku dziecięcego Sebastian Rutka (Samsung)	not only Process Hollowing Mateusz Garncarek (EY GDS)	Czego informatyka powinna się nauczyć od: kolei, lotnictwa i transportu morskiego Marcin Marciniak (EY)	Jak budować zespoły IT Security? Artur Józefiak (Accenture)
	Przerwa obiadowa											
			Legal & Regulatory		Threat Hunting						Hardware & OT Hacking	
13:40 - 14:20	Explore Adventures in the Underland: Forensic Techniques Against Hackers Evading the Hook Paula Januszkiewicz (CQure)	Kryptografia w przededniu komputera kwantowego Mariusz Jurkiewicz (WCY WAT)	Jak uniknąć odpowiedzialności za incydent ...będąc jego ofiarą Maciej Gawroński	Czy „P" w PSD2 znaczy Problem? – czyli doświadczenia z pola bitwy Wiktor Szymański, Mateusz Nalewajski, Mateusz Szyper	Z wędką na zakupy Dawid Osojca (ComCERT)	XSS w Google, obejście CSP, błąd w Chrome - jak jeden błąd rodzi drugi Michał Bentkowski (Securitum)	Microsoft Exchange na celowniku Paweł Łakomski (Microsoft)	100 gier za 2zł - zjawisko piractwa komputerowego Piotr Zarzycki (mbank)	Obszary (nie)bezpieczeństwa 5G Renata Bilecka (Accenture)	Fuzz testing intepreterów języka JavaScript Wojciech Rauner (Instapage), Marcin Dominiak (Sumo Logic)	Kariera specjalisty ds. Bezpieczeństwa OT - jakie umiejętności są niezbędne, co się przydaje, a o czym trzeba zapomnieć Marcin Majszyk (Accenture)	Czego boją się eksperci ds. bezpieczeństwa Adrian Kapczyński (PTI)
14:35 - 15:15	My kung fu is stronger czyli programiści kontra hakerzy Paweł Maziarz (APT Masterclass)	Kryptografia kwantowa i hakowanie kwantowe Teodor Buchner (Exatel), Michał Jachura	Atak hakerski - co można i trzeba robić od strony prawnej? Radosław Nożykowski, Martyna Czapska (Baker McKenzie)	PSD2 - nowe wyzwania dla cyberbezpieczeństwa Michał Kurek (KPMG)	Obserwacja, werdykt, wyrok: Efektywny Threat Hunting z Cisco Threat Response Mateusz Pastewski (Cisco)	Błędy, o których nie słyszałeś Kacper Szurek (ESET)	Sposoby omijania Web Application Firewall i filtrowania w aplikacjach internetowych Bartłomiej Głośnicki (Accenture)	Atak na Cyber policjanta czy to możliwe? Dominik Rozdzialowski (Policja)	Bezpieczeństwo emulatorów Androida Maciej Miszczyk (Seqred)	Anykernels meet fuzzing Mateusz Kocielski (LogicalTrust)	Cyberbezpieczeństwo w systemach przemysłowych (z perspektywy IT) Jakub Plusczok (ING Tech)	Czy mamy szanse w starciu z hakerami? Jak mądrze inwestować w bezpieczeństwo. Michał Ostrowski
15:30 - 16:10	Securing.Social - poznaj swój elektroniczny "kill chain" Tomasz Onyszko (Predica)	Security i Machine Learning - czyli dlaczego warto testować model przed jego wdrożeniem. Monika Sadlok (X-Caliber), Jakub Plusczok (ING Tech)	Jak hackować legalnie? Ireneusz Piecuch (Kancelaria IMP)	Jak zgodnie z prawem napadać na bank Piotr Szeptyński (ISEC)	Bot or not. That's the question Bartosz Naumowicz (OLX)	Aaa, tego nie przewidzieliśmy - modelowanie zagrożeń w praktyce Jakub Kałużny (SecuRing)	COM to me, baby Błażej Kantak (Sektor7), Łukasz Mikuła (Afine / eLearn Security)	Pranie pieniędzy pochodzących z cyberprzestępczości - studium przypadku Agnieszka Gryszczyńska (UKSW)	Challenges in the Android supply chain analysis Łukasz Siewierski (Google)	Parę sztuczek z Portable Executable, czyli ciekawe rzeczy które można zrobić w Windowsie Michał Leszczyński (CERT), Paweł Srokosz (CERT)	Wykorzystanie emulacji i symbolicznej egzekucji w poszukiwaniu CVE w urządzeniach IoT Grzegorz Wypych (IBM)	Już wkrótce Robert Kosla (Min. Cyfryzacji)
16:25 - 17:05	Biometria behawioralna - przyszłość uwierzytelniania Mateusz Chrobok (Digital Fingerprints)	Bezpieczeństwo europejskich danych w światowej chmurze Marcin Zmaczyński (Aruba Cloud)	Jak stworzyć wewnętrzny zbiór zasad kontrolnych (ang. control framework) - aspekty prawne. Paweł Gruszecki (TML - Gruszecki Law Firm)	Prescriptive Security – manage your enterprise security as if you were driving an autonomous car Maciej Żarski (Atos)	Polowanie na komunikację Command and Control (C2) Bartosz Jerzman (Standard Chartered)	Security code review - lesson learned. Bartosz Różański (7n)	Jak budować zdolności i prowadzić operacje ofensywne "like a pro" - na przykładzie projektów red teaming Marcin Ludwiszewski (Deloitte)	Fraud as service, czyli jak palić i grabić nie mając pojęcia o cardingu? - ewolucja narzędzi używanych do obchodzenia systemów antyfraudowych Marcin Mostek (Nethone)	Wykorzystywanie fałszywych BTS-ów jako element pen testu urządzeń korzystających z kart SIM do transmisji danych Marcin Dudek (CERT Polska)	Crash Analyzing with Reverse Tainting (Powered By Taintgrind) Marek Zmysłowski (Cycura)	Bezpieczeństwo sprzętowe systemów biometrycznych Maciej Szymkowski (Politechnika Białostocka, Symmetra Ltd), Tomasz Grześ (Politechnika Białostocka)	Coma wspólnego Kierownik Łodzi Patrolowej, Kuchmistrz i Ekspert, czyli o metodach budowania SOC w administracji publicznej Jan Kosztewa (Min. Sprawiedliwości)
17:20 - 18:00	Cyberhydraulik w akcji - czyli skąd i jak cieknie! Adam Lange (Standard Chartered)	Roboty, samoloty a w nich AI i cyber - czy to nie za dużo? Kamil Frankowicz (CERT Polska)	Aktualne trendy prawne i biznesowe w cyberbezpieczeństwe Artur Piechocki (APLaw)	Jak ocenić bezpieczeństwo giełdy kryptowalutowej? Krzysztof Surgut (MyBenefit)	Rok z życia łowczego Maciej Kotowicz (Kaspersky GReAT)	Just a minor finding - stories of web vulnerabilities' chaining Jacek Kołodziej (Procter & Gamble)	DNS ATT&CK Piotr Głaska (Infoblox)	Jak zatruć życie cyberprzestępcy? Jarosław Jedynak, Michał Praszmo (CERT Polska)	Mechanizmy ochrony danych szyfrowanych komunikatorów dla systemu Android Kamil Kaczyński (WCY WAT)	root.txt - Chciałbym zacząć zdobywać flagi, ale ${losowa_wymówka} Radosław Żuber (Standard Chartered)	Bezpieczeństwo platform sprzętowych, a bezpieczeństwo procesów Artur Zięba-Kozarzewski (KRYPTON Polska)	
	14.12.2019 21:00 - ... AfterParty (Karova Music Club, Karowa 31)											