1 dzień konferencji

09.30–09.40

Powitanie uczestników. Rozpoczęcie konferencji.

Adam Mizerski, Wiceprezes, ISACA Katowice Chapter
Barbara Nerć-Szymańska, Prezes, ISACA Warsaw Chapter
Izabela Sakowicz, Managing Director, IDG Poland S.A.
Tomasz Wodziński, Prezes, ISSA Polska

09.40–10.10

Implementing an Effective Zero Trust Architecture.

dr Eric Cole, Founder & CEO, Secure Anchor Consulting

10.10–10.40

ITnorance (I invented this sh*t).

Bruno Horta Soares, CISA®, CGEIT®, CRISC™, PMP®, Founder & Senior Advisor, GOVaaS

10.40–11.10

FortiGuard Regional Threat Briefing and how an AI can supplement the Security Operations Team.

Kash Valji, Director of Consulting Systems Engineering, Fortinet

11.10–11.40

Zero Trust starts with MFA.

Dominik Bieszczad, Technical Solutions Architect, Duo Security at Cisco

11.40–12.00

Przerwa na odwiedziny Stref Partnerskich.

12.00–12.30

Nie tylko audyty...

Tomasz Wlaź, Naczelnik Wydziału w Departamencie Cyberbezpieczeństwa, Kancelaria Prezesa Rady Ministrów

12.30–13.00

Zero trust – modne słowo czy przełomowa innowacja.

Tomasz Jedynak, Cybersecurity Sales Manager, Cisco
Marcin Krzemieniewski, Manager Zespołu Bezpieczeństwa, NTT

13.00–13.20

KSC - jak wdrożyć wymogi rzetelnie (i przygotować się na KSC 2).

Cezar Cichocki, Szef Centrum Kompetencyjnego, OpenBIZ

13.20–13.40

V2X. V2H? H2V? WTF?

Rafał Jaczyński, Regional Cyber Security Officer CEE&Nordics, Huawei

13.40–14.00

Przerwa na odwiedziny Stref Partnerskich.

Sesja stolików eksperckich do wyboru

14.00–14.30

Sesja stolików eksperckich - roundatables 2

14.30–15.00

Sesja stolików eksperckich - roundatables.

Audyt IT

15.00–15.30

Od backup'u do disaster recovery.

Zbigniew Kupisz-Andrzejewski, Konsultant audytu (CISA, CRISC), ISACA Warsaw Chapter

Cyberbezpieczeństwo, Hacking i Forensic

15.00–15.30

Nie samymi sukcesami człowiek żyje, czyli historia pewnego incydentu...

Krzysztof Szmigielski, Kierownik Sekcji Informatyki, Szpital Wolski w Warszawie

Zarządzanie bezpieczeństwem informacji

15.00–15.30

Dyrektywa NIS 2 - jakie zmiany w zakresie cyberbezpieczeństwa proponuje Komisja Europejska?

Barbara Nerć-Szymańska, Prezes, ISACA Warsaw Chapter

Technologie i innowacje

15.00–15.30

Rzecz o bezpieczeństwie kontenerów, czyli dobre praktyki w pracy z Docker.

Tomasz Janczewski, Security Architect

Audyt IT

15.30–16.00

Audit, czy audyt, czyli kto może badać stan cyberbezpieczeństwa?

Andrzej Brągiel, Główny Specjalista w Zespole Analiz Stanu Bezpieczeństwa Cyberprzestrzeni, Ministerstwo Sprawiedliwości

Cyberbezpieczeństwo, Hacking i Forensic

15.30–16.00

Co w sieci piszczy...?

Jacek Grymuza, Członek Zarządu, (ISC)² Poland Chapter
Tomasz Winiarski, Sr. Solutions Architect, CISSP, CISA,CCSK, (ISC)² Poland Chapter

Zarządzanie bezpieczeństwem informacji

15.30–16.00

Cyberbezpieczeństwo-RODO-Pandemia. Czy cyber ubezpieczenia mogą być panaceum na nasze słabości w zarządzaniu cyberbezpieczeństwem?

Krzysztof Radecki, Audytor Wewnętrzny CGAP®, DPO (Inspektor Ochrony Danych), ISACA Warsaw Chapter

Technologie i innowacje

15.30–16.00

Bezpieczeństwo identyfikacji - elektroniczne dokumenty tożsamości.

Jan Szajda, CEO/Współwłaściciel, IDENTT

Audyt IT

16.00–16.30

Audytowanie procesu zarządzania ryzykiem.

dr Piotr Dzwonkowski, CISA, CISM, CRISC, ISACA Warsaw Chapter, ISSA Polska

Cyberbezpieczeństwo, Hacking i Forensic

16.00–17.00

Cyberastronomia, czyli atak na łańcuch dostaw.

Ireneusz Tarnowski, Analityk cyberzagrożeń, Santander Bank Polska

Zarządzanie bezpieczeństwem informacji

16.00–16.30

Analiza ryzyka w okresie pandemii - jak radzić sobie z nowymi ryzykami.

Anna Słodczyk, CRISC, EITCA/IS, Audytor ISO/IEC 27001, Inspektor ochrony danych, Menadżer ryzyka

Technologie i innowacje

16.30–17.00

Zapewnienie jakości i bezpieczeństwa aplikacji w środowiskach regulowanych.

Jan Anisimowicz, Director Audit, Risk & Compliance, ISACA Warsaw Chapter

16.30

Zakończenie pierwszego dnia konferencji.

2 dzień konferencji

09.30 **Otwarcie drugiego dnia konferencji.**

09.30–10.00 **Czy możemy ufać systemom?**

Joanna Karczewska, Audytor SI, DPO (Inspektor Ochrony Danych), ISACA Warsaw Chapter

10.00–10.30 **Paradigm Shift to an Operational Resilience Model.**

William B. Nelson, Chair & CEO, Global Resilience Federation

10.30–11.00 **Dostęp do infrastruktury krytycznej - fakty, mity i dobre porady.**

Marcin Marciniak, Manager, Implementation Expert, EY Business Advisory, Cyber Security Implementations

11.00–11.30 **Przerwa na odwiedziny Stref Partnerskich.**

11.30–12.00 **Dlaczego hackowanie aplikacji webowych jest proste?**

Michał Sajdak, Twórca portalu sekurak.pl, założyciel Securitum

12.00–12.30 **The Future of Blockchain: Analytics and the Data Trail**

Marc Taverner, Executive Director, INATBA - International Association for Trusted Blockchain Application

12.30–13.00 **5 metaphors that can make CISO's conversations with the business easier.**

Omar Khawaja, Chief Information Security Officer, Highmark Health

13.00–13.30 **Przerwa na odwiedziny Stref Partnerskich.**

Audyt IT

13.30–14.00

Blockchain – jak kontrolować za pomocą frameworku ISACA.

Małgorzata Michniewicz, Member of the Audit Committee, ISACA Warsaw Chapter

Cyberbezpieczeństwo, Hacking i Forensic

13.30–14.00

Radykalne ataki na systemy przemysłowe (OT) poprzez infrastrukturę wspierającą (IT/ICT) - przykłady i dobre praktyki.

Artur Zięba-Kozarzewski, Lider zespołu ds. Badań i Rozwoju, ISSA Polska

Zarządzanie bezpieczeństwem informacji

13.30–14.00

Jak audytować odporność organizacji (resilience).

Alina Zając, Kierownik Zespołu ds. Bezpieczeństwa Informacji i Analiz Ryzyka, BNP Paribas

Technologie i innowacje

13.30–14.00

Banki spółdzielcze w chmurze? Ocena ryzyka w różnych modelach outsourcingu.

Marek Moszkowski, System Engineer - Operating Systems Specialist, ISACA Katowice Chapter

Audyt IT

14.00–14.20

Cyberbezpieczeństwo, Hacking i

Zarządzanie bezpieczeństwem

Technologie i innowacje

Reagowanie na incydenty i kryzysy [cyberbezpieczeństwa] na dużą skalę w Unii Europejskiej.

Jakub Dysarz, Naczelnik wydziału, KPRM, Ekspert narodowy delegowany do Komisji Europejskiej

Cyberbezpieczeństwo, Hacking i Forensic

14.00–14.20

Scenariusz i reżyseria...” rzecz o tym, jak zaplanować i przeprowadzić dobry atak socjotechniczny”

Adrian Kapczyński, 1753c – Stowarzyszenie na rzecz cyberbezpieczeństwa
Jakub Plusczok, 17 53c – Stowarzyszenie na rzecz cyberbezpieczeństwa

Zarządzanie bezpieczeństwem informacji

14.00–14.20

Jak pandemia zmieniła VPNy?

Bartosz Chmielewski, Członek, ISSA Polska

Technologie i innowacje

14.00–14.20

Mechanizmy AI w służbie cyberbezpieczeństwa.

Sebastian Krystyniecki, Principal Systems Engineer, Fortinet

Audyt IT

14.20–14.50

Audyt chmury - jak się do tego zabrać? Standardy, metodyki, narzędzia.

Anna Chałupska, Audytor Bezpieczeństwa, ISACA Warsaw Chapter

Cyberbezpieczeństwo, Hacking i Forensic

14.20–14.50

Top 10 – czyli o czym pamiętać, aby korzystać bezpiecznie z chmury.

Tomasz Stachlewski, CEE Senior Solutions Architecture Manager, Amazon Web Services

Zarządzanie bezpieczeństwem informacji

14.20–14.50

Jak przejść do chmury zgodnie z wymogami UKNF i nie zwariować?

Paweł Kulpa, Architekt bezpieczeństwa, ISACA Warsaw Chapter

Technologie i innowacje

14.20–14.50

Normalizacja technologii blockchain i rozproszonych rejestrów DLT.

Michał Łoniewski, Kierownik Wydziału Rozwoju Usług Technicznych i Metod Badawczych Departament Innowacji i Rozwoju, Urząd Dozoru Technicznego

Audyt IT

14.50–15.20

Zdobywanie niebronionej twierdzy – przykłady audytu w sektorze finansowym i ochrony zdrowia.

Marek Ujejski, IT Security Expert - CISM, CPDSE Board Adviser, COIG S.A.

Cyberbezpieczeństwo, Hacking i Forensic

14.50–15.20

Ojejku. Ktoś się pod nas podszywa!

Piotr Zarzycki, Ekspert ds. cyberbezpieczeństwa, Orange

Zarządzanie bezpieczeństwem informacji

14.50–15.20

Disaster Recovery w chmurze - potrzebne czy nie? - lekcja z OVH Fire Case Study.

Jacek Bochenek, Cloud and Security Team Leader, ITEO

Technologie i innowacje

14.50–15.20

Red teaming - nowa filozofia testowania bezpieczeństwa.

dr inż. Mariusz Stawowski, Senior Member, ISSA Polska

Audyt IT

15.20–15.50

Audyt procesu zarządzania incydentem.

Adam Mizerski, Wiceprezes,

Cyberbezpieczeństwo, Hacking i Forensic

15.20–15.50

Jeden obraz - tysiąc słów, a może więcej? OSINTowa analiza

Zarządzanie bezpieczeństwem informacji

15.20–15.50

Operacyjna odporność cyfrowa sektora finansowego

Sesja warsztatowa

15.50–16.50

Jak zacząć audyt infrastruktury w jeden dzień - dla osób technicznych i nie (czas trwania 1h)

ISACA Katowice Chapter

zdjęć w praktyce.

Przemysław Feruś, Pentester, Schenker Technology Center Warsaw

- czy przełom w zapewniania ciągłości działania?

Krzysztof Maderak, Kierownik Zespołu Cyberbezpieczeństwa Rynku Finansowego w Departamencie Cyberbezpieczeństwa, Komisja Nadzoru Finansowego

Wojciech Ciemski, Specjalista i Trener, Eksperckie Centrum Szkolenia Cyberbezpieczeństwa

15.50 **Zakończenie konferencji SEMAFOR 2021 Online.**

Organizatorzy dołożą wszelkich starań, aby konferencja odbyła się zgodnie z prezentowanym programem, jednak zastrzega się możliwość częściowych zmian godzin poszczególnych wystąpień.