

AGENDA

Kongres CyberTrust 2024 – Dzień 1

07.10.2024 r. – poniedziałek

9:00	Przywitanie	
10:00	Sylvian Schellenberg: <i>"Cyber Resilience for the Swiss Finance Industry - an Industry example"</i>	
11:00	Agnieszka Wilk: <i>"AI jako budowniczy naszej Cyber Twierdzy - jak wykorzystać możliwości sztucznej inteligencji dla naszej ochrony"</i>	Sala 10ABCD [Budynek D-20]
11:30	Marek Ujejski: <i>"Problemy dowodowe w informatyce śledczej"</i>	
12:10	Lunch	Strefa Kultury Studenckiej (SKS) [Budynek C-18]
13:00 – 15:00	Grupy tematyczne	Szczegóły na stronie nr 2
19:00	Sesja Networkingowa	Strefa Kultury Studenckiej (SKS) [Budynek C-18]

Grupy tematyczne:

GRUPA 1 - Informatyka śledcza i cyberwojny

GRUPA 2 - Zarządzanie cyberbezpieczeństwem

GRUPA 3 - Technologie przyszłości w cyberbezpieczeństwie

GRUPA 4 - Człowiek, dane i cyberbezpieczeństwo

GRUPA 5 - Analiza przypadków i badań dla cyberbezpieczeństwa

GRUPA 6 - Ścieżka praktyków

Grupy tematyczne

	10AC [Bud. D-20]	10B [Bud. D-20]	113 [Bud. D-20]	201 [Bud. D-21]	10D [Bud. D-20]	007 [Bud. D-21]
	GRUPA 1	GRUPA 2	GRUPA 3	GRUPA 4	GRUPA 5	GRUPA 6
13:00	Tomasz Budziński: <i>„Techniczna analiza kampanii dezinformacyjnej realizowanej przeciwko RP”</i>	Wojtek Wodo: <i>„Nowe regulacje prawne: PSD3 i jej wpływ na bankowość elektroniczną”</i>	Prof. Surma: <i>“Wstęp do red teaming dużych modeli językowych (LLM)”</i>	1) Paweł Fortuna: <i>„Czy technologia może rozwijać człowieka, czy raczej jest zagrożeniem”</i> 2) Paweł Zegarow: <i>„Psychologiczne aspekty cyberbezpieczeństwa”</i>	Monika Raulinajtys-Grzybek: <i>„Zapewnienie bezpiecznego dostępu do danych zdrowotnych”</i>	Ireneusz Tarnowski: <i>„Magia analityka dla każdego, czyli czy analiza malware musi być trudna”</i>
14:00	Tomasz Ladra: <i>„Praktyczne zastosowanie narzędzi inżynierii inżynierii śledczej”</i>	Tomasz Bujala Agnieszka Kwiecień Paulina Krakowska Dyskusja: <i>„Krajobraz formalnoprawny z perspektywy przedstawicieli różnych organizacji - wyzwania i szanse”</i>	Adrian Kapczyński: <i>„Ewolucja łańcucha bloków w erze obliczeń kwantowych”</i>	Angelina Piątkowska: <i>„Czyli jak przeżyć incydent bez uszczerbku na zdrowiu”</i>	Karolina Wilanowska: <i>„AI Act jak zapewnić bezpieczeństwo wdrożeń systemów opartych na AI”</i>	Paweł Maziarz: <i>„PowerShell - czy warto się z nim zakumplować?”</i>
15:00	Konrad Kałużny: <i>“Ransomware as a Service (RaaS): Threat Hunting Case Study”</i>	Jerzy Judycki: <i>„Tożsamość cyfrowa: e-Doręczenia”</i>	Bartłomiej Skowronek: <i>„Wyścig zbrojeń w cybersecurity”</i>	Liwia Palus Mateusz Pękala Ryszard Piotrowski Dyskusja: <i>„Ciemne strony internetu - jak darknet, grooming i przestępczość zorganizowana wpływają na bezpieczeństwo internautów”</i>	Marek Doering: <i>„Gdzie nie spełniamy wymagań prawnych Krajowej Rady Interoperacyjności i UoKSC na przykładach podmiotów medycznych i samorządowych”</i>	Dawid Golak: <i>„Red teaming w praktyce”</i>

AGENDA

Kongres CyberTrust 2024 – Dzień 2

08.10.2024 r. - wtorek

9:00 – Grupy tematyczne
12:00

Szczegóły na stronie
nr 4

12:00 | Lunch

Strefa Kultury
Studenckiej (SKS)
[Budynek C-18]

13:00 Kamil Sutuła | Jacek Oko | Agnieszka Kwiecień
| Ryszard Piotrowski | Michał Kurek
Debata:
"NIS2 i co dalej?"

14:00 Artur Kalinowski:
"Siła automatyzacji: techniki zwiększania efektywności deserializacji.
Od ręcznego sterowania po pełną automatyzację ataków"

Sala 10ABCD
[Budynek D-20]

15:00 Rozdanie nagród | Zakończenie

Grupy tematyczne:

GRUPA 1 - Informatyka śledcza i cyberwojny

GRUPA 2 - Zarządzanie cyberbezpieczeństwem

GRUPA 3 - Technologie przyszłości w cyberbezpieczeństwie

GRUPA 4 - Człowiek, dane i cyberbezpieczeństwo

GRUPA 5 - Analiza przypadków i badań dla cyberbezpieczeństwa

GRUPA 6 - Ścieżka praktyków

Grupy tematyczne

	10AC [Bud. D-20]	10B [Bud. D-20]	113 [Bud. D-20]	201 [Bud. D-21]	10D [Bud. D-20]	007 [Bud. D-21]
	GRUPA 1	GRUPA 2	GRUPA 3	GRUPA 4	GRUPA 5	GRUPA 6
9:00	Grzegorz Matecki: „Wywiad w epoce rewolucji cyfrowej”	Dariusz Czerniawski: „Sfederowany ISMS jako odpowiedź na złożoność organizacji”	Krzysztof Trojan: „Użyteczność Zdalnej Identyfikacji osób w usługach zaufania w obliczu wektorów ataków opartych na AI”	Debata: „Kariera w cyber w oparciu o certyfikację”	Ireneusz Tarnowski: „Bankomat z perspektywy cyberbrońców”	Łukasz Cepok: „Księżę mobilnego malware”
10:00	Marcin Ratajczyk: „Problem atrybucji cyberoperacji w kontekście stosunków międzynarodowych”	Jan Szajda: „Tożsamość cyfrowa: cyfrowe portfele tożsamości i EUDI”	Borys Łącki: „Czy szczoteczka do zębów to wektor ataku”	Debata: „Świadomość i zachowania wobec zagrożeń w Internecie”	Pani Ania Kuba: „Kiedy MFA nie wystarcza, czyli o aktualnych sposobach wykradania danych uwierzytelniających”	Andrzej Dyjak Krzysztof Korozej: „Mroczna strona OSS”
11:00	Mec. Marcin Serafin Pani Ania: „Skrzydlate konie i szczury na urządzeniach mobilnych, czyli o zagrożeniach dla prywatności”	Michał Tabor: „Tożsamość cyfrowa rozporządzenie eIDAS2 i co nas czeka”	Kamil Sutuła Artur Bicki Debata: „Technologie przyszłości a cyberbezpieczeństwo”	<tba>	Paulina Krakowska Marta Struzik: „Jak utrudnić ataki oszustom - technologia czy edukacja?”	1) Maciej Kisielewicz: „Podstawy bezpieczeństwa webowego” 2) Karol Słomczyński Mateusz Głuchowski Artur Kręgiel: „Od zera do profilera, czyli jak znaleźć informacje o wszystkim i o wszystkich”