HARMONOGRAM

KYBER

9:00	Prezence a ranní občerstvení
10:00	Zahájení konference
10:05	Metodika pro řízení bezpečnostních incidentů v režimu nižších i vyšších povinností – Denisa Drappanová
10:25	LeakSentinel – nástroj pro odhalování úniků přihlašovacích údajů – Adam Maczkó
10:45	Kontinuita činností na univerzitě – Jiří Bořík
11:05	AI ano, ale s pravidly – Petr Vlachynský
11:25	Ochrana koncových stanic před škodlivým kódem – Tomáš Zach
11:45	Řízení technických zranitelností – Petr Švec
12:05	Experimentální využití AI nástrojů pro identifikaci kompromitovaných účtů autentizační služby – Pavel Witassek
12:25	Obědová pauza

13:25	Zabezpečení dat v Power BI – Daniel Tovarňák
13:50	Spolupráce organizací a podpora řešení IT bezpečnosti – Martin Pustka
14:05	Systém MUDRC, evidence koncových zařízení – Vítězslav Grygar
14:20	SIEM, logování a vyhodnocování – Jakub Kalnik
14:35	Audit NÚKIB – Jakub Sauer a Denisa Drappanová
15:00	Institucionální odolnost – Jan Kolouch
15:25	Coffee break
15:40	AI mění pravidla phishingu. MUNI přepisuje pravidla simulací – Natalia Peterek
16:05	Detekce exfiltrace dat v univerzitním prostředí – Daniel Tovarňák
16:30	Diskuze
17:00	Ukončení konference

KYBER