Programm | Programme
IT-SECX 11.10.2024

IT SECX — IT SECURITY COMMUNITY EXCHANGE

WKO WIRTSCHAFTSKAMMER NIEDERÖSTERREICH Unternehmensberatung · Buchhaltung · IT

IT WELT.at

fh st.pölten — UNIVERSITY OF APPLIED SCIENCES

ab 13:30	**Get Together und Registrierung**										
	Großer Festsaal | Large Assembly Hall										
14:00	**Katharina Windhör**	**Eröffnung & Begrüßung** Johann Haag (Geschäftsführer, FH St. Pölten) Markus Aulenbach (Berufsgruppensprecher IT, WKO UBIT NÖ)									
14:15		**Neues aus dem Department Informatik und Security** Simon Tjoa (Departmentleiter Informatik und Security, FH St. Pölten)									
14:30		**KEYNOTE: Red Teaming in an AI World** Daniel Fabian (Lead Machine Learning Red Team at Google)									
15:30–16:15	**Pause | Break**										
	Katharina Windhör	**Großer Festsaal | Large Assembly Hall**	**Herfried Geyer**	**Mittlerer Festsaal | Medium Assembly Hall**	**Robert Luh**	**Audimax | Main Auditorium**	**Martin Pirker**	**Hörsaal 1 | Lecture Hall 1**	**Lukas König**	**Future Lab**	
		AI		**DEFENSE**		**OFFENSE**		**OT / INDUSTRIAL**		**MIXED SECURITY TOPICS**	
16:15		**AI: The Next Chapter in Pentesting's Evolution? - Revisited** Nino Fürthauer, Darius Pavelescu | Limes Security		**Breaching Bad: Unpacking the Root Causes of recent Incidents** Petar Kosic | Erste Digital		**Der Tag, an dem wir die Domäne fast nicht übernommen hätten…** Florian Bogner | Bee Security		**KI und Cybersecurity in der Konvergenz von IT und OT** Johann Schlaghuber | Siemens AG		**Code Analyse in Open-Source Projekten des Gesundheitsbereichs** Zoe Herzig | SBA Research	
16:45		**The Big LLMbowski: Ensuring AI Abides (Sicherheitsbedenken bei LLMs)** Matthias Holzgethan | Elastic		**King SIEM is dead – Long live Princess-XDR** Daniel Kroiß, Stefan Prinz | KPMG		**Tagebuch eines Red Teamers: Kapitel 2 - Burning (Out)** Philipp Allmer, Philipp Reiter | Cancom Austria AG		**Mit der NIS-Kanne durchs Unternehmen? Umsetzung der NIS2 Maßnahmen aus Sicht eines kritischen Infrastrukturbetreibers** Wolfgang Löw, Alexander Novotny | EVN AG		**The humans who stare at source code. A primer on Source Code Review and analyzing some of the most critical CVEs of the last year.** Martin Haunschmid | Adversary GmbH	
17:15		**GPT, ignore previous instructions! Prompt injection attacks and how to avoid them** Sebastian Schrittwieser, Caroline Lawitschka | Universität Wien		**Tausend und Ein Logevent – zeitreisende Logs und andere Inkonsistenzen** Susanne Schön | Materna Radar Cyber Security		**SMTP Smuggling Revisited – Still Spoofing E-mails Worldwide?!** Timo Longin | SEC Consult		**OT Security im Kontext Manufacturing AI** Anna Habenegg, Gerald Ortner | PwC		**Entropie im Sinkflug: rand() und srand()** Johannes Kruchem | SEC Consult	
17:45–18:30	**Pause | Break**										
	Katharina Windhör	**Großer Festsaal | Large Assembly Hall**	**Sebastian Ehresheim**	**Mittlerer Festsaal | Medium Assembly Hall**	**Peter Kieseberg**	**Audimax | Main Auditorium**	**Gerald Weinberger**	**Hörsaal 1 | Lecture Hall 1**	**Timea Pahi**	**Future Lab**	
18:30		**Sicherheitslücken in AI-Chatbots: Risiken und Schutzmaßnahmen** Benjamin Medicke | Deloitte		**Unlocking Agile Security: The Community Rollercoaster Ride of (in)sanity** Florian Schier, Marco Macala, Christian Buchinger | Raiffeisen Bank International		**Observing Clouds: container attacks for embedded use cases** Reinhard Kugler | SBA Research		**ICS Firing Range: Erfolgreiches Abwehren eines Hackerangriffes auf ein Wasserkraftwerk** Christoph Kukovic, Tobias Schwabel | Verbund AG		**Conformance auf Business Prozessebene - Concept Drifts und Abweichungen entdecken mittels Process Mining Algorithmen** Florian Stertz | Condignum GmbH	
19:00		**Double-Edged Sword: AI for Cyber Defense** Stefan Pfeiffer, Alexander Ressl | Accenture		**Überwachung Angriffserkennung und Analysemögkichkeiten auf Container-Umgebungen zur Laufzeit** Johannes Bär | Condignum GmbH		**Who Let the Hounds Out - Fehler in der Implementierung vom Active Directory Tier Modell** Martin Grottenthaler | VidraSec e.U.		**Industrial Security in der Praxis - First Steps, IDS & Betrieb eines Industrial Honeypots** Martin Strommer | IKARUS Security Sofware GmbH, Fachhochschule St. Pölten		**Deep Fakes, Fake News and Disinformation** Martin Boyer | AIT Roland Pucher | PwC	
19:30–20:00	**Pause | Break**										
	Katharina Windhör	**Großer Festsaal | Large Assembly Hall**	**Stefan Machherndl**	**Mittlerer Festsaal | Medium Assembly Hall**	**Michael Kirchner**	**Audimax | Main Auditorium**	**Henri Ruotsalainen**	**Hörsaal 1 | Lecture Hall 1**	**Patrick Kochberger**	**Future Lab**	
20:00		**Skynet Wants Your Passwords! - The Role of AI in Automating Social Engineering** Alexander Hurbean, Wolfgang Ettlinger | Certitude Consulting		**The Always-On Purple Team: An automated CI/CD for detection engineering** Jeroen Vandeleur | NVISO		**Who Watches the Watchmen: How Kernel-Level Anti-Cheat systems are similar to Rootkits** Christoph Dorner | Fachhochschule St. Pölten		**Embedded Security Testing: Concepts and Practice** Rainer Poisel | honeytreeLabs		**"Computer, bring mir IT-Security bei." - Securityawareness & KI** Thomas Steinbrenner | Section 8 e.U. Jochen Kranzer | ovos GmbH	
20:30		**Large Language Models in Cybersecurity: The Good, The Bad, and The Ugly** Andreas Ekelhart | Universität Wien		**Maturing Threat Modeling: A Five-Year Journey Integrating Security** Jaroslaw Kupczak | Sportradar		**NIS2/DORA/CRA Compliance durch Penetration Tests: Deshalb ist die Zusammenarbeit von Technikern und Managern notwendig** Daniel Mrskos | Security mit Passion		**Situation-Adaptive Machine Communication Control in Industrial Networks** Harald Gattermeyer | Anapur AG			
21:00	**Veranstaltungsende | End of the event**										