AI VILLAGE
SWISS CYBER STORM

SCHEDULE

Time	Aare	Aare 1	Aare 2	Aare Foyer
10:50 – 11:55	**AI Security – What Could Possibly Go Wrong?** Workshop 10:50 - 12:30 Andrea Hauser, Offense Team at scip Ralph Meier, Offense Team at scip Yann Santschi, Offense Team at scip Lucie Hoffmann, Offense Team at scip Dr. Marisa Tschopp, Researcher at scip	**Your Personal AI Infrastructure** Workshop 10:50 - 12:30 Daniel Miessler, Founder and CEO of Unsupervised Learning	**AI and Human Rights** Demos & Presentations 10:50 - 11:55 Jan Kleijssen, Member of the Advisory Board at ALLAI	**Seeing Yourself Through the Hacker's Eyes: Building an Automated Pipeline with Deepfakes & Vishing** Demos & Presentations 10:50 - 11:55 Andrey Lazarev, Co-founder and COO of Brightside AI
12:00 – 12:30				
12:30 – 14:00	Lunch Break	Lunch Break	Lunch Break	
14:00 – 15:05	**Navigating the AI Crisis: An Interactive Crisis Experience** Workshop 14:00 - 15:40 Katie Koetke, Managing Partner at Resilienz Adivsors Maxine Moleman, Partner at Resilienz Adivsors		**Threat Modeling LLMs and Their Integrations** Workshop 14:00 - 15:05 Prof. Dr. Andrei Kucharavy, Assistant Professor at Informatics Institute of HES-SO Valais-Wallis	**Poster Sessions & Flash Talks** Poster Sessions 12:30 - 16:20 Prof. Dr. Ariane Trammell, Head of Information Security Research at ZHAW Maurice Amon, Research Assistant at ZHAW Dr. Nicolas Badoux, EPFL (HexHive) Paul Bagourd, Graduate Intern at Cyber Defense Campus (Armasuisse S&T) Tomas Joaquin Anderegg, Master Student at EPFL Dr. Anastasiia Kucherenko, Scientific Collaborator at HES-SO Valais-Wallis (IEM) Dr. Elena Nazarenko, Lecturer at Lucerne University of Applied Sciences and Arts (HSLU) Alexander Sternfeld, Associate Researcher at HES-SO Valais-Wallis (IEM) Dr. Loic Marechal, Scientific Collaborator at HES-SO Valais-Wallis (IEM) Dr. Sébastien Rouault, Co-founder and CTO at Calicarpa
15:10 – 15:40		**Dark Prompts and Malicious Agents: Offensive AI in Action** Demos & Presentations 15:10 - 15:40 Candid Wüest, Principal Security Advocate at xorlab	**Leveraging AI for Strategic Technology Monitoring in the Defense Sector** Demos & Presentations 15:10 - 16:10 Dr. Julian Jang-Jaccard, Scientific Project Manager at armasuisse Paul Bagourd, Graduate Intern at Cyber Defense Campus (Armasuisse S&T) Tomas Joaquin Anderegg, Master Student at EPFL	
15:40 – 16:10		**Automation of Cyber Defense** Demos & Presentations 15:40 - 16:10 Dr. Roland Meier, Scientific Project Manager at armasuisse Dimitri Francolla, Student at ETH Zürich Siim Marvet, Master's Student at EPFL		