Cybersecurity Across Cultures: Language, Society, and the Global Threat Landscape

Day 1

8:00 – 9:00: Registration, Tea/Coffee,

Networking

Start: 09:30 | **End:** 17:00 | **Conference Dinner:** 18:00–21:00

Time	Session	Description
09:00 – 09:30	**Opening Ceremony**	Opening and Welcome
09:30 – 11:00	**Opening Keynote Address and panel discussion**	*Cybersecurity in the Global South: Language, Locality, and Policy*
11:00 – 11:30	**Tea/Coffee Break**	Informal networking
11:30 – 12:30	**Panel 1:** *One Threat, Many Responses*	National and regional case studies of culturally contextualised cybersecurity frameworks
12:30 – 13:30	**Lunch Break**	Informal networking and discussions
13:30 – 14:30	**Windows Incident Response Artifact Primer**	Participants will explore key Windows system artifacts such as event logs, registry hives, and file system metadata that reveal attacker behavior. The session highlights how these artifacts fit into the incident response process and map to specific attack techniques.
13:30 – 15:00	**Tea/Coffee Break**	Informal networking
15:00 – 16:00	**Targeted Log and Artifact Collection using KAPE and EvtxEcmd**	Learn to rapidly collect and parse logs and forensic data using KAPE (Kroll Artifact Parser and Extractor) and EvtxEcmd. The session emphasizes targeted evidence collection and validation to support efficient analysis.
16:00 – 17:00	**Analytical Log Analysis using Timeline Explorer and the PANICS Framework**	Participants will perform structured log analysis using Timeline Explorer, applying the PANICS framework to interpret events, correlate activity, and build an investigative narrative from the collected data.
18:00 – 21:00	Conference Dinner, venue TBC	

Day 2 –

Registration, Tea/Coffee, Networking

Start: 09:00 | **End:** 16:00

Time	Session	Description
09:00 – 11:00	**Log Analysis using Hayabusa and the PANICS Framework**	This session introduces Hayabusa, a fast and powerful event log analysis tool that helps detect suspicious activity using Sigma rules. Participants will practice mapping findings to attacker TTPs and use PANICS to contextualize alerts.
11:00 – 11:30	**Tea/Coffee Break**	Informal networking
11:30 – 13:00	**Log Analysis using Wazuh SIEM and the PANICS Framework**	Participants will transition to analyzing logs at scale using Wazuh, an open-source SIEM platform. The session focuses on detection correlation, alert interpretation, and mapping observed behaviors to MITRE ATT&CK TTPs through guided investigations.
13:00 – 14:00	**Lunch**	
14:00 – 15:30	**Panel 2: Designing Multicultural Cyber Awareness Campaigns**	Practical, all-participant session with facilitators guiding the creation of context aware tools and messaging
15:30 – 16:00	**Closing**	Closing remarks, certificates, awards
16:00 – 17:00	**Tea/coffee**	Networking

Accepted papers will be presented via round-table discussions in the relevant sessions. This program is subject to change.