https://www.threatcon.co.za/

National Computer Emergency Response Team (CERT) Roundtable

STRENGTHENING AFRICAN CYBERSECURITY:

STRATEGIES AND BEST PRACTICES FOR MATURING NATIONAL CERTs

DATE: **28th October 2025**
VENUE: **Mauritius**

28th October 2023		
Program Director: Professor Manoj Maharaj, THREAT 2023 Conference Chair		
08:00 – 08:30	**Registration**	
08:30 – 08:45	**Welcome** **Opening Address**	**SADC Secretariat**
08:45 – 09:45	**Session 1: CERT Status update** This CLOSED session will allow National CERTs / CSIRTs to update the meeting on the status of their national CERT / CSIRT initiatives. The proposed format for the status update: Brief Introduction CERT name and country of origin, Primary mission, and objectives Status of national legislation and national CERT(s) Achievements in the past year Major incidents handled or mitigated. Partnerships formed, collaborations or joint exercises including with other national CERTS and private sector-CERTs. Challenges and Opportunities (country and national CERT) Looking Ahead Plans and strategies for the upcoming year **Facilitator: Dr Kaleem Usmani** Head Computer Emergency Response Team of Mauritius (CERTMU) and Mauritius Cyber Security Center of Excellence (CoE) Chair of the SADC Policy, Procedures and Governance Technical Working Group	

	Vice-Chair of the SADC Regional CIRT (SR-CIRT) Steering Committee
09:45 – 10:00	**Tea and Networking**
10:00 – 11:00	**Session 2: Maturing National CERTs** Session Two explores best practices, and strategies to maturing national CERTS, specifically looking at: - **Services of a national CERT: What to offer when?** A properly deployed CERT has a clear mandate, a governance model, a tailored services framework, technologies, and processes to provide, measure, and continuously improve defined services. This session will discuss how the services of a national CERT can evolve towards full maturity. It will also discuss the Computer Security Incident Response Team (CSIRT) Services Framework, which describes the structured way the services of a national CERT are implemented. - **Platforms, tools, and technologies: Navigating the Maze!** National CERTs have access to a diverse array of tools and technologies, spanning both open-source and proprietary solutions, to enhance their cybersecurity capabilities. Both open-source and proprietary technologies offer advanced features and sometimes specialized capabilities tailored to the unique requirements of national CERTs. Choosing between options can be a daunting task and this session will delve into these issues. - **Cyberdrills, capture-the-flag: practical exercises for national CERTs** Practical training like cyber drills and capture-the-flag exercises enhance cybersecurity readiness. They provide an opportunity for CERT members to simulate real-world cyber incidents in a controlled environment, allowing them to practice coordinating responses across different stakeholders, including government agencies, private sector entities, and international partners, fostering collaboration and communication during emergencies. This session explores these initiatives and provides practical steps on how to run these programs effectively. **Facilitator: Forum of Incident Response and Security Teams (FIRST)**
11:00 – 12:15	**Session 4: OSINT. Making sense of threat feeds** The community of ***open-source threat intelligence feeds*** has grown over time with new sources being offered all the time. These services span freemium to paid services. There are community projects that aggregate data from new sources of threat intelligence and also emerging markets of companies that pull all this and other data into Threat Intelligence solutions. Security companies also often offer their threat intelligence as a community service. The result is a massive amount of information, which needs to be aggregated to be useful. **Facilitator: Shadowserver Foundation**
12:15 – 12:45	**Session 4: Fostering relationships with industry and sector-based CERTs.** Sector-based or industry-specific Computer Emergency Response Teams (CERTs) play a crucial role in enhancing cybersecurity resilience within specific sectors or industries. By focusing on the unique challenges, threats, and technologies prevalent in their respective sectors, these CERTs can develop specialized expertise and tailored solutions to address emerging cyber threats effectively. Collaborating in the establishment of sector-CERTs is a fraught opportunity for national CERTs and needs to be navigated carefully. This session will delve into these issues in more detail.

	Facilitator: Dr Kiru Pillay Department of Communications and Digital Technologies (South Africa) Chair of the SADC CERT Task Force
12:45 – 13:00	**Session 4: Way Forward & Closing** Close out of the workshop identifying practical steps and a way forward. Nations CERTs to highlight upcoming events or initiatives, training initiatives or workshops. **Facilitator: SADC Secretariat**