

NICIS

COLLABORATE. INNOVATE. ADVANCE.



SANReN

COLLABORATE
INNOVATE
ADVANCE

**Cyber
Security
Challenge
2022**

Overview

The National Integrated Cyber Infrastructure System (NICIS), which comprises of the Centre for High Performance Computing (CHPC), the South African National Research Network (SANReN) and the Data Intensive Research Initiative of South Africa (DIRISA) will be hosting the CHPC National Conference in November 2022. At this conference, SANReN will host the sixth annual Cyber Security Challenge (CSC). The purpose of the competition is to stimulate interest in Cyber Security in general, but more specifically in the field of Network Security within South African Tertiary institutions. Therefore, this competition is aimed at university students who are interested in information security fields such as penetration testing, incident response, digital forensics, cryptography, and cyber security training.

The sixth annual Cyber Security Challenge will consist of:

- A jeopardy-styled Capture the Flag (CTF) event that will test the problem-solving skills of participating teams by requiring them to complete challenges that replicate real-world scenarios. The challenges include binary exploitation, cryptography, web exploitation, reverse engineering, digital forensics, and mobile phone security.
- An Attack/Defend system for team vs. team battles. Here every team has their own system that consists of dedicated preconfigured hardware and software. In the Attack/Defend competition, the teams must hack each other but also fix vulnerabilities in their own system (through patching).
- Independently manned scoring system.
- Professionally managed challenge competition

The key benefit of the CSC is the opportunity for university students to receive exposure to current and trending cyber security topics. Such exposure will stimulate interest in the field of cyber and information security, growing the next generation of ethical hackers. Additionally, during the competition, the students may discover new 0-day vulnerabilities. These vulnerabilities can then be negated before they can be used by malicious hackers. Finally, the CSC competition offers an opportunity to discover innovative thinkers and identify cyber security specialists in the making.

Due to the high interest among students, the CSC competition is divided into two rounds. The qualifier rounds allow students from universities across South Africa (including Botswana and Namibia) to compete for positions in the final. Upon completion of the qualifier rounds, the top eight teams will be invited to represent their university in the final at the CHPC National Conference. The eventual aim is for SANReN to sponsor the winning student team to compete in an appropriate international competition, such as the European Cyber Security Challenge or the BRICS skills challenge, similar to the CHPC's sponsorship of the CHPC Student Cluster Competition winners to participate in the ISC Student Cluster Competition. There is also an opportunity to initiate and grow the Cyber Security Challenge into an African Cyber Games event to potentially be hosted in collaboration with the three Regional Research and Education Networks (RRENs) spanning Africa.

Capture the Flag

The main event of the CSC competition is a CTF challenge, which is designed to test students' abilities in a wide range of cyber security skills. The CTF will be composed of a variety of challenges that includes binary exploitation, cryptography, web exploitation, reverse engineering, forensics, and mobile phone security. The 2021 CTF challenge was won by CyberFury, a team from the University of Pretoria.

Attack/Defend

The Attack/Defend challenge presents the students with an alternative twist. Teams are given 3 hours to identify and patch all vulnerabilities on their dedicated server, after which teams must penetrate and change banners on opposing teams' server to score points. The 2021 Attack/Defend challenge was also won by CyberFury.

Hash Challenge

Previous CSC competitions included a Hash Challenge. To test students' abilities to maximise computational efficiency, each team is given a set of ~1M hashes distributed between short and very long inputs and hashed using a variety of algorithms. The challenge is simple: the team that can reverse the most hashes within a time and cloud compute limit wins.

Social Engineering Challenge

Breaching the perimeter security of a network becomes harder each passing day. The modern approach to gain a foothold in a network is to focus on the softer targets: people. The social engineering challenge is awarded to the team that can prove a successful social engineering attack was executed against an opposing team.

Custom Challenge

Custom challenges are also accepted, offering a unique opportunity to test students' skills and abilities.





Cyber Security Challenge 2022

Why Sponsor?

The aim of the CHPC National Conference is to bring together students and professionals in the fields of high-performance computing, big data, and high-speed networking to enable collaboration and communication of work being done. Therefore, the conference provides an excellent opportunity to promote your brand to a wide variety of professionals. Additionally, you will gain direct exposure to students who are interested in cyber and information security during the CSC competition.

Sponsorship Opportunities for 2022

We offer a range of sponsorship opportunities designed to meet your needs and resources. The CSC competition will give exposure to sponsors through the CSC website, pull-up banner at the conference, student medals, mentor trophies, and a talking slot during the induction of the students to this year's competition. Your contribution will allow us to sponsor several students in our quest to build the cyber security pipeline in Southern Africa.

All sponsors receive an opportunity to place custom content on the CSC website.

Should circumstances allow, sponsor logos will be placed on t-shirts shipped out to students.

Podium Sponsorship

Acknowledgement of sponsorship during the CSC 2022 Prize Giving Ceremony. All podium placement sponsors will have their respective logos placed on the medals received by the winning teams, as well as the trophies received by the mentors of the winning teams.

Challenge Sponsorship

For challenge sponsors, logos will be placed on the medals received by the winning teams. It is important to note that challenge sponsors have insight and input into challenge development and might be required to form part of the judging panel for challenge winner selection.

Contact

For any queries or questions, please contact us at csc@sanren.ac.za



Cyber Security Challenge 2022

2022 Sponsorship Packages

If you are interested in sponsoring, please complete the following form and return to csc@sanren.ac.za

International Competition	Sponsorship Value	Check Applicable	In Kind ²
Top 10 Students to Attend International Competition ¹	R 500k		N/A
Podium Sponsorship	Sponsorship Value	Check Applicable	In Kind ²
1st Place	R 100k		
2nd Place	R 50k		
3rd Place	R 30k		
Challenge Sponsorship	Sponsorship Value	Check Applicable	In Kind ²
Hash Challenge	R 30k		
Attack/Defend Challenge	R 30k		
Social Engineering Challenge	R 30k		
Custom Challenge	R 50k		
Sponsor Details			
Name of sponsor			
Company name on invoice			
Currency			
Billing Address			
Contact Person			
Contact Cell			
Contact Landline			
Contact Email			

¹ This sponsorship entails taking a team of students to an International Competition in 2023, where the sponsor will cover the students' flights, travel and accommodation for the students competing at the event.

² In Kind contributions are accepted, subject to approval by the CSC organizing committee.

Company Name _____

Name and Surname _____

Signed _____

At _____ on the _____ day of _____ 2022