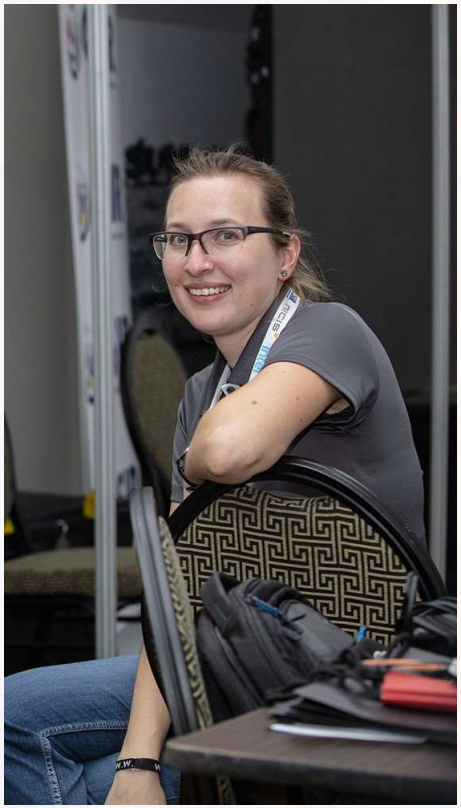

AN INITIATIVE OF:
science, technology & innovation
Department:
Science, Technology and Innovation
REPUBLIC OF SOUTH AFRICA
CSIR
Touching lives through innovation
80th anniversary
NICIS
NATIONAL INTEGRATED
CYBERINFRASTRUCTURE SYSTEM
SANReN
SANReN
Cyber Security
Challenge (CSC) 2025

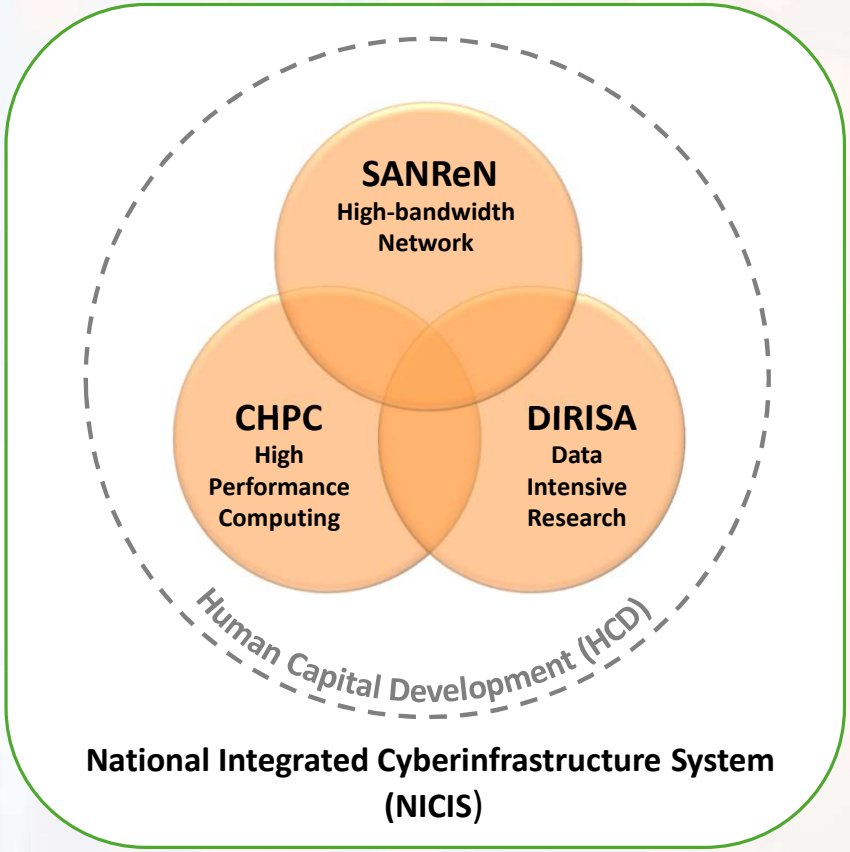
Who Am I

- Heloise Meyer
- 10+ years at the CSIR
- PhD Computer Science (2019)
- Research Interests:
  - Cybersecurity, mobile security, and digital forensics
  - *Passionate about CTF competitions*
- Joined SANReN, NICIS in July 2022
  - Lead organiser of the CSC
  - Managing the SANReN CSIRT



Background: NICIS

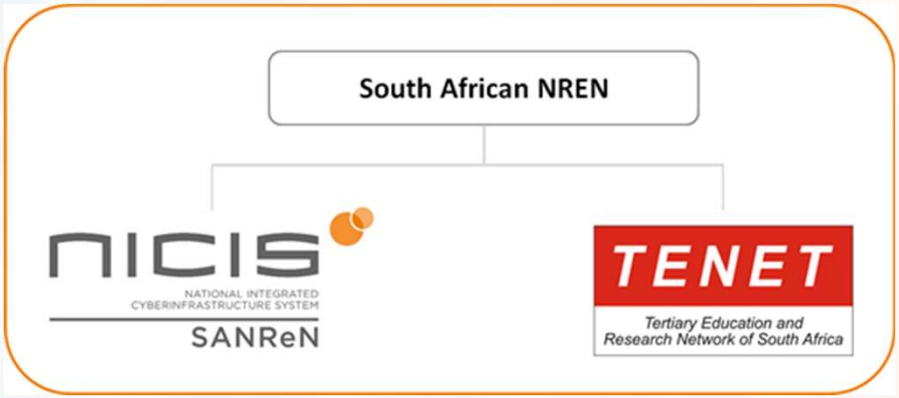
- National Integrated Cyberinfrastructure System (NICIS)
- Structure
  - South African Research Network (SANReN)
  - Centre for High Performance Computing (CHPC)
  - Data Intensive Research Initiative of South African (DIRISA)
  - HCD encompasses the 3 pillars
- NICIS is a hosted programme of the DSTI
- Hosted at the CSIR as a centre in NGEI Cluster, Smart Society Division



SANReN, https://www.sanren.ac.za/ | CHPC, https://www.chpc.ac.za/ | DIRISA, https://www.dirisa.ac.za/ | https://www.dsti.gov.za/

What are NRENs?

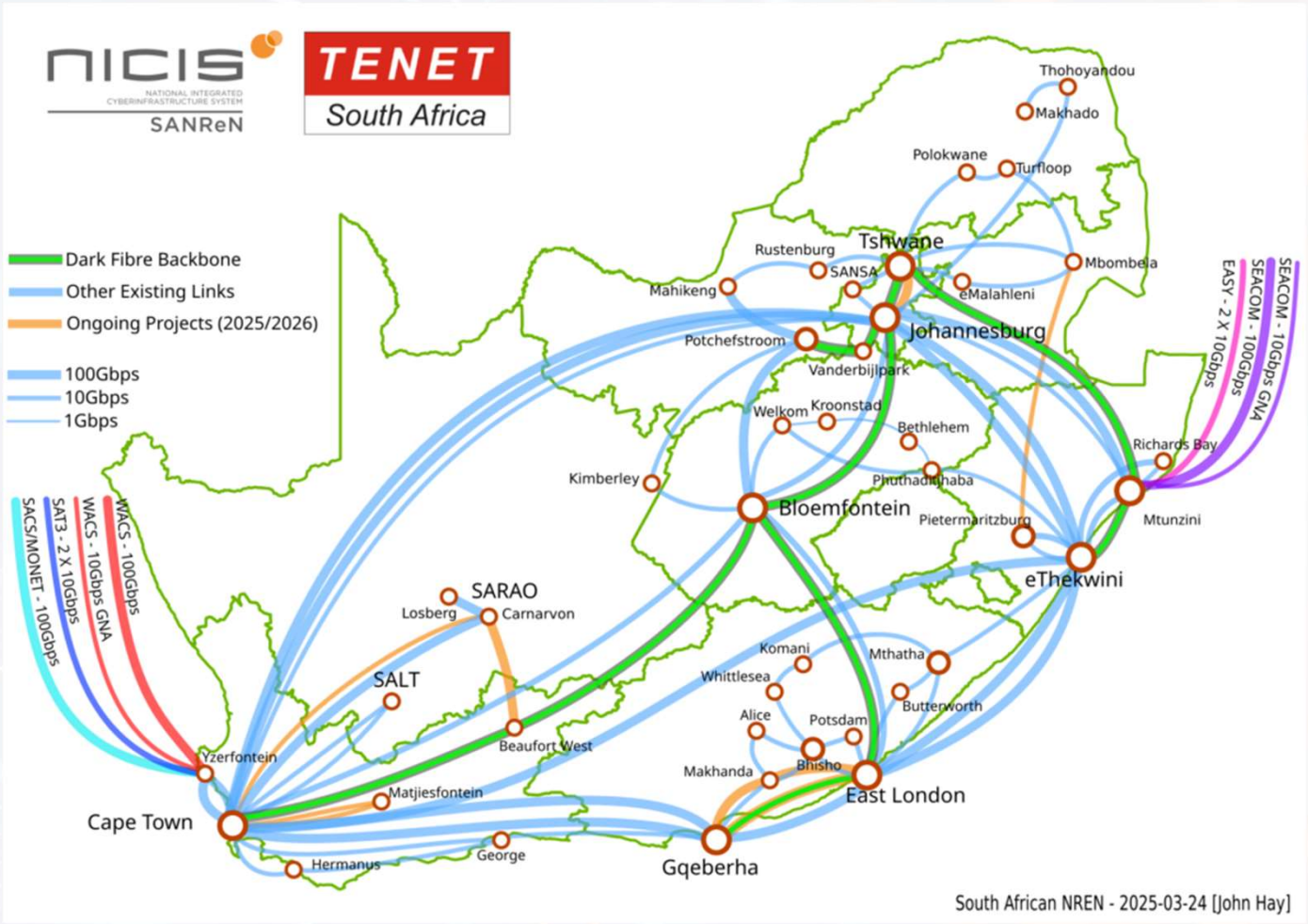
- **N**ational **R**esearch and **E**ducation **N**etworks (NRENs) are specialised network infrastructure and service providers that exclusively support a country's research, education and innovation communities.
- SA NREN
  - South African National Research Network (SANReN).
  - Tertiary Education and Research Network of South Africa (TENET).
- Currently more than 130 NRENs are active globally,
  - e.g., JISC, RNP, ZAMREN, KENET, RENU, AARNet.
- Major paradigm shift from commercial networks:
  - Provide as much bandwidth as possible at as little cost as possible,
- Quality of Service through provisioning NREN services such as
  - eduroam, Large File Transfer (PERT), identity federation (SAFIRE), CSIRT



SANReN CSIRT
Computer Security Incident Response Team

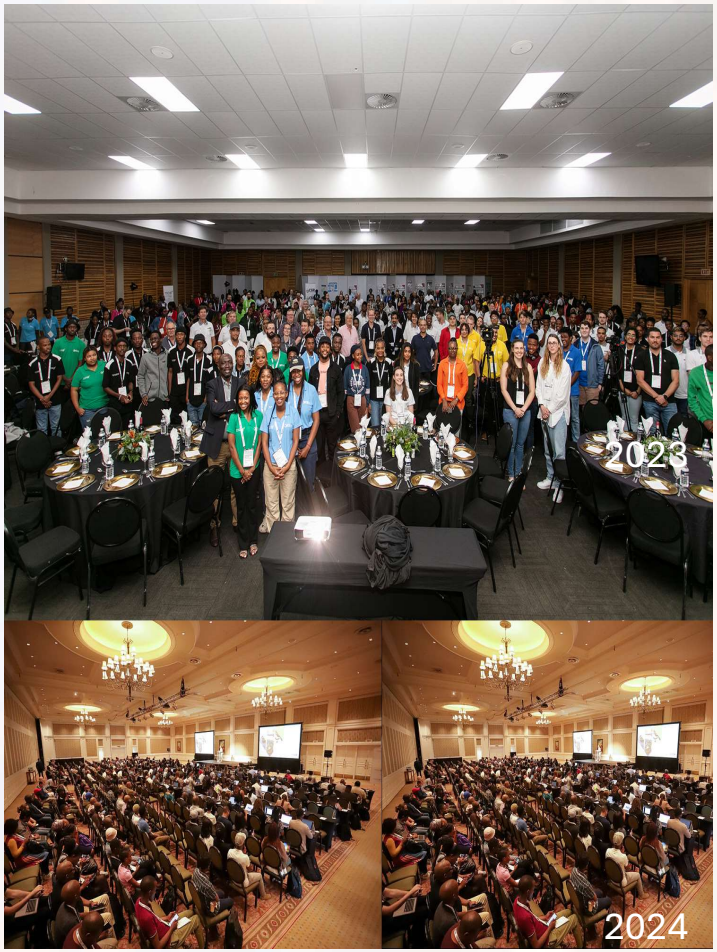
SAFIRE
FEDERATING RESEARCH & EDUCATION SYSTEMS

eduroam


NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN
TENET
South Africa
Dark Fibre Backbone
Other Existing Links
Ongoing Projects (2025/2026)
100Gbps
10Gbps
1Gbps
Thohoyandou
Makhado
Polokwane
Turfloop
Tshwane
Rustenburg
SANSA
Mbombela
Mahikeng
eMalahleni
Johannesburg
Potchefstroom
Vanderbijlpark
Welkom
Kroonstad
Bethlehem
Richards Bay
Kimberley
Phuthaditjhaba
Bloemfontein
Pietermaritzburg
Mtunzini
eThekwini
SEACOM - 10Gbps GNA
SEACOM - 100Gbps
EASY - 2 X 10Gbps
SACS/MONET - 100Gbps
SAT3 - 2 X 10Gbps
WACS - 10Gbps GNA
WACS - 100Gbps
SARAO
Losberg
Carnarvon
SALT
Komani
Mthatha
Whittlesea
Butterworth
Alice
Potsdam
Beaufort West
Yzerfontein
Makhanda
Bhisho
East London
Matjiesfontein
Cape Town
George
Hermanus
Gqeberha
South African NREN - 2025-03-24 [John Hay]

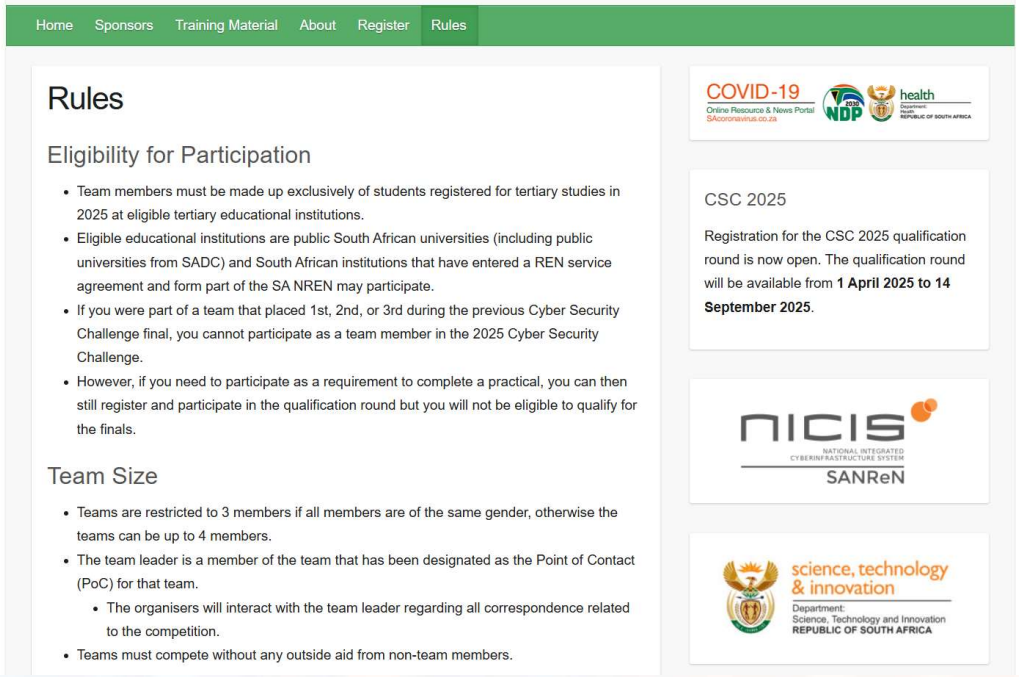
Overview: CSC 2025

- Cybersecurity challenge for all South African universities.
- Invitations extended to Universities from the SADC region.
- Why?
  - Safe environment to practice infosec (hacking) skills.
  - Learn new skills or measure your current skillset.
  - Offensive thinker – think like a hacker.
  - Improve problem-solving skills.
  - Help to think out of the box and intuitively.
  - Job, credentials.
  - Participate in the CHPC National Conference
- For more information: www.csc.ac.za



https://www.csc.ac.za/


Home
Sponsors
Training Material
About
Register
Rules
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/December 2025. At this conference, SANReN will host the seventh annual Cyber Security Challenge (CSC) competition. The purpose of the competition is to stimulate interest in Cyber Security in general, but more specifically in the field of Network Security within Southern 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 annual Cyber Security Challenge competition 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/defence competition, the teams must hack each other but also fix vulnerabilities in their own system (through patching).
Sponsored challenges that provide students with the opportunity to gain exposure to unique cybersecurity challenges.
An opportunity to conduct and experience social engineering in a controlled environment.
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 Southern Africa (including Botswana, Namibia, Eswatini and Lesotho) to compete for positions in the final. Upon completion of the qualifier rounds, the top teams will be invited to represent their university in the final at the CHPC National Conference.
COVID-19
Online Resource & News Portal
SAcoronavirus.co.za
NDP 2030
health
Department:
Health
REPUBLIC OF SOUTH AFRICA
CSC 2025
Registration for the CSC 2025 qualification round is now open. The qualification round will be available from 1 April 2025 to 14 September 2025.
NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN
science, technology & innovation
Department:
Science, Technology and Innovation
REPUBLIC OF SOUTH AFRICA
STAY SAFE
PROTECT SOUTH AFRICA
TOGETHER WE CAN BEAT THE CORONAVIRUS
CSIR
Touching lives through innovation


Home
Sponsors
Training Material
About
Register
Rules
Rules
Eligibility for Participation
Team members must be made up exclusively of students registered for tertiary studies in 2025 at eligible tertiary educational institutions.
Eligible educational institutions are public South African universities (including public universities from SADC) and South African institutions that have entered a REN service agreement and form part of the SA NREN may participate.
If you were part of a team that placed 1st, 2nd, or 3rd during the previous Cyber Security Challenge final, you cannot participate as a team member in the 2025 Cyber Security Challenge.
However, if you need to participate as a requirement to complete a practical, you can then still register and participate in the qualification round but you will not be eligible to qualify for the finals.
Team Size
Teams are restricted to 3 members if all members are of the same gender, otherwise the teams can be up to 4 members.
The team leader is a member of the team that has been designated as the Point of Contact (PoC) for that team.
The organisers will interact with the team leader regarding all correspondence related to the competition.
Teams must compete without any outside aid from non-team members.
COVID-19
Online Resource & News Portal
SAcoronavirus.co.za
NDP 2030
health
Department:
Health
REPUBLIC OF SOUTH AFRICA
CSC 2025
Registration for the CSC 2025 qualification round is now open. The qualification round will be available from 1 April 2025 to 14 September 2025.
NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN
science, technology & innovation
Department:
Science, Technology and Innovation
REPUBLIC OF SOUTH AFRICA

Registration

- Requirements:
  - Team members must be registered for tertiary studies in 2025 at eligible tertiary educational institutions.
  - Teams are restricted to 3 members if all members are of the same gender, otherwise, the teams can be up to 4 members.
  - If you were part of a team that placed 1st, 2nd, or 3rd during the 2024 CSC finals, you will not be eligible to participate in the CSC 2025 final
    - If you need to participate as a requirement to complete a practical, you can then still register and participate in the qualification round.
  - Interested teams to inform and notify their respective University Mentor – if the team is unsure who the mentor is for the University, contact the CSC organisers.

If the requirements are met, teams can complete the registration form.

Home | Sponsors | Training Material | About | Register | Rules

Register

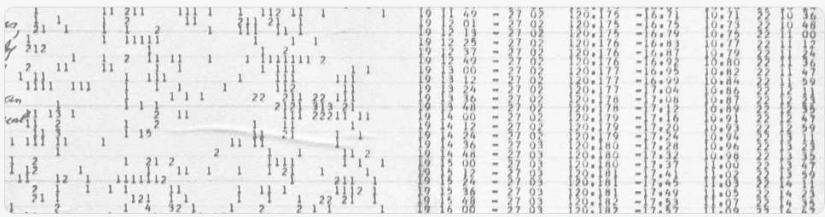
Registration for the 2025 Cyber Security Challenge is open.

Students interested should consult the Rules regarding eligibility to participate. If eligible and interested, students should form teams, select a team name and complete the registration form. Teams are also advised to reach out to their respective University Mentor to enquire about potential participation dates.

Click here to register

Participation in the 2025 CSC qualification round will close on the *14th of September 2025*.

Register



Cyber Security Challenge (CSC) 2025 Registration

Privacy Notice

All data and personal information collected during registration will be used exclusively for the organisation and execution of the SANReN Cyber Security Challenge 2025.

- All data and personal information collected will be subject to the CSIR Privacy Policy and applicable legislation.
- All data and personal information collected will be disposed of at the conclusion of the SANReN Cyber Security Challenge 2025.
- All data and personal information collected is necessary for the organisation and execution of the SANReN Cyber Security Challenge 2025.

Contact details of challenge winners will be shared with the respective challenge sponsors for delivery of prizes, if any.

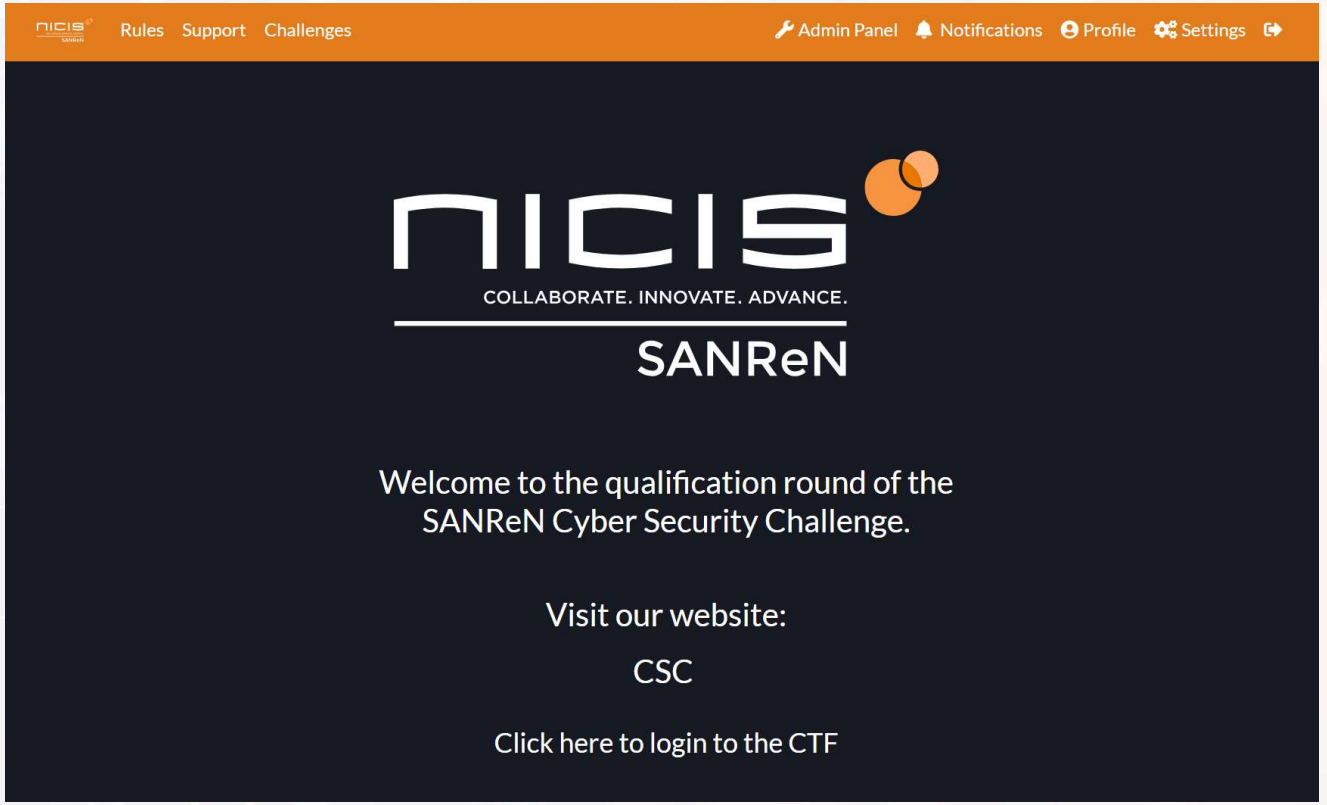
The details of challenge winners will be kept on file for a maximum of 2 years in the event that participation in additional events be required.

Additional consent will be obtained to share contact details with external 3rd parties or sponsors.

In the event that you do not have the necessary consent to share personal information, or you do not wish to share personal information, do not complete this form. You may contact the SANReN Cyber Security Challenge organisers at csc@sanren.ac.za to arrange for alternative methods for registration, if feasible.

Participation

- Qualification
- Final



Qualification

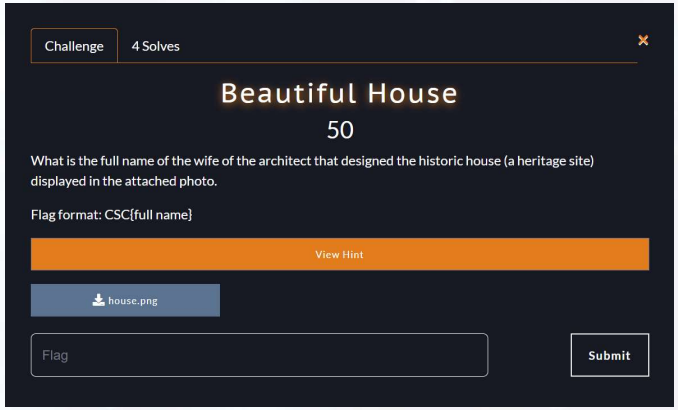
- Each team is expected to participate in the qualification round remotely.
- Qualification round will remain open for ***10 Days***.
- ***Qualification round – available options:***
  - 1 August – 10 August 2025
  - 21 August – 30 August 2025
  - 1 September – 10 September 2025
- Registered teams will receive notification via email with credentials ***on the day the qualification round opens***.
- Qualified teams are to be notified by **12 September 2025**.
- Technical support to be provided - Organisers will respond to participant queries by the next business day.
- Jeopardy-style CTF challenges.

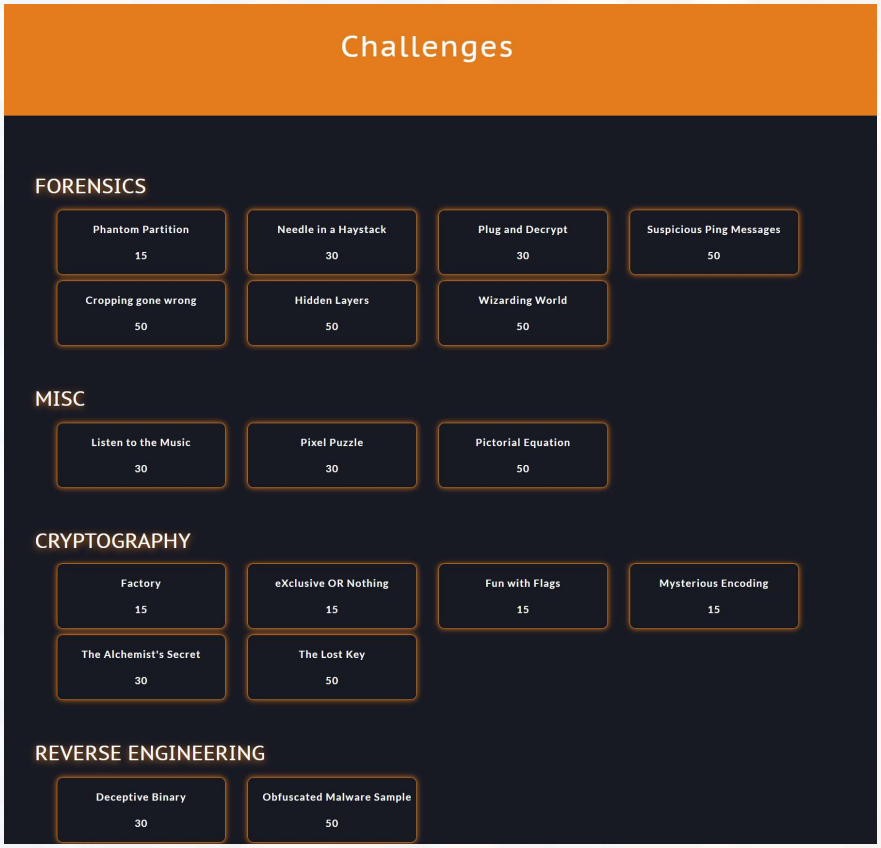
Jeopardy-styled CTF

- A collection of "*hacking*" challenges or puzzles focusing on cybersecurity.
- Often involves real and current vulnerabilities.
- Organised according to different categories such as web, forensics, cryptography, steganography, networking, and binary.
- The challenges are often sorted by difficulty levels, allowing beginners to also easily participate
- Once the team successfully solve a challenge, a "*flag*" will be revealed, which can be a specially formatted string, password, file name, etc.
- The flag can be submitted for points – points received depend on the difficulty of the challenge.
- Hints are made available for certain challenges and used by teams at their own discretion - ***Used hints will not be reversed by the organisers.***

How to solve challenges

- Click on the challenge name to see the question.
- Submit your answer to the challenge as a flag.
- Submissions are auto-marked.
- Certain flags might be case-sensitive.



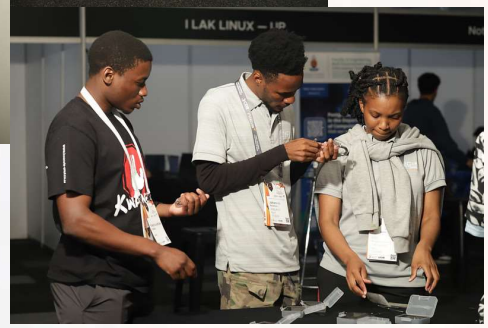


Qualification Challenges

- Bonus Challenges
- Cryptography
- MATLAB Onramp
- Forensics (Network Analysis)
- Open-source Intelligence
- Reverse Engineering (Mobile)
- Mobile Security
- Web Exploitation
- Miscellaneous

Finals

- Top 10 teams*
- Fully Sponsored by SANReN
  - Accommodation, Meals
  - Transportation (local)
- In-person event
  - 29 November to 4 December 2025
  - Venue: Century City Conference Centre in Cape Town
- Interact and Network



https://www.youtube.com/watch?v=AEZadxBgIPQ

***Please note**: *Only the top team (1) per university department can qualify for the CSC finals (a team from both the Computer Science and Engineering departments can be considered). The top team from the university department must still place in the top 10 overall (of all universities participating) in order to qualify for the CSC finals.*

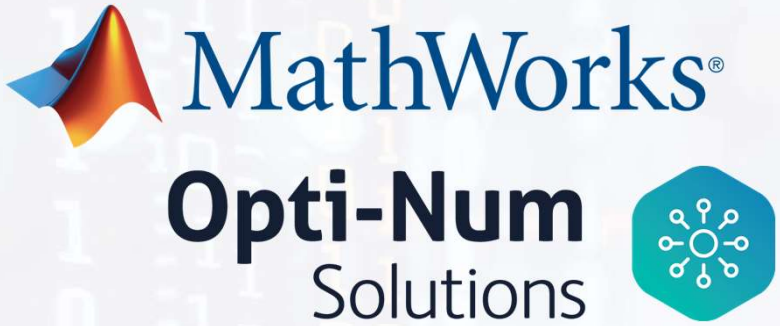
Finals

- Capture The Flag
- Attack/Defend
- Social Engineering
- Lockpicking
- Sponsored Challenges

Training Material

- Beginner's Guide
- CTF Challenge Material
  - Basic background
  - Links to write-ups of CTF Challenges
  - TryHackMe rooms
  - Tools and Resources
- CTF Introductory Training
- Discord Server: https://discord.gg/yYhyx8CeMr

Past Sponsors



Tips & Tricks for CTFs

- Do not overthink the challenge.
  - Usually, challenges have a score associated with them, which helps you determine how much effort should be invested in each challenge.
- Tools help, but often the challenges test your understanding of the concept rather than your knowledge of a tool.
  - Toolkit Arsenal: Cyberchef, Hex Editor, Burp Suite, Exiftool, Wireshark, John the Ripper, Hashcat, Kali Linux.
- Learn to spot various hash algorithms, especially base64, these encodings are often used to hide data, display binary data or encode variables.
- Unless the challenge is specifically a password challenge, passwords used in a challenge are usually related to the subject matter or can be cracked using common password lists or by basic brute force.
  - Challenges are made to be solved in a short period of time.
  - If this still does not work, you might have overlooked some other clue in the challenge.
- Golden rule of CTF
  - Practice, practice, practice…
- *"don't forget during a CTF, Google is your friend… or ChatGPT"*

Thank You – Q&A

Email: heloise@sanren.ac.za

NICIS
NATIONAL INTEGRATED CYBERINFRASTRUCTURE SYSTEM
SANReN