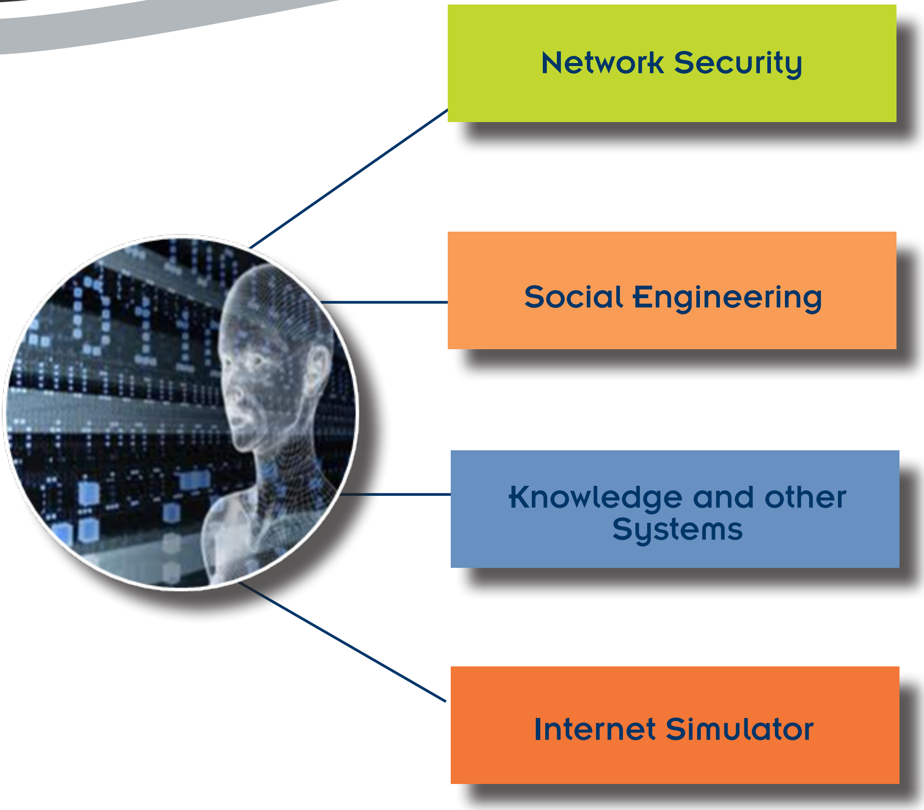
Focus on CSIR services in
Cyber Defence Research

Your research, development and innovation partner in cyber defence



Network Security

- Tools: Offensive and Defensive
- Threats & Trends
- Network Perimeter Defence
- Network Security Incident Management
- Cybersecurity awareness

Social Engineering

- Behaviour influencing
- Social Network Information Exploitation

Knowledge and other Systems

- Morphological analysis Semantic Technologies
- Cyber Security Policy, Standards & Implementation

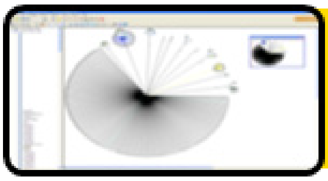
Internet Simulator

- System Testing
- Attack predictions
- System simulations
- Tool development

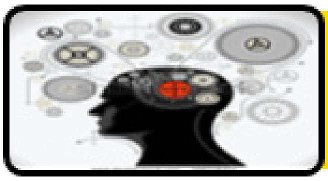
CSIR

our future through science

The CSIR's Cyber Defence Research Group is a national capability with a track record as an independent, unbiased strategic Science, Engineering and Technology partner. We develop and operate R&D infrastructure and cutting edge competence and intellectual property for the security cluster.



Predicting network attacks. The purpose of this research is to identify and model unauthorised access and attacks on cyber networks. The aim is to mitigate networks attacks. The internet simulator is used to study the effects of network traffic on large-scale networks and network-connected equipment in a closed environment not exposed to external monitoring.

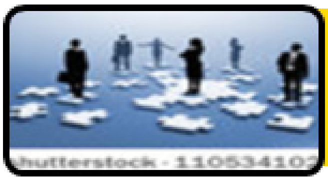


Preventing and Mitigating Social Engineering Attacks. Models are provided that are used to analyse social networks, to harvest online data that is used to predict online behaviour, to prevent and mitigate social engineering.

Knowledge Systems Development : Decision support services are provided through structuring complex problem spaces and developing shared knowledge representation. The group uses highly skilled facilitators using own developed software aided resources to facilitate diverse groups.

Awareness. To create a cyber savvy citizens, the CSIR has engaged developed a cyber security awareness programme that has been delivered to ordinary communities across the country. The programme is designed for learners, parents, and professionals. Through the project, the grouped has forged collaborations with universities and communities (rural and urban).

Auditing. To ensure that standards, policies and procedure are adhered to, the Blue Team audits network, while the Red Team searches for any network vulnerabilities and configuration errors.



Expertise. Diverse expertise exists in fields such as software development, project management, computer science, operations research, forensics, group facilitation, psychology, and cyber security policy development. A number of staff members are Certified Information Systems Security Professional (CISSP) and have Security Clearances.

Cyber defence research, development and innovation solutions in support of joint operations

Contact details

Joey Jansen van Vuuren
JJvVuuren@csir.co.za
012 841 4194

dpss@csir.co.za

CSIR
our future through science