IDEAS THAT WORK FOR INDUSTRIAL DEVELOPMENT

CSIR work on improving cybersecurity for the South African industry

Dr BJE Taute

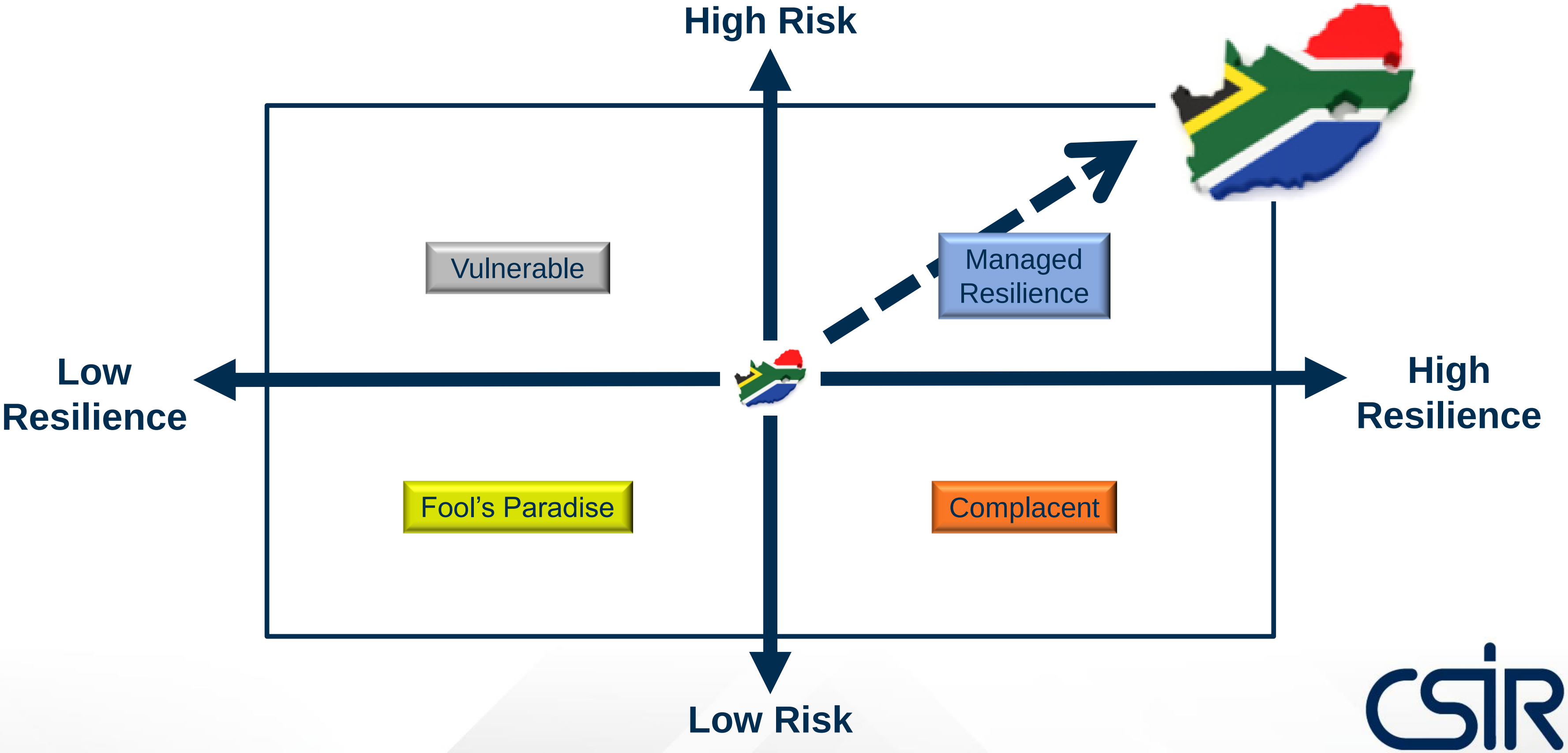
6 October 2017

CSIR

our future through science

How cyber-resilient is South Africa?

Vision: *South Africa is resilient even against high cybersecurity risk and threat levels*



our future through science

Cybersecurity research and innovation includes

Understanding the threats
Developing

- technical expertise,
- security standards,
- integrated security solutions,
- processes to identify, protect, detect, respond and if all else fails
- the ability to recover from cyber-attacks

IDEAS THAT WORK FOR
INDUSTRIAL
DEVELOPMENT

CSIR track record

CSIR
our future through science

Cybersecurity at the CSIR

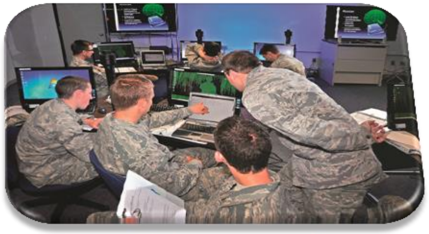
The CSIR has a track record of working with government departments and industries to

- write policy and strategy,
- enable smart buying decisions,
- build capacity and infrastructure,
- develop cybersecurity technology and tools,
- share threat intelligence, and
- respond to cyber attacks.

CSIR cybersecurity RDI focus areas

A - Securing ICT Systems

B - Combating Cybercrime



C - Cyberwarfare

D - Identity Management

E - Awareness & HCD

F - Governance, Risk & Compliance

G - Embedded Security

Key R&D partnerships for implementation of the National Cybersecurity Policy Framework (2015)

Defence, State Security

- Information warfare, cyber defence, strategy

Telecommunications & postal services

- Policy, advisory, National Cybersecurity Hub support

Science and Technology

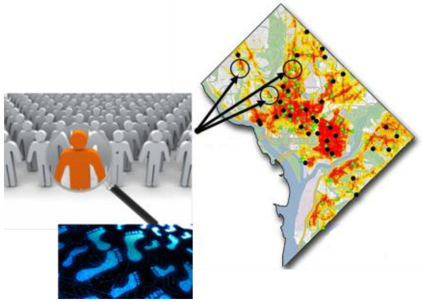
- Masters, PhDs, National RDI Programme
- Research infrastructure, research projects

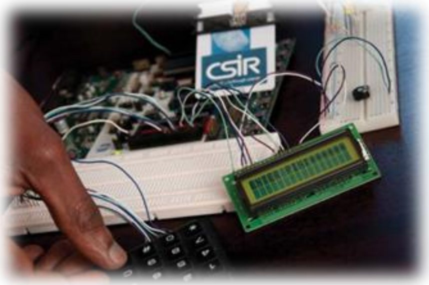
Police

- Investigation, evidence, forensics, training, strategy

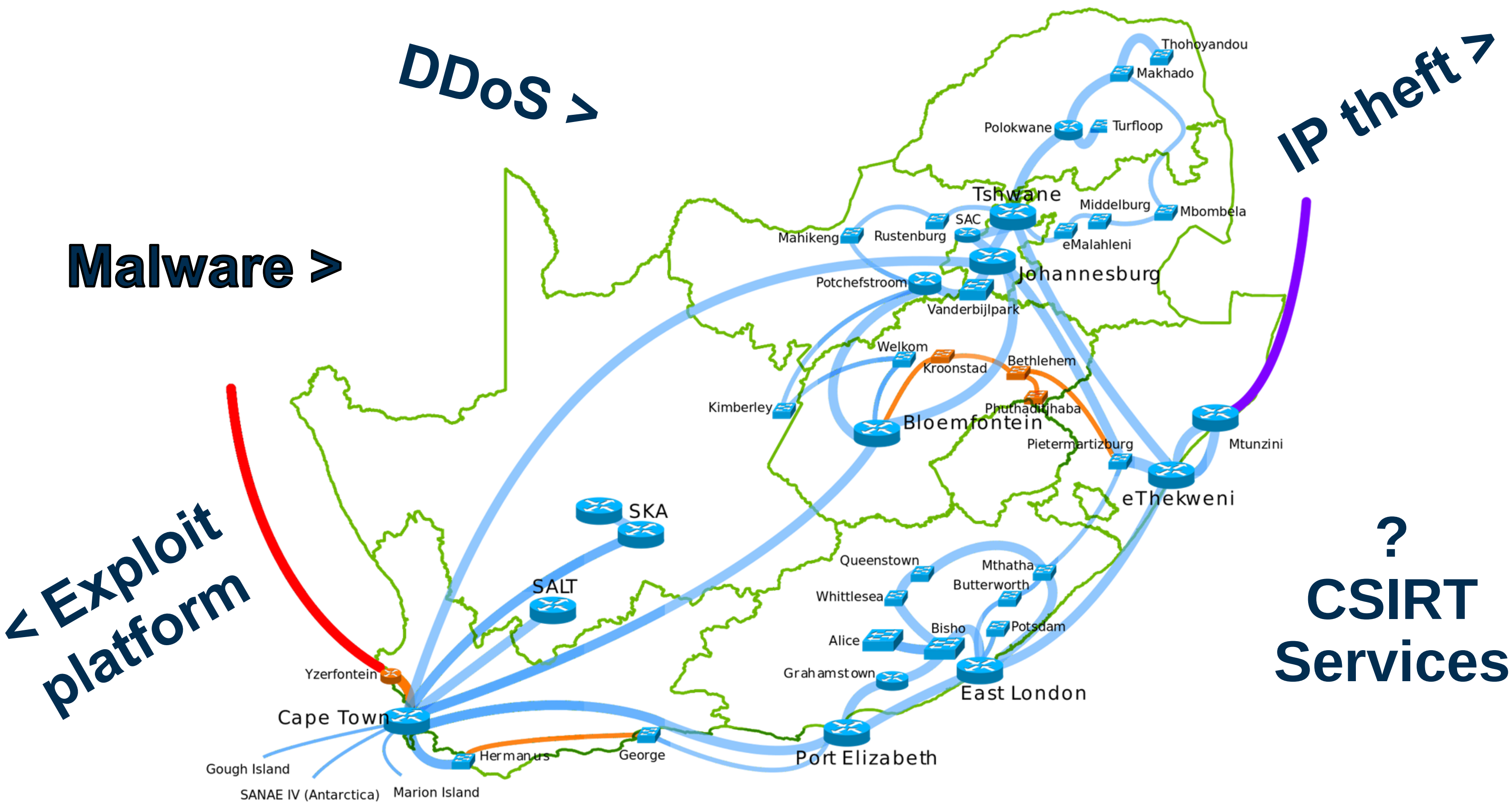
Other Sectors

- National identity system (Home Affairs, SITA)
- Biometrics and smart cards (Home Affairs, PASA)
- Health information exchange security architecture
- Cyber legislation (Justice)
- E-commerce policy and devices (FSB, PASA)





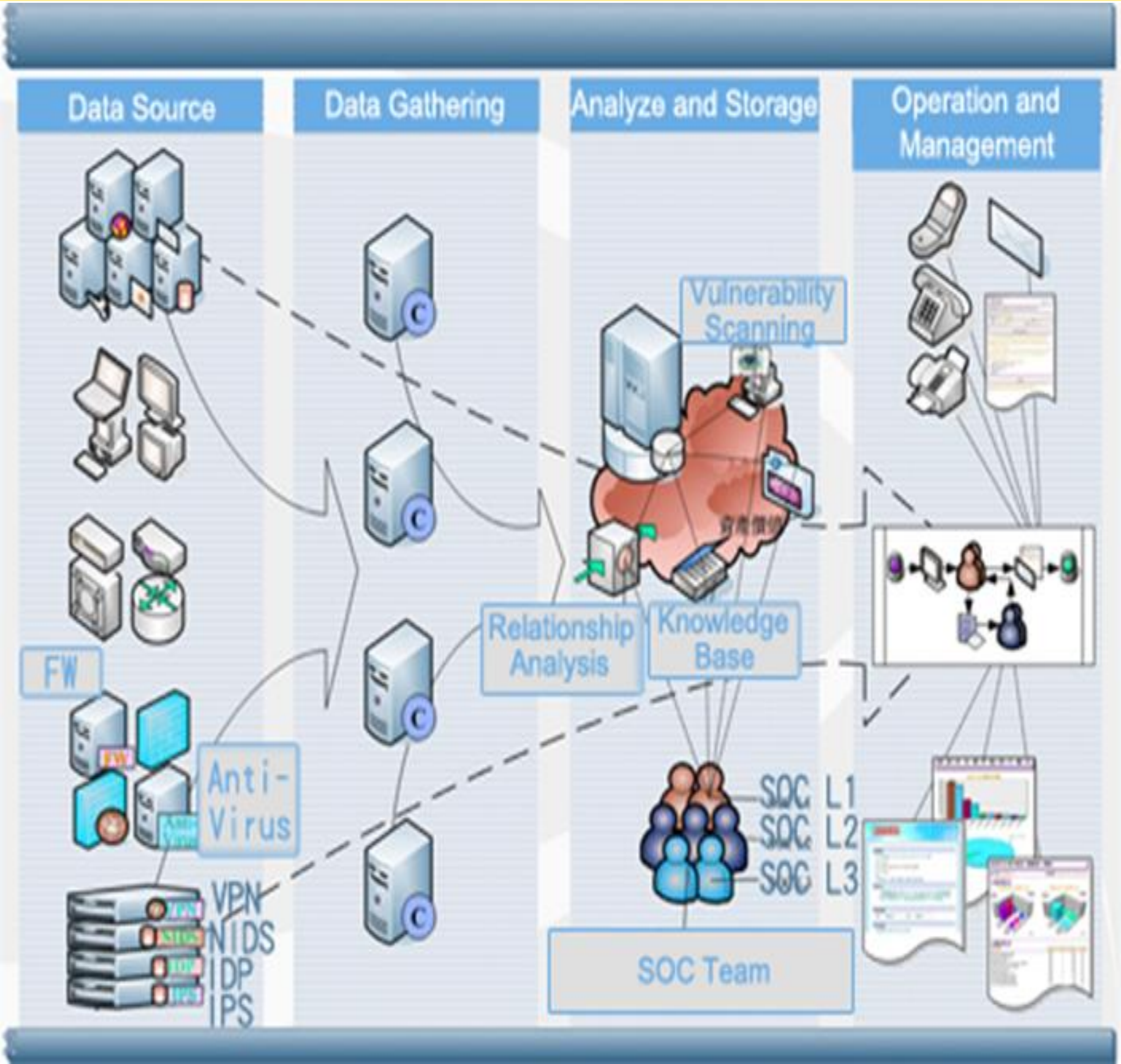
A Computer Security Incident Response Team (CSIRT) for SANReN



? CSIRT Services

Malware >

Security Operations and Security Operation Centres (SOC)

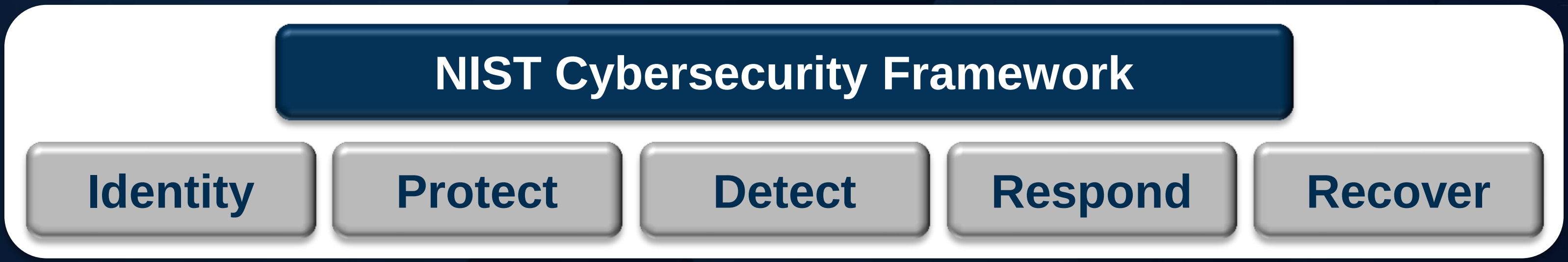


Design, implementation, validation and verification of SOCs

IDEAS THAT WORK FOR INDUSTRIAL DEVELOPMENT

CSIR research infrastructure

Ready to support and collaborate with industry ….. to



NIST Cybersecurity Framework

Identity

Protect

Detect

Respond

Recover

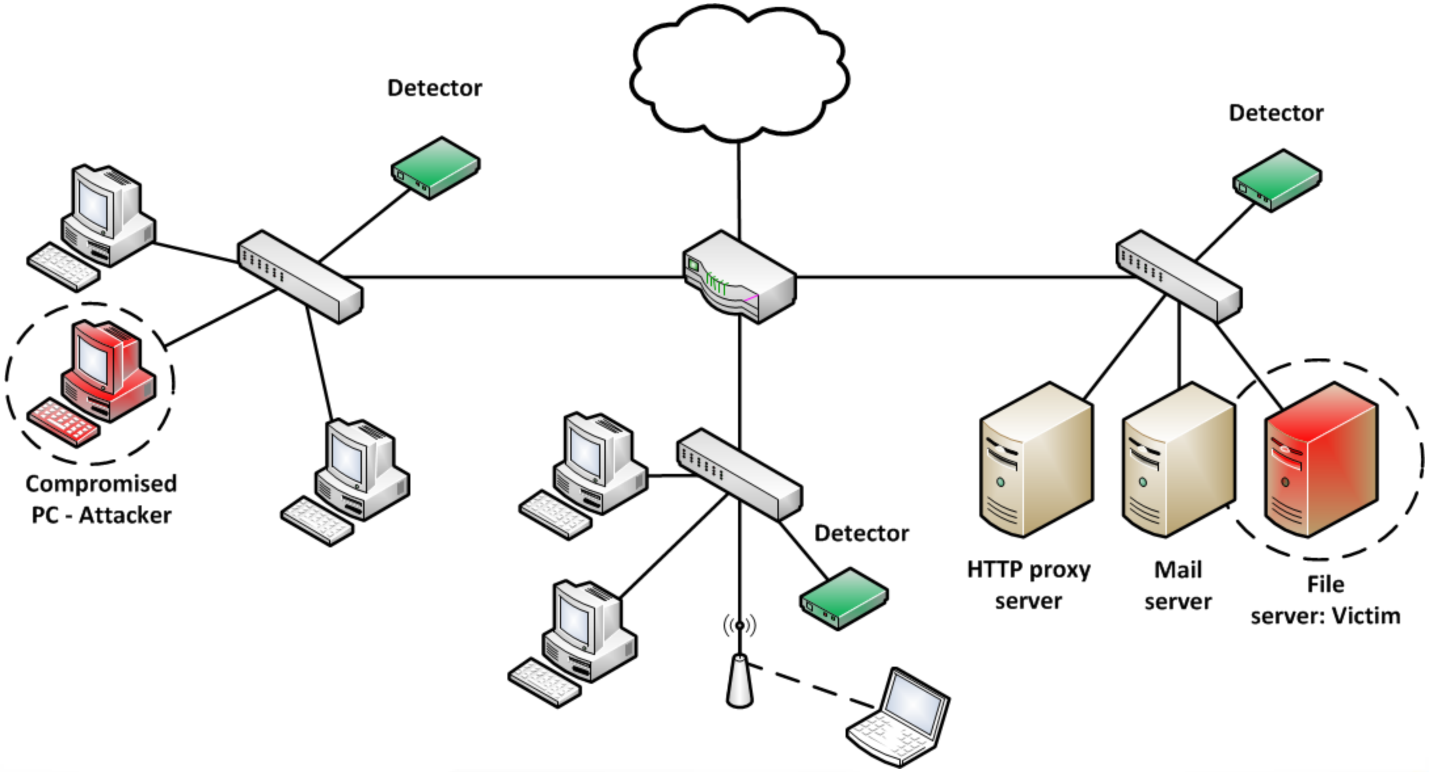
CSIR

our future through science

Early warning detection technology

IDEAS THAT WORK FOR INDUSTRIAL DEVELOPMENT

East - west cyberattacks – intranet - anomaly detection – during reconnaissance phase

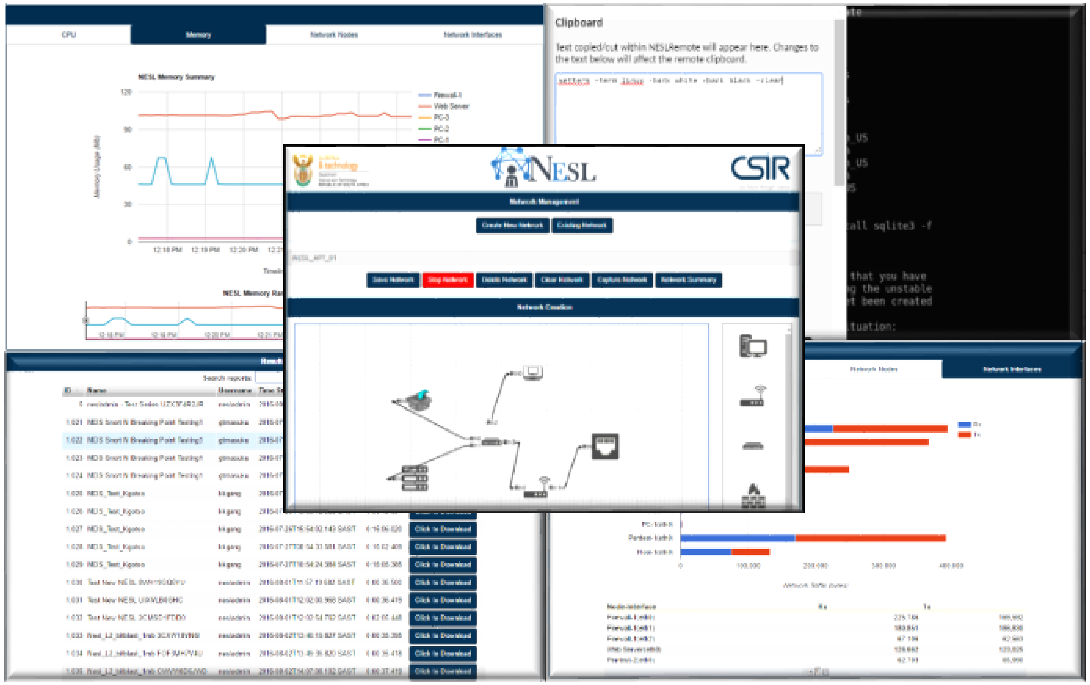


CSIR
our future through science

Network Emulation and Simulation Laboratory (NESL)

IDEAS THAT WORK FOR INDUSTRIAL DEVELOPMENT

Creating, assessing and deploying complex networks, cost-effective, timely



Clipboard

Text copied/cut within NESLRemote will appear here. Changes to the text below will affect the remote clipboard.

Infrastructure funding supported by DST

science & technology
Department:
Science and Technology
REPUBLIC OF SOUTH AFRICA

CSIR
our future through science

NESL Platform - Capabilities

- Web-based application – remote + isolated
- Multi-tenanted environment - concurrently
- Deployment of custom applications
- Realistic network traffic generation
- Flexibility - client use cases

Host

Firewall

Lightweight Switch

OpenVSwitch

Router

PC

Ubuntu Repo

Virtual Machine

Pentest VM

Vulnerable Webserver

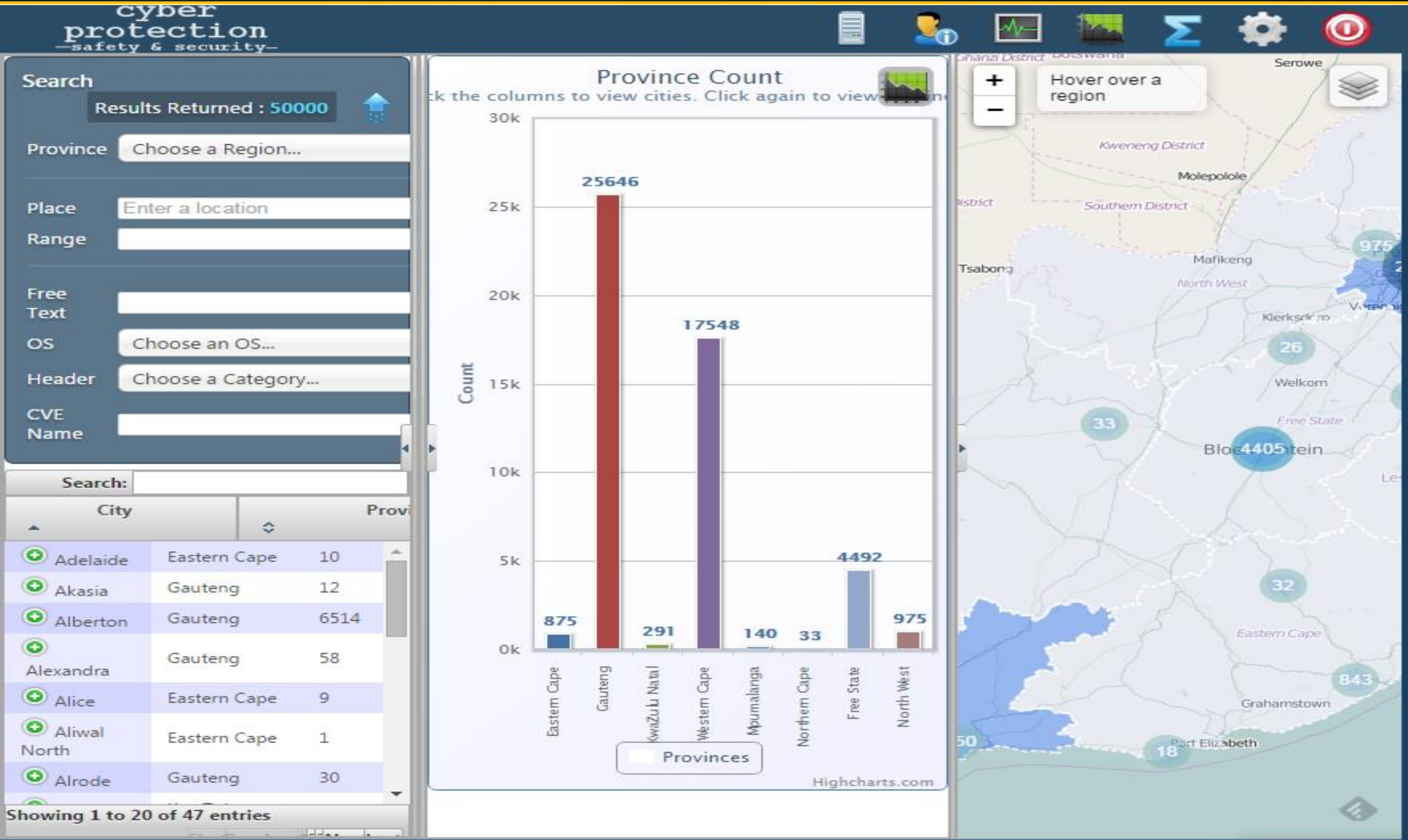
Eport

Cyber Protect - 1

Find device vulnerabilities on the internet

SCADA

Cyber Protect – Device vulnerabilities



Search

Results Returned : 50000

Province: Choose a Region...

Place: Enter a location

Range:

Free Text:

OS: Choose an OS...

Header: Choose a Category...

CVE Name:

Search:

City	Provi	
Adelaide	Eastern Cape	10
Akasia	Gauteng	12
Alberton	Gauteng	6514
Alexandra	Gauteng	58
Alice	Eastern Cape	9
Aliwal North	Eastern Cape	1
Alrode	Gauteng	30

Showing 1 to 20 of 47 entries

Cyber Protect - 2

Find Personal Identifiable Information (PII) being disclosed on the internet

LEGEND

SOCIAL SECURITY NUMBER

CONTACT INFORMATION
(email address, physical address, telephone and mobile numbers)

GOVERNMENT-ISSUED IDENTIFICATION
(driver’s license, passport,
birth certificate, library card)

BIRTH DATE, BIRTH PLACE

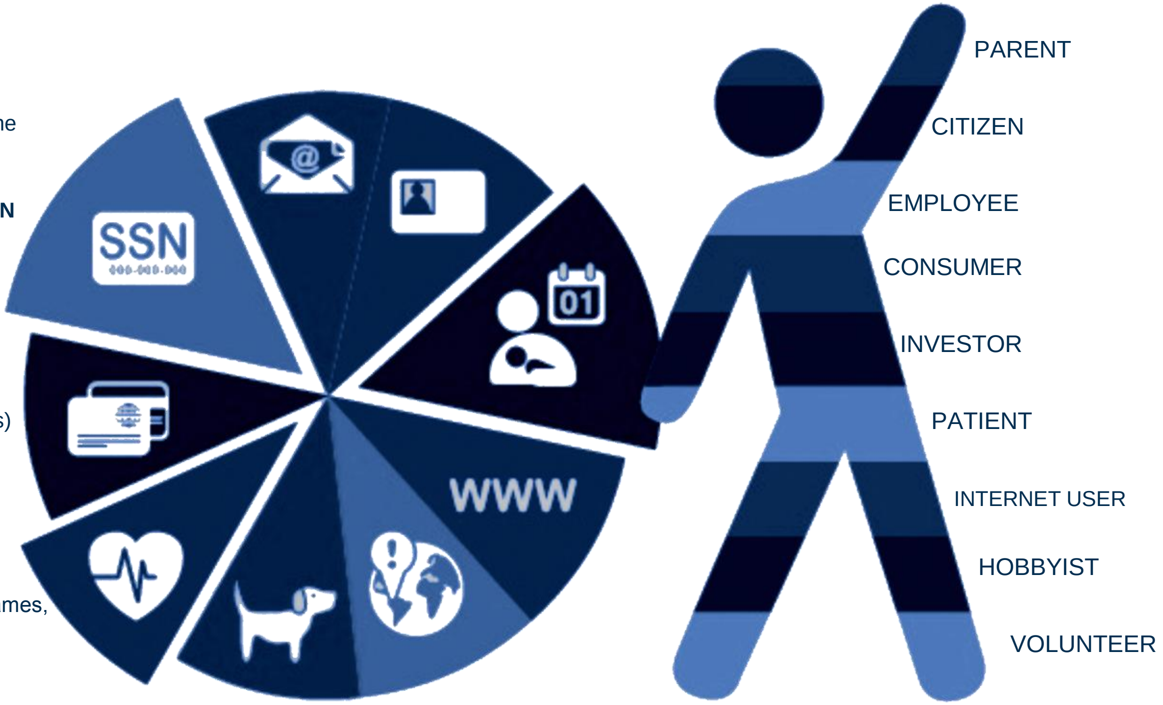
ONLINE INFORMATION
(Facebook, social media, passwords, PINs)

GEOLOCATION
(smartphone, GPS, camera)

VERIFICATION DATA
(mother’s maiden name, pets’ and kids’ names,
high school, passwords)

MEDICAL RECORDS INFORMATION
(prescriptions, medical records, exams, images)

ACCOUNT NUMBERS
(bank, insurance, investments, credit cards)



PARENT

CITIZEN

EMPLOYEE

CONSUMER

INVESTOR

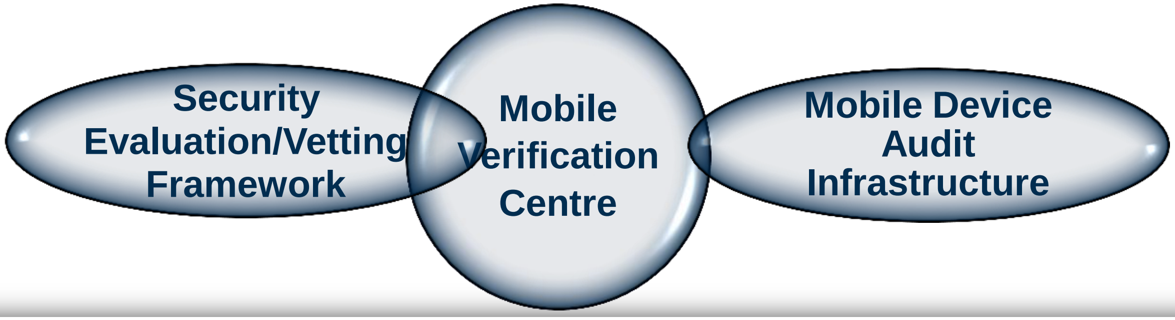
PATIENT

INTERNET USER

HOBBYIST

VOLUNTEER

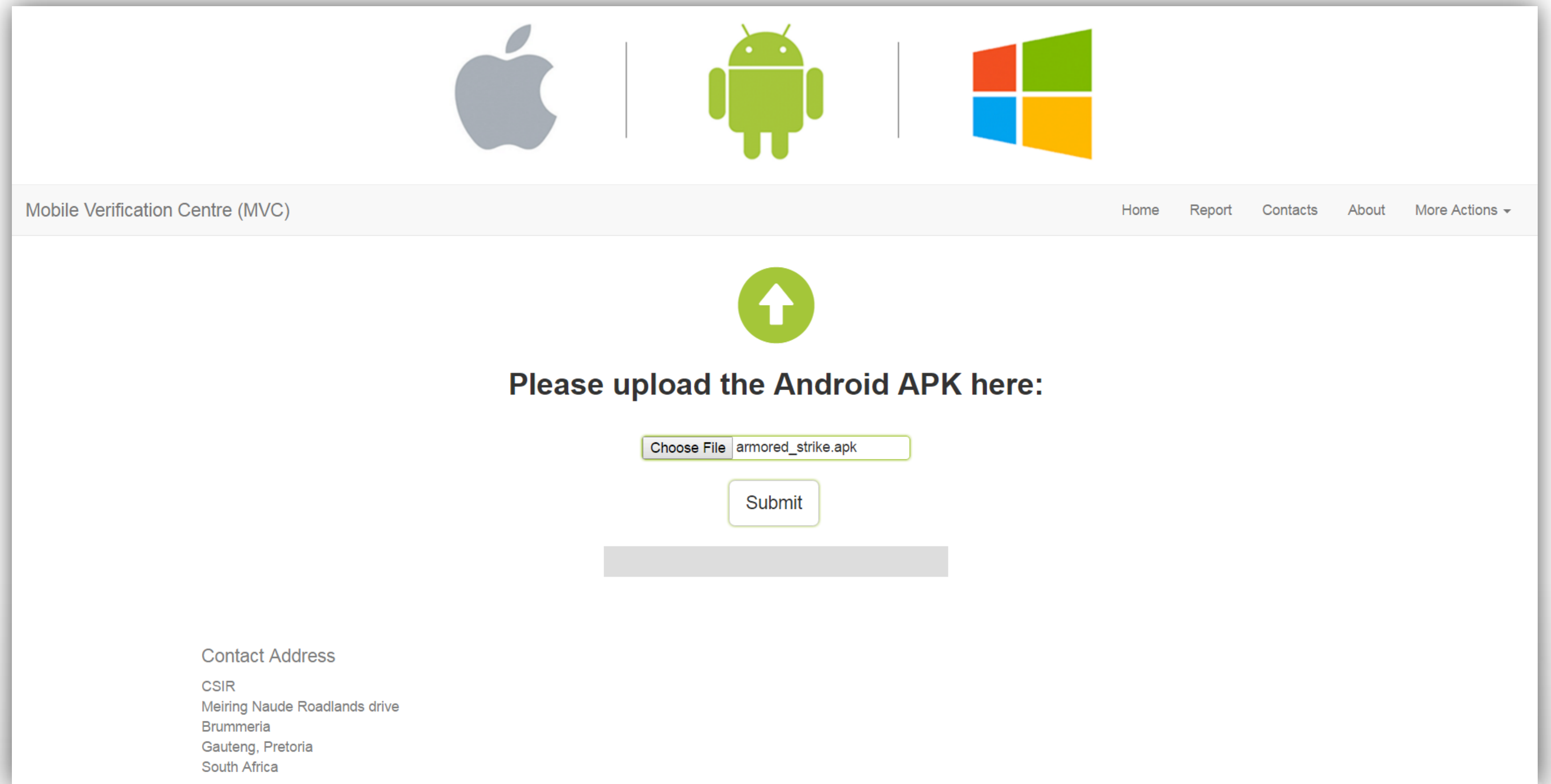
Mobile Verification Centre



Security Evaluation/Vetting Framework

Mobile Verification Centre

Mobile Device Audit Infrastructure



Please upload the Android APK here:

armored_strike.apk

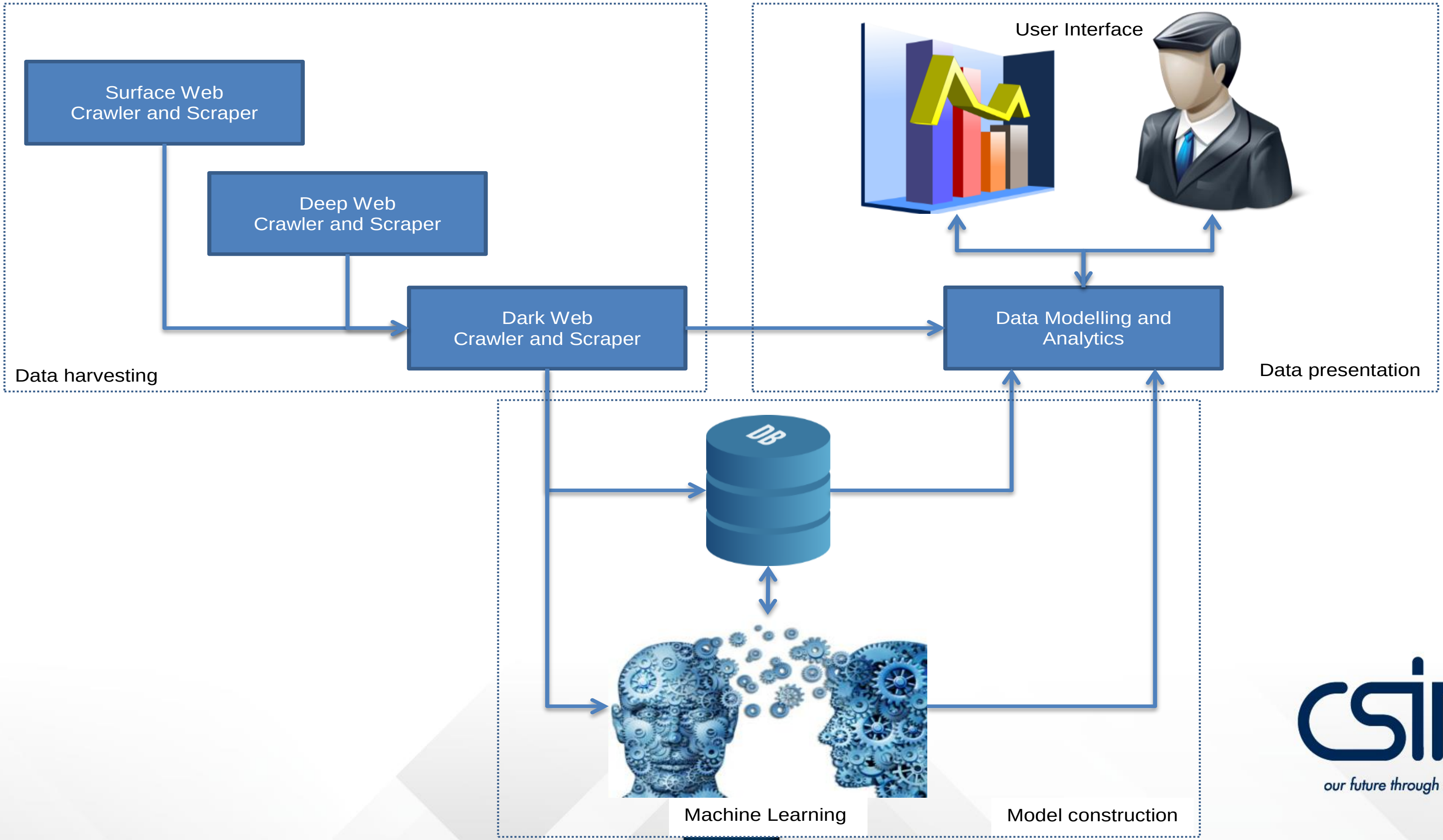
Contact Address

CSIR
Meiring Naude Roadlands drive
Brummeria
Gauteng, Pretoria
South Africa

Cybercrime Combating Platform – C3P

IDEAS THAT WORK FOR INDUSTRIAL DEVELOPMENT

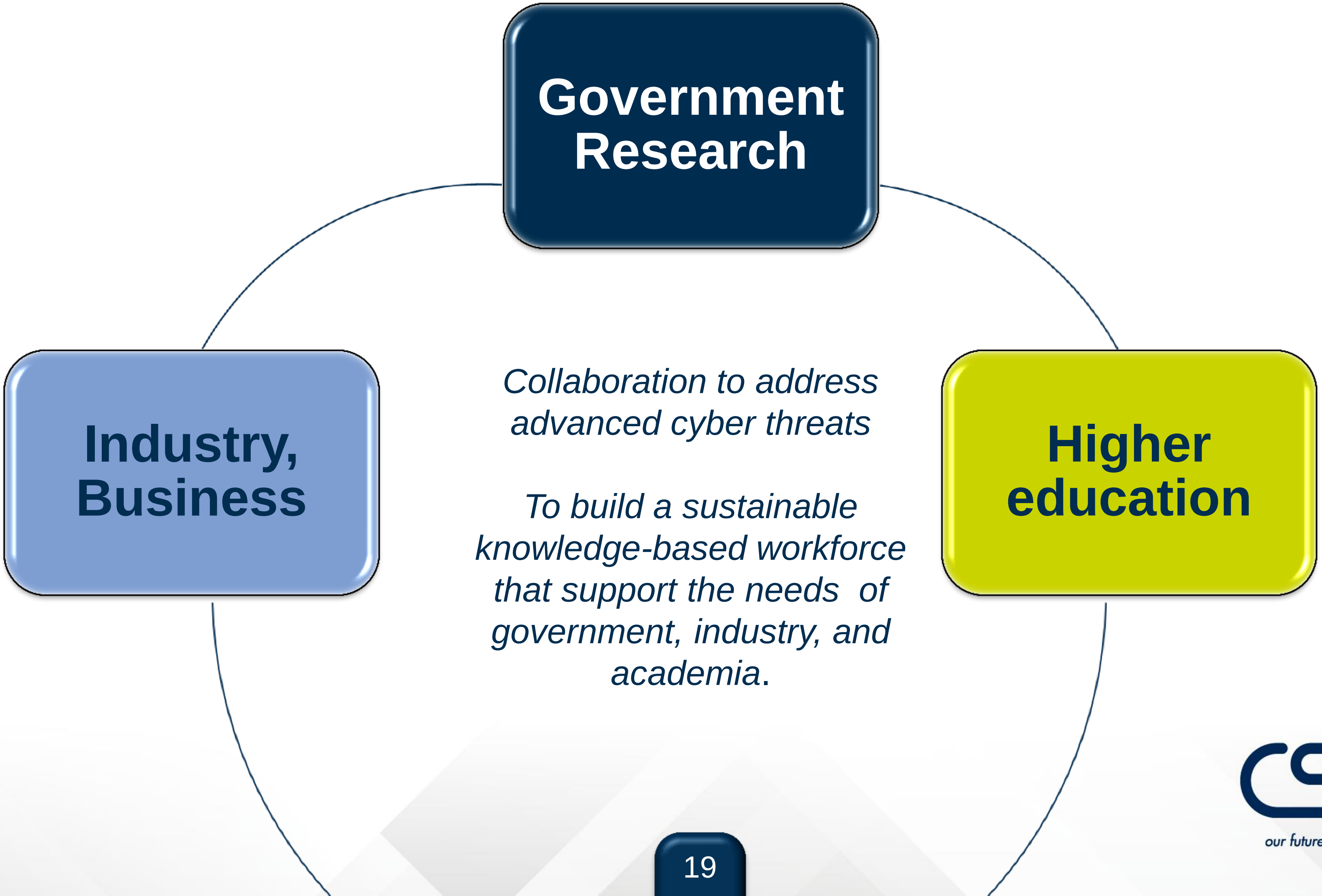
Dark web data collection



User Interface
Surface Web Crawler and Scraper
Deep Web Crawler and Scraper
Dark Web Crawler and Scraper
Data Modelling and Analytics
Data harvesting
Data presentation
DB
Machine Learning
Model construction

CSIR
our future through science

Cybersecurity Centre for Innovation South Africa



Government Research

Industry, Business

Higher education

Collaboration to address advanced cyber threats

To build a sustainable knowledge-based workforce that support the needs of government, industry, and academia.

Let’s collaborate for a safer RSA

CSIR is ready to support industrial and national cybersecurity and resilience through

- implementable policies and strategies,
- smart buyer support,
- building capacity and infrastructure,
- developing cybersecurity technology and tools,
- sharing threat intelligence, and
- responding to attacks.

Questions to the panel:

1. Is the South African industry prepared for the threats in cyberspace?
2. What is lacking?
3. What research, development and innovation is needed beyond current solutions?

Contact us ….

A - Securing ICT Systems

B - Combating Cybercrime

C - Cyberwarfare

D - Identity Management

E - Awareness & HCD

F - Governance, Risk & Compliance

G - Embedded Security

Alex Lucouw alucouw@csir.co.za (A)
Christo Coetzer ccoetzer2@csir.co.za (A)
Roderick Mooi rmooi@csir.co.za (A)
Dr Joey J van Vuuren jjvvuuren@csir.co.za (B, E, F)
Dr Jabu Mtsweni jmtsweni@csir.co.za (C, G)
Rethabile Khutlang rkhutlang@csir.co.a (D)
Prof Nkqubela Ruxwana nruxwana@csir.co.za (E, F)