SANReN
South African National
Research Network

CSIRT
Information
Security

South African National Research Network (SANReN)

CSIRT Update

Roderick Mooi – CSIRT Manager

roderick@sanren.ac.za

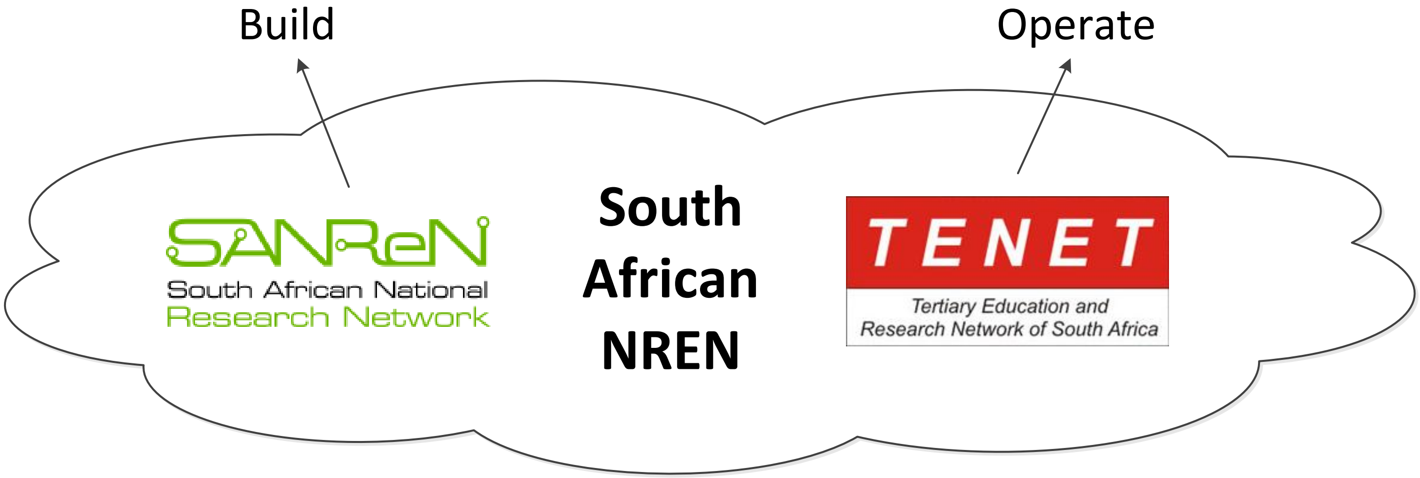
csirt.sanren.ac.za

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

12 February 2018
6th SIG-ISM Workshop

CSIR
our future through science

SA NREN
(simplified)



Background - 2012

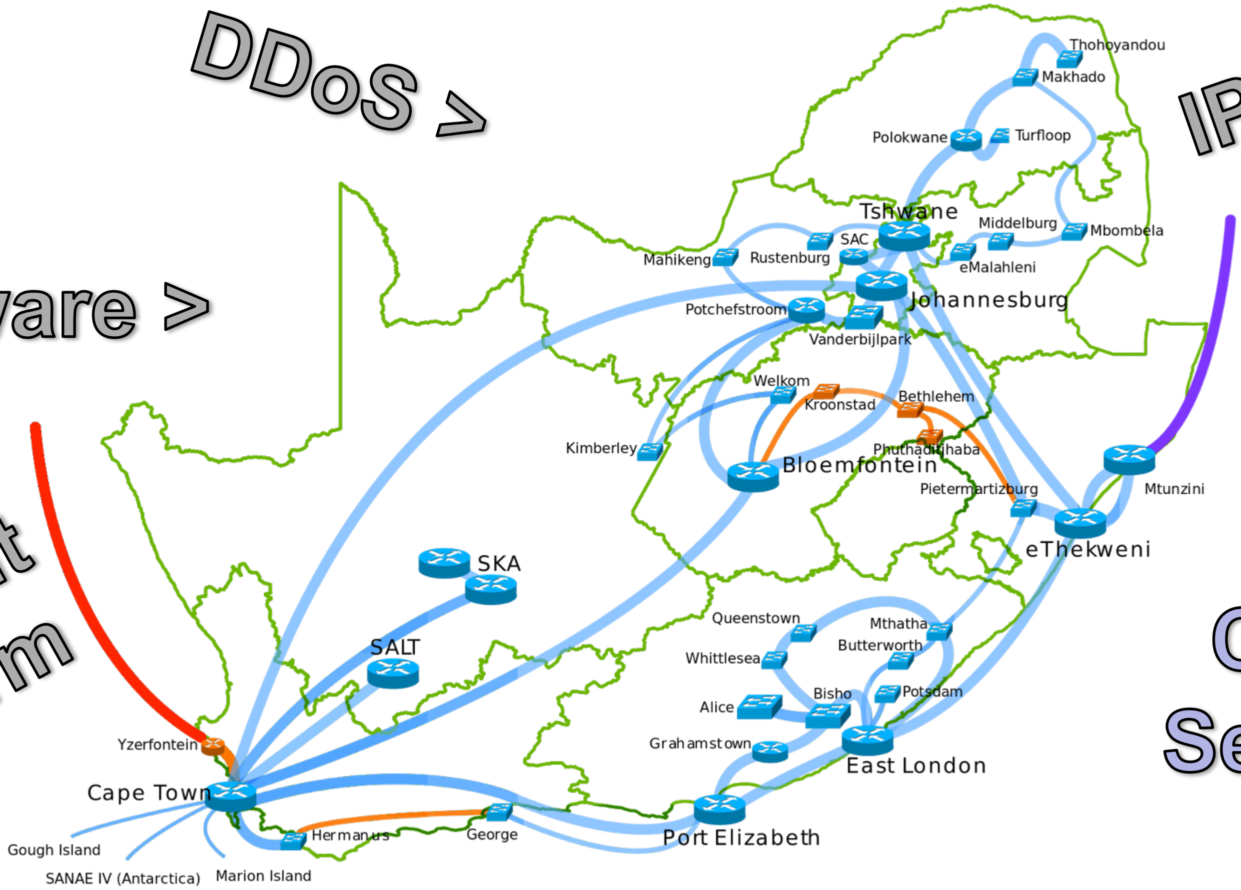
We *think* we need a CSIRT – but where to start?

DDoS >

Malware >

< Exploit platform

IP theft >

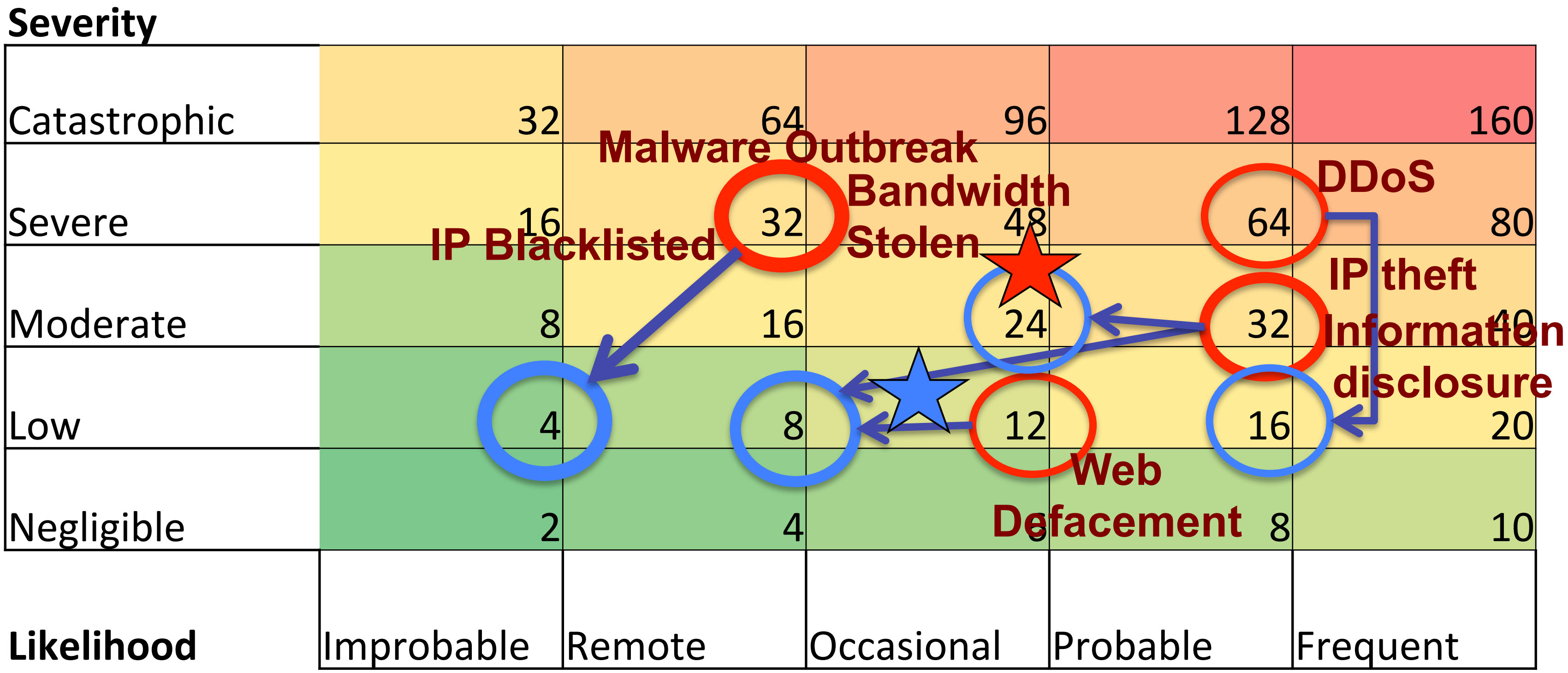


?

CSIRT Services

Impact/effect of a CSIRT

Community workshop – May 2015



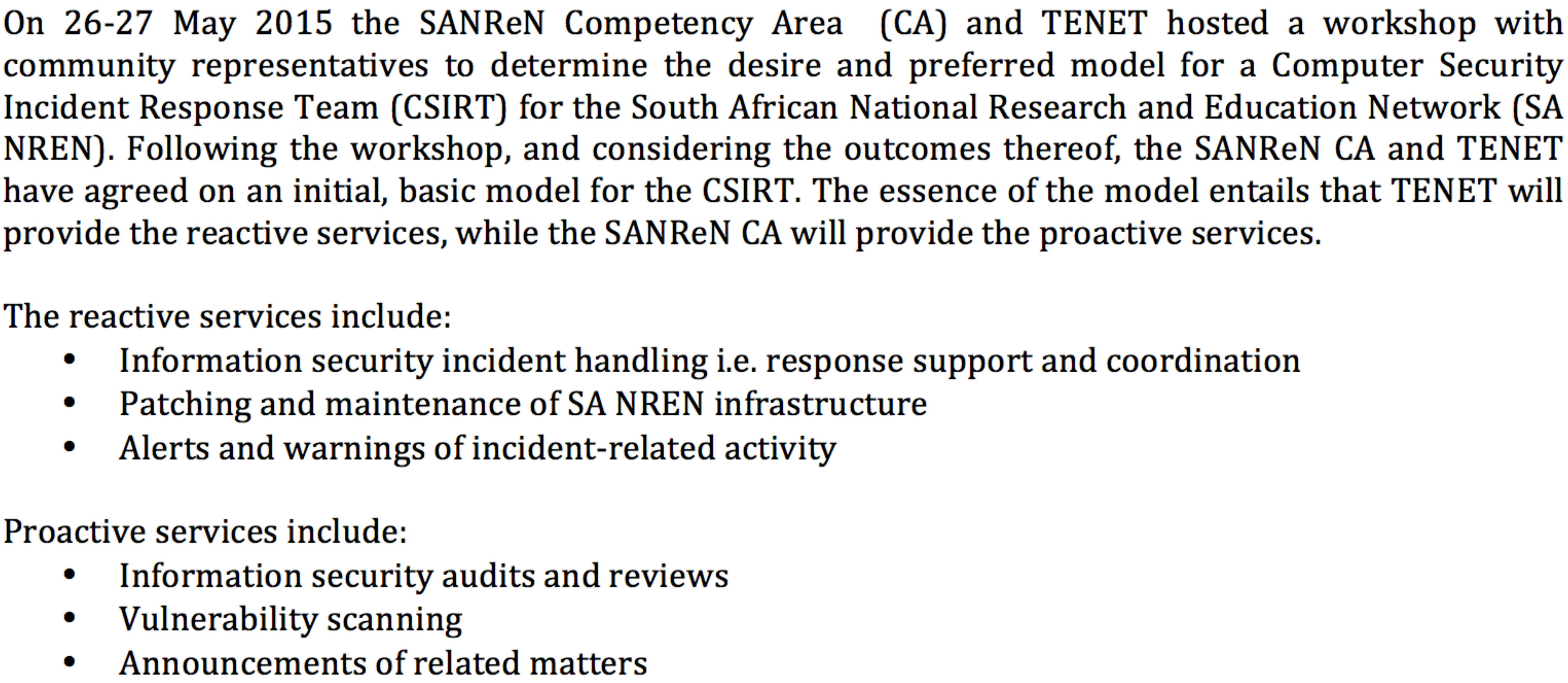
Severity					
Catastrophic	32	64	96	128	160
Severe	16	32	48	64	80
Moderate	8	16	24	32	40
Low	4	8	12	16	20
Negligible	2	4	6	8	10
Likelihood	Improbable	Remote	Occasional	Probable	Frequent

Average ★ 32 → 10 ★

SA NREN CSIRT	Independent	TENET Embedded	**TENET and SANReN**	Distributed	**Minimal**
Announcements	X	X	**X**	X	**X**
Technology watch	X	X	**X**	X	**X**
Security Audits	X	X	**X**		
Security Tools	X	X			
Alerts and warnings	X	X	**X**	X	**X**
Incident handling: Coordination	X	X	**X**	X	**X**
Incident handling: Support	X	X	**X**	X	
Incident handling: Response on site	X				
Security consulting	X	X	**X**	X	
Training	X	X	**X**		
Staffing (FT / PT)	8	4 + 4	**3 + 5**	2 + 6	**0 + 2**

“Official” launch

14 March 2016



On 26-27 May 2015 the SANReN Competency Area (CA) and TENET hosted a workshop with community representatives to determine the desire and preferred model for a Computer Security Incident Response Team (CSIRT) for the South African National Research and Education Network (SA NREN). Following the workshop, and considering the outcomes thereof, the SANReN CA and TENET have agreed on an initial, basic model for the CSIRT. The essence of the model entails that TENET will provide the reactive services, while the SANReN CA will provide the proactive services.

The reactive services include:

- Information security incident handling i.e. response support and coordination
- Patching and maintenance of SA NREN infrastructure
- Alerts and warnings of incident-related activity

Proactive services include:

- Information security audits and reviews
- Vulnerability scanning
- Announcements of related matters

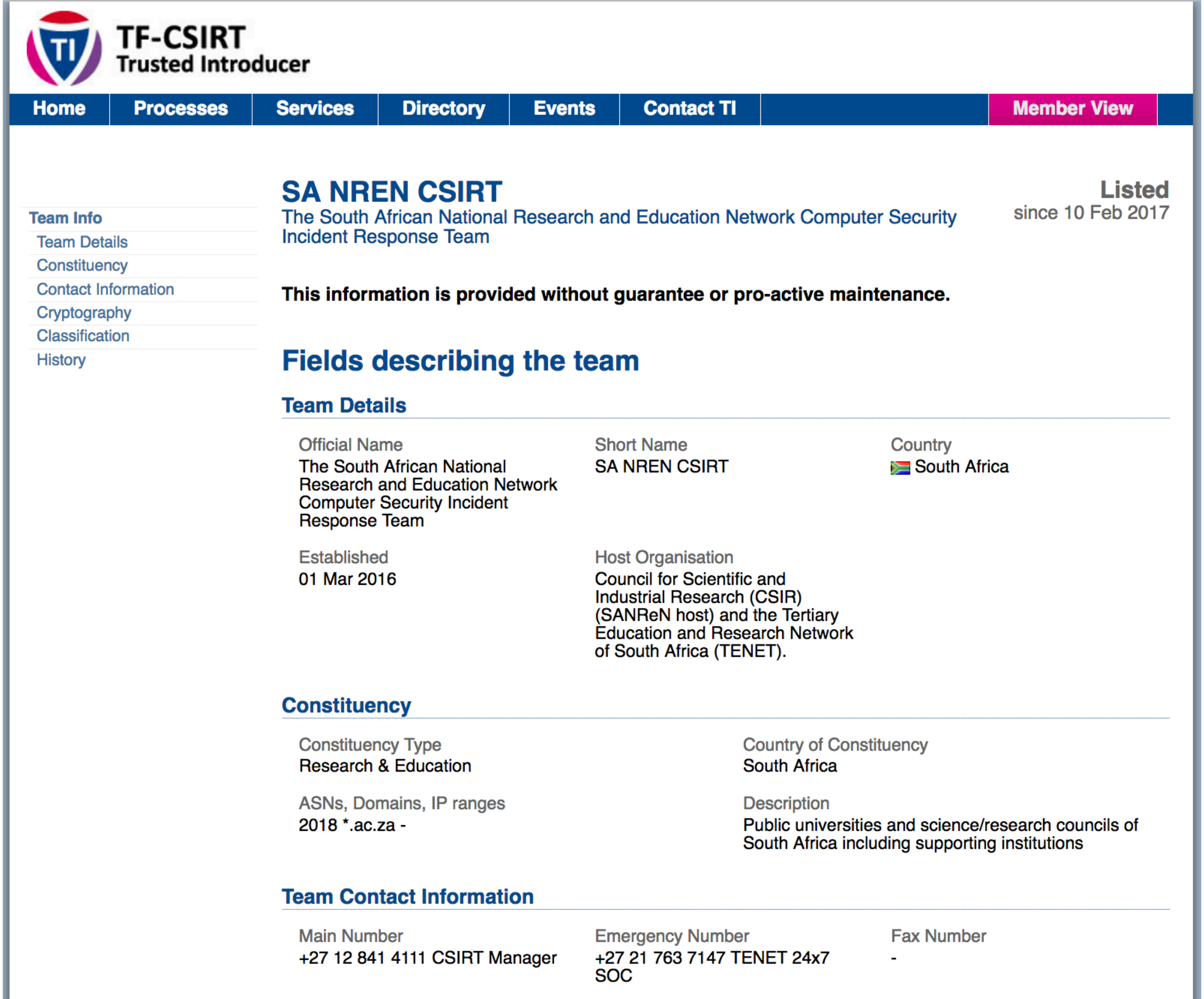
SANReN CSIRT

Mission, etc.

(for now)

The SANReN CSIRT is a proactive, academic sector, coordinating CSIRT. We provide services and support to the beneficiaries and customers of the South African National Research and Education Network (NREN) for preventing and responding to IT security incidents.

Our constituency includes the South African public universities, science councils, research organisations and supporting institutions (AS 2018 (TENET) / .ac.za domains).



SA NREN CSIRT

The South African National Research and Education Network Computer Security Incident Response Team

Listed
since 10 Feb 2017

This information is provided without guarantee or pro-active maintenance.

Fields describing the team

Team Details

Official Name	Short Name	Country
The South African National Research and Education Network Computer Security Incident Response Team	SA NREN CSIRT	South Africa

Established	Host Organisation
01 Mar 2016	Council for Scientific and Industrial Research (CSIR) (SANReN host) and the Tertiary Education and Research Network of South Africa (TENET).

Constituency

Constituency Type	Country of Constituency
Research & Education	South Africa

ASNs, Domains, IP ranges	Description
2018 *.ac.za -	Public universities and science/research councils of South Africa including supporting institutions

Team Contact Information

Main Number	Emergency Number	Fax Number
+27 12 841 4111 CSIRT Manager	+27 21 763 7147 TENET 24x7 SOC	-

SANReN CSIRT (cont.)

- Partner engagements
  - NREN CSIRTs: CESNET, SURF, DEIC, Nordunet, RESTENA, (DFN-CERT)
  - Locally: Cybersecurity Hub; other sectors (e.g. SABRIC)
- We actively participate in
  - GÉANT SIG-ISM (Information Security Management)
  - Global NREN CEO Forum Information Security working group,
  - We have attended TF-CSIRT and FIRST meetings as well as presented at numerous forums.

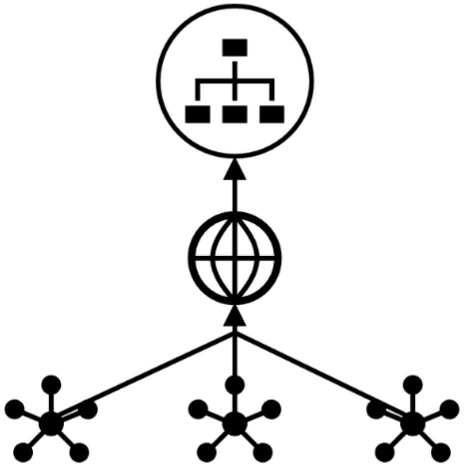
SANReN CSIRT Services

- csirt.sanren.ac.za
- **Vulnerability assessments**
  - 21 completed so far
- **Announcements**
  - Alerts (e.g. security incident notification)
  - Advisories
  - Articles
- **Csirt-news mailing list**

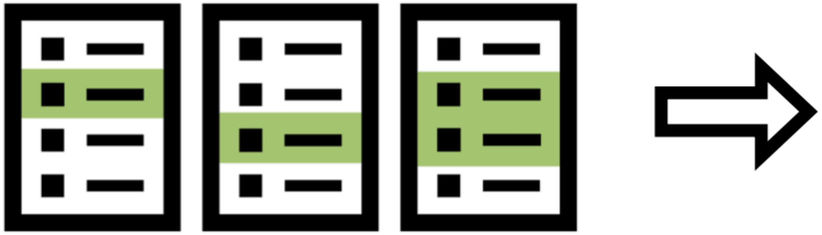
SANReN
South African National
Research Network

CSIRT Vulnerability Scanning Service

"ScanMan": Data aggregation and reporting



An effective external vulnerability assessment requires the use of multiple vulnerability scanners, each using it's own reporting format



Results from vulnerability scanners that address the same vulnerability type are aggregated into report items

Host 1

Report Item	Max CVSS	Confirmed
Report Code 1	9.8	✓
Report Code 2	7.3	×
Report Code 3	7.3	?
⋮	⋮	⋮
Report Code N	2.0	✓
Host Max CVSS	**9.8**	

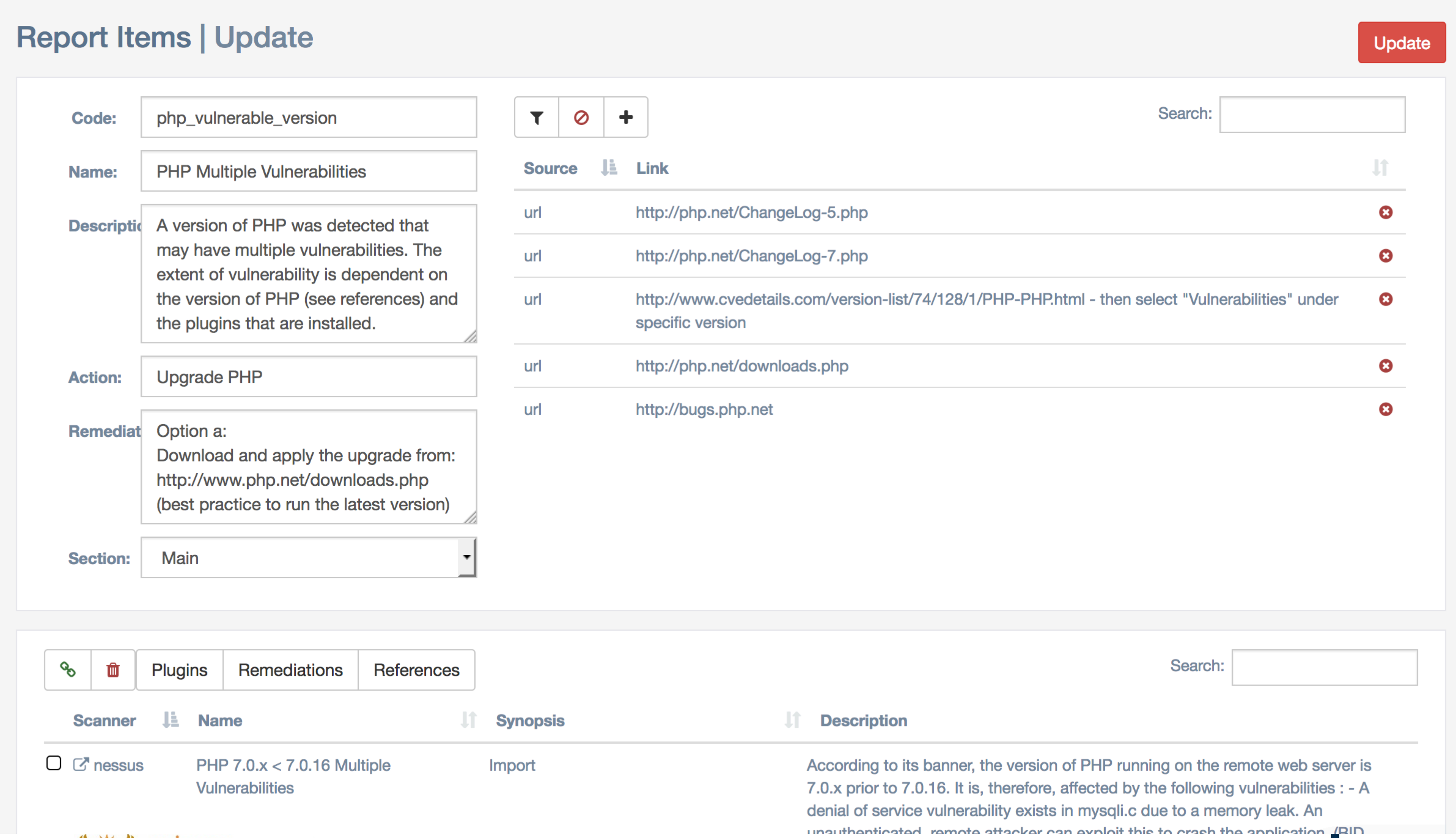
Institution 1 - Scan X

	Max CVSS	Critical	High	Medium
Host 1	9.8	8	2	20
Host 2	9.3	12	8	11
Host 3	7.1	0	1	13
⋮	⋮	⋮	⋮	⋮
Host N	4.3	0	0	9

Report items are verified per host to determine the host vulnerability

Per institution, the host results are aggregated into a holistic report

ScanMan v2



Report Items | Update

Update

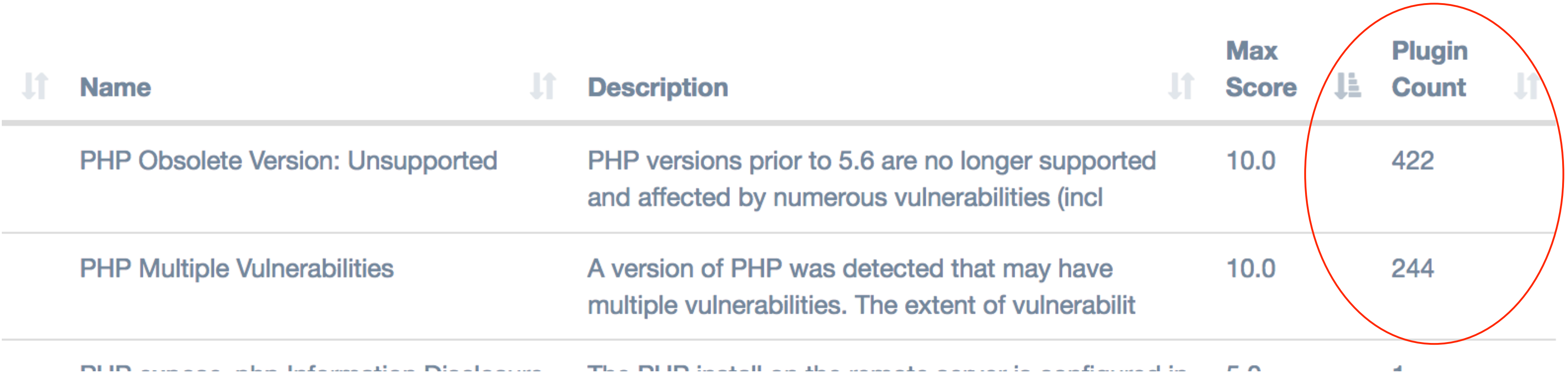
Code:	php_vulnerable_version
Name:	PHP Multiple Vulnerabilities
Descripti	A version of PHP was detected that may have multiple vulnerabilities. The extent of vulnerability is dependent on the version of PHP (see references) and the plugins that are installed.
Action:	Upgrade PHP
Remediat	Option a: Download and apply the upgrade from: http://www.php.net/downloads.php (best practice to run the latest version)
Section:	Main

Search:

Source	Link
url	http://php.net/ChangeLog-5.php
url	http://php.net/ChangeLog-7.php
url	http://www.cvedetails.com/version-list/74/128/1/PHP-PHP.html - then select "Vulnerabilities" under specific version
url	http://php.net/downloads.php
url	http://bugs.php.net

Search:

	Scanner	Name	Synopsis	Description
□	nessus	PHP 7.0.x < 7.0.16 Multiple Vulnerabilities	Import	According to its banner, the version of PHP running on the remote web server is 7.0.x prior to 7.0.16. It is, therefore, affected by the following vulnerabilities : - A denial of service vulnerability exists in mysqli.c due to a memory leak. An unauthenticated, remote attacker can exploit this to crash the application. (BID



Name	Description	Max Score	Plugin Count
PHP Obsolete Version: Unsupported	PHP versions prior to 5.6 are no longer supported and affected by numerous vulnerabilities (incl	10.0	422
PHP Multiple Vulnerabilities	A version of PHP was detected that may have multiple vulnerabilities. The extent of vulnerabilit	10.0	244
PHP expose_php Information Disclosure	The PHP install on the remote server is configured in	5.0	1

Infosec bits for week 02-18

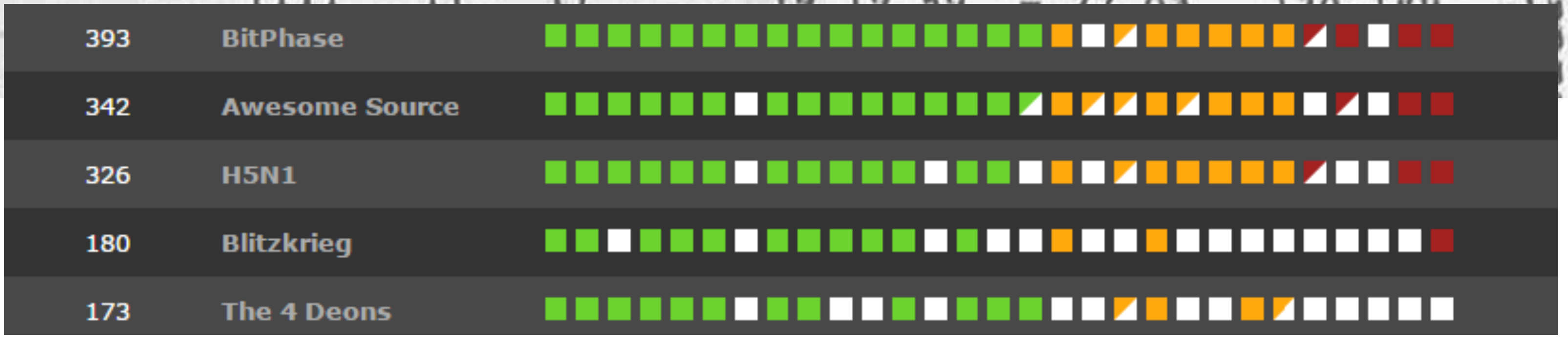
2018-01-12 16:11 - Roderick Mooi

1. **Meltdown and Spectre Updates Causing Problems for Some Users**
   - Meltdown & Spectre Patches Causing Boot Issues for Ubuntu 16.04 Computers
   - Warning: Microsoft Fix Freezes Some PCs With AMD Chips
   - Important: Windows security updates released January 3, 2018, and antivirus software
   - "We'll display this in red so it sticks out. Do not run the .reg file unless you've confirmed with your AV vendor that they're compatible with the Meltdown and Spectre patches."
   - Intel Releases Linux CPU Microcodes To fix Meltdown & Spectre Bugs
   - Qualcomm joins Intel, Apple, Arm, AMD in confirming its CPUs suffer hack bugs, too
   - List of Meltdown and Spectre Vulnerability Advisories, Patches, & Updates + see the US-CERT advisory
   - How to Protect Your Devices Against Meltdown and Spectre Attacks
   - You could resort to running everything on Raspberry Pi's ;) jaxenter.com/spectre-meltdown-not-raspberry-pi-140201.html
   - And for the curious... Triple Meltdown: How So Many Researchers Found a 20-Year-Old Chip Flaw At the Same Time
2. **WPA3 announced**
   - With WPA3, Wi-Fi security is about to get a lot tougher
   - WPA3 WiFi Standard Announced After Researchers KRACKed WPA2 Three Months Ago
3. **MADIoT – The nightmare after XMAS**
4. **The Week in Ransomware – January 5th 2018 – Slow For The Holidays**

SANReN

South African National Research Network

Cyber Security Challenge 2017



393	BitPhase	🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟩🟧⬜◩🟧🟧🟧🟧🟧◩🟥⬜🟥🟥
342	Awesome Source	🟩🟩🟩🟩🟩🟩⬜🟩🟩🟩🟩🟩🟩🟩🟩◩🟧◩◩🟧◩🟧🟧🟧⬜◩⬜🟥🟥
326	H5N1	🟩🟩🟩🟩🟩🟩⬜🟩🟩🟩🟩🟩⬜🟩🟩⬜🟧⬜◩🟧🟧🟧🟧🟧◩⬜⬜🟥🟥
180	Blitzkrieg	🟩🟩⬜🟩🟩🟩⬜🟩🟩🟩🟩🟩⬜🟩⬜⬜🟧⬜⬜🟧⬜⬜⬜⬜⬜⬜⬜⬜🟥
173	The 4 Deons	🟩🟩🟩🟩🟩🟩⬜🟩🟩⬜⬜🟩⬜🟩🟩🟩⬜⬜◩🟧⬜⬜🟧◩⬜⬜⬜⬜⬜

science & technology

Department: Science and Technology REPUBLIC OF SOUTH AFRICA

SANReN CSIRT update

Roderick Mooi, TF-CSIRT/FIRST Symposium 2018

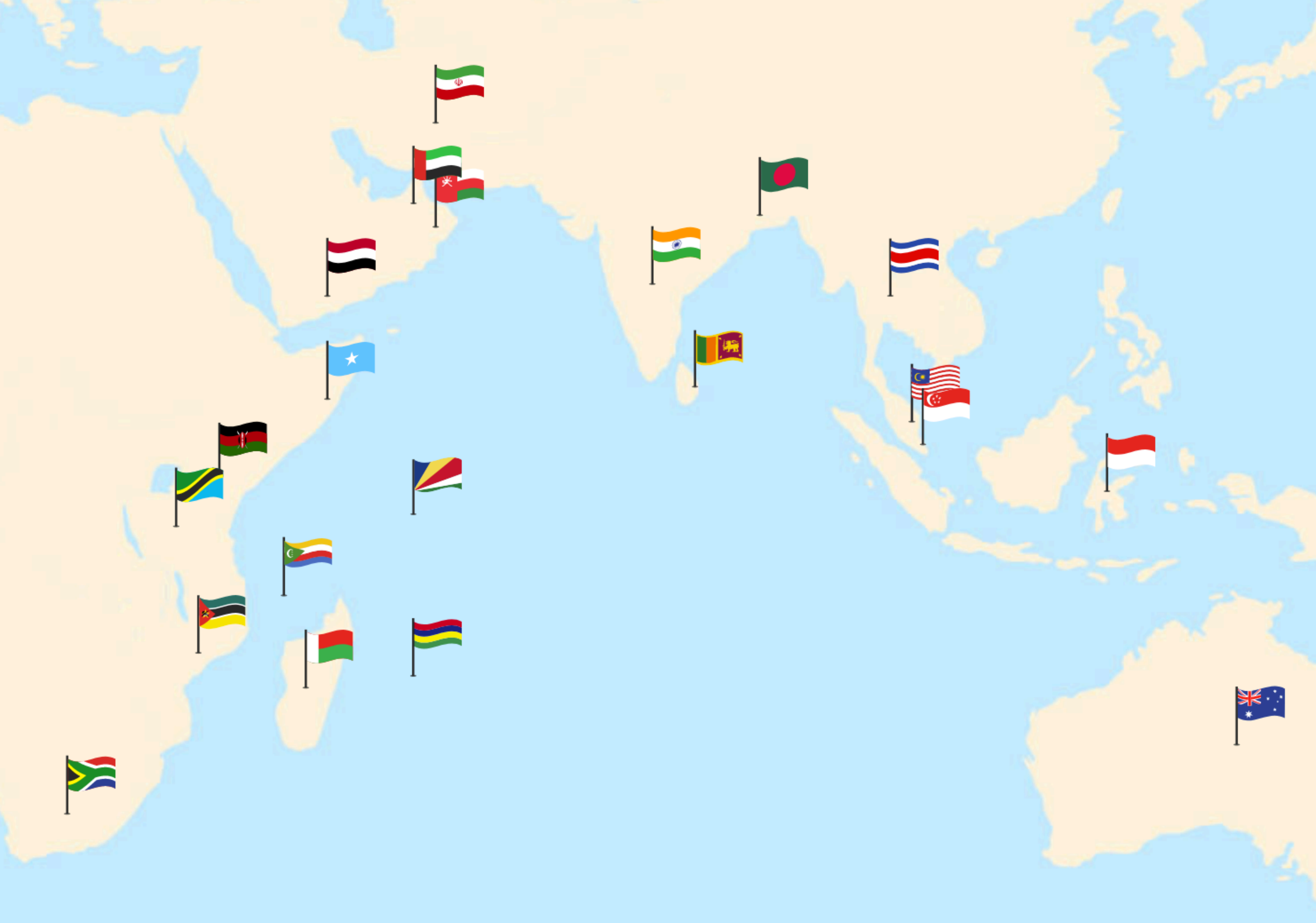
CSIR our future through science

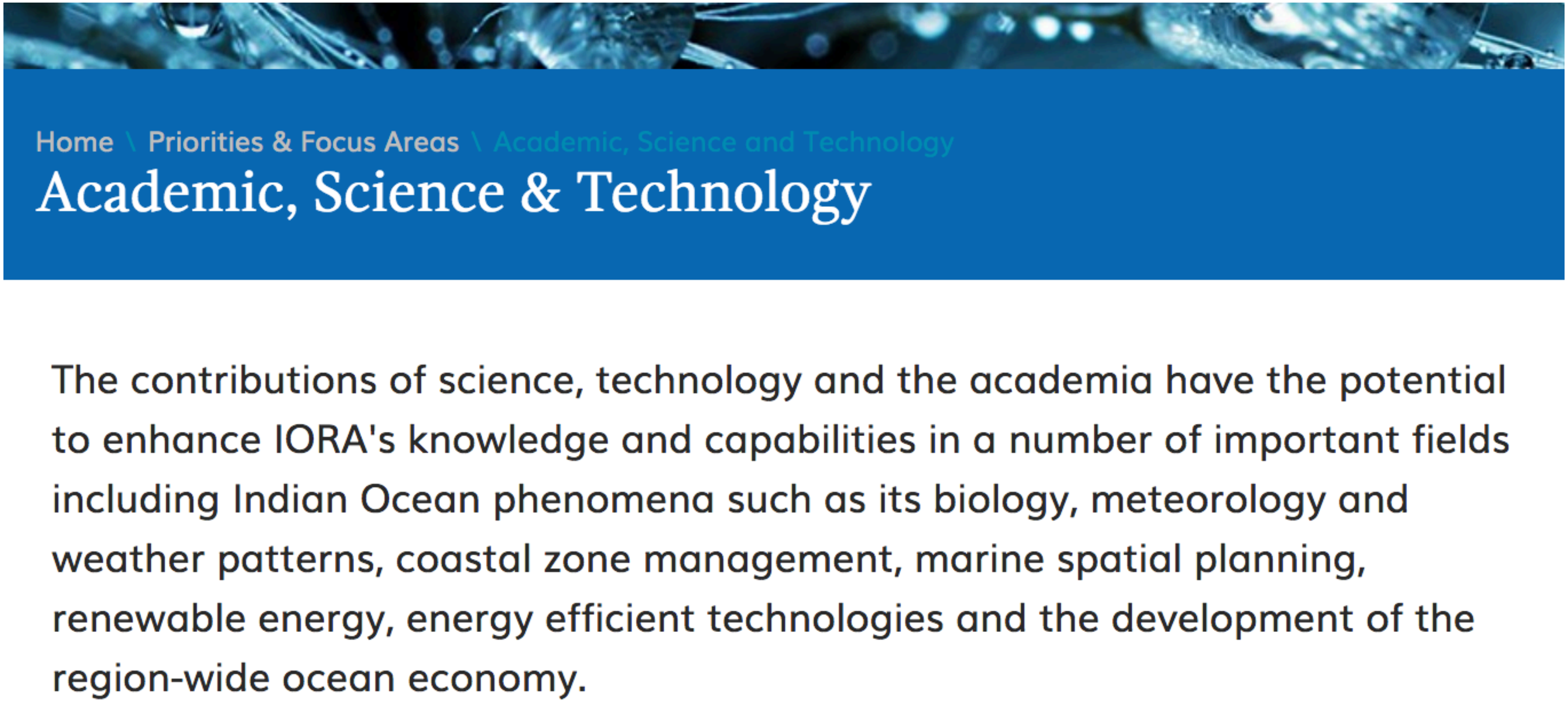
Indian Ocean Rim Association

IORA

The Indian Ocean Rim Association (IORA) is a dynamic inter-governmental organisation aimed at strengthening regional cooperation and sustainable development within the Indian Ocean region through its 21 Member States and 7 Dialogue Partners.

Commonwealth of **Australia**, People's Republic of **Bangladesh**, Union of **Comoros**, Republic of **India**, Republic of **Indonesia**, Islamic Republic of **Iran**, Republic of **Kenya**, Republic of **Madagascar**, **Malaysia**, Republic of **Mauritius**, Republic of **Mozambique**, Sultanate of **Oman**, Republic of **Seychelles**, Republic of **Singapore**, Federal Republic of **Somalia** , Republic of **South Africa**, Democratic Socialist Republic of **Sri Lanka**, United Republic of **Tanzania**, Kingdom of **Thailand**, **United Arab Emirates** and Republic of **Yemen**.



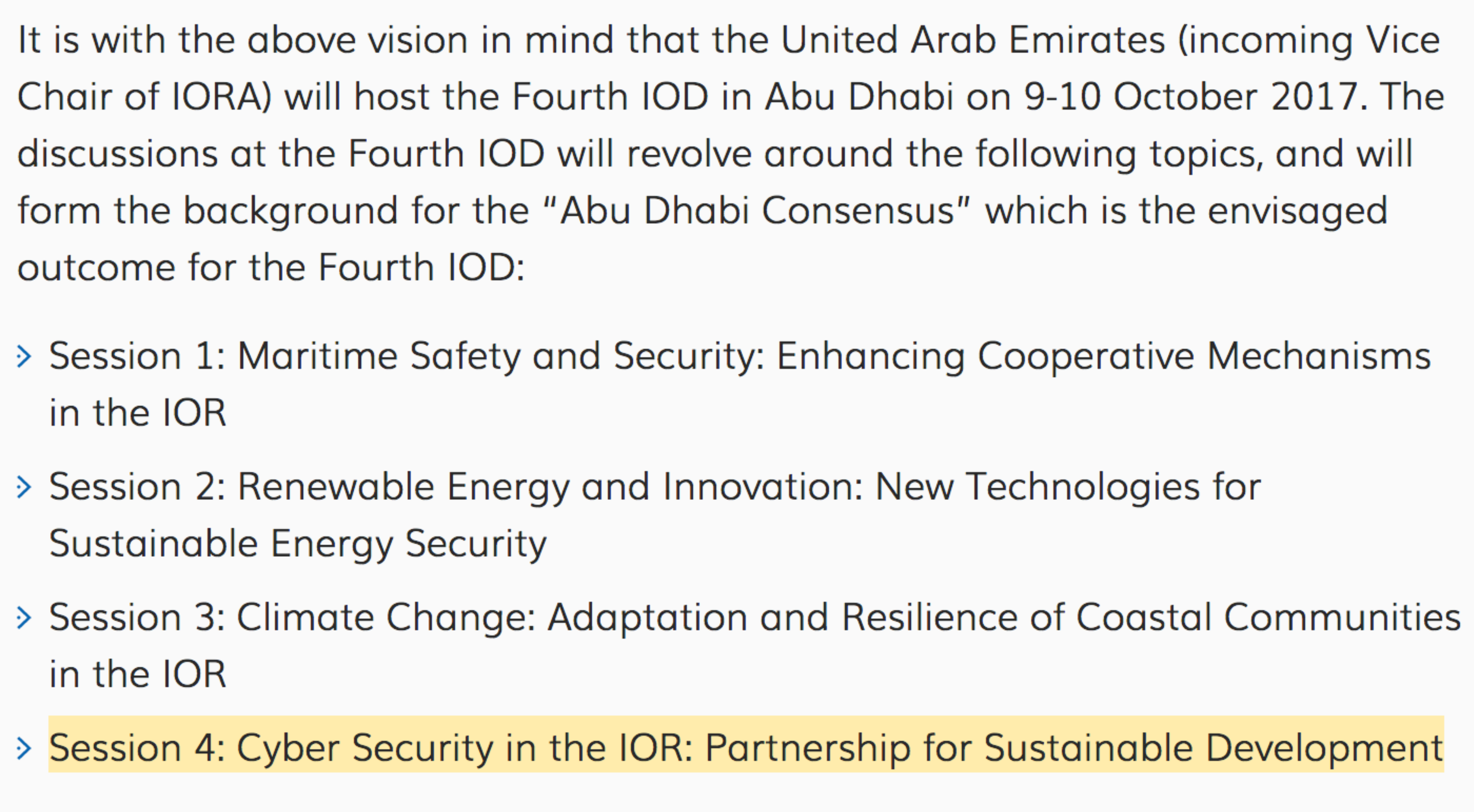


Home \ Priorities & Focus Areas \ Academic, Science and Technology

Academic, Science & Technology

The contributions of science, technology and the academia have the potential to enhance IORA's knowledge and capabilities in a number of important fields including Indian Ocean phenomena such as its biology, meteorology and weather patterns, coastal zone management, marine spatial planning, renewable energy, energy efficient technologies and the development of the region-wide ocean economy.

IORA Indian Ocean Dialogue



It is with the above vision in mind that the United Arab Emirates (incoming Vice Chair of IORA) will host the Fourth IOD in Abu Dhabi on 9-10 October 2017. The discussions at the Fourth IOD will revolve around the following topics, and will form the background for the "Abu Dhabi Consensus" which is the envisaged outcome for the Fourth IOD:

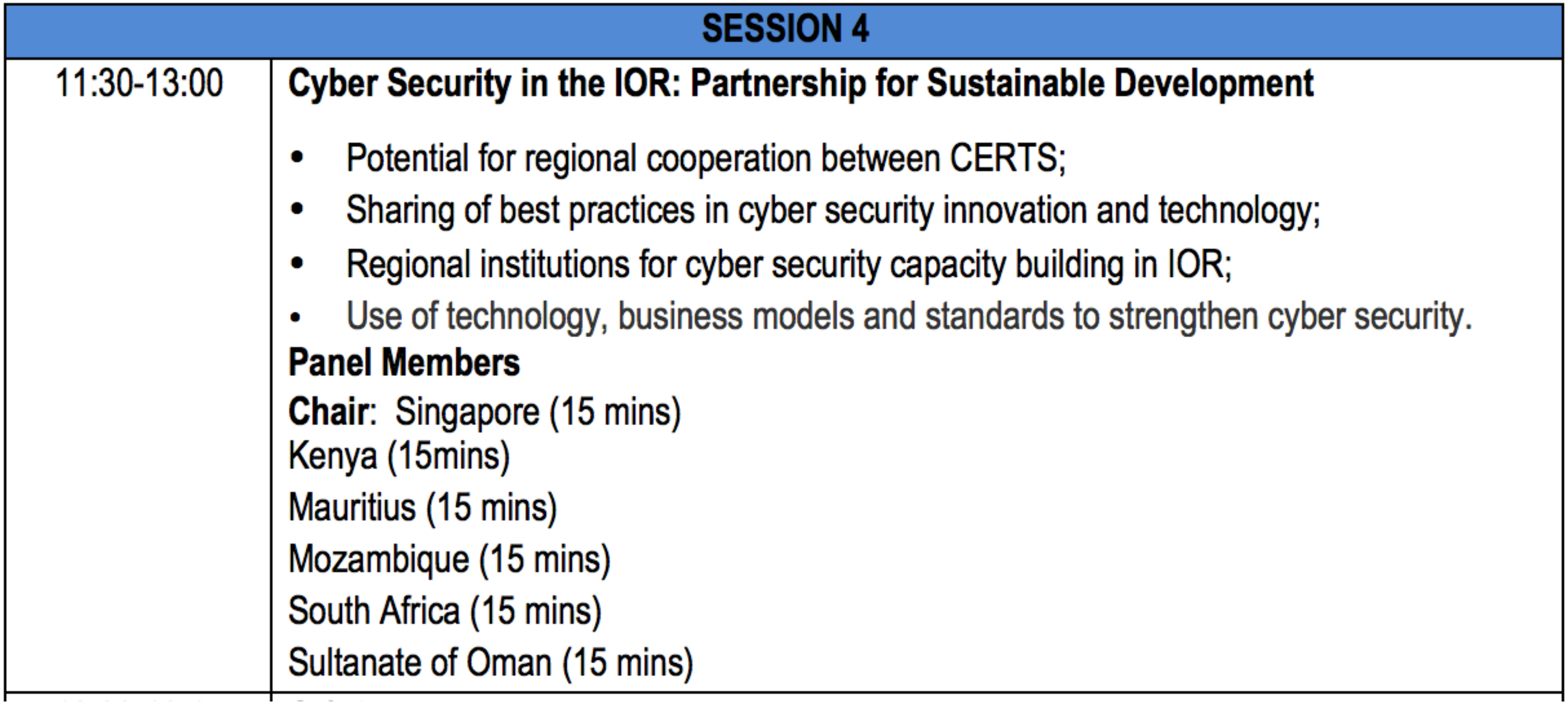
- Session 1: Maritime Safety and Security: Enhancing Cooperative Mechanisms in the IOR
- Session 2: Renewable Energy and Innovation: New Technologies for Sustainable Energy Security
- Session 3: Climate Change: Adaptation and Resilience of Coastal Communities in the IOR
- Session 4: Cyber Security in the IOR: Partnership for Sustainable Development

IORA IOD: 9-10 Oct 2017

Our Department of Science and Technology requested SANReN to participate. The SANReN CSIRT represented the South African contingent in the cyber security track. The academic and not-for-profit status of SANReN provided for a fresh perspective in multi-national cybersecurity collaboration to the IORA Dialogue.

The Abu Dhabi Consensus acknowledged that cybersecurity is a real and relevant risk, and that models for cooperation should be placed on a high priority. Schalk Peach participated in the discussion regarding the establishment of an IORA CERT, with the input that a distributed model centred around establishing formal agreements would be more suitable.

IORA IOD: 9-10 Oct 2017



SESSION 4	
11:30-13:00	**Cyber Security in the IOR: Partnership for Sustainable Development** • Potential for regional cooperation between CERTS; • Sharing of best practices in cyber security innovation and technology; • Regional institutions for cyber security capacity building in IOR; • Use of technology, business models and standards to strengthen cyber security. **Panel Members** **Chair**: Singapore (15 mins) Kenya (15mins) Mauritius (15 mins) Mozambique (15 mins) South Africa (15 mins) Sultanate of Oman (15 mins)

Where to from here?

- Follow-up constituency workshop
- TF-CSIRT Accreditation, FIRST membership
  - Mainly need policies and procedures
- "Community of practice" forum coordination
- More resources, skills, services
  - Processing and integration of threat intel / data feeds (e.g. ShadowServer reports)
  - SIEM development – netflow, sensors, IDS?
- ISM

Information Security Management

What the developed NRENs are doing…

- Roles and Responsibilities
- Resources
- Critical assets
- **Risk inventory**
- Standards and frameworks
- **Guiding policies**
- **Baselines**
- Awareness
- **Incident response**
- **Training**

Ref:
White paper Information Security Management
November 2015, Géant SIG ISM
Author: Alf Moens

Thanks!

roderick@sanren.ac.za

csirt.sanren.ac.za