GÉANT
Networks • Services • People

Security Operations: What do we have and what do we need?

→ delving into Threat Intelligence

Roderick Mooi
GÉANT

SIG-ISM, Virtual, 27 Oct 2021

Restricted

www.geant.org

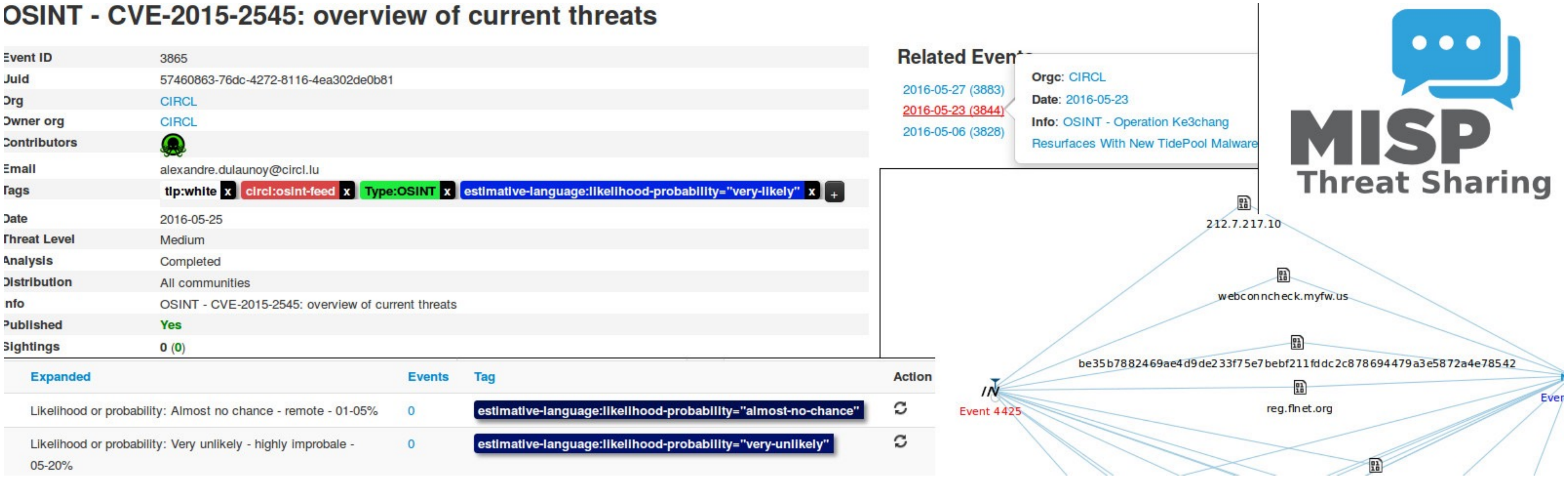
Intelligence sharing and threat analysis

- Initial platform: MISP
- Extensive list of default feeds
  - Add others as we go along
- Integrate (share) with other instances
- We need: participants ☺ (please)

MISP
Threat Sharing

MISP - Open Source Threat Intelligence Platform &
Open Standards For Threat Information Sharing

https://www.misp-project.org/



OSINT - CVE-2015-2545: overview of current threats

Event ID	3865
Juid	57460863-76dc-4272-8116-4ea302de0b81
Drg	CIRCL
Dwner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	tlp:white x circl:osint-feed x Type:OSINT x estimative-language:likelihood-probability="very-likely" x +
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
nfo	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability="almost-no-chance"	
Likelihood or probability: Very unlikely - highly improbale - 05-20%	0	estimative-language:likelihood-probability="very-unlikely"	

Related Events

2016-05-27 (3883)
2016-05-23 (3844)
2016-05-06 (3828)

Orgc: CIRCL
Date: 2016-05-23
Info: OSINT - Operation Ke3chang Resurfaces With New TidePool Malware

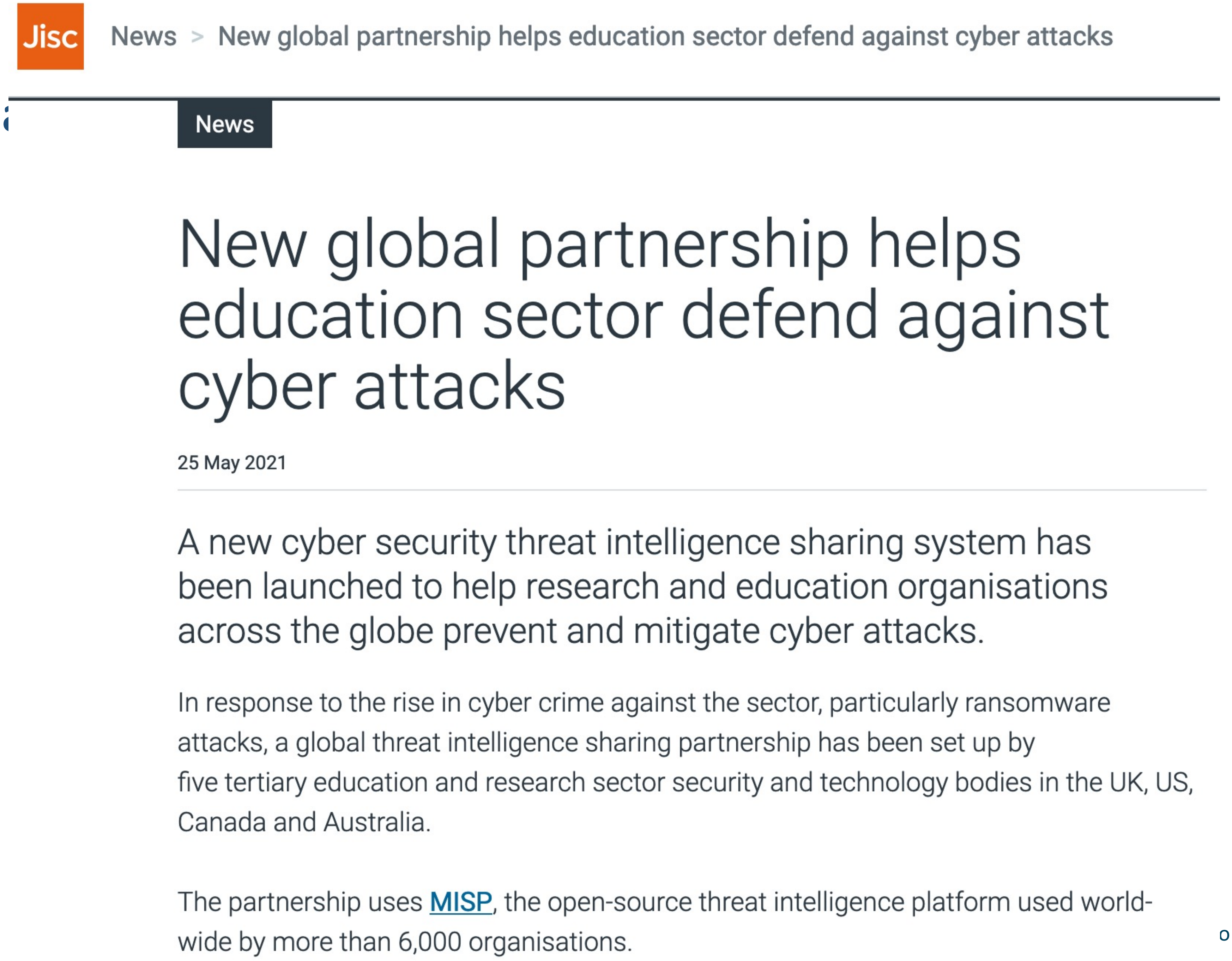
212.7.217.10
webconncheck.myfw.us
be35b7882469ae4d9de233f75e7bebf211fddc2c878694479a3e5872a4e78542
reg.flnet.org
Event 4425
Ever

MISP Threat Sharing

Integration / Sharing IOCs

- FIRST
  - https://www.first.org/global/sigs/information-sharing/misp
- CIRCL
  - https://circl.lu/services/misp-malware-information-sharing-platform/
- WLCG Academic MISP instance
  - Previous SIG-ISM presentations ☺
  - https://wlcg-soc-wg-doc.web.cern.ch/misp/sync.html
- NRENs
  - Global partnership: JISC, AARNet, CanSSOC, OmniSOC, REN-ISAC…

Glob



Jisc News > New global partnership helps education sector defend against cyber attacks

News

New global partnership helps education sector defend against cyber attacks

25 May 2021

A new cyber security threat intelligence sharing system has been launched to help research and education organisations across the globe prevent and mitigate cyber attacks.

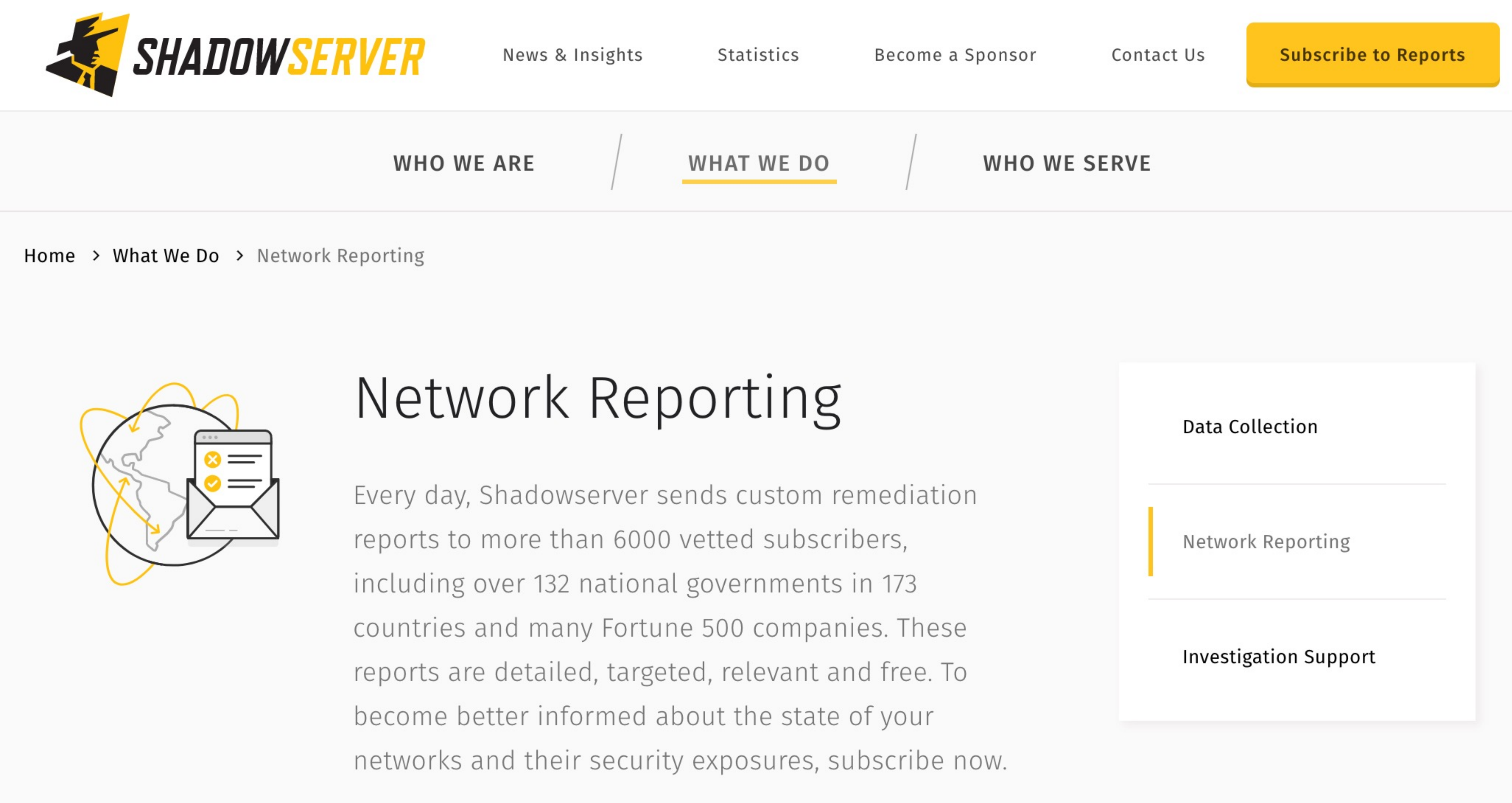
In response to the rise in cyber crime against the sector, particularly ransomware attacks, a global threat intelligence sharing partnership has been set up by five tertiary education and research sector security and technology bodies in the UK, US, Canada and Australia.

The partnership uses MISP, the open-source threat intelligence platform used world-wide by more than 6,000 organisations.

- https://www.jisc.ac.uk/news/new-global-partnership-helps-education-sector-defend-against-cyber-attacks-25-may-2021
- https://news.aarnet.edu.au/new-global-partnership-helps-education-sector-defend-against-cyber-attacks/
- https://canssoc.ca/2021/05/25/new-global-partnership-helps-education-sector-defend-against-cyber-attacks/
- https://itnews.iu.edu/articles/2021/Global-collaboration-in-the-face-of-a-gobal-threat-.php

What about?

- Flow data analysis / IOCs
- SOCTools
  - https://gitlab.geant.org/gn4-3-wp8-t3.1-soc/soctools
  - “SOCTools is a collection of tools for collecting, enriching and analysing logs and other security data, threat information sharing and incident handling. ”
  - → MISP for enrichment
- Reports from the likes of Shadowserver, Team Cymru, etc.
  - https://www.shadowserver.org/what-we-do/network-reporting/
  - https://team-cymru.com/community-services/csirt-ap/
- Ideas?



SHADOWSERVER

News & Insights Statistics Become a Sponsor Contact Us **Subscribe to Reports**

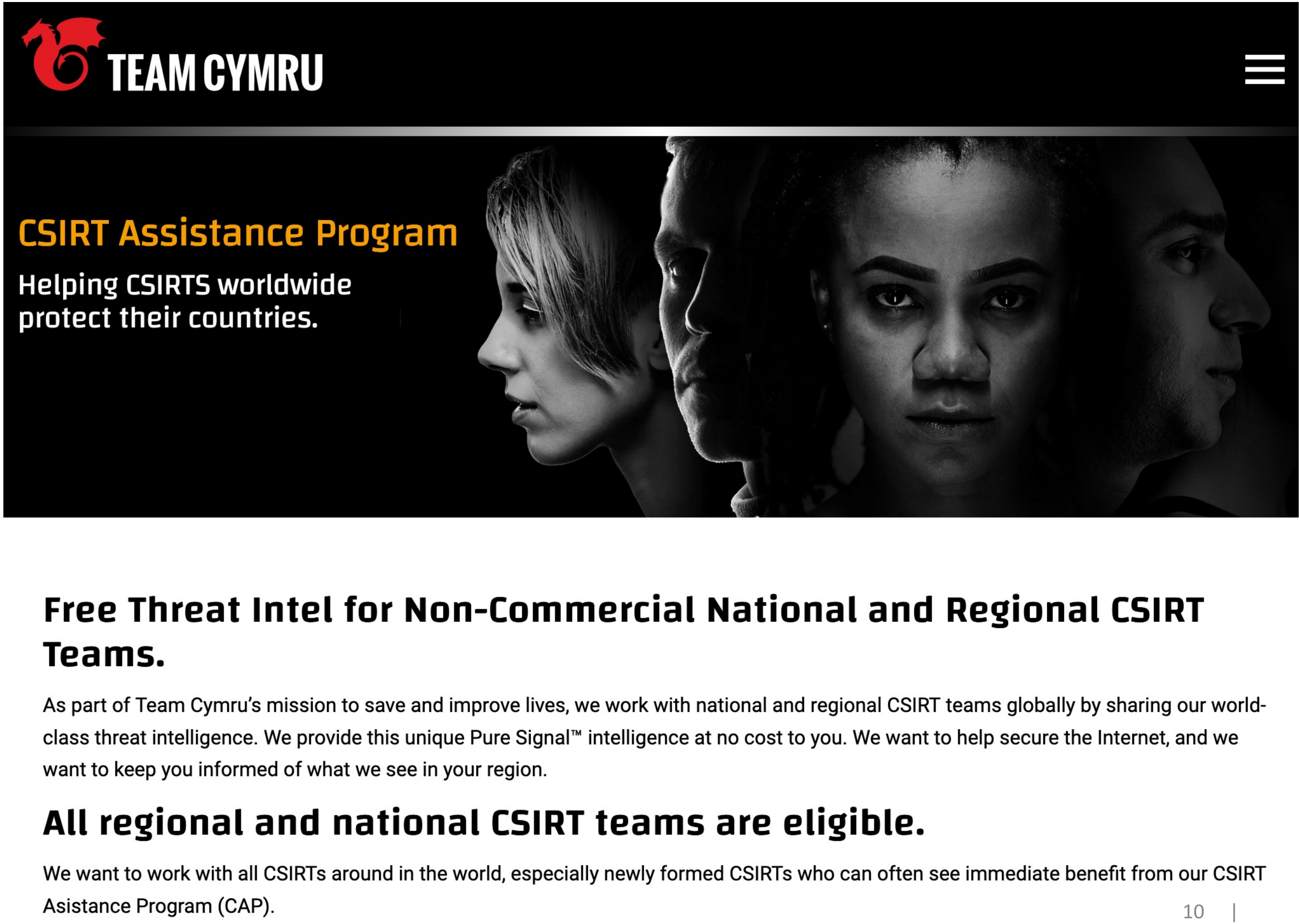
WHO WE ARE / WHAT WE DO / WHO WE SERVE

Home > What We Do > Network Reporting

Network Reporting

Every day, Shadowserver sends custom remediation reports to more than 6000 vetted subscribers, including over 132 national governments in 173 countries and many Fortune 500 companies. These reports are detailed, targeted, relevant and free. To become better informed about the state of your networks and their security exposures, subscribe now.

- Data Collection
- Network Reporting
- Investigation Support


TEAM CYMRU

CSIRT Assistance Program

Helping CSIRTS worldwide
protect their countries.

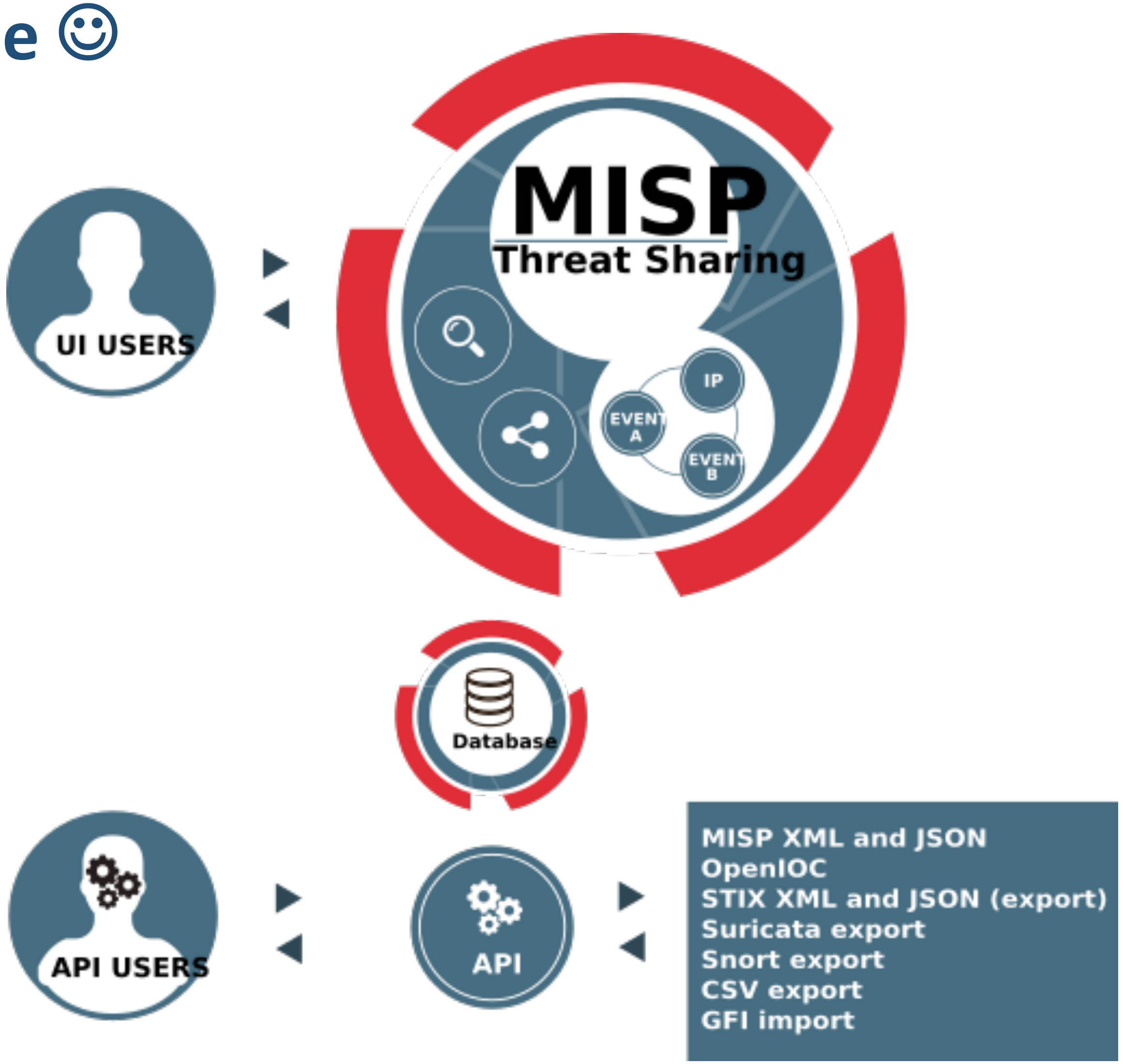
Free Threat Intel for Non-Commercial National and Regional CSIRT Teams.

As part of Team Cymru's mission to save and improve lives, we work with national and regional CSIRT teams globally by sharing our world-class threat intelligence. We provide this unique Pure Signal™ intelligence at no cost to you. We want to help secure the Internet, and we want to keep you informed of what we see in your region.

All regional and national CSIRT teams are eligible.

We want to work with all CSIRTs around in the world, especially newly formed CSIRTs who can often see immediate benefit from our CSIRT Asistance Program (CAP).

Users please ☺



MISP XML and JSON
OpenIOC
STIX XML and JSON (export)
Suricata export
Snort export
CSV export
GFI import

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

© GÉANT Association
As part of the GÉANT 2020 Framework Partnership Agreement (FPA), the project receives funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).