TLP:GREEN

RNEP-GW

MÓDULO MATURIDADE (DE UM CSIRT)

fct csirt

RNEP-GW

O MODELO SIM3

45 Parâmetros

Quatro Eixos:

- Organizacional
- Humano
- Ferramentas
- Processos

Medir cada Parâmetro em um de cinco níveis

COMO AVALIO A MATURIDADE DO MEU CSIRT?

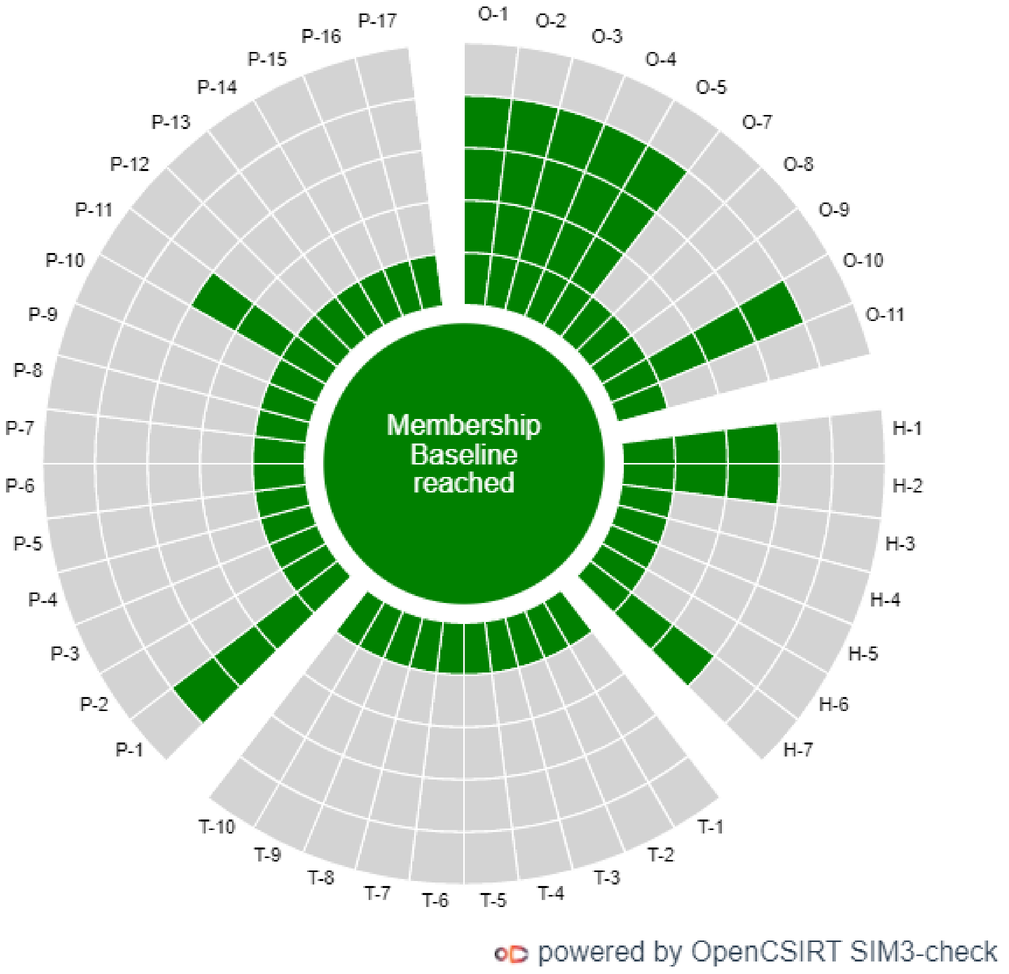
0: Não existe

1: Implícito

2: Escrito mas não formalizado

3: Explícito & formalizado

4: Auditado



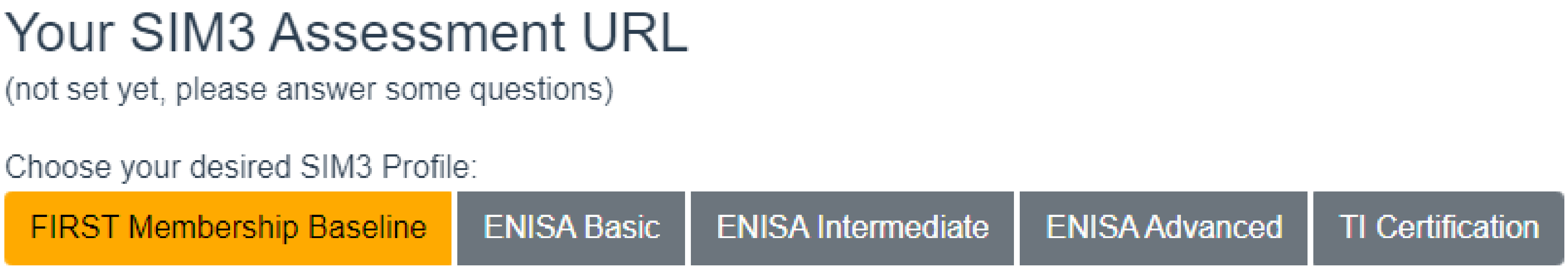
SIM3-CHECK

Medir «o que já temos»

Identificar «o que podemos melhorar»

sim3-check.opencsirt.org

SIM3-CHECK: DIFERENTES PERFIS



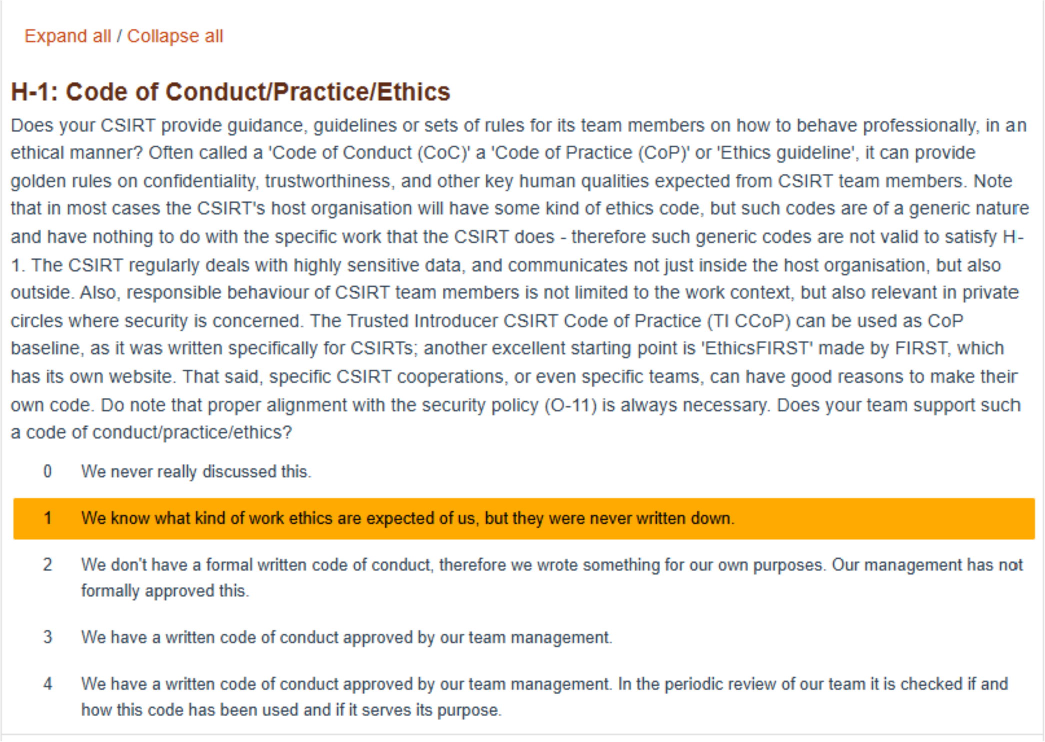
Your SIM3 Assessment URL

(not set yet, please answer some questions)

Choose your desired SIM3 Profile:

[✓ FIRST Membership Baseline] ENISA Basic | ENISA Intermediate | ENISA Advanced | TI Certification

SIM3-CHECK: DIFERENTES PERFIS



Expand all / Collapse all

H-1: Code of Conduct/Practice/Ethics

Does your CSIRT provide guidance, guidelines or sets of rules for its team members on how to behave professionally, in an ethical manner? Often called a 'Code of Conduct (CoC)' a 'Code of Practice (CoP)' or 'Ethics guideline', it can provide golden rules on confidentiality, trustworthiness, and other key human qualities expected from CSIRT team members. Note that in most cases the CSIRT's host organisation will have some kind of ethics code, but such codes are of a generic nature and have nothing to do with the specific work that the CSIRT does - therefore such generic codes are not valid to satisfy H-1. The CSIRT regularly deals with highly sensitive data, and communicates not just inside the host organisation, but also outside. Also, responsible behaviour of CSIRT team members is not limited to the work context, but also relevant in private circles where security is concerned. The Trusted Introducer CSIRT Code of Practice (TI CCoP) can be used as CoP baseline, as it was written specifically for CSIRTs; another excellent starting point is 'EthicsFIRST' made by FIRST, which has its own website. That said, specific CSIRT cooperations, or even specific teams, can have good reasons to make their own code. Do note that proper alignment with the security policy (O-11) is always necessary. Does your team support such a code of conduct/practice/ethics?

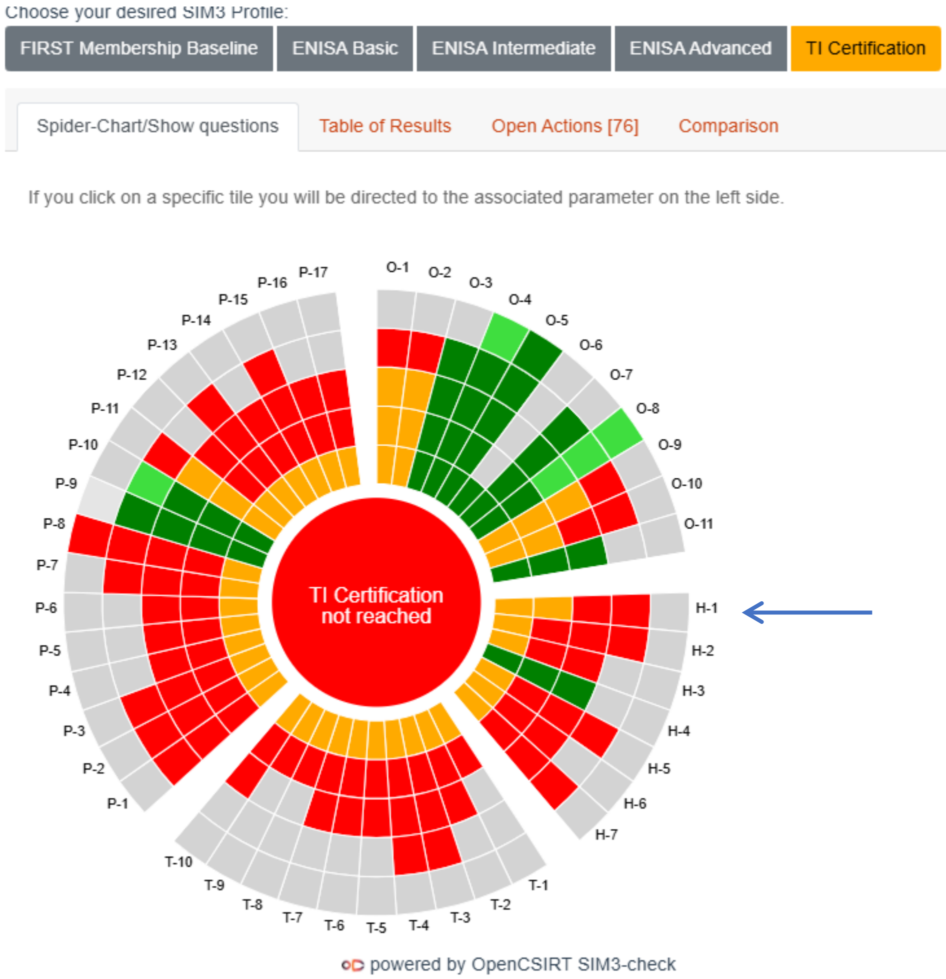
0 We never really discussed this.

1 We know what kind of work ethics are expected of us, but they were never written down.

2 We don't have a formal written code of conduct, therefore we wrote something for our own purposes. Our management has not formally approved this.

3 We have a written code of conduct approved by our team management.

4 We have a written code of conduct approved by our team management. In the periodic review of our team it is checked if and how this code has been used and if it serves its purpose.



Choose your desired SIM3 Profile:

If you click on a specific tile you will be directed to the associated parameter on the left side.

powered by OpenCSIRT SIM3-check

FIRST, ENISA, TRUSTED INTRODUCER

FIRST™
Improving Security Together

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

TI
TF-CSIRT
Trusted Introducer

IDEIAS CHAVE

- A avaliação da maturidade promove a melhoria contínua
- Existe uma framework pronta a usar: o SIM3
- Diferentes organizações exigem diferentes níveis de maturidade aos seus membros

Questões?

Obrigado.

PODCAST
CERT RCTS
DIZ-ME A TUA PASSWORD, DIR-TE-EI QUEM ÉS
\\:podcast\segurança-informática
fct Fundação para a Ciência e a Tecnologia
FCCN

csirt.fct.pt/podcast

Exact Sciences and Technology
CSIRT in a Box: Capacitação Inicial de Equipas de Resposta a Incidentes
nau SEMPRE A APRENDER by FCCN fct

csirt.fct.pt/mooc

csirt.fct.pt/etc