nic.br cgi.br | cert.br

10º Fórum Brasileiro de CSIRTs

19 de setembro de 2022

São Paulo / SP

SIM3, FIRST CSIRT Services Framework e TLP 2.0: Novidades dos Padrões e Impactos para o Tratamento de Incidentes e o Compartilhamento de Ameaças

Dra. Cristine Hoepers
Gerente
cristine@cert.br

cert.br nic.br cgi.br

TLP:CLEAR

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CERT Nacional de Último Recurso

Serviços Prestados à Comunidade

Gestão de Incidentes

- Coordenação
- Análise Técnica
- Suporte à Mitigação e Recuperação

Consciência Situacional

- Aquisição de Dados
  - *Honeypots* Distribuídos
  - SpamPots
  - *Threat feeds*
- Compartilhamento das Informações

Transferência de Conhecimento

- Conscientização
  - Desenvolvimento de Boas Práticas
  - Cooperação, Eventos e Reuniões (*Outreach*)
- Treinamento
- Aconselhamento Técnico e de Políticas

Filiações e Parcerias:

FIRST Improving Security Together MEMBER

ACCREDITED BY TI TRUSTED INTRODUCER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

SEI Partner Network

HN/P

Criação:

Agosto/1996: CGI.br publica o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil"[1]

Junho/1997: CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório[2]

[1] https://cert.br/sobre/estudo-cgibr-1996.html | [2] https://nic.br/pagina/gts/157

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Público Alvo (*Constituency*)

Redes que utilizam recursos administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Governança

Mantido pelo **NIC.br** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial
- responsável por coordenar e integrar as iniciativas e serviços da Internet no País

https://cert.br/sobre/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

Grupos de Segurança, CSIRTs e PSIRTs: **Evolução e Desafios**

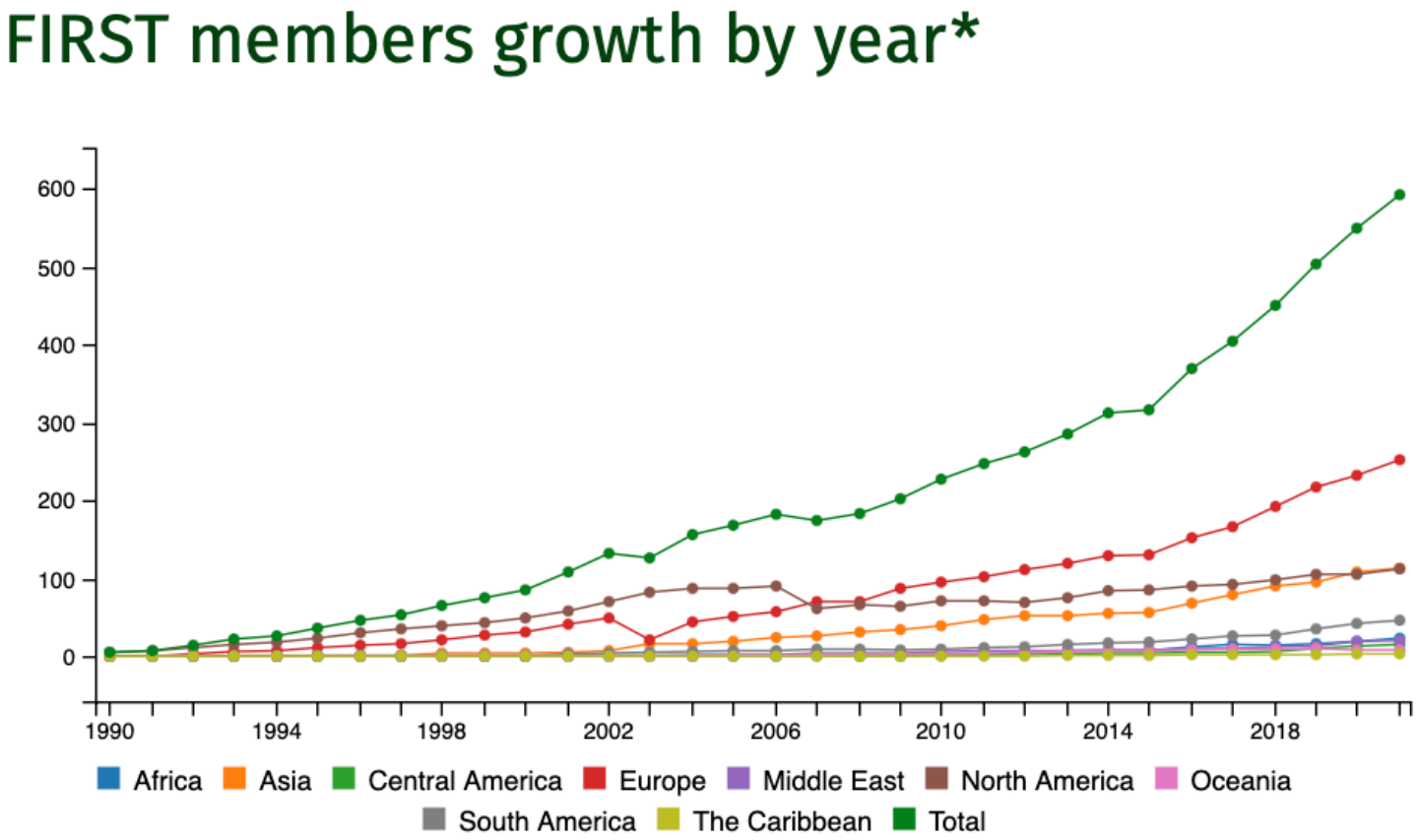
TLP:CLEAR

Número crescente
- Diversos países
- Diversos setores
- Variados níveis de maturidade

Confiança (*trust*) é pré-requisito para cooperação

Desafios na comunicação
- Como comunicar expectativa de confidencialidade?
- Como identificar serviços disponíveis?
- Como quantificar maturidade e qualidade do serviço?

Adicionalmente
- Como identificar habilidades e conhecimentos necessários aos profissionais dessa área?



(*) The statistic measurement method and regional breakdown changed in 2007.

Fonte: *FIRST History*, *link* visitado em 17/09/2022
https://www.first.org/about/history

Padrões e Guias Construídos pela Comunidade

Organizações envolvidas

- FIRST – *Forum of Incident Response and Security Teams*
  - SIGs (*Special Interest Groups*) e Comitês
- *Open* CSIRT *Foundation*
  - TF-CSIRT *Trusted Introducer*
- ENISA (*European Union Agency for Cybersecurity*)
- GFCE (*Global Forum on Cyber Expertise*)

Padrões

- FIRST:
  - CVSS (*Common Vulnerability Scoring System*)
  - **TLP (*Traffic Light Protocol*)**
  - **CSIRT *Services Framework***
  - PSIRT *Services Framework*
  - IEP (*Information Exchange Policy*)
  - Passive DNS
  - EPSS (*Exploit Prediction Scoring System*)
- *Open* CSIRT *Foundation*
  - **SIM3 (*Security Incident Management Maturity Model*)**

Traffic Light Protocol 2.0

cert.br nic.br cgi.br

TLP:CLEAR

Traffic Light Protocol (TLP):
Troca e Compartilhamento de Dados e Informações

O que é?
– um conjunto de **marcações**
– 4 cores para indicar os **limites de compartilhamento**

Por que?
– facilitar a adoção e a colaboração mais frequente
– aumentar a legibilidade
– facilitar **compartilhamento entre pessoas**

Onde usar?
– documentos, *e-mails*, *slides*, notificações
– plataformas de CTI, como MISP
– qualquer outro lugar (ex: Conferências)

https://cert.br/tlp/

Traffic Light Protocol (TLP) Versão 2.0:
Tradução Oficial - Português Brasileiro

TLP:CLEAR

Tradução

CERT.br/NIC.br

- Cristine Hoepers

Revisão

CAIS/RNP

- Edilson Lima
- Emilio Nakamura

CSIRT PETROBRAS

- Marcos Vinicio Rabello da Silva
- Kildane de Souza Castro

CERT.br/NIC.br

- Klaus Steding-Jessen
- Miriam von Zuben

https://www.first.org/tlp/
https://www.first.org/tlp/docs/v2/tlp-pt-br.pdf

TLP:CLEAR

TLP 2.0:
Por que uma nova versão?

- Melhorar a linguagem
  - usar consistentemente os mesmos termos (ao invés de sinônimos)
  - deixar o texto menos coloquial para facilitar as traduções
  - explicitar melhor os limites de compartilhamento, por exemplo:
    - TLP:RED é para indivíduos - não pode usar para proteger a organização
    - TLP:AMBER e TLP:AMBER+STRICT são somente para “quem precisa saber” (*need to know basis*)
- Novo conteúdo
  - definição de termos
    - comunidade, organização e clientes
  - criação do TLP:AMBER+STRICT
  - TLP:WHITE ➡ TLP:CLEAR
  - melhorias na acessibilidade das cores e tabela com definições em RGB, CMYK e Hexadecimal

Obs.: Ficou em consulta pública de nov/2021 a mar/2022

TLP:CLEAR

Definições:
Comunidade, Organização e Clientes

- **Comunidade: um grupo que compartilha objetivos, práticas e relacionamentos informais de confiança**. Uma comunidade pode ser tão ampla quanto todos os profissionais de segurança cibernética em um país (ou em um setor ou região).

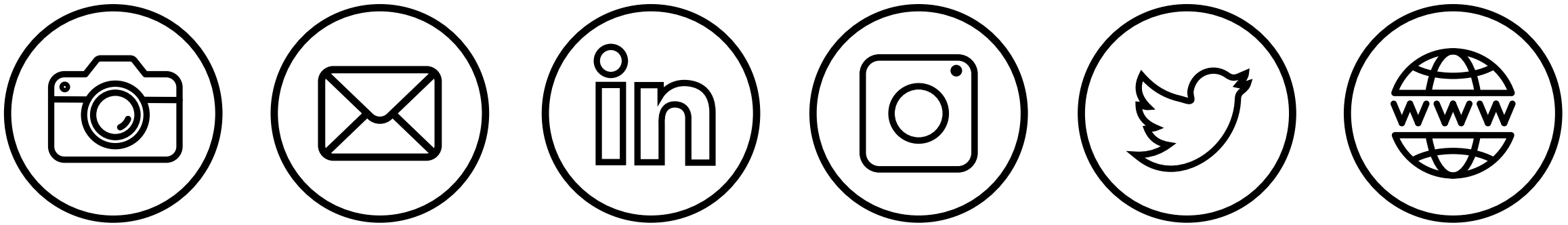
- **Organização:** um grupo que compartilha uma mesma afiliação através de um **processo formal de filiação e que está sujeito a um conjunto de políticas em comum definidas pela organização**. Uma organização pode ser tão ampla quanto todos os membros de uma organização para compartilhamento de informações, mas raramente mais ampla que isso.

- **Clientes: as pessoas ou entidades que recebem serviços de segurança cibernética de uma organização**. Clientes são incluídos por padrão no TLP:AMBER, de modo que os destinatários possam compartilhar informações adiante, permitindo que os clientes possam tomar ações para se proteger. Para times com responsabilidade nacional esta definição inclui as partes interessadas (*stakeholders*) e o público-alvo (*constituents*).

https://cert.br/tlp/

TLP:CLEAR

NÃO HÁ LIMITES NA DIVULGAÇÃO

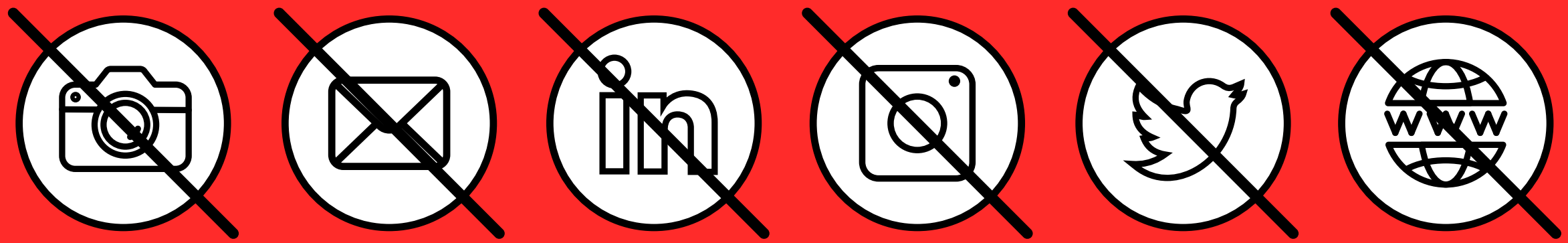


https://cert.br/tlp/

TLP:RED

NÃO DEVE SER DIVULGADO

- SOMENTE PARA OS **OLHOS E OUVIDOS DO INDIVÍDUO** DESTINATÁRIO

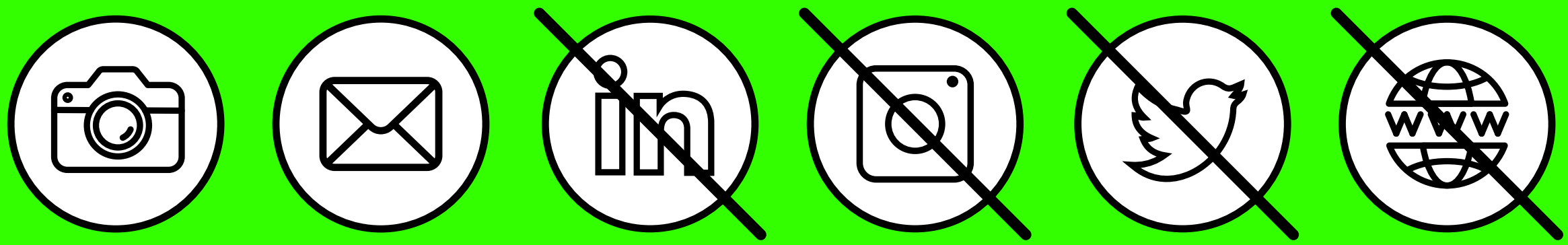


https://cert.br/tlp/

TLP:GREEN

DIVULGAÇÃO LIMITADA:

- À COMUNIDADE DE SEGURANÇA CIBERNÉTICA
- NÃO PODE USAR CANAIS PUBLICAMENTE ACESSÍVEIS



https://cert.br/tlp/

TLP:AMBER

DIVULGAÇÃO LIMITADA A **QUEM PRECISA SABER**:

- EM SUA ORGANIZAÇÃO
- EM SEU PÚBLICO-ALVO OU CLIENTES

⚠ **AO REPASSAR** MUDE PARA **TLP:AMBER+STRICT**

https://cert.br/tlp/

TLP:AMBER+STRICT

DIVULGAÇÃO LIMITADA A **QUEM PRECISA SABER**:

- SOMENTE INTERNA À **SUA ORGANIZAÇÃO**
- **NÃO** COMPARTILHAR
  COM PÚBLICO-ALVO OU CLIENTES

https://cert.br/tlp/

TLP	Quando deve ser usado?	Como pode ser compartilhado?
TLP:RED **Somente para os olhos e ouvidos dos indivíduos destinatários, não é permitido compartilhamento nenhum.**	Fontes podem usar TLP:RED quando não é possível atuar sobre a informação sem colocar em risco significativo a privacidade, reputação ou operações das organizações envolvidas.	Destinatários **não podem compartilhar informações TLP:RED com mais ninguém**. No contexto de uma reunião, por exemplo, informações TLP:RED são limitadas àqueles presentes na reunião.
TLP:AMBER **Divulgação limitada, destinatários só podem disseminar para aqueles que necessitam saber (*need-to-know basis*) dentro de sua própria organização e com seus clientes.**	Fontes podem usar o TLP:AMBER quando é necessário apoio para agir de maneira efetiva sobre a informação, mas ainda assim há riscos para a privacidade, reputação ou operações das organizações envolvidas.	Destinatários **podem compartilhar TLP:AMBER com membros de sua própria organização e com seus clientes**, mas somente com aqueles que necessitam saber da informação (*need-to-know basis*) para proteger sua organização e seus clientes e evitar danos continuados.
TLP:AMBER+STRICT **Divulgação limitada, destinatários só podem disseminar para aqueles que necessitam saber (*need-to-know basis*) e somente dentro de sua própria organização.**	Fontes podem usar o TLP:AMBER+STRICT quando é necessário apoio para agir de maneira efetiva sobre a informação, mas ainda assim há riscos para a privacidade, reputação ou operações das organizações envolvidas. **Se a fonte quiser restringir o compartilhamento somente para a organização ela deve especificar TLP:AMBER+STRICT.**	Destinatários **podem compartilhar TLP:AMBER+STRICT somente com membros de sua própria organização**, e somente com aqueles que necessitam saber da informação (*need-to-know basis*) para proteger sua organização e evitar danos continuados.
TLP:GREEN **Divulgação limitada, destinatários podem divulgar dentro de sua comunidade.**	Fontes podem usar TLP:GREEN quando a informação é útil para a conscientização dentro de sua comunidade mais ampla.	Destinatários podem compartilhar informações TLP:GREEN com seus pares e organizações parceiras dentro de sua comunidade, mas não por meio de canais publicamente acessíveis. Informações TLP:GREEN não podem ser compartilhadas fora de uma comunidade. Nota: quando a "comunidade" não estiver definida, assume-se que é a comunidade de segurança/defesa cibernética.
TLP:CLEAR **Não há limites na divulgação.**	Fontes podem usar TLP:CLEAR quando há um risco mínimo ou não há previsão de risco de mau uso da informação, de acordo com regras e procedimentos aplicáveis para divulgação pública.	Destinatários podem disseminar para o mundo, não há limites na divulgação. Desde que respeitadas as regras padrão de direitos autorais, as informações TLP:CLEAR podem ser compartilhadas sem restrições.

TLP SIG:
Próximos Passos

TLP:CLEAR

- **Adotar TLP 2.0 até janeiro de 2023!**
  - **Ajude a divulgar e a identificar quem precisa sabe da mudança**
    - **desenvolvedores de ferramentas, comunidades de CTI**
- Trabalhar em "*Use Cases*" com exemplos específicos de cenários de compartilhamento
  - O que pode compartilhar com Provedores de Serviços ou com Terceirizados?
  - Com quem um CSIRT Nacional ou Setorial pode compartilhar um TLP:AMBER? E um TLP:AMBER+STRICT?
  - Em que situações devo mudar um TLP:AMBER para TLP:AMBER+STRICT na hora de repassar?
    - Cuidados com TLP:AMBER para que não se torne um TLP:GREEN na prática

Quer ajudar?

- Envie cenários de situações que não estão claras para:
  - `<cristine@cert.br>` - com [TLP Use Cases] no *subject*
- Entre para o SIG!
  https://www.first.org/global/sigs/tlp/

Referências

Página do CERT.br com um resumo do TLP e *links* para materiais de referência

– Uso do TLP pelo CERT.br
https://cert.br/tlp/

Palestra de Anúncio do TLP 2.0

– *Traffic Light Protocol 2022: Updates for An Improved Sharing Experience*
Tom Millar (CISA, US), Don Stikvoort (Elsinore, NL), Ted Norminton (CCCS, CA)
FIRST Conference 2022, Duration: 1:07:09
https://youtu.be/2q8IFVOYRjM

Referências Oficiais

– TRAFFIC LIGHT PROTOCOL (TLP) *FIRST Standards Definitions and Usage Guidance* — Version 2.0
https://www.first.org/tlp/

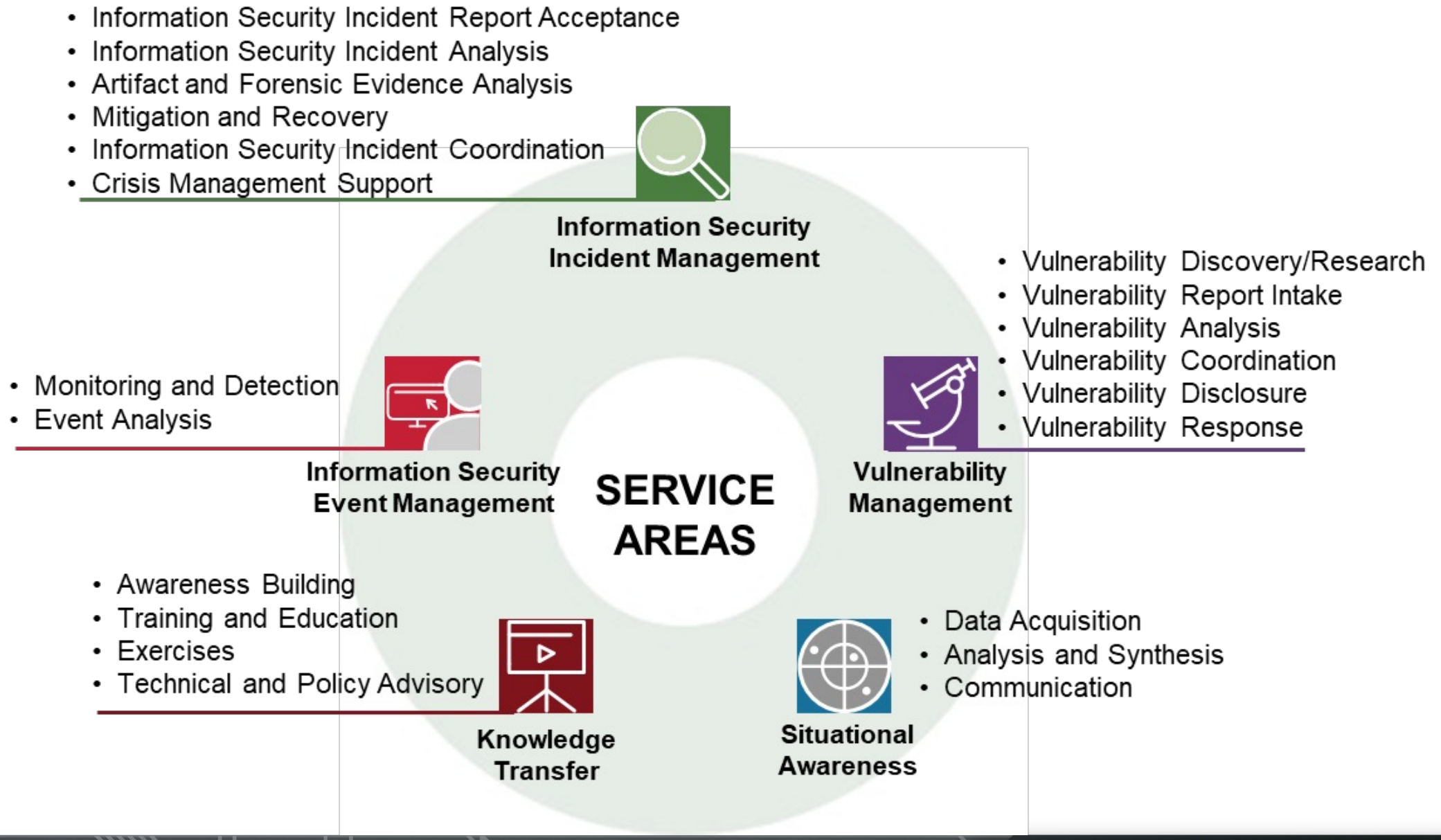
– *Press Release: FIRST Releases Traffic Light Protocol Version 2.0 with important updates*
https://www.first.org/newsroom/releases/20220805

CSIRT *Services Framework*

cert.br nic.br cgi.br

CSIRT *Services Framework v2.1*

TLP:CLEAR



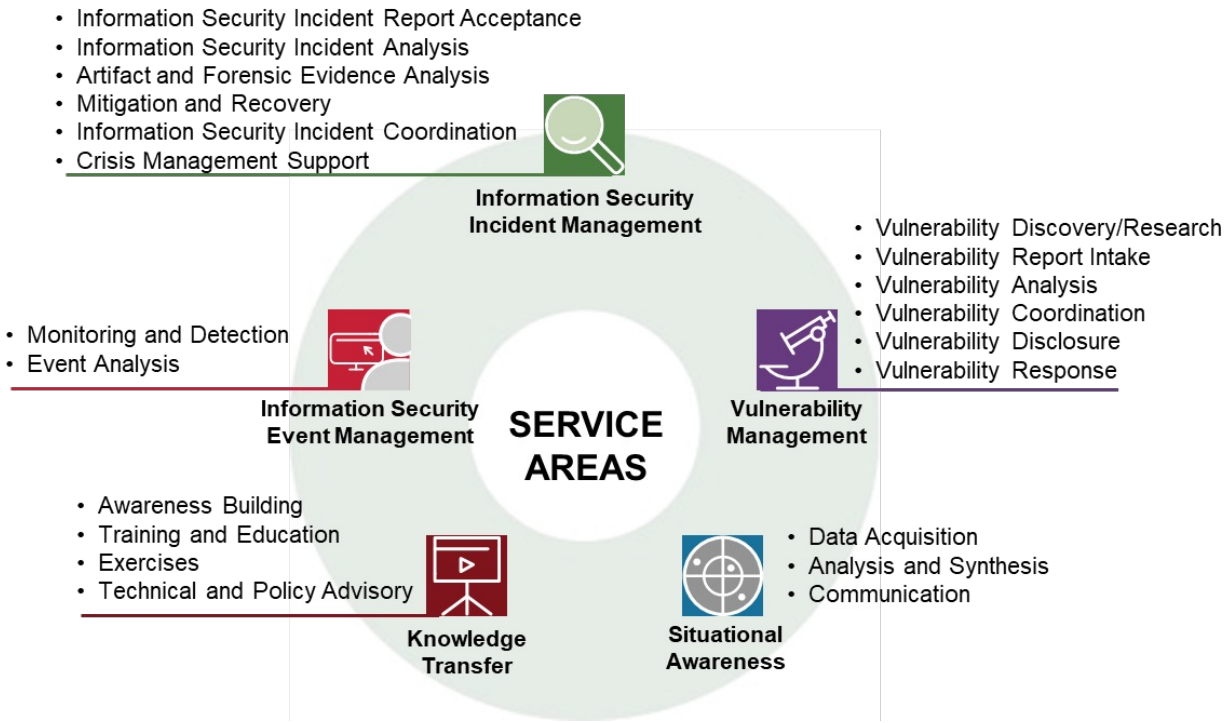
CSIRT *Services Framework v2.1*

Descrição em alto nível dos possíveis serviços que possam ser oferecidos

- por um CSIRT
- por times com serviços relacionados com gestão de incidentes

Visão do FIRST sobre o que são boas práticas

- Auxiliar times a
  - identificar e definir as principais categorias de serviços
  - um ponto de partida para a padronização de termos e definições a serem usados pela comunidade



https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

CSIRT *Services Framework v2.1 Addendum*

TLP:CLEAR

CSIRT Roles and Competences v0.9 - open for comments!

For each CSIRT services area

– *the applicable roles are listed in alphabetical order*

– *and described in more detail.*

– *the text for each role includes the following fields:*

Description – *Characteristics of the role context in the FIRST CSIRT Services Framework*

General Tasks – *List of tasks for the role based on the context, services, and service area*

Associated Functions from FIRST CSIRT Services Framework – *Reference to the specific functions*

Generic Competencies (from NICE) – *List of competencies in reference to the NICE Framework categories not specific to the role*

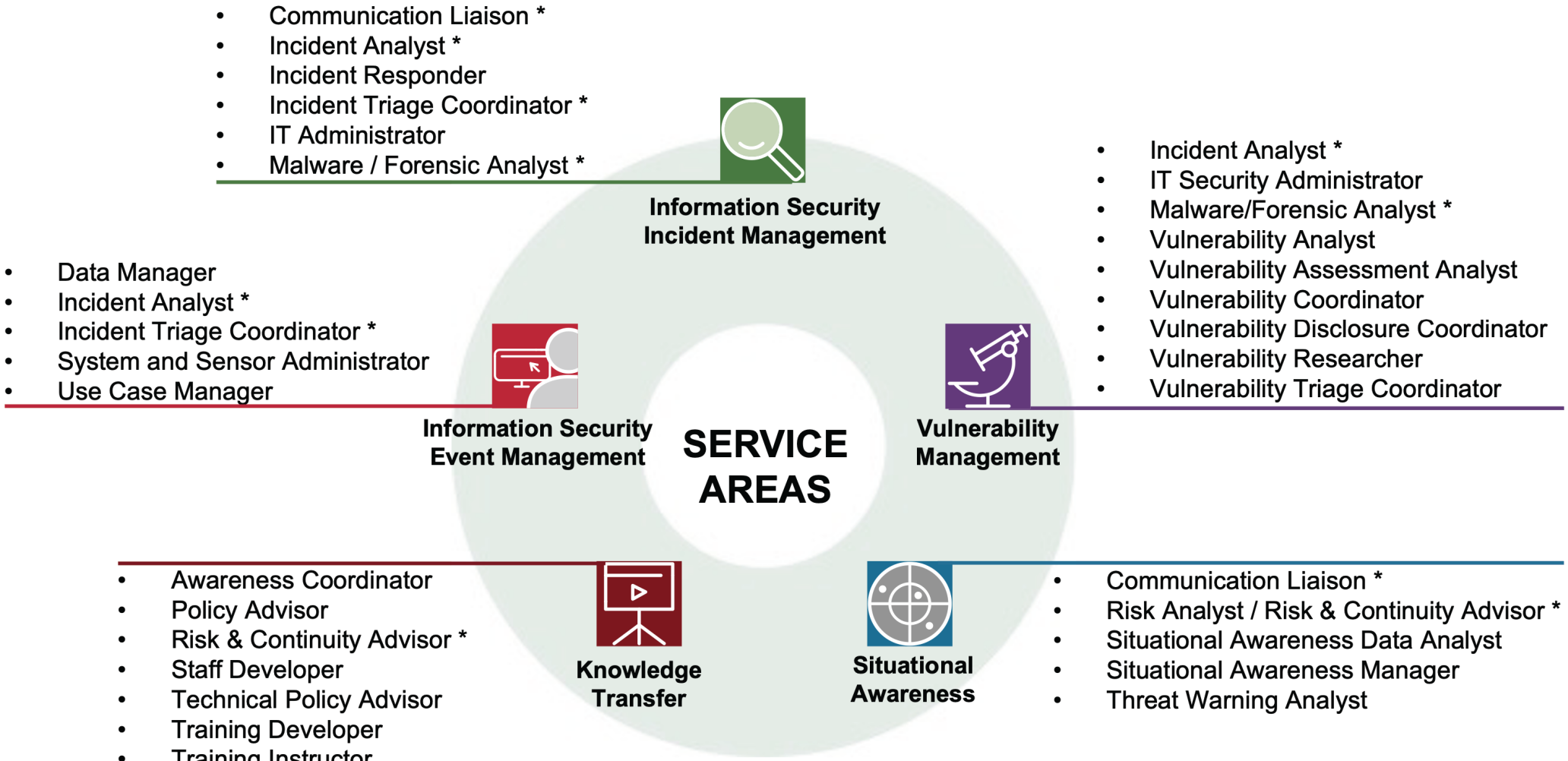
Role-Specific Competencies (from NICE) – *List of specific competencies for the role referenced to the NICE Framework categories*

https://www.first.org/standards/frameworks/csirts/csirt_roles_competences

CSIRT *Services Framework v2.1 Addendum*

CSIRT Roles and Competences v0.9 - open for comments!

TLP:CLEAR



* role defined for multiple service areas

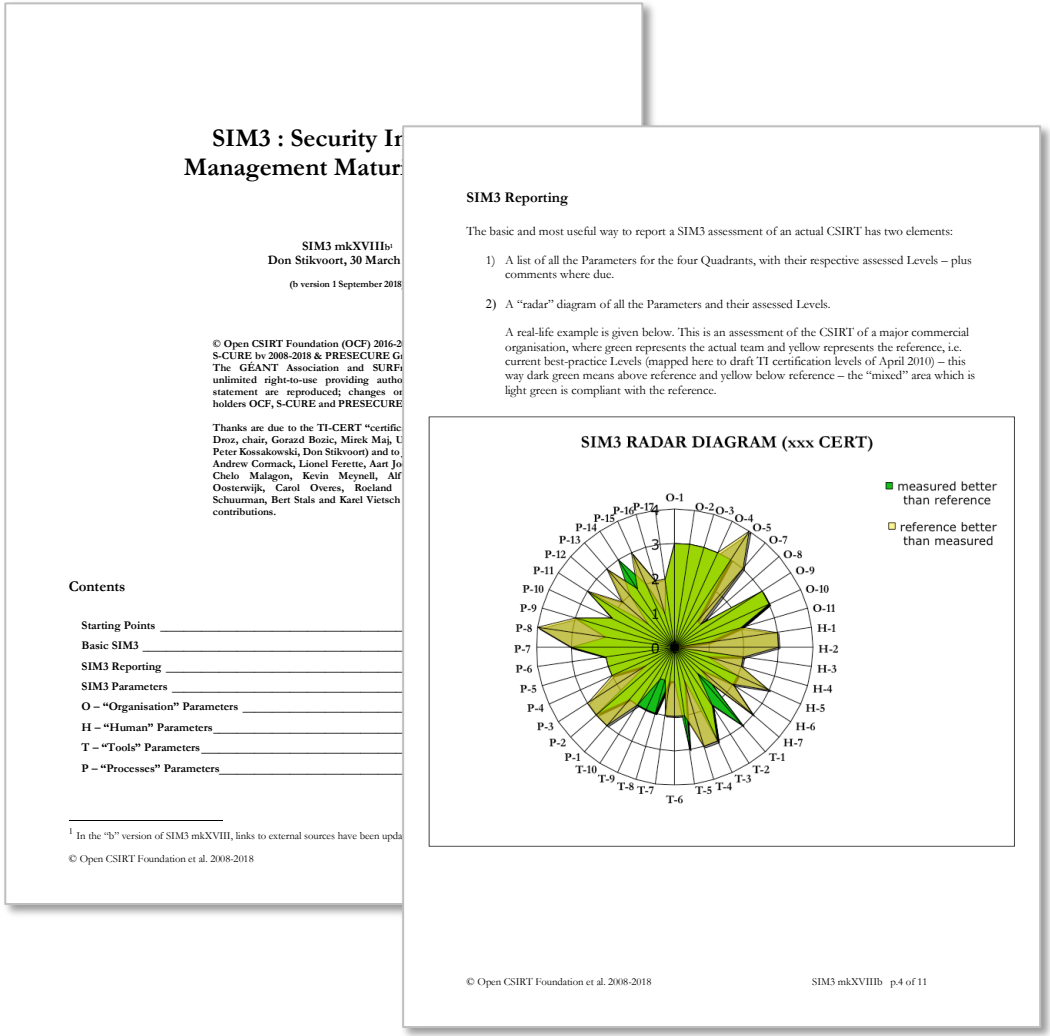
SIM3
Security Incident Management Maturity Model

cert.br nic.br cgi.br

TLP:CLEAR

SIM3 – *Security Incident Management Maturity Model*

- Quatro pilares
  - Prevenção
  - Detecção
  - Resolução
  - Controle de qualidade e *feedback*
- Quatro quadrantes
  - O – Organisation (11 parâmetros)
  - H – Human (7 parâmetros)
  - T – Tools (10 parâmetros)
  - P – Processes (17 parâmetros)
- Quem usa
  - TF-CSIRT Trusted Introducer
  - ENISA, requerimento para CERTs Nacionais (NIS Directive)
  - Nippon CSIRT Association
  - FIRST: será adotado no processo de filiação


SIM3 : Security In
Management Matur

SIM3 mkXVIIIb[1]
Don Stikvoort, 30 March

(b version 1 September 2018

© Open CSIRT Foundation (OCF) 2016-2
S-CURE bv 2008-2018 & PRESECURE G
The GÉANT Association and SURFn
unlimited right-to-use providing autho
statement are reproduced; changes or
holders OCF, S-CURE and PRESECURE

Thanks are due to the TI-CERT "certific
Droz, chair, Gorazd Bozic, Mirek Maj, U
Peter Kossakowski, Don Stikvoort) and to
Andrew Cormack, Lionel Ferette, Aart Jo
Chelo Malagon, Kevin Meynell, Alf
Oosterwijk, Carol Overes, Roeland
Schuurman, Bert Stals and Karel Vietsch
contributions.

Contents

Starting Points
Basic SIM3
SIM3 Reporting
SIM3 Parameters
O – "Organisation" Parameters
H – "Human" Parameters
T – "Tools" Parameters
P – "Processes" Parameters

[1] In the "b" version of SIM3 mkXVIII, links to external sources have been upda

© Open CSIRT Foundation et al. 2008-2018

SIM3 Reporting

The basic and most useful way to report a SIM3 assessment of an actual CSIRT has two elements:

1) A list of all the Parameters for the four Quadrants, with their respective assessed Levels – plus comments where due.
2) A "radar" diagram of all the Parameters and their assessed Levels.

A real-life example is given below. This is an assessment of the CSIRT of a major commercial organisation, where green represents the actual team and yellow represents the reference, i.e. current best-practice Levels (mapped here to draft TI certification levels of April 2010) – this way dark green means above reference and yellow below reference – the "mixed" area which is light green is compliant with the reference.

SIM3 RADAR DIAGRAM (xxx CERT)

© Open CSIRT Foundation et al. 2008-2018 SIM3 mkXVIIIb p.4 of 11

https://opencsirt.org/maturity/sim3/
https://www.thegfce.com/initiatives/c/csirt-maturity-initiative/documents/reports/2019/06/12/maturity-framework-for-national-csirts

TLP:CLEAR

SIM3: **Parâmetros**

0 = not available / undefined / unaware

1 = implicit (known/considered but not written down, “between the ears”)

2 = explicit, internal (written down but not formalized in any way)

3 = explicit, formalized on authority of CSIRT head (rubberstamped or published)

4 = explicit, audited on authority of governance levels above the CSIRT head (subject to control process/audit/enforcement)

Como usar:

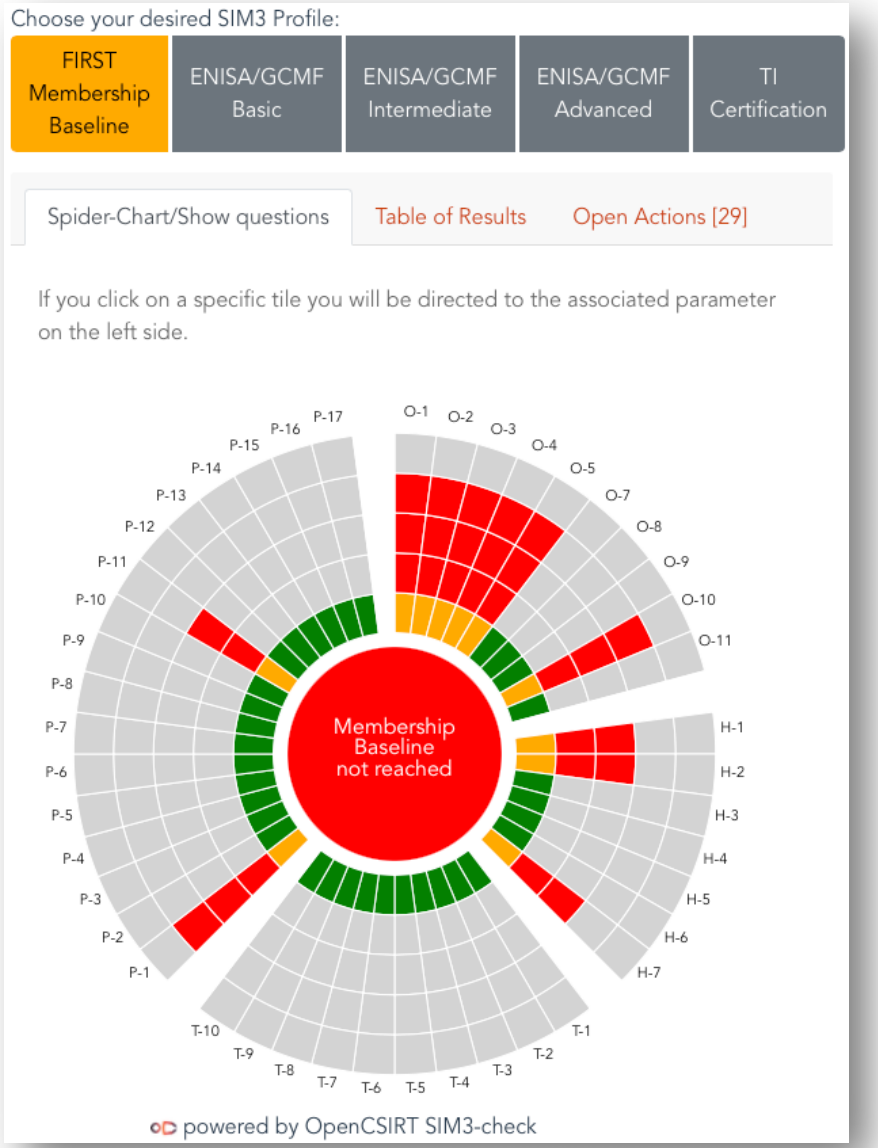
- Os parâmetros são em comum
- Cada comunidade escolhe os níveis de maturidade para seu contexto

ENISA CSIRT Maturity - Self-assessment Tool
https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity

Parameter number	Parameter description	Parameter number	Parameter description
O-1	Mandate	T-6	Resilient E-Mail
O-2	Constituency	T-7	Resilient Internet Access
O-3	Authority	T-8	Incident Prevention Toolset
O-4	Responsibility	T-9	Incident Detection Toolset
O-5	Service Description	T-10	Incident Resolution Toolset
O-7	Service Level Description	P-1	Escalation to Governance Level
O-8	Incident Classification	P-2	Escalation to Press Function
O-9	Integration in existing CSIRT Systems	P-3	Escalation to Legal Function
O-10	Organisational Framework	P-4	Incident Prevention Process
O-11	Security Policy	P-5	Incident Detection Process
H-1	Code of Conduct/Practice/Ethics	P-6	Incident Resolution Process
H-2	Personnel Resilience	P-7	Specific Incident Processes
H-3	Skillset Description	P-8	Audit/Feedback Process
H-4	Internal Training	P-9	Emergency Reachability Process
H-5	External Technical Training	P-10	Best Practice E-mail and Web Presence
H-6	(External) Communication Training	P-11	Secure Information Handling Process
H-7	External Networking	P-12	Information Sources Process
T-1	IT Resources List	P-13	Outreach Process
T-2	Information Sources List	P-14	Reporting Process
T-3	Consolidated E-Mail System	P-15	Statistics Process
T-4	Incident Tracking System	P-16	Meeting Process
T-5	Resilient Phone	P-17	Peer-to-Peer Process

SIM3 – Perfis

- Quem define os perfis são as comunidades
  - o SIM3 em si não tem níveis a serem atingidos
  - o objetivo não é ter 4 em todos os parâmetros!
- Perfis atuais
  - *First Membership Baseline*
  - *ENISA/GCMF Basic*
  - *ENISA/GCMF Intermediate*
  - *ENISA/GCMF Advanced*
  - *TI Certification*



https://sim3-check.opencsirt.org/

Obrigada

cristine@cert.br

Notificações para: cert@cert.br

@certbr

https://cert.br/

25 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br