nic.br cgi.br | cert.br

Autoridade Nacional de Proteção de Dados, ANPD

05 de março de 2021 | Evento *Online*

Gestão de Riscos e de Incidentes no Contexto da Proteção de Dados

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

Dr. Klaus Steding-Jessen
Gerente Técnico
jessen@cert.br

cert.br nic.br cgi.br

cert.br

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 Político

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/

Foco do CERT.br nestes 23 anos:
Aumentar a Capacidade Nacional de Tratamento de Incidentes

Nenhum grupo ou estrutura única conseguirá fazer sozinho a segurança ou a resposta a incidentes

Comunidade Nacional

- Ações junto a setores chave, para **criação e treinamento de Grupos** de Tratamento de Incidentes de Segurança (CSIRTs)
- **Auxiliar na análise** técnica e **facilitar** o tratamento de incidentes por outros CSIRTs
- Gerar massa crítica para possibilitar a **cooperação** e melhora na segurança das redes
- Ter uma visão sobre as principais **tendências** de ataques no Brasil

Comunidade Internacional

- Estabelecer **relações de confiança**
  - facilitar a comunicação em casos de incidentes
  - dar acesso a informações que ajudem a comunidade local
- **Influenciar** os padrões e certificações sendo construídos para CSIRTs
- Levar a **visão nacional** aos fóruns pertinentes

Contexto

cert.br nic.br cgi.br

Antes de Falar em Gestão de Incidentes:
Análise e Gestão de Riscos é Pré-requisito

Riscos:
- indisponibilidade de serviços
- furto ou destruição de dados
- perda de privacidade
- perdas financeiras
- danos à imagem
- perda de confiança na tecnologia

Ativos
(Sistemas, Dados e Pessoas)

Ameaças

- criminosos
- espionagem industrial
- governos
- vândalos

Vulnerabilidades

- projeto sem priorizar segurança
- defeitos de *software*
- falhas de configuração
- uso inadequado / falha humana
- fraquezas advindas da complexidade dos sistemas

Opções para lidar com o risco:

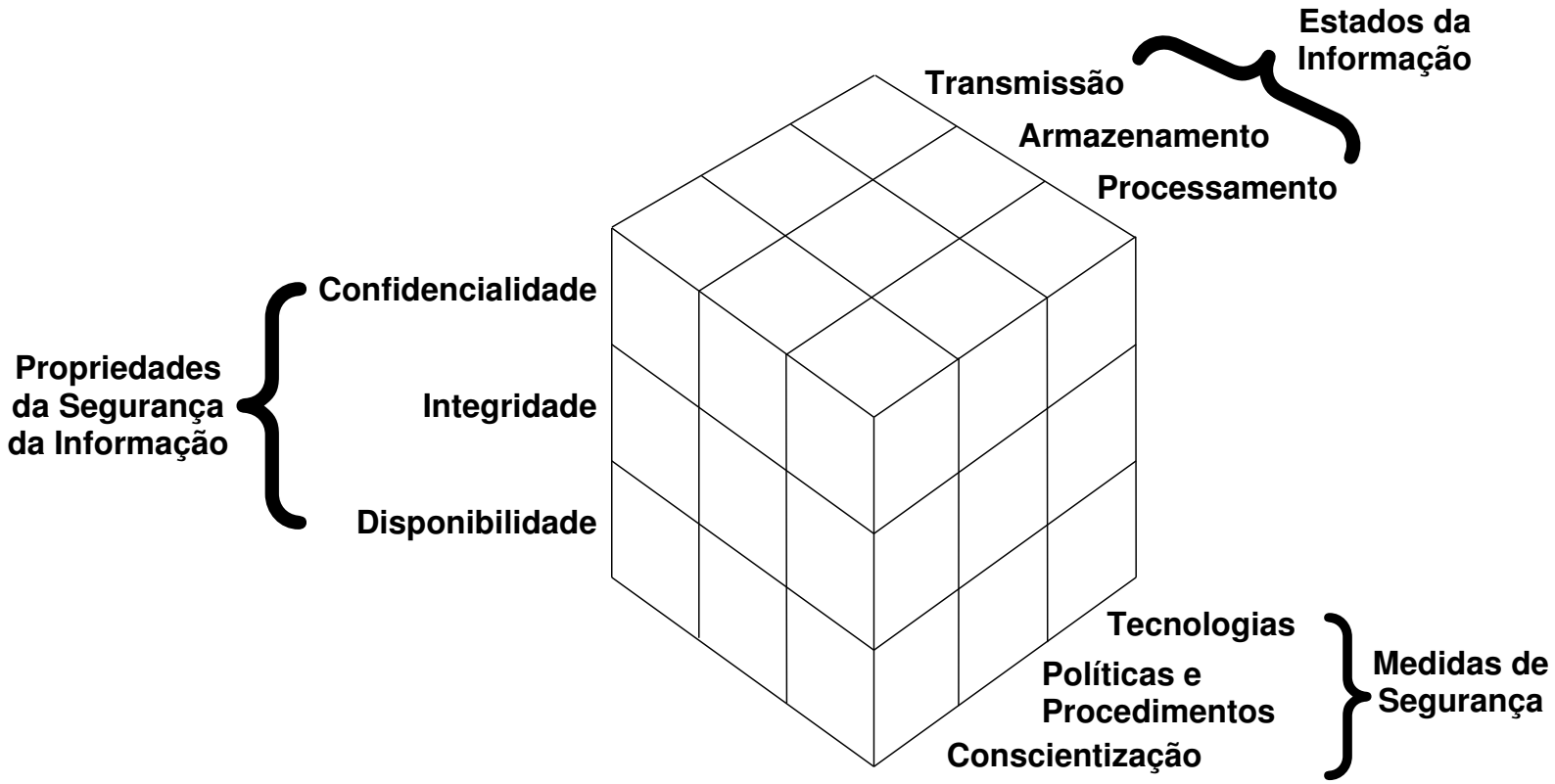
Aceitar

Transferir
- ex: seguro

Eliminar
- remover um dos vértices

Mitigar (gestão de risco)
- única real opção

Segurança da Informação:
É um Processo Complexo



McCumber Information Security Model
http://www.ibm.com/developerworks/security/library/s-confnotes2/

Considerações:

Os dados estão em diversos locais e a segurança depende de múltiplos fatores

Não é possível "garantir" segurança

- fator humano (*insiders*)
- novas vulnerabilidades (*0-day vulnerabilities*)
- sistemas legados (*n-day/forever-day vulnerabilities*)

É possível:

- mitigar os riscos e reduzir a probabilidade de vazamentos e acessos indevidos
- **ter gestão de incidentes: detectar precocemente e reduzir os danos**

Incidentes Observados pelo CERT.br:
Causas Mais Comuns de Invasões e Vazamentos

Ataques mais reportados e mais observados em sensores:

- Força bruta de senhas em serviços protegidos só com conta e senha. Exemplos:
  - *e-mails* e serviços em nuvem
  - acesso remoto e gestão remota de ativos de rede e servidores
- Comprometimento via exploração de vulnerabilidades conhecidas
  - falta de aplicação de correções
  - erros de configuração
  - falta/falha de processos

Mais de 80% dos incidentes seriam evitados se

- todas as correções (*patches*) fossem aplicadas
- houvesse mais atenção a erros e configurações
- todos os serviços tivessem 2FA/MFA

É necessário focar no básico

- *Patches* + configuração segura (*hardening*)
- Adotar MFA (*Multi-Factor Authentication*)
  - ex: aplicativo autenticador ou *token* (ex: Yubikey)
  - motivos usuais para não adoção
    - diminui a conveniência e pode ter custos
    - requer treinamento dos técnicos e usuários
    - medo de perder acesso aos serviços

Fonte: Principais Ataques na Internet: Dados do CERT.br
https://youtu.be/nHh8hHaomFE?t=714
https://cert.br/stats/

Mas existem os outros 20% dos incidentes:
Organizações Precisam Alcançar Resiliência

Um sistema 100% seguro é impossível de atingir: incidentes ocorrerão

Resiliência: Continuar funcionando mesmo na presença de falhas ou ataques

***Checklist*:**

- **Identificar o que é crítico** e precisa ser mais protegido (Análise de Risco)
- **Definir políticas** (de uso aceitável, acesso, segurança, etc)
- **Treinar profissionais** para implementar as estratégias e políticas de segurança
- **Treinar e conscientizar os usuários** sobre os riscos e medidas de segurança necessários
- **Implantar medidas de segurança** que implementem as políticas de segurança
  - ex: aplicar correções ou instalar ferramentas de segurança
- Formular **estratégias e processos para gestão de incidentes** de segurança e formalizar **grupos de tratamento de incidentes (CSIRTs)**

Gestão de Incidentes

cert.br nic.br cgi.br

Gestão de Incidentes: **Definições**

Incidente de Segurança – cada organização tem sua própria definição, em geral com base na missão, serviços e recursos disponíveis.

Gestão de Incidentes – políticas e estratégias

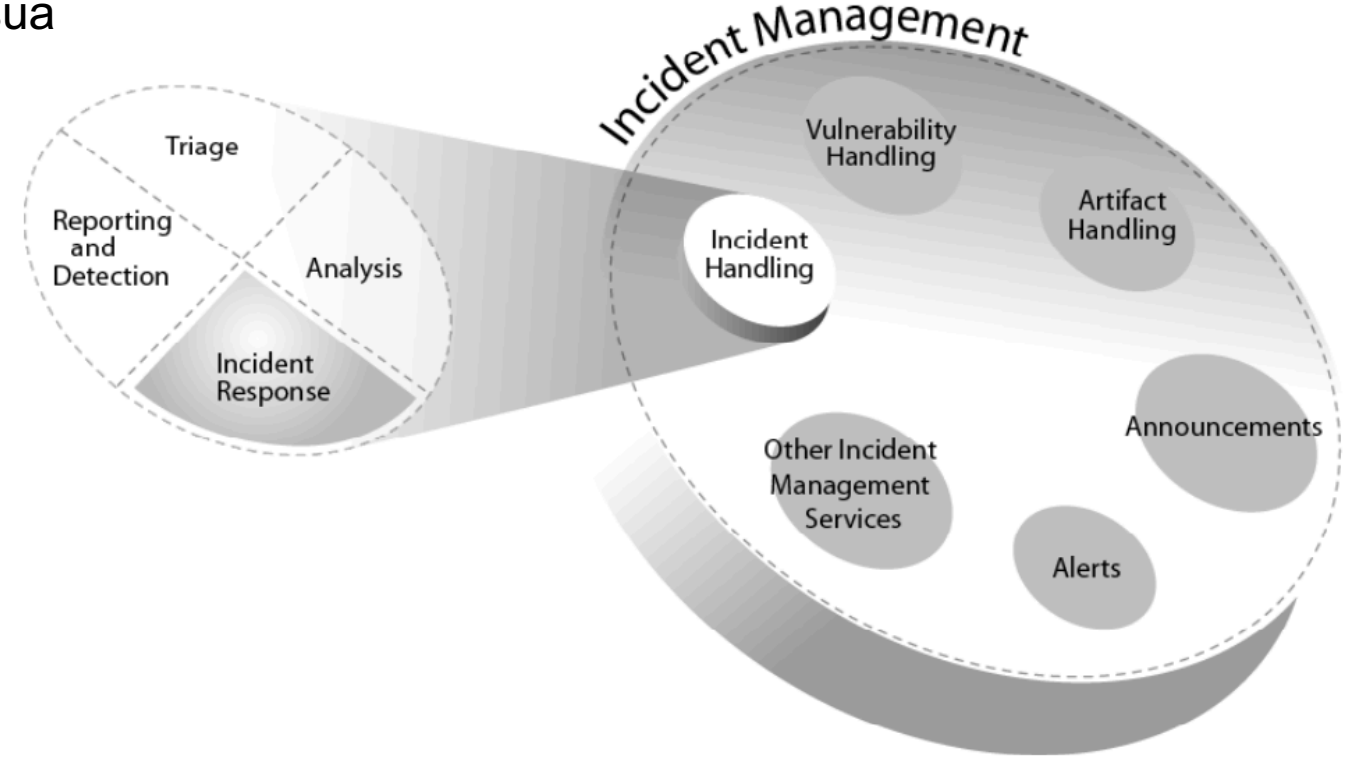
- gestão fim a fim de eventos e incidentes
- envolve toda a organização

Tratamento de Incidentes – processos

- identificar, prevenir, mitigar e responder

Resposta a Incidentes – ações

- resolver ou mitigar incidentes
- disseminar informações
- implementar estratégias para impedir que o incidente ocorra novamente



Fonte: *Defining Incident Management Processes for CSIRTs: A Work in Progress*. Figura utilizada com permissão do CERT®/CC e do SEI/CMU.
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153

Gestão de Incidentes: **Processos**

Preparação da organização

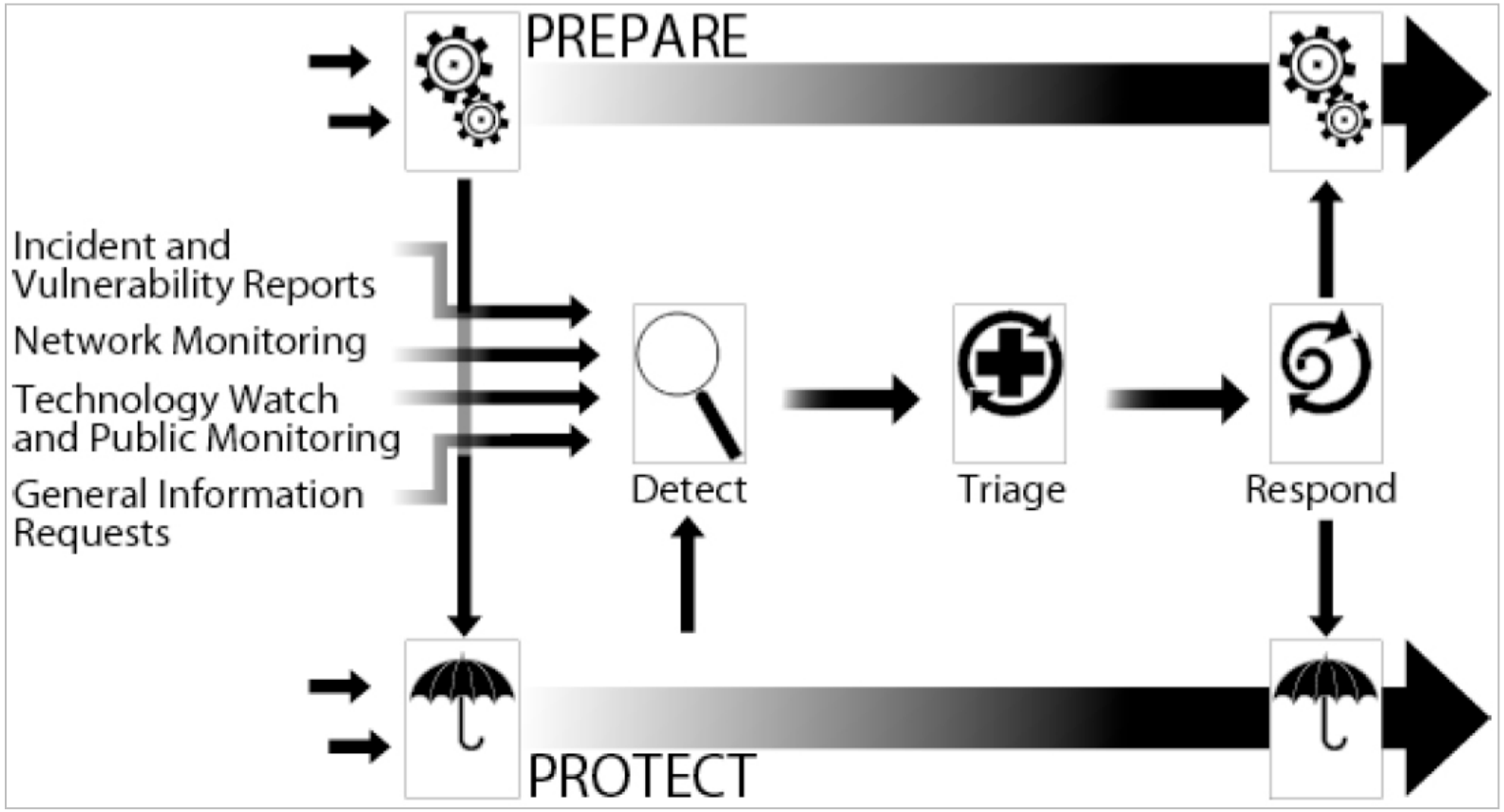
- reconhecer a importância do adequado tratamento de incidentes
- estabelecer políticas para notificação
- planejar e implantar um CSIRT

Proteção da infraestrutura

- processo contínuo de implementação de medidas de segurança

Tratamento de incidentes

- recebe informações de, e alimenta os outros processos
- depende de integração com todas as áreas e alta qualificação das equipes



Fonte: ***Defining Incident Management Processes for CSIRTs: A Work in Progress*****. Figura utilizada com permissão do CERT®/CC e do SEI/CMU.**
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153

O que é um CSIRT

A CSIRT is an organizational unit (which may be virtual) or a capability that provides services and support to a defined constituency for preventing, detecting, handling, and responding to computer security incidents, in accordance with its mission.

Fonte: *FIRST CSIRT Services Framework*
https://www.first.org/standards/frameworks/csirts/

O que um CSIRT não é

- Vítima
- Atacante
- Auditor
- Investigador
- Regulador
- Polícia

Questões chave para o sucesso de um CSIRT

- Criar relações de confiança
- Ter uma rede de contatos
  - especialistas e outros CSIRTs
- Criar um ambiente favorável à notificação
  - sem caráter punitivo
  - sem possibilidade de impacto de auditoria

Características de uma notificação de incidente

- Informal
- Foco é pedir ajuda
- Requer análise técnica para verificar
  - se é mesmo incidente
  - qual a natureza do incidente
  - qual o escopo

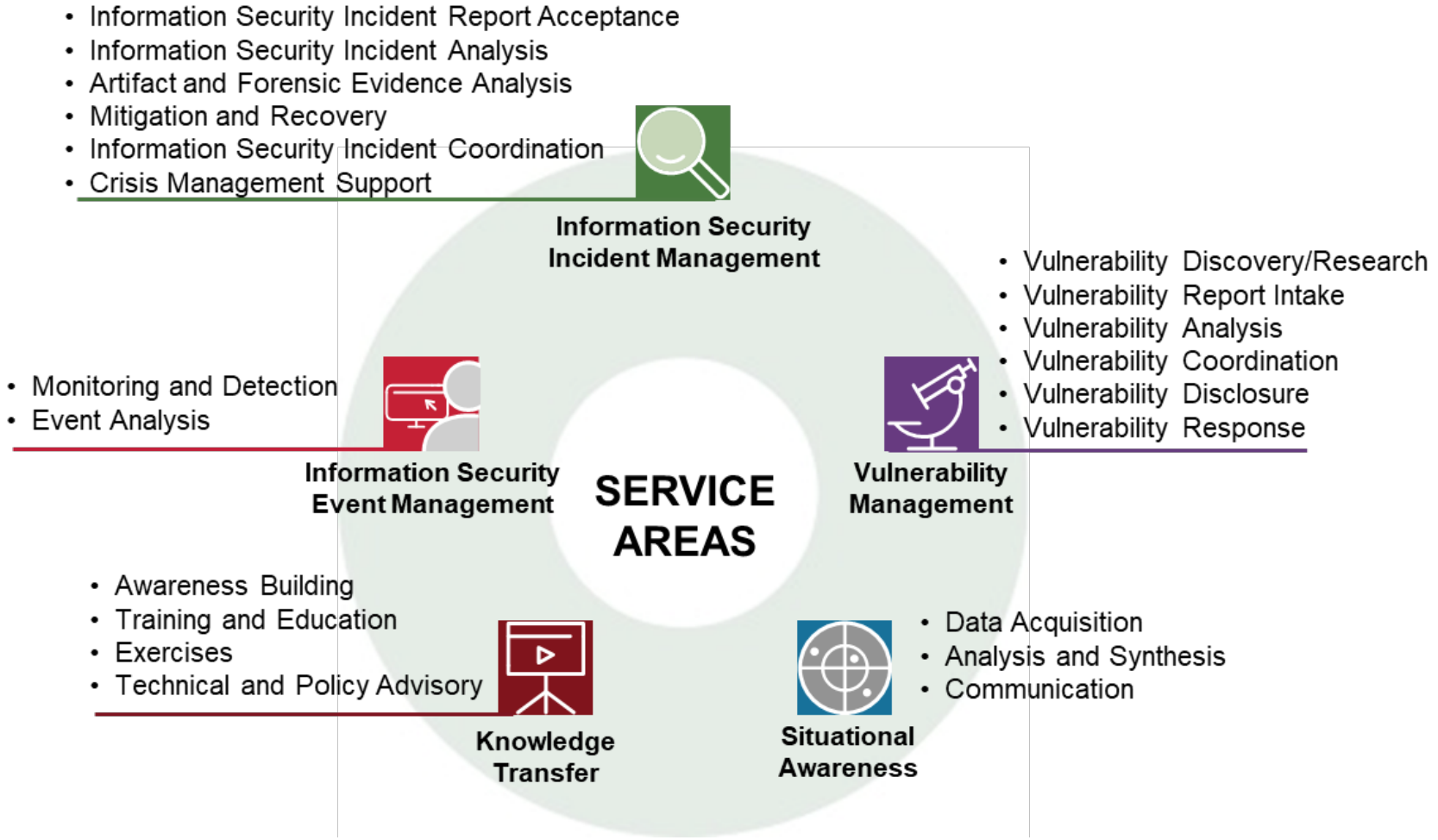
FIRST CSIRT Services Framework: **Estabelecimento e Melhoria Contínuas da Gestão de Incidentes**

"The Computer Security Incident Response Team (CSIRT) Services Framework is

- *a high-level document*
- *describing in a structured way*
- *a collection of cyber security services and associated functions*

that Computer Security Incident Response Teams and other teams providing incident management related services may provide."

"The services described are those potential services a CSIRT could provide. No CSIRT is expected to provide all described services."



***Computer Security Incident Response Team (CSIRT) Services Framework*:**
https://www.first.org/standards/frameworks/csirts/

FIRST CSIRT Services Framework: **Estrutura, Autores e Próximos passos**

Estrutura

Formato de cada área

- *Service Area*
  - *Service*
    - *Function*
      - *Sub-Function*

Próximos passos

- matriz de competências
- material de treinamento

Autores

Editor

- Klaus-Peter Kossakowski, Hamburg University of Applied Science

Coordenadores de área

- Olivier Caleff, OpenCSIRT Foundation (FR)
- **Cristine Hoepers, CERT.br/NIC.br (BR)**
- Amanda Mullens, CISCO (US)
- Samuel Perl, CERT/CC (US)
- Daniel Roethlisberger, Swisscom (CH)
- Robin M. Ruefle, CERT/CC (US)
- Mark Zajicek, CERT/CC (US)

Contribuidores

- Vilius Benetis, NRD CIRT (LT)
- Angela Horneman, CERT/CC (US)
- Allen Householder, CERT/CC (US)
- Art Manion, CERT/CC (US)
- Sigitas Rokas, NRD CIRT (LT)
- Mary Rossell, Intel (US)
- Désirée Sacher, Finanz Informatik (DE)
- Krassimir T. Tzvetanov, Fastly (US)

FIRST CSIRT Services Framework:
Overview of all CSIRT Services and related Functions

SERVICE AREA
Information Security Event Management

Monitoring and Detection
- Log and Sensor Management
- Detection Use Case Management
- Contextual Data Management

Event Analysis
- Correlation
- Qualification

SERVICE AREA
Information Security Incident Management

Information Security Incident Report Acceptance
- Information Security Incident Report Receipt
- Information Security Incident Triage and Processing

Information Security Incident Analysis
- Information Security Incident Triage (Prioritization and Categorization)
- Information Collection
- Detailed Analysis Coordination
- Information Security Incident Root Cause Analysis
- Cross-Incident Correlation

Artifact and Forensic Evidence Analysis
- Media or Surface Analysis
- Reverse Engineering
- Runtime or Dynamic Analysis
- Comparative Analysis

Mitigation and Recovery
- Response Plan Establishment
- Ad Hoc Measures and Containment
- System Restoration
- Other Information Security Entities Support

Information Security Incident Coordination
- Communication
- Notification Distribution
- Relevant Information Distribution
- Activities Coordination
- Reporting
- Media Communication

Crisis Management Support
- Information Distribution to Constituents
- Information Security Status Reporting
- Strategic Decisions Communication

SERVICE AREA
Vulnerability Management

Vulnerability Discovery/Research
- Incident Response Vulnerability Discovery
- Public Source Vulnerability Discovery
- Vulnerability Research

Vulnerability Report Intake
- Vulnerability Report Receipt
- Vulnerability Report Triage and Processing

Vulnerability Analysis
- Vulnerability Triage (Validation and Categorization)
- Vulnerability Root Cause Analysis
- Vulnerability Remediation Development

Vulnerability Coordination
- Vulnerability Notification/Reporting
- Vulnerability Stakeholder Coordination

Vulnerability Disclosure
- Vulnerability Disclosure Policy and Infrastructure Maintenance
- Vulnerability Announcement/ Communication/Dissemination
- Post-Vulnerability Disclosure Feedback

Vulnerability Response
- Vulnerability Detection/Scanning
- Vulnerability Remediation

SERVICE AREA
Situational Awareness

Data Acquisition
- Policy Aggregation, Distillation, and Guidance
- Asset Mapping to Functions, Roles, Actions, and Key Risks
- Collection
- Data Processing and Preparation

Analysis and Synthesize
- Projection and Inference
- Event Detection (through Alerting and/or Hunting)
- Situational Impact

Communication
- Internal and External Communication
- Reporting and Recommendations
- Implementation

SERVICE AREA
Knowledge Transfer

Awareness Building
- Research and Information Aggregation
- Report and Awareness Materials Development
- Information Dissemination
- Outreach

Training and Education
- Knowledge, Skill, and Ability Requirements Gathering
- Educational and Training Materials Development
- Content Delivery
- Mentoring
- CSIRT Staff Professional Development

Exercises
- Requirements Analysis
- Format and Environment Development
- Scenario Development
- Exercise Execution
- Exercise Outcome Review

Technical and Policy Advisory
- Risk Management Support
- Business Continuity and Disaster Recovery Planning Support
- Policy Support
- Technical Advice

Gestão de Incidentes não está Isolada:
Pode ser Encontrada em Outros *Frameworks*

"The Framework is

- *voluntary guidance,*
- *based on existing standards, guidelines, and practices*
- *for organizations to better manage and reduce cybersecurity risk.*

In addition to helping organizations manage and reduce risks, it was designed to

- *foster risk and cybersecurity management communications*
- *amongst both internal and external organizational stakeholders."*

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Incident Management

Original em Inglês e tradução para o Português disponíveis em:
https://www.nist.gov/cyberframework/framework
https://www.uschamber.com/sites/default/files/intl_nist_framework_portugese_finalfull_web.pdf

Dinâmica de Trabalho dos CSIRTs e Relação com Eficiência, Efetividade e Maturidade

cert.br nic.br cgi.br

Tratamento de Incidentes:
Pessoas e Relações de Confiança Fazem a Diferença

Incidentes não acontecem no vácuo

– envolvem múltiplas organizações, redes e países

– resolução requer análise de informações internas e externas

CSIRTs operam em um esquema de governança em rede

– não há hierarquia

– há a construção de redes de confiança globais e locais

Diversas Comunidades formadas ao redor do Globo

– FIRST – TF-CSIRT – APCERT – AfricaCERT

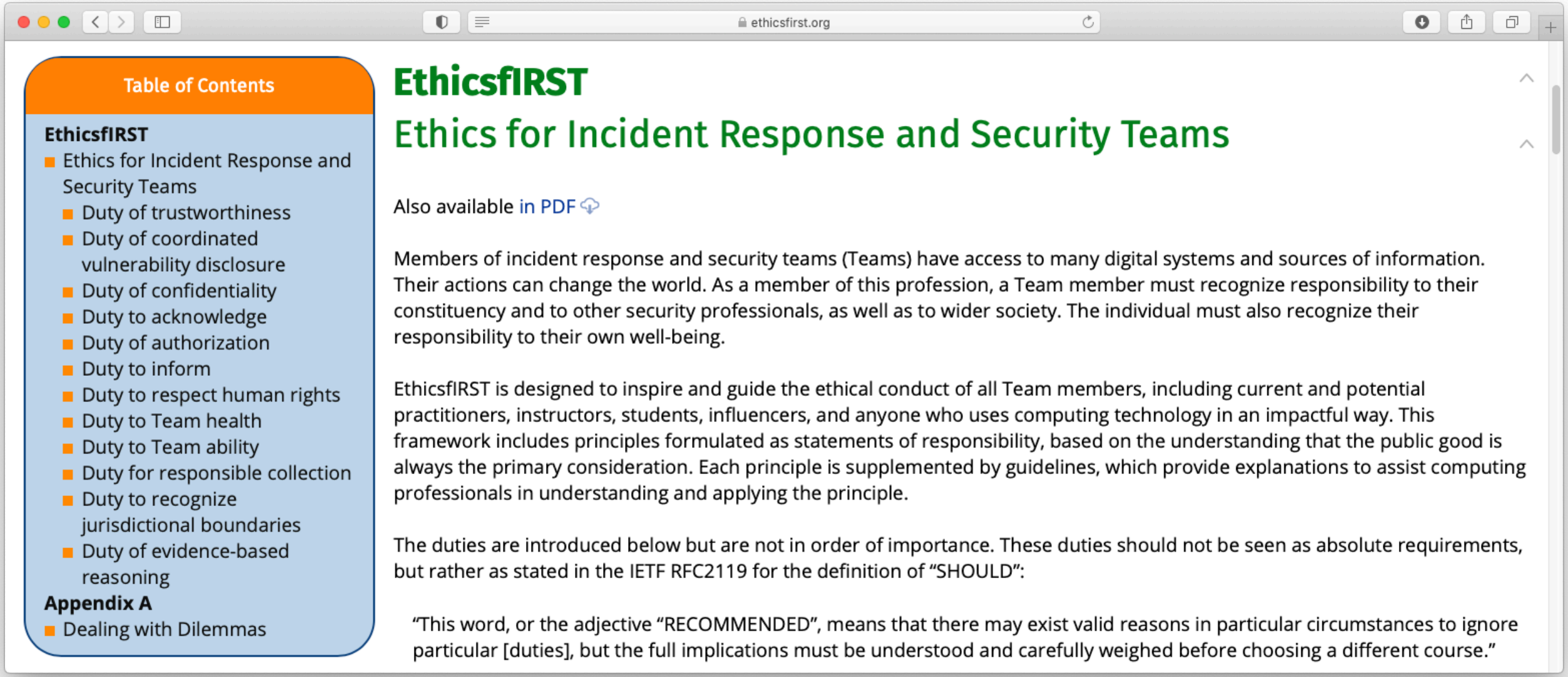
– NatCSIRTs – EU e-CSIRT Network – LAC-CSIRTs – OIC-CERT

Maturidade evoluiu para um código de ética e modelos de acreditação e certificação

– SIM3 – EthicsfIRST

– TF-CSIRT Trusted Introducer

EthicsfIRST.org:
Código de Ética da Comunidade Global de CSIRTs



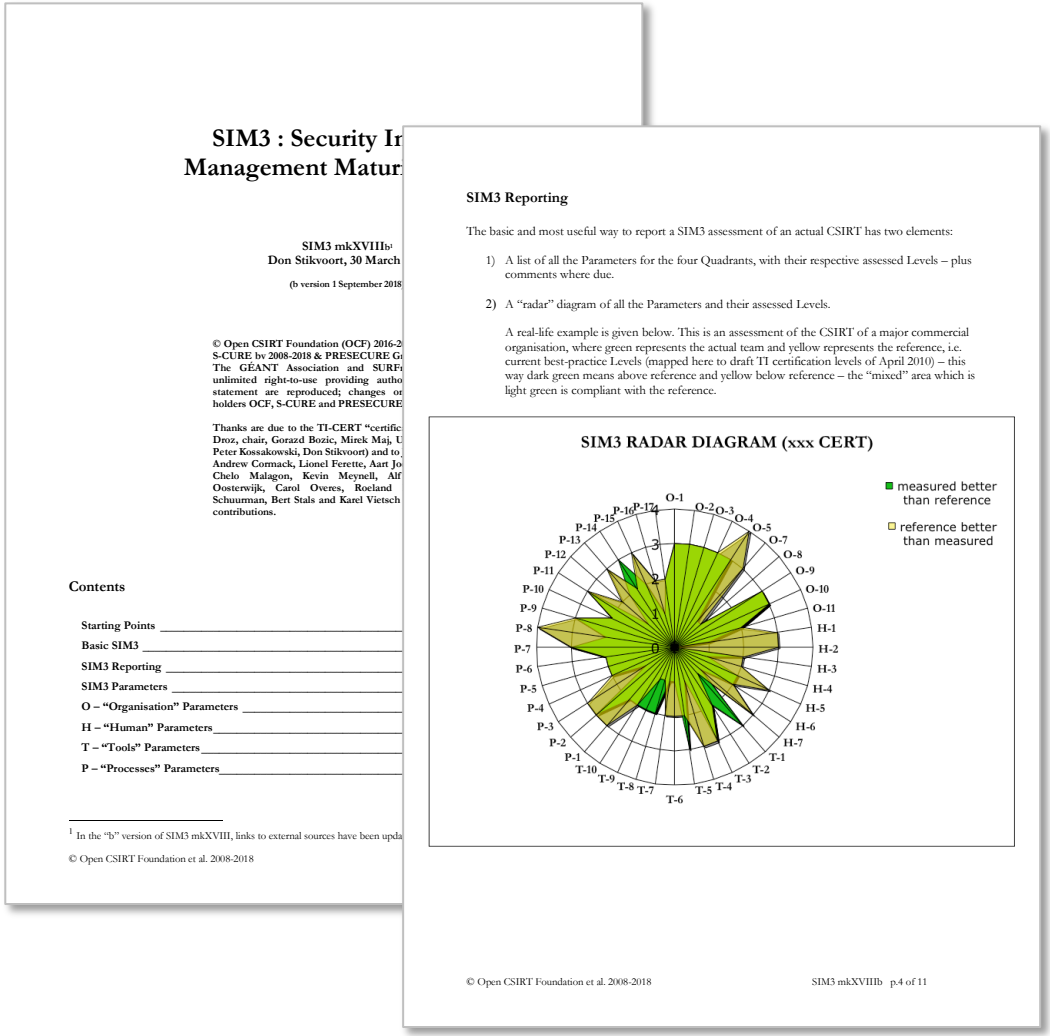
Avaliação de Maturidade:
SIM3 – *Security Incident Management Maturity Model*

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)

Como usar
– Cada comunidade escolhe os níveis de maturidade para seu contexto
– Os parâmetros são o ponto em comum

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://thegfce.org/initiatives/csirt-maturity-initiative/

SIM3:
Online Tool

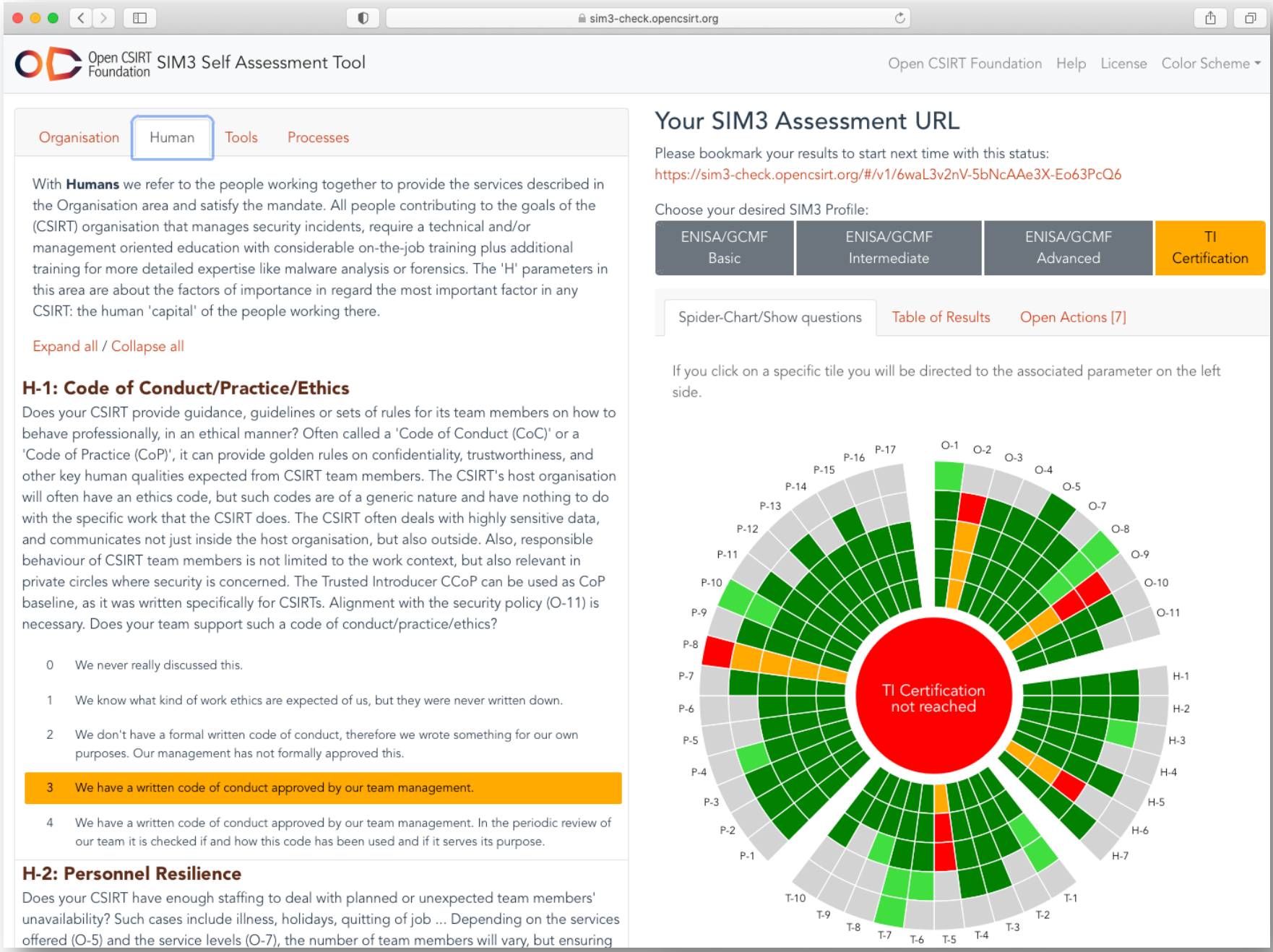
Auto avaliação em forma de perguntas

Possui 4 perfis

- *Trusted Introducer TI Certification*
- ENISA
  - *Basic*
  - *Intermediate*
  - *Advanced*

Será incluído um perfil para o FIRST, quando for adotado para filiação

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



Considerações Finais

cert.br nic.br cgi.br

Segurança é Papel de Todos:
Ecossistema é Complexo e Interdependente

Quase tudo é *software* e está conectado à Internet

- Empresas "tradicionais" agora são empresas de *software*

Ataques são constantes

- Motivações diversas
- Volume crescente
  - ferramentas facilitam a perpetração por atacantes não especializados

Organizações precisam

- Operar mesmo sob ataque
- Estar preparadas para lidar com estes ataques

Melhora do cenário depende de cada ator fazer sua parte

Atividades de Fomento do CERT.br:
Criação de Uma Comunidade Atuante

Foco

- Criar/aproximar CSIRTs (Grupos de Tratamento de Incidentes de Segurança) no Brasil
- Possuir profissionais preparados para resolver os problemas de segurança no país

Fórum Brasileiro de CSIRTs

- Evento anual para profissionais da área de Tratamento de Incidentes
- *Workshops* sobre assuntos específicos

Lista de CSIRTs Brasileiros

- https://cert.br/csirts/brasil/

Fomento à adoção de MISP

- https://cert.br/misp/

Cursos de Gestão de Incidentes

Ministra os cursos do *CERT® Division, do SEI/Carnegie Mellon,* desde 2004:

- https://cert.br/cursos/

SEI Partner Network

Obrigado

cristine@cert.br jessen@cert.br

notificações para: cert@cert.br @certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br