nic.br cgi.br | cert.br

II Seminário de Segurança e Defesa Cibernética
Desafios da Defesa Cibernética na Projeção Espacial Brasileira

03 de novembro de 2020

Grupos de Tratamento de Incidentes de Segurança (CSIRTs): Cenário Global, Maturidade e Padrões

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

cert.br nic.br cgi.br

É Possível Segurança 100%?

cert.br nic.br cgi.br

Ambientes de Operação (TO) e Infraestruturas Críticas: **Realidades e Desafios para a Gestão dos Riscos**

Safety* vs. *Security

- *Safety*: foco em tolerância a falhas, em manter operando por anos, com o menor número de intervenções possíveis
- *Security*: foco em impedir ou conter ataques, identificar vulnerabilidades e manter constantemente atualizado

Mentalidade de *safety* predomina

- Sistemas feitos para rodar por anos
- Projetos não preveem mecanismos de atualização e gerência remota
- Processos não acomodam a necessidade de atualizações e correções constantes

Sistemas Legados

- Sistemas utilizam *softwares* de uso geral (por exemplo, Sistemas Operacionais “de prateleira”)
- Sem haver previsão de atualização constante, é necessário monitorar de maneira redobrada
- Estar preparado para detectar e conter ataques, sabendo que está vulnerável

Processos e pessoas são mais importantes que ferramentas

Exemplos Concretos da Dificuldade de Impedir a Invasão de Sistemas

- Comprometimento da RSA/EMC, para furto de material criptográfico – levou ao comprometimento do DoD (*US Department of Defense*)
  https://www.sec.gov/Archives/edgar/data/790070/000119312511070159/dex991.htm

- Comprometimento do *Office of Personnel Management*, para furto dos antecedentes de todos os funcionários do Governo Americano
  https://www.opm.gov/cybersecurity/cybersecurity-incidents

- Comprometimento da Autoridade Certificadora da Holanda – usada para gerar chaves falsas do Google, usadas em espionagem no Irã
  http://www.slate.com/articles/technology/future_tense/2016/12/how_the_2011_hack_of_diginotar_changed_the_internet_s_infrastructure.html

Frameworks: Organizam Pessoas, Processos e Tecnologias

cert.br nic.br cgi.br

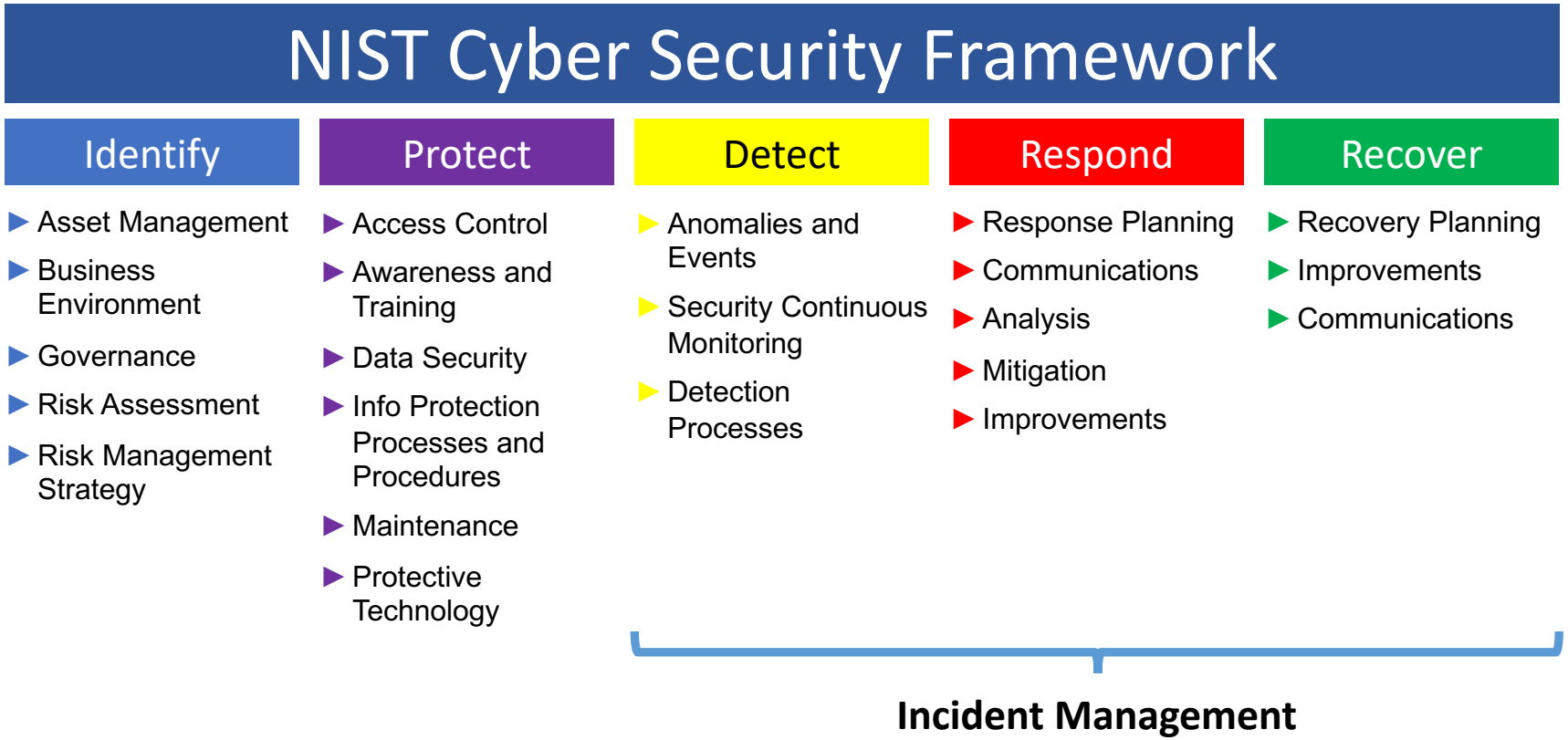
NIST Cyber Security Framework: **Segurança e Gestão de Riscos em Ambientes Complexos**

"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."*



Original em Inglês e tradução para o Português disponíveis em:
https://www.nist.gov/cyberframework/framework

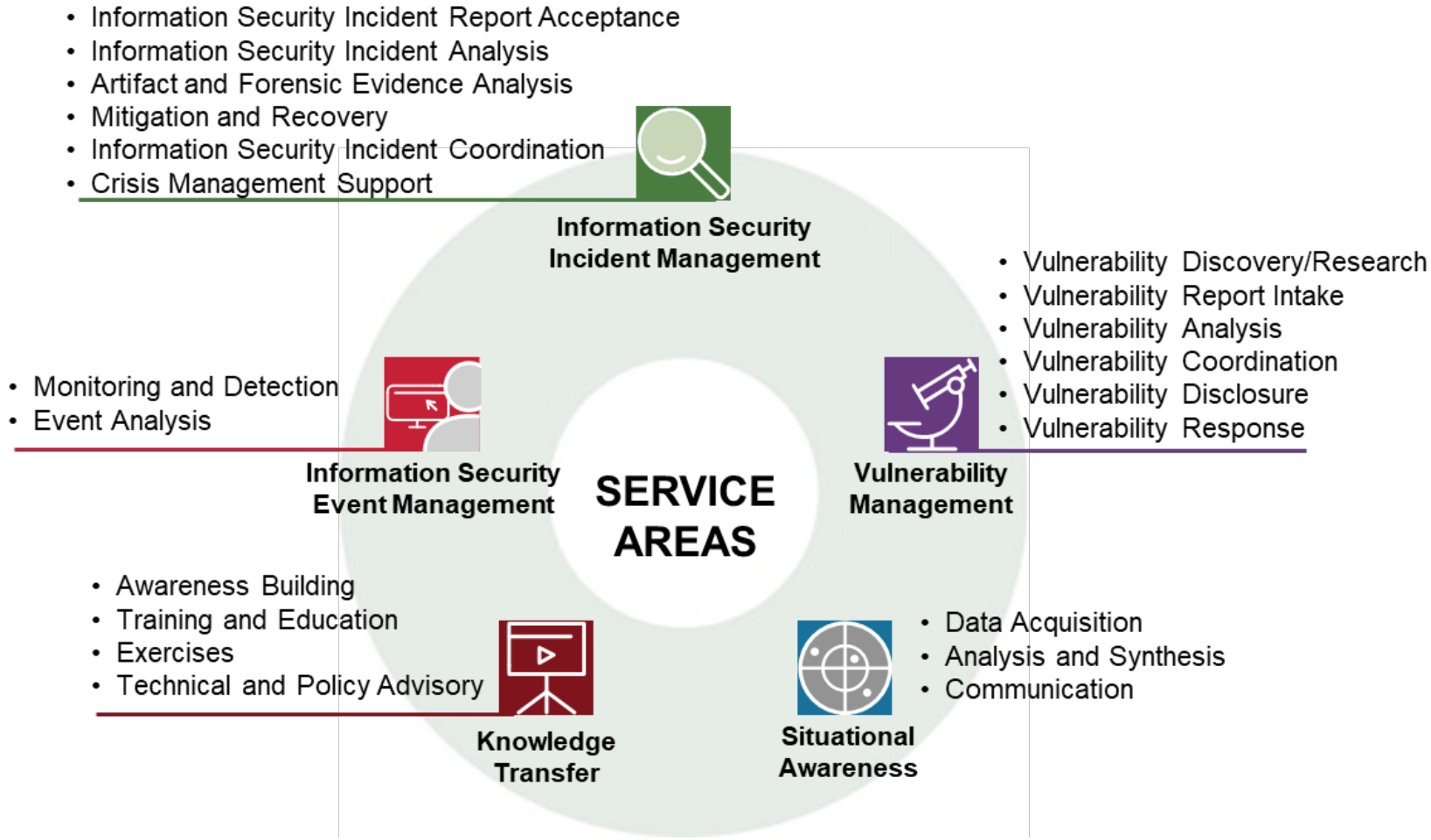
FIRST CSIRT Services Framework:
Estabelecimento e Melhoria Contínuas da Gestão de Incidentes

"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

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 modelos de Acreditação e Certificação

– SIM3

– TF-CSIRT Trusted Introducer

SIM3 – *Security Incident Management Maturity Model*

Quatro pilares

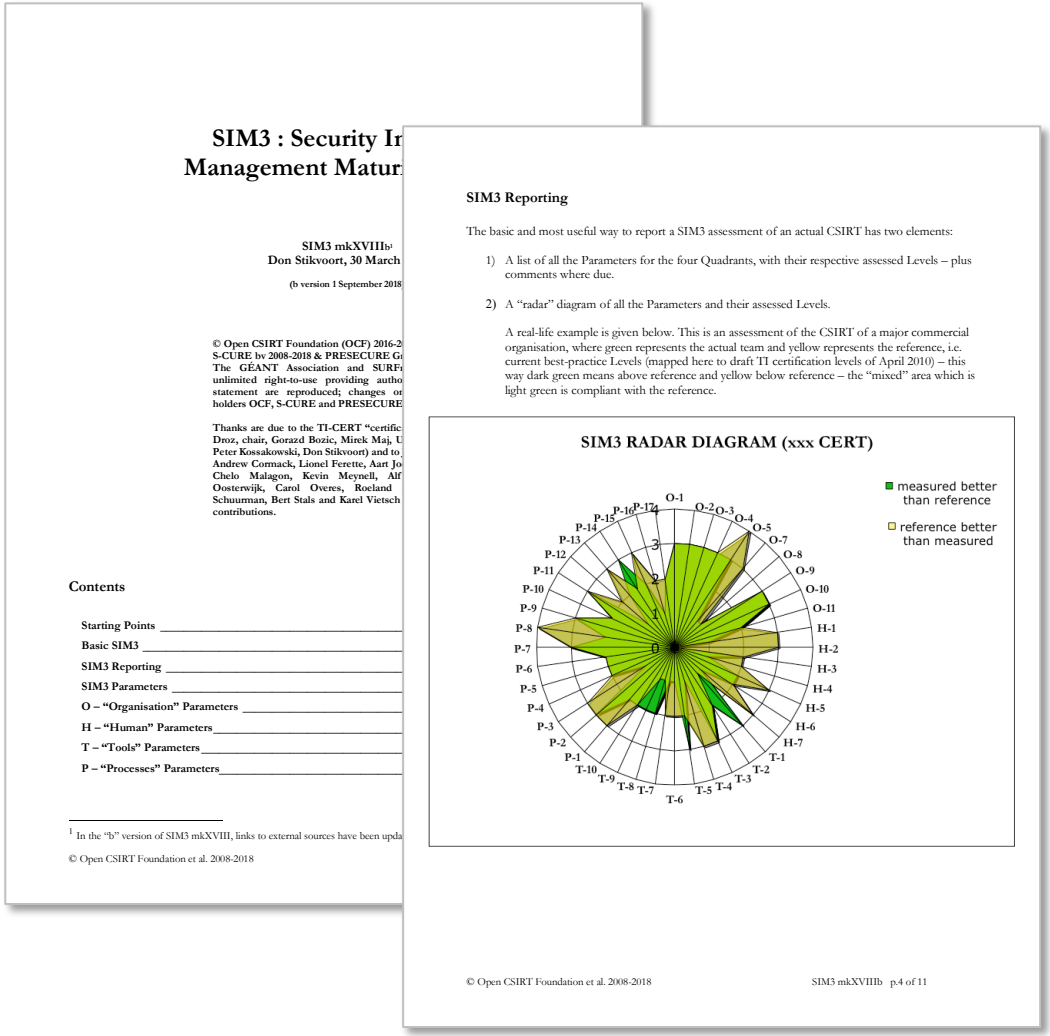
- Prevenção
- Detecção
- Resolução
- Controle de qualidade e *feedback*

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



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

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:
Online Tool

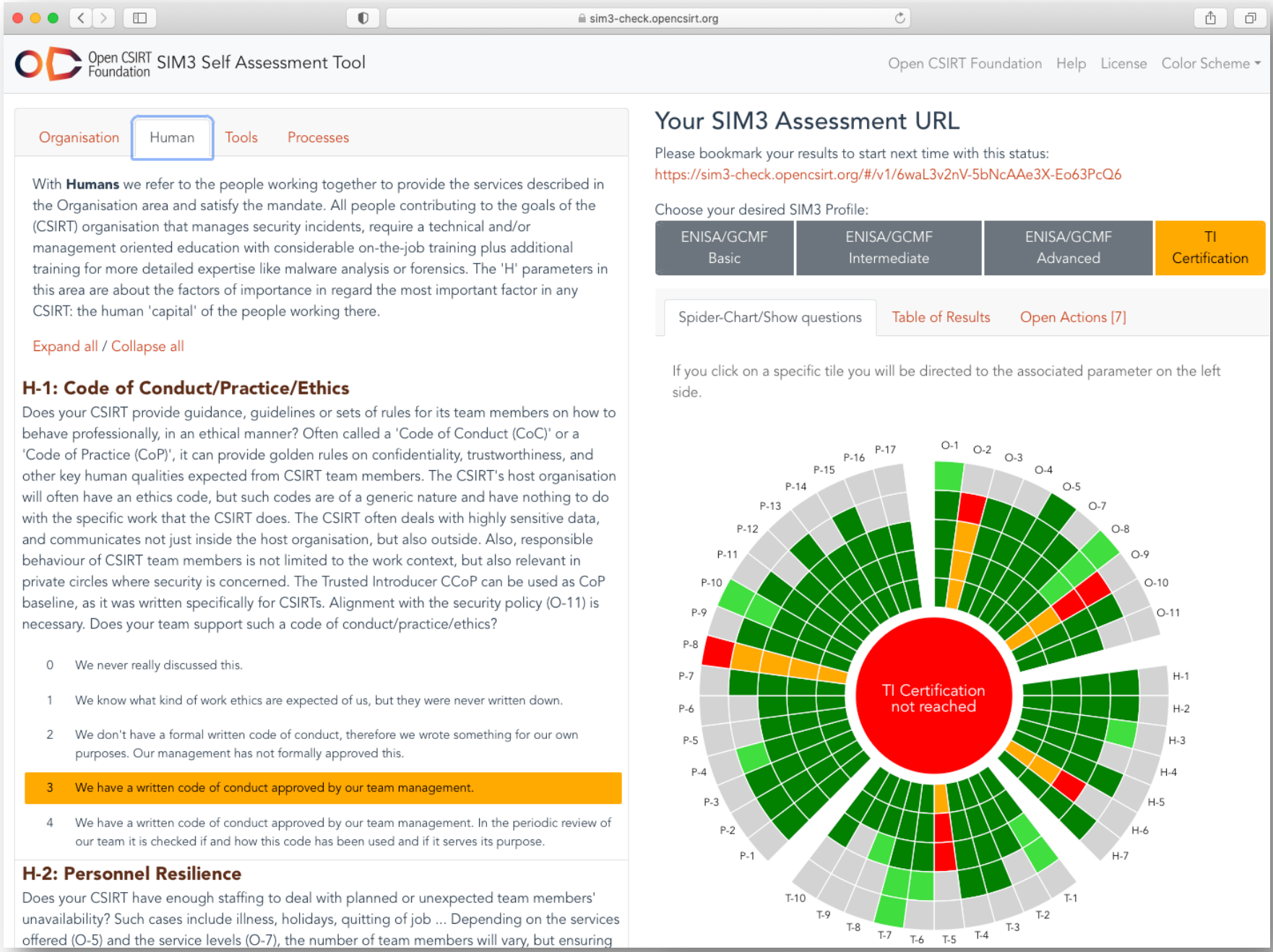
Auto avaliação em forma de perguntas

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/



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

Cooperação Internacional: **Construção de Confiança**

FIRST

Fórum existe desde 1992

- membro desde 2002

É uma Rede Global de CSIRTs

- fomenta a cooperação
- acesso a times e especialistas do mundo todo

Destaques da Participação do CERT.br:

- *Co-chair* do *Membership Committee* e do *Security Lounge SIG*
- *Chair* da Conferência 2020
- Coordenação de conteúdo do padrão *FIRST CSIRT Services Framework*
- Viabilização da parceria entre o FIRST e o LACNIC
  - CERT.br é *co-host* dos TCs e Simpósios na região

Rede de CSIRTs Nacionais

Existe desde 2006

Fórum para discussão de assuntos específicos para grupos de responsabilidade nacional

- CERT.br e CTIR Gov são membros

Maiores parceiros do CERT.br:

CERT/CC	US-CERT	CERT.at
NCSC-NL	NCSC-FI	CERT.LV
JPCERT/CC	NISC JP	HKCERT
TWCERT/CC		

LAC-CSIRTs

Reunião de Grupos de Resposta a Incidentes de Segurança (CSIRTs) da região da América Latina e o Caribe – ocorre durante o LACNIC

Cooperação Nacional:
Capacitação e Criação de Uma Comunidade Atuante

Objetivo

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

Cursos de Gestão de Incidentes

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

- https://cert.br/cursos/
  - *Overview of Creating and Managing CSIRTs*
  - *Fundamentals of Incident Handling*
  - *Advanced Topics in Incident Handling*

SEI Partner Network

Obrigada

cristine@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br