nic.br cgi.br | cert.br

Mesa Redonda: Quanto Valem Seus Dados?
TCU + Seguro

06 de agosto de 2021 | Evento *Online*

Incidentes de Segurança no Contexto da Proteção de Dados

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

cert.br nic.br cgi.br

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 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, coordenada pelo MCTI
- 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/

Cenário Atual

Contextos Global e Nacional

cert.br nic.br cgi.br

You weren't hacked because you lacked space-age network defenses. Nor because cyber-gurus picked on you. It's far simpler than that

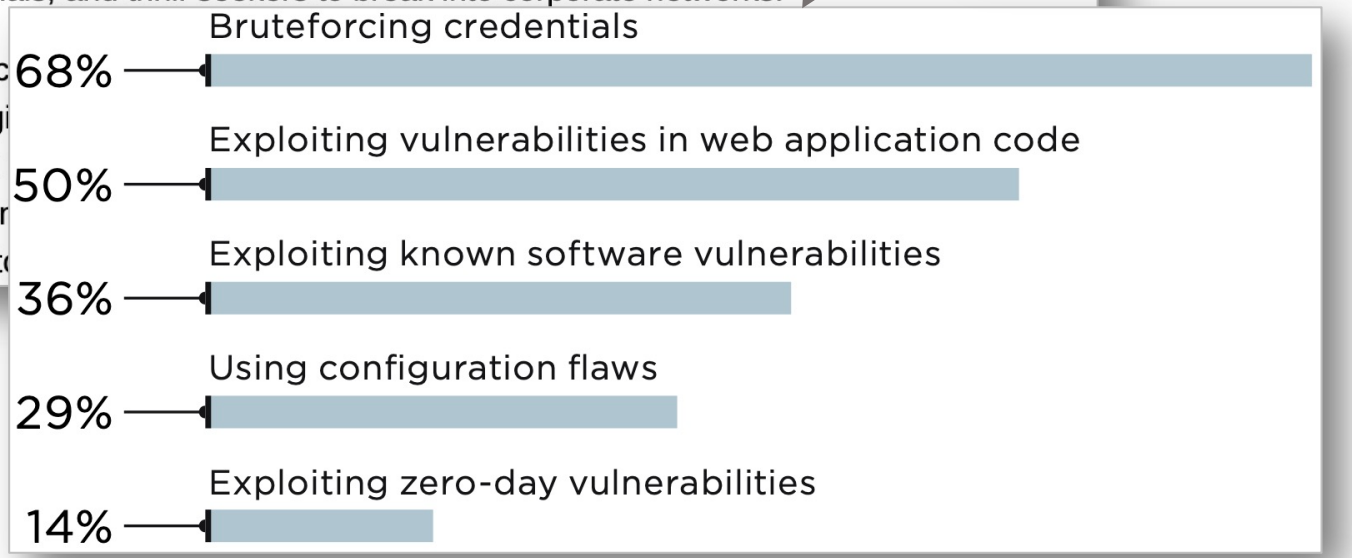
Three little words: Patches, passwords, policies

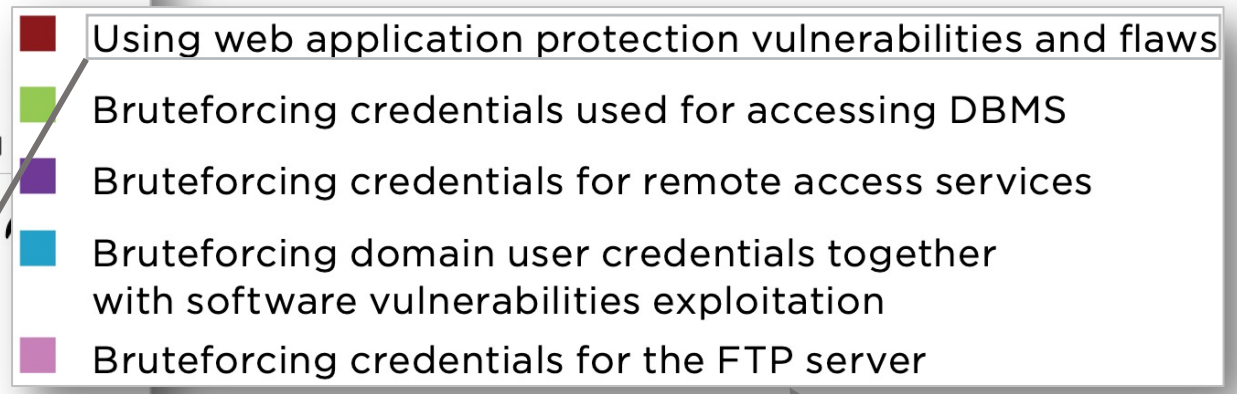
Thu 13 Aug 2020 // 07:06 UTC 31

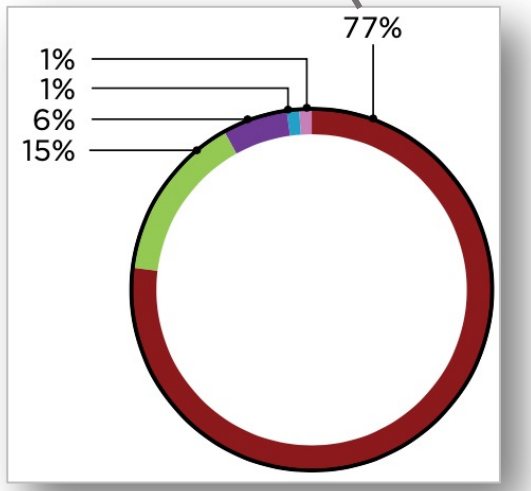
Shaun Nichols in San Francisco BIO EMAIL TWITTER

The continued inability of organizations to patch security vulnerabilities in a timely manner, combined with guessable passwords and the spread of automated hacking tools, is making it pretty easy for miscreants, professionals, and thrill-seekers to break into corporate networks.

This is acc
Technologi
and found
its red tear
available t







https://www.theregister.com/2020/08/13/pentest_networks_fail/
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/external-pentests-2020-eng.pdf

Cybersecurity
INSIDERS

Insider Threat Awareness Month Reminds Us That the Biggest Threats Can Arise from Within

Posted By **cyberinsiders**

Insider Threat Awareness Month offers a great opportunity to make organizations realize that today's modern cyberattack is no longer carried out by a dark cyber-assassin with sophisticated hacking techniques. The reality is that they no longer hack in at all, they log in using weak, stolen, or otherwise compromised passwords. And a shocking amount of the time, it is actually an insider doing the "hacking."

https://www.cybersecurity-insiders.com/insider-threat-awareness-month-reminds-us-that-the-biggest-threats-can-arise-from-within/

Top 10 Most Exploited Vulnerabilities 2016–2019

U.S. Government reporting has identified the top 10 most exploited vulnerabilities by state, nonstate, and unattributed cyber actors from 2016 to 2019 as follows: CVE-2017-11882, CVE-2017-0199, CVE-2017-5638, CVE-2012-0158, CVE-2019-0604, CVE-2017-0143, CVE-2018-4878, CVE-2017-8759, CVE-2015-1641, and CVE-2018-7600.

Alert (AA20-133A)

Top 10 Routinely Exploited Vulnerabilities

Original release date: May 12, 2020

Print Tweet Send Share

Summary

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the broader U.S. Government are providing this technical guidance to advise IT security professionals at public and private sector organizations to place an increased priority on patching the most commonly known vulnerabilities exploited by sophisticated foreign cyber actors.

s Exploited in 2020

10 vulnerabilities from 2016 to 2019 listed above, the U.S. orted that the following vulnerabilities are being routinely cated foreign cyber actors in 2020:

- Malicious cyber actors are increasingly targeting unpatched Virtual Private Network vulnerabilities.
  - An arbitrary code execution vulnerability in Citrix VPN appliances, known as CVE-2019-19781, has been detected in exploits in the wild.
  - An arbitrary file reading vulnerability in Pulse Secure VPN servers, known as CVE-2019-11510, continues to be an attractive target for malicious actors.
- March 2020 brought an abrupt shift to work-from-home that necessitated, for many organizations, rapid deployment of cloud collaboration services, such as Microsoft Office 365 (O365). Malicious cyber actors are targeting

https://us-cert.cisa.gov/ncas/alerts/aa20-133a

Alert (AA21-209A)

More Alerts

Top Routinely Exploited Vulnerabilities

Original release date: July 28, 2021 | Last revised: August 04, 2021

Print Tweet Send Share

Summary

This Joint Cybersecurity
(CISA), the Australian Cy
(NCSC), and the U.S. Fec

This advisory provides c
(CVEs)—routinely exploi

Table 1:Top Routinely Exploited CVEs in 2020

Vendor	CVE	Type
Citrix	CVE-2019-19781	arbitrary code execution
Pulse	CVE 2019-11510	arbitrary file reading
Fortinet	CVE 2018-13379	path traversal
F5- Big IP	CVE 2020-5902	remote code execution (RCE)
MobileIron	CVE 2020-15505	RCE
Microsoft	CVE-2017-11882	RCE
Atlassian	CVE-2019-11580	RCE
Drupal	CVE-2018-7600	RCE
Telerik	CVE 2019-18935	RCE
Microsoft	CVE-2019-0604	RCE
Microsoft	CVE-2020-0787	elevation of privilege
Netlogon	CVE-2020-1472	elevation of privilege

https://us-cert.cisa.gov/ncas/alerts/aa21-209a

bloomberg.com

Menu Search **Bloomberg** Sign In **Subscribe**

Bloomberg Cybersecurity

Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra
June 4, 2021, 4:58 PM GMT-3

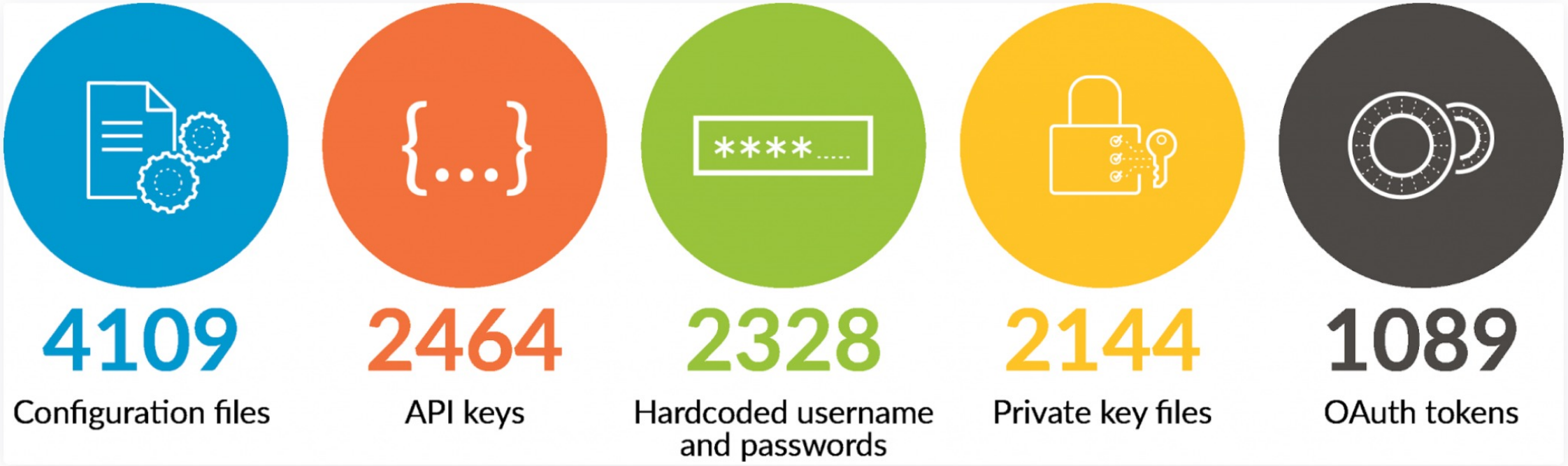
- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Não são só usuários que comprometem senhas:
Desenvolvedores expõe senhas e chaves no GitHub

Key Findings

Unit 42 researchers analyzed more than 24,000 public GitHub data uploads via the GitHubs Event API and found thousands of files containing potentially sensitive information, which included:



https://unit42.paloaltonetworks.com/github-data-exposed/

SolarWinds – Ataque atribuído à Russia pelos EUA
Possível vetor do comprometimento: senha no GitHub

SolarWinds FTP credentials were leaking on GitHub in November 2019 Featured

3 Shares | Share | Tweet 3

By Sam Varghese

More details are emerging about poor security at SolarWinds, following the compromise of its Orion network management software that was then used to effect attacks on many companies in a number of regions around the globe.

A researcher from India had advised SolarWinds in November 2019 that he had found a public GitHub repository which was leaking the company's FTP credentials.

bounty hunter, said in a tweet: "Was
raging SolarWinds. Hmmm, how that
d was *****123 Rolling on the floor

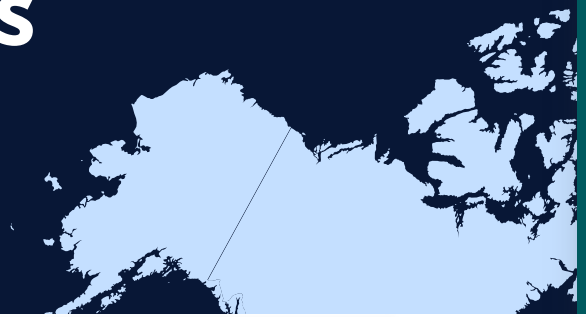
Downloads Url: http://downloads.solarwinds.com
FTP Url: ftp://solarwinds.upload.akamai.com
Username:
Password:
POC: http://downloads.solarwinds.com/test.txt

I was able to upload a test POC.
Via this any hacker could upload malicious exe and update it with release SolarWinds product.

https://www.itwire.com/security/solarwinds-ftp-credentials-were-leaking-on-github-in-november-2019.html
https://threatpost.com/solarwinds-default-password-access-sales/162327/

TOP 10

Where leaks come from



01	India
02	Brazil
03	United States
04	Nigeria
05	France
06	Russia
07	UK
08	Canada
09	Bangladesh
10	Indonesia

Uber Data Breach*

May 2014

Hackers discovered credentials in a personal public repository on GitHub that granted access to a database containing private information of thousands of Uber drivers.

*Read the article

Starbucks Data Breach*

January 2020

JumpCloud API key found in GitHub repository.

*Read the article

Equifax Data Breach*

April 2020

Leaked secrets in personal GitHub account granted access to sensitive data for Equifax customers.

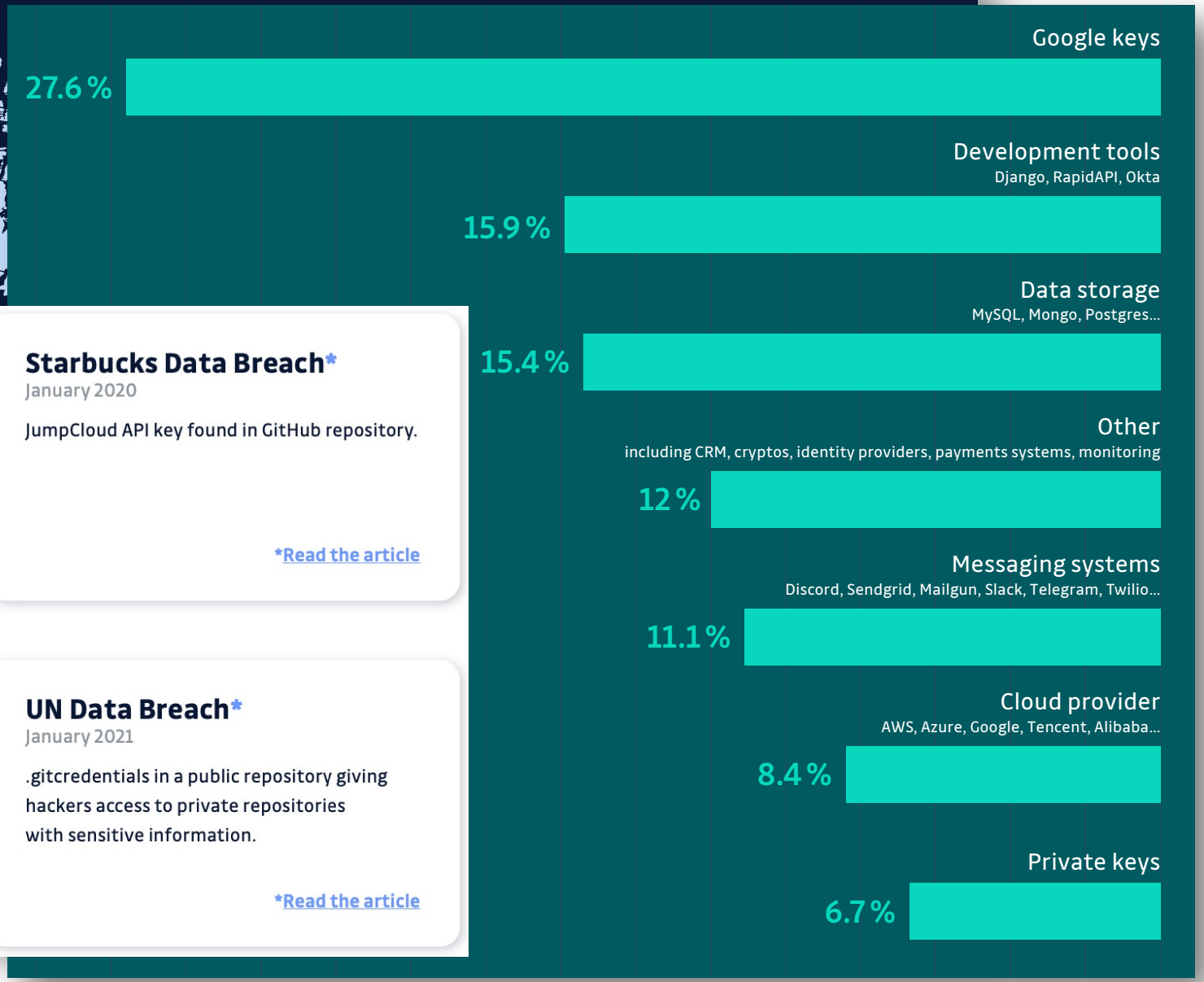
*Read the article

UN Data Breach*

January 2021

.gitcredentials in a public repository giving hackers access to private repositories with sensitive information.

*Read the article



State of Secrets Sprawl on GitHub - 2021: https://blog.gitguardian.com/state-of-secrets-sprawl-2021/

Resumo sobre os Incidentes Observados pelo CERT.br: **Causas Mais Comuns de Invasões e Vazamentos de Dados**

Ataques mais reportados e mais observados em sensores:

- Força bruta de senhas / senhas vazadas

  Bastante frequente em redes .gov.br:

  - contas de *e-mails* comprometidas enviando *spam* e *phishing*

    (via força bruta no *webmail* / Zimbra)
  - senhas *hardcoded* em códigos fonte expostos no GitHub e Pastebin

- Comprometimento via exploração de vulnerabilidades conhecidas
  - falta de aplicação de correções
  - erros de configuração
  - falta/falha de processos

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

Mais de 80% dos incidentes seriam evitados se

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

Estudo Setorial
Segurança digital: uma análise de gestão de risco em empresas brasileiras
https://cetic.br/pt/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

Você teria um conselho para as empresas para reduzir o número de incidentes?

"*Multifactor Everything*"

-- Katie Moussouris (Luta Security, US)
https://youtu.be/4tuC32PlyJk

O que Priorizar

Manter Sistemas Atualizados

- Acompanhe alertas de todos os fabricantes do seu parque
- Atualize **TODOS** os sistemas e aplicações
  - mesmo que sejam “só internos”
  - movimentação lateral na rede interna é regra em todos os ataques
- Defina regras para priorizar a aplicação de correções de segurança

  https://www.first.org/cvss/

Adotar Múltiplos Fatores de Autenticação

- Impede sucesso de força bruta de senhas
- Reduz impacto do comprometimento de credenciais

Tecnologias:

- Chaves criptográficas / certificados
- *Tokens*
  - em *hardware* (FIDO2/U2F)
  - em *software* (HOTP/TOTP)

O mais importante:

- **Não usar somente senhas**

Identificar e Tratar Incidentes de Segurança

Não depende somente de ferramentas

Acompanhe todas as notificações enviadas para

- *e-mail* de abuse
- contato de whois do domínio
- *e-mail* da ETIR
  - Divulgue amplamente o contato para notificações

Para órgãos da APF

- normas do GSI
- CTIR Gov
  - Rede Federal de Gestão de Incidentes Cibernéticos

Mesmo Assim Incidentes Ocorrerão

cert.br nic.br cgi.br

Gestão de Incidentes: **Definições Técnicas**

Incidente de Segurança – cada organização precisa definir o que é um incidente para ela, em geral com base na missão, serviços e recursos disponíveis.

Notificação de Incidente – ato informal de reportar a uma rede/empresa a ocorrência de um potencial incidente, normalmente um *e-mail* ou formulário *online*

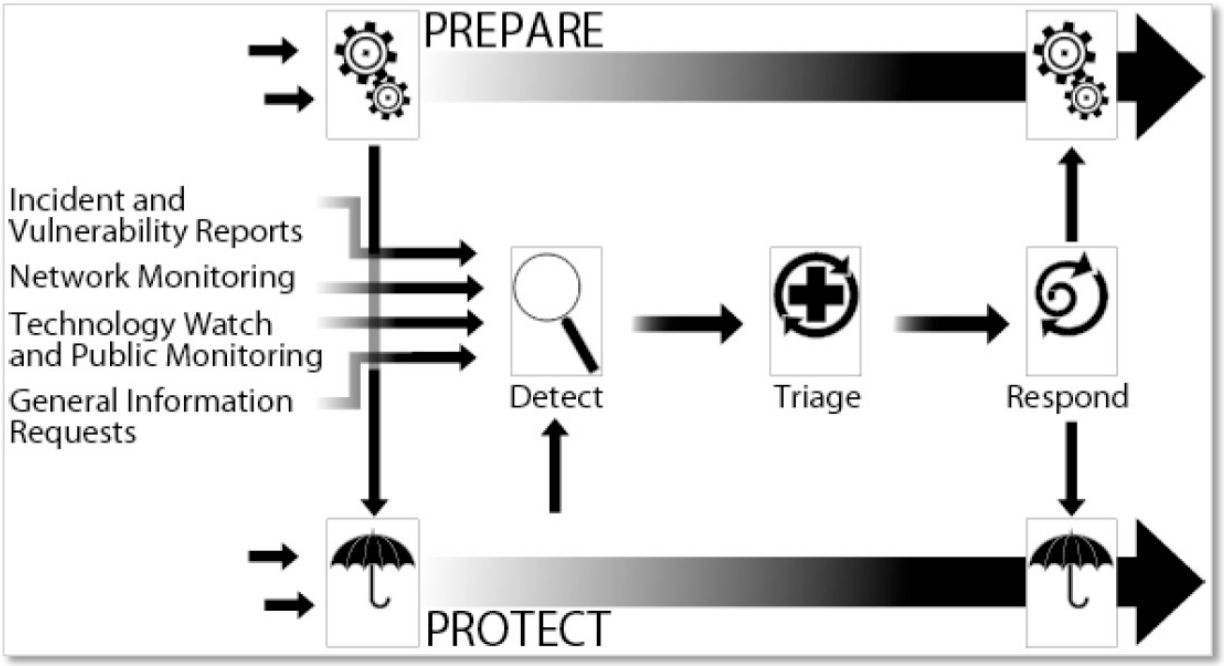
- Foco é pedir/oferecer ajuda
- Requer análise técnica para verificar
  - se é mesmo incidente
  - qual a natureza, escopo e impacto do incidente

Gestão de Incidentes – políticas e estratégias

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

Tratamento de Incidentes – processos

- prevenir, identificar, mitigar e responder



Resposta a Incidentes – ações

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

CSIRT – acrônimo conhecido globalmente para Equipe de Tratamento de Incidentes de Segurança

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

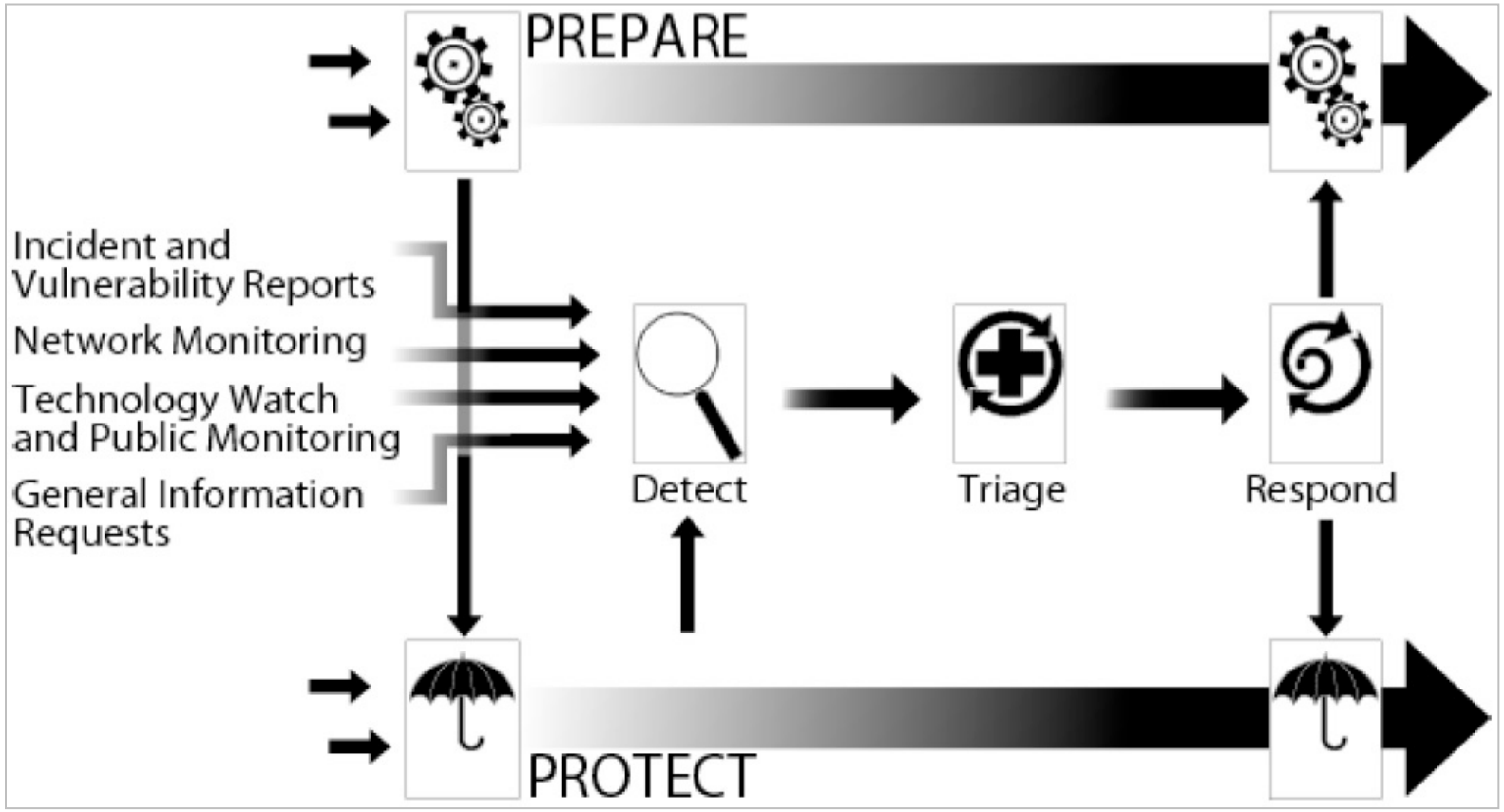
- reconhecer a importância do adequado tratamento de incidentes
- estabelecer políticas para notificação
- planejar e implantar um CSIRT (ETIR)

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

Incidente vs. Vazamento de Dados

Incidente de Segurança – cada organização precisa definir o que é um incidente para ela, em geral com base na missão, serviços e recursos disponíveis.

Dois **possíveis exemplos** de definições são:

> Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

-ou-

> O ato de violar uma política de segurança, explícita ou implícita.

Exemplos de incidentes incluem atividades como:

- tentativas (com ou sem sucesso) de ganhar acesso não autorizado a sistemas ou a seus dados;
- interrupção indesejada ou negação de serviço;
- uso não autorizado de um sistema para processamento ou armazenamento de dados;
- modificações nas características de *hardware*, *firmware* ou *software* de um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema.

Fonte:
https://cert.br/certcc/csirts/csirt_faq-br.html

Violação ou Vazamento de Dados (*Data Breach* ou *Data Leak*)

> "Divulgação não autorizada de informações sensíveis para um terceiro, normalmente fora da organização, que não está autorizado a ter ou ver a informação."

> "Vazamentos de dados (*data leak*) ocorrem quando dados são indevidamente acessados, coletados e divulgados na Internet, ou repassados a terceiros."

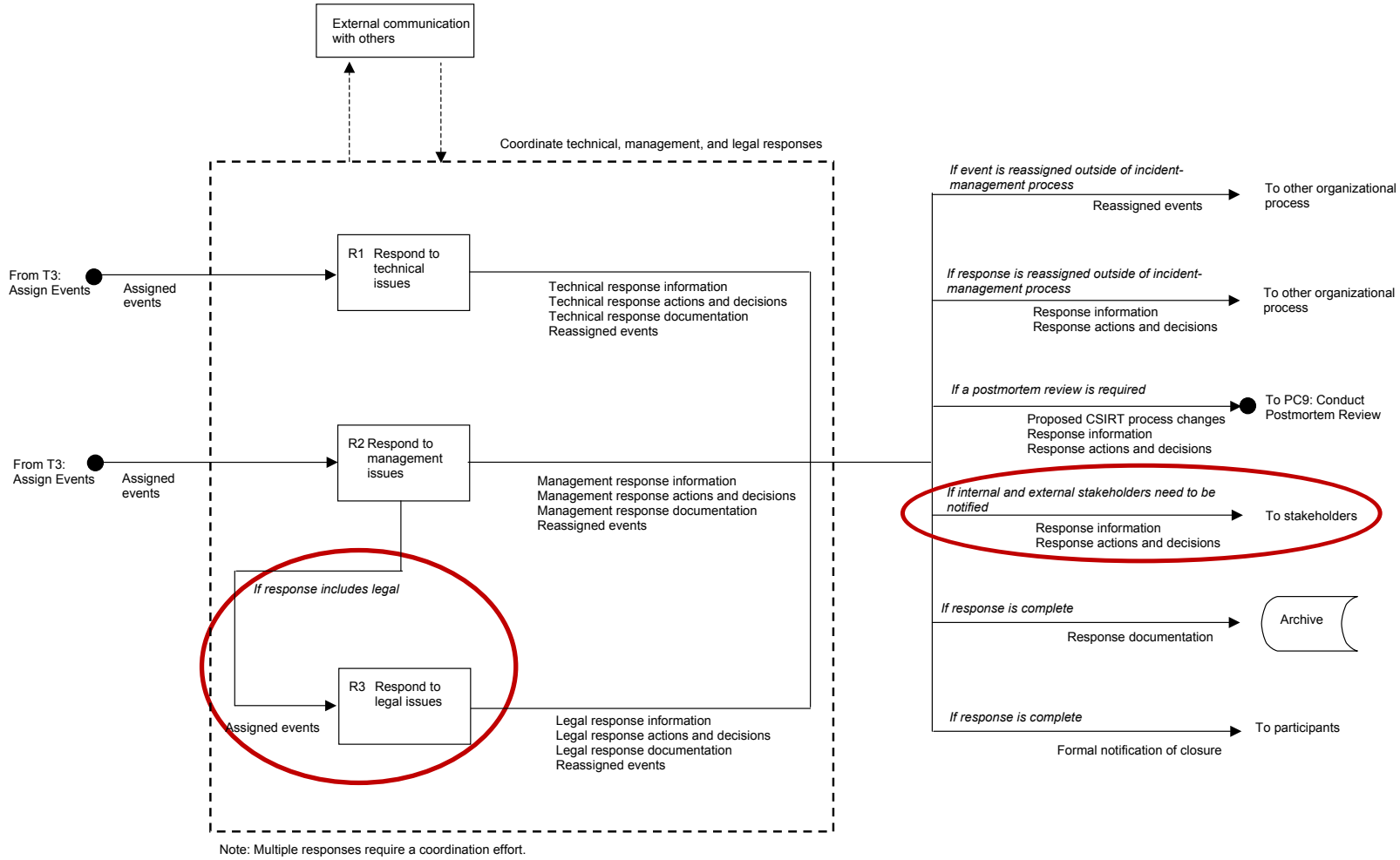
> "Perda de Dados: a exposição de informações proprietárias, sensíveis ou classificadas via furto ou vazamento de dados."

Fontes:
https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#D
https://cartilha.cert.br/fasciculos/#vazamento-de-dados
https://csrc.nist.gov/glossary/term/data_loss

Incidentes Envolvendo Dados Pessoais ou Crimes: **Tipos de Resposta no Fluxo de Tratamento de Incidentes**

Existe mais de um tipo de resposta que pode ser dada a um incidente de segurança

- a **resposta legal** é uma decisão de cunho **gerencial**
  - uma equipe técnica não pode, por via de regra, decidir sozinha se é necessária uma resposta legal
  - os Operadores da Justiça e a ANPD são *stakeholders* externos a serem envolvidos em alguns casos
  - importante definir claramente em políticas o que fazer
- a **resposta técnica** ao incidente ocorre em paralelo à resposta gerencial e segue tempos diferentes



Fonte: *Defining Incident Management Processes for CSIRTs: A Work in Progress,* **páginas 152 e 221.**
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153

Nem todo incidente é crime ou envolve dados pessoais

Dia-a-dia da Equipe de Tratamento:

- identifica e trata vários incidentes, seguindo o processo mostrado anteriormente
- o processo inclui a análise do incidente e a identificação de
  - escopo e natureza
  - se há necessidade de resposta gerencial
    - esta identifica se é necessária resposta legal
    - a resposta legal é requerida, por exemplo
      - se for identificado crime,
      - quebra de contrato
      - incidente que envolva dados pessoais e que possa acarretar risco ou dano relevante aos titulares
    - em todos estes casos é necessário seguir normas e legislação pertinentes a cada setor/órgão

Em outras palavras:

Do ponto de vista de uma empresa/instituição, o fluxo de de tratamento de incidentes envolvendo dados pessoais ou possíveis crimes se diferencia apenas na fase final.

Por exemplo:

1. Incidente é detectado
2. Análise mostra que quebrou um contrato?
   - se sim, aciona jurídico para providências
3. Análise mostra que é crime?
   - se sim, aciona jurídico para avaliar se necessita notícia aos operadores da justiça
4. Análise mostra que afetou dados pessoais?
   - se sim, aciona jurídico para avaliar se necessita envio de relatório para a ANPD

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."*

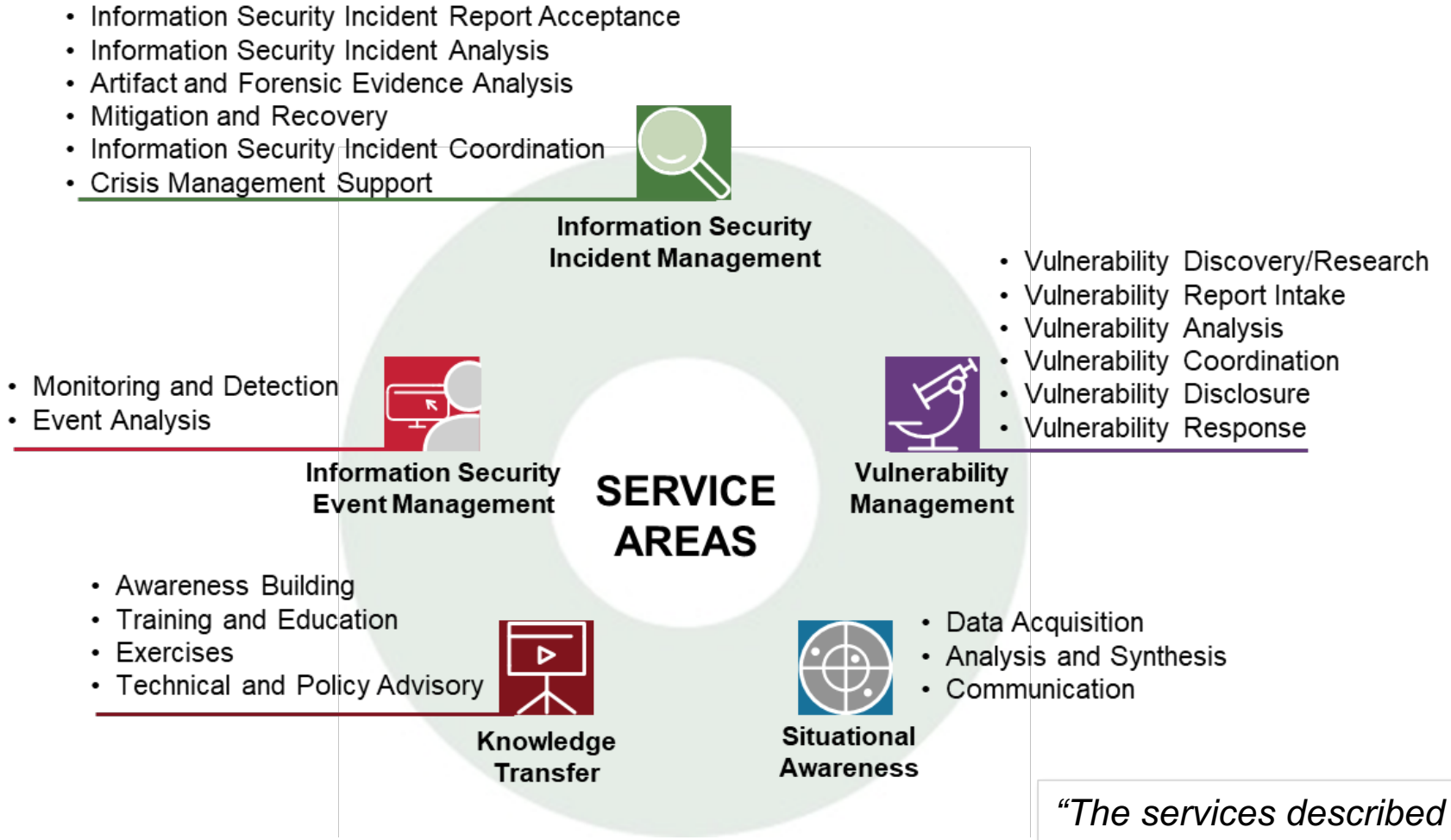
NIST Cyber Security Framework

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

FIRST CSIRT Services Framework:
CSIRTs Atuam Além da Gestão de Incidentes



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

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

Todos Tem um Papel na Segurança e Proteção de Dados: **Ecossistema é Complexo e Interdependente**

Quase tudo é *software* e está conectado à Internet

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

Por um Ecossistema mais Saudável:
Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

https://bcp.nic.br/i+seg

Conscientização de Todos é Essencial:
Portal InternetSegura.br – materiais gratuitos

Cartilha de Segurança para Internet:
Fascículos e Slides para Palestras e Treinamento

Conteúdo disponível *online* gratuitamente sob Licença *Creative Commons*

- **Fascículos** que cobrem assuntos específicos relacionados com segurança na Internet
- ***Slides*** sobre cada um dos temas, que podem ser utilizados, por exemplo, para dar aulas ou palestras de conscientização
  - Dica do dia no *site*, via *Twitter* e RSS
  - Impressões em pequena escala enviadas a escolas e centros de inclusão digital
  - Possível gerar versões personalizadas com logo da instituição

    Exemplos de parceiros de impressão e distribuição:

    Itaipu, Eletronuclear, ELO, Microsoft, Procergs e Metrô SP

https://cartilha.cert.br/

Obrigada

cristine@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br

Referências Adicionais sobre a Dinâmica de Trabalho e Maturidade dos CSIRTs

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

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: **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

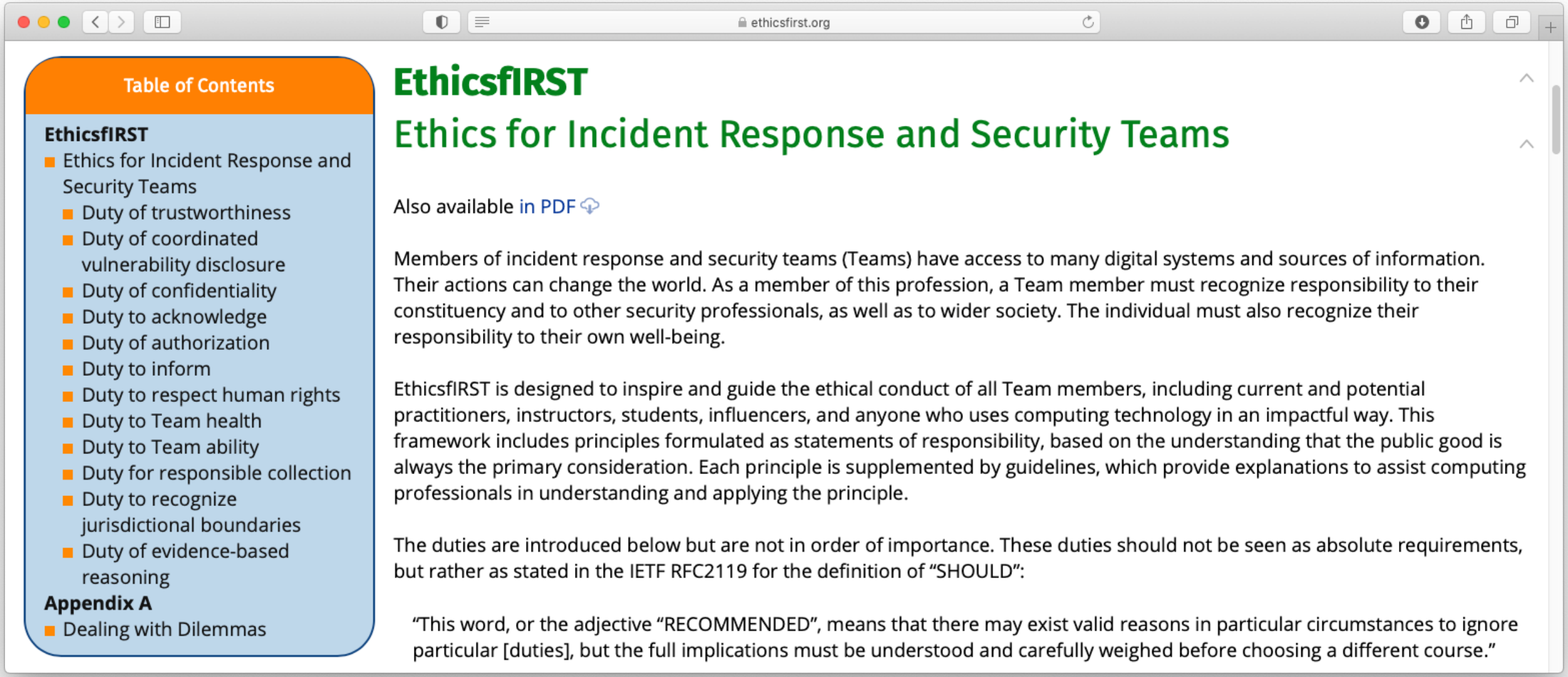
Awareness Building
- Research and Information Aggregation
- Report and Awareness Materials Development
- Information Dissemination
- Outreach

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

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



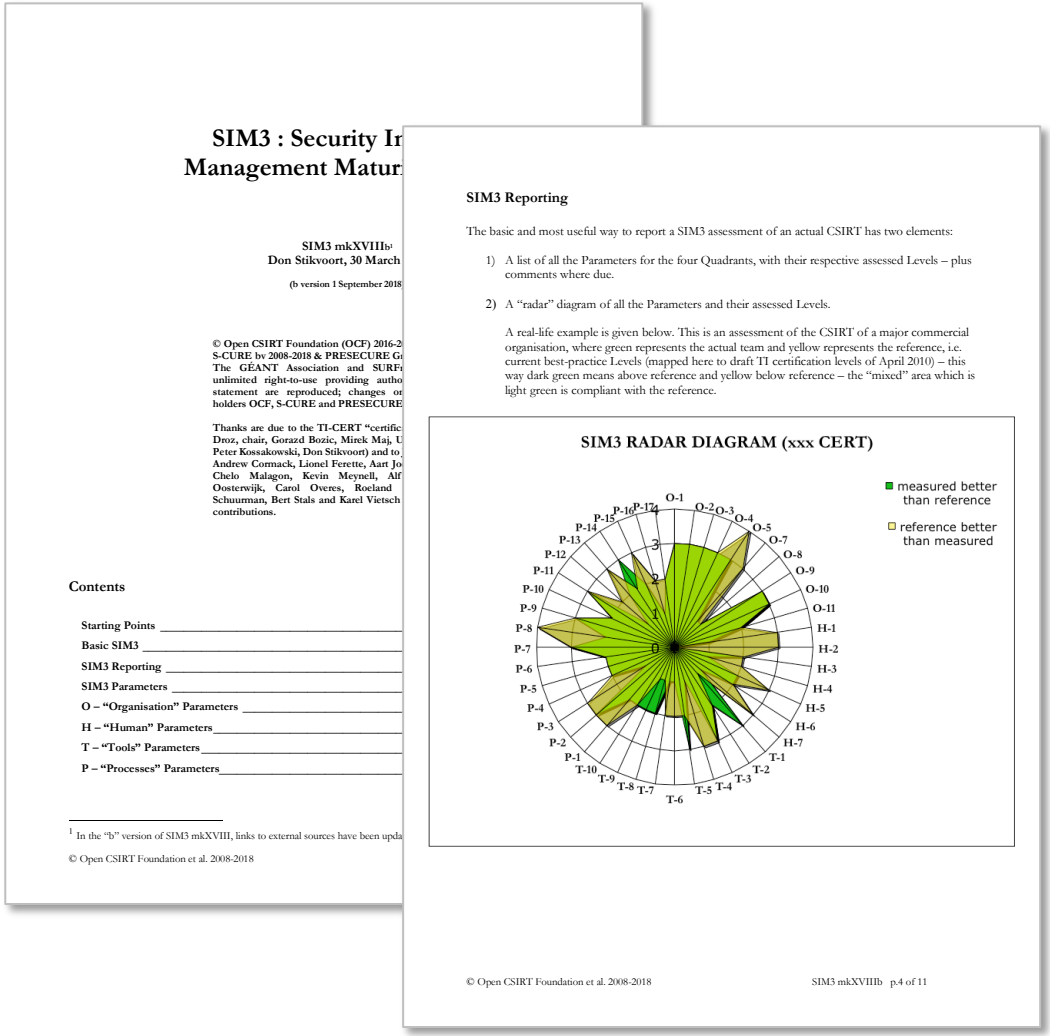
Avaliação de Maturidade:
SIM3 – *Security Incident Management Maturity Model*

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)

measured better than reference
reference better than measured

© 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/