

FCT

Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

FCCN

Computação
Científica Nacional

Pacote CSIRT-In-A-Box

Carlos Friaças



Agenda

- Introdução
- Documentação
- Ferramentas
- Formação



INTRODUÇÃO

Porquê o CSIRT-In-A-Box?

- **Motivações**
 - Capacitar as instituições de um conjunto mínimo de recursos de resposta a incidentes
 - Facilitar a coordenação das instituições com o RCTS CERT
 - Dar a conhecer os serviços do RCTS CERT em maior detalhe

Expectativas

- Da NOSSA parte:
 - Não se pretende que no imediato todas as instituições formem uma equipa dedicada
 - Começar “pequeno” e, se necessário, ir crescendo
 - Falarmos a mesma “linguagem”
 - Maior interoperabilidade
 - Melhorar a comunicação

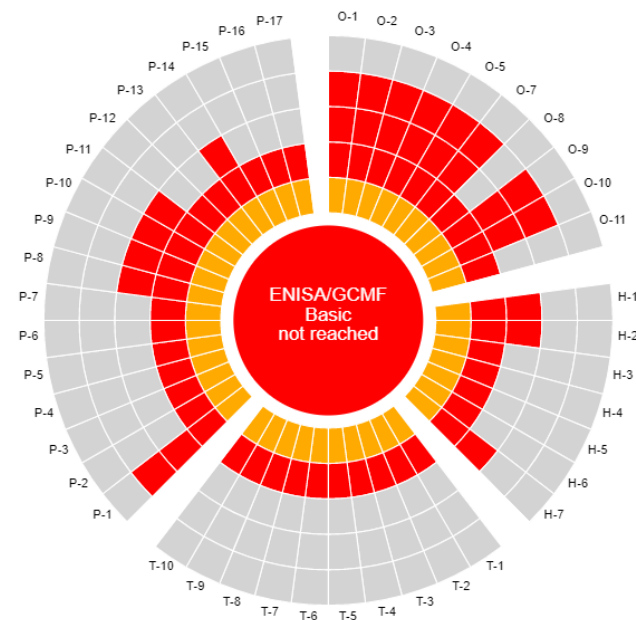


DOCUMENTAÇÃO



Documentação

- Templates:
 - RFC2350 (nível mínimo)
 - Charter (nível avançado)
- Políticas e Procedimentos RCTS CERT
- Manuais e Documentos de Boas Práticas
- O modelo SIM3



SIM3 (1/2)

Security Incident **M**anagement **M**aturity **M**odel

SIM3 mkXVII, Don Stikvoort, 11 November 2012

- 3 elementos básicos:
 - Parâmetros (mais de 40)
 - Quadrantes
 - Organização
 - Humano
 - Ferramentas
 - Processos



SIM₃ (2/2)

– Níveis

- 0 – indisponível / indefinido / desconhecido
- 1 – implícito (conhecido, mas não escrito) (“estamos cientes”)
- 2 – explícito interno (escrito, mas não formalizado) (“leiam, é isto que fazemos”)
- 3 – explícito formalizado (aprovado ou publicado) (“é a isto que nos comprometemos”)
- 4 – sujeito a processo de controlo / auditado / fiscalizado (“é assim que garantimos”)

SIM₃ - Organização



0-1 : MANDATE

Description: The CERT's assignment as derived from upper management.

0-2 : CONSTITUENCY

Description: Who the CERT functions are aimed at – the “clients” of the CERT.

0-3 : AUTHORITY

Description: What the CERT is allowed to do towards their constituency in order to accomplish their role.

0-4 : RESPONSIBILITY

Description: What the CERT is expected to do towards their constituency in order to accomplish their role.

0-5 : SERVICE DESCRIPTION

Description: Describes what the CERT service is and how to reach it.

Minimum requirement: Contains the CERT contact information, service windows, concise description of the CERT services offered and the CERT's policy on information handling and disclosure.

APENAS PARA REFERÊNCIA

SIM₃ – Organização (cont.)

0-7 : SERVICE LEVEL DESCRIPTION

Description: Describes the level of service to be expected from the CERT.

Minimum requirement: Specifies the speed of reaction to incoming incident reports and reports from constituents and from peer CERTs. For the latter a human reaction within two working days is the minimum expected.

0-8 : INCIDENT CLASSIFICATION

Description: The availability and application of an incident classification scheme to recorded incidents.

Incident classifications usually contain at least “types” of incidents or incident categories. However they may also include “severity” of incident.

0-9 : INTEGRATION IN EXISTING CERT SYSTEMS

Description: Describes the CERT's level of membership of a well established CERT co-operation, either directly or through an "upstream" CERT of which it is a customer/client. This is necessary to participate and integrate in the regional/worldwide CERT system(s).

APENAS PARA REFERÊNCIA

SIM₃ – Organização (cont.)



0-10 : ORGANISATIONAL FRAMEWORK

Description: Fits 0-1 to 0-9 together in a coherent framework document serving as the controlling document for the CERT.

Minimum requirement: Describes the CERT's mission and parameters 0-1 to 0-9.

0-11 : SECURITY POLICY

Description: Describes the security framework within which the CERT operates. This can be part of a bigger framework, or the CERT can have their own security policy.

APENAS PARA REFERÊNCIA

SIM₃ - Humanos

H-1 : CODE OF CONDUCT/PRACTICE/ETHICS

Description: A set of rules or guidelines for the CERT members on how to behave professionally, potentially also outside work.

Clarification: E.g. the TI CCoP. Behaviour outside work is relevant, because it can be expected of CERT members that they behave responsibly in private as well where computers and security are concerned.

H-2 : PERSONAL RESILIENCE

Description: How CERT staffing is ensured during illness, holidays, people leaving, etc.

Minimum requirement: three (part-time) CERT members.

H-3 : SKILLSET DESCRIPTION

Description: Describes the skills needed on the CERT job(s).

APENAS PARA REFERÊNCIA

H-4 : INTERNAL TRAINING

Description: **Internal** training (of any kind) available to train new members and to improve the skills of existing ones.

SIM₃ – Humanos (cont.)

H-5 : EXTERNAL TECHNICAL TRAINING

Description: Program to allow staff to get job-technical training externally – like TRANSITS, ENISA CERT Exercises, or commercial training programs (CERT/CC, SANS, etc.)

H-6 : EXTERNAL COMMUNICATION TRAINING

Description: Program to allow staff to get communication training externally.

H-7 : EXTERNAL NETWORKING

Description: Going out and meeting other CERTs. Contributing to the CERT system when feasible.

APENAS PARA REFERÊNCIA

SIM₃ - Ferramentas

T-1 : IT RESOURCES LIST

Description: Describes the hardware, software, etc. commonly used in the constituency, so that the CERT can provide targeted advice.

T-2 : INFORMATION SOURCES LIST

Description: Where does the CERT get their vulnerability/trend/scanning information from.

T-3 : CONSOLIDATED E-MAIL SYSTEM

Description: When all CERT mail is (at least) kept in one repository open to all CERT members, we speak of a consolidated e-mail system.

T-4 : INCIDENT TRACKING SYSTEM

Description: A trouble ticket system or workflow software used by the CERT to register incidents and track their workflow.

Clarification: AIRT, RTIR, trouble ticket systems in general.

APENAS PARA REFERÊNCIA

SIM₃ – Ferramentas (cont.)

T-5 : RESILIENT PHONE

Description: The phone system available to the CERT is resilient when its uptime and time-to-fix service levels meet or exceed the CERTs service requirements.

Clarification: Mobile phones are the easiest fallback mechanism for when a team's landlines are out of order.

Minimum requirement: Fallback ability to phone out.

T-6 : RESILIENT E-MAIL

Description: The e-mail system available to the CERT is resilient when its uptime and time-to-fix service levels meet or exceed the CERTs service requirements.

T-7 : RESILIENT INTERNET ACCESS

Description: The Internet access available to the CERT is resilient when its uptime and time-to-fix service levels meet or exceed the CERTs service requirements.

APENAS PARA REFERÊNCIA

SIM₃ – Ferramentas (cont.)

T-8 : INCIDENT PREVENTION TOOLSET

Description: A collection of tools aimed at preventing incidents from happening in the constituency. The CERT operates or uses these tools or has access to the results generated by them.

Clarification: E.g. IPS, virusscanning, spamfilters, portscanning. If not applicable as for a purely coordinating CERT, choose -1 as Level and will be omitted from “scoring”.

T-9 : INCIDENT DETECTION TOOLSET

Description: A collection of tools aimed at detecting incidents when they happen or are near happening. The CERT operates or uses these tools or has access to the results generated by them.

Clarification: E.g. IDS, Quarantainenets, netflow analysis.

T-10 : INCIDENT RESOLUTION TOOLSET

Description: A collection of tools aimed at resolving incidents after they have happened. The CERT operates or uses these tools or has access to the results generated by them.

Clarification: E.g. basic CERT tools including whois, traceroute etc; forensic toolkits.

APENAS PARA REFERÊNCIA

SIM₃ - Processos

P-1 : ESCALATION TO GOVERNANCE LEVEL

Description: Process of escalation to upper management for CERTs who are a part of the same host organisation as their constituency. For external constituencies: escalation to governance levels of constituents.

P-2 : ESCALATION TO PRESS FUNCTION

Description: Process of escalation to the CERT's host organisation's press office.

P-3 : ESCALATION TO LEGAL FUNCTION

Description: Process of escalation to the CERT's host organisation's legal office.

P-4 : INCIDENT PREVENTION PROCESS

Description: Describes how the CERT prevents incidents, including the use of the related toolset. Also, this includes the adoption of pro-active services like the issuing of threat/vulnerability/patch advisories.

APENAS PARA REFERÊNCIA

P-5 : INCIDENT DETECTION PROCESS

Description: Describes how the CERT detects incidents, including the use of the related toolset.

SIM₃ – Processos (cont.)

P-6 : INCIDENT RESOLUTION PROCESS

Description: Describes how the CERT resolves incidents, including the use of the related toolset.

P-7 : SPECIFIC INCIDENT PROCESSES

Description: Describes how the CERT handles specific incident categories, like phishing or copyright issues.

Clarification: may be part of P-6.

P-8 : AUDIT/FEEDBACK PROCESS

Description: Describes how the CERT assesses their set-up and operations by self-assessment, external assessment and a subsequent feedback mechanism. Those elements considered not up-to-standard by the CERT and their management are considered for future improvement.

P-9 : EMERGENCY REACHABILITY PROCESS

Description: Describes how to reach the CERT in cases of emergency.

Clarification: Often only open to fellow teams.

APENAS PARA REFERÊNCIA

SIM₃ – Processos (cont.)

P-10 : BEST PRACTICE E-MAIL AND WEB PRESENCE

Description: Describes (1) the way in which generic, security related mailbox aliases @org.tld are handled by the CERT or by parties who know when what to report to the CERT – and (2) the web presence.

Minimum Requirement:

(1) The handling of the following mailbox aliases (from RFC-2142 and best practice) is secured in such a way that the handlers either are part of the CERT or know the CERT, what it is for, and how to reach it when needed:

- Security: security@ ; cert@ ; abuse@
- E-mail: postmaster@
- IP-numbers & domain names: hostmaster@
- WWW: webmaster@ ; www@

(2) Some form of web presence for the CERT, at least internally. That presence must at least explain what the CERT is for, who it is for, and how it can be reached and when. Additional recommendations are (a) to link rfc-2350 from that presence, and (b) to enable a slash-security page, that is a page like www.org.tld/security , which can serve a wider security purpose than just the CERT.

APENAS PARA REFERÊNCIA

SIM₃ – Processos (cont.)

P-11 : SECURE INFORMATION HANDLING PROCESS

Description: Describes how the CERT handles confidential incident reports and/or information. Also has bearing on local legal requirements.

P-12 : INFORMATION SOURCES PROCESS

Description: Describes how the CERT handles the various information sources available to the CERT (as defined in the related tool, if available – see T-2).

P-13 : OUTREACH PROCESS

Description: Describes how the CERT reaches out to their constituency not in regard incidents but in regard PR and awareness raising.

P-14 : REPORTING PROCESS

Description: Describes how the CERT reports to the management and/or the CISO of their host organisation, i.e. internally.

APENAS PARA REFERÊNCIA

SIM₃ – Processos (cont.)

P-15 : STATISTICS PROCESS

Description: Describes what incident statistics, based on their incident classification (see 0-8), the CERT discloses to their constituency and/or beyond.

Clarification: If not applicable as in case of an explicit choice only to report internally, choose -1 as Level and will be omitted from “scoring”.

P-16 : MEETING PROCESS

Description: Defines the internal meeting process of the CERT.

P-17 : PEER-TO-PEER PROCESS

Description: Describes how the CERT works together with peer CERTs and/or with their “upstream” CERT.

APENAS PARA REFERÊNCIA

FERRAMENTAS



Serviços RCTS CERT



- Processamento e disseminação de eventos
- Tratamento de Incidentes
- Auditorias de segurança
- Campanhas de Phishing
- DNS Firewall
- Gestão de Vulnerabilidades



Eventos

- NÃO constituem um incidente
- NÃO resultam de uma denúncia
- NÃO são confirmados por um humano
- São processados e distribuídos automaticamente
 - Semanalmente, pelo RCTS CERT

Tipos de Incidentes

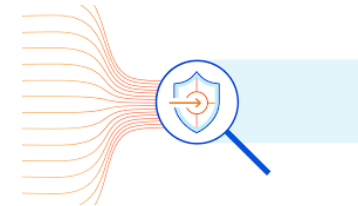
- **Abusive Content**
 - SPAM, Violações de Copyright, conteúdos ilegais, ...
- **Fraud**
 - Phishing (páginas)
- **Information Gathering**
 - Portscans, Network Scan, emails de phishing



Tipos de Incidentes

- **Intrusion Attempts**

- Brute-force SSH, Telnet



- **Malicious Code**

- Botnet activity (contacto com C&C), distribuição de malware

- **Vulnerable**

- Serviços vulneráveis (Open resolver, SNMP, NTP, SSL, ...)

Tratamento de Incidentes

- Resultam, quase sempre, de **denúncias**
- Têm tratamento humano
- Importante diferenciar
 - ATACANTE vs. VÍTIMA

Denúncia (exemplo)

Dear Network Manager :

This warning is from the <...>.

Our job is to protect <...>financial organizations from illegal intrusion attacks.

We have received a report of unauthorized access trial originating from your site as shown below.

Date/Time(GMT+9): 2015-10-26 18:22:44 ~ 2015-10-26 18:24:57

Source IP : x.x.12.1

Destination IP : x.x.8.48

Attack Type : 108-Bash_RCE_Vulnerability_CVE-2014-6271_01-140926

We are seriously considering notifying these illegal attempts to the related authorities of both your and our countries and requesting proper legal actions.

So, please take appropriate measures to identify and stop the attacker. And, please inform us of the results. (isac@)*

Thank you for your cooperation.

p.s. : If you are not the correct person to deal with this incident, please forward this to the proper person and inform us for future convenience.

Notificação (exemplo)



[RCTS-CERT #xxxxx] Intrusions - Exploiting known vulnerabilities - FCCN:UNIV-*

Caro(a) Senhor(a),

O RCTS CERT é um serviço de resposta a incidentes de segurança informática da FCT/FCCN para a Rede Ciência, Tecnologia e Sociedade (RCTS).

Agradecemos a sua compreensão e cooperação, e solicitamos que nas comunicações subsequentes mantenha o IDENTIFICADOR [RCTS CERT #ID] presente no assunto desta mensagem. Identificamos um sistema informático da sua responsabilidade envolvido em incidente de segurança classificado como:

Classe de Incidente: Tentativa de Intrusão

Tipo de Incidente: Exploração de Vulnerabilidades

IP(s):

x.x.12.1

Date/Time: 14/04/15 13:46 GMT

Vimos por este meio solicitar a seguinte tomada de ação:

- a) Verificação dos dados apresentados;*
- b) Interrupção da atividade identificada garantindo que o acesso é descontinuado;*
- c) Tomada de medidas que evitem possíveis reincidências;*
- d) Resposta a esta mensagem com indicação das ações tomadas.*

Vimos chamar a atenção para o constante nas Medidas de Controlo de Incidentes de Segurança Informática e na Carta ao Utilizador na RCTS, onde se refere, nomeadamente, que a FCT/FCCN se reserva o direito de penalizar as instituições incumpridoras das Regras constantes dessa mesma Carta, incluindo situações que configurem violação da lei.

Informação adicional: Website - <http://www.cert.rcts.pt>

*Disponíveis para quaisquer esclarecimentos adicionais,
Melhores cumprimentos,*

RCTS CERT - FCT/FCCN

Email: report@cert.rcts.pt

Telefone: +351 218440177

Fax: +351 218472167

Logs:

Date/Time(GMT+9): 2015-10-26 18:22:44 ~ 2015-10-26 18:24:57

Source IP : x.x.12.1

Destination IP : x.x.8.48

Attack Type : I08-Bash_RCE_Vulnerability_CVE-2014-6271_01-140926

FCT

Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

FCCN

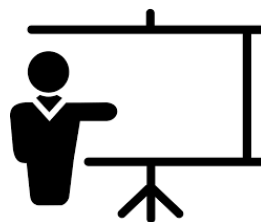
Computação
Científica Nacional

Workflow

- Denúncia (Report)
- Incidente (Incident)
- Investigação (Investigation)
- Fecho (Close)

FORMAÇÃO

(para equipas de resposta a incidentes)



TRANSITS-I & TRANSITS-II

https://www.geant.org/services/trust_identity_and_security/pages/transits_training.aspx



TRANSITS-I course fees are €1,100 for commercial companies, or €750 for non-commercial organisations. These fees include accommodation for three nights, two lunches, two evening meals, coffee breaks, and course materials.

TRANSITS-II course fees are €1,450 for commercial companies, or €1,100 for non-commercial organisations. These fees include three lunches, two evening meals, coffee breaks, and course materials. Please note - unlike TRANSITS-I courses - hotel accommodation is not included in the fee and students are expected to fund their own travel and accommodation. VAT is in addition to the above fees, if applicable in the host member state.

Outros



<https://www.eccouncil.org/>



<https://www.sans.org/>



<https://www.offensive-security.com/>

Em Resumo



SIM3 é um modelo de maturidade para CSIRTs



RFC2350 é a base da definição de uma equipa



Os incidentes são o centro da actividade de um CSIRT, mas os eventos são importantes



Obrigado