

SIM3 : Security Incident Management Maturity Model

SIM3 mkXV
Don Stikvoort, 1 September 2010

© S-CURE bv and PRESECURE GmbH 2008-2010 ;
TERENA and SURFnet bv have an unlimited right-to-use
providing author and copyright statement are reproduced;
changes only by copyright holders S-CURE and
PRESECURE.

Thanks are due to the TI-CERT “certification” WG (Serge
Droz, chair, Gorazd Bozic, Mirek Maj, Urpo Kaila, Klaus-
Peter Kossakowski, Don Stikvoort) and to Jimmy
Arvidsson, Andrew Cormack, Lionel Ferette, Aart Jochem,
Peter Jurg, Chelo Malagon, Kevin Meynell, Alf Moens,
André Oosterwijk, Carol Overes, Jacques Schuurman, Bert
Stals and Karel Vietsch for their valuable contributions.

Contents

Starting Points _____	2
Basic SIM3 _____	3
SIM3 Reporting _____	4
SIM3 Parameters _____	6
O – “Organisation” Parameters _____	7
H – “Human” Parameters _____	8
T – “Tools” Parameters _____	9
P – “Processes” Parameters _____	10

Starting Points

- The topic here is the Maturity of Security *Incident Management* (SIM) rather than just “CERT” which by virtue of the name is about “response” primarily. SIM has four major pillars, including prevention, detection and feedback alongside with resolution.
- The primary scope here is IT & information security incidents: incidents that are limited to computers, network appliances, networks and the information therein and conveyed thereon. One can however extend this scope, or narrow it down, often with no significant consequences for the model.
- For reasons of word economy, the term “CERT” is used here to describe any SIM capability to which SIM3 is applied, whether team, service or function. “ISIMC” – Information Security Incident Management Capability – is really a better word than “CERT” but the latter is widely known and therefore already rings all the right bells.
- The author promotes widespread use of this model. The copyright statement is intended to keep the model together, i.e. avoid various versions being used at the same time. Both maturity and certification gain in meaning when there is an agreed on starting point. This can be further taken up by the Trusted Introducer, the IETF and FIRST – in co-operation.

Basic SIM3

The maturity model is built on three basic elements:

- 1) Maturity Parameters
- 2) Maturity Quadrants
- 3) Maturity Levels

The Parameters are the quantities that are measured in regard maturity – some forty exist and they are detailed below. Each Parameter belongs to one of four Quadrants - the Quadrants are therefore the main four categories of Parameters:

- O - Organisation
- H - Human
- T - Tools
- P - Processes

These four Quadrants have been chosen in such a way that the parameters in there are as mutually independent as possible.

What we really measure are the Levels for each Parameter. A desirable simplicity of the SIM3 has been reached by specifying a unique set of Levels, valid for all of the Parameters in all of the Quadrants:

- 0 = not available / undefined / unaware
- 1 = implicit (known/considered but not written down, “between the ears”)
- 2 = explicit internal (written down but not formalised in any way)
- 3 = explicit formalised (rubberstamped or published)
- 4 = subject to control process / audited / enforced

To make these five Levels even clearer, let’s have a look at what needs to be added to go from one level to the next:

- 0 → 1 : addition of *consideration* - “listen, we are aware of this”
- 1 → 2 : addition of *written description* - “read, this is the way we do it”
- 2 → 3 : addition of *accountability* - “look, this is what we are bound to do”
- 3 → 4 : addition of *control mechanism* - “and this is how we make sure that it happens”

Such simplicity is great in terms of ease of use and presentation – but has its drawbacks too. This is especially noticeable in a few Parameters that, when you apply them in real life, are reluctant to be mapped onto a specific Level. However the advantages of this simplified scheme far outweigh the few quirks encountered.

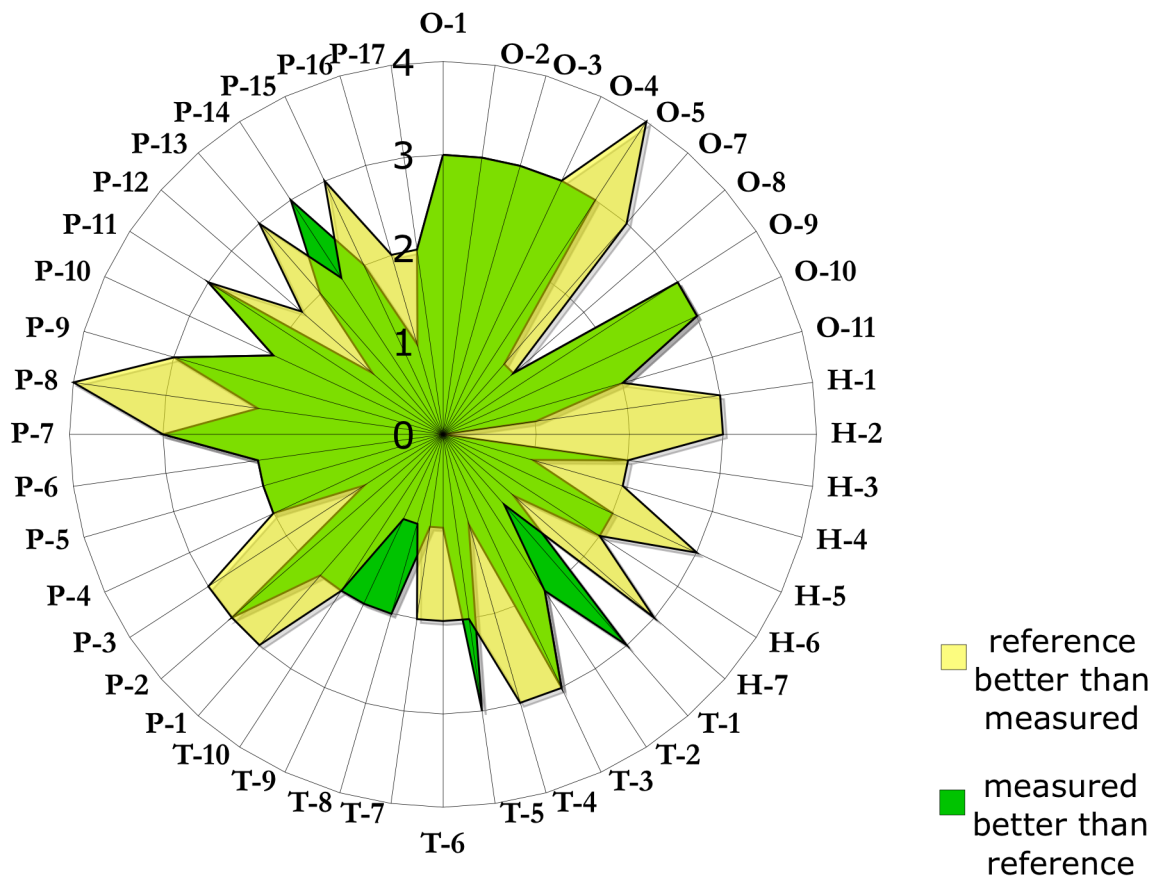
SIM3 Reporting

The basic and most useful way to report a SIM3 assessment of an actual CERT 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 CERT 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 in compliance with the reference ¹.

SIM3 RADAR DIAGRAM (xxx CERT)

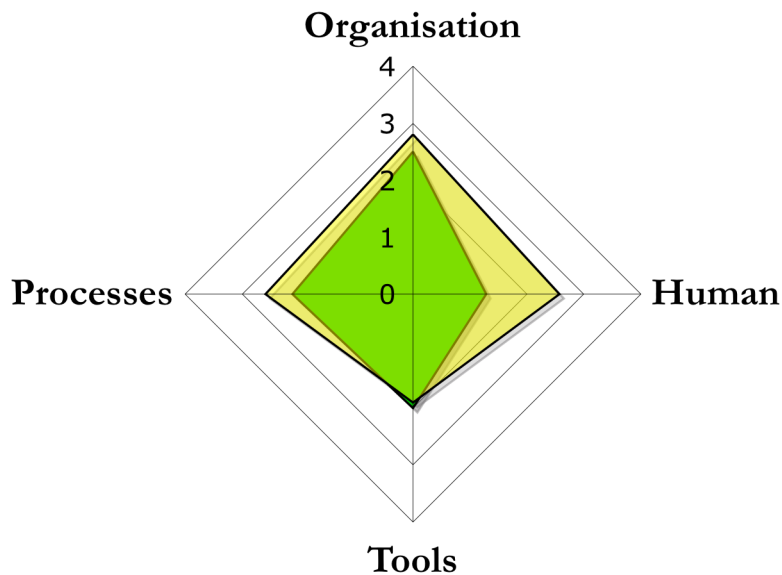


¹ currently found no way to make a key for the light green “mixed area” in the plot

3) A high level simplified chart.

A simplified presentation of the above radar diagram is desirable for management or constituency level presentations. Averaging Levels per Quadrant is acceptable for that purpose, providing the simplification and resulting lack of granularity is properly explained. Averaging over all four Quadrants is not acceptable as it suggests that one number can represent the overall SIM3 level, which is a misleading simplification. An averaging per Quadrant leads to a chart as below, derived from the radarplot above. Again, green is the actual score, dark green (not present here) above reference, yellow below reference, light green the “mixed” area which is compliant with the reference.

SIM3 OVERVIEW CHART (xxx CERT)



SIM3 Parameters

The Maturity Parameters come with the following tags:

[Parameter Identifier] : [Parameter Name:]
Description:
{ OPTIONAL: Clarification: }
{ OPTIONAL: Minimum Requirement: }
{ OPTIONAL: Accreditation Requirement: }
{ OPTIONAL: Certification Requirement: }

This is mostly self-explanatory, with the exception of “minimum requirement” – now this field will be empty in many cases, but sometimes it is not sufficient for a Parameter to be only defined: the definition must also achieve some minimum level to be acceptable to the professional CERT community. An example is O-7, which is about "service level description" where the minimum level requires a human response within a certain number of working days. This way, the "minimum requirement" could help avoid empty placeholders, as clearly e.g. a defined and approved policy (Level 3) which states that reactions will be within one month, is useless and immature in the context of CERT operations.

The optional field “Accreditation Requirement” is not foreseen to be used by the TI yet in 2010, as SIM3 is proposed to be used as a self-assessment tool in the accreditation phase, and hence not as a fixed standard. Of course, the field could be changed into “Accreditation Recommendation” along the line.

The full list of parameters is provided below.

O – “Organisation” Parameters

O-1 : MANDATE

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

O-2 : CONSTITUENCY

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

O-3 : AUTHORITY

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

O-4 : RESPONSIBILITY

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

O-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.

O-6 : (intentionally left blank – not included in “scoring”)

O-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.

O-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.

O-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).

O-10 : ORGANISATIONAL FRAMEWORK

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

Minimum requirement: Describes the CERT’s mission and parameters O-1 to O-9.

O-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.

H – “Human” Parameters

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).

H-4 : INTERNAL TRAINING

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

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.

T – “Tools” Parameters

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.

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 CERT's 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 CERT's 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 CERT's service requirements.

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.

P – “Processes” Parameters

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.

P-5 : INCIDENT DETECTION PROCESS

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

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, provided that at least three different categories of incident are defined there.

P-8 : AUDIT/FEEDBACK PROCESS

Description: Describes how the CERT improves their set-up and operations by self-assessment, external assessment and a subsequent feedback mechanism to implement the audit results.

P-9 : EMERGENCY REACHABILITY PROCESS

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

Clarification: Often only open to fellow teams.

P-10 : HANDLING OF “COMMON MAILBOX NAMES“

Description: Describes 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.

Minimum Requirement: the handling of the following mailbox aliases (from RFC-2142 and best practice) are documented:

Security: security@ ; cert@ ; abuse@

E-mail: postmaster@

IP-numbers & domain names: hostmaster@

WWW: webmaster@ ; www@

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.

P-15 : STATISTICS PROCESS

Description: Describes what incident statistics, based on their incident classification (see O-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.