Introduction of SIM3 training in Japan

Oct. 20th 2022

Seiichi “Ichi” Komura and Yoshi “Yo” Sugiura
1. Introduction of SIM3
2. Usage examples of SIM3
   - TF-CSIRT, ENISA, FIRST, NCA
   - An application example in Japan
3. SIM3 trainings
   - OCF SIM3 Auditor Training
   - NCA SIM3 intermediate training (self assessment training)
4. Summary
杉浦 芳樹
Yoshiki yo!! Sugiura
CSIRT Distiller

Since 1998
- NTT-CERT, IL-CSIRT
- NCA Board member

Team building

About SIM3
- Follower since 2008
- Certified Auditor since 2017
- Certified Trainer since Jul. 2022
Who I am?

If you want to enjoy eating in Japan, Please call me !!

Seiichi “ichi” Komura

• certified sim3 trainer and auditor, cissp
• poc and incident handler
• leader of csirt evaluation and maturity model wg, nca
• doctoral student in institute of information security
• visiting lecturer at tokyo denki university

If you want to enjoy eating in Japan, Please call me !!
What about SIM3?
Do you satisfy your team?

Can you explain it with evidence?

Do your constituency and governance layer also satisfy it?
Do you satisfy your team?

- How will the sufficiency of CSIRT to its constituency and governance layer be checked?

- How to improve the quantity and quality of CSIRT activities?

Understanding the current situation and improving your team

various viewpoint

- not only team internally
- also constituency, governance and related CSIRT
What is SIM3?

SIM3: Security Incident Management Maturity Model

- Developed by Don Stikvoort, one of authors of CSIRT handbook

- The model to help assess and improve the maturity of CSIRT management.

- Define levels for measuring implementation of the above parameters
The configuration of SIM3

1. 44 parameters in 4 quadrants, Organisation, Human, Tools and Processes

2. Levels based on documentation, approval and evaluation improvements of parameters

<table>
<thead>
<tr>
<th>Maturity level of SIM3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0  not available/undefined/unaware</td>
</tr>
<tr>
<td>1  implicit, considered but not written down</td>
</tr>
<tr>
<td>2  explicit, internal, written down but not formalized in any way</td>
</tr>
<tr>
<td>3  explicit, formalized on authority of CSIRT head</td>
</tr>
<tr>
<td>4  explicit, audited on authority of governance levels above the CSIRT head</td>
</tr>
</tbody>
</table>

★★★ Not all parameters are required to be 4 ★★★
Notes on SIM3 levels

The high level is not necessarily better

- Actual activities and scope of impact
- Frequency of change
- Spendable costs of documents and procedure
SIM3 shows issues beyond CSIRT
Quadrants of SIM3 parameters

- **Organisation**
  Basic definition of the team

- **Human**
  Defining member behavior, skill, so on

- **Tools**
  Defining the treatment tools and information sources

- **Processes**
  Common parts of a CSIRT's activities
### SIM3: Organisation

Parameters to check the CSIRT's scope of defense (constituency), authority, mission, services, policy, etc.

<table>
<thead>
<tr>
<th>num</th>
<th>parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>O-1</td>
<td>mandate</td>
</tr>
<tr>
<td>O-2</td>
<td>constituency</td>
</tr>
<tr>
<td>O-3</td>
<td>authority</td>
</tr>
<tr>
<td>O-4</td>
<td>responsibility</td>
</tr>
<tr>
<td>O-5</td>
<td>Service description</td>
</tr>
<tr>
<td>O-6</td>
<td>Intentionally left blank</td>
</tr>
<tr>
<td>O-7</td>
<td>Service level description</td>
</tr>
<tr>
<td>O-8</td>
<td>Incident classification</td>
</tr>
<tr>
<td>O-9</td>
<td>Integration of existing CSIRT systems</td>
</tr>
<tr>
<td>O-10</td>
<td>Organisational framework</td>
</tr>
<tr>
<td>O-11</td>
<td>Security policy</td>
</tr>
</tbody>
</table>
SIM3: Human

Parameters such as behavior guidelines, staffing, skill sets, training, external linkages, etc.

<table>
<thead>
<tr>
<th>Num</th>
<th>parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>H-1</td>
<td>Code of conduct/practice/ethics</td>
</tr>
<tr>
<td>H-2</td>
<td>Personnel resilience</td>
</tr>
<tr>
<td>H-3</td>
<td>Skillset description</td>
</tr>
<tr>
<td>H-4</td>
<td>Internal training</td>
</tr>
<tr>
<td>H-5</td>
<td>External training</td>
</tr>
<tr>
<td>H-6</td>
<td>Communication training</td>
</tr>
<tr>
<td>H-7</td>
<td>External networking</td>
</tr>
</tbody>
</table>
SIM3: Tools

Parameters related to the various tools and in addition to some information sources used by the CSIRT

<table>
<thead>
<tr>
<th>Num</th>
<th>parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>T-1</td>
<td>IT resources list</td>
</tr>
<tr>
<td>T-2</td>
<td>Information sources list</td>
</tr>
<tr>
<td>T-3</td>
<td>consolidated e-mail system</td>
</tr>
<tr>
<td>T-4</td>
<td>incident tracking system</td>
</tr>
<tr>
<td>T-5</td>
<td>resilient phone</td>
</tr>
<tr>
<td>T-6</td>
<td>resilient e-mail</td>
</tr>
<tr>
<td>T-7</td>
<td>resilient internet access</td>
</tr>
<tr>
<td>T-8</td>
<td>incident prevention toolset</td>
</tr>
<tr>
<td>T-9</td>
<td>incident detection toolset</td>
</tr>
<tr>
<td>T-10</td>
<td>incident resolution toolset</td>
</tr>
</tbody>
</table>
## SIM3: Processes

Parameters related to CSIRT activity processes such as incident handling, escalation, management and improvement of team

<table>
<thead>
<tr>
<th>Num</th>
<th>parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>P–1</td>
<td>Escalation to governance level</td>
</tr>
<tr>
<td>P–2</td>
<td>Escalation to press function</td>
</tr>
<tr>
<td>P–3</td>
<td>Escalation to legal function</td>
</tr>
<tr>
<td>P–4</td>
<td>Incident prevention process</td>
</tr>
<tr>
<td>P–5</td>
<td>Incident detection process</td>
</tr>
<tr>
<td>P–6</td>
<td>Incident resolution process</td>
</tr>
<tr>
<td>P–7</td>
<td>Specific incident process</td>
</tr>
<tr>
<td>P–8</td>
<td>Audit/feedback process</td>
</tr>
<tr>
<td>P–9</td>
<td>Emergency reachability process</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Num</th>
<th>parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>P–10</td>
<td>Best practice e–mail and web presence</td>
</tr>
<tr>
<td>P–11</td>
<td>Secure information handling process</td>
</tr>
<tr>
<td>P–12</td>
<td>Information sources process</td>
</tr>
<tr>
<td>P–13</td>
<td>Outreach process</td>
</tr>
<tr>
<td>P–14</td>
<td>Reporting process</td>
</tr>
<tr>
<td>P–15</td>
<td>Statistics process</td>
</tr>
<tr>
<td>P–16</td>
<td>Meeting process</td>
</tr>
<tr>
<td>P–17</td>
<td>Peer–to–peer process</td>
</tr>
</tbody>
</table>
SIM3 radar diagram

- diagram showing the level of each SIM3 parameter
- easy to identify team’s strengths and issues for improvement
What is a matured CSIRT?

The quality of the services is stable
Team has the resources (operation, environment, etc.)
to carry out the necessary activities

It does not evaluate advanced technical skills
or the ability to handle huge volumes
Usage examples
example 1: certified teams of TF-CSIRT

TF-CSIRT evaluates the members who wish to be by SIM3

It certifies organisations that meet the criteria as a ‘certified team’

<table>
<thead>
<tr>
<th>Certified teams in TF-CSIRT (on Jul. 28, 2022)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Public organisation</td>
<td>9</td>
</tr>
<tr>
<td>Research and educational Institutions</td>
<td>6</td>
</tr>
<tr>
<td>ISP</td>
<td>4</td>
</tr>
<tr>
<td>others</td>
<td>7</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>26</strong></td>
</tr>
</tbody>
</table>

https://www.trusted-introducer.org/directory/teams.html
example 2 : national CSIRTs in EU by ENISA

European Union Agency for Cybersecurity (ENISA) developed documents for national CSIRT maturity step-up by SIM3.

- Objective: Improve the maturity of national CSIRTs in EU countries
- Methods: Self-check and pair-check methods

https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process
FIRST: self-checking for joining

Self-assessment of 11 out of 44 SIM3 parameters at a certain level or above.
## Self-check parameters for FIRST joining

<table>
<thead>
<tr>
<th>Num</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>O-1</td>
<td>mandate</td>
</tr>
<tr>
<td>O-2</td>
<td>constituency</td>
</tr>
<tr>
<td>O-3</td>
<td>authority</td>
</tr>
<tr>
<td>O-4</td>
<td>responsibility</td>
</tr>
<tr>
<td>O-5</td>
<td>Service description</td>
</tr>
<tr>
<td>O-10</td>
<td>Organisational framework</td>
</tr>
<tr>
<td>H-1</td>
<td>Code of conduct/practice/ethics</td>
</tr>
<tr>
<td>H-2</td>
<td>Personnel resilience</td>
</tr>
<tr>
<td>H-7</td>
<td>External networking</td>
</tr>
<tr>
<td>P-1</td>
<td>Escalation to governance level</td>
</tr>
<tr>
<td>P-11</td>
<td>Secure information handling process</td>
</tr>
</tbody>
</table>
SIM3 self assessment tool

OCF web site serves online tool for SIM3 assessment

https://sim3-check.opencsirt.org/#/
SIM3 Use and Assessment Cases

- Use of support for Creating & Development of CSIRTs
  - Not use all parameters
  - Not use Levels
  - Useful

- Almost every year assessment
  - Interview to a representative and manager
  - Find gaps and challenges
  - Assessment report, not only levels also gap analysis
Comparison
SIM3 Trainings
OCF SIM3 auditor training

3-day course (from 9 to 17 except last day) with certification test

- consist of all quadrants and level
- test is held in the afternoon of the last day
- some lectures, mainly exercises and discussions
OCF SIM3 training
Seminar in Japan in 2019
OCF SIM3 training

Seminar in Ireland in 2022

In this seminar, 3 trainer were certified with auditors
Self Assessment Training

Training objectives

• To learn how to assess the situation of your team using SIM3

Specific learning content:

• the composition and activities of CSIRT operation and management
• key concepts to be decided and implemented
• assessment based on data and edidence
Auditor training and assessment training

**Auditor training**:  
- certifying OCF certified auditors  
- mainly, discussion and sharing experience

**Assessment training**:  
- developing people who can evaluate their own organization  
- mainly, lecture of key concepts, issues and precautions, and have them practise using SIM3
Timetable of Assessment training

Day 1.
• Warm-up exercise: ice-breaking
• CSIRT forms and components of activities
  Overview of SIM3
• Organisation quadrant

Day 2.
• Human quadrant
• Tools quadrant
• Process quadrant

Day 3.
• Assessment of levels
• Assessment Exercise
• Summary
Contents

CSIRT shape and composition

What are activities and tasks of a CSIRT?

1. Provisioning activities for the Constituency
2. External cooperation activities
3. Activities to optimise services
4. Activities to optimise the role of the CSIRT within their organisation
5. Working as an department within an organisation (without CSIRT features)
Keypoints of Organisation quadrant

- Definition of CSIRT as an team and in their organisation
- CSIRT should be recognized by management, law, etc., and determine a framework of mission, constituency and authority
- Define services, SLAs, incident classification, policies and relationships with relevant CSIRTs
- Combine them in one document (CSIRT Definition (Charter))

Defining the CSIRT framework

O-8: example of description

The incident classification shall be as follows. The classification shall be reviewed as necessary.

- Receipt of suspicious emails (excluding dissemination-type attack emails)
- Suspicious access
- Unauthorised relay of server
- Intrusion into internal systems and internal network equipment
- Attacks leading to denial of service (DoS)
- Infection with computer viruses, worms or other malware
- Leakage of information due to employee negligence or deliberate intent
- Other

O-3: if the authority is not fixed?

What bothers you? Not troubling?

CSIRTs cannot fulfil their responsibilities
- Cannot quarantine from NW to stop infection

CSIRTs are forced accountability they are not responsible
- Who makes the decision to shut down commercial servers when a serious vulnerability is disclosed?
Future plans

Hold Auditor training in Japan
• Targetting Feb. 2023

Improve and develop assessment training
• Development and implementation of online teaching materials
• Translating into English and implementation abroad
Effect of evaluate by SIM3

simply self-check by SIM3
  • Getting some analytical bases to improve teams
    • maturity issues
    • not maturity issues
  • being aware of comprehensive conditions
    • CSIRT
    • enterprise viewpoint

We plan to make materials and examples for supporting self-check and raising the level of CSIRTs
At last,

There is a famous Chinese strategist words,

*If you know your enemies and know yourself, you will not be warried in a hundred battles.*

CSIRTs network share enemies information from the beginning.

We want to share how to know ourselves for become not to be warried.
Thank you for your listening

Q&A

Dizekuje
Dank u well
Danke shoen
Merci beaucoup
ありがとうございました