TLP:CLEAR

Introduction of SIM3 training in Japan

Oct. 20th 2022
Seiichi “Ichi” Komura and Yoshi “Yo” Sugiura

TLP:CLEAR

Contents

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
  - JPCERT/CC(1998-2002)
  - 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?

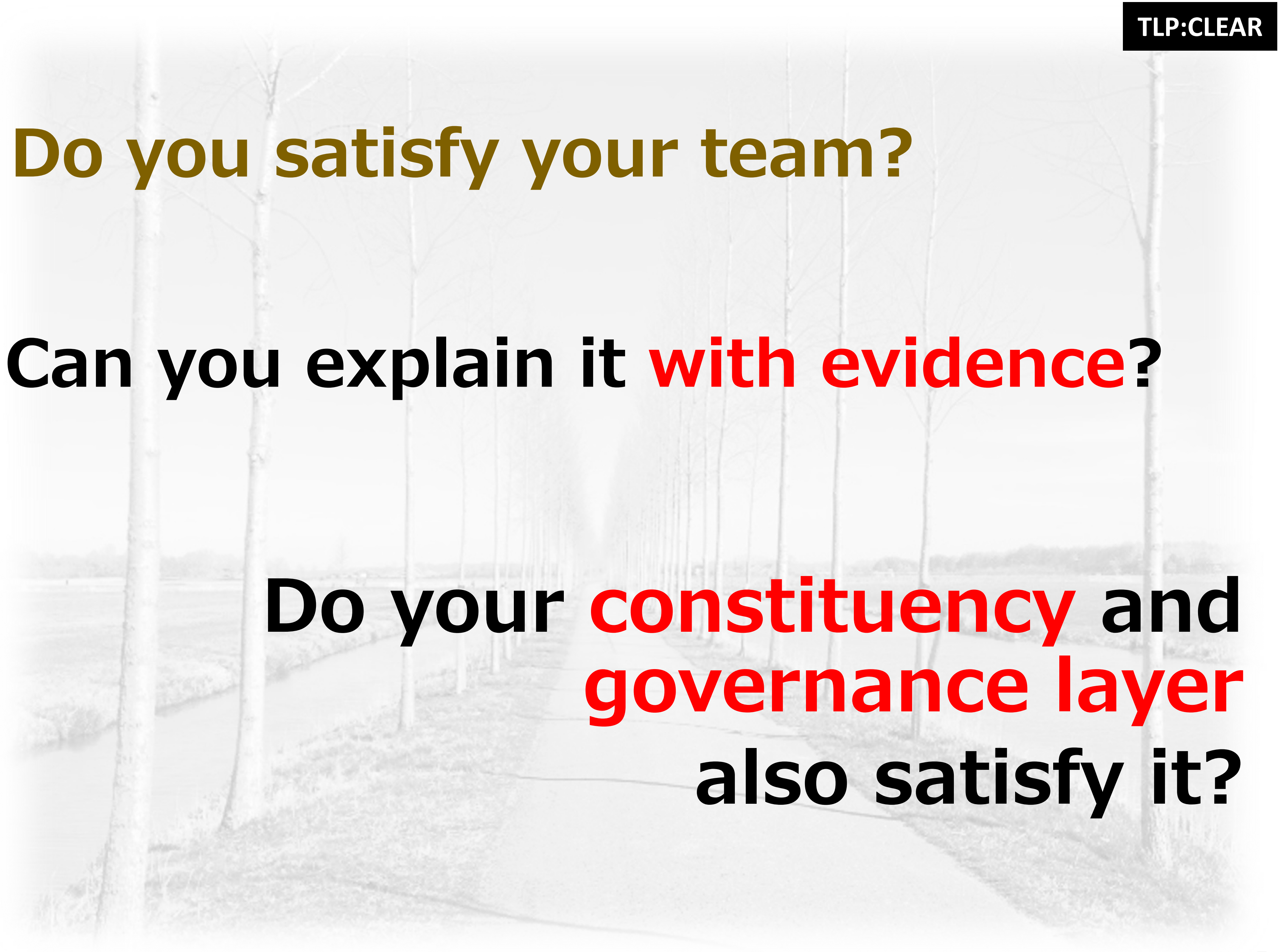
If you want to enjoy eating in Japan,
Please call me !!

Seiichi *"ichi"* *K*omura

- **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**

TLP:CLEAR

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

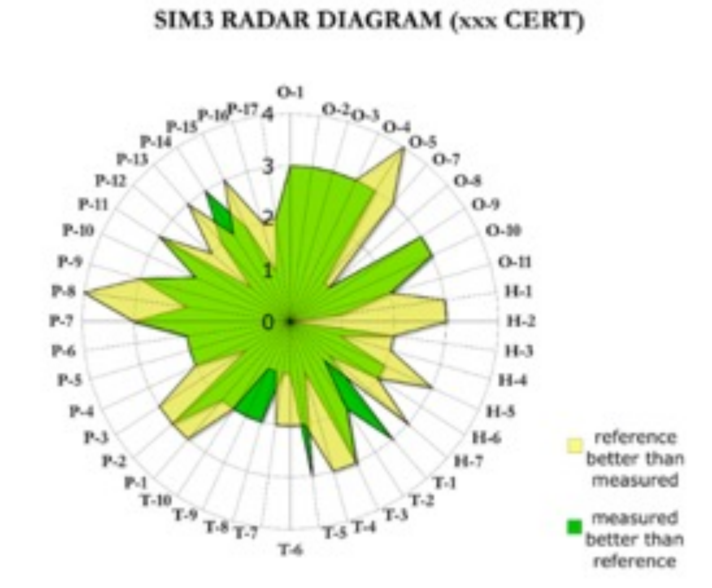
- **Developed by Don Stikvoort,**
  one of authors of CSIRT handbook
- **The model to help assess and improve the maturity of CSIRT management.**
- **Define levels for measuring implementation of the above parameters**

TLP:CLEAR

The configuration of SIM3

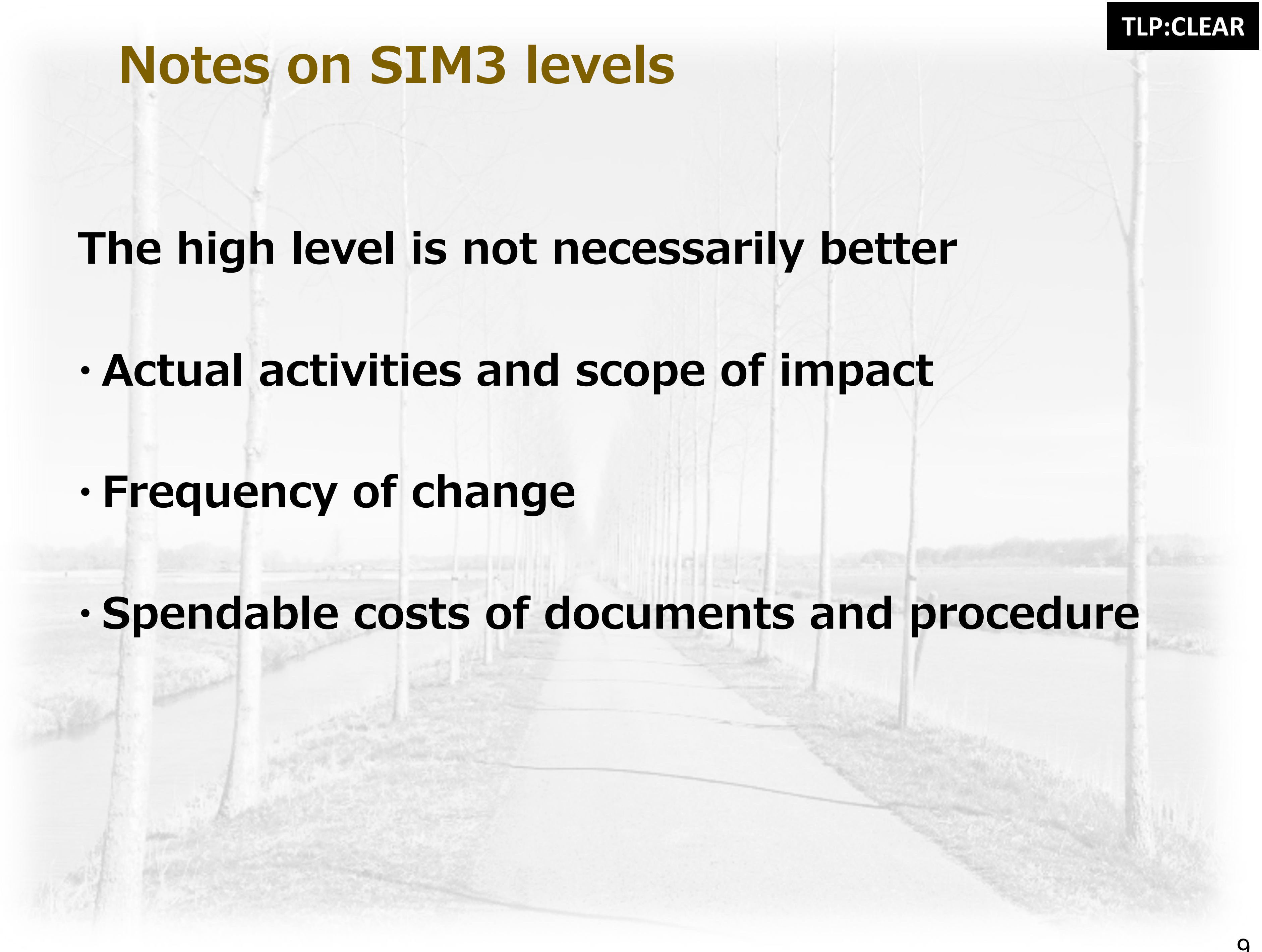
1. 44 parameters in 4 quadrants,
   Organisation, Human, Tools and Processes
2. Levels based on documentation, approval and evaluation improvements of parameters

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



☆★ Not all parameters are required to be 4 ★☆

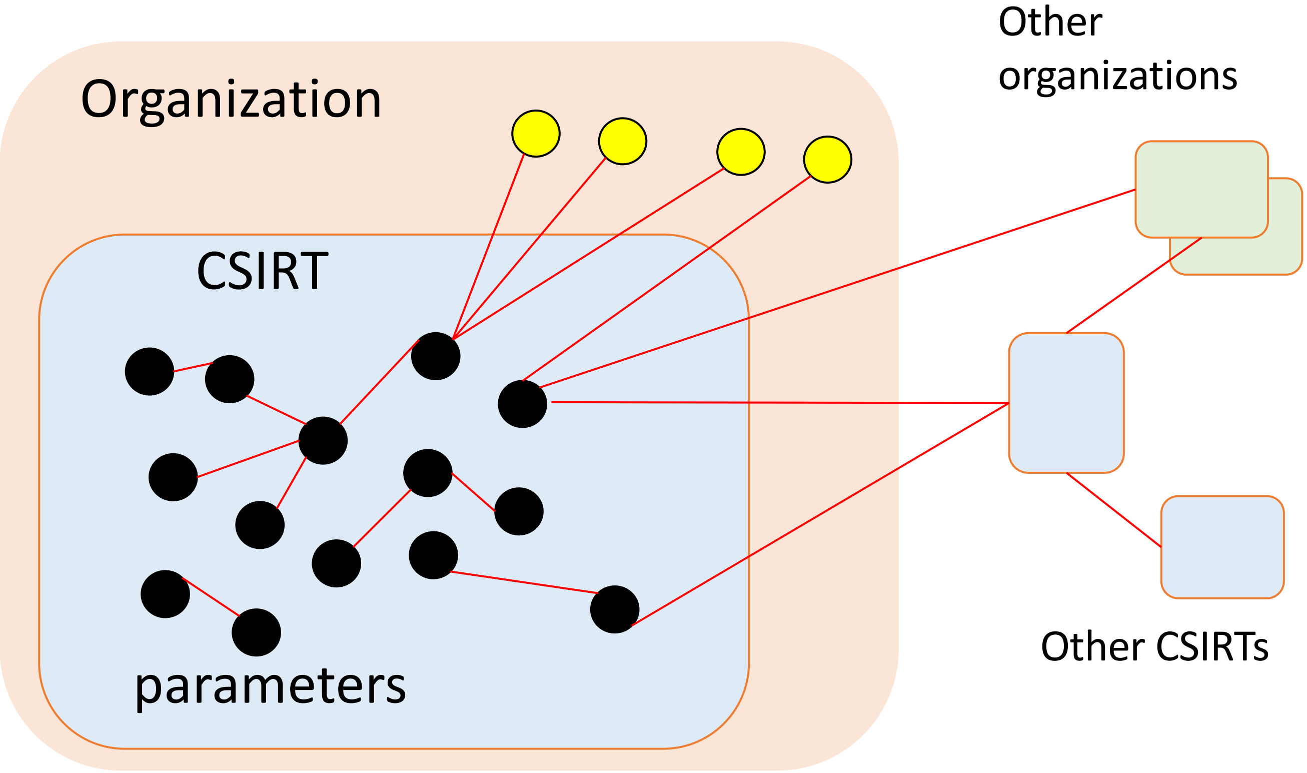
Notes on SIM3 levels



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

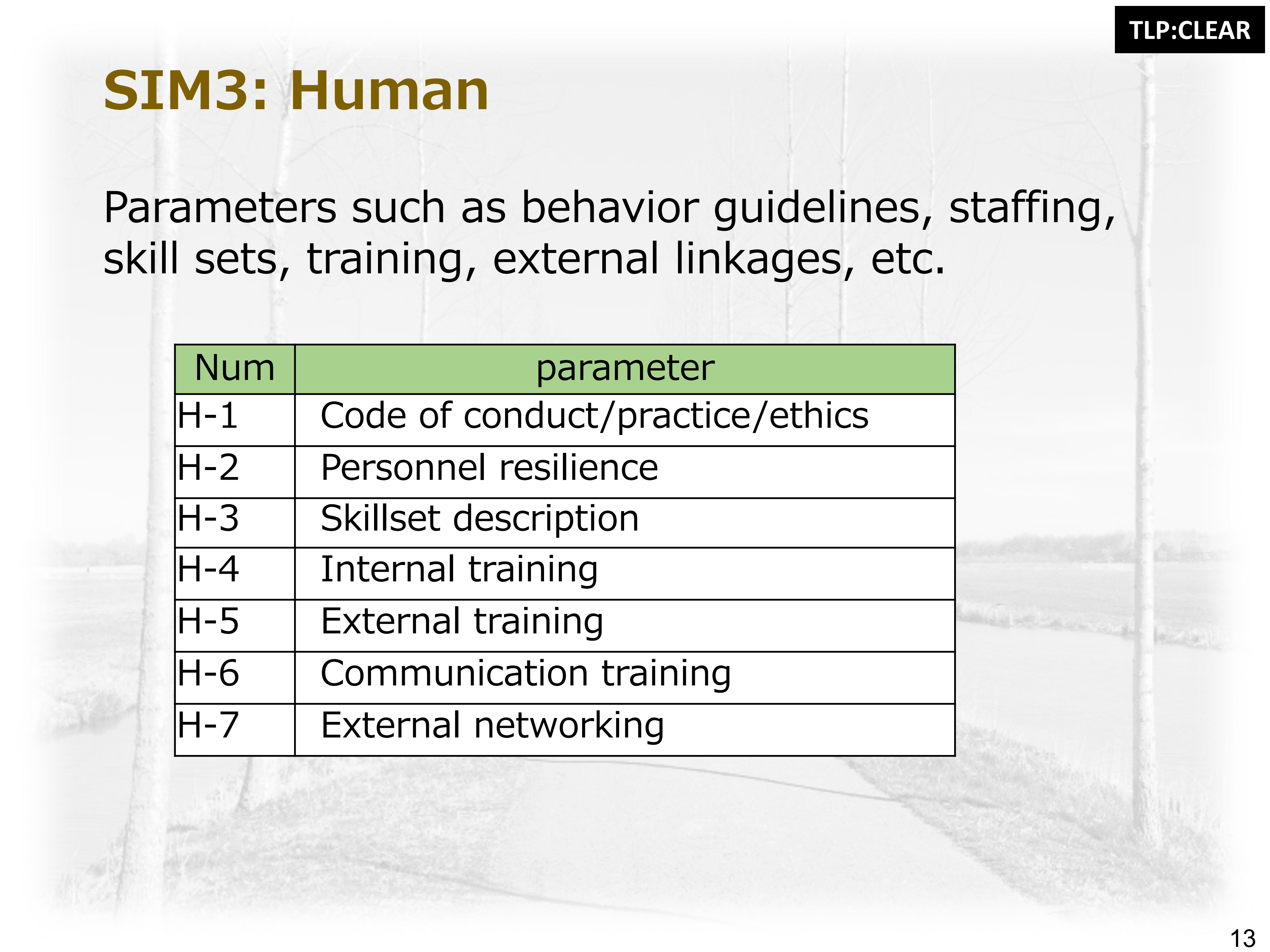
- **Tools**
  Defining the treatment tools and information sources

- **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.

num	parameters
O-1	mandate
O-2	constituency
O-3	authority
O-4	responsibility
O-5	Service description
O-6	Intentionally left blank
O-7	Service level description
O-8	Incident classification
O-9	Integration of existing CSIRT systems
O-10	Organisational framework
O-11	Security policy



SIM3: Human

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

Num	parameter
H-1	Code of conduct/practice/ethics
H-2	Personnel resilience
H-3	Skillset description
H-4	Internal training
H-5	External training
H-6	Communication training
H-7	External networking

TLP:CLEAR

SIM3: Tools

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

Num	parameter
T-1	IT resources list
T-2	Information sources list
T-3	consolidated e-mail system
T-4	incident tracking system
T-5	resilient phone
T-6	resilient e-mail
T-7	resilient internet access
T-8	incident prevention toolset
T-9	incident detection toolset
T-10	incident resolution toolset

TLP:CLEAR

SIM3: Processes

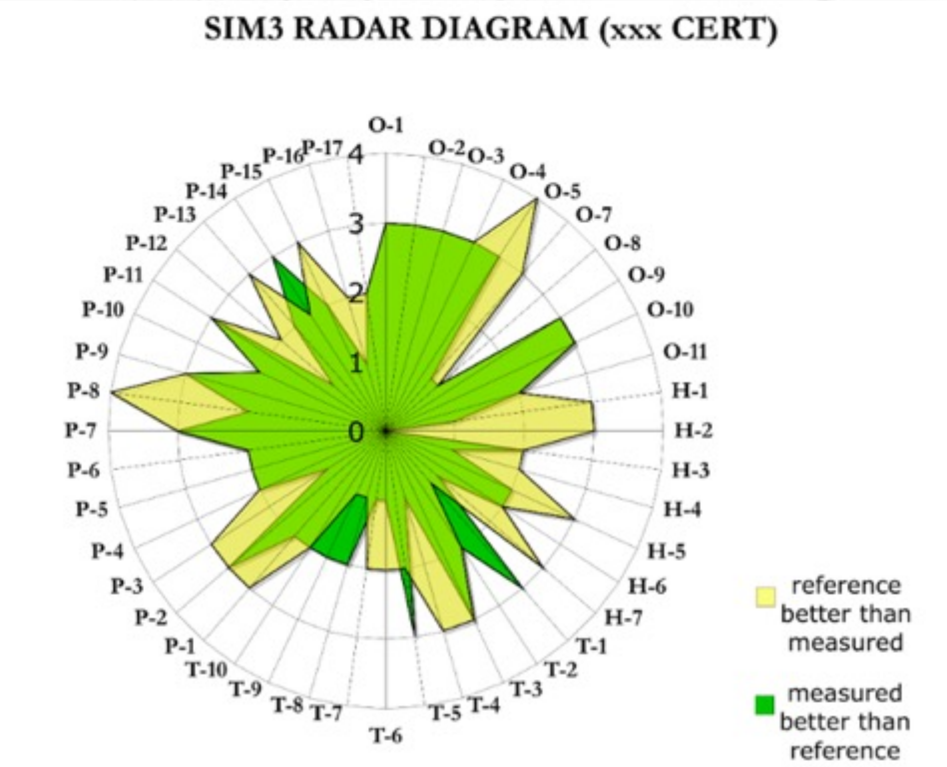
Parameters related to CSIRT activity processes such as incident handling, escalation, management and improvement of team

Num	parameter
P-1	Escalation to governance level
P-2	Escalation to press function
P-3	Escalation to legal function
P-4	Incident prevention process
P-5	Incident detection process
P-6	Incident resolution process
P-7	Specific incident process
P-8	Audit/feedback process
P-9	Emergency reachability process

num	parameter
P-10	Best practice e-mail and web presence
P-11	Secure information handling process
P-12	Information sources process
P-13	Outreach process
P-14	Reporting process
P-15	Statistics process
P-16	Meeting process
P-17	Peer-to-peer process

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

TLP:CLEAR

Usage examples

TLP:CLEAR

example１ : 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'

Certified teams in TF-CSIRT(on Jul. 28, 2022)	
Public organisation	9
Research and educational Institutions	6
ISP	4
others	7
Total	26

https://www.trusted-introducer.org/directory/teams.html

example２:national CSIRTs in EU by ENISA

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

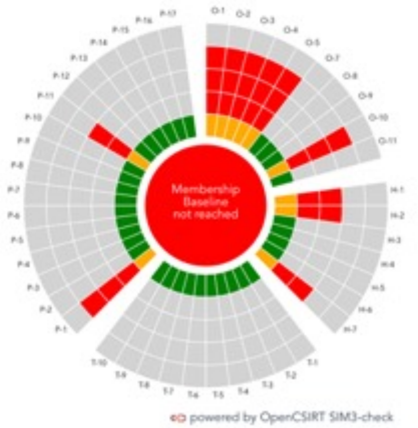
- Objective: Improve the maturity of national CSIRTs in EU countries
- Methods: Self-check and pair-check methods

ENISA Maturity Evaluation Methodology for CSIRTs

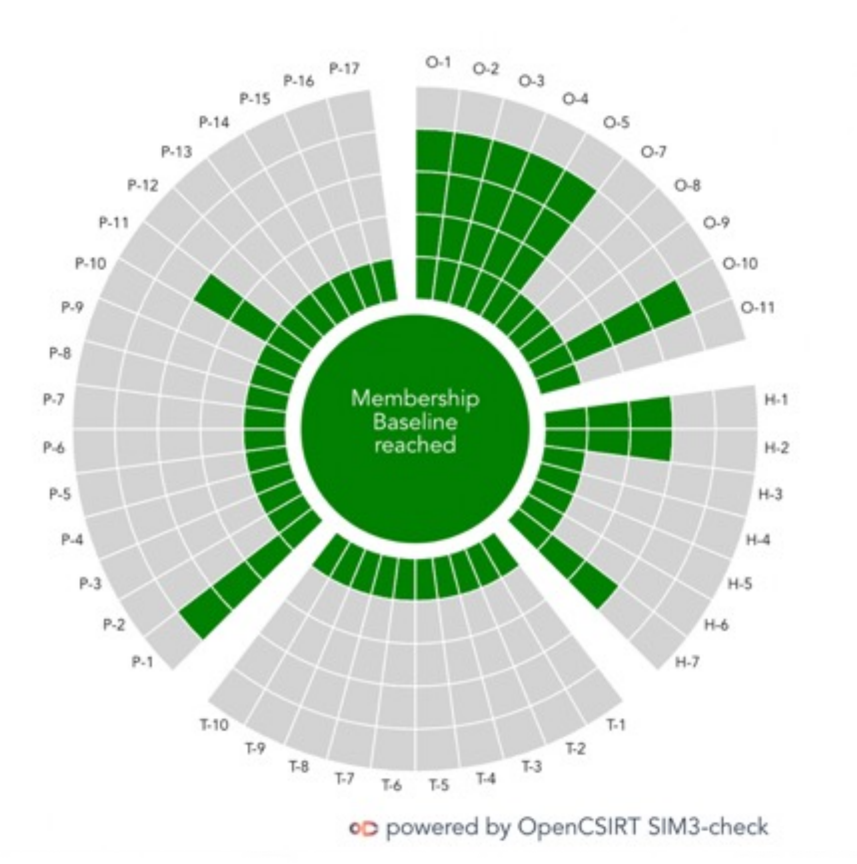
https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process

FIRST: self-checking for joining

Self-assessment of 11 out of 44 SIM3 parameters at a certain level or above.



powered by OpenCSIRT SIM3-check



powered by OpenCSIRT SIM3-check

TLP:CLEAR

Self-check parameters for FIRST joining

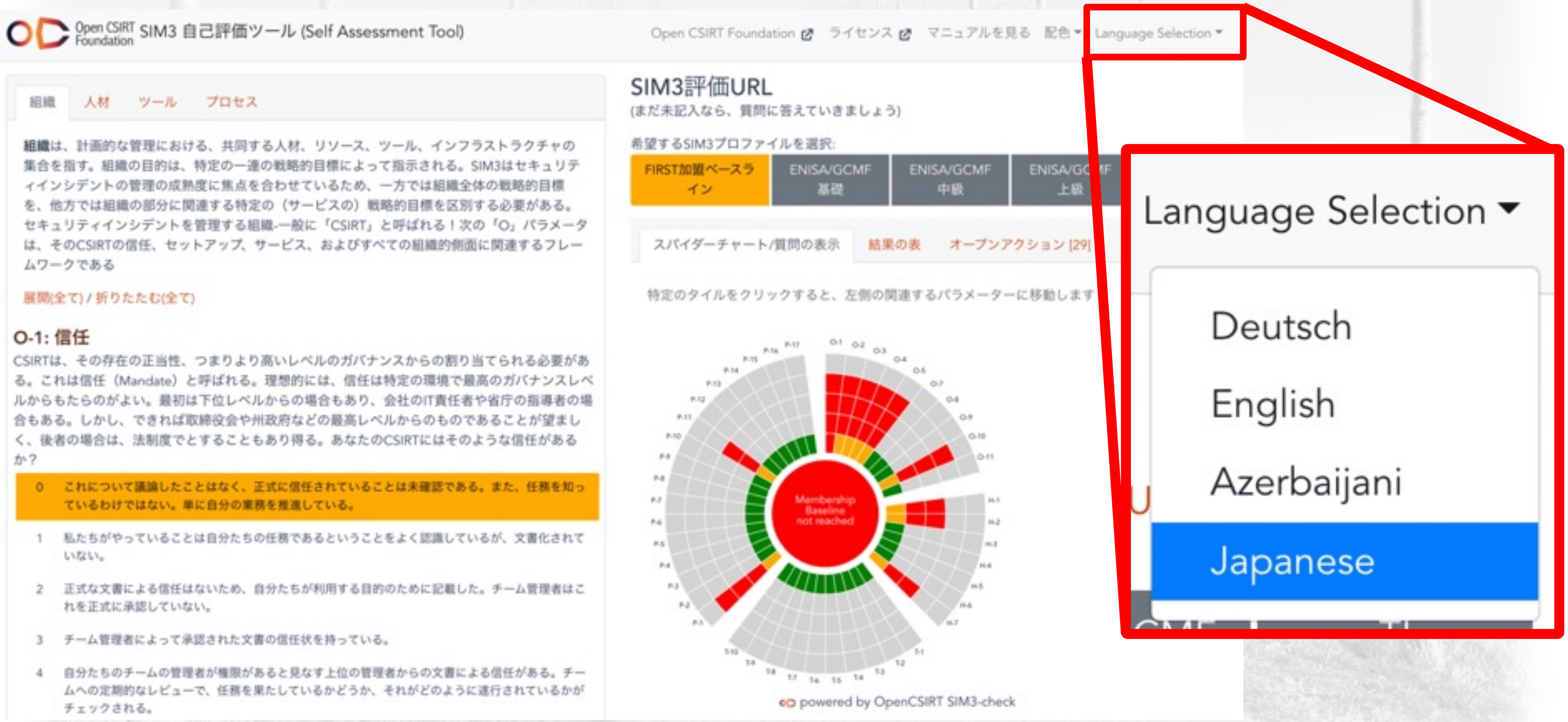
Num	parameter
O-1	mandate
O-2	constituency
O-3	authority
O-4	responsibility
O-5	Service description
O-10	Organisational framework
H-1	Code of conduct/practice/ethics
H-2	Personnel resilience
H-7	External networking
P-1	Escalation to governance level
P-11	Secure information handling process

TLP:CLEAR

SIM3 self assessment tool

OCF web site serves online tool for SIM3 asssessment

https://sim3-check.opencsirt.org/#/



Open CSIRT Foundation SIM3 自己評価ツール (Self Assessment Tool)

組織は、計画的な管理における、共同する人材、リソース、ツール、インフラストラクチャの集合を指す。組織の目的は、特定の一連の戦略的目標によって指示される。SIM3はセキュリティインシデントの管理の成熟度に焦点を合わせているため、一方では組織全体の戦略的目標を、他方では組織の部分に関連する特定の（サービスの）戦略的目標を区別する必要がある。セキュリティインシデントを管理する組織-一般に「CSIRT」と呼ばれる！次の「O」パラメータは、そのCSIRTの信任、セットアップ、サービス、およびすべての組織的側面に関連するフレームワークである

展開(全て) / 折りたたむ(全て)

O-1: 信任

CSIRTは、その存在の正当性、つまりより高いレベルのガバナンスからの割り当てられる必要がある。これは信任（Mandate）と呼ばれる。理想的には、信任は特定の環境で最高のガバナンスレベルからもたらのがよい。最初は下位レベルからの場合もあり、会社のIT責任者や省庁の指導者の場合もある。しかし、できれば取締役会や州政府などの最高レベルからのものであることが望ましく、後者の場合は、法制度でとすることもあり得る。あなたのCSIRTにはそのような信任があるか？

0 これについて議論したことはなく、正式に信任されていることは未確認である。また、任務を知っているわけではない。単に自分の業務を推進している。

1 私たちがやっていることは自分たちの任務であるということをよく認識しているが、文書化されていない。

2 正式な文書による信任はないため、自分たちが利用する目的のために記載した。チーム管理者はこれを正式に承認していない。

3 チーム管理者によって承認された文書の信任状を持っている。

4 自分たちのチームの管理者が権限があると見なす上位の管理者からの文書による信任がある。チームへの定期的なレビューで、任務を果たしているかどうか、それがどのように遂行されているかがチェックされる。

SIM3評価URL

(まだ未記入なら、質問に答えていきましょう)

希望するSIM3プロファイルを選択:

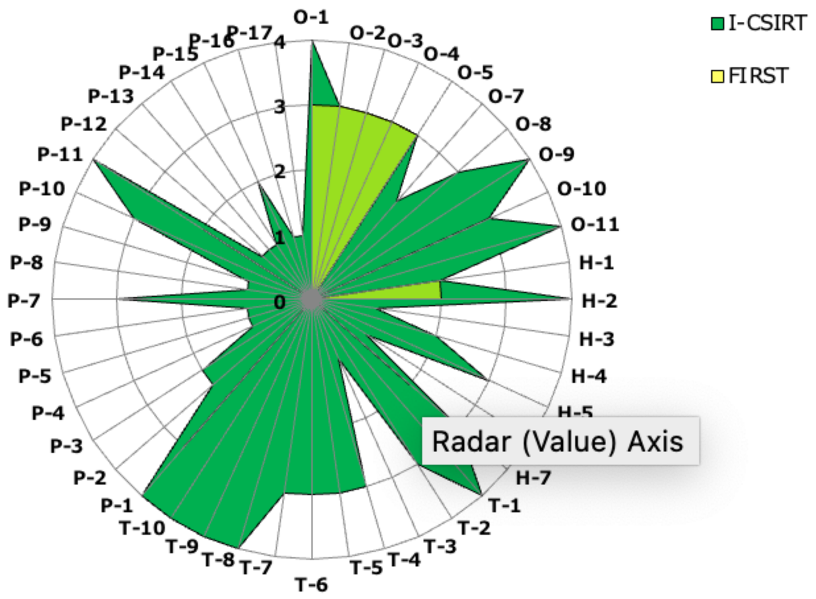
特定のタイルをクリックすると、左側の関連するパラメーターに移動します

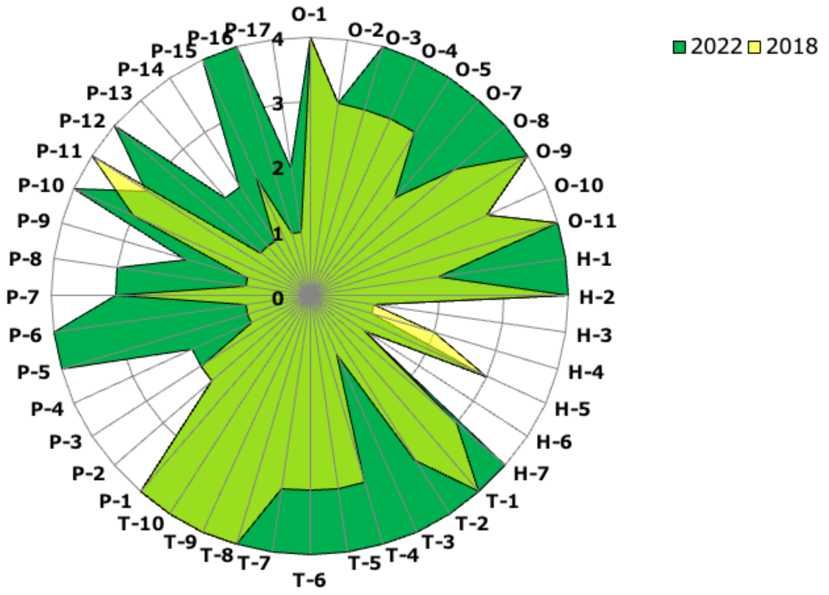
powered by OpenCSIRT SIM3-check

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


O-1
O-2
O-3
O-4
O-5
O-7
O-8
O-9
O-10
O-11
H-1
H-2
H-3
H-4
H-5
H-7
T-1
T-2
T-3
T-4
T-5
T-6
T-7
T-8
T-9
T-10
P-1
P-2
P-3
P-4
P-5
P-6
P-7
P-8
P-9
P-10
P-11
P-12
P-13
P-14
P-15
P-16
P-17
0
1
2
3
4
🟩 I-CSIRT
🟨 FIRST
Radar (Value) Axis


O-1
O-2
O-3
O-4
O-5
O-7
O-8
O-9
O-10
O-11
H-1
H-2
H-3
H-4
H-5
H-6
H-7
T-1
T-2
T-3
T-4
T-5
T-6
T-7
T-8
T-9
T-10
P-1
P-2
P-3
P-4
P-5
P-6
P-7
P-8
P-9
P-10
P-11
P-12
P-13
P-14
P-15
P-16
P-17
0
1
2
3
4
🟩 2022
🟨 2018

TLP:CLEAR

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 discusstions

SIM3 Certified Auditor training

From 4 - 6 July 2022, the Open CSIRT Foundation (OCF) will organise the next 3-day training to become a Certified SIM3 Auditor – live in Dublin, Ireland. See below for details.

TLP:CLEAR

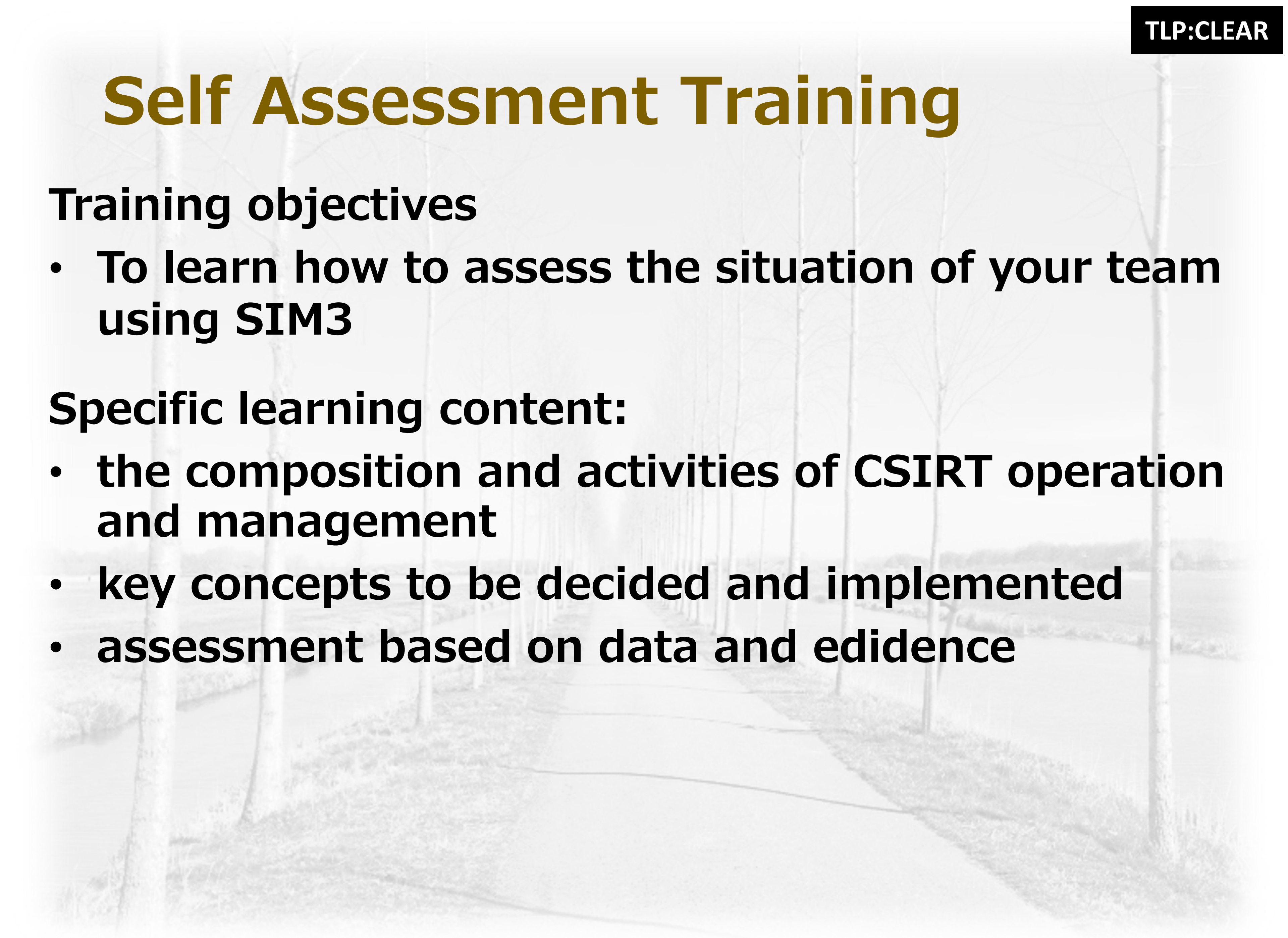
OCF SIM3 training

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

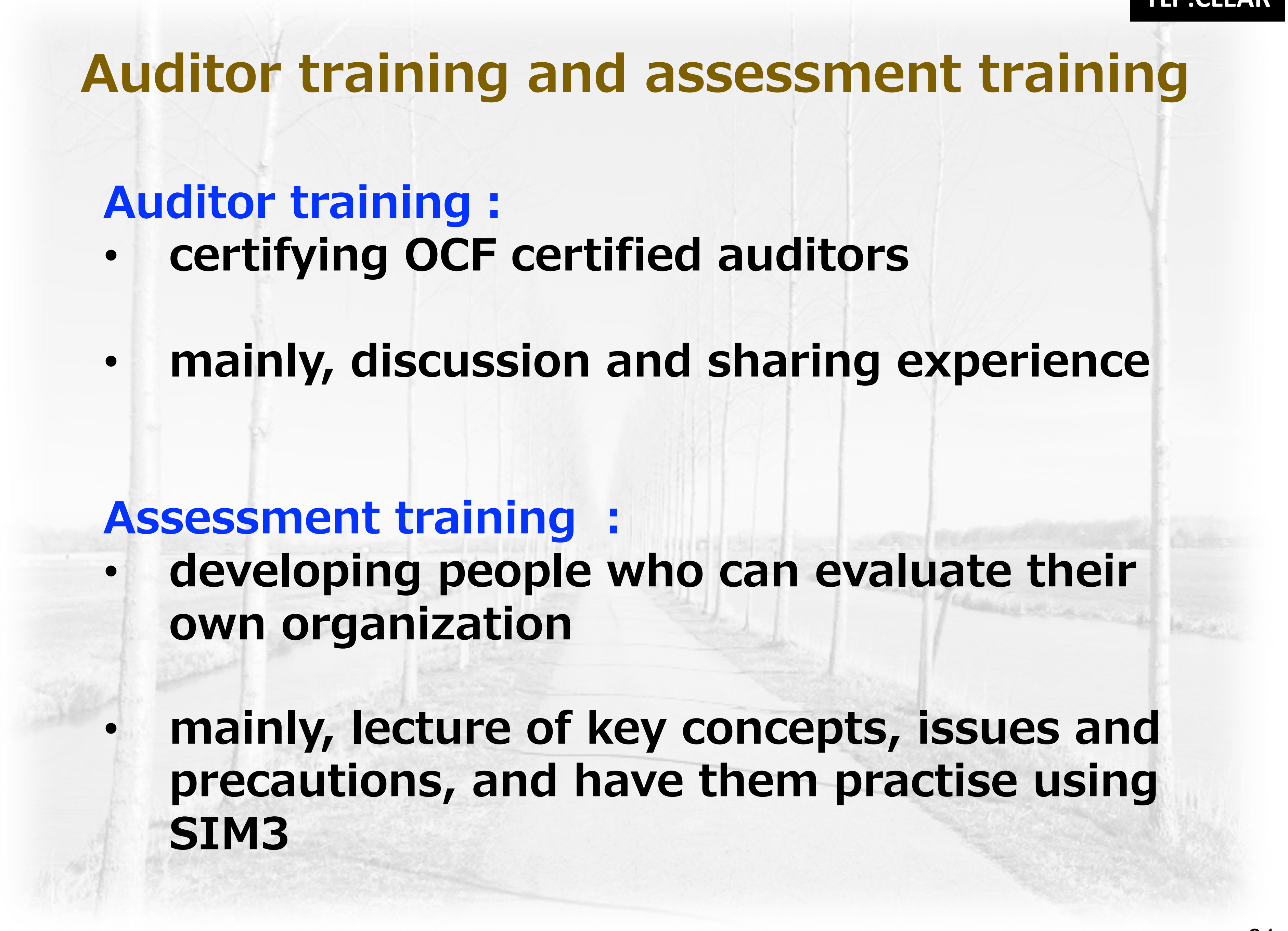
Training objectives

- 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



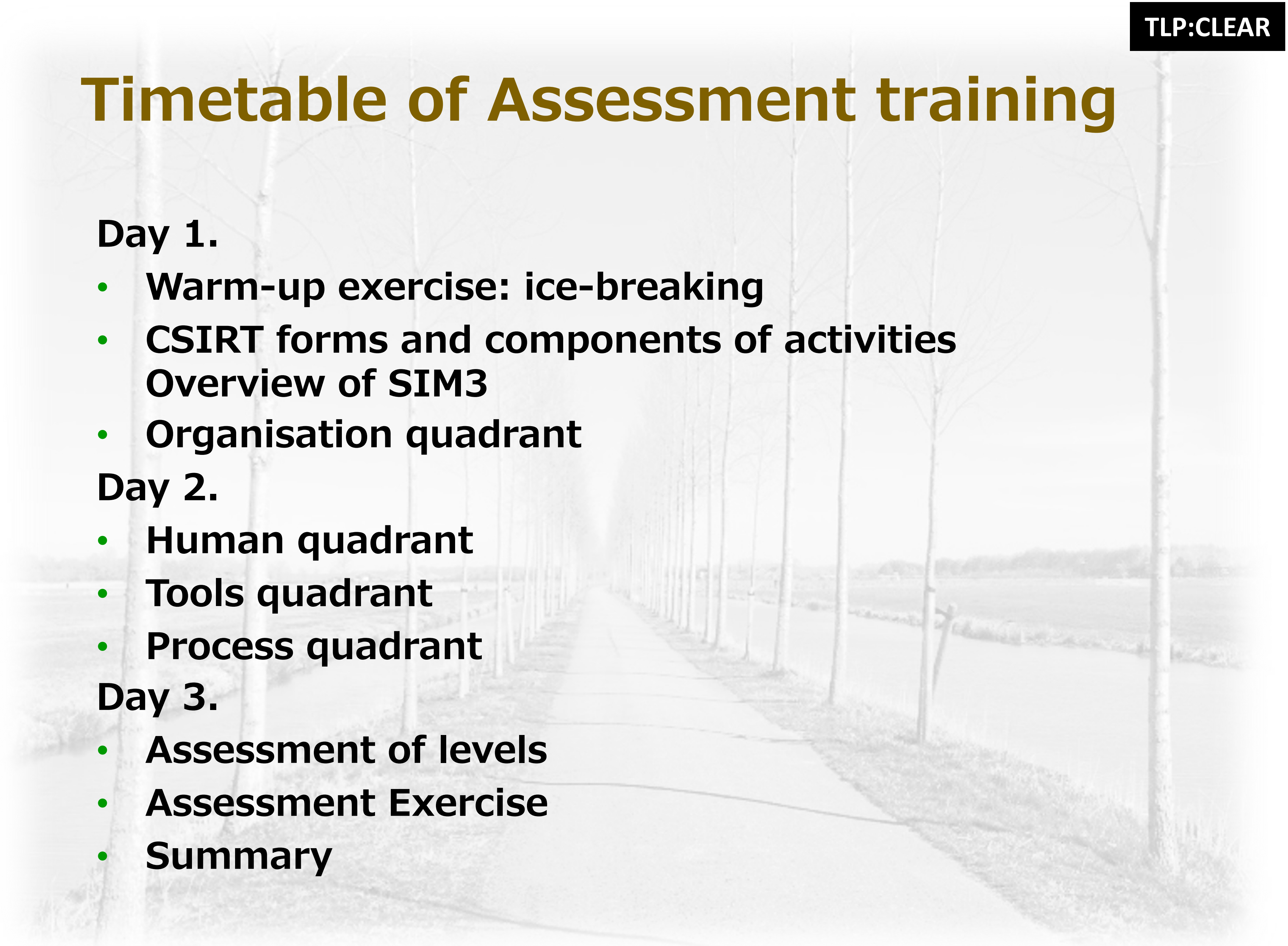
Auditor training :

- 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

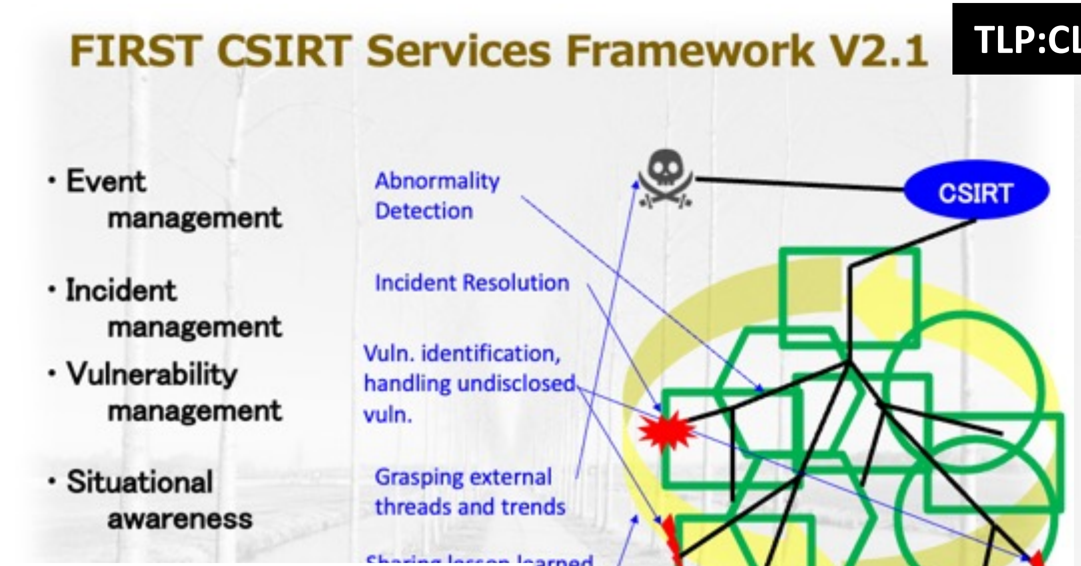
Day 3.

- Assessment of levels
- Assessment Exercise
- Summary

TLP:CLEAR

Contents

CSIRT shape and composition

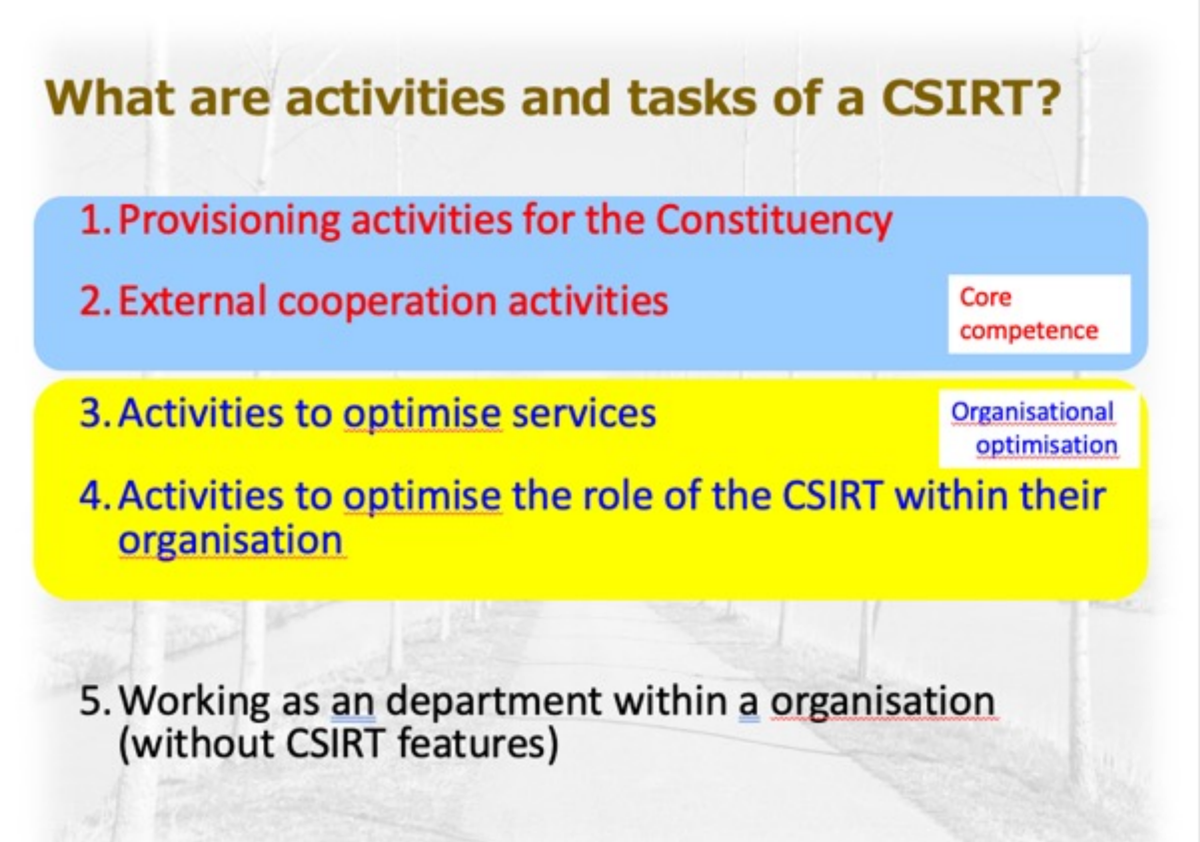


FIRST CSIRT Services Framework V2.1

- Event management
- Incident management
- Vulnerability management
- Situational awareness

Abnormality Detection
Incident Resolution
Vuln. identification, handling undisclosed vuln.
Grasping external threads and trends
Sharing lesson learned
rcise
CSIRT
internal Information systems and network

SIRT_Services_Framework_v2.1.0_ja.pdf



What are activities and tasks of a CSIRT?

1. Provisioning activities for the Constituency
2. External cooperation activities

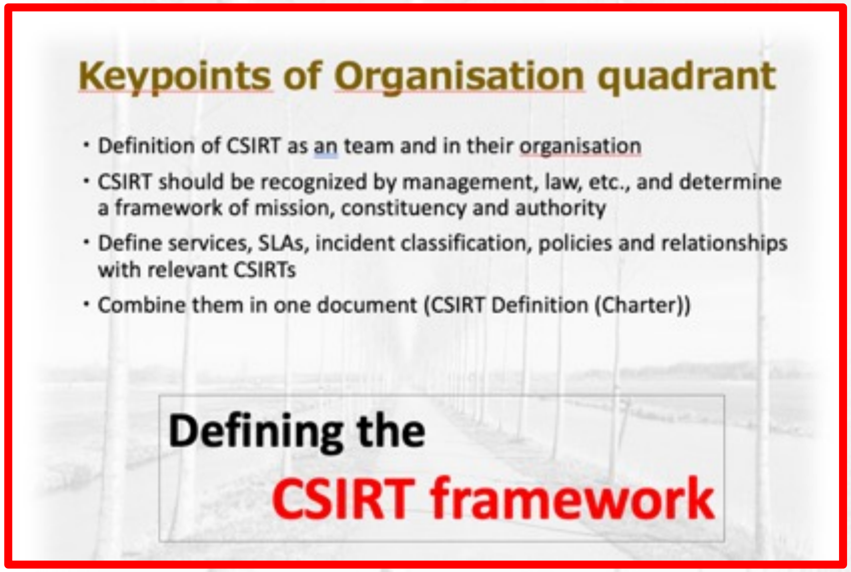
Core competence

3. Activities to optimise services
4. Activities to optimise the role of the CSIRT within their organisation

Organisational optimisation

5. Working as an department within a organisation (without CSIRT features)

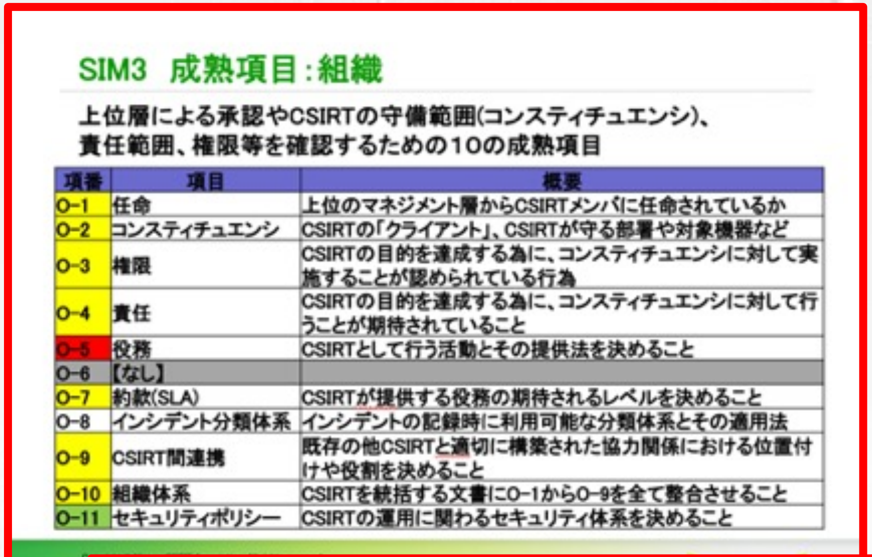
Outline of a quadrant



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))

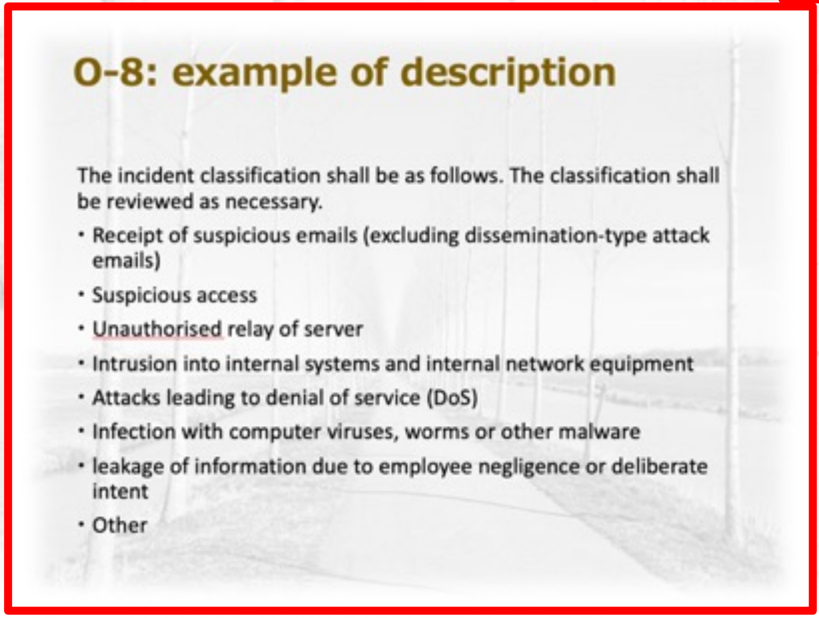
Defining the
CSIRT framework



SIM3　成熟項目：組織

上位層による承認やCSIRTの守備範囲(コンスティチュエンシ)、
責任範囲、権限等を確認するための10の成熟項目

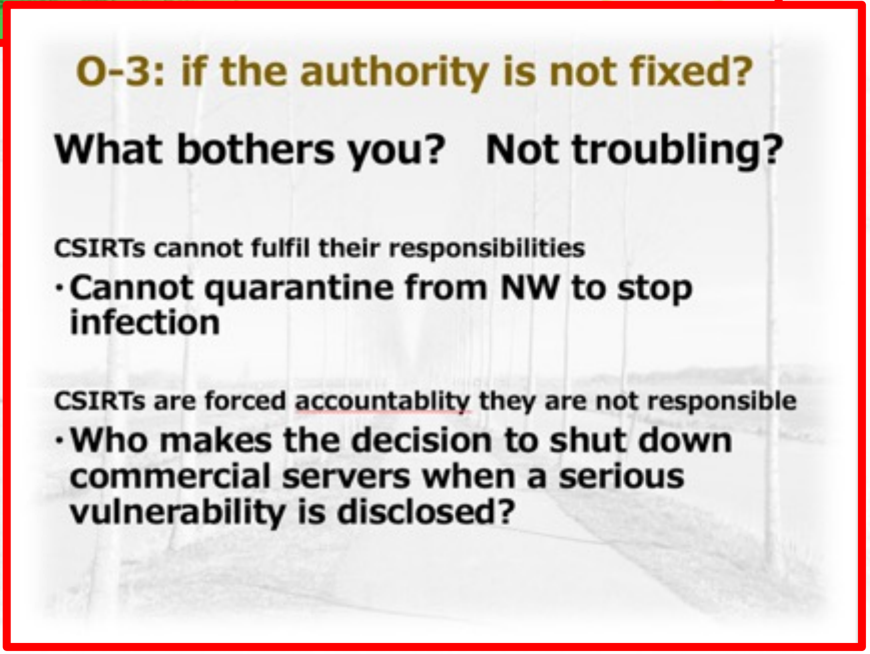
項番	項目	概要
O-1	任命	上位のマネジメント層からCSIRTメンバに任命されているか
O-2	コンスティチュエンシ	CSIRTの「クライアント」、CSIRTが守る部署や対象機器など
O-3	権限	CSIRTの目的を達成する為に、コンスティチュエンシに対して実施することが認められている行為
O-4	責任	CSIRTの目的を達成する為に、コンスティチュエンシに対して行うことが期待されていること
O-5	役務	CSIRTとして行う活動とその提供法を決めること
O-6	【なし】	
O-7	約款(SLA)	CSIRTが提供する役務の期待されるレベルを決めること
O-8	インシデント分類体系	インシデントの記録時に利用可能な分類体系とその適用法
O-9	CSIRT間連携	既存の他CSIRTと適切に構築された協力関係における位置付けや役割を決めること
O-10	組織体系	CSIRTを統括する文書にO-1からO-9を全て整合させること
O-11	セキュリティポリシー	CSIRTの運用に関わるセキュリティ体系を決めること



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 accountablity they are not responsible

- **Who makes the decision to shut down commercial servers when a serious vulnerability is disclosed?**

Future plans

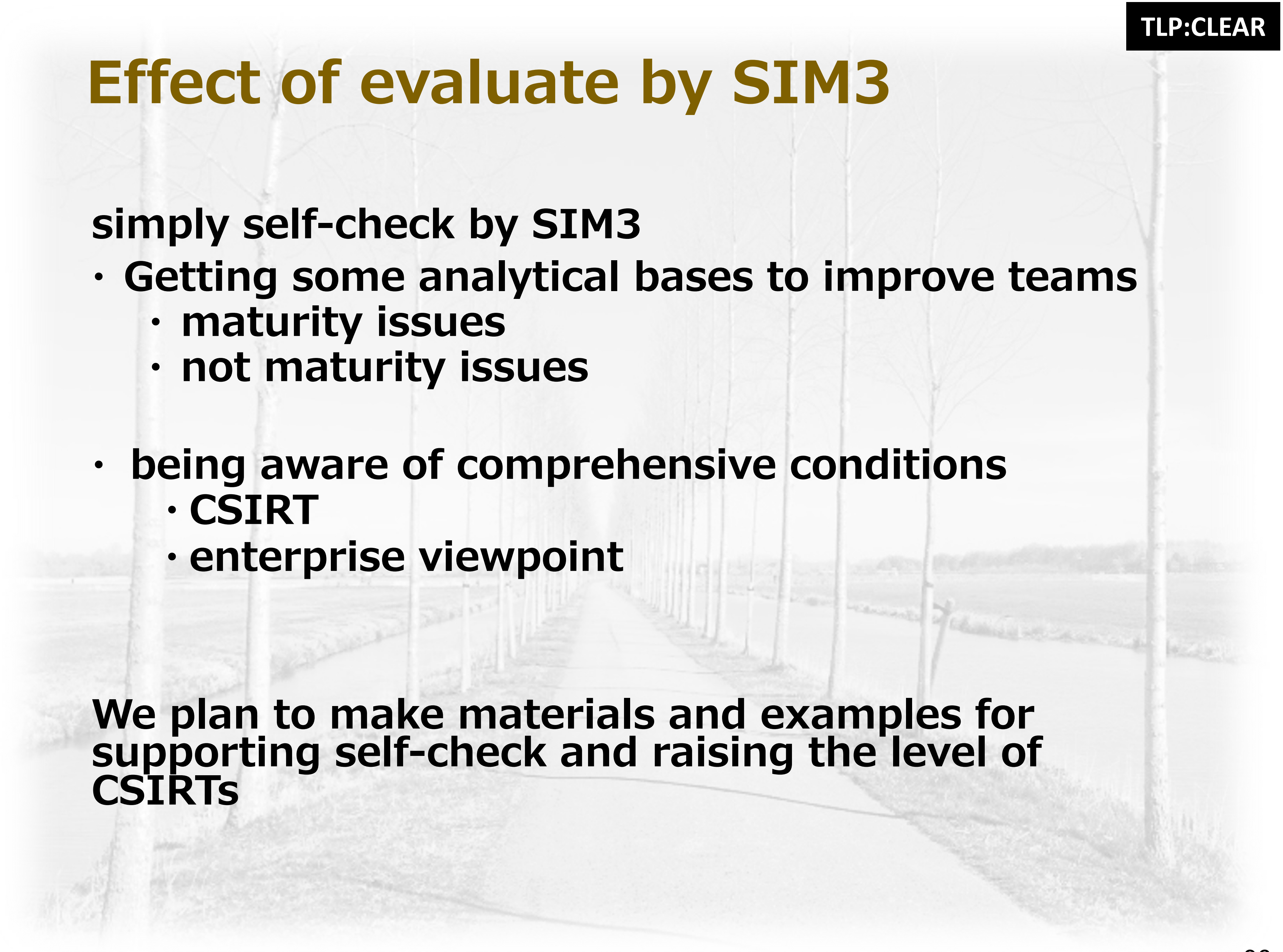
Hold Auditor training in Japan

- 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す