Establishing a CSIRT

Martijn van der Heide

Version 1.2 (November 2017)

Table of Contents

Introduction 4
Intended Audience 4
Terminology 5
Structure of this handbook 5
Legal Notice 6
Acknowledgements 6
Revision history 6
1. Team Life Cycle Management 7
1.1 Measuring and improving maturity 10
1.1.1 SIM3: Security Incident Management Maturity Model 11
1.1.2 CSIRT maturity self-assessment 11
2. Draft a CSIRT Framework 12
2.1 Mission Statement 12
2.2 Constituency 12
2.3 Authority 13
2.4 Responsibility 13
2.5 Organizational structure 14
2.5.1 Independent business model 14
2.5.2 Embedded model 14
2.5.3 Campus model 14
2.6 Availability 15
2.7 Core services 15
2.8 Staffing requirements 16
2.8.1 Capacity 16
2.8.2 Capabilities 16
2.8.3 Code of conduct/practice/ethics 17
2.8.4 Training 17
2.9 Infrastructure and tooling 17
2.10 Internal and external relationships 18
2.11 Funding model 18
3. Get approval from senior management 20
3.1 Agree on a reporting structure to keep them involved and interested 20
4. Setup the team and work environment 21
4.1 Create an information sources overview 21

4.2 Create an Incident handling policy 21
4.3 Create an Information handling and exchange policy 21
4.3.1 Laws and regulations 22
4.3.2 Secure communications with PGP 23
4.4 Assess the installed base of the constituency 23
4.5 Communicate the existence of the CSIRT 23
4.6 Build trusted network, go to conferences and seminars 24
4.7 Practice the processes 24
5. The Incident Handling process 25
5.1 Incident report 25
5.1.1 Notification 25
5.1.2 Registration 26
5.2 Triage 26
5.2.1 Incident classification 27
5.3 Incident resolving 28
5.3.1 Data analysis 28
5.3.2 Resolution research 29
5.3.3 Action proposed 29
5.3.4 Action performed 30
5.3.5 Eradication and recovery 30
5.4 Incident closing 30
5.4.1 Final information 30
5.4.2 Final classification 30
5.4.3 Incident archiving 30
5.5 Post analysis 30
6. Add services as needed 32
6.1 Service Descriptions 33
6.1.1 Reactive Services 33
6.1.2 Proactive Services 36
6.1.3 Security Quality Management Services 38
Appendix A: CSIRT Framework template 40
Appendix B: Sample Incident Reporting form 41
Appendix C: Security tools 42
Appendix D: Information resources 45

Introduction

With the ever-expanding Internet and the fact that more and more critical organizations require Internet access these days, the stability and availability becomes ever more important.
Critical Infrastructure (e.g. Financial Sector, Energy, Transport or Government) rely more and more on the possibilities of citizens to access their services through the Internet. At the same time, they themselves use the Internet more and more to provide services between each other. Primary processes of many organizations have become reliant on the availability of the Internet, too.

An outage of several hours is no longer deemed acceptable and sufficiently long outages can actually destabilize the economy. Organizations that utilize web shops face severe impact from even short outages.
Looking at media reports, even an outage of Facebook of 15 minutes becomes headline news.
Apart from outages, breaches of organizations worldwide are reported every day and customer data or intellectual property is stolen or destroyed as a form of vandalism or corporate espionage in many cases.

Incidents are expensive. There will be direct cost involved to lost revenues and profits and to contain and solve the incident, but also indirect cost by potential brand damage, lost customers, claims from customers or fines by a regulator.
There are various documented cases where security incidents led to the bankruptcy of organizations because they could not recover from them.

Whenever there is an information security incident, quick and adequate response is key. And this is where CSIRTs enter the picture.

A CSIRT is a team of IT security experts who respond to information security incidents or threats. They have the capacity and capabilities to detect and handle them and to help their constituency to recover from breaches.
Proactively, the CSIRT can offer various services to help mitigate vulnerabilities and risks, raise awareness and educate the constituents in development and improvement of secure services.

Intended Audience

This handbook is designed for organizations who wish to learn more about CSIRT teams and start one themselves.
It describes both the process to establish a team and the various requirements. Examples are given where possible, to show how each step can be completed.
The intended audience is management level, but the handbook can also directly be used by operational staff, as a reference guide.

Terminology

There are several terms associated with security teams and you will come across see them when further researching this subject on the Internet. We will try to explain the most common ones here.

- **CERT**, or Computer Emergency Response Team
  "CERT" is a worldwide registered trademark of the CERT Coordination Center (CERT/CC)[1], which falls under the Software Engineering Institute (SEI) of Carnegie Mellon University (CMU) in the USA.
  This was the first official incident response team to be set up, in response to the large scale outage caused by the Morris worm[2] in 1988.
  If a new team wishes to use the term "CERT" as part of their name, a license agreement is required.[3]
- **CSIRT**, or Computer Security Incident Response Team
  This is a generic name to describe an incident response team. Its function is identical to a CERT, but, as shown above, the term CERT is trademarked.
  In this handbook we use the term CSIRT.
- **ISAC**, or Information Sharing and Analysis Center
  A cooperation platform for security teams in the same sector or with a shared goal, which can offer many of the services a CSIRT can offer, but does not do incident handling.
- **SOC**, or Security Operating Center
  A physical area or room in a building where centralized real-time monitoring and incident dispatch and coordination takes place, similar to how ISPs (also) have NOCs (Network Operating Centers) but for security events.
  Generally, only advanced CSIRT teams or large organizations with many IT assets spread over many locations will need a dedicated SOC.

There is no hard distinction between the activities of a CSIRT and a SOC, as there is much overlap between the functions; also, a CSIRT can be located inside a SOC and some teams utilize a SOC as the first-line for their CSIRT.

Whichever term is used, and whichever name the team will be given (if any), the important thing is having the capability.

Structure of this handbook

Chapter 1 provides a structured approach to guide the Life Cycle and maturity of the team.
Chapters 2-4 describe the various steps needed to come to a plan, obtain senior management approval and start the CSIRT team.
Although it is best to have senior management involvement throughout the process, we chose to add the definitive approval at the second phase, as we find that management usually wants a clear and complete proposal before spending time on the idea.
Chapter 5 outlines the most important service of the team, Incident Handling.
Chapter 6 is about later steps: adding additional services to the CSIRT catalog.

---

[1] CERT/CC: <https://www.cert.org/>
[2] The Morris Worm: <https://en.wikipedia.org/wiki/Morris_worm>
[3] Further information and the process to apply for a license can be found on their website: <https://www.cert.org/incident-management/csirt-development/cert-authorized.cfm>

Legal Notice

This handbook has been developed with the aim to help both future and existing CSIRT teams in their setup and operation, during the startup phase as well as during their lifetime. The content is based on the collective knowledge and experience of the CSIRT community and not solely the view of ThaiCERT and ETDA. It may not necessarily represent state-of-the-art and it might be updated from time to time.

Third party sources are quoted as appropriate. ThaiCERT is not responsible for the content of the external sources, including external websites, nor their continued availability, referenced in this handbook. Where specific product names are given, those do not mean endorsement from ThaiCERT, but serve as examples only.

This handbook is intended for educational and information purposes only. Neither ThaiCERT nor any person acting on its behalf is responsible for the use that might be made of the information contained in this handbook. All information contained herein is provided on an “As Is” basis with no warranty whatsoever. ThaiCERT/ETDA does not promise any specific result, effects or outcome from the use of the information herein.

This handbook is published under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License[4].

Copyright © Electronic Transactions Development Agency (Public Organization), 2017

Acknowledgements

ThaiCERT would like to thank all institutions and individuals who contributed to this handbook.
In particular, a special Thank You goes out to:

- CERT/CC and especially the CSIRT development team, who’s Service Descriptions are integrally used in chapter 6.
- ENISA, for their insights into personnel, laws and regulations.
- The TRANSITS team for suggestions in the Incident Handling process.
- Everyone who kindly peer-reviewed this handbook.

Revision history

Version	Date	Remarks
1.0	June 2016	First publication
1.1	July 2016	Small number of changes from peer-review
1.2	November 2017	Brought up-to-date plus expanded on team maturity (new paragraph 1.1)

[4] Creative Commons License: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

1. Team Life Cycle Management

Setting up a CSIRT team has many facets and factors to consider and implement. It is highly advisable to use a project management approach and implement a Plan-Do-Check-Act (PDCA) cycle[5] for continuous improvement.

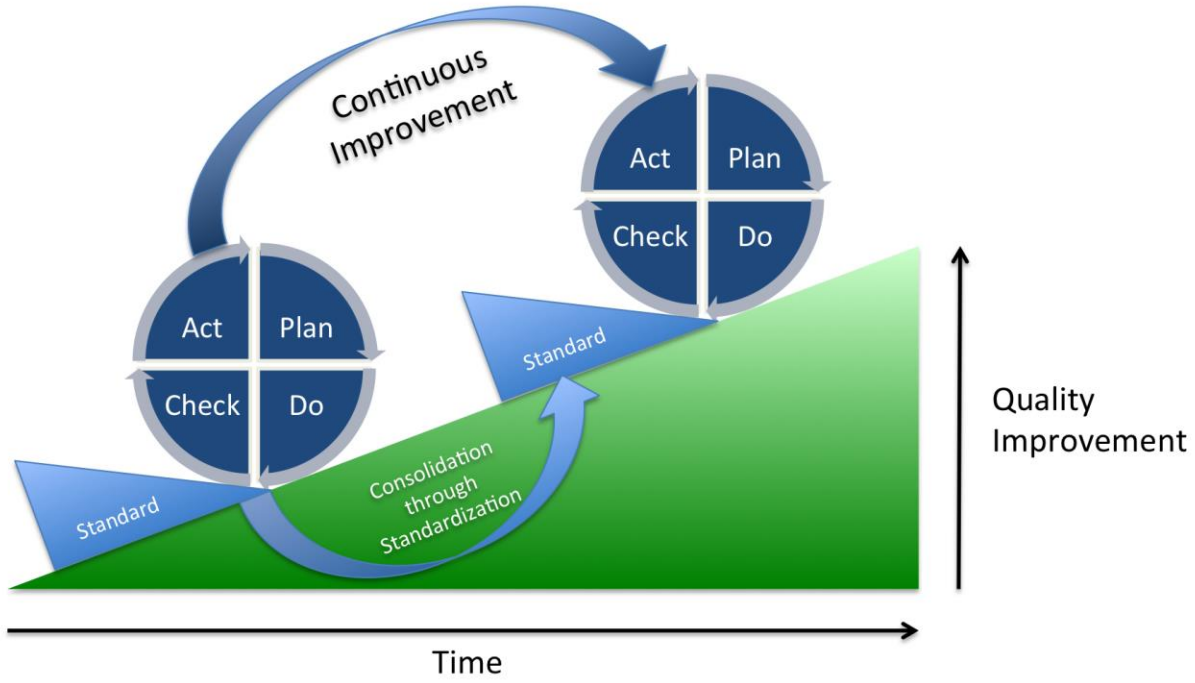

Figure 1: Depiction of the PDCA cycle (or Deming cycle). Continuous quality improvement is achieved by iterating through the cycle and consolidating achieved progress through standardization (Johannes Vietze)

The project management team should ideally include a consultancy role from an Executive Sponsor, who is familiar with the top management of the organization and the business goals and strategy, and may help gather support for the plans.

There are case studies available from existing CSIRT teams, who described their journey with the aim to help future teams with their establishment, such as:

- AusCERT[6]
- A financial institution[7]
- CERT Polska[8]

As a further reference, KPN (Royal Dutch Telecom) publish their complete Security Policy Framework online[9], which can be used as a starting point as well.

[5] PDCA Cycle: <https://en.wikipedia.org/wiki/PDCA>
[6] AusCERT: <https://www.auscert.org.au/render.html?it=2252>
[7] Financial Institution: <http://www.cert.org/incident-management/publications/case-studies/afi-case-study.cfm>
[8] CERT Polska: <https://www.terena.org/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf>
[9] KPN Security Policy Framework: <https://github.com/KPN-CISO/kpn-security-policy>

PLAN

Create the CSIRT Framework

- This will be described in chapter 2, as well as Appendix A: CSIRT Framework template.

Create a budget

- Lay out a multi-year budget, differentiating between operational costs and investment costs.
- Don't overcommit and don't pad your budget.
- Be as succinct as possible and upfront about all tangibles and intangibles.

Create a business plan

- Examine examples and coaching sites for business plans.
- Your Executive Sponsor should be able to assist you.
- The business plan should reflect the CSIRT's goals for the organization and how these goals work in conjunction with the budget.
- Speak about Return on Investment (ROI).

Present your budget and plan

- As outlined in chapter 3.
- Conduct research so that you are able to defend your budget and the necessity of every item.
- Present the plan first to your Executive Sponsor to receive feedback from a supportive source.
- Then present it to others who have to approve your plans and your funding.

DO

Implement the plan

- As described in chapter 4.
    - Create an information sources overview.
    - Create an Incident handling policy.
    - Create an Information handling and exchange policy.
    - Assess the installed base of the constituency.
    - Communicate the existence of the CSIRT.
    - Build trusted network, go to conferences and seminars.
    - Practice the processes.
- Perform the day-to-day operations for Incident Handling (chapter 5) and other core services (chapter 6).

CHECK

Analyze the team's performance

- Focus on important workflows, processes and tasks
  - Frequently performed.
  - Inconsistent execution.
  - Under your control to improve.
- Use appropriate measurements and metrics
  - Remember "you get what you measure".
  - Metrics must result in appropriate incentives.
- Involve team members
  - Inclusion and involvement leads to shared commitment.
  - Share what they do well and where they could improve.
  - Work with Quality Assurance department if available.
  - Consider using an external consultant and facilitator.
- Interview your constituency
  - What the CSIRT does well.
  - The key improvement areas.
- General quality management
  - Does the team work according to the processes and standards?
  - Is everything documented?
  - Does everyone know where the documentation can be found?
  - Are minutes created of all meetings and available for later reference?
  - How does everyone work together and keep each other updated about ongoing incidents?
  - Who attended which trainings, conferences and seminars?

ACT

Decide on additions and improvements

- As an outcome from the CHECK phase, improvements to the operations can be made.
- As the team matures, additional services may be desired, as described in chapter 6.
- Start a new PLAN phase to implement them and go back another circle for continuous improvement.

After the team has been established, it is common that the PDCA cycle is performed annually, coinciding with the fiscal year of (if available) the parent organization, to ensure that the CSIRT requirements are included in all budget negotiations.

1.1 Measuring and improving maturity

One way to look at the selection of services is as the maturity level of the CSIRT, ranging from strictly reactive to the implementation of proactive services and quality management. This schema was devised sby ThaiCERT.

In this handbook, the minimal CSIRT we describe is a level 2 (Basic) organization.

Maturity Level	Description
1. Introduction	The CSIRT exists as a Point of Contact (POC) for incident coordination and resolution. It also has rules and regulations for notifications to the relevant authorities.
2. Basic	As 1, plus a process is implemented to handle new threats. A ticketing system is used to handle all reported incidents and advisories are provided to the organization.
3. Active	As 2, plus threat analysis tools are implemented and procedures exist for information classification and handling.
4. Proactive	As 3, plus security information dissemination is done, tools are implemented to regularly check and maintain the security status and ongoing training of the team members is planned.
5. Comprehensive	As 4, but real-time monitoring of incidents and threats. Guidelines for new threats and incident prevention are drafted and shared both inside and outside the organization for awareness building.

CSIRT maturity initiatives refer to five pillars of CSIRT maturity:

- **Foundation**
  Business plan, understanding of legal constraints
- **Organization**
  Mandate and other internal organizational structures within the parent organization, and coordination with other CSIRTs
- **Human**
  Team's staffing, structure, expertise, code of conduct, and training options
- **Tools**
  Everything needed to perform the given tasks
- **Processes**
  For threat and incident handling or interaction with the media

Trusted Introducer developed a standard for CSIRT maturity in 3 levels[10]:

1. Listed
2. Accredited
3. Certified

The Certification process is based on SIM3 as explained in the next paragraph.

ThaiCERT was the first team outside Europe to be TI Accredited in 2015.

1.1.1 SIM3: Security Incident Management Maturity Model

This Model was developed in support of measuring the maturity of a security or incident response team in terms of four areas: organization, human issues, tools and processes. It is used in support of the Trusted Introducer Certification framework and is also being adopted by various membership organizations such as FIRST and the Nippon CSIRT Association (NCA).

The SIM3 maturity model[11] 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 – Organization (11)
- H – Human (7)
- T – Tools (10)
- P – Processes (17)

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

What is really measured 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 formalized in any way)
3 = explicit formalized (rubberstamped or published)
4 = subject to control process / audited / enforced

1.1.2 CSIRT maturity self-assessment

Online self-assessments, based on or similar to SIM3, are available from:

- GCCS and NCSC-NL[12].
- ENISA[13].

---

[10] Trusted Introducer process: <https://www.trusted-introducer.org/processes/overview.html>
[11] SIM3 model: <https://www.trusted-introducer.org/SIM3-Reference-Model.pdf>
[12] CSIRT Maturity Quick Scan: <https://check.ncsc.nl/>
[13] CSIRT Maturity - Self-assessment Survey: <https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey>

2. Draft a CSIRT Framework

The CSIRT Framework describes in detail what the CSIRT is going to do, for whom, and which resources will be required to deliver these services.
Although each CSIRT will be different, all the various elements will apply for each team. A template for all these elements is given in Appendix A: CSIRT Framework template.

We follow the internationally agreed Best Practice, to make it easier to later become a member of international cooperation initiatives; their membership applications generally need the same elements to be filled in, so having them available already will make that process much easier.

Due to its complete scope, the Framework can also be used to announce the CSIRT to the constituency and the outside world (also see 4.5)

Where feasible, we add the situation for ThaiCERT as an example at each element.

2.1 Mission Statement

The team's mission should be documented. It explains the purpose and function of the CSIRT in a clear manner and should list a brief overview of the core goals and objectives of the team.
It is good practice to make the mission statement compact (2-3 sentences) but not too short, to avoid ambiguity, as it will generally stay the same for a couple of years.
The mission describes the future ultimate goal of the team.

> ThaiCERT is the National CERT of Thailand, established to accomplish the mission to make cyberspace and electronic transactions more secure by being the official point of contact for computer security incidents in Thailand's Internet community.

2.2 Constituency

The constituency is the recipient of the CSIRT services.
Understanding a CSIRT's constituency will help the team determine what needs they have, what assets need to be protected, and what the interactions with the CSIRT will be.
Each team must have a clearly defined constituency. If there is overlap with any other team that must be made known and the constituency must be clear when to engage which team.
Verification of the constituency can be found in any charters, mission statements, concept of operations documents, or similar documents that describe the CSIRT's purpose and function.
ENISA[14] distinguishes the following 'sectors' of CSIRTs:

Sector	Focus	Typical constituents
Academic Sector CSIRT	Academic and educational institutions, such as universities or research facilities, and the campus Internet environments.	University staff and students.
Commercial CSIRT	Commercial services. This can be an independent organization, an ISP or managed services provider.	Paying customers.

[14] From ENISA "A step-by-step approach on how to set up a CSIRT", page 8

CIP/CIIP Sector CSIRT	Critical Information Protection and/or Critical Information and Infrastructure Protection. This covers the IT of all critical sectors in a country.	Government, critical sectors and citizens.
Governmental Sector CSIRT	The government itself.	Government agencies.
Internal CSIRT	The hosting organization itself.	Internal staff and IT department.
Military Sector CSIRT	Military organizations with responsibilities in IT infrastructure.	Staff of military institutions and closely related entities such as the Ministry.
National CSIRT	National focus, considered as the central security point of contact.	No direct constituents, although a National CERT is sometimes combined with a Governmental CERT.
Small & Medium Enterprises (SME) Sector CSIRT	This is a self-organized CSIRT to provide services to its own business branch or similar user group.	The SMEs and their staff.
Vendor CSIRT/PSIRT	Vendor-specific products, usually to address vulnerabilities or advise on specific attack mitigations. A common acronym is PSIRT, or Product Security Incident Response Team.	Product owners.

ThaiCERT is the National CERT of Thailand, as well as a Governmental CSIRT; therefore the constituency is composed of all people, networks and organizations within Thailand.

2.3 Authority

The team's authority describes what a team is allowed to do. This can range from only having an advisory role to a full mandate to disable vulnerable or compromised services.
In general, it is advised that a CSIRT is only responsible for technical aspects and never for repression or punishment, as constituents may stop reporting incidents out of fear.

ThaiCERT coordinates security incidents related to its constituency, and has no further mandate.

2.4 Responsibility

What the CSIRT is expected to do towards their constituency in order to accomplish their role.
Generally, this includes the typical services from the CSIRT service catalog (as described in chapter 6), but the CSIRT may have additional functions such as specific relations and responsibilities with regulators or Law Enforcement.
When such functions are to be added, great care must be taken that no conflict of interest occurs, such as when the CSIRT is given operational tasks where it also has the role to supervise those same tasks.
For National CSIRTs and Governmental CSIRTs, this responsibility should generally appear in a law.

ThaiCERT handles every type of information security incident. In addition, ThaiCERT provides technical and operational recommendations and advisories, awareness raising, training and consultancy.

2.5 Organizational structure

This element is sometimes also called Sponsorship or Affiliation.
The organizational home of the CSIRT indicates the team's position within the parent organization or constituency.
Many national teams are located in government organizations, while others may be associated with a commercial enterprise, research network or university.

2.5.1 Independent business model

In this model, the CSIRT is an independent organization itself, with its own management, employees and support staff. This model may be applicable for commercial CSIRTs.

2.5.2 Embedded model

For Internal CSIRTs, it is common to place it in an existing IT department. This makes sense, as much of what a CSIRT does is directly related to IT systems. For larger organizations this may not be the optimal place; a CSIRTs aims to protect all (information) assets of the company, not only IT.
If the CSIRT is placed "too low" in the organization chart, it may effectively sit isolated as an "IT toy" and lack the support of the rest of the organization. Likewise, if it is placed "high", employees of the organization may see the CSIRT as an ivory tower and ignore it altogether.
We see a slow shift and CSIRT teams are beginning to be placed higher, to better serve the whole organization.
The organizational home of a CSIRT should appear in an organization chart or diagram, or in any announcement from management.
Wherever the CSIRT is located in the hierarchy, it is crucial to stay in close contact with the departments.

There are several possible models to physically organize the CSIRT, depending on the structure of the organization:

- Centralized: all CSIRT team members are located in the same office.
- Distributed: CSIRT team members are spread over more than 1 location, for example if there are multiple operational facilities. This requires some coordination to work together on a day-to-day basis.
- Time zone distributed: for multi-nationals. This is an advanced version of the distributed model, sometimes called the 'Follow the sun' model. In this model, the operational office of the CSIRT switches around the globe depending on the daylight. For each operational office, the working hours can be the regular office hours, after which an office in another country takes over.

2.5.3 Campus model

As the name suggests, this model is adopted mostly for academic and research CSIRTs, but it can also apply for Military Sector CSIRTs and Small & Medium Enterprises (SME) Sector CSIRT.
In this case, the participating members (universities or enterprises) may or may not have their own CSIRTs, depending on their size and budgets, and a dedicated 'mother' or core CSIRT is set up to coordinate the efforts for the sector and act as the point of contact for the outside world.
This core CSIRT itself can be either an independent organization or embedded.

For members without their own dedicated CSIRT, the core CSIRT can provide all CSIRT services for them.

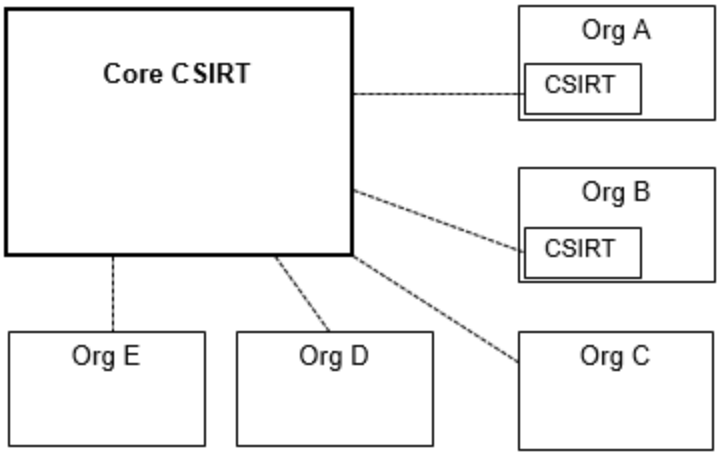

Figure 2: Campus model organization structure

ThaiCERT is part of the Thai government and operates from an office of one of the agencies.
As such, ThaiCERT is a centralized, embedded team.

2.6 Availability

The availability of the CSIRT services will largely depend on the working hours of the parent organization. Unless the CSIRT is available 7x24, provisions need to be made for the reporting of incidents outside of office hours. This could simply be that all incoming e-mail will be picked up on the next working day, another way is to have a team member on-call to monitor incoming reports and decide whether it can wait for the next working day or immediate action is required.

It is important to consider the organization's environment when determining the availability of the CSIRT services. For example, if the IT department is only available during office hours, it may not be beneficial to operate the CSIRT services 7x24, as problems cannot be fixed outside office hours.

Note that having team members work outside office hours may bring extra cost in the form of extra allowances.

ThaiCERT was available only during office hours until early 2015, with an emergency number outside office hours, and is now available 7x24.

2.7 Core services

There are many services a CSIRT can offer, but there is no need to offer more than 1 or 2 when starting the team; additional services can always be added later, as needed. We will cover this in chapter 6.
To be called a CSIRT team, Incident Response is a fundamental required service which will be covered in chapter 5.
A second service is usually Announcements.

ThaiCERT offers most of the services covered in chapter 6.

2.8 Staffing requirements

2.8.1 Capacity

There are no hard figures available on the amount of technical staff needed to populate a CSIRT team, as each CSIRT team is different, works in a different environment and has a differently sized constituency. However, from the collective experience from the CSIRT community, the following values have proven to be a good approach:

- In order to deliver 2 core services, Incident Response and Announcements: a minimum of **4** FTE.
- For a full service CSIRT that operates only during office hours and maintains its own systems: a minimum of **6 to 8** FTE.
- For a fully staffed 7x24 operation (3 shifts per day), the minimum is **12** FTE.

These numbers include redundancies for sickness and holidays.

ThaiCERT's staff consists of 30 team members

2.8.2 Capabilities

The following is a brief overview of key competencies for the technical experts for a CSIRT, as suggested by ENISA[15]. Certifications and diplomas to prove such competencies may be needed.
Depending on the services being delivered, additional specialist skills will be required.
General technical staff job description items:

Personal competences

- Flexible, creative and a good team spirit
- Strong analytical skills
- Ability to explain difficult technical matters in easy wording
- A good feeling for confidentiality and working in a procedural matter
- Good organizational skills
- Stress durable
- Strong communicative and writing skills
- Open minded and willing to learn

Technical competences

- Broad knowledge of internet technology and protocols
- Knowledge of Linux and Unix systems (depending on the equipment of the constituency)
- Knowledge of Windows systems (depending on the equipment of the constituency)
- Knowledge of network infrastructure equipment (Router, switches, DNS, Proxy, Mail, etc.)
- Knowledge of Internet applications (SMTP, HTTP(s), FTP, telnet, SSH, etc.)
- Knowledge of Security threats (DDoS, Phishing, Defacing, sniffing, etc.)
- Knowledge of risk assessment and practical implementations

Additional competencies

- Willing to work 24x7 or on-call duty (depending on the service model)
- Maximum of travelling distance (in case of emergency availability in the office; maximum travelling time)
- Level of education
- Experience in working in the field of IT security

[15] From ENISA "A step-by-step approach on how to set up a CSIRT", page 25

2.8.3 Code of conduct/practice/ethics

A code of conduct/practice/ethics is a set of rules or guidelines for the CSIRT members on how to behave professionally, potentially also outside work. Behavior outside work is relevant, because it can be expected of CSIRT members that they behave responsibly in private as well where computers and security are concerned.
A good example is the CSIRT Code of Practice from Trusted Introducer.[16]

Make sure the staff is trustworthy and avoid hiring (ex)-crackers. After all, it will take your CSIRT at least a year to build trust and it can lose it overnight. Screening of employees is good practice.

ThaiCERT uses the CSIRT Code of Practice from Trusted Introducer.

2.8.4 Training

A staff training plan includes two phases or training: internal training for new staff members to learn how the CSIRT operates, as well as external training for continuous improvement of skills and to keep up with the developments in technology (including new threats and attack methods).

High quality external training for CSIRT staff can for example be found at

- TRANSITS[17]
- CERT/CC[18]
- SANS Institute[19]
- FIRST[20]

If possible, make sure there is also budget reserved to attend conferences and seminars as part of ongoing training (also see 4.6).

ThaiCERT uses all of the above.

2.9 Infrastructure and tooling

CSIRT facilities and network and telecommunications infrastructure must be designed with great care to not only protect the sensitive data collected by the CSIRT but also to protect the CSIRT staff. Information and staff areas should be built and protected in the same manner and meeting the same requirements as a data center.

Physical security considerations

- Secured rooms or security operations center (SOC) for the location of any CSIRT servers and data repositories.
- Secured and sound-proof rooms for discussion of CSIRT activities and investigations.
- Safe for storage of non-electronic data and notes.
- Shredder and facility to thoroughly destroy media (e.g. EMP) that are no longer needed.
- Physical separation of CSIRT staff from other parts of the organization, including some sort of access controls.

[16] Trusted Introducer CSIRT Code of Practice: <https://www.trusted-introducer.org/CCoPv21.pdf>
[17] TRANSITS: <https://www.terena.org/activities/transits/>
[18] CERT/CC: <http://cert.org/training/>
[19] SANS Institute: <https://www.sans.org/>
[20] FIRST: <https://www.first.org/>

- Policy on accommodating visitors if not included in the policy on general access controls.

IT equipment considerations

- Secured communications mechanisms such as secure phones, faxes, and e-mail.
- Hardened systems, including the work computers.
- Own CSIRT network, separated from the office network.
- Facility to quickly reinstall systems that have been outside the secure area or used for malware analysis.

CSIRT specific tooling considerations

- Ticketing system.
- Contact database of team members, constituents and other POCs.
- Any other material required to deliver the core services of the team.
- Appendix C: Security tools shows a selection of commonly used tools.

Some CSIRT services, such as digital forensics, may add specific physical and IT requirements.

ThaiCERT has all of the above.

2.10 Internal and external relationships

In order to get support and recognition from your organization, it is important to build a good working relationship. When incidents occur, you will need each other to resolve the problem or consult about possible actions, and knowing each other already will make this process much faster and smoother. Relationships with operational (IT, network) departments are helpful, but also with e.g. the physical security department, communications department, legal counsel and HR.

Local external relationships that can benefit the team are your National CSIRT and potentially Law Enforcement or a Regulator. If there is a Sector-based CSIRT or ISAC available for your sector[21], you should consider joining it.

Also see 4.6 for some examples of international collaboration initiatives that could benefit the team.

ThaiCERT has all of these relationships.

2.11 Funding model

To ensure long-term stability, the CSIRT requires a funding model to be in place which provides incoming funds to ensure continued operation of the team and continued provision of CSIRT services to the constituency.
Funding should cover initial investments to start the team (CAPEX) as well as recurring operational costs (OPEX) for personnel, facilities and software licenses, as well as the costs required for the delivery and maintenance of the individual services.

[21] See ThaiCERT's "Establishing a Sector-based ISAC"

The funding model can be:

- A cost center within an organization (where the host or parent covers all expenses and does not receive any revenue from it), or
- The team can be funded in whole or in part by grants, if so:
    - Who will give grants?
    - What is the purpose of the grant?
    - How much will the grants be for and how much of the operations will they cover?
    - How secure is the funding source?
    - How long is the grant in place?

  The team should detail the grant include issuer and source, purpose, amount and duration of the grant.
- The team may sell its service either internally or externally (there could be a charge-back or fee to internal or external customers), or
- Funded through a consortium of organizations such as universities in a research network.

or a combination of any of those listed above.

ThaiCERT is fully funded by the government and also provides various specialized services for a fee.

3. Get approval from senior management

Support for the CSIRT should come from the highest management level of the organization (preferably the Board of Directors for a commercial enterprise, or the Ministry or Cabinet for a governmental CSIRT). This is important for several reasons:

- To ensure that any organization-wide policies are implemented and enforced throughout the organization.
- To ensure support in case critical or costly actions need to be taken.
- To secure continued operation during reorganizations and budget cuts.

When discussing the plans for the setup of a CSIRT, keep in mind that managers look differently at IT and speak a different language than technical people. To convince senior management that a CSIRT could help them establish their business goals requires business rather than technical arguments.

Arguments could include

- Legal or contractual requirements that demand a certain level of information security being in place.
- Having a trained and equipped CSIRT can help reduce the damage (both in terms of downtime cost and in terms of brand damage) of incidents as the organization can contain and recover more quickly, so the CSIRT can save money.
- Preventative services can reduce vulnerabilities and threats before they are exploited.
- Centralizing information security into a CSIRT will save each department having to duplicate the same security efforts and can improve the security baseline for the organization as a whole.
- Depending on the sector, having a CSIRT could be a Unique Selling Point.
- From a PR standpoint, having a CSIRT shows commitment to security (‘Your data is safe with us’).
- “Our competitors do it too.”

3.1 Agree on a reporting structure to keep them involved and interested

Usually the same reporting structure as for any other department of the parent organization is sufficient, such as regular meetings as well as quarterly and annual reports.
However, it is important to keep in mind that a CSIRT is usually a cost center while it can save the parent organization money. If possible, therefore, add cost saving figures in the reports to show how the team contributes to the financial result.

> For government transparency, ThaiCERT publishes monthly incident statistics on the website and also publishes detailed annual reports in electronic and paper form.

4. Setup the team and work environment

4.1 Create an information sources overview

Create and maintain a list of all sources to be used

- To automatically detect potential incidents.
- To be alerted of incidents by others (e.g. e-mail, telephone, web form).
- To obtain threat and vulnerability information from.
- To communicate directly with constituents during an incident (POC list).
- For general communication with the constituency (awareness and PR).

4.2 Create an Incident handling policy

The incident handling policy should define who has responsibility for handling what type of computer security incidents and who can be called in to assist in the response implementation from other areas. This includes:

- The types of incidents that fall within the jurisdiction or expertise of the CSIRT
- Who handles the analysis and response
- What work, if any, should be done with law enforcement
- What to do with reports and activity outside the scope of the CSIRT

The policy should outline the basic process to follow in handling an incident. It should include:

- Time-frames for response
- Methods for escalation
- How incidents are classified and prioritized
- How incidents are tracked and recorded
- When and how incidents are closed
- How additional assistance is procured for analysis or for implementing suggested mitigation and recovery strategies.

A complete overview of an incident response process will be covered in chapter 5.

4.3 Create an Information handling and exchange policy

Information classification describes the CSIRT categorizations or classifications of information including distinctions between sensitive, confidential, or public information and how each is handled for storage, transit, access, etc.
These classifications should apply to information in any form; electronic or hard-copy.
A commonly used classification system is the Traffic Light Protocol.[22]

The policy should include what type of information must stay within the CSIRT facility and how information should be handled on laptops and other mobile devices. It should also detail what type of information can and cannot be discussed on mobile or non-secure devices along with what information must be transmitted and discussed and stored in a secure fashion and should not be shared or discussed with non-authorized persons.
The policy should also state the manner in which information received from other CSIRTs should be handled, protected, and shared within the CSIRT and its parent/host organization.

[22] Traffic Light Protocol: <https://www.us-cert.gov/tlp>

4.3.1 Laws and regulations

Like any organization, the CSIRT is bound by national laws and international agreements. Standards are not necessarily binding directly, but can be mandated or recommended by laws and regulations. Similarly, contracts with customers (for the commercial sector) may mandate the implementation of specific standards.

Below is a short list of possible laws and policies[23]:

National

- Various laws on information technology, telecommunication, media
- Laws on data protection and privacy
- Laws and regulations on data retention
- Legislation on finance, accounting, and corporate management
- Codes of conduct for corporate governance and IT governance
- For Thailand: Computer Crimes Act and Electronic Transactions Act (article 35)[24]

International

- Basel II agreement (especially with regard to management of operational risk)
- Council of Europe‘s Convention on Cybercrime
- Council of Europe‘s Convention on Human Rights (article 8 on privacy)
- International Accounting Standards (IAS; they mandate to some extent IT controls)

Standards

- British Standard BS 7799 (Information Security)
- International Standards ISO2700x (Information Security Management Systems)
- German IT-Grundschutzbuch, French EBIOS and other national variations

Be aware that legal aspects do not only apply for information that is being handled locally, but also for any exchange of information with foreign parties.
Also note that laws and regulations may limit the type of actions that are permissible during incident response (e.g. traffic sniffing to analyze an attack may not be allowed for privacy reasons).

Some countries have laws that require notification to the relevant Regulator in case a data breach occurs. Once the CSIRT is operational, this notification function might be added to their process (as part of their responsibility, see also 2.4).

On a final note, the Internet is a very quickly developing environment and laws are generally behind on technology. As a result, there currently are no laws for various areas, not all laws have been tested in court yet and some laws could conflict with other laws.

To determine if your CSIRT is acting in compliance with national and international legislation, please consult your legal counsel and verify that your organization supports what you plan to do.

---

[23] From ENISA “A step-by-step approach on how to set up a CSIRT”, page 28
[24] For implementation guidelines of the Electronic Transactions Act, see “Information Technology Law” from ETDA’s ICT Law Center

4.3.2 Secure communications with PGP

Since PGP or GPG is recommended for secure communications in the CSIRT community (and required for most memberships), how PGP is used in the team environment should be described.
Although it is only a recommendation, it becomes mandatory if you want to join organizations such as FIRST or Trusted Introducer.

General key policy considerations:

- Who should have keys (management, responders, etc.)
- How keys will be created, managed, distributed and archived.
- Key management issues such as
    - Who will create the keys
    - What type of key should be created
    - What size key should be created
    - When will keys expire
    - If a revocation key ('designated revoker') is required
    - Where keys and revocations will be stored
    - Who needs to sign a key
    - Any password policies including password escrow
    - Who manages the keys and corresponding policies and procedures for key management.

4.4 Assess the installed base of the constituency

Create and maintain an overview of the software and hardware products (and versions) commonly used in the constituency, to be able to give targeted advice.

Alternatively, if an Announcement service is provided by the CSIRT, the Constituency could be asked to subscribe to advisories for the products they use from a list of all possible products (so they effectively maintain their own product overview).

4.5 Communicate the existence of the CSIRT

Once established, it is important to regularly inform the constituency that the team exists, how to interact with the team and what can be expected.
Particularly if a CSIRT intends to serve as a single point of contact for its constituency for security incident reports, it must ensure that all concerned know to report incidents directly to the CSIRT. Similarly, other parties who may need support from a constituent (for example during an incident) should be aware of the CSIRT and what interactions they might expect.

A common way to advertise this is by publishing a document to describe the CSIRT and its services on the intranet (for internal teams) or internet, for example using the RFC2350 template[25]

Regardless of the CSIRT's (authority) relationship with its constituency, it must do more than simply define and publicize the constituency that it claims to serve. It cannot operate effectively without gaining and maintaining the constituency's trust and respect.
This trust must be earned and nurtured. As the team gains the trust and respect of its declared constituency, more of the declared constituency will begin to recognize and support the team.

[25] RFC2350: <https://www.ietf.org/rfc/rfc2350.txt>

Regular newsletters about incidents handled can be published, or, on a more ad-hoc basis, topics to raise awareness or to share lessons-learned from particularly interesting threats or incidents.

4.6 Build trusted network, go to conferences and seminars

Keep in mind that every organization faces many of the same threats and learned from incidents. By sharing experiences and lessons-learned, we all have the benefit of Best Practices to improve security and mitigate threats and incidents.

These days, incidents rarely involve only 1 organization. In many cases the attacker is located elsewhere, often in a different country. Worse, one attack may involve many sources at once (DDoS attacks).
To solve such incidents, the team will need to work together with other teams, typically the team(s) where the attack originates from.

There are several organizations where CSIRT teams collaborate and help each other with training, knowledge and incident resolution. Examples are FIRST (Forum of Incident Response and Security Teams)[26] where several hundred CSIRT teams worldwide are members, APCERT (Asia Pacific CERT)[27] for National CSIRTs in the Asia Pacific region, Trusted Introducer[28] for all CSIRT teams in Europe or AfricaCERT[29] for CSIRT teams in Africa.
Becoming a member of such organizations is very beneficial.
Those organizations, as well as a number of the larger individual CSIRT teams, regularly organize conferences and seminars that can be attended as training and as an opportunity to network with fellow CSIRT teams and build relationships.

4.7 Practice the processes

Since larger incidents should hopefully not happen often, the team may not have enough experience with the process and procedures involved. Also, the procedures may not actually work well or do not cover all aspects. This can cause unnecessary delays when such an incident occurs.
One of the practical ways to train and improve procedures is by table-top exercise, simulating an incident and resolving it through a role-playing game.
ENISA provides a large number of process training options on-line, free of charge.[30]

[26] FIRST: <http://www.first.org/>
[27] APCERT: <http://www.apcert.org/>
[28] Trusted Introducer: <https://www.trusted-introducer.org/>
[29] AfricaCERT: <http://www.africacert.org/>
[30] ENISA on-line training material: <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material>

5. The Incident Handling process

The description in this chapter is the complete process and workflow for a basic incident handling service. Each of the steps in the workflow will be explained in the following paragraphs.
A selection of tools will be given in Appendix C: Security tools

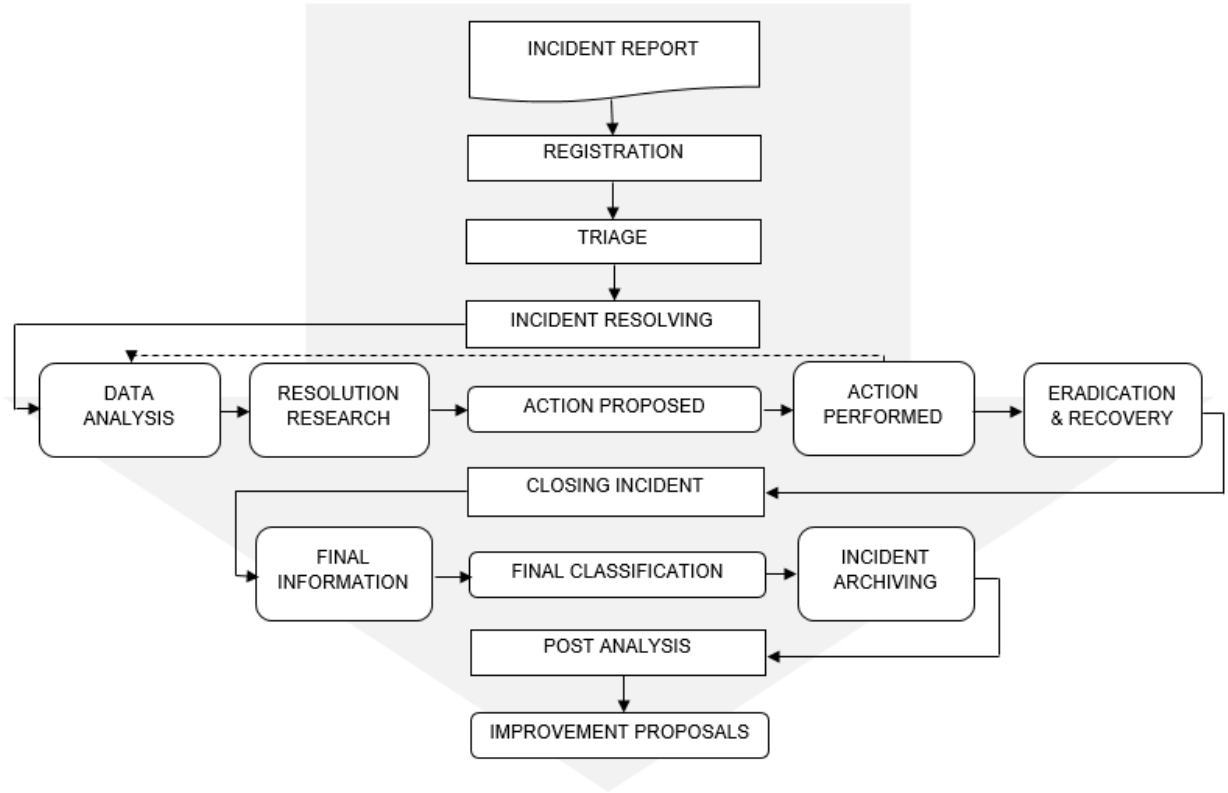

Figure 3: The Incident Handling process workflow

5.1 Incident report

5.1.1 Notification

Incident reports can come from various sources, either by own observations (monitoring) or by notifications from other sources.
Appendix B: Sample Incident Reporting form contains a template with all information items you may ideally want to receive in a notification.

For direct contact, a CSIRT team can have published facilities such as

- E-mail
- Telephone
- Website contact form
- Social media

Be careful not to create a single point of failure when setting up the facilities. Almost all of the options above require Internet access (and if VoIP is used for telephone services, all of them), so a single Internet outage may render the team inaccessible. Think about a backup facility.

Other sources can include

- Events reported by own network monitoring
- Mailing-list memberships from vendors or security groups
- Subscriptions to automatic feeds, refer to Appendix D: Information resources
- Radio, television and newspaper

5.1.2 Registration

All notifications should be registered in a ticket. This ticket will be used throughout the incident handling process.
Each ticket should be assigned a unique ticket number, which is the reference number used for all communication related to this incident.

Many ticketing systems can be configured to automatically read an e-mail account. All e-mail sent to that account will automatically create a new ticket (for new incidents), or add the communication to an existing ticket (if the ticket number is included in the e-mail subject).

It is important to manage all incidents from one place (the CSIRT), even if the actual incident resolution takes place elsewhere. This is necessary because further notifications could be related to existing tickets, for example a virus outbreak could result in incidents in various departments, while they are really all the same incident.
Central registration will also allow to reuse known communications and mitigations.

Commonly used (free) ticketing systems by CSIRTs are RTIR (Request Tracker for Incident Response)[31] and OTRS (Open Technology Real Services)[32].

ThaiCERT uses RTIR as ticketing system.

5.2 Triage

This is one of the most important steps in the incident handling process, as this is the point where critical decisions are made.
First, verification is needed; is this really an incident? How trustworthy is the source where the report came from?

Once it has been established that an incident is indeed happening:

- Is this incident in scope for the CSIRT? Does it pertain to the constituency and is the CSIRT responsible for this type of incident?
- What is the impact?
- Is there possible collateral damage?
- How urgent is it? Can damage increase over time? Can it spread to other constituents?

Respond to the notifier

- Acknowledge reception of the report
- Explain how it will be processed and what can be expected
- Suggest what to do in the meantime, until the incident is resolved

[31] RTIR: <https://bestpractical.com/>
[32] OTRS: <https://www.otrs.com/>

Response templates can be very useful and save time.

5.2.1 Incident classification

Classify the incident. There may not be enough information available at this point to classify with confidence, but this can easily be corrected later.
Classification may help determine severity and priority and required resources to handle the incident further.

Severity and priority example, as used by some governments and large enterprises:

Group	Severity	Examples
Red	Very High	DDoS, phishing website
Amber	High	Trojan, unauthorized access
Yellow	Normal	Spam, copyright issue

Priority	Government	SLA customer	Other
Red	1	1	2
Amber	2	1	3
Yellow	3	2	3

It also provides a very useful statistical function, allowing the CSIRT to

- recognize trends in incident types
- provide statistics/graphs to management
- compare with other CSIRT teams

Commonly used taxonomies (classifications)[33] are:

- Common Language for Incident Response (by CERT/CC)
- eCSIRT.net taxonomy (developed during the eCSIRT.net project)
- Self-defined by the team
  While defining one's own taxonomy may fit better with the organization, comparing with other teams may become difficult.
  Also make sure not to create a too complex taxonomy (e.g. a different incident type for each kind of malware); although this may create a very detailed overview of the types of incidents handled, it also means much time will be spent determining the correct type rather than solving the incident at hand.

ThaiCERT uses the eCSIRT.net taxonomy and publishes monthly incident statistics on the website[34].
An example graph of the incidents handled in 2015:

[33] Full descriptions of these taxonomies can be found at <https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies>
[34] ThaiCERT monthly statistics: <https://www.thaicert.or.th/statistics/statistics-en.html>

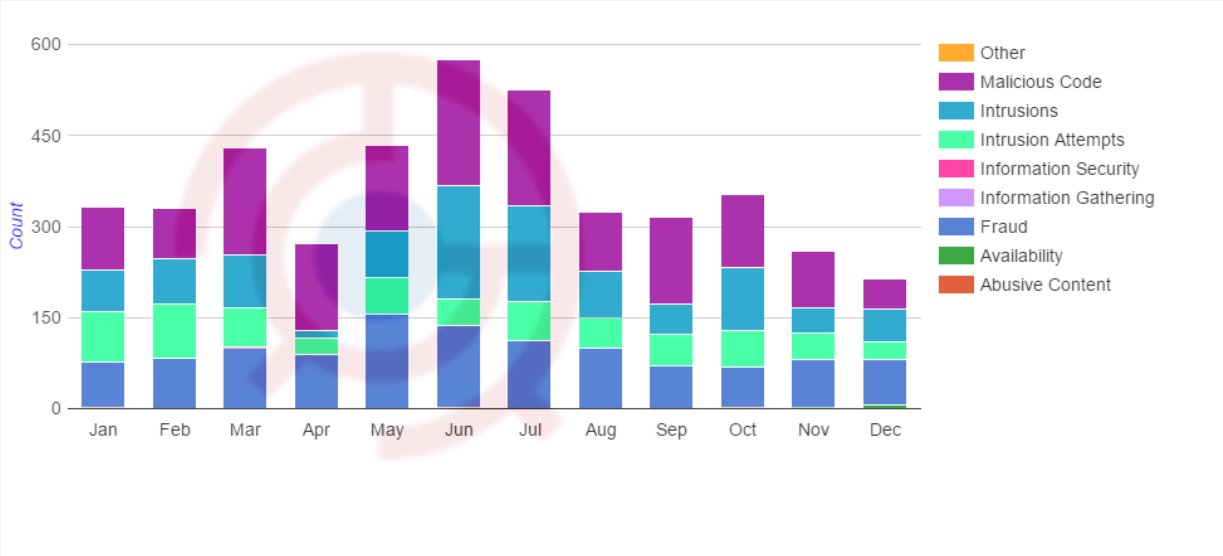

Figure 4: ThaiCERT monthly incident statistics

The final step of triage is to assign one or more incident handlers to this incident, who will perform all further actions.

5.3 Incident resolving

5.3.1 Data analysis

In this step, we will try to find as much information as possible to get a complete overview of the incident and its cause.

Gather data from the report and the environment of the affected system(s):

- Detailed contact information
- Detailed description of the incident
- Incident classification suggested by the incident reporter
- Operating systems and network setup
- The exact time and time zone info of the incident
- Security systems setup
- Incident severity
- Log file(s) included with the report

There are many repositories where data may reside related to the incident:

- Netflow data
- Router logs
- Proxy server logs
- Web application logs
- Mail server logs
- DHCP server logs
- Authentication server logs
- Referring databases
- Security equipment, such as firewall or intrusion detection logs

Information from other parties may be needed, when the source of an attack lies outside the constituency.

- Identify who you need
- Notify them
- Politely ask for the information that could help you

While it is important to have as much details as possible, be pragmatic and don't wait too long for data from other parties, as the incident may still be on-going and delays may increase the problem or give an intruder time to cover his tracks.
In general, 20% of the data may give you 80% of the knowledge needed to find a solution.

5.3.2 Resolution research

With all information gathered from the previous phase, this phase involves finding the best solution from a set of potential solutions.
This can be accomplished by thinking or talking about observations and conclusions, perhaps comparing configuration features from known mitigation facilities (either already in use or potentially beneficial for this incident).
For more complicated incidents, brainstorming sessions are a good idea.

5.3.3 Action proposed

Depending on the complexity of the incident, one or more actions may be required to mitigate the incident.
Keep your audience in mind when proposing actions - technical people will understand technical solutions, but if for example additional services need to be acquired or a costly action need to be performed, adjust your language for management or financial people.

Actions could include

- Turning off a service
- Scanning for malware
- Patching a system
- Hardening a system
- Isolating or fencing a system or service
- Auditing a system
- Collecting more information (maybe by hiring an external party)
- Buying a service (such as DDoS protection)
- Escalating to higher management or legal council
- Involving Corporate Communications or Public Relations
- Involving Law Enforcement for a criminal investigation
- If the system or application is provided by a third party (e.g. cloud-based, Github, Pastebin or social media), alerting those and working with them will be required

5.3.4 Action performed

Verify the action taken:

- Is the attack target reachable as it is supposed to be reachable?
- Did the action indeed solve the problem?
- Is the traffic filtered properly?

If the attack target is still vulnerable and/or the proposed solution does not fix the incident completely, repeat the previous steps to find further solutions.

5.3.5 Eradication and recovery

After the incident has been resolved, the system can be cleaned up and taken back into production.
Note that some actions may need more time after the incident itself has been resolved, for example a criminal investigation may proceed.
If Corporate Communications or Public Relations departments have been involved in the incident, make sure they have the information to update their statements.

5.4 Incident closing

There should be a clear policy on how and when to close incidents, as the amount of time each incident is kept open is an often used performance metric.
Some teams choose to never close incidents (new information could arrive, but most ticketing systems allow re-opening tickets), some will decide an incident can be closed when it is technically solved, other teams will close incidents only after all follow-up actions have also been performed.

5.4.1 Final information

Make sure all supporting documents are included with the ticket.
This is the time to inform the parties involved

- A short description of what happened
- The result of the mitigating work
- Findings and recommendations

5.4.2 Final classification

Now that all information is available about the incident, it is good practice to verify (and correct when needed) the classification.
If the original classification was very different from the currently known classification, perhaps the triage function could benefit from additional information to improve classifications.

5.4.3 Incident archiving

The incident can now be closed and archived.

It is advisable to keep closed tickets available to the team in an information system (which could be the same ticketing system) that allows searching. Similar incidents may happen again later and it can save a lot of time if earlier mitigation strategies can be consulted.

5.5 Post analysis

Various things can usually be learned from incidents, to prevent them from happening in the future, or to mitigate them faster.

Examples of lessons learned and improvement proposals:

- Additions or clarifications in the security policy
- Improvement in network architecture
- Improvement of detection mechanisms
- Missing tools that could have improved the analysis
- New types of attacks

CSIRT teams can share their lessons-learned with the security community so that all teams can benefit from the new knowledge (see 4.6).

6. Add services as needed

Following is the full list of common CSIRT services, as defined by CERT/CC[35]:

Reactive Services	Proactive Services	Security Quality Management

• **Alerts and Warnings**
• **Incident Handling**
  ○ **Incident analysis**
  ○ **Incident response on site**
  ○ **Incident reports support**
  ○ **Incident response coordination**
• Vulnerability Handling
  ○ Vulnerability analysis
  ○ Vulnerability response
  ○ Vulnerability response coordination
• Artifact Handling
  ○ Artifact analysis
  ○ Artifact response
  ○ Artifact response coordination
	• **Announcements**
	• Technology Watch
	• Security Audits or Assessments
	• Configuration & Maintenance of Security Tools, Applications & Infrastructures
	• Development of Security Tools
	• Intrusion Detection Services
	• Security-Related Information Dissemination
		• Risk Analysis
		• Business Continuity & Disaster Recovery Planning
		• Security Consulting
		• Awareness Building
		• Education/Training
		• Product Evaluation or Certification

The highlighted services are the minimal services a CSIRT should offer when it starts.

Further services can be added later as and when needed.
Services should be carefully selected to best serve the business goals of the constituency for the budget that is available, as each additional service will have an impact on the required resources, skill sets and partnerships of the CSIRT. It is better to offer fewer services at good quality than to offer many services poorly.

Apart from providing a service by the CSIRT itself, some services can also be outsourced to other, specialized, organizations. This may be a good alternative for expensive, rarely needed, services such as digital forensics.
The CSIRT can still be the point of contact to acquire a service externally.

Note that no CSIRT provides *all* of the listed services.

[35] From "Handbook for Computer Security Incident Response Teams (CSIRTs), 2nd edition", page 25

6.1 Service Descriptions[36]

6.1.1 Reactive Services

Reactive services are designed to respond to requests for assistance, reports of incidents from the CSIRT constituency, and any threats or attacks against CSIRT systems. Some services may be initiated by third-party notification or by viewing monitoring or IDS logs and alerts.

Alerts and Warnings

This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of action for dealing with the resulting problem. The alert, warning, or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected. Information may be created by the CSIRT or may be redistributed from vendors, other CSIRTs or security experts, or other parts of the constituency.

Incident Handling

Incident handling involves receiving, triaging and responding to requests and reports, and analyzing incidents and events. Particular response activities can include

- taking action to protect systems and networks affected or threatened by intruder activity
- providing solutions and mitigation strategies from relevant advisories or alerts
- looking for intruder activity on other parts of the network
- filtering network traffic
- rebuilding systems
- patching or repairing systems
- developing other response or workaround strategies.

Since incident handling activities are implemented in various ways by different types of CSIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Incident analysis

There are many levels of incident analysis and many sub-services. Essentially, incident analysis is an examination of all available information and supporting evidence or artifacts related to an incident or event. The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. The CSIRT may use the results of vulnerability and artifact analysis (described below) to understand and provide the most complete and up-to-date analysis of what has happened on a specific system.
The CSIRT correlates activity across incidents to determine any interrelations, trends, patterns, or intruder signatures. Two sub-services that may be done as part of incident analysis, depending on the mission, goals, and processes of the CSIRT, are:

- **Forensic evidence collection**
  The collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise. This gathering of information and evidence must be done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evidence. Tasks involved in forensic evidence collection include (but are not limited to)

[36] From "Handbook for Computer Security Incident Response Teams (CSIRTs), 2nd edition", page 25-34

making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports; and checking for Trojan horse programs and toolkits. CSIRT staff performing this function may also have to be prepared to act as expert witnesses in court proceedings.

- **Tracking or tracing**
  The tracing of the origins of an intruder or identifying systems to which the intruder had access. This activity might involve tracking or tracing how the intruder entered the affected systems and related networks, which systems were used to gain that access, where the attack originated, and what other systems and networks were used as part of the attack. It might also involve trying to determine the identity of the intruder. This work might be done alone but usually involves working with law enforcement personnel, Internet service providers, or other involved organizations.

Incident response on site

The CSIRT provides direct, on-site assistance to help constituents recover from an incident. The CSIRT itself physically analyses the affected systems and conducts the repair and recovery of the systems, instead of only providing incident response support by telephone or email (see below). This service involves all actions taken on a local level that are necessary if an incident is suspected or occurs. If the CSIRT is not located at the affected site, team members would travel to the site and perform the response. In other cases a local team may already be on site, providing incident response as part of its routine work. This is especially true if incident handling is provided as part of the normal job function of system, network, or security administrators in lieu of an established CSIRT.

Incident response support

The CSIRT assists and guides the victim(s) of the attack in recovering from an incident via phone, email, fax, or documentation. This can involve technical assistance in the interpretation of data collected, providing contact information, or relaying guidance on mitigation and recovery strategies. It does not involve direct, on-site incident response actions as described above. The CSIRT instead provides guidance remotely so site personnel can perform the recovery themselves.

Incident response coordination

The CSIRT coordinates the response effort among parties involved in the incident. This usually includes the victim of the attack, other sites involved in the attack, and any sites requiring assistance in the analysis of the attack. It may also include the parties that provide IT support to the victim, such as Internet service providers, other CSIRTs, and system and network administrators at the site. The coordination work may involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange and analysis. Part of the coordination work may involve notification and collaboration with an organization’s legal counsel, human resources or public relations departments. It would also include coordination with law enforcement.
This service does not involve direct, on-site incident response.

Vulnerability Handling

Vulnerability handling involves receiving information and reports about hardware and software vulnerabilities; analyzing the nature, mechanics, and effects of the vulnerabilities; and developing response strategies for detecting and repairing the vulnerabilities. Since vulnerability handling activities are implemented in various ways by different types of CSIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Vulnerability analysis

The CSIRT performs technical analysis and examination of vulnerabilities in hardware or software. This includes the verification of suspected vulnerabilities and the technical examination of the hardware or software vulnerability to determine where it is located and how it can be exploited. The analysis may include reviewing source code, using a debugger to determine where the vulnerability occurs, or trying to reproduce the problem on a test system.

Vulnerability response

This service involves determining the appropriate response to mitigate or repair vulnerability. This may involve developing or researching patches, fixes, and workarounds. It also involves notifying others of the mitigation strategy, possibly by creating and distributing advisories or alerts. This service can include performing the response by installing patches, fixes, or workarounds.

Vulnerability response coordination

The CSIRT notifies the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability. The CSIRT verifies that the vulnerability response strategy has been successfully implemented. This service can involve communicating with vendors, other CSIRTs, technical experts, constituent members, and the individuals or groups who initially discovered or reported the vulnerability. Activities include facilitating the analysis of a vulnerability or vulnerability report; coordinating the release schedules of corresponding documents, patches, or workarounds; and synthesizing technical analysis done by different parties. This service can also include maintaining a public or private archive or knowledge base of vulnerability information and corresponding response strategies.

Artifact Handling

An artifact is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures.
Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.
Artifact handling involves receiving information about and copies of artifacts that are used in intruder attacks, reconnaissance, and other unauthorized or disruptive activities.
Once received, the artifact is reviewed. This includes analyzing the nature, mechanics, version, and use of the artifacts; and developing (or suggesting) response strategies for detecting, removing, and defending against these artifacts. Since artifact handling activities are implemented in various ways by different types of CSIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Artifact analysis

The CSIRT performs a technical examination and analysis of any artifact found on a system. The analysis done might include identifying the file type and structure of the artifact, comparing a new artifact against existing artifacts or other versions of the same artifact to see similarities and differences, or reverse engineering or disassembling code to determine the purpose and function of the artifact.

Artifact response

This service involves determining the appropriate actions to detect and remove artifacts from a system, as well as actions to prevent artifacts from being installed. This may involve creating signatures that can be added to antivirus software or IDS.

Artifact response coordination

This service involves sharing and synthesizing analysis results and response strategies pertaining to an artifact with other researchers, CSIRTs, vendors, and other security experts. Activities include notifying others and synthesizing technical analysis from a variety of sources. Activities can also include maintaining a public or constituent archive of known artifacts and their impact and corresponding response strategies.

6.1.2 Proactive Services

Proactive services are designed to improve the infrastructure and security processes of the constituency before any incident or event occurs or is detected. The main goals are to avoid incidents and to reduce their impact and scope when they do occur.

Announcements

This includes, but is not limited to, intrusion alerts, vulnerability warnings, and security advisories. Such announcements inform constituents about new developments with medium- to long-term impact, such as newly found vulnerabilities or intruder tools.

Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited.

Technology Watch

The CSIRT monitors and observes new technical developments, intruder activities, and related trends to help identify future threats. Topics reviewed can be expanded to include legal and legislative rulings, social or political threats, and emerging technologies. This service involves reading security mailing lists, security web sites, and current news and journal articles in the fields of science, technology, politics, and government to extract information relevant to the security of the constituent systems and networks. This can include communicating with other parties that are authorities in these fields to ensure that the best and most accurate information or interpretation is obtained.

The outcome of this service might be some type of announcement, guidelines, or recommendations focused at more medium- to long-term security issues.

Security Audits or Assessments

This service provides a detailed review and analysis of an organization's security infrastructure, based on the requirements defined by the organization or by other industry standards that apply. It can also involve a review of the organizational security practices. There are many different types of audits or assessments that can be provided, including

- Infrastructure review: Manually reviewing the hardware and software configurations, routers, firewalls, servers, and desktop devices to ensure that they match the organizational or industry best practice security policies and standard configurations.
- Best practice review: Interviewing employees and system and network administrators to determine if their security practices match the defined organizational security policy or some specific industry standards
- Scanning: Using vulnerability or virus scanners to determine which systems and networks are Vulnerable.
- Penetration testing: Testing the security of a site by purposefully attacking its systems and networks.

Obtaining upper management approval is required before conducting such audits or assessments. Some of these approaches may be prohibited by organizational policy.
Providing this service can include developing a common set of practices against which the tests or assessments are conducted, along with developing a required skill set or certification requirements for staff that perform the testing, assessments, audits, or reviews. This service could also be outsourced to a third party contractor or managed security service provider with the appropriate expertise in conducting audits and assessments.

Configuration and Maintenance of Security Tools, Applications, Infrastructures and Services

This service identifies or provides appropriate guidance on how to securely configure and maintain tools, applications, and the general computing infrastructure used by the CSIRT constituency or the CSIRT itself. Besides providing guidance, the CSIRT may perform configuration updates and maintenance of security tools and services, such as IDS, network scanning or monitoring systems, filters, wrappers, firewalls, virtual private networks (VPN), or authentication mechanisms. The CSIRT may even provide these services as part of their main function. The CSIRT may also configure and maintain servers, desktops, laptops, tablets, smartphones, and other wireless devices according to security guidelines. This service includes escalating to management any issues or problems with configurations or the use of tools and applications that the CSIRT believes might leave a system vulnerable to attack.

Development of Security Tools

This service includes the development of any new, constituent-specific tools that are required or desired by the constituency or by the CSIRT itself. This can include, for example, developing security patches for customized software used by the constituency or secured software distributions that can be used to rebuild compromised hosts. It can also include developing tools or scripts that extend the functionality of existing security tools, such as a new plug-in for a vulnerability or network scanner, scripts that facilitate the use of encryption technology, or automated patch distribution mechanisms.

Intrusion Detection Services

CSIRTs that perform this service review existing IDS logs, analyze and initiate a response for any events that meet their defined threshold, or forward any alerts according to a predefined service level agreement or escalation strategy. Intrusion detection and analysis of the associated security logs can be a daunting task—not only in determining where to locate the sensors in the environment, but collecting and then analyzing the large amounts of data captured. In many cases, specialized tools or expertise is required to synthesize and interpret the information to identify false alarms, attacks, or network events and to implement strategies to eliminate or minimize such events. Some organizations choose to outsource this activity to others who have more expertise in performing these services, such as managed security service providers.

Security-Related Information Dissemination

This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include

- reporting guidelines and contact information for the CSIRT
- archives of alerts, warnings, and other announcements
- documentation about current best practices
- general computer security guidance
- policies, procedures, and checklists
- patch development and distribution information
- vendor links

- current statistics and trends in incident reporting
- other information that can improve overall security practices

This information can be developed and published by the CSIRT or by another part of the organization (IT, human resources, or media relations), and can include information from external resources such as other CSIRTs, vendors, and security experts.

6.1.3 Security Quality Management Services

Services that fall into this category are not unique to incident handling or CSIRTs in particular. They are well-known, established services designed to improve the overall security of an organization. By leveraging the experiences gained in providing the reactive and proactive services described above, a CSIRT can bring unique perspectives to these quality management services that might not otherwise be available. These services are designed to incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities, and attacks. Feeding such experiences into the established traditional services (described below) as part of a security quality management process can improve the long-term security efforts in an organization. Depending on organizational structures and responsibilities, a CSIRT may provide these services or participate as part of a larger organizational team effort.

The following descriptions explain how CSIRT expertise can benefit each of these security quality management services.

Risk Analysis

CSIRTs may be able to add value to risk analysis and assessments. This can improve the organization's ability to assess real threats, to provide realistic qualitative and quantitative assessments of the risks to information assets, and to evaluate protection and response strategies. CSIRTs performing this service would conduct or assist with information security risk analysis activities for new systems and business processes or evaluate threats and attacks against constituent assets and systems.

Business Continuity and Disaster Recovery Planning

Based on past occurrences and future predictions of emerging incident or security trends, more and more incidents have the potential to result in serious degradation of business operations. Therefore, planning efforts should consider CSIRT experience and recommendations in determining how best to respond to such incidents to ensure the continuity of business operations. CSIRTs performing this service are involved in business continuity and disaster recovery planning for events related to computer security threats and attacks.

Security Consulting

CSIRTs can be used to provide advice and guidance on the best security practices to implement for constituents' business operations. A CSIRT providing this service is involved in preparing recommendations or identifying requirements for purchasing, installing, or securing new systems, network devices, software applications, or enterprise-wide business processes. This service includes providing guidance and assistance in developing organizational or constituency security policies. It can also involve providing testimony or advice to legislative or other government bodies.

Awareness Building

CSIRTs may be able to identify where constituents require more information and guidance to better conform to accepted security practices and organizational security policies. Increasing the general security awareness of the constituent population not only improves their understanding of security issues but also helps them perform their day-to-day operations in a more secure manner. This can reduce the

occurrence of successful attacks and increase the probability that constituents will detect and report attacks, thereby decreasing recovery times and eliminating or minimizing losses.
CSIRTs performing this service seek opportunities to increase security awareness through developing articles, posters, newsletters, web sites, or other informational resources that explain security best practices and provide advice on precautions to take.
Activities may also include scheduling meetings and seminars to keep constituents up to date with ongoing security procedures and potential threats to organizational systems.

Education/Training

This service involves providing information to constituents about computer security issues through seminars, workshops, courses, and tutorials. Topics might include incident reporting guidelines, appropriate response methods, incident response tools, incident prevention methods, and other information necessary to protect, detect, report, and respond to computer security incidents.

Product Evaluation or Certification

For this service, the CSIRT may conduct product evaluations on tools, applications, or other services to ensure the security of the products and their conformance to acceptable CSIRT or organizational security practices. Tools and applications reviewed can be open source or commercial products. This service can be provided as an evaluation or through a certification program, depending on the standards that are applied by the organization or by the CSIRT.

Appendix A: CSIRT Framework template

CSIRT FRAMEWORK
Team name: Mission Statement: Constituency: Authority: Responsibility: Organizational structure: Availability: Services: Staffing: Infrastructure and tooling: Internal and external relationships: Funding model:

Appendix B: Sample Incident Reporting form

INCIDENT REPORTING FORM

Please fill out this form and Fax or email it to: …….
Lines marked with * are required.

Name and Organization

1. Name*:
2. Name of Organization*:
3. Sector type:
4. Country*:
5. City:
6. E-Mail address*:
7. Telephone number*:
8. Other:

Affected Host(s)

9. Number of Hosts:
10. Hostname & IP*:
11. Function of the Host*:
12. Time-Zone:
13. Hardware:
14. Operating System:
15. Affected Software:
16. Affected Files:
17. Protocol/port:

Incident

18. Reference number ref #:
19. Type of Incident:
20. Incident Started:
21. This is an ongoing incident: YES NO
22. Time and Method of Discovery:
23. Known Vulnerabilities:
24. Suspicious Files:
25. Countermeasures:
26. Detailed description*:

Appendix C: Security tools

There are many tools available to assist CSIRT teams in their work for Incident Handling, many of which are free to use.

Keep in mind that most log files are stored in plain text format and can be easily searched by (Unix/Linux) command-line tools such as `sed`, `awk` and `grep`. These same tools can be used to normalize log files from different sources or convert them into different formats to allow the use of more advanced tools.

Following is a selection of regularly used tools.

Domain and IP address query tools	
DomainTools	<https://www.domaintools.com/>
Domain Dossier	<http://centralops.net/co/DomainDossier.aspx>
IP to ASN Mapping	<http://www.team-cymru.org/IP-ASN-mapping.html>
GeoLite2	<http://dev.maxmind.com/geoip/geoip2/geolite2/>
RIPEstat	<https://stat.ripe.net/>
E-mail header analysis tools	
Google Apps Messageheader	<https://toolbox.googleapps.com/apps/messageheader/>
MXToolbox	<http://mxtoolbox.com/EmailHeaders.aspx>
Network monitoring tools	
nfdump	<http://nfdump.sourceforge.net/>
nfsen	<http://nfsen.sourceforge.net/>
Network auditing tools	
nmap	<https://nmap.org/>
AutoScan-Network	<http://autoscan-network.com/>
Wireshark	<https://www.wireshark.org/>
AbuseHelper	<https://github.com/abusesa/abusehelper>
Vulnerability assessment tools	
Nessus	<http://www.tenable.com/products/nessus-vulnerability-scanner>
Metasploit	<https://www.metasploit.com/>
Vega	<https://subgraph.com/vega/index.en.html>

OWASP ZAP	<https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project>
SQLcheck	<http://www.softpedia.com/get/Internet/Servers/Database-Utils/SQL-Check.shtml>
Burp Suite	<https://portswigger.net/burp/>
Kali	<https://www.kali.org/>
Intrusion detection tools	
Snort	<https://www.snort.org/>
Tripwire	<https://sourceforge.net/projects/tripwire/>
Forensic tools	
Sleuth Kit	<http://www.sleuthkit.org/>
Autopsy	<http://www.sleuthkit.org/autopsy/>
Tcpxtract	<http://tcpxtract.sourceforge.net/>
EnCase	<https://www.guidancesoftware.com/encase-forensic>
FTK, Forensic Toolkit	<http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk>
Malware analysis tools	
VirusTotal	<https://www.virustotal.com/>
Malware Domain List	<http://www.malwaredomainlist.com/>
Malware Hash Registry	<http://www.team-cymru.org/MHR.html>
MISP, Malware Information Sharing Platform	<https://mispriv.circl.lu/>
AlienVault Open Threat Exchange	<https://otx.alienvault.com/>
Malwr	<https://malwr.com/>
Hybrid Analysis	<https://www.hybrid-analysis.com/>
Honeypots	
honeyd	<http://www.honeyd.org/index.php>
WiFi tools	
inSSIDer	<http://www.metageek.com/products/inssider/>

Acrylic WiFi Scanner	<https://www.acrylicwifi.com/en/wlan-software/wlan-scanner-acrylic-wifi-free/>
SIEM tools	
Splunk	<http://www.splunk.com/>
Encryption tools	
GnuPG	<https://www.gnupg.org/>
VeraCrypt	<https://veracrypt.codeplex.com/>
Incident-tracking tools	
RTIR	<https://bestpractical.com/>
OTRS	<https://www.otrs.com/>
Databases	
SQLite	<https://www.sqlite.org/>
MySQL	<https://www.mysql.com/>
PostgreSQL	<https://www.postgresql.org/>

Appendix D: Information resources

For incident notifications, there are various automated feeds one can subscribe to, offered by the security community, most of them free of charge. The following are routinely used by many teams:

Incident notifications		
APWG, Anti-Phishing Working Group	<http://apwg.org/>	• Phishing
PhishTank	<http://www.phishtank.com>	• Phishing
Dark-H	<http://dark-h.org>	• Web defacements
Mirror-Zone	<http://mirror-zone.org>	• Web defacements
Zone-H	<http://zone-h.org>	• Web defacements
Zone-HC	<http://zone-hc.com>	• Web defacements
Shadowserver	<https://www.shadowserver.org>	• Botnet • Open DNS resolver • Open proxy server • etc.
Team Cymru	<http://www.team-cymru.org/services.html>	• Botnet • Brute force • DDoS • Malware URL • Open DNS resolver • Open proxy server • Phishing • Scanning

To find contact information for a team whose constituency is involved in an incident, the following website repositories can be consulted:

Contact information (member teams)	
FIRST, Forum of Incident Response and Security Teams	<https://www.first.org/>
APCERT, Asia Pacific CERT	<http://www.apcert.org/>
Trusted Introducer	<https://www.trusted-introducer.org/>
AfricaCERT	<http://www.africacert.org>
Latin American CSIRTs	<http://www.lacnic.net/en/web/lacnic/csirts>
OIC-CERT, Organisation of the Islamic Cooperation CERT	<http://www.oic-cert.org/>
NatCSIRT, National CSIRTs	<http://www.cert.org/incident-management/national-csirts/national-csirts.cfm>