

PART I

A basic collection of good practices for running a CSIRT

Deliverable WP2007/2.4.9/1 (CERT-D3.1)



Table of Contents

- 1 Management Summary 9**
- 2 Acknowledgements 9**
- 3 Introduction 9**
 - 3.1 TARGET AUDIENCE 10
 - 3.2 HOW TO USE THIS DOCUMENT 10
 - 3.3 WHAT IS A CSIRT? 11
 - 3.4 POSSIBLE SERVICES THAT A CSIRT CAN DELIVER 12
- 4 CSIRT external relations: Management 14**
 - 4.1 CSIRTS AS PART OF THE INFORMATION SECURITY STRATEGY 16
 - 4.2 MARKET APPROACH WITHIN THE CSIRT 17
- 5 CSIRT external relations: Constituency 18**
 - 5.1 BUILDING UP THE BASIC CONSTITUENCY 18
 - 5.2 PROCEDURE FOR NEW CONSTITUENTS 21
 - 5.3 MANAGING CONSTITUENCY EXPECTATIONS 23
 - 5.4 ENHANCEMENT OF THE CONSTITUENT RELATIONSHIP 23
 - 5.5 BUILDING UP A COMMUNITY AMONG THE CONSTITUENCY 31
 - 5.6 REVIEW OF THE SERVICE PORTFOLIO 32
 - 5.7 MANAGING DEVELOPING EXPECTATIONS 33
- 6 CSIRT external relations: CSIRT communities 35**
 - 6.1 LEGAL BASIS FOR COLLABORATION 38
- 7 CSIRT internal management 41**
 - 7.1 (RE)ASSURING THE MANDATE 41
 - 7.2 CSIRT ORGANIZATIONAL STRUCTURE 42
 - 7.3 CSIRT TEAM ROLES AND STAFFING 45
 - 7.4 TRAINING AND EDUCATION 47
 - 7.5 CERTIFICATION POSSIBILITIES FOR THE CSIRT STAFF 49
 - 7.6 BENCHMARKING 50
 - 7.7 CONTINUOUSLY STAYING UP TO DATE 52
- 8 CSIRT tools and equipment 54**
 - 8.1 INCIDENT TRACKING AND REPORTING 54
 - 8.2 SECURE COMMUNICATION SOFTWARE 55
 - 8.3 CUSTOMER RELATIONSHIP MANAGEMENT 56
- 9 Annex 60**
 - 9.1 ISO27001 / ISO27002 60
 - 9.2 CRM DEFINITIONS AND DETAILS 60
 - 9.3 BUILDING A COMMUNITY 63
 - 9.4 OTHER WAYS OF VIEWING THE SAME PROBLEMS 64
 - 9.5 SECURITY INFORMATION SOURCE LIST 67
 - 9.6 CSIRT SERVICES 75
 - 9.7 OTHER AVAILABLE INFORMATION AND MATERIAL 84



1 Management Summary

The document at hand contains a basic set of good practice on how to successfully run a Computer Security and Incident Response team (CSIRT). It mainly focuses on external relationships to management, constituency and communities, and team internal measures to keep or enhance the level of quality in which the services of the team are provided.

The document at hand is one part of the ENISA deliverable CERT2007-D2.4.9 "Collecting good practices for quality assurance for CERTs" from the ENISA Work Programme 2008. It is supplemented by a pre-study about "Enhanced mechanisms of trust building" (CERT2007-D2.4.9/2) that mainly deals with the feasibility of certification of CSIRTs, and a pre-study about "CSIRT exercises" (CERT2007-D2.4.9/3). Both of these studies are intended to prepare future ENISA deliverables.

2 Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special "Thank You" goes to the following contributors:

- Henk Bronk, who as a consultant produced the first version of this document.
- The CERT/CC and especially the CSIRT development team, who contributed most useful material.
- GovCERT.NL for providing CERT-in-a-box
- The countless people who reviewed this document

3 Introduction

Communication networks and information systems have become an essential factor in economic and social development. Computing and networking are now becoming ubiquitous utilities in the same way electricity or water supply are.

The security of communication networks and information systems and their availability in particular, is therefore of increasing concern to society. This stems from the risk of problems to key information systems, due to system complexity, accidents, mistakes and attacks to the physical infrastructures that deliver services critical to the well being of EU citizens.

On 10 March 2004 a European Network and Information Security Agency (ENISA) was established¹. Its purpose is to ensure a high and effective level of network and information security within the community and to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations within the European Union, thus contributing to the smooth functioning of the internal market.

¹ Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. A "European Community agency" is a body set up by the EU to carry out a very specific technical, scientific or management task within the "Community domain" ("first pillar") of the EU. These agencies are not provided for in the Treaties. Instead, each one is set up by an individual piece of legislation that specifies the task of that particular agency.

For several years now, a number of security communities in Europe like CERT/CSIRTs, Abuse Teams and WARPs have collaborated for a more secure Internet. ENISA intends to support these communities in their endeavours by providing information about measures for assuring an appropriate level of service quality. Furthermore ENISA intends to enhance its ability to advise the EU member states and the EU bodies in questions of the coverage of specific groups of IT users with appropriate security services.

This document builds on recommendations of the 2006 ENISA CERT Working Group on “CERT Services”² and also aims to serve as the next logical step to the previous ENISA deliverable: “A step-by-step approach on how to set up a CSIRT”³.

ENISA supports the establishment of new CSIRTs and enhancing their capabilities by publishing this ENISA report, “*Basic set of good practice for running a CSIRT*”, which aims at assisting CSIRTs in maturing their services and team capabilities.

3.1 Target audience

The primary target groups for this report are governmental and other institutions that have already established a CSIRT and are ready to take the initial capabilities to the next level of a well established team.

3.2 How to use this document

This document intends to provide guidance on what a CSIRT needs in order to enhance its functions and to deliver the CSIRT services that progressively meet the expectation of its constituency.

This guideline should be seen as the continuation of the first document, “*A step-by-step approach on how to set-up a CSIRT*”, and at times it may be beneficial to revisit its contents.

This document does not have the ambition to prescribe all actions that a well established team should be taking, but rather provide a basic set of good practices that team managers could take into account when reassessing their CSIRT activities.

This document addresses both, internal and external, challenges of running a CSIRT. As a result, this document should also help with internal team management and CSIRT positioning in order to deliver the right services to the constituents.

When to use this guide

Launching of CSIRT activities is a demanding task and experience shows that “start small but think big” is a good and promising motto. A year after the start of the initial CSIRT operations might be a good time to reassess the situation. Everyday operations will most likely provide plenty of feedback for improvement, but this guide will hopefully give additional ideas and help to structure the assessment of how to continue with the development of the CSIRT and how to extend the services and probably the number of constituents.

² ENISA ad-hoc working group on CERT Services:

http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

³ ENISA’s A step-by-step approach on how to set up a CSIRT: http://www.enisa.europa.eu/cert_guide/

Also, any CSIRT about to embark on major changes, such as increase in mandate, services or constituency, could benefit from this guide.

Although the audience of this document should be already well familiar with what the CSIRT is, below is a short recap of CSIRT nature and its definition for reference.

3.3 What is a CSIRT?

CSIRT stands for Computer Security Incident Response Team. The name CSIRT is the name used predominantly in Europe for the protected CERT© or CERT-CC name.

The following abbreviations are used for the same sort of teams:

- CERT© or CERT-CC (Computer Emergency Response Team / Coordination Centre)
- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)

The first major outbreak of a worm in the global ICT infrastructure occurred in the late 1980s. This worm was named after his creator Morris⁴ and it spread swiftly, effectively infecting a great number of ICT systems around the world.

This incident acted as a wake-up call: suddenly people got aware of a strong need for cooperation and coordination between system administrators and IT managers in order to deal with cases like this. Due to the fact that time was a critical factor, a more organised and structural approach on handling IT security incidents had to be established. And so a few days after the “Morris-incident” the Defence Advanced Research Projects Agency (DARPA) established the first CSIRT: the CERT Coordination Centre (CERT/CC), located at the Carnegie Mellon University in Pittsburgh (Pennsylvania).

This model was soon adopted within Europe, and 1992 the Dutch Academic provider SURFnet launched the first CSIRT in Europe, named SURFnet-CERT. Many teams followed and at present ENISAs Inventory of CERT activities in Europe (ENISA Inventory) lists more than 100 known teams located in Europe.

Over the years CERTs extended their capacities from being a mere reaction force to a complete security service provider, including preventative services such as alerts, security advisories, training and security management services. The term “CERT” was soon considered insufficient. As a result, the new term “CSIRT” was established at the end of the 1990s. At the moment both terms (CERT and CSIRT) are used synonymously, with CSIRT being the more precise term.

⁴ Morris-Worm at Wikipedia: http://en.wikipedia.org/wiki/Morris_worm

Definition of a CSIRT

From now on the (in the CSIRT communities) well established term ‘constituency’ will be used to refer to the customer base of a CSIRT. A single customer will be addressed as "constituent", a group as "constituents".

A CSIRT is a team that responds to computer security incidents by providing all necessary services to solve the problem(s) or to support the resolution of them. In order to mitigate risks and minimize the number of required responses, most CSIRTs also provide preventative and educational services for their constituency. They issue advisories on vulnerabilities and viruses in the soft- and hardware running on their constituent’s systems. These constituents can therefore quickly patch and update their systems.

This definition is very important for setting the borders on what the CSIRT can and will deliver and for ensuring that the needs of the constituency are properly understood. The constituents on their side should also clearly understand what the CSIRT will deliver and what are the focal points (“manage expectations”).

3.4 Possible services that a CSIRT can deliver

There are many services that a CSIRT can deliver, but so far no existing CSIRT provides all of them. So the selection of the appropriate set of services is a crucial decision. Below you will find a short overview of all known CSIRT services, as defined in the “Handbook for CSIRTs” published by the CERT/CC.

<u>Reactive Services</u>	<u>Proactive Services</u>	<u>Artifact Handling</u>
<ul style="list-style-type: none"> • <u>Alerts and Warnings</u> • <u>Incident Handling</u> • <u>Incident analysis</u> • <u>Incident response support</u> • <u>Incident response coordination</u> • <u>Incident response on site</u> • <u>Vulnerability Handling</u> • <u>Vulnerability analysis</u> • <u>Vulnerability response</u> • <u>Vulnerability response coordination</u> 	<ul style="list-style-type: none"> • <u>Announcements</u> • <u>Technology Watch</u> • <u>Security Audits or Assessments</u> • <u>Configuration and Maintenance of Security</u> • <u>Development of Security Tools</u> • <u>Intrusion Detection Services</u> • <u>Security-Related Information Dissemination</u> 	<u>Artifact Handling</u>
		<ul style="list-style-type: none"> • <u>Artifact analysis</u> • <u>Artifact response</u> • <u>Artifact response coordination</u>
		<u>Security Quality Management</u>
		<ul style="list-style-type: none"> • <u>Risk Analysis</u> • <u>Business Continuity and Disaster Recovery</u> • <u>Security Consulting</u> • <u>Awareness Building</u> • <u>Education/Training</u> • <u>Product Evaluation or Certification</u>

Figure 1. CSIRT Services list from CERT/CC⁵

⁵ CSIRT services list kindly provided by the CERT Coordination Centre: <http://www.cert.org>

The core services (marked in bold letters on *Figure 1*):

There is a distinction made between reactive and proactive services. Proactive services aim at prevention of incidents through awareness building and training, while reactive services aim at handling incidents and mitigating the resulting damage.

Artifact handling contains the analysis of any file or object found on a system that might be involved in malicious actions, like leftovers from viruses, worms, scripts, trojans, etc. It also contains the handling and distribution of resulting information to vendors and other interested parties, in order to prevent further spreading of malware and to mitigate the risks.

Security and Quality management services are services with longer term goals and include consultancy and educational measures.

See the appendix for a detailed explanation of CSIRT services.

Most CSIRTs start with distributing 'Alerts and Warnings', make 'Announcements' and providing 'Incident Handling' for their constituents. These core-services usually give a good profile and attention value with the constituency, and are mainly considered as real "added value".

A good practice is to start with a small group of 'pilot'-constituents, deliver the core-services for a pilot-period of time and request feedback afterwards.

In addition, providing these select core services will provide an opportunity to learn and understand the real needs of the constituency before progressing to more elaborate services and relationships. Meeting constituents in person and being open for discussions are also likely to lead to business and service improvements for the CSIRT. The customers' feedback is essential for improvements and should not be forgotten to act upon. At the minimum, credit should be given for valuable input.

Interested pilot-users usually provide constructive feedback and help to develop tailor-made services.

The second ENISA ad-hoc working group "CERT services" looked into what kind of standard services a particular CSIRT should deliver to various constituency groups. See chapter 5.6 for more information.

4 CSIRT external relations: Management

A good relation to the management of the hosting organisation is at least as important as a good relationship to the constituency that the CSIRT serves. Good relations to the decision makers mean proper funding, proper support and a better perspective to develop the team further. The key factor to a good relationship is a constant awareness building referred to the added value the CSIRT provides to the hosting organisation.

A way to achieve this good relationship is giving regular presentations of statistics about incidents (including an estimation of money saved via incident handling⁶) and constituency satisfaction. The management must be made aware of the negative impact that the absence of the team would have. PR training for key persons in the team to enhance its promotional capability might be appropriate (this is also true for the relationship with the constituency). The provision of a proper business case is another important key factor that should be addressed as soon as possible, as the business case is a basis for a good relation to management and it should stay stable over time. Dedicated training for managers, CEOs and other decision makers in issues of computer and network security might help to raise awareness about IR capabilities among senior management, e.g. while outsourcing or procuring services (proper use of terms in contracts, proper service agreements and SLAs).

The current trend to outsource security poses a big problem to the incident response capabilities of (for example) a company. Senior management must be made aware that internal bodies will have to control the management of incidents for outsourced services. In case of outsourcing regular reports about incident response must be provided and a constant monitoring must take place. It should be considered good practice to keep IR capabilities in house.

Keywords:

- Added value / return of investment
- Business case
- Training (also for management)
- Outsourcing

Having a dedicated ICT-security team helps to mitigate and prevent major incidents and helps to protect valuable assets of the organization.

⁶ For an example see: <http://www.cert.org/podcast/show/roi.html>

Further possible benefits are:

- Having a centralized coordination for ICT-security issues within the organization (or industry sector, region, country).
- Having a central and specialized organization in handling and responding to ICT-incidents.
- Having dedicated support available to assist in taking the appropriate steps and helping the constituent with quick recovery of the ICT infrastructure.
- Dealing with legal issues and preserving evidence in the event of a lawsuit.
- Developing experience about ICT-security
- Stimulating cooperation within the constituency on ICT-security and preventing possible losses.

It is imperative to understand the possibilities of the CSIRT and the needs of its constituents. These statements then become positive communication items towards CSIRT sponsors and new customers. It's also recommended to clarify these benefits to the existing constituents and to review them for validity.



CSIRT team members should practice the above statements in an “elevator pitch” exercise⁷. This way they will contribute to the success of the team and become part of a very important communication channel.

⁷ Elevator Pitch at Wikipedia: http://en.wikipedia.org/wiki/Elevator_pitch

4.1 CSIRTs as part of the Information Security strategy

While talking about the different environments, also more elaborated in the guide “*A step-by-step approach on how to set up a CSIRT*”⁸, it’s important to look at business expectations and needs.

Naturally, interleaving the information security strategy with the business strategies of the management is a good way to highlight the necessity for CSIRT capabilities.

The international ISO/IEC 27001⁹ and ISO/IEC 27002¹⁰ standards contain many requirements that point out the necessity for adopting CSIRT capacity into the business model.

The ISO27001 standard adopts and explains a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's **Information Security Management System (ISMS)**.

This process approach includes everything that uses resources, transforming inputs into outputs for next processes, also called the “Plan-Do-Check-Act” model.

The process approach for information security management presented in this standard encourages its users to emphasize the importance of:

- Understanding an organization’s information security requirements and the need to establish policy and objectives for information security;
- Implementing and operating controls to manage an organization's information security risks in the context of the organization’s overall business risks;
- Monitoring and reviewing the performance and effectiveness of the ISMS;
- Continuing improvement based on objective measurement.

For example: a requirement might be that breaches of information security will not cause serious financial damage to an organization and/or cause embarrassment to the organization (Important for SOX¹¹ and revenue loss)

An expectation might be that if a serious incident occurs (like the compromise of an organization’s essential system or an eBusiness website) people with sufficient training in appropriate procedures to minimize the impact have to be available to solve the problems.

This last example provides a good reason for implementing a CSIRT operation with skilled people into the organisation.

The ISO27002 standard describes security techniques and is a code of practice for information security management. Chapter 12 gives a good overview of the linking areas of a CSIRT operation and a standard business approach.

⁸ ENISA’s A step-by-step approach on how to set up a CSIRT:

http://www.enisa.europa.eu/cert_guide/index_guide.htm

⁹ ISO/IEC 27001 at Wikipedia: <http://en.wikipedia.org/wiki/ISO27001>

¹⁰ Includes since 04/2007 the former ISO/IEC 17799, at Wikipedia: <http://en.wikipedia.org/wiki/ISO17799>

¹¹ Sarbanes-Oxley Act at Wikipedia: http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act

Chapters 12 and 13 of the standard, the actual incident response related chapters, describe how to prepare for and respond to security incidents.

Due to copyright issues, please refer to the actual ISO standards.

- ISO/IEC 27001¹²
- ISO/IEC 27002¹³

4.2 Market approach within the CSIRT

It is a business approach of simple supply and demand for working with the community and was used for example in the case of building Govcert.nl.

Question

What does a market approach mean for a CSIRT?

For a CSIRT it's an ongoing effort to get enough funding and support for the continuation of its services. Often CSIRTs have to continuously justify their existence to its stakeholders, especially the management.

Organizing statistical information about CSIRT services should be done anyway, in order to stay in control of all information required by law and privacy regulations.

The way of using it could differ, allowing the CSIRT to do a business analysis on constituents. Some questions that should be addressed in this process:

- Who is the most profitable constituent?
- Who is the least profitable constituent?
- What is the most wanted service?
- What is the most delivered service?
- What is the least delivered service?
- Can services be (easily) adjusted to satisfy more constituents?
- Can the needs of constituents be combined?

Experience shows that from simply commercial perspective, a cost effective service that can satisfy around 80% of the constituency is the most beneficial and profitable one that can and should be delivered.

It does not mean that this most profitable service should be the only focus. Simply, this service will reliably meet the needs for most of the constituency, helps to gain trust and free up time to investigate other needs and develop more well-targeted services.

¹² Overview of the ISO 27001 standard in Wikipedia: http://en.wikipedia.org/wiki/ISO_27001

¹³ Includes since 04/2007 the former ISO/IEC 17799, at Wikipedia: <http://en.wikipedia.org/wiki/ISO17799>

5 CSIRT external relations: Constituency

The main reason for the existence of a security team is the constituency, so a satisfied constituency is necessary for the survival of a team. To be able to measure the level of satisfaction periodical surveys among the constituency have proved a good instrument, also for developing ideas for new or extended services. Regular events like a workshop or a conference dedicated to the relation between team and constituency are an important lever for constituency retention and a good way to deliver information. Training and exercises including parts of the constituency enhance not only the level of engagement but will also lead to a better interface between the CSIRT and its constituency, for example for incident handling. Besides this a team must make clear the added value its existence holds for the constituency, for example by providing incident statistics, statistics about security advisories or by educating the constituents in security issues (for example best practices, how-tos, background information, etc.)

The premier tool to provide this kind of information is a CSIRT's website. It is also a good way to keep team staff active in contacting the constituency. A renowned certificate that attests the team provides services of a specified level of quality may further enhance the acceptance of the team amongst the constituency.

Keywords:

- Feedback
- Customer retention
- Training
- Exercises
- Marketing
- Certification

Question

How to build fair expectations for constituency and to meet these expectations?

5.1 Building up the basic constituency

This guide assumes that the target constituency for the CSIRT is already established. If that is not the case, it would be useful to refer to chapter 5.3 Analysis of the constituency and mission statement of the previous guide "A step-by-step approach on how to set up a CSIRT"¹⁴.

A short summary:

SWOT and PEST analysis models, already used in the previous guide, help to gather a more holistic overview. They help to outline constituents' needs and help in focusing on clearly defined goals.

¹⁴ ENISA's A step-by-step approach on how to set up a CSIRT: http://www.enisa.europa.eu/cert_guide/

It's essential, especially in the beginning, to re-evaluate CSIRT original goals and targets approximately on a quarterly basis for accurate adjustments.

SWOT analysis

A SWOT Analysis is a strategic planning tool used to evaluate the **S**trengths, **W**eaknesses, **O**pportunities, and **T**hreats involved in a project or in a business venture or in any other situation requiring a decision. The technique is credited to Albert Humphrey, who led a research project at Stanford University in the 1960s and '70s, using data from the Fortune 500 companies.¹⁵

Strength	Weakness
Opportunities	Threats

Figure 2. *Swot analysis model*

¹⁵ SWOT analysis at Wikipedia: http://en.wikipedia.org/wiki/SWOT_analysis

PEST analysis

The PEST analysis is another important and widely used tool to analyse the constituency with the goal to understand **Political**, **Economic**, **Socio-cultural** and **Technological** circumstances of the environment a CSIRT is operating in. The analysis will help to determine whether the planning is still in tune with the environment and probably helps to avoid actions taken out of wrong assumptions.

<p>Political</p> <ul style="list-style-type: none"> • Ecological/environmental issues • Current legislation home market • Future legislation • European/international legislation • Regulatory bodies and processes • Government policies • Government term and change • Trading policies • Funding, grants and initiatives • Home market lobbying/pressure groups • International pressure groups 	<p>Economic</p> <ul style="list-style-type: none"> • Home economy situation • Home economy trends • Overseas economies and trends • General taxation issues • Taxation specific to product/services • Seasonality/weather issues • Market and trade cycles • Specific industry factors • Market routes and distribution trends • Customer/end-user drivers • Interest and exchange rates
<p>Social</p> <ul style="list-style-type: none"> • Lifestyle trends • Demographics • Consumer attitudes and opinions • Media views • Law changes affecting social factors • Brand, company, technology image • Consumer buying patterns • Fashion and role models • Major events and influences • Buying access and trends • Ethnic/religious factors • Advertising and publicity 	<p>Technological</p> <ul style="list-style-type: none"> • Competing technology development • Research funding • Associated/dependent technologies • Replacement technology/solutions • Maturity of technology • Manufacturing maturity and capacity • Information and communications • Consumer buying mechanisms/technology • Technology legislation • Innovation potential • Technology access, licensing, patents • Intellectual property issues

Figure 3. PEST analysis model

A detailed description of the PEST analysis can be found in Wikipedia¹⁶.

Both tools give a comprehensive and structured overview of what the need of the constituents are. The results will complement the business proposal and by this help to obtain funding for the setting up of the CSIRT.

¹⁶ PEST analysis at Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

5.2 Procedure for new constituents

When connecting to new constituents, all the relevant information regarding the CSIRT and its services should be readily available to the “newcomers”. Standardizing the intake procedures helps to organize this step in an efficient way, so that the essential information does not need to be repetitively explained while delivering services to the new constituents.

Question

What should be done to easily include new constituents?

The best start is to have the right information collected and well organized so that it can be easily made available when needed. This allows building up a good and individualized relationship with constituents through value-added services that meet the actual demand.

There are many ways for providing this crucial information to new constituents in a precompiled package. For example:

1. **A contract** between the CSIRT and its constituents could cover the following:
 - a. Payment and services to be delivered
 - b. Legal issues (liability and confidentiality)
 - c. Operational agreements
 - Contact information of the CSIRT
 - Business hours of the CSIRT
 - Response times to a telephone call
 - Response times to an e-mail
 - Escalation information, who to contact in times of crisis.
 - d. Regular meeting schedule

2. Information brochure

A more general promotional brochure could be tailored to be also suitable for informing new constituents.

3. Annual report

Like any other business, annual reports are a good way of promoting the CSIRT and they give the constituents a structured overview of the services and achievement of the CSIRT along with other useful information.

4. Manual or instruction booklet

CSIRT services and processes can be described in a manual along with instructions or flowcharts of reporting and other interactions with the CSIRT.

5. Public website

The Internet is a natural channel for informing constituents about CSIRT services and contacts. However, at least the CSIRT contact information should be well promoted to constituents via other alternative mediums since in the time of need they might not be able to reach the web for contact details.

Crucial information on how to reach the CSIRT “out-of-band” must be provided in an “offline” format like business cards, guides or other means. In case of large scale attacks online information will not be available!

 Some teams provide configurable websites for their constituents. These “myCSIRT” web portals provide information tailored to the needs of single groups of constituents. Such environment allows more targeted interaction and better overview for constituents through automated reporting.

Customer relations management (CRM)

Customer-relation is an essential and much underestimated aspect of performing a smooth and cost-efficient incident handling. Cost efficiency in this context means: maximum leverage of resources with the right tools in a minimum of time.

There are many CRM tools available that will do a sufficient job in. Chapter 8.3 provides more details about what information is generally needed for CRM operations.

CRM is always also the management of interfaces and channels to various groups important for a CSIRT. CRM should also be used to manage these channels.

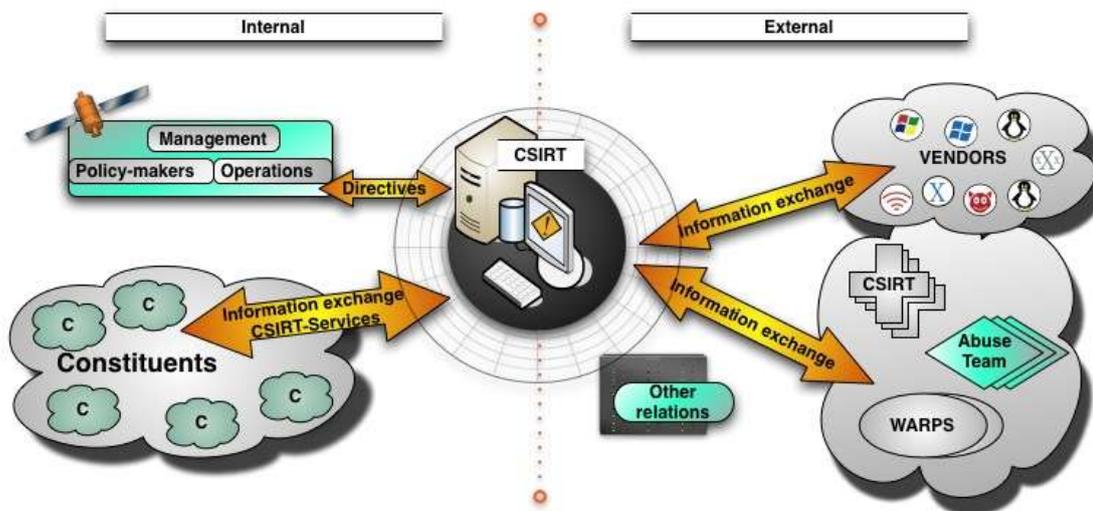


Figure 4. CSIRT Interfaces

Figure 4 above shows possible relationships of a CSIRT.

Other relationships could be an interface with:

- Government
- Law enforcement
- Secret services
- Public-private partnerships

Please also refer to chapter 8.3 under CSIRT tooling for more on CRM topic.

5.3 Managing constituency expectations

Question

How to assess and manage the expectations of the constituents?

A challenging task for every CSIRT is the management of expectations from the constituency in order to have a satisfied customer base. The following chapters (5.4 - 5.7) will examine the areas:

- Enhancement of the relationship to the constituency
- Building up a community among the constituency
- Review of the service portfolio
- Managing developing expectations

5.4 Enhancement of the constituent relationship

A set of services must be delivered at consistent quality. This is the basis of all expectation management.

It's better to start with a small set of services and to do it properly then to create expectations that can't be met. This should be clear from the start to the management, the team and to the CSIRT constituency.

A "group feeling" among active constituents works better for co-operation and teamwork rather than singled out leadership (of the CSIRT) and a passive constituency.

CSIRT achievements should be accompanied by putting constituents in the spotlight in case of success, but also the sharing of lessons-learned from mishaps should be encouraged (of course without compromising the persons behind).



Tip: It is often acceptable to individually highlight a success story of a constituent, but when talking about improvements or failures, it is more appropriate to share general, non-constituent specific or anonymous examples unless the constituent itself is willing to share lessons-learned within a group.

5.4.1 Communication channels

Good and clear communication is essential while building up trust with the constituency and adding more elaborate CSIRT services at the same time. Knowing the target groups and how to address them properly provides essential advantage to good communication.

Successful relationship is best initiated in person!

Attracting new constituents to the CSIRT will often need more than a public website or a brochure, and e-mail is hardly the best choice to make a first impression.

Meeting constituents face-to-face on a regular basis or at least for initial contacts is still crucial for successful co-operation. Even in today's networked world, people are more open and willing to work together when they have had a chance to meet in person.

Contacts established in person will help to gain trust, clarify most questions up-front and will help to adjust further communication and services to the needs of the constituent.

The analysis of CSIRT communication and information distribution methods must answer the following question: What, how and when should be communicated with constituents?

Answers to this question and all the above should form the CSIRT communication strategy.

External help can be used, if necessary, to get the communication strategy right and to make it as clear and simple as possible. This strategy must reflect on many aspects of the CSIRT, such as its goals, achievements, external look and feel, and mission statement.

Different messages call for different communication channels!

Hard copy information

Experience shows that the majority of constituents still prefer information provided in a "conventional" way, that means printed. So it is always good to have something to physically give to the constituents. Additionally, it is a good idea to include the essential incident reporting contacts on these items as in times of need information provided only online could be unreachable for constituents.

The most common print material are

- Brochures
- Flyers
- Gadgets, pencils, stickers

Public Website

Publicly accessible information should cover:

- CSIRT mission and goals



- constituency definition
- CSIRT services
- Contact details
- Publicly available projects and papers

Closed member area on the Website

Secured information only displayed to constituents

- Sent bulletins
- Archive of all advisories
- Best practices
- (More granular) contact details

Web-forms for reporting incidents

Web-forms can provide a very well structured method for reporting incidents to the CSIRT team. Constituents can be instructed to fill in all the right information required for solving the incident without accidentally omitting crucial details.

The CERT/CC developed widely used templates in text form¹⁷ and in interactive form¹⁸.

Mailing lists

Mailing lists provide a highly efficient way to distribute e-mail to many people. CSIRT can address various target groups through different mailing lists and/or constituents can refine this communication by subscribing only to lists that are most relevant to them.

SMS /text messaging

In case of emergencies such as major infrastructure outages or as an extra service it's a good alternative for informing constituents that there is something going on and that they have to check their email or contact the CSIRT.

Video conferencing /VOIP

Video conferencing and VOIP techniques have become increasingly more convenient and more affordable in the last few years. It's something to get used to, but videoconferencing can add a more personal touch than voice alone.

Chat

Chat is a very fast and efficient way to communicate with large groups or for searching for help online. Secured chat systems are also useful for quickly involving all crucial parties in case of more wide scale emergencies. Such environments are

¹⁷ Incident reporting at CERT/CC (text): https://www.cert.org/reporting/incident_form.txt

¹⁸ Incident reporting at CERT/CC (interactive): <https://irf.cc.cert.org>

best set up well in advance to interact with constituents and peers so that everyone is accustomed to using the system.

Public Forums

Public forums are beneficial for spreading general knowledge to the wider public. Running or assisting in running such forums increases publicity and helps with returning a service to the public.



A couple of things to consider when using mailing lists

Also the CSIRT itself can use external mailing lists for various reasons. Experience shows that, when subscribing to an external mailing list, it is best to use a different email address per subscription. This offers an easy way to manage all the various subscriptions with an email filter or to automate message handling within a system or tool. Mailing lists allow managing distribution networks for different groups and such groups must be carefully targeted.

Providing sensitive information over mailing lists

There are multiple options for providing sensitive information to the constituents.

The structure of the mailing lists and information classification scheme should be well organized before using them. For example, there could be following classification scheme:

- Secret
- Highly trusted
- Trusted
- Sensitive
- Public

For maintaining trust, it is a good practice to always sign messages and to use PGP-encryption for non-public messages. For available secure protocols please refer to the Annex.

Separation between different organisational roles, for example the Security officer and technician role, gives the opportunity to send out the email to a specific group that can be overseen and trusted.

Also, using different PGP-groups that corresponds to the information classification scheme, helps preventing possible mistakes.

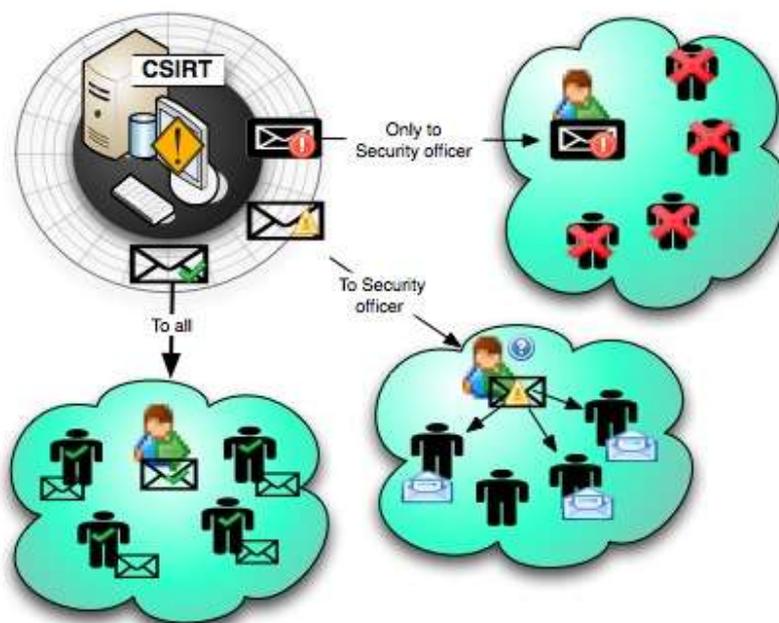


Figure 5. Mailing list distribution methods

As described in the figure above, mailing list can be used to address all the members within the constituency directly, or a security officer can decide on further distribution. The third option is to remain in control and to prevent accidental forwarding by addressing the security officer with his PGP key, so only he can read the message.

To prevent misunderstandings, the recipients should have clear understanding of dissemination restrictions when dealing with non-public information and classification labels should be used in such cases.

5.4.2 Communication events

This chapter describes some action points that can be taken into consideration while setting up a CSIRTs annual planning.

Marketing strategy

Have a marketing strategy ready. Which channels are available for the CSIRT and which ones could be used? For example: use of the media is often crucial and even unavoidable, but care must be taken as media may distort the messages. Also promotional actions could help.



Figure 6. The marketing mix

The marketing mix, also known as the 4 P's of marketing are:

- **P**roduct
- **P**rice
- **P**lace (distribution)
- **P**romotion

These “four Ps” help to control the marketing environment¹⁹. The goal of this model is to involve all the four aspects in the product approach, creating value and generating positive response to the product.

More information about the 4P's:

Several case studies for finding the correct marketing mix were made and are available online. For examples please refer to material provided by The Times²⁰, Fractal²¹ and the UK governments Business Link²².

¹⁹ Marketing mix at Wikipedia: http://en.wikipedia.org/wiki/Marketing_mix

²⁰ Case study at The Times 100: <http://www.thetimes100.co.uk/case-study--marketing-mix--83-244-5.php>

²¹ Case study at Fractal: http://www.fractalanalytics.com/casestudies/marketing_mix_modeling_casestudy.pdf

²² Case study by Business Link: http://www.businesslink.gov.uk/Promotions_files/businesslinkgovuk_run.pdf

Awareness campaigns

Contributing to the security awareness of the constituents and the general public is a good preventive practice that helps to generate positive publicity and is always a valuable investment in a long run. A good start is to share the lessons learned. It contributes to the knowledge of others and lets the constituents get the appreciation of what the CSIRT is doing for them. For peers and more technical audience sharing an expert paper and organising an expert session might be a good approach.

Knowing the constituency

Building up knowledge about the constituents is essential for delivering the right services. Important are not only the technical details like the contact information and the technical environment of the constituents, but also the bigger picture, like how they conduct their business, for example.

Unifying information

Getting all the information about constituents structured and stored in a database makes the information much easier to process. This needs to be taken equally seriously when launching a new system or when consolidating legacy systems.

Exercising with constituency and other CSIRTs

It is important to exercise the possible scenarios of what could happen or has happened and to highlight the lessons learned. Exercises are very useful for clarifying the roles and actions of parties involved in incident handling.

Co-operation between CSIRTs on national level and with the rest of the world

Efficient co-operation between the CSIRTs in many countries is often essential for mitigating even fairly limited incidents and more so when the scope of the issue is larger. It is a good investment to interact and collaborate with as many peers as possible. Collaboration works best when both sides benefit from it.

Enhancing 'new' relationships outside the CSIRT community

It is extremely valuable to invest into relationships surrounding the CSIRT realm of operations, such as:

- Law enforcement
- Professional organizations involved with security issues (Bank associations, ISPs, ISAC's)
- Professional organizations, outside the security community (chambers of commerce, consumer communities)
- Other security service providers (abuse-teams, WARPS, NOC's)
- Regional/Local/domestic cooperation between CSIRT. (CERT-Verbund, o-IRT-o, UK-CSIRT en other initiatives).

If such network of interactions is not in place, it needs to be built!

5.4.3 Quality and satisfaction reports

Question

How to stimulate cooperation with the constituents and to make them part of the CSIRT's success?

Knowledge through measurement!

It is important to query the constituents about their experiences with the services that the CSIRT provides. A good and mostly appreciated thing is to conduct questionnaires on a quarterly or half-year basis. The outcome and proposals for improvement should be honestly communicated in return.

This can be followed up with meetings or (annual) reports where improvements made (based on constituents feedback) are presented.

This helps to build up a very direct relationship to the constituents and to provide them trust and commitment through their own involvement in the CSIRT's development.

Examples of public periodic reports of CSIRTs:

The Swedish IT Incident Centre:

<http://www.sitic.se/publikationer>

CERT-FI (Ficora from Finland)

<http://www.cert.fi/en/reports.html>

German BSI

<http://www.bsi.de/literat/jahresbericht/index.htm>

GovCERT.NL

<http://www.govcert.nl/render.html?it=135>

Statistics provided by CSIRTs:

CERT Polska

<http://arakis.cert.pl>

CERT/CC

<http://www.cert.org/stats/>

Special reports on security matters:

Australian Computer Crime and Security Survey

<http://www.uscert.org.au/crimesurvey>

5.5 Building up a community among the constituency

Question

How to build an active community among the constituency that will support the CSIRT in reaching its goals?

First, it is necessary to build a solid relationship to the constituency, and only then it is possible to start exploring what can be done in order to build a community.

5.5.1 How to build a constituent community?

Building a community is hard work, but a worthy investment. It needs a lot of energy to start and keep it going.

Some tips are described below:

Being a “power listener”

Listening is as important as talking (if not more). These dialogs with the constituency must be maintained live for continuous feedback. And most importantly the feedback must be acted upon.

Using marketing skills

This isn't a pure marketing job. This isn't to create sales. It's about constituent care and constituent relationships. Marketing lingo is not necessary here. Instead, it is important to be transparent, open and honest.

Getting the whole CSIRT staff onboard

It takes more than a team leader or just a PR person to build strong ties with the constituency. Every area that the constituents interact with should be given serious consideration. If one department fails to give outstanding service or gives the constituent a negative experience or simply fails to communicate the whole CSIRT success could be affected.

Being open and accessible

It shows openness to constituents when they can approach the CSIRT staff through their direct phone numbers and real email addresses. Hiding behind the voicemail and an email alias might result in missing a great opportunity for building stronger bonds with key constituents. Another way to show openness is to provide VIP tours and to arrange meetings with constituent.

Having a passion for the task

Believing in what the CSIRT does and being passionate about the services it delivers is a good way to earn the trust of the constituents.

5.5.2 Community needs a leader

Although it seems to be merely a group effort, **it takes a strong leader or moderator to build a community.**

Depending on the goals, the community can be organized in a more organic or tighter group in the beginning. Facilitating gives more influence into carefully guiding the group towards the (adjusted) group goals.

When everything seems to go naturally (without any effort) then the direction must be right!

Leader should still be aware if the topics discussed with the group are that of the group or that of the leader only.

It is worth to take a look at the (Warning, Alerting and Reporting Point) WARP²³ website. WARP concept is built around the community effort to address security matters within a group that already shares other common interests and a common “language”. Still, as with any organized effort, practice shows that WARPs need a good “champion” to get them going and to sustain their momentum.

CSIRT surroundings analysis, covered earlier, probably brings out several groups and associations within and outside the constituency that could take of use the WARP concept.

5.6 Review of the service portfolio

The needs of the constituents depend on many factors such as skill level, ICT usage, resource availability and other things.

ENISA’s working group on “CERT Services”²⁴ in 2006 discussed what basic services could be needed for different user groups.

Question

How do I determine the right services for my constituents?

The working group made a distinction between the following users of CSIRT services.

1. Home user - beginner
2. Home user - Intermediate
3. Home user - expert
4. SME
5. Enterprise

²³ WARPS: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

²⁴ ENISA ad-hoc working group CERT Services:
http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm



- 6. Academic
- 7. Government

All defined groups had a different need for ICT Security services. We based ourselves on the available and comprehensive CERT/CC CSIRT services listing and came up with five basic services that most CSIRTs “should” deliver.

- 1. Alerts, Advisories and Warnings. (Short term information)
- 2. Incident management
 - Security incidents
 - Malware handling
 - Forensic, data recovery
- 3. Vulnerability Handling /mgt.
- 4. Security Operations
- 5. Security Quality Management
 - Auditing
 - Certification
 - Policy development
 - Educational activities
 - Best practices
 - Training
 - Long-term information

This matrix gives an overview and focus on what services to deliver and to whom to target. For the detailed list see Annex 9.6 CSIRT Services.

The area “which users need what services and how” must be further examined, starting with an ENISA study about “User needs for CSIRT services” carried out and delivered end of 2007 (as part of the Work Programme 2007).

5.7 Managing developing expectations

Question
How can a change in expectations be detected?

Different expectations can be positive if managed as soon as they appear and if they are handled swiftly. The positive approach is that constituents get involved and demands more attention!



Usually the differences and trouble arise when there is a lack of communication between the involved parties.

Constant “monitoring” of the constituency is necessary!

Keep talking to the constituents and explain what the CSIRT can deliver and what is expected of constituents themselves to serve their needs. Be open and transparent in your communication and the most important rule:

Deliver the promised!

Over ambitiousness is even worse than having a small set of services in the portfolio. With a busy (and in a lot of cases understaffed) CSIRT it is hard to manage the everyday work with even the basic set of services. Experience shows that it is better to offer a limited (and manageable) set of services to the constituency, and to make sure that the services provided have a high quality, instead of trying to deliver “everything” and risk failing during delivery.

As always, when doing business it is a thin line of balancing between expectations and delivery. CSIRTs should keep it open and transparent and involve the constituency as much as possible.

6 CSIRT external relations: CSIRT communities

Co-operation among security teams, not only during incident handling, is essential. Even though a couple of cooperation activities around the globe exist, there is room for improvement. On a more abstract level various co-operation approaches for CSIRT teams is covered in ENISA study “CERT cooperation and its further facilitation by relevant stakeholders”²⁵ from 2006.

A broader set of agreed standards in various areas (like standard NDAs, standard SLAs, collaboration agreements, agreed procedures for information sharing, data exchange formats, etc.) will help to enhance the level of cooperation. When talking about cooperation it must be kept in mind that CSIRTs are not the only providers of security services. WARPs for example get more and more important, as their role as information sharing facilities among small communities of users makes them well suited for bridging various gaps. CSIRTs and WARPs can learn a lot from each other, and so mixed events or even staff exchange among them might be very beneficial. Agreements and advanced exercises that include parts of the WARP and the CSIRT communities will add benefit to network users on various levels. But what is valid for CSIRTs and WARPs is also good in other areas: interdisciplinary collaboration is a key component of an overall enhancement of internet security and in the end for the establishment of a culture of security in Europe and beyond. CSIRTs for example should meet with law enforcement entities (that relationship is already slowly evolving), abuse teams and WARP people could explore fields of common interest and mutual benefit, etc. And finally the importance of regional cooperation initiatives (as pointed out in the ENISA study) must be stressed: if they do not exist in a country than they have to be set up. There are already various regional and national cooperation activities in place that can provide good practice in setting up such an activity.

Keywords:

- Standardisation
- Interdisciplinary collaboration
- Information and Resource Sharing
- Regional cooperation

Question

What are the surroundings that influence the operations of a CSIRT?

SWOT and PEST analyses, mentioned earlier, help to summarize essential contacts and essential environments for the CSIRT. It's important to investigate and research them on a periodic base to answer the following questions:

- Are external contacts best utilized and beneficial enough?
- Are there gaps?
- Are all groups covered?

²⁵ ENISA study CERT cooperation: http://www.enisa.europa.eu/cert_cooperation/

- What areas can be influenced?
- Do these interactions provide all the input needed for serving the constituents?
- Do any services need adjustments?

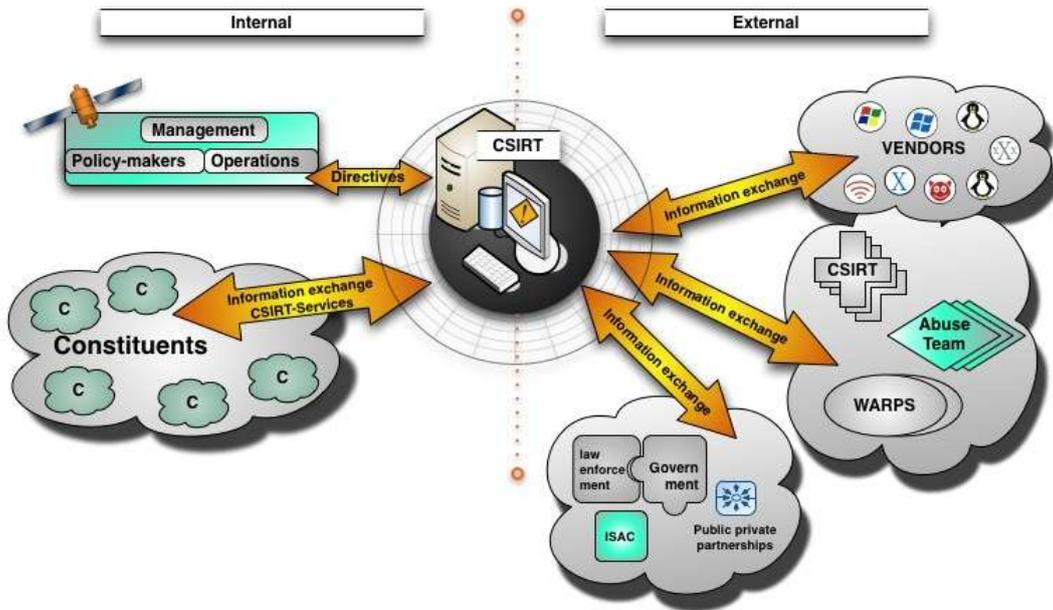


Figure 7. Possible Surrounding of a CSIRT

The above picture shows the possible relationships a CSIRT could have.

Besides external contacts also internal contacts and their expectations need to be addressed:

- Steering committee / sponsors
- Management and Team
- Internal relationships
- Technical and non-technical staff
- Constituency

Within the CSIRT community there are several CSIRT groups that organize information exchange and periodic meetings. These gatherings are necessary for building and maintaining the ties with the rest of the CSIRT community.

TF-CSIRT²⁶

Computer security incidents require fast and effective responses from the organizations concerned. Computer Security Incident Response Teams (CSIRTs), either internal or outsourced, are service providers responsible for receiving, reviewing and responding to computer security incident reports and activity. The TF-CSIRT task force promotes the collaboration between CSIRTs at a European level.

FIRST²⁷

FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents – reactive as well as proactive.

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

WARP²⁸

A WARP is a community-based service where members can receive and share up-to-date advice on information security threats, incidents and solutions.



Experiences from practice

With the start of the Dutch Govcert.NL a research of CSIRT surroundings from various perspectives have been made. The focus of this research was “Is it beneficial to start a Governmental CSIRT in the Netherlands and under what conditions”. All thinkable surroundings were investigated:

- Who could the target groups (constituents) be; who is “waiting for a governmental CSIRT?”
- Future constituents, creating a development/acquisition path
- Existing Public groups
- Possible public private partnerships
- What CSIRT services are needed and wanted?
- Where is a short of knowledge and where could people benefit of sharing best practices and knowledge?
- Sponsors; who could help in the starting phase?

²⁶ Terena’s Task Force CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

²⁷ Forum of Incident Response and Security Teams: http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm

²⁸ Warning, Alerting and Reporting Points: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

This research took some time, but was essential in building up focus and writing the business case. It also directly gave a direction on acquisitioning the right constituents and contacting the essential specialists and existing CSIRTs in the field.

Knowing who is surrounding the CSIRT environment and how they connect to each other is essential in doing swift business and make as much impact as possible with the minimal (efficient) use of existing resources²⁹.

6.1 Legal basis for collaboration

Due to a wide diversity in the legislation around Europe there is still a lack of standardized collaboration documents for the different CSIRTs, and most companies have their own legal requirements.

Question

What are the most beneficial standard documents?

Investing in thorough and standard agreements saves time and money in the long run. It is also one of the most important steps in expectation management and in setting borders for the constituents. They need to know what to expect and this allows the CSIRT to commit to delivering exactly what is promised.

Below are some examples that are usable and easy to adapt to the needs of the CSIRT.

All documents must be checked by a legal department or the legal staff before publishing them.

6.1.1 Standard Non Disclosure Agreement (NDA)

The NDA is one of the most important documents in the CSIRT business. Taking care of information, delivering and handling it under agreed conditions is the key to gaining trust of the fellow CSIRTs and constituents.

A non-disclosure agreement (NDA), sometimes also called a confidential disclosure agreement (CDA), confidentiality agreement or secrecy agreement, is a legal contract between at least two parties which outlines confidential materials or knowledge that the parties wish to share with one another for certain purposes, but wish to restrict from generalized use. In other words, it is a contract through which the parties agree not to disclose information covered by the agreement. A NDA creates a confidential relationship between the parties to protect any type of trade secret. As such, a NDA can protect non-public business information³⁰.

For example the Austrian venture capital firm TVP uses an industry standard NDA which can be used to formally notify other of the confidentiality of the materials (see FAQ on usage).

<http://www.tvp.com.au/ip/NDA.pdf>

²⁹ CERT-IN-A-BOX: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#02

³⁰ From ENISA's study CERT cooperation: http://www.enisa.europa.eu/cert_cooperation/pages/05_02.htm

6.1.2 Standard Acceptable Use policy (AUP)

FIRST³¹ provides a template for an Acceptable Use Policy:

http://www.first.org/resources/guides/aup_generic.doc

The document is an Acceptable Use Policy that can be used as a template. The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources in conjunction with its established culture of ethical and lawful behaviour, openness, trust, and integrity.

6.1.3 Terms of Reference

A Terms of Reference (ToR) is a document that describes the purpose and structure of a project. Otherwise known as a TOR or a Project Charter, the Terms of Reference is created during the initiation of a project management life cycle. Creating a detailed Terms of Reference is critical to the success of an association, as it defines its purpose of existence:

- Vision, objectives, scope and deliverables (i.e. what has to be achieved)
- Stakeholders, roles and responsibilities (i.e. who will take part in it)
- Resource, financial and quality plans (i.e. how it will be achieved)
- Work breakdown structure and schedule (i.e. when it will be achieved)

A good example is the ToR of Terena's Task Force CSIRT³², that can be reviewed online:

http://www.enisa.europa.eu/cert_cooperation/pages/10.htm

6.1.4 Standard Service Level Agreement (SLA)

A Service level Agreement helps the CSIRT to reflect what is promised to deliver and under what conditions. It should be considered as a more detailed operational working relationship document.

An example from SUN Microsystems can be found online:

<http://www.sun.com/blueprints/0402/sla.pdf>

6.1.5 Collaboration agreements

Memorandum of Understanding

A Memorandum of Understanding (MOU) is a legal document describing a bilateral agreement between parties. It expresses a convergence of will between the parties, indicating an intended common line of action, rather than a legal commitment. It is a more formal alternative to a gentlemen's agreement, but generally lacks the binding

³¹ FIRST: http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm

³² TF-CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04.htm



power of a contract. As an example of a MoU see the TF-CSIRT/AP-CERT agreement:

http://www.enisa.europa.eu/cert_cooperation/pages/09.htm

Bilateral team-team cooperation

Cooperation between CERTs may assume different legal bases. Cooperation between teams (especially in the team-team model) can obviously be informal in many cases. If there is a need to formalize the cooperation, it can assume different legal forms that we list in this chapter. The motivation for formalizing cooperation may be the involvement of funds, fulfilling legal requirements or the exchange of sensitive data.

Contract

A contract is a "promise" or an "agreement" made of a set of promises. Breach of this contract is recognised by the law and legal remedies can be provided. In civil law, contracts are considered to be part of the general law of obligations. The law generally sees performance of a contract as a duty.

7 CSIRT internal management

This chapter describes the daily necessities needed in order to have an operational CSIRT team that functions well.

Question

How to manage the CSIRT internally?

When a team reached a level of expertise and experience where daily work is mostly daily routine without or with very few surprises, it might be the time to think about measures that make work more interesting, challenging or rewarding again. Advanced training, certifications that improve a CV, broadening of scope (offering new or enhanced services or assignment of new tasks to staff members), and an overall improvement of working environment and atmosphere will be useful to (re-)motivate the staff and, as a consequence, enhance the quality of the provided services.

Following starting conditions should be in place:

- Clear and approved task definition
- Clear and delimited mandate
- Clear and delimited responsibility
- Good legislation framework in place
- What are the success factors of the CSIRT?
- Have the right people on board with the right attitude and spirit
- Execute the communication plan
- Join (inter) national organizations

It is necessary to be clear about what are the do's and don't for the CSIRT.

It is also important to be aware of the responsibilities and of the limited time and the risk of making mistakes.

7.1 (Re)assuring the mandate

As mentioned in earlier chapters, it's essential to organize the sponsors or budget owners. Without them it's going to be hard to survive, so experience shows to have a strategy available for convincing them and for keeping them satisfied is a good practice, as much as gaining their trust in order to have as much level plain field as possible to operate in.

Ask questions and invest in the relationship, find out what is important for them and how they want to be informed and what the boundaries are for the CSIRT operation!

Have it sorted out beforehand; during operational crisis or incidents there will be no time for that!

Internal relationships

- Steering committee / sponsors
- Management and Team
- Technical and non-technical staff
- Constituents

Managing changes in mandate in a CSIRT in full operational business will be challenging. There is a lot of pressure and ad hoc tasks that have to be executed in a short amount of time, leaving limited time for framework and organizational discussions.

7.2 CSIRT organizational structure

Question

CSIRT needs a clear structure and transparent responsibilities – but which?

When taking in new constituents, having a change in the mandate or having doubts about the organizational status of the team, it is necessary to invest some time and effort to straighten the CSIRT structure out first. It's worth looking at the organizational structures and to compare them to the existing CSIRT organization. Are all the roles and responsibilities recognizable and clear to all team members?

Before serving its constituents the CSIRT must have its framework solidly in place.

As described before in the ENISA guide on how to set up a CSIRT³³ document there are different ways of organizing the CSIRT. Following is a short overview:

7.2.1 Possible structures for CSIRTs

Independent business model

CSIRT organized as an independent organization with its own staff.

³³ ENISA CSIRT Setting up guide: http://www.enisa.europa.eu/cert_guide/

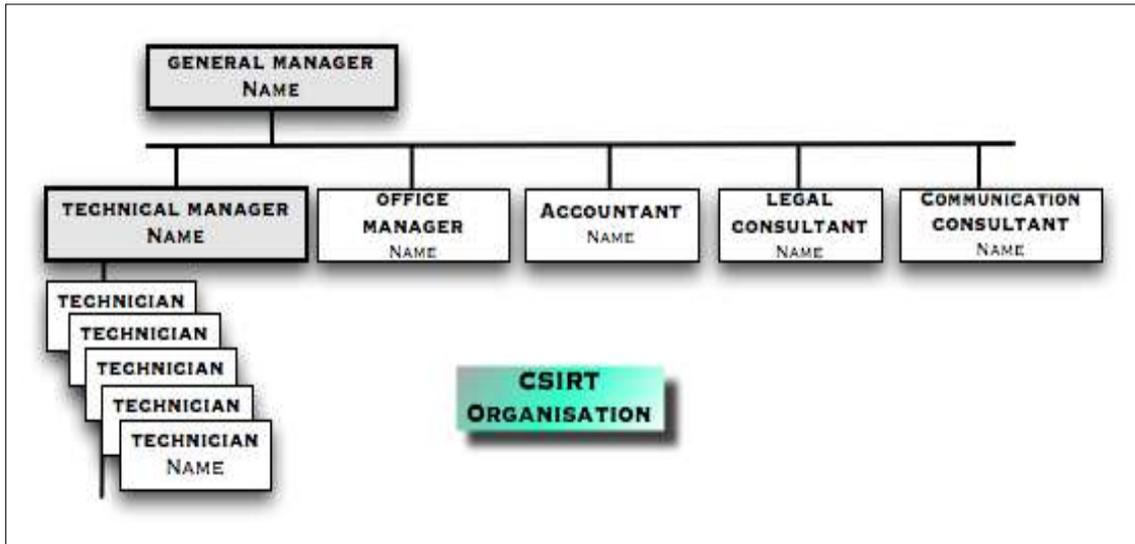


Figure 8. Independent business model

Organisational embedded model

This model can be used if the CSIRT will be part of a bigger, already existing organization.

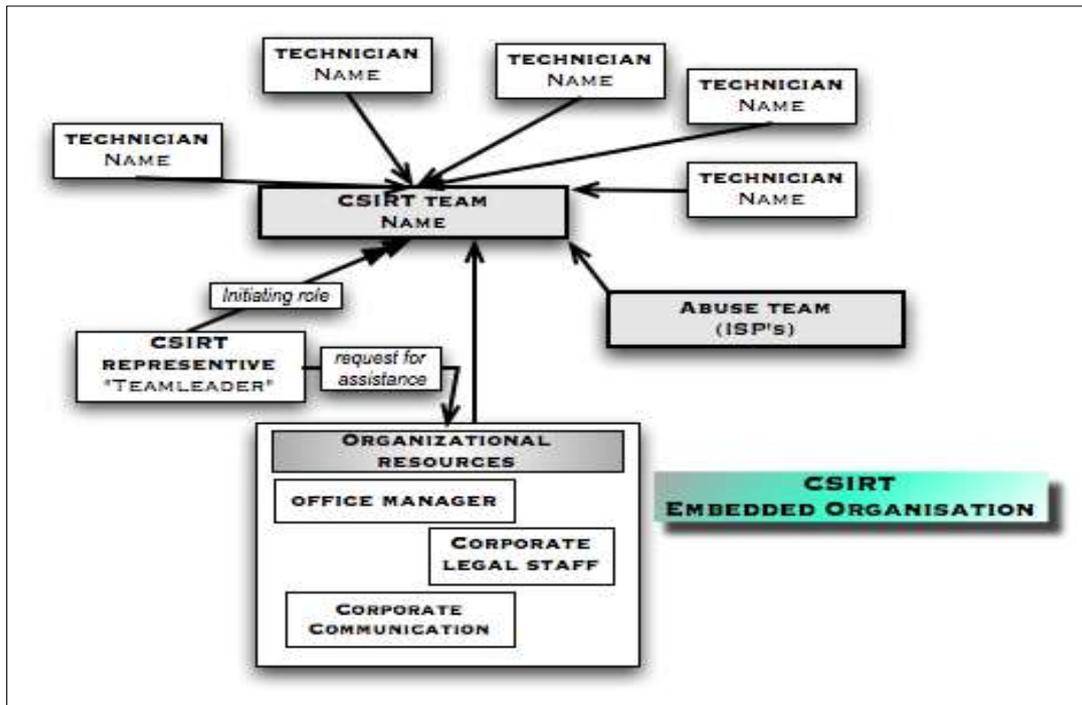


Figure 9. Organizational embedded model

Campus model

A model that can be used when the organization is comprised of various facilities at different locations spread over a country or region. They are mostly independent entities and they are organized under the umbrella of the 'Mother' or Core CSIRT.

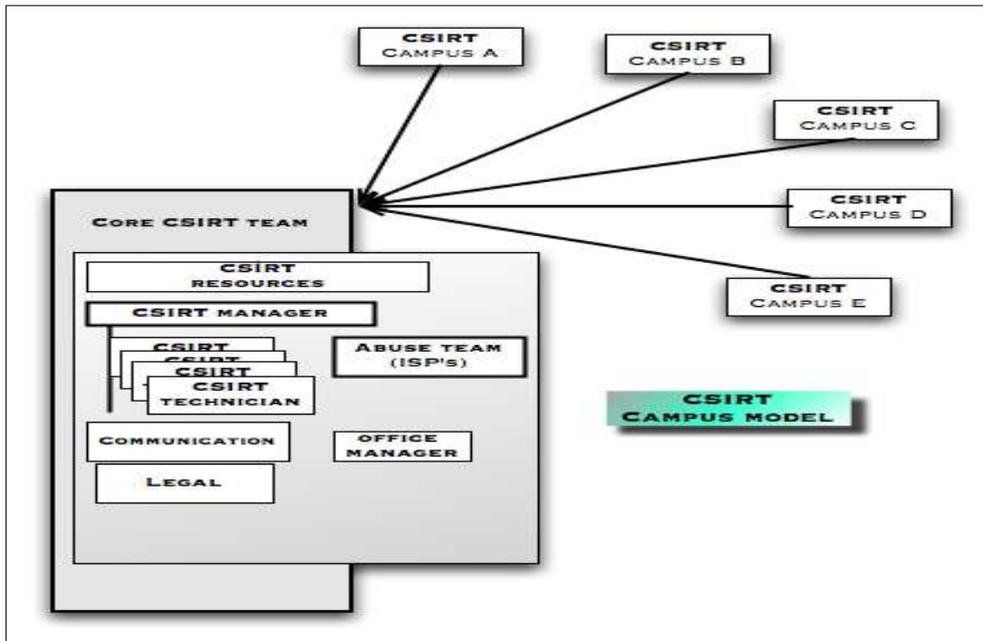


Figure 10. Campus model

Voluntary model

Within this organizational model a group of people/specialists join together to provide advice and support each other on a voluntary basis. It's a loosely fitted community.



Figure 11. Voluntary model

7.3 CSIRT team roles and staffing

Question

What team roles should exist within the CSIRT?

Many CSIRT teams start only with a few people, but there are many roles to be filled. As the team and services mature, various roles need may more attention.

A CSIRT could have following roles within the CSIRT-team:

General

- General manager

Staff

- Office manager
- Accountant
- Communication consultant
- Legal consultant

Operational Technical team

- Technical team leader
- Technical CSIRT technicians, delivering the CSIRT services
- Researchers

External consultants

- Hired when needed.

Staffing considerations

It is good practice from time to time assess the workload and the existing resources (team members) to see if planning still match's reality. If the workload is too heavy, new staff must be planned in. An alternative to hiring new staff can be to recruit already employed experts from other parts of the hosting organisation (like helpdesk, documentation, legal, or other specialists).

Keywords:

- Workload (too much or too little)
- Service portfolio
- Promotion
- Service quality

It is extremely helpful to have a **legal specialist** on board, especially during the starting of the CSIRT. At the end of the day it saves time and it also keeps the focus on the legal do's and don'ts when starting new projects and products for the CSIRT.

Depending on the CSIRT and constituents, it could be very beneficial to also have a **communication expert** on the team. Such expertise is useful in translating difficult technical issues to a language that is readily understood by the constituents and media-partners. These skills should be transferred to other staff members as well, and a consultant can help this process by providing training on the job.

Overall staff welfare

Also in periods of high workloads team members must be treated like human beings with families, own wishes and needs, etc. Team building is an important factor, especially for CSIRTs where only the team as a whole can be successful. A periodical staff survey and personal talks between team leader and members is necessary to early spot potential problems, for example in internal communication. If the team can not solve their problems internally, an external professional consultant, who can provide an independent perspective, may be helpful.

Keywords:

- Team building
- Feedback
- Personal talks

Treat the CSIRT staff as a normal business department, go drink beer and socialize!
Have a normal staff evaluation structure! **Take care of the staff!**

Defining the organizational structure of the CSIRT depends on the existing structure of the organization. It also depends on the accessibility of skills that should be permanently available to the CSIRT or which can be used on an ad-hoc basis.



For maintaining good grip on the team, it is good to conduct weekly meetings with the operational staff and at least a monthly meeting with all of the CSIRT staff.

7.4 Training and education

Question

What kind of training needs should be addressed?

Keywords:

- Career building
- Certification
- Advanced training, also non-technical
- Soft skills

In most cases acquiring CSIRT knowledge is received on the job. However, being part of the daily business it's something that tends to slip easily.

It is a good practice is to have elaborated procedures in place to smooth the introduction of newly hired staff, including appointing a senior team member as mentor, guided tours through the premises, introductory training for the workflows and tools, etc.

A good way to start training new employees internally is to organize the existing knowledge within the CSIRT into the mentioned procedures and course materials. An added benefit of conducting internal training is that it highlights the areas where the CSIRT already has acquired extensive knowledge and allows the staff to become better trainers themselves.

Becoming a good speaker and a trainer is important for the CSIRT staff members involved in these activities. Good communication skills are also crucial for working with the constituents and the general public and for contributing to their awareness and security practices.

The basic education of new CSIRT employees should at least consist of the following subjects:

New staff Information package

- Existing procedures, basic education.
- New constituents procedure
 - How to connect a new constituent
 - What information is needed
- Constituent handling training
 - Helpdesk training
 - Stress management

As a reward for good performance, new operational staff could also attend the external TRANSITS training, listed at the end of the chapter.

Optional but most handy types of training

Due to their technical nature, CSIRTs often address technical training first, but “soft” skills and people skills should not be neglected. Following are the examples of some of these “soft” skills:

- PR training
 - Selling CSIRT services
 - “Elevator pitch”
- Project management
- Building a business case
- Training the surrounding environment
 - Training involved parties (law enforcement, justice, politicians, forensic)
 - Training people and groups that directly influence the CSIRT (Managers, CEO-level, decision makers, money makers)

External training

Most employees feel appreciated when managers invest in their knowledge and skills by organizing courses for them.

Providing external training for staff members is very beneficial, although it may affect the availability of sufficient staffing for several days.

Other ways of acquiring skills

In a lot of cases CSIRT staff members are most of the times very focused on their CSIRT technical operation. Aside from the official training courses, meeting other people in the field, exchanging information and establishing contacts is very fruitful to the CSIRT and builds a stronger bond with the constituents and peers. This can be achieved also through staff exchange with organizations surrounding the CSIRT realm.

For example, sending staff member to work with a WARP or an abuse team within a constituency may help to bring them up to speed and to learn about the constituency needs at the same time.

Existing training materials, courses and guides:

Terena TRANISTS (Training of Network Security Incident Teams Staff)
<http://www.ist-transits.org/>

Highly recommended, focused CSIRT training with secondary benefits, establishing new contacts and colleagues and exchanging experiences, knowledge

FIRST <http://www.first.org>
<http://www.first.org/resources/guides/>

SANS <http://sans.org/>

CERT-CC <https://www.vte.cert.org/vteWeb>

Local technical training courses:

- System Hardening
- Computer Forensics
- Programming languages

7.5 Certification possibilities for the CSIRT staff

A certificate reached through training and proving experience, skills and knowledge in exams are highly sought after additions to the personal CV of most CSIRT staff members. Below can be found some references to documents dealing with certification for IT security staff:

- RFC 2350 - Expectations for Computer Security Incident Response
<http://www.ietf.org/rfc/rfc2350.txt>
- Handbook of Legal Procedures of Computer and Network Misuse in EU Countries for assisting Computer Security Incident Response Teams
<http://www.csirt-handbook.org.uk/>
- CERT®-Certified Computer Security Incident Handler
<http://www.cert.org/certification/>
- CISSP – Certified Information Systems Security Professional
<https://www.isc2.org/>

7.6 Benchmarking

Benchmarking³⁴ can be used to assess and really understand performance by comparing with others in the same field.

Benchmarking keeps the organization vigilant to its performance and offers a way to collect new ideas, methods and tooling, thus, improving effectiveness. Benchmarking can also act as a lever for new services and strategies.

Competitive benchmarking is

1. A better understanding of customer's expectations that is based on the real market and estimated in an objective way
2. A better economic planning of the organization's objectives through focusing on what takes place outside of the organization
3. A better increase of the productivity: resolving real problems and understanding of the processes and their impact
4. Improving current practices and a search for the change.
5. Higher competitiveness thanks to: a solid knowledge of the competition, a strong implication of the staff, new ideas on practices and tried techniques
6. Benchmarking has consequences that go beyond the process itself: it reforms all the levels of the organization
7. Modifies the process of manufacture of the product leads (drives)
8. Also reforms the hierarchical organization of the company, the product itself, and the state of mind of the employees.

Procedure

Re-using the SWAT and the PEST analyses (please refer to chapter 5.1) helps to identify the problem areas and the most critical parts of the CSIRT.

The following techniques can be used:

Informal conversations with customers, employees, or suppliers;

- In depth Marketing Research³⁵
- Qualitative Marketing Research³⁶
- Quantitative Marketing Research³⁷
- Focus Groups³⁸

³⁴ Benchmarking at Wikipedia: <http://en.wikipedia.org/wiki/Benchmarking>

³⁵ Marketing Research at Wikipedia: http://en.wikipedia.org/wiki/Marketing_research

³⁶ Qualitative Marketing Research at Wikipedia: http://en.wikipedia.org/wiki/Qualitative_marketing_research

³⁷ Quantitative Marketing research at Wikipedia: http://en.wikipedia.org/wiki/Quantitative_marketing_research

- Statistical Surveys³⁹
- Questionnaires⁴⁰
- Reengineering analysis, process mapping, quality control variance reports, or financial ratio analysis⁴¹.



Identifying other industries that have similar processes

It could be very fruitful to enlarge the scope and to look for similarities outside the CSIRT and even ICT business. Good examples are businesses with high-risk operations and a high level of security awareness and procedures, such as critical infrastructure providers. Even if they are not directly related to ICT security, these industries likely have a lot of working experience within security and awareness matters.



Identifying organizations that are leaders in the field

The very best in any industry and in any country must have some special aspects to their success. Customers, suppliers, financial analysts, trade associations and magazines may help to determine which companies are worth studying.



Using surveys of companies for measures and practices

Companies target specific business processes using detailed surveys of measures and practices used to identify business process alternatives and leading companies. Surveys are typically masked to protect confidential data by neutral associations and consultants.

Some examples from anti-virus vendors:

McAfee: http://www.mcafee.com/us/local_content/misc/sage_0407.pdf

Symantec: <http://www.symantec.com/enterprise/library/>



Visiting the "best practice" companies to identify leading edge practices

Companies typically agree to mutually exchange information beneficial to all parties in a benchmarking group and share the results within the group.



Implement new and improved business practices

Take the leading edge practices and develop implementation plans which include identification of specific opportunities, funding the project and selling the ideas to the organization for the purpose of gaining demonstrated value from the process.

³⁸ Focus Groups at Wikipedia: http://en.wikipedia.org/wiki/Focus_group

³⁹ Statistical Surveys at Wikipedia: http://en.wikipedia.org/wiki/Statistical_survey

⁴⁰ Questionnaires at Wikipedia: http://en.wikipedia.org/wiki/Questionnaire_construction

⁴¹ Reengineering at Wikipedia: <http://en.wikipedia.org/wiki/Reengineering>

Cost of benchmarking

Benchmarking is a moderately expensive process, but most organizations find it's worth their money. Main costs are:

- Visit costs
- Time costs
- Benchmarking database
- Evaluation, comparing services

7.7 Continuously staying up to date

It is important for a CSIRT to constantly collect trend and vulnerability information for the constituents' systems. As described in the document "A step-by-step approach on how to set up a CSIRT"⁴², the CSIRT is collecting a lot of information from different sources.

Depending on the kind, relevance and severity of the information this information is distributed to the constituents in the appropriate format.

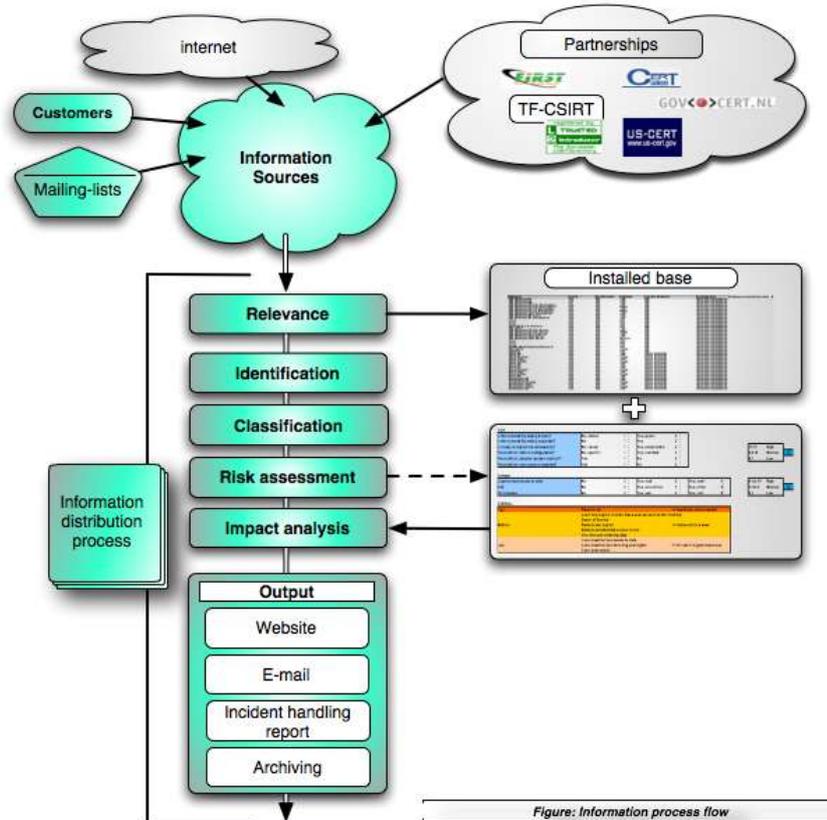


Figure 12. Information process flow

⁴² ENISA's CSIRT Setting-Up Guide: http://www.enisa.europa.eu/cert_guide/index_guide.htm



The 2nd ad hoc working group composed a list with information sources that most CSIRTs use in their daily watch routine, gaining vulnerability information and keep on track with new exploits and new techniques.

The full list prepared by the working-group is included in Annex 9.5.

8 CSIRT tools and equipment

Even the most basic tools do the job for quite a while when a team is young, enthusiastic and still has the impetus of starting operations. But after a while the shortcomings appear and have a more and more negative impact on the performance. Working with basic text editors and plain text files during incident handling is sufficient for a while, but when the numbers of handled incidents increases the hardship gets more and more important, and staff members start to write their own scripts to automate recurring tasks. The other extreme would be a team that starts operation with the most sophisticated tools which they can hardly use, because they have not been taught how to use the full complexity. In all cases after some time of operation the existing tooling should be assessed and necessary changes should be made. Custom tools may have to be built either by the team itself or an external programmer, but it is more economic to first evaluate the choice of existing tools. It is also important in improving tools to not discourage team members from further development of the new tools.

When it comes to working environment also the ergonomics of office equipment should be evaluated, especially when new staff arrives.

Keywords:

- Proper tooling
- Ergonomics
- Service improvement

This chapter shortly introduces some commonly used tools and practices for various tasks in the everyday work of a CSIRT, like:

- CRM tooling
- Incident handling tooling
- Standardizations of forms
- Handy software

Question

What tooling is needed and what are other teams using?

8.1 Incident tracking and reporting

AIRT: Application for Incident Response Teams

<http://www.airt.nl/>

Platform: Web based (needs PHP and Postgresql)

AIRT is an application for Computer Security Incident Response. The target audience of AIR is incident response groups which provide end-user support.



Request Tracker for Incident Response (RTIR)

<http://www.bestpractical.com/rtir/index.html>

Platform: Unix

Some teams in TF-CSIRT together produce a version of Request Tracker specifically designed for incident response work. The first beta release is now available for other teams to download. Mail addresses for bug reports, comments and suggestions, as well as a discussion list for CSIRT teams interested in using the product, can be found on the web page.

SIRIOS, system for Incident Response in Operational Security

<http://sirios.org/>

SIRIOS is a modular application framework designed for Computer Security and Incident Response Teams (CSIRTs) with main focus on incident management and vulnerability handling. It is licensed under the GNU General Public License (GPL). Download and use are free of charge. The core system is based on OTRS, an open-source trouble ticket system. The SIRIOS project was funded in 2003 by CERT-Bund, the German governmental CERT.

Jitterbug

<http://samba.anu.edu.au/cgi-bin/jitterbug>

Platform: Various web servers

Jitterbug is an open-source web-based tracking system. Problems can be reported through web forms or e-mail and authenticated users can classify them, add notes and reply to messages from within the system. Various documentation and demonstrations are accessible through the web page.

Remedy Action Request system

<http://www.remedy.com/>

Platform: Unix, Windows

Remedy is a commercial toolkit for building tracking systems. Remedy also sell applications, such as helpdesk and inventory tracking, which have been built using the toolkit; incident response teams have also used the system to build their own incident tracking and reporting applications.

8.2 Secure communication software

Pretty Good Privacy (PGP)

<http://www.pgpi.org/>

Platform: Unix, Windows

PGP, developed by Phil Zimmerman, is used to encrypt/decrypt mail or files with a mix of symmetric and asymmetric encryption. PGP is widely used by CSIRTs around

the world to communicate confidential/sensitive data. PGP will be further developed by pgp.com. A free version of older PGP(i)versions is available at the link above.

The GNU Privacy Guard (GPG)

<http://www.gnupg.org/>

Platform: Unix, Windows

GPG is a powerful alternative to PGP. Like PGP, GPG encrypts/decrypts mail or data with a mix of symmetric and asymmetric encryption. GPG is widely used by CSIRTs around the world to communicate confidential/sensitive data. GPG is a command-line tool, some graphical user interfaces and plug-ins for mail programs exist. German government sponsors the program.

Listserv

<http://www.lsoft.com/products/default.asp?item=manuals>

Platform: Windows

Listserv is a commercial mailing list package that can be used to maintain distribution lists for incident response teams.

Have a look and find the latest updates of useful CSIRT tooling at CHIHT – Clearing House for Incident Handling Tools.

Clearinghouse for Incident Handling Tools

This is a pilot site for a proposed collection of tools and guidelines of their use intended for incident handling teams. Information on this site reflects the experience of a number of European CSIRTs, working together as a project in the framework of the TERENA's Task Force TF-CSIRT.

http://chiht.dfn-cert.de/functions/csirt_procedures.html

8.3 Customer relationship management

CRM (Customer Relationship Management) is an information industry term for *methodologies, software, and usually support capabilities* that help an enterprise manage customer relationships in an organized way.

Methodologies

Experience shows that a good administration of the constituency is essential in doing accurate and efficient incident handling. It's not something that most technical people have as a second habit, but it's essential for business and information exchange!

It's like doing proper system administration, having a good, accurate and correct overview of the system hardware, software versions, location, network connectivity and physical entrance procedures.

8.3.1 What kind of information is needed for CRM?

Providing employees with the information and processes necessary for knowing their constituents, understand their needs, and effectively build relationships between the CSIRT, its constituent base, and distribution partners.

The question is what information is needed for delivering services correctly and in time to the constituents?

First it needs a good and clear overview of the services that the CSIRT wants to deliver to its constituents.

For now the focus will be laid on delivering the so called ‘core services’.

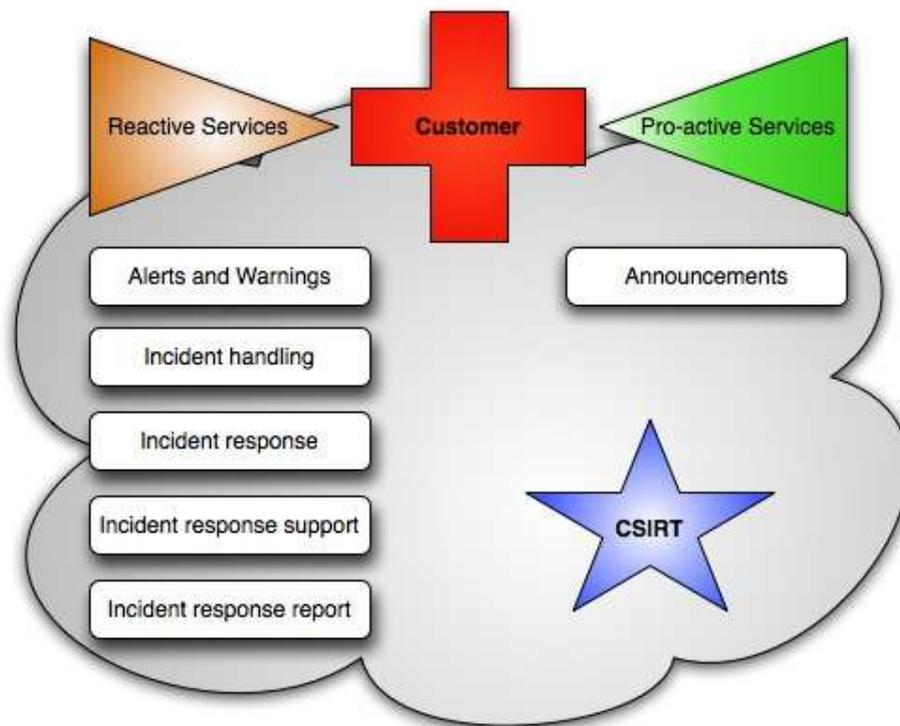


Figure 13. Customer relationship management

Service deliverance should be done by the credo:

Delivering the right services on the right time to the right persons!

Of course it all depends on the quality and accuracy of the information that is stored in the constituent’s records.

The following is a basis set of information:

1. Company/constituent information:

- Company name
- Organization / Department
- Visiting Address
- Post address
- General telephone number
- General fax number
- General information field
- *Amount of employees*
- *Kind of company (use predefined definitions)*
- *Budget*
- *Services to deliver*
- PGP-key

2. Contact person information

- Name (First – Last + degrees)
- Job Title(s)
- Responsible for ...
- Telephone number
- Mobile phone
- Fax number
- Email address (office / private)
- PGP-key
- Other contact information

3. Backup contact person information

- Name (First – Last + degrees)
- Job Title(s)
- Responsible for ...
- Telephone number

- Mobile phone
- Fax number
- Email address (office / private)
- PGP-key
- Other contact information

Other roles

- Communication contact person information
- Commercial leads
- Managers
- Management assistants

Other information

- Mailing list addresses

Most companies have a mailing list to inform their constituency and the broader public about news and ongoing activities.



Note: sending information to a group can be efficient, although it has to be realised that information is out of control of the sender. This is especially important to keep in mind before sending sensitive information out.

It's sometimes better to send information to persons directly, so and they can distribute the information according to the right non-disclosure agreements within their group. This way it is guaranteed that the right receivers are reached.

Another way is to have the information send out to the contact persons PGP-encrypted to the PGP-keys of the contact persons.

9 Annex

The Annex lists additional material that is referred to from various chapters.

9.1 ISO27001 / ISO27002

The international ISO/IEC 27001 and ISO/IEC 27002 standards give a bright and clear vision and show the necessity for adopting CSIRT capacity into every business model. The ISO27001 standard adopts and explains a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's **Information Security Management System (ISMS)**.

It's recommended to take notice of the standard and use it as much as feasible. It gives an organisation all best practices and guidance to organize information security in all aspects, therefore giving the constituents, when implemented, the assurance that all information is handled secure.

It relates the efforts to the international accepted standards and experience shows that is very useful to give the constituency confidence in the information management of a CSIRT.

9.2 CRM definitions and details

Below is listed more information about:

- Basic ingredients for CRM
- Using the collected CRM data for different purposes

An enterprise might build a database about its constituents that describes relationships in sufficient detail so that management, salespeople, people providing service, and perhaps the constituency itself can access information directly, match constituent needs with product plans and offerings, remind constituents of service requirements, know what other products a constituent has purchased, and so forth. According to one industry view, CRM consists of:

- Helping an enterprise to enable its marketing departments to identify and target their "best" constituents, manage marketing campaigns with clear goals and objectives, and generate quality leads for the sales team.
- Assisting the organization to improve telesales, account, and sales management by optimizing information shared by multiple employees, and streamlining existing processes (for example, taking orders using mobile devices).
- Allowing the formation of individualized relationships with constituents, with the aim of improving constituent satisfaction and maximizing profits; identifying the most profitable constituents and providing them the highest level of service.
- Providing employees with the information and processes necessary to know their constituents, understand their needs, and effectively build relationships between the company, its constituent base, and distribution partners.

There are three aspects of CRM, each of them can be implemented in isolation:

- Operational CRM: The automation or support of constituent processes involving sales or service representatives
- Collaborative CRM: Direct communication with constituents not involving sales or service representatives (“self service”)
- Analytical CRM: The analysis of constituent data for a broad range of purposes
- Active CRM: Comprehensive & Automatic

9.2.1 Operational CRM

Operational CRM provides support to "front office" business processes, including sales, marketing and service. Each interaction with a constituent is generally added to a constituents contact history, and staff can retrieve information on constituents from the database if necessary.

Focus on constituents' value is the key to a successful CRM strategy. Different constituents have to be treated differently. Variables like constituents' ranking, actual value and potential value are strategy drivers.

9.2.2 Collaborative CRM

Collaborative CRM covers the direct interaction with constituents. This can include a variety of channels, such as internet, email, or automated phone answering system. It can generally be equated with “self service”.

The objectives of Collaborative CRM can be broad, including cost reduction and service improvements. Driven by authors from the Harvard Business School (Kracklauer/Mills/Seifert), Collaborative CRM seems to be the new paradigm to succeed the leading Efficient Consumer Response and Category Management concept in the industry/trade relationship. Many organizations are searching for new ways to use constituent intimacy to gain and retain a competitive advantage. Collaborative CRM provides a comprehensive view of the constituent, with various departments pooling constituent data from different sales and communication channels.

Collaborative CRM also includes Partner Relationship Management (PRM) which enables organizations to manage their relationships with partners (consultants, resellers and distributors), and potentially the constituents of those partners

9.2.3 Analytical CRM

- Analytical CRM analyzes constituent data for a variety of purposes, including:
- design and execution of targeted marketing campaigns to optimize marketing effectiveness
- design and execution of specific constituent campaigns, including constituent acquisition, cross-selling, up-selling, retention
- analysis of constituent behaviour to aid product and service decision making (e.g. pricing, new product development, etc)
- management decisions, e.g. financial forecasting and constituent profitability analysis
- Risk assessment and fraud detection for credit card transactions
- Analytical CRM generally makes heavy use of Predictive analytics

9.2.4 Strategy

Several commercial CRM software packages are available which vary in their approach to CRM. However, CRM is not just a technology, but rather a holistic approach to an organization's philosophy in dealing with its constituents. This includes policies and processes, front-of-house constituent service, employee training, marketing, systems and information management. CRM therefore also needs to consider broader organizational requirements.

A company's CRM strategy is dependent on both the company's current situation and the needs and expectations of its constituents.

9.2.5 Technology considerations

The technology requirements of a CRM strategy are very complex and far-reaching. The basic building blocks include:

- A database to store constituent information. This can be a CRM specific database or an enterprise data warehouse.
- Operational CRM requires constituent agent support software.
- Collaborative CRM requires constituent interaction systems, eg an interactive website, automated phone systems etc.
- Analytical CRM requires statistical analysis software, as well as software that manages any specific marketing campaigns.
- Support CRM systems require interactive chat software to provide live help and support to web site visitors.

9.3 Building a community

More examples for building up communities:

Community Building Resources (prepared by The Benton Foundation)

Learn from others in the field

<http://www.benton.org/publibrary/practice/community/communitytips.html#learn>

Research online communities

<http://www.benton.org/publibrary/practice/community/communitytips.html#research>

Begin planning an online community

<http://www.benton.org/publibrary/practice/community/communitytips.html#planning>

Articulate the purpose for an online community

<http://www.benton.org/publibrary/practice/community/communitytips.html#purpose>

Improve upon moderating/facilitating skills

<http://www.benton.org/publibrary/practice/community/communitytips.html#moderate>

Choose the tools for your online community

<http://www.benton.org/publibrary/practice/community/communitytips.html#tools>

Promote an online community

<http://www.benton.org/publibrary/practice/community/communitytips.html#promote>

Clearinghouses for building online communities

<http://www.benton.org/publibrary/practice/community/communitytips.html#clearinghouses>

Additional learning opportunities

<http://www.benton.org/publibrary/practice/community/communitytips.html#seminars>

9.4 Other ways of viewing the same problems

This part of the Annex analyses an approach to build up a community that is not related to ICT and Network and Information security.

It quotes experiences that people from the Center for Civic Partnerships, Sacramento, California made while setting up a community garden and gives a relation to solving the same problem of fulfilling the same task in building a community among the constituency of a CSIRT.

Lessons Learned From California Healthy Cities and Communities in building up a community garden⁴³

The California Healthy Cities and Communities (CHCC) run several programs to set up community gardens in some cities. The process of building has several similarities with the process of setting up a community among the constituency of a CSIRT.

Key element for success

While each city's approach was unique, the following key elements were integral to their efforts:

- Commitment of local leadership and staffing
- Involvement of volunteers and community partners
- The opportunities for participants to have skill building.

Local Leadership and Staffing

A city's commitment of staff, financial, and in-kind resources is critical to the success of community gardens. City councils in each of 2 cities purchased land valued at \$70 000 or more for gardens, one using funds from the Community Development Block Grant, the other using money from the city's general fund. Both provide staffing on an ongoing basis.

Conclusion: Create constituents' commitment. Giving your constituent a sound FTE estimation makes clear how much resources he/she has to invest.

Volunteers and Community Partners

The participation and support of diverse community members help a community garden to thrive. These members include residents, partner institutions (e.g., schools, county health departments, universities), and volunteers (e.g., businesses, civic associations). The inclusiveness of gardens allows individuals and groups to contribute their knowledge, skills, and experience.

The business community contributes tools and lends equipment. Residents and volunteers often identify innovative strategies to leverage resources, such as the interim use of property and volunteer stipends as an alternative to hiring staff.

⁴³ Copyright © American Journal of Public Health 2003,

<http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1447988>

Conclusion: Use volunteers as much as possible, create an exclusive feeling and don't forget to give them recognition for their efforts. There is much more willingness into cooperation than noticed at first hand. Look for the similarities in constituents goals and what you can do to help achieving them.

Skill-Building Opportunities

Gardening workshops provide opportunities for residents, staff, volunteers of all ages to develop skills in leadership, community organizing, cultural competency, and program planning, implementation, and evaluation. Leadership development is enhanced through experiential learning, which includes intergenerational and peer-to-peer mentoring and train-the-trainer models. Volunteers and staff lead workshops, organize taste-testing events, facilitate discussions, advocate for the garden, and develop culturally appropriate resources (e.g., training materials, cookbooks, newsletters, Web sites). These ongoing, interactive learning opportunities help to sustain momentum for the garden.

Conclusion: Running a community keeps you fresh, new ideas open up and give contributors the opportunity to spread their knowledge and create a mutual benefit for the group. It also creates new opportunities to establish you as a serious partner.

Educating Stakeholders

Informing decision makers about the benefits of community gardens can be time-intensive. Changes in leadership can slow momentum. Communicating the benefits beyond the traditional leadership to the community at large can mitigate those challenges, help build a broad-based constituency, and provide long-term, consistent support of community gardening as a norm. Publications, electronic networks, and convening's can support learning across communities.

Conclusion: Using the group at large to communicate your results. This creates a dependency with your stakeholders and therefore success is more tangible because you have created a reference.

Integrating Community Gardens into Development

While the benefits of community gardens are many, land and housing shortages may compete for gardening space. Because community gardens are flexible in their design (e.g., containers on patios and rooftops as options to ground planting), they can be incorporated harmoniously into new structures or into existing facilities (e.g., school campuses, parks, community centres).

Conclusion: Related to NIS this means to integrate information security into the daily ICT operations and start with it during the development phase or research of new products.

Supporting Research

The dearth of data on the positive impacts of community gardens hinders the ability to make a *convincing argument* when resources (e.g., funding, land, water) are at stake. Anecdotal evidence abounds, but important outcomes such as the physical benefits of gardening and community connectedness are *difficult to measure*. User-friendly, multilingual, and adaptable evaluation tools are urgently needed given the diversity of participants and disciplines. The development of strategies to measure

the benefits of community gardens would sustain and promote this activity within an active living agenda.

Conclusion: Logical facts and incident data prove that a CSIRT can be very beneficial and efficient to reduce impact. Things like the cultural changes within the constituency or prevented incidents by preventive services are hard to measure and therefore should be considered as a “soft” benefit of having a CSIRT.

Investing for the Long Term

Given the opportunities and challenges inherent in this work, long-term investments - policymaking, funding, staffing, and acquiring in-kind resources - are needed to support planning, implementation, and evaluation. Community visioning and strategic planning processes are additional opportunities to integrate this work.

Conclusion: Creating a community is a long-term effort. You will definitely need to have a plan or vision about where you want to go with this community and in what direction you want to lead the group.

More information: <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1447988>

Thinking out of the box – what does a garden have to do with a CSIRT?

Like the community garden project, building a CSIRT community costs a lot of energy and effort. There are some similarities:

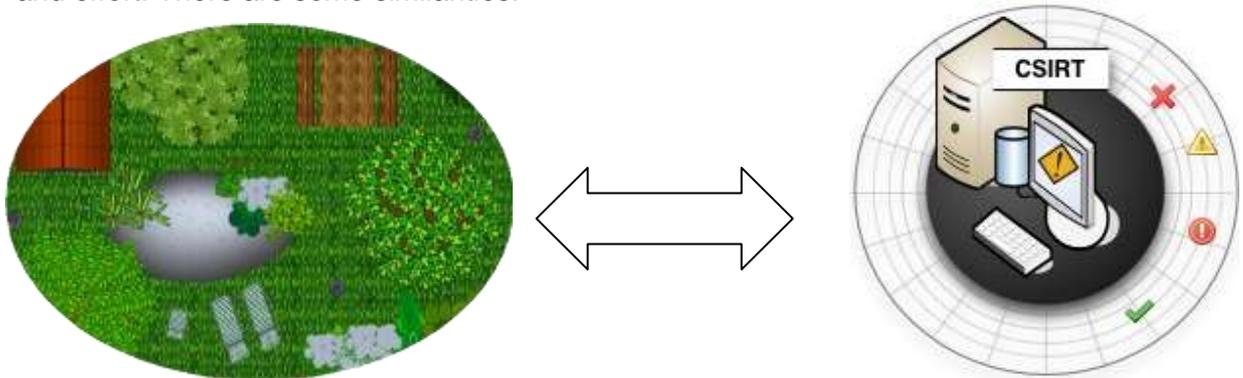


Figure 14. A community garden and a CSIRT

- How can you explain the “soft” factors without any concrete figures
- How can you manage your sponsors
- How do you convince the stakeholders and involve them into the development.
- Managing and organizing the different disciplines
- Keep making adjustments to your final goal due to changing expectations

Lesson learned while building a community: involve participation but transform the high expectations into realistic expectations.

9.5 Security information source list

The 2nd ad hoc working group “CERT Services” composed a list with information sources that most CSIRTs use in their daily watch routine, gaining vulnerability information and keep on track with new exploits and new techniques.

The list produced by the group can be found below.

Disclaimer

The inventory at hand was produced by the ENISA ad-hoc working group “CERT Services” in 2006. The information contained in that inventory was provided by the participants of this group based on their experience and may be incomplete, though it aims at being as comprehensive as possible at the time of creation.

Name	Weblink	Topics	Info Provider	Distribution	Language
Adobe	http://www.adobe.com/cfusion/entitlement/index.cfm?e=szalert	Vulnerabilities	Commercial Vendor /	Mailing list	English
Antivirus	http://antivirus.about.com/	Viruses	Commercial Vendor /	Website	English
Apache	http://httpd.apache.org	Vulnerabilities	Commercial Vendor /	Website	English
Apache	http://httpd.apache.org/lists.html#http-announce	Vulnerabilities	Non-Commercial	Mailing list	English
Apache	http://www.apacheweek.com/features/security-13	Vulnerabilities	Commercial Vendor /	Website	English
Apple	http://docs.info.apple.com/article.html?artnum=61798	Vulnerabilities	Commercial Vendor /	Website	English
Apple	http://lists.apple.com/mailman/listinfo/security-announce	Vulnerabilities	Commercial Vendor /	Mailing list	English
Apple Product Security	http://www.apple.com/support/security/	Notifications	Commercial Vendor /	Website	English
Arkoon	http://www.arkoon.net/FR/veillearkoon.php	Vulnerabilities	Commercial Vendor /	Website	French, English
AusCERT	http://www.auscert.org.au/	Vulnerabilities	CERT Academic	Website	English
BEA	http://dev2dev.bea.com/resourcelibrary/advisoriesnotifications/index.jsp	Vulnerabilities	Commercial Vendor /	Website	English
BELNET CERT	http://cert.belnet.be	Vulnerabilities	CERT	Website	English
BugTraq	http://www.securityfocus.com/archive	Vulnerabilities	Commercial Vendor /	Mailing list	English



Business objetscs	http://support.businessobjects.com/fix/hot/critical/default.asp	Vulnerabilities	Commercial Vendor	/ Website	English
CA	http://supportconnectw.ca.com	Vulnerabilities	Commercial Vendor	/ Website	English
Canadian Cyber Incident Response Centre	http://www.psepc-sppcc.gc.ca/prg/em/ccirc/index-en.asp	Vulnerabilities	Government	Website	English, French
CERT BUND	http://www.bsi.bund.de/certbund	Vulnerabilities	CERT (gov)	Website	German
CERT Estonia	http://www.cert.ee	Vulnerabilities	CERT	Website	Estonian
CERT FI	http://www.cert.fi	Vulnerabilities	CERT	Website	Finish
CERT Hungary	http://www.cert-hungary.hu	Vulnerabilities	CERT	Website	Hungarian
Cert IST	http://www.cert-ist.com/	Vulnerabilities	CERT Commercial Vendor	- / Mailing lists, Website, discussion lists, RSS feeds	French & English
CERT LEXSI	http://www.lexsi.com	Vulnerabilities	CERT	Website	French
CERT Polska	http://www.cert.pl	Vulnerabilities	CERT	Website	Polish
CERT.PT	http://www.cert.pt	Vulnerabilities	CERT	Website	Portuguese
CERT/CC	http://www.cert.org/	Vulnerabilities	CERT Academic	Website	English
CERT/CC	http://www.cert.org/other_sources/viruses.html#I	Viruses	CERT Acedemic	Website	English
CERTA	http://www.certa.ssi.gouv.fr	Vulnerabilities	CERT (gov)	Website, Mailing list	French
Certcom	http://www.certcom.de/	Vulnerabilities	Commercial Vendor	/ Website	German
CERT-Renater	http://www.renater.fr/spip.php?rubrique19	Vulnerabilities	CERT	Website, Mailing list	French
Checkpoint	http://www.checkpoint.com/services/mailling.html	Vulnerabilities	Commercial Vendor	/ Mailing list	English
Checkpoint	http://www.checkpoint.com/techsupport/alerts/	Vulnerabilities	Commercial Vendor	/ Website	English
CIAC – US Department of Energy	http://www.ciac.org	Vulnerabilities	Government	Mailing list	English



Cisco	http://www.cisco.com/en/US/products/products_security_advisories_listing.htm	Vulnerabilities	Commercial Vendor	Website	English
Cisco	http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html#subscribe	Vulnerabilities	Commercial Vendor	Mailing list	English
Citrix	http://support.citrix.com/latestsecurityall!execute.jspa	Vulnerabilities	Commercial Vendor	Website	English
CME	http://cme.mitre.org/data/list.html	Monitoring	Commercial Vendor	Website	English
Corsaire	http://www.corsaire.com/advisories/	Vulnerabilities	Commercial Vendor	Website	English
CVE	https://cassandra.cerias.purdue.edu/CVE_changes/	Vulnerabilities	Commercial Vendor	Website	English
CybSec	http://www.cybsec.com/ES/noticias/default.php	Vulnerabilities	Commercial Vendor	Website	Spanish
dCERT	http://www.dcert.de	Vulnerabilities	CERT	Website	German / English
DFN-CERT	http://www.dfn-cert.de/infoserv/mls/win-sec-ssc.html#TOPIC	Vulnerabilities	CERT	Security Advisories	English
DK CERT	http://www.cert.dk	Vulnerabilities	CERT	Website	Danish
dShield	http://dshield.org/	Status Monitoring	Commercial Vendor	Website	English
eEye	http://www.eeye.com/html/index.html	Status Monitoring	Commercial Vendor	Website	English
EISPP Project	http://www.eispp.org/	Awareness raising	Academic	Mailing list	English
ESACERT	http://www.esacert.esa.int	Vulnerabilities	CERT	Website	German
esCERT-UPC	http://escert.upc.es	Vulnerabilities	CERT	Website	Spanish
Fedora Legacy	http://www.fedoralegacy.org/updates/F_C1/	Vulnerabilities	Commercial Vendor	Website	French, English
Fedora Legacy	http://www.fedoralegacy.org/updates/	Vulnerabilities	Commercial Vendor	Website	French, English
FIRST	http://www.first.org/	General information	Non-Commercial	Mailing list	English
FIRST NEWS	http://www.first.org/newsroom/globalsecurity/	Vulnerabilities, Awareness raising	Commercial Vendor	Mailing list	English
FreeBSD	http://www.freebsd.org/security/index.html	Vulnerabilities	Commercial Vendor	Website	English

FreeBSD	http://lists.freebsd.org/mailman/listinfo/freebsd-security-notifications	Vulnerabilities	Non-Commercial	Mailing list	English
F-Secure	http://support.f-secure.com/enu/corporate/downloads/hotfixes/	Vulnerabilities	Commercial Vendor	Website	English
F-Secure	http://www.f-secure.com/products/radar/alerts/	Vulnerabilities	Commercial Vendor	Website	English
F-Secure	http://www.f-secure.com/security/	Vulnerabilities	Commercial Vendor	Website	English
F-Secure	http://www.f-secure.com/security_center/	Vulnerabilities	Commercial Vendor	Website	English
F-Secure	http://www.f-secure.com/v-descs/_new.shtml	Viruses	Commercial Vendor	Website	English
Full Disclosure	http://lists.grok.org.uk/full-disclosure-charter.html	Vulnerabilities	Non-Commercial	Mailing list	English
GARR CERT	http://www.cert.garr.it	Vulnerabilities	CERT	Website	Italian
GOVCERT.IT	http://www.govcert.it	Vulnerabilities	CERT (gov)	Website	Italian
GOVCERT.NL	http://www.govcert.nl	Vulnerabilities	CERT (gov)	Website	Dutch
GRNET CERT	http://cert.gnet.gr	Vulnerabilities	CERT	Website	Greek
HP	http://www.hp.com	Vulnerabilities	Commercial Vendor	Mailing list	English
IBM	http://www.ibm.com	Vulnerabilities	Commercial Vendor	Mailing list	English
Idefense	http://www.iddefense.com/	Status Monitoring	Commercial Vendor	Website	English
ISS	https://gtoc.iss.net/issEn/delivery/gtoc/index.jsp	Internet activity monitoring	Commercial Vendor	Website	English
ISS	http://xforce.iss.net/xforce/maillists/	Vulnerabilities	Commercial Vendor	Mailing list	English
ISS XForce	http://xforce.iss.net/	Vulnerabilities	Commercial Vendor	Website	English
Juniper	http://www.juniper.net/support/security/security_notices.html	Vulnerabilities	Commercial Vendor	Website	English
KB US-CERT	http://www.kb.cert.org/vuls	Vulnerabilities	CERT (gov)	Website	English
KPN-CERT	http://www.kpn-cert.nl	Vulnerabilities	CERT	Website	English



Linux Debian	http://lists.debian.org/debian-security-announce/	Vulnerabilities	Commercial Vendor	/ Mailing list	English
Linux Fedora	http://www.redhat.com/mailman/listinfo/fedora-package-announce	Vulnerabilities	Commercial Vendor	/ Mailing list	English
Linux Fedora Legacy	http://www.fedoralegacy.org/mail/	Vulnerabilities	Commercial Vendor	/ Mailing list	English
Linux Kernel	http://www.kernel.org	Vulnerabilities	Commercial Vendor	/ Website	English
Linux Mandriva	http://www.mandriva.com/en/community/resources/node_838#security	Vulnerabilities	Commercial Vendor	/ Mailing list	English
Linux Red Hat	https://www.redhat.com/archives/enterpriserise-watch-list/	Vulnerabilities	Commercial Vendor	/ Mailing list	English
Linux Slackware	http://www.slackware.com/lists/	Vulnerabilities	Non-Commercial	Mailing list	English
Linux SuSE	http://www.novell.com/linux/security/securitysupport.html	Vulnerabilities	Commercial Vendor	/ Website	English
Linux SuSE	suse-security-announce-subscribe@suse.com	Vulnerabilities	Commercial Vendor	/ Mailing list	English
Linux Trustix	http://lists.trustix.org/mailman/listinfo/tsl-announce	Vulnerabilities	Commercial Vendor	/ Mailing list	English
LITNET CERT	http://cert.litner.lt	Vulnerabilities	CERT	Website	Lithuanian
Lotus	http://www-10.lotus.com/ldd/security	Vulnerabilities	Commercial Vendor	/ Website	English
Macromedia	http://www.adobe.com/cfusion/entitlement/index.cfm?e=szalert	Vulnerabilities	Commercial Vendor	/ Mailing list	English
Macromedia	http://www.macromedia.com/v1/developer/securityzone/securitybulletins.cfm	Vulnerabilities	Commercial Vendor	/ Website	English
McAfee	http://vil.nai.com/vil/signup_DAT_notification.aspx	Viruses	Commercial Vendor	/ Mailing list	English
mCERT	http://www.mcert.de	Vulnerabilities	CERT	Website	German
Messagelabs	http://www.messagelabs.com	Viruses	Commercial Vendor	/ Website	English
Micro-BIT	http://www.microbit.uni-karlsruhe.de	Vulnerabilities	CERT	Website	German
Microsoft	http://www.microsoft.com/technet/security/advisory/default.mspx	Vulnerabilities	Commercial Vendor	/ Website	English
Microsoft	http://www.microsoft.com/technet/security/bulletin/notify.mspx	Vulnerabilities	Commercial Vendor	/ Mailing list	English

Mozilla	http://www.mozilla.org/projects/security/known-vulnerabilities.html#mozilla1.7	Vulnerabilities	Commercial Vendor	/ Website	English
mtCERT	http://www.mcert.gov.mt	Vulnerabilities	CERT	Website	Maltese
Nagios	http://www.nagios.org/development/cha ngelog.php	Vulnerabilities	Commercial Vendor	/ Website	English
NAI	http://vil.nai.com/vil/newly_discovered_viruses.aspx	Viruses	Commercial Vendor	/ Website	English
NAI	http://www.nai.com/us/downloads/updates/hotfixes.asp	Vulnerabilities	Commercial Vendor	/ Website	English
NetASQ	http://www.netasq.com/en/index.php	Vulnerabilities	Commercial Vendor	/ Mailing list	French, English
NetBSD	http://www.netbsd.org/fr/Mailing_lists/#netbsd-announce	Vulnerabilities	Commercial Vendor	/ Mailing list	English
Netscape	http://browser.netscape.com/ns8/security/alerts.jsp	Vulnerabilities	Commercial Vendor	/ Website	English
NISCC	http://www.niscc.gov.uk/niscc/vulnAdvisen.html?yr=2005	Vulnerabilities	Government	Website	English
NIST	http://csrc.ncsl.nist.gov/	Vulnerabilities	Academic	Website	English
Nortel	http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?cscat=SECUREADVISORY	Vulnerabilities	Commercial Vendor	/ Website	English
Novell	http://support.novell.com/filefinder/security/index.html	Vulnerabilities	Commercial Vendor	/ Website	English
Novell	http://www.novell.com/company/subscribe/	Vulnerabilities	Commercial Vendor	/ Mailing list	English
NTA Monitor	http://www.nta-monitor.com/news/nta-in-news.htm	Vulnerabilities	Commercial Vendor	/ Website	English
NTBugTraq	http://www.ntbugtraq.com/	Vulnerabilities	Commercial Vendor	/ Mailing list	English
OpenBSD	http://www.openbsd.org/errata.html	Vulnerabilities	Commercial Vendor	/ Website	English
Oracle	http://otn.oracle.com/deploy/security/alerts.htm	Vulnerabilities	Commercial Vendor	/ Website	English
Oracle (unofficial)	http://www.petefinnigan.com/alerts.htm	Vulnerabilities	Commercial Vendor	/ Website	English
OSSIR	http://www.ossir.org/	Vulnerabilities	Academic	Mailing list	French
OSVDB	http://www.osvdb.org	Vulnerabilities	Commercial Vendor	/ Website	English
Outpost24	http://www.outpost24.com/	Viruses	Commercial	/ Website	English



			Vendor		
Packet Storm	http://packetstormsecurity.org/	Vulnerabilities	Commercial Vendor	Website	English
Pionier CERT	http://cert.pionier.gov.pl	Vulnerabilities	CERT	Website	English
PostgreSQL	http://archives.postgresql.org/pgsql-announce/	Vulnerabilities	Non-Commercial	Mailing list	English
RUS-CERT	http://cert.uni-stuttgart.de/ticker	Vulnerabilities	CERT	Website	German
SANS	http://www.incidents.org	Internet activity monitoring	Commercial Vendor	Website	English
SANS Incidents Diary	http://isc.incidents.org/	Vulnerabilities General information System administration	Commercial Vendor	Website	English
SCO	http://sco.com/support/security/2006.html	Vulnerabilities	Commercial Vendor	Website	English
Secunia	http://secunia.com/virus_information/	Viruses	Commercial Vendor	Website	English
Secunia	http://secunia.com/mailling_lists/	Vulnerabilities	Commercial Vendor	Mailing list	English
Securiteam	http://www.securiteam.com/Mailinglist.html	Vulnerabilities	Commercial Vendor	Mailing list	English
Security News Portal	http://www.securitynewsportal.com/index.shtml	Vulnerabilities	Commercial Vendor	Website	English
Security Tracker	http://www.securitytracker.com/signup/signup_now.html	Vulnerabilities	Commercial Vendor	Mailing list	English
Secuser	http://www.secuser.com/	Vulnerabilities	Commercial Vendor	Mailing list	French
SGI	http://www.sgi.com/support/security/wir etap.html	Vulnerabilities	Commercial Vendor	Mailing list	English
SI CERT	http://www.arnes.si/si-cert/	Vulnerabilities	CERT	Website	Slovenian
SITIC	http://www.sitic.se	Vulnerabilities	CERT	Website	Swedish
Sophos	http://www.sophos.com/security/notifications/	Viruses	Commercial Vendor	Mailing list	English
SQUID	http://www.squid-cache.org/Advisories/	Vulnerabilities	Commercial Vendor	Website	English
SUN	http://sunsolve.sun.com/	Vulnerabilities	Commercial Vendor	Website	English



Sun (blog)	http://blogs.sun.com/security	Vulnerabilities	Commercial Vendor	/ Website	English
SURFnet-CERT	http://cert.surfnet.nl	Vulnerabilities	CERT	Website	Dutch
Symantec	http://securityresponse.symantec.com/avcenter/security/SymantecAdvisories.html	Vulnerabilities	Commercial Vendor	/ Website	English
Symantec	http://www.symantec.com/enterprise/security_response/threatexplorer/threats.jsp	Viruses	Commercial Vendor	/ Website	English
TF-CSIRT	http://www.terena.nl/activities/tf-csirt/	General information	Academic	Mailing list	English
TP CERT	http://www.tp.pl/cert	Vulnerabilities	CERT	Website	Polish
Trend	http://uk.trendmicro-europe.com/enterprise/about_us/worldwide_select.php	Viruses	Commercial Vendor	/ Website	English
Trend Micro	http://www.trendmicro.com/subscriptions/default.asp	Viruses	Commercial Vendor	/ Mailing list	English
Trendmicro	http://www.trendmicro.com/vinfo/default.asp?advis=&sort=date&order=desc	Viruses	Commercial Vendor	/ Website	English
Trustix	http://www.trustix.net/errata/2006/	Vulnerabilities	Commercial Vendor	/ Website	English
Typo3	http://typo3.org/teams/security/security-bulletins/	Vulnerabilities	Commercial Vendor	/ Website	English
UNIRAS	http://www.uniras.gov.uk	Vulnerabilities	CERT (gov)	Website	English
US-CERT	http://www.us-cert.gov/	Vulnerabilities	CERT Government	Website	English
US-CERT	http://www.us-cert.gov/current/current_activity.html	Status Monitoring	CERT Government	Website	English
US-CERT Alert Tech	https://forms.us-cert.gov/maillists/	Vulnerabilities	Government	Mailing list	English
Virustotal	http://www.virustotal.com/en/indexf.html	Viruses	Non-Commercial	Website	English
Webmin	http://www.webmin.com/security.html	Vulnerabilities	Commercial Vendor	/ Website	English

9.6 CSIRT Services

Special thanks to CERT/CC⁴⁴, who kindly provided this CSIRT service list!

<u>Reactive Services</u>	<u>Proactive Services</u>	<u>Artifact Handling</u>
<ul style="list-style-type: none"> • <u>Alerts and Warnings</u> • <u>Incident Handling</u> • <u>Incident analysis</u> • <u>Incident response support</u> • <u>Incident response coordination</u> • <u>Incident response on site</u> • <u>Vulnerability Handling</u> • <u>Vulnerability analysis</u> • <u>Vulnerability response</u> • <u>Vulnerability response coordination</u> 	<ul style="list-style-type: none"> • <u>Announcements</u> • <u>Technology Watch</u> • <u>Security Audits or Assessments</u> • <u>Configuration and Maintenance of Security</u> • <u>Development of Security Tools</u> • <u>Intrusion Detection Services</u> • <u>Security-Related Information Dissemination</u> 	<ul style="list-style-type: none"> • <u>Artifact analysis</u> • <u>Artifact response</u> • <u>Artifact response coordination</u>
		<u>Security Quality Management</u>
		<ul style="list-style-type: none"> • <u>Risk Analysis</u> • <u>Business Continuity and Disaster Recovery</u> • <u>Security Consulting</u> • <u>Awareness Building</u> • <u>Education/Training</u> • <u>Product Evaluation or Certification</u>

Figure 15. CSIRT services list from CERT/CC

9.6.1 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.

9.6.2 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.

⁴⁴ CERT Coordination Centre: <http://www.cert.org>

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

9.6.4 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

9.6.5 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) 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.

9.6.6 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.

9.6.7 Incident response on site

The CSIRT provides direct, on-site assistance to help constituents recover from an incident. The CSIRT itself physically analyzes 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.

9.6.8 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.

9.6.9 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.

9.6.10 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:

9.6.11 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.

9.6.12 Vulnerability response

This service involves determining the appropriate response to mitigate or repair a 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.

9.6.13 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 knowledgebase of vulnerability information and corresponding response strategies.

9.6.14 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:

9.6.15 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.

9.6.16 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.

9.6.17 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.

9.6.18 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.

9.6.19 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.

9.6.20 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.

9.6.21 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

9.6.22 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

9.6.23 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

9.6.24 Scanning

Using vulnerability or virus scanners to determine which systems and networks are vulnerable

9.6.25 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 part contractor or managed security service provider with the appropriate expertise in conducting audits and assessments.

9.6.26 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, personal digital assistants (PDAs), 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.

9.6.27 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.

9.6.28 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 pre-defined 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.

9.6.29 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.

9.6.30 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.

9.6.31 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.

9.6.32 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.

9.6.33 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.

9.6.34 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.

9.6.35 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.

9.6.36 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.

9.7 Other available information and material

There are a lot of standards to be found and a lot of organizations that are involved in the standardization process. Listed links provide a lot of valuable information on different topics. It is good to ask around to learn what people use and what is working for them and why.

One of the key values to consider is the amount of users within the standardization community. This way supporting a product or standard and deciding when investing in a product is beneficial for the entire community.

General operational issues

Internet Engineering Task Force IETF

<http://www.ietf.org/>

National Institute of Standards and Technology NIST

<http://www.nist.gov/>

Organization for the Advancement of Structured Information Standards OASIS

<http://www.oasis-open.org/>

Open Group Security Forum OGSF

<http://www.opengroup.org/security/>

Terena's Task Force CSIRT (TF-CSIRT)

http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

Forum of Incident Response and Security Teams FIRST

http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm

Good practices

CERT Coordination Centre CERT/CC

<http://www.cert.org>

SANS Institute

<http://www.sans.org>

Information Systems Audit and Control Association ISACA

<http://www.isaca.org/>



Information Systems Security Association ISSA

<http://www.issa.org/>

Relevant "Requests for Comment" RFC's

RFC 2196: Site Security Handbook (replacing RFC1244)

<http://www.ietf.org/rfc/rfc2196.txt>

RFC 2350: Expectation for Security Incident Response Teams

<http://www.ietf.org/rfc/rfc2350.txt>

RFC 2505: Users' Security Handbook

<http://www.ietf.org/rfc/rfc2505.txt>

RFC 3013: Recommended Internet Service Provider Security Services and Procedures

<http://www.ietf.org/rfc/rfc3013.txt>

RFC 3227: Guidelines for Evidence Collection and Archiving

<http://www.ietf.org/rfc/rfc3227.txt>

RFC 2828: Internet Security Glossary

<http://www.ietf.org/rfc/rfc2828.txt>

