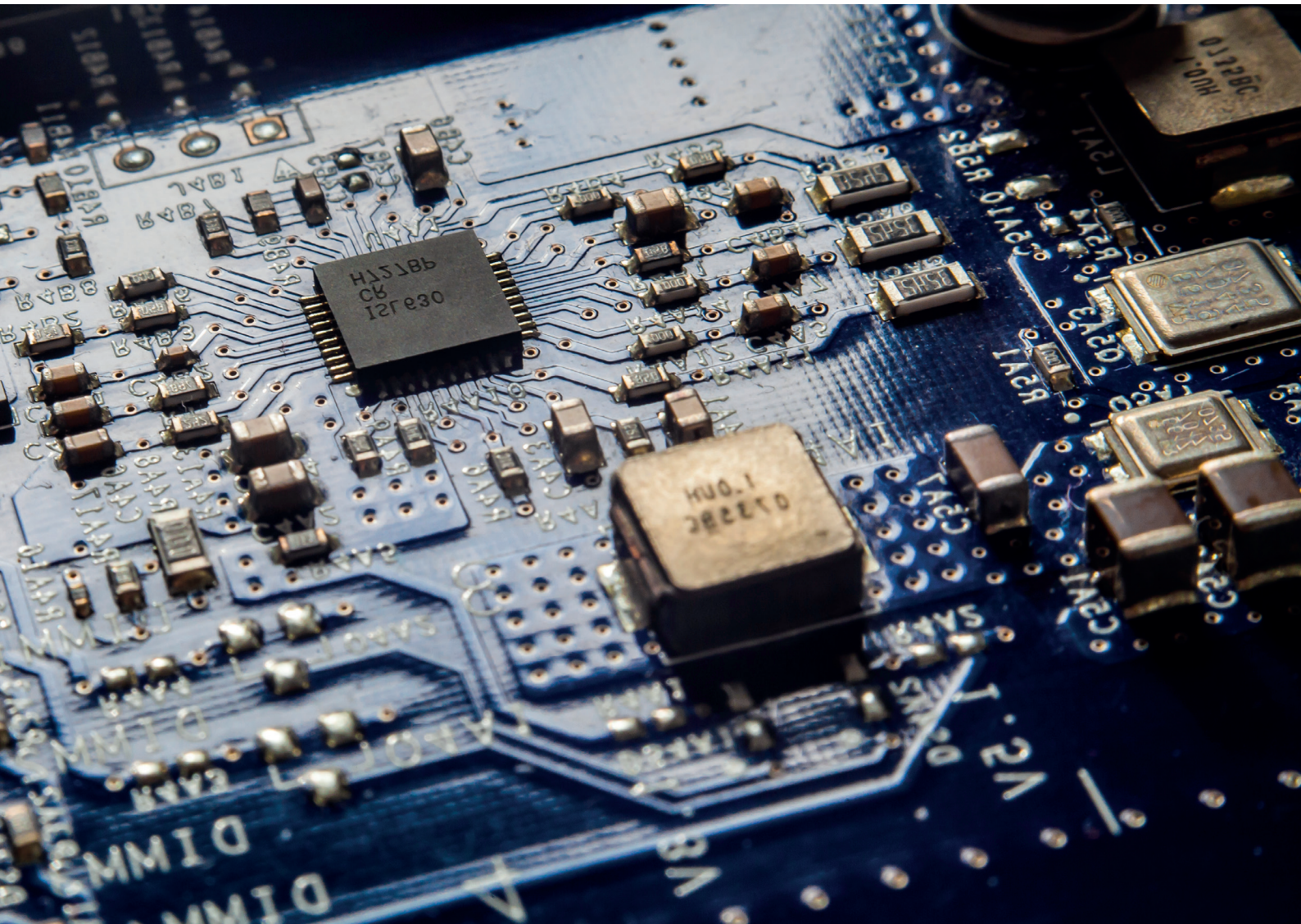
National Cyber Security Centre
Ministry of Justice and Security

Starting a collective CSIRT

Guide



Roadmap collective CSIRT

The NCSC and its partners have created a roadmap if you want to set up a collective CSIRT. In this roadmap, you will find three stages your organisation can undertake to create a successful collective CSIRT.

Stage 1: **Explore**

Create support, build trust and seek consensus:

- Identify the shared needs within the working group.
- Conduct a feasibility study.
- Ensure sufficient critical mass.

Stage 2: **Consensus**

Define the mandate, services and activities:

- Define the organisational structure.
- Outsource the collective tasks to the right party.
- Define the mandate in both the preparatory and the response phase.
- Decide what services and activities the collective CSIRT will offer.

Stage 3: **Grow**

Increase capabilities and continue to evolve:

- Don't grow too fast, but keep an eye on the ambitions.
- Increase the number of participants and activities.
- Build and intensify collaborations.

Starting a collective CSIRT

A collective Computer Security Incident Response Team (CSIRT) increases the capabilities, the awareness and the resilience of the participating organisations. Collective CSIRTs act as the coordinator when one or more participating parties experience an incident or crisis. The team is the dedicated contact point for both participants and non-affiliated organisations. In addition, the collective CSIRT fulfils the function of information hub by providing interpretations and maintaining an overview.

In this guide, the NCSC and organisations that have already set up a (collective) CSIRT share their experiences of the setting-up process, the added value of a collective CSIRT and the activities that are entrusted to a collective CSIRT.

Target audience

Information security officers of businesses and organisations who want to set up a collective CSIRT.

The following parties have contributed to this guide

CERT-EU, CERTFin (Italy), Cyber Synergie Schiphol Ecosysteem (CYSSEC), FERM-Rotterdam, FinancialCERT, i-CERT, CSIRT for Dutch municipalities (IBD), NATO Computer Incident Response Capability (NCIRC), Dutch Productivity Alliance (NPAL) and SURFcert.

What is a collective CSIRT?

A collective CSIRT[1] is a form of collaboration in which CSIRT services are performed for a number of organisations. A collective CSIRT handles the coordination and collaboration in the event of threats or incidents that occur at one or more participating organisations.

Although in general terms a collective CSIRT performs the same activities and has the same responsibilities as the CSIRT in a single organisation, the emphasis in a collective CSIRT is on a coordinated collective response capacity.

In general, CSIRTs are responsible for preventing, isolating and mitigating computer and information security incidents to guarantee the availability of services and/or information flows. This requires technical and non-technical activities. During incidents, actions are performed within systems to isolate or mitigate the incident or event. In the aftermath of an incident, a CSIRT also handles the evaluation to prevent the incident recurring. This requires information from systems and individuals (log files, automated detection messages, report analysis).

In a collective CSIRT, the emphasis is on coordination and supporting participating organisations to guarantee the availability of services and/or information flows. The degree to which technical activities are performed by the CSIRT depends on the collaboration model being used and agreements on roles, activities and mandate.

The need and benefit of a collective CSIRT

The added value of the collective CSIRT is evidenced when a cybersecurity challenge or digital threat occurs. The advantages of a collective CSIRT are as follows:

Increased capabilities

The capabilities during incidents increases, because you have made concrete agreements beforehand with the other organisations on coordination, information sharing, analysis and responsibilities. You can also run simulations together to practise how you handle incidents. Or you can organise specific training for the members of the CSIRT.

Combining forces for incident response

Combining forces into a team for incident response is an important reason for many organisations to participate in a CSIRT. Capacity is used more efficiently, partly because information and interpretation are available from various perspectives. To combine capacity efficiently and effectively, we recommend physically getting together for incident response.

Increased resilience

Individual businesses or smaller organisations are often not in the position to build up effective CSIRT capacity due to a lack of knowledge or financial resources, while they do need to make proper preparations for support during an incident. The resilience of other related organisations is important, even in (larger) organisations that have built up sufficient capacity. If all organisations have a higher level of resilience this benefits everyone.

Cost-effectiveness

The incident response capacity can be set up cost-effectively because the services of several participants are offered at the same time or joint procurement is possible.

Customised information and interpretation

The organisations involved are connected to each other because they are active in the same domain (sectoral relationship), are connected to each other physically and/or digitally (supply chain dependence) or because they are located in the same region (geographic relationship).[2] Because of this connecting factor, participating organisations receive customised information on specific threats, developments, new technologies and laws and regulations.

1 The terms CSIRT and Computer Emergency Response Team (CERT) are often used synonymously. We have chosen to use the term CSIRT in this guide because CERT is a brand name owned by Carnegie Mellon University.

2 See https://www.ncsc.nl/english/cooperation for more tips about setting up a sectoral, supply chain or regional collaboration.

Collaborating with other partnerships and organisations

Setting up collective CSIRTs brings about the structural and coordinated exchange of information, communication and collaboration with other relevant organisations nearby, other collective CSIRTs and the NCSC for instance.

"As the CSIRT for Dutch Municipalities, we see that one of our most significant added values is that we ourselves assume the central coordination role and sometimes even the entire spokesperson function in the event of digital incidents within the collective. This not only lightens the load on municipalities during the crisis, it also ensures that communication to the outside world is consistent."

CSIRT for Dutch Municipalities (IBD)

The concrete steps in setting up the CSIRT are set out in the following three stages.

Stage 1: Explore

Create support, build trust and seek consensus

When, for instance, several organisations are confronted with a real incident or threat, people very quickly come to the realisation that cybersecurity is a topic worthy of attention. Exploring whether a partnership in the field of cybersecurity incident response is worthwhile is subsequently no longer such a big step after all.

The initiative for setting up a collective CSIRT often occurs because people start discussing cybersecurity amongst themselves, during a networking meeting in a sector or region for instance. The initiative first creates an idea of the need to shape a collective partnership. Energy is generated by the informal setting and the personal involvement of this initial group. This enthusiasm is needed to attract other people and organisations.

When the initial ideas begin to take shape, form a working group which will further explore and elaborate the possibilities of a collective CSIRT. This working group lists the requirements of the prospective organisations that could participate in the CSIRT.

Conduct a feasibility study

Once the shared needs of the prospective organisations become clear, conduct a feasibility study. Based on these analyses, determine as a group whether you will proceed with the initiative and in what format. This means establishing a collective vision and strategy, and finding a suitable partnership structure.

A feasibility study contributes to:
- creating support from directors and participants through a structured approach
- gaining insight into various partnership models
- understanding the needs of the initiators.

The feasibility study is the basis for the initial cost-benefit analysis which forms the basis upon which you can formulate a business plan (including a growth model).

Tip: This initial stage thus involves making important design choices regarding establishing and structuring a collective CSIRT. In this phase you should also consider growth models and further development so that the selected model suits your ambitions.

In practice, the next step will be slightly different for every situation. Important points for attention: having sufficient support and commitment from the participating organisations, insight into the (sometimes differing) needs of the participating organisations and working on trust between the organisations.

"In the run-up to setting up i-CERT we conducted an extensive feasibility study and stakeholder analysis. The requirements and the support among insurance companies were also identified. An important part of the study was elaborating and assessing different scenarios. These scenarios were cumulative in nature, where it was also possible to start with the least advanced model and to further develop it later. The scenarios were analysed by experts and prospective participants (costs, benefits, governance, feasibility of objectives and risk analysis). Based on the study, we chose to further elaborate a single scenario, which eventually led to setting up i-CERT in 2017."

i-CERT for the insurance sector

Make an early start on creating support

To get something off the ground collectively, you must begin creating support early on in the initiators' organisations and in ones that are potential participants.

Ensure that the initiative does not rest too long with a few enthusiastic individuals and ensure that you have support and endorsement at strategic level within your own organisation. Setting up a collective CSIRT is impossible without support and endorsement at strategic level in the participating organisations. Regularly exchanging thoughts with others on plans, activities, capacities and services is essential at the start.

Ensure recognition and support of the initiative in other places in the participating organisations. Remember, the process of creating sufficient support can take up quite a lot of time. For example, regularly publish a newsletter which allows you to keep a wide group of organisations up to speed. In addition, organising specific meetings or sessions during other events can contribute to solid support. There is a need to remain visible even after setting up. By (continually) bringing your initiative to the attention of a wider public, you ensure that organisations become better acquainted and get in touch with each other more easily.

Tip: Distribution channels such as email lists or a digital platform ensure that participating parties can share information with each other in a secure (and uniform) way. The Traffic Light Protocol[3] can provide such support. To foster mutual trust, all parties must have access to the distribution channels and stick to the agreements on information sharing.

Trust is the basis

The most important collective objective must be the digital resilience and security of participating organisations. Organisations that collaborate on digital resilience must be prepared to trust each other and therefore let go of their feelings about their competitive position or possible negative aspects of collaboration. Process agreements and other agreements are needed to guarantee the security and integrity of sensitive information and activities. Such agreements can be included in the membership guidelines and communication resources.

Ensure sufficient critical mass

The size of the partnership has an effect on its success. The participation of all prospective organisations is not required before a start can be made. It is often more effective to begin with a smaller group of three to five organisations. The group can then be expanded step by step. What is crucial is that sufficient mass is created for the next steps, to cover the costs and/or allocate activities among each other.

Right from the start, the working group must be thinking about the process for expansion and enrolment. These questions serve as preparation:

- What size of partnership is eventually envisaged and why? Is it possible or desirable to set a lower or upper limit?
- Is the scope and availability of the current services ample, limited or exactly right for new participants?
- Can new participants be accommodated within the existing structure or should other partnerships be set up?
- Will the group only grow larger through expansion or will its scope also be widened? And does this have consequences for the capabilities?
- Will new or additional coordination and/or response capacity become available in the event of expansion? Is this desirable?
- Will all future participants take part in the same way or are different 'membership levels' conceivable?
- What is the ideal phasing (e.g. maximum intake per year)?
- What is the maturity level of the incoming organisations?
- Do current participants have a trust relationship with the incoming organisations and if so, based on what?

3 www.first.org/tlp

Stage 2: Consensus

Define the mandate, services and activities

Think about the organisational issues in setting up a collective CSIRT together and reach agreement.

Organisational structures

Firstly, various organisational structures are conceivable for setting up a collective CSIRT:

1. Facilitated by an existing organisation in the partnership, such as a branch organisation. With this option, there is no need to set up a new organisation because there is already capacity and a relationship within the partnership. A disadvantage could be that the organisation has a different task description and perhaps has not yet had any experience with this type of role in information security.
2. As a new organisation, such as a foundation to carry out the CSIRT tasks. The advantage of this is that the new organisation is fully dedicated to the CSIRT tasks and can be set up toaccommodate the requirements of the partnership. A possible disadvantage is that the start-up, design and administration require more investment (time, funds, personnel) to build and maintain trust.
3. Outsourcing the collective CSIRT tasks to a third party. The advantage here is that the party to be contracted can be selected based on quality and expertise. A possible disadvantage is that the party to be contracted does not know the participants in the partnership and may have less knowledge about requirements and challenges. In addition, trust will have to be built first.

Tip: Interested parties can sometimes only become affiliated at a later stage because, for example, they have ongoing contracts (for incident response, threat information, security information and event management (SIEM)). This does not have to be a problem if they are able to engage in other activities (information sharing, community-building). Once the current contract has expired they can then decide to enter into the partnership. Include this in your considerations.

Operational implementation of the tasks

The execution of the tasks must suit the type of partnership that is chosen.

Possibilities include:

1. The tasks of the CSIRT are carried out by a number of participating organisations. They are usually organisations that already have a CSIRT capacity.
2. The incident response team is newly established within the collective. When doing so, a team of experts is appointed to manage the CSIRT.
3. The incident response team is contracted as a service from a third party (outside of the collective).

Define the mandate and the role in both the preparatory and the response phases

There are three levels of authority in the collective CSIRT:

1. **Full authority**: the members of the team have the authority to take the necessary actions or decisions on behalf of all participating organisations.
2. **Partial authority**: the members of the team influence the selection processes but cannot decide what actions or decisions are taken by the participating organisations.
3. **No authority**: the members of the team have no formal authority, but are recognised as content experts and can act as trusted advisers.

For many organisations, the exchange of information about incidents within the collective CSIRT is the driving force for the collective. Depending on the trust in and maturity level of the CSIRT, certain incident response tasks and responsibilities can be assigned in whole or in part to the collective CSIRT.

During the preparatory phase, when no incidents are taking place, it is important to reach agreements on the level of support during the operational phase in response to an incident. Responsibilities of the collective CSIRT differ per collective. An organisation will normally always bear final responsibility for its own services and infrastructure. The collective CSIRT therefore has a supporting role and provides assistance and advice to the individual organisation to de-escalate the incident as quickly as possible (partial authority).

Essential personnel and roles

As a collective CSIRT, first develop a vision and objective(s) that are supported by everyone before considering the staffing. Based on the mutually agreed vision, you can choose what the staffing should be and what education and training is needed to realise the vision. This is an essential choice during the design.

You can hire experts, seconded personnel from participating organisations or even choose something in between that suits the vision and objective(s). In any event, the staff of a collective CSIRT will need proper training and education with a focus on collaboration. It is important to also retain to your own ideas and specialisations. Doing so keeps everyone other on their toes.

Employees with executive tasks must have experience in the discipline and understand the material they receive incident reports about. In addition, there are also non-technical roles to be considered, such as relationship managers, legal consultants, data privacy officers, and communication specialists for setting up internal and external communications.

Funding

Estimate the investment required based on the design choices, the mission and the objective(s). When doing so, always consider the balance between the functionality and (expected) return on investment. A cost-benefit analysis is a good starting point for this. Draw up a funding model to answer the following questions:

- 24/7 availability or not?
- Remote collaboration or in a shared physical location?
- Autonomy of staff versus autonomy of participating organisations?
- Extensive communications strategy or operate in the background?
- Active monitoring and detection or mainly focus on coordination of the response?
- Which role, task and responsibility in the preparatory phase and in the response phase?
- Appoint personnel or use a rotation model for participating organisations?
- Membership fee versus contribution with no exchange of funds?
- Can the partnership be funded from existing resources or is additional funding required from the participating organisations?
- Equal contributions from everyone or scalable by size of participants (a staggered membership model, for instance)?
- Purchasing services and information and/or contribution from participants?

Legal aspects

In the design and the further development of the collective CSIRT, choices must be made. Agreements need to be reached between the participating organisations on many points, including agreements on conditions for participation and associated responsibilities. From a legal standpoint, it is advisable to properly record these agreements.

A CSIRT is a place where information is received which may contain personal data and where incidents are reported.

Tip: The agreements between organisations affiliated to the collective CSIRT can be recorded in a partnership agreement or statutes for instance.[4]

To do this, the relevant laws and regulations[5] will have to be monitored and you will have reach agreement on how the collective will deal with them.

Identify services and activities

In the design phase you have to decide what services and activities the collective CSIRT will offer and what responsibilities it will assume. The service package can start off small and be expanded in the course of time from a collectively determined growth model or roadmap. The tasks that will be tackled first depend on the situation.

What are those initial tasks?

Coordination on incident response

This involves deciding on the scope at which action will be undertaken. You also determine who will take what actions as a result of an incident. A collective CSIRT can act as a reporting and recording point for instance that only passes incidents on to the correct bodies. Of course, the team can also act itself when incidents have taken place.

Information sharing

Stimulating the exchange of information is an important basis for being able to continue functioning, for building trust and continuously professionalising. For example, information about developments in cybersecurity (legislation, new technology, trends, threats, attack techniques), incidents relative to the CSIRT's target group and best practices.

4 See e.g. https://www.verzekeraars.nl/branche/zelfregulering/overzicht/cert-verzekeringssector-convenant.

5 Sector-specific (i.e. supervisory bodies, inspection, statutory frameworks) and specific to topic (i.e. privacy, information security).

Distribution channel

Secure information sharing between participating organisations is facilitated by a secure distribution channel, such as email, a platform (forum) or another system.

Spokesperson function and communications

A collective CSIRT can have a spokesperson function and communicate about incidents to inform other organisations. Examples include the NCSC, customers, stakeholders, other government organisations and the media.

Knowledge and analysis capacity

The knowledge and analysis capacity built up within the collective CSIRT benefits the collective. To this end, collaboration can also be sought with the NCSC, other CSIRTs, universities, knowledge institutions and other organisations. The same applies to the specific expertise of participating organisations which can be better used in this way.

"We provide a basic service package which is mandatory for all affiliated parties. There are also additional services which are optional. We have also set up a SURFnet Community for Incident Response Teams (SCIRT) within which CSIRTs from the participating organisations can exchange information. As result of this we can continue to focus on the primary services and at the same time foster the mutual relationship between the participating organisations."[6]

SURFcert

The physical space

Choosing whether to physically accommodate the collective CSIRT somewhere or to have it operate as a virtual team from within its own organisation depends on the configuration and interpretation of the tasks. Physically collaborating in a single location can be a basis for expanding the operational collaboration, through activities such as monitoring systems and eventually bringing network traffic under the collective CSIRT. Using a liaison structure combines physical and virtual collaboration.

For side-by-side collaboration, a special physical location contributes to becoming better acquainted and to the growth of mutual trust. Naturally, this makes information sharing easier. When a virtual team of experts is set up, experts in the team remain closely involved with their own organisation. As a result, they can also maintain awareness and support in their own organisation. This eliminates the need to incur additional costs for a new location or infrastructure.

In partnerships with many participants it may be useful to coordinate activities from a central location. Participating organisations can then assume remote responsibility for some of the tasks.

"We have noticed that our organisational structure and the capacities we have are continuously subject to change. By holding a review and looking ahead each year, we are continuously working on the further development of the team and embedding it. As a result, we were able to respond to changes and continue to improve."

CERT-EU

Level of maturity of affiliated organisations

During the founding of the collective CSIRT, any differences in the level of maturity of the individual organisations could have an effect on the distribution of tasks and the ambition of the collective. If the participating organisations acknowledge these differences to each other, this promotes trust. Moreover, mature organisations can support the less mature organisations. This will be a positive experience for all organisations.

6 At https://www.surf.nl/en/services-and-products from SURFcert you will find a comprehensive summary of the services that they provide to the participants.

Stage 3: Grow

Increase capabilities and continue to evolve

Don't grow too fast, but keep an eye on the ambitions

You will always encounter unexpected issues in the initial operational stage. There could also be external developments that have an effect on the follow-on steps.

If growth opportunities and ambition were on the agenda in the design phase, it is now time to reconsider the follow-up. Who will consult with the new participants? How can you share more (confidential) information with each other? Is an own location or personnel required? Is there a need for other expertise or funding?

"We, the sectoral CSIRT for the Italian financial sector (CERTFin), were set up as a public-private initiative to support collaboration between banks and other financial institutions. Because of the related domain, a subsequent step that is being proposed is expanding into the insurance sector."

CERTFin

Increasing the number of participants

When consulting with a potential new participant, closely examine the motive, expectations and added value of this organisation.

By way of preparation, make sure to start from the common vision for the collective CSIRT and define what would be a logical and relevant expansion. Because collective CSIRTs usually develop from an existing connection or collective, the common characteristics can be scrutinised once again. There may be other relevant target groups to collaborate with, from a shared theme or interest. Examples include a sector or domain that is facing similar threats.

Expansion of activities

During setting up, you can already be looking towards possible expansion of activities. Often, the initial activities focus on coordinating collective efforts and information sharing.
The next step could be:

- conducting more in-depth analyses (or having them conducted);
- joint acquisition of cyber threat intelligence, software and/or hardware;
- convergence of anonymised data (networks and incidents) from the affiliated organisation;
- requesting accreditation;
- active participation in the CSIRT community by affiliation with TF-CSIRT Trusted-Introducer and/or FIRST.[7]

The next steps that are feasible and desirable depend on the needs and circumstances of the collective.

Collaboration

A logical next step is to enter into a partnership with the NCSC, other (collective) CSIRTs and other relevant organisations. Within these partnerships, trust can be expanded and additional information can be gained. Active management of relations is crucial for this since substantive collaboration can go further than simply exchanging information. Working together on specific dossiers or a shared threat is one of the possibilities. Entering into partnerships of this kind contributes to increasing resilience and capacities of your collective CSIRT.

Professionalisation

Further professionalisation of a collective CSIRT means that action is taken on:

- the basis of the collective – what can be done better?
- the organisation of the collective – what aspects still need to be arranged?
- the personnel – are the employees performing the right tasks?
- expertise – what expertise is lacking?
- tooling – what do we still need?
- exercising – is there a suitable simulation?
- work processes – is there a missing link in the chain?

At this point, the ambition during the establishment phase becomes relevant once again to determine the direction in which growth can (or must) be achieved. The current level of maturity of the collective CSIRT must be determined for this. You can read more about this in the CSIRT Maturity Kit or by taking ENISA's CSIRT Maturity – Self-Assessment Survey.[8]

7 For more information about the conditions for accreditation for internationally renowned communities of CSIRTs, see TF CSIRT' Trusted Introducer (https://www.trusted-introducer.org) and the Forum of Incident Response and Security Teams (FIRST, https://first.org).

8 You can take the survey via https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Relevant sources

Public information about existing collective CSIRTs

i-CERT

- Setting-up: https://www.verzekeraars.nl/publicaties/actueel/verzekeraars-verhogen-digitale-weerbaarheid-met-i-cert
- Agreement: https://www.verzekeraars.nl/branche/zelfregulering/overzicht/cert-verzekeringssector-convenant

SURFcert

- Service Description (RFC 2350): https://www.surf.nl/en/services-and-products/surfcert/operational-information/surfcert-service-description/index.html
- Summary of services and products and other information: https://www.surf.nl/diensten-en-producten/surfcert/index.html
- SCIRT: https://www.surf.nl/diensten-en-producten/beveiligingscommunitys/scirt/index.html

IBD

- General: https://www.informatiebeveiligingsdienst.nl
- Incident coordination fact sheet: https://www.informatiebeveiligingsdienst.nl/product/factsheet-incidentcoordinatie

Z-Cert

- General: https://www.z-cert.nl

Guidelines, tools and information about CSIRTs

- Create a CSIRT (2017). https://resources.sei.cmu.edu/asset_files/WhitePaper/2017_019_001_485695.pdf
- CSIRT Maturity Kit (2015). https://check.ncsc.nl/static/CSIRT_MK_guide.pdf
- Organizational Models for CSIRTs (2003). https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14099.pdf
- Outsourcing Managed Security Services (2003). https://resources.sei.cmu.edu/asset_files/SecurityImprovementModule/2003_006_001_14105.pdf
- Resources for Creating a CSIRT (2018). https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=485643
- The Handbook for CSIRTs (2003). https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

Other

- CSIRT Effectiveness and Social Maturity (2016). https://www.incidentresponse.com/wp-content/uploads/GMU-Cybersecurity-Incident-Response-Team_social_maturity_handbook-updated_10.20.16.pdf
- Cyber Security Incident Response Guide (2014). https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf
- Global Good Practices - National Computer Security Incident Response Teams (CSIRTs) (2017). https://www.thegfce.com/initiatives/c/csirt-maturity-initiative/documents/publications/2017/11/21/national-computer-security-incident-response-teams-csirts
- Guide for Alerts, Warnings and Announcements (2013). https://www.enisa.europa.eu/publications/awa/at_download/fullReport
- Incident Response Reference Guide (nd). https://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-emergency-doc-digital.pdf
- Inventarisatie en classificatie van standaarden van cybersecurity (2015). https://www.wodc.nl/onderzoeksdatabase/2552-inventarisatie-van-standaarden-en-normen-voor-cyber-security.aspx
- Security Incident Management Maturity Model. https://www.terena.org/activities/tf-csirt/publications/SIM3-v15.pdf
- Study on CSIRT Maturity – Evaluation Process (2017). https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process/at_download/fullReport
- Traffic Light Protocol (TLP). https://www.first.org/tlp
- Definitions and Usage | US-CERT (nd). https://www.us-cert.gov/tlp
- CSIRT Maturity - Self-assessment Survey. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Publication details

Based on research conducted by TNO.

Publication
National Cyber
Security Centre (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (0)70 751 5555

More information
www.ncsc.nl/english/cooperation
samenwerken@ncsc.nl
@ncsc_nl

October 2018