National Cyber Security Centre
Ministry of Justice and Security

Benefit more from your ISAC

A practical guide

ISAC level checklist

In order to determine how you want your Information Sharing and Analysis Centre (ISAC) to develop, you first need to understand its present status. This checklist will help you establish your current ISAC level for each capability. It could be that your ISAC is at different levels for the various capabilities. The recommendation is to review this together with all participants so as to arrive at a shared overall picture.

Strategy and action plan

	Capability	*Status*
Level 1	Has an information exchange objective been formulated in mutual consultation?	
	Have common features of the ISAC participants been shared? Consider aspects such as business processes, systems, chain responsibilities, shared challenges and incidents.	
	Do the participants free up time to be able to participate in the ISAC?	
	Do the participants receive support from their own organisation to be able to participate in the ISAC?	
	Are the job profiles and roles of the ISAC participants known?	
	Have individuals in the right job profiles been delegated to attend the ISAC meeting to achieve the intended information sharing?	
	Have agreements been made to ensure that information is shared?	
Level 2	Are the working methods and results of the ISAC discussed on an annual basis?	
	Are the ambitions, added value and activities recorded in an annual plan?	
	Are resources (funding, in-kind, personnel) made available for ISAC objectives on an ad hoc basis?	
	Has the ISAC adopted a coordinated communication strategy?	
Level 3	Have joint products and/or processes been developed?	
	Is there a road map for information sharing for the intermediate or long term?	
	Are resources (funding, in-kind, personnel) being made available for ISAC objectives on a structural basis?	
	Is the ISAC independent?	
	Are any PR activities being undertaken on behalf of the ISAC?	
	Is the ISAC accountable for the activities and results of the participating organisations?	
	Do the participants have a mandate to take decisions and act in the ISAC on behalf of their organisation?	
	Has the value case for the ISAC been explicitly formulated and recorded?	

Working method

	Capability	*Status*
Level 1	Are participants required to sign guidelines and agreements prior to being allowed to participate in information sharing?	
	Is the Traffic Light Protocol (TLP) being used?	
	Have the admission criteria, process agreements and ways of dealing with confidential (and other) information been recorded in membership guidelines?	
	Are agendas drawn up for the meetings?	
	Have the roles of chair, vice-chair and secretary been assigned?	
	Do the ISAC meetings have a clear structure (based on agendas and minutes, for example)?	
Level 2	Do the ISAC members also meet in smaller groups to address certain themes?	
	Do any activities take place outside the ISAC meetings?	
	Are the practical agreements on information sharing being adhered to?	
	Are formal documents (e.g. membership guidelines, minutes, agendas, etc.) subject to central management and accessible to ISAC participants?	
	Do the chair, vice-chair and secretary prepare the ISDAC meetings and share duties?	
Level 3	Has dedicated capacity (communications consultant, analyst, project staff, technical expert, etc.) been made available to the ISAC?	
	Are efforts being made to systematically improve the working method?	
	Are formal agreements and procedures in place with regard to the functioning of the ISAC, information exchange and internal and external cooperation?	

Information structure and information management

	Capability	*Status*
Level 1	Is information currently being shared verbally between participants?	
Level 2	Is information being recorded and exchanged according to a fixed method?	
	Is information being shared digitally whenever this is considered to be needed?	
Level 3	Is information also being shared (in a non-traceable manner) outside the ISAC?	
	Do collaboration and information exchange take place on an online platform?	
	Is information managed and stored securely on an online platform?	
	Do the participants agree on the differences between operational, tactical and strategic information?	
	Is information shared in a standardised manner, where possible?	

Situational awareness and lessons learned

	Capability	*Status*
Level 1	Has – mutual – situational awareness improved thanks to participation in the ISAC?	
	Does participation in the ISAC increase the effectiveness of mitigating measures in participants' organisations?	
Level 2	Is a sectoral environmental assessment drawn up and is this done regularly?	
	Is the environmental assessment shared with other, relevant organisations?	
	Is information interpreted and translated into strategic and tactical information?	
	Is perspective for action, when appropriate, added by sharing information (TLP: AMBER and TLP: GREEN)?	
	Are good practices determined from time to time, based on previous ISAC meetings?	
Level 3	Is the jointly prepared sectoral threat assessment shared with other relevant parties and organisations to enhance collective situational awareness?	
	Are analyses conducted and developments evaluated in a structured manner, including extrapolation regarding possible future impact?	
	Is perspective for action structurally added in sharing information (TLP AMBER and TLP GREEN)?	
	Do ISAC participants determine good practices on a structural basis, based on insights from sectoral and other trend analyses, incidents and information from previous ISAC meetings	

Action

	Capability	*Status*
Level 1	Do participants primarily engage in information exchange in order to keep their own business or organisation safe?	
Level 2	Are activities or initiatives (conducting joint research, exchanging personnel, joint threat analyses, etc.) being undertaken that focus on increasing the resilience of the sector or region?	
Level 3	Are joint activities or initiatives being undertaken to increase the resilience of the sector, region and the country as a whole?	
	Is the ISAC visible in the media, branch or region?	

Preface

You have engaged with your organisation in collaboration within your sector and have started an Information Sharing and Analysis Centre (ISAC). Of course this is a great first step, but you would like to further develop your ISAC. This practical guide is intended to help you do so.

The NCSC commissioned TNO to design an ISAC development model, based on the experiences of other ISACs. This practical guide has translated the model into practice. The checklist, for instance, will provide you with a picture of the current level of your ISAC and will help you formulate your ambition.

You will find the checklist in the cover of this document, or on english.ncsc.nl/get-to-work/cooperation. Otherwise, this guide offers various tools and strategies which could be of service in the further development of your ISAC. That way you can benefit even more from your ISAC.

Permitted dissemination TLP: WHITE
(Traffic Light Protocol)

This Next Generation ISAC guide has been given the label TLP: WHITE and is disseminated by the NCSC. The NCSC uses the Traffic Light Protocol (TLP) to clearly and unambiguously define how information may be used. The TLP designation will tell you with whom you may share the information concerned. This is described in the FIRST standard (www.first.org/tlp).

Recipients may publish information from this guide and share it within their organisation and outside of it.

Please send your responses or feedback to info@ncsc.nl.

Benefit more from your ISAC

An Information Sharing and Analysis Centre (ISAC) is an excellent way of cooperating with other players in your sector to increase the digital resilience of your organisation. By now, quite a number of ISACs have been set up in the Netherlands. They differ in various aspects (meeting frequency, number of members, focus, level of maturity), which is entirely in keeping with the ISAC model.

The NCSC commissioned TNO to design an ISAC development model, based on the experiences gained. That model has been transformed into the present practical guide. It will help existing ISACs to analyse their current working method and define their ambitions for collaboration. Offering numerous tools and strategies, this guide will contribute to the further development of your ISAC.

Target group

Information security officers (and their superiors) of businesses and organisations that already participate in an ISAC.

The following parties have contributed to this guide

ISACs in various sectors: Airports, Chemical/Oil, Energy, Financial Institutions, Port, Water Management (Keren en Beheren), Nuclear, National Government, Telecom and Water, and NZKG.

This guide is a collaboration between

the National Cyber Security Centre of the Ministry of Justice and Security, and TNO.

What is an ISAC?

An ISAC is a sectoral[1] body for consultation on issues related to cyber security in particular. Other topics such as cybercrime and data leaks can also be discussed in an ISAC. An ISAC is a trusted environment where organisations from the same sector share – and, if applicable, analyse – sensitive and confidential information on incidents, threats, vulnerabilities, measures and lessons learned in relation to cyber security.

There is no 'standard format' for an ISAC. Cooperation in an ISAC can be either formal or informal, structured or flexible, with face-to-face meetings, teleconferences or consultations via a digital platform, or a mix of these. It is up to the participants to select the most suitable format. The 'Start an ISAC' guide contains advice that allows ISAC participants to make the right choices to ensure the launch of a successful collaboration.

The ISAC development model

Experience has shown that cooperation works best when the participants themselves choose the format and working method most suited to them. This is also reflected in the current ISAC landscape. The existing ISACs differ in terms of the frequency of their meetings, the number of participating organisations, the types of information shared, and the degree of detail of this information. The added value of information exchange also differs between the participating organisations. Developing the way that information is shared therefore requires a custom approach.

If an ISAC has existed for some time, participants tend to want to get more out of their collaboration. The ISAC development model will help ISAC participants achieve that. The model has three premises:

1. Flexibility of the development model

Each ISAC determines its own ambition. The development model can be used flexibly and does not aim to impose a uniform working method.

2. Proportionality is key

The collaboration and information exchange should suit your sector, chain or region. How this is put into practice depends on various factors, such as threat level, type of technology, product or service, and the potential risks and effects of incidents. The ISAC development model offers the latitude required to achieve the right balance between the objective of the ISAC, its further development and the model itself. The development model is a tool, not an objective in and of itself.

3. Phased development

The further development of an ISAC requires time and effort invested by the participants. You can choose your own route with your ISAC and implement it in steps, using the ISAC development model, which has a modular structure

1 Although most ISACs are sectoral, the ISAC model also lends itself to cooperation within a particular chain or region. Consult english.ncsc.nl/get-to-work/cooperation for more specific advice on establishing chain or regional collaboration.

What does the model look like?

The model comprises five capabilities and three development levels.

The five capabilities are: strategy and action plan; working method; information structure and information management; situational picture and lessons learned; and action.

Strategy and action plan relates to identifying the sector's ambitions and needs, which can either remain implicit or be recorded in a joint action plan.

The ***Working method*** capability focuses on the activities and agreements that facilitate effective and efficient interaction between the ISAC participants.

Information structure and information management concerns agreements intended to efficiently specify cyber security information and possibly to classify it as well. This competence also includes the methods and means for sharing, collecting, exchanging and storing information.

The ***Situational picture and lessons learned*** capability focuses on the working methods for understanding and interpreting information and thus the capability for gaining insights and joint learning.

Due to their strong focus on information exchange, the ability of current ICASs to foster collaboration and collective follow-up based on shared information is limited. Follow-up and action perspective are subsequent responsibilities of the participating organisations themselves. The ***Action*** capability is intended for ISACs that aspire to achieve actual and practical collaboration.

The capabilities described above have been divided into three development levels. Level 1 focuses on the basic capabilities of an ISAC. Level 2 contains more developed capabilities that require additional time and effort. Level 3 comprises the advanced ISAC capabilities.

The ISAC-development model	*Level 1*	*Level 2*	*Level 3*
Strategy and action plan			
Working method			
Information structure and information management			
Situational picture and lessons learned			
Action			

How can I use the model?

The capabilities and levels are related because the development of many capabilities requires a certain basic level. The recommendation is to use the model from the top down where it concerns building capabilities. For each separate capability, it is advisable to start at and complete level 1 before moving on to level 2, etc.

Please note that this is a *recommendation* regarding the use of the model, not a strict requirement. A custom approach is possible and indeed desirable at all times.

"'To have insight, you need to know where you stand."

Step 1: Insight

Determine the current level of your ISAC

In order to determine how you want your ISAC to develop, you first need to understand its present status. A checklist has been drawn up that will help you determine your level for each capability. The advice is to do this together with all of the ISAC participants, so you end up with a shared picture and a common point of departure.

The answers to the checklist questions will help you form an impression of the current level of your ISAC. Perhaps you cannot answer 'Yes' to all the questions in the list. In that case, it is up to the ISAC to determine whether those questions are necessary for the collaboration and further development of your ISAC. Only the ISAC itself can determine whether this is the case.

The checklist can be found on the inside cover.

"If the desired situation is an improvement on the existing one, this means that there is a need to develop."

Step 2: Growth

Determine your ambition

Use the checklist to determine your ambition. However, this time you will not be looking at the existing situation, but at the desired situation.

If the desired situation is an improvement on the existing one, this means that there is a need to develop. By developing certain capabilities, you can continue to grow as an ISAC to the desired level.

In order to support this process, the overview below presents the features of each capability at each of the three levels. In addition, tools and strategies are offered that could help you achieve the desired development.

It is up to each ISAC to determine the level it wants to attain. Reaching the third level should not be viewed as an objective in and of itself. It is more important for the ISAC to consider which level is attainable and, even more crucially, which is required for its own situation. Not every ISAC will need to reach level 3. In brief, the ISAC should determine its ambition itself.

The following pages explain the various levels per capability in a table.

Strategy and action plan

An important task of an ISAC is to explicitly state its course and direction. It is advisable to describe ambitions and objectives and to reach agreement on these within the ISAC. Next, it is useful to create an action plan describing the actions required to realise those ambitions. The various development levels run from meetings with an ad hoc agenda, to the use of a road map for the long term. Note that while it is useful to explicitly state the ambitions and objectives, a bureaucratic working method should be avoided. Taking a pragmatic approach which suits your ISAC is recommended.

Points for attention:

- Monitor whether all participants are clear on the ambitions and the intended development path for their ISAC.
- If any participants are unable or unwilling to free up enough time for active participation, be sure to discuss the fact.

	Features of the 'Strategy and action plan' capability, per level:	*Tools and strategies*
Level 1	ISAC participants receive support from their own organisation to be able to participate in the ISAC. The ISAC participants have formulated their joint interest in, and objective of the collaboration. All ISAC participants have an equal status, i.e. there are no hierarchic relationships. The participants have discussed what types of information are to be shared. The participants have discussed the manner in which information is to be shared.	The NCSC has provided a guide on starting an ISAC; see: 'Launch an ISAC: Sectoral collaboration'. More information is provided by the American Information Sharing and Analysis Organisations, which was founded to share information on cyber security, in a low-threshold publication on the basic principles of information sharing: 'Sharing and Analysis Organisation 100-1 Introduction to Information Sharing and Analysis Organizations' (2016).
Level 2	The ISAC has drafted an annual plan setting out its ambition, added value and activities for the year. Resources (funding, in-kind, personnel) are made available for ISAC objectives on an ad hoc basis. Periodic (annual) evaluation takes place, discussing the working method and results of the ISAC. The ISAC encourages the sector participants to make agreements related to communication and spokesmanship in the event of any incidents, such as data leaks, and on trends and threats in the sector.	Consider staging a workshop to determine a strategy and activities schedule for the forthcoming year. Record the strategy and activities schedule in an annual plan. Schedule an evaluation at the end of the year to review the annual plan and make new agreements for the next year. Ensure that the colleagues involved in communications and/or press relations know each other or can readily get in touch, by holding a meeting or creating an overview.
Level 3	A long-term vision and/or long-term road map has been drafted for the ISAC. The ISAC has drawn up a communication strategy. Resources (i.e funding, in-kind, personnel) have been made available for ISAC objectives on a structural basis. The value case for the ISAC has been formulated explicitly and in writing.	Organise a workshop to draft the long-term vision and communication strategy. The TNO publication on value cases could provide useful information for writing the ISAC value case; see: 'TNO Value Case Methodology'.

Working method

Sharing information is made easier by making agreements. The three development levels vary from using the Traffic Light Protocol and establishing membership guidelines, to upholding formal agreements and procedures.

Points for attention:

- As a group, keep tabs on the number of ISAC participants and take measures when the number of participants is too high to ensure mutual trust.
- The working method can have a major influence on sharing information efficiently and effectively, so it should have your constant attention.
- Make agreements on what to do if an ISAC participant repeatedly fails to attend ISAC meetings.

	Features of the 'Working method' capability, per level:	*Tools and strategies*
Level 1	The Traffic Light Protocol (TLP) is used to encourage information sharing and to determine the extent of the target group. The roles of chair, vice-chair and secretary have been assigned. The admission criteria, procedural agreements and approach to confidential (and other) information have been set out in membership guidelines which have been signed by all of the participants. ISAC meetings are structured by using an agenda and taking minutes. Each ISAC participant has a standard substitute in order to safeguard continuity.	Ensure that all participants inform each other of the TLP rules and adhere to these. To this end, read the FIRST Normdefinities en Gebruiksrichtlijnen (FIRST standards definitions and guidelines for use) and consult the webpage entitled 'Considerations on the Traffic Light Protocol' on the ENISA website. The NCSC has made publications available on setting up a collaboration within a region or chain, with various example templates.
Level 2	The chair, vice-chair and secretary prepare the ISAC meetings and divide up the tasks (e.g. inviting guest speakers, drawing up the annual plan, taking specific actions based on the annual plan, creating or appointing working groups). Activities will also be taking place outside the ISAC meetings, with ISAC participants gathering in smaller (thematic) groups to discuss specific subjects and delve further into topics in working groups. Formal documents (membership guidelines, meeting minutes, agendas etc.) are subject to central management and accessible to all ISAC participants.	Analyse and evaluate the tasks, responsibilities and time required for holding an ISAC meeting. Organise ad hoc working groups on specific themes and ensure that the resulting knowledge then flows back to all ISAC participants. Organise introductory sessions or joint meetings with other ISACs.
Level 3	The ISAC allocates dedicated capacity to achieving its objectives (as formulated in the annual plan). The working method is being systematically improved. Formal agreements and procedures are in place with regard to the functioning of the ISAC, information exchange and internal and external cooperation.	Experiment with various and/or new ways of working by learning from other national and international ISACs and partnerships. A document detailing best practices for secure information management is available in the ISO/IEC 27002 Best Practice for Information Management System.

Information structure and information management

The ISAC is only as good as the information which is shared. In this regard, that information should also be useful for the ISAC members' own organisations and for others in their environment (customers, buyers, suppliers). Agreements for this, procedures to ensure that information is recorded in a uniform fashion, central information management – these are all examples of matters that contribute to ISAC development. They will increase the information's findability, security and scope. A digital platform for confidentially sending and receiving information on incidents, threats, vulnerabilities, measures, administrative data and learning points will help to put information sharing on a more professional footing. The three levels of the 'Information sharing and information management' capability vary from the ad hoc sharing and storage of cyber security information to the standardised and structured storage and exchange of information.

Points for attention:

- Evaluate regularly whether the right parameters exist for sharing information.
- Make agreements on the management and use of tools.

	Features of the 'Information structure and information management' capability, per level:	*Tools and strategies*
Level 1	Information is shared verbally between ISAC participants.	Make a list of the various types of incidents (DDOS, data breach, phishing, etc.) and use it for sharing information during the agenda item referred to as the 'Indepth Sharing TLP: RED' (*rondje rood*).
Level 2	Information which is shared in an ISAC meeting is methodically recorded and exchanged. Digital exchange of information takes place as needed.	The information shared in 'Indepth Sharing TLP: RED' during the meeting may only be used by the ISAC participants. In order to disseminate this information further so that other internal and external parties can also benefit from it, it will have to be assigned AMBER status. The Template Ambering form on ncsc.nl can be used to this end. Use mailing lists, secure app groups, conference call software, etc. Publication: ENISA, Group Communications for incident response and operational communities.
Level 3	Information is shared with parties outside the ISAC. Information is managed, stored and exchanged securely using an online platform. ISAC participants exchange information and collaborate on an online platform. A distinction is drawn between operational, tactical and strategic information. For as far as possible, information exchange is standardised.	Reach agreements with other ISACs and organisations on sharing information outside the ISAC, and record these agreements, for example in the membership guidelines. Establish guidelines for (safely) using a platform. Existing common standards (such as ISO/EC 2700:x) can serve as guide to the secure management, storage and sharing of information. Information on and best practices concerning information security (from a government perspective) are available via the Centre for Information Security and Privacy Protection (*Centrum Informatiebeveiliging en Privacybescherming*).

Situational awareness en *lessons learned*

When information about developments in a sector or branch is shared, this ensures that everyone is aware of important events. The 'Situational awareness and lessons learned' capability contributes to increasing the learning ability of the ISAC. This comprises the analysis, explanation and enrichment of information (incidents, threats and the mitigation of incidents) and the structural exchange of best practices and action perspectives. In brief, this capability focuses on aspects related to the 'A' (analysis) in ISAC. The development levels of situational awareness and lessons learned vary from ad hoc discussions on incidents, developments and threats, to adopting methods to record information, analyse it, disseminate it and learn from it in a structural sense.

Points for attention:

- The absence of clear agreements on information sharing can erode mutual trust.
- Note that ISAC participants may have different ideas about sharing and disseminating situational awareness insights which are specific to their business, despite any efforts to anonymise the information.

	Features of the 'Situational awareness and lessons learned' capability, per level:	*Tools and strategies*
Level 1	Participating in an ISAC increases the insight of organisations with regard to threats and vulnerabilities, and so supports the effectiveness of the mitigating measures of individual ISAC participants.	
Level 2	Regular sectoral environmental assessments help to improve situational awareness. The environmental assessment is shared with other relevant organisations. Information is interpreted within its proper context and translated into strategic and tactical information. In sharing information (TLP AMBER and TLP GREEN), an action perspective is added when appropriate.	Establish a working group to record the most important insights from the ISAC in a sectoral report. Record the action perspective and share it with other ISACs.
Level 3	Sharing sectoral threat and environmental assessments helps to enhance situational awareness. Developments are analysed and the resulting insights translated to future developments to enhance situational awareness. Action perspectives are added which can be structurally divided up when information (TLP AMBER and TLP-GREEN) is shared. Good practices are determined on a structural basis, based on insights from sectoral and other trend analyses, incidents and information from previous ISAC meetings.	Request support from ISAC partners in drafting a sectoral report. Use information from other ISACs (in the Netherlands and abroad) and other partnerships. Publication: MS-ISAC, Water ISAC Announce Partnership to Promote Cross-Sector Security Collaboration. There are various future-oriented methods available which allow signals and potential threats to be recognised at an earlier stage. This could include horizon scanning activities, for instance. Get in touch with European ISACs or with similar ISACs abroad.

Action

The information exchange and analysis in an ISAC create opportunities to work together more closely or differently, and to jointly follow up on the insights gained. Examples include shared research programmes, exchanging personnel, publishing reports, and acting as a group on behalf of a sector or chain. Within the 'Action' capability, the levels of development vary from focusing on the resilience of your organisation to focusing on the sector or Dutch society at large.

Points for attention:

- Not all participants in the ISAC have the same mandate. If any activities other than information sharing are undertaken, the mandate of individual ISAC participants must be taken into account. Make explicit agreements about this.

	Features of the 'Action' capability, per level:	*Tools and strategies*
Level 1	Activities are focused on the resilience of the individual ISAC participants.	
Level 2	Activities are undertaken which focus on increasing the resilience of the sector and/or the region.	Conducting or commissioning research together can have added value for ISAC participants and for the sector. Provide students, interns and researchers the opportunity to conduct research focused on the sector. Promote staff exchanges to facilitate the sharing of knowledge and experiences. Encourage knowledge sharing between ISACs by organising joint meetings.
Level 3	Activities are undertaken which focus on increasing the resilience of the sector and of the Netherlands at large. The ISAC has a visible presence in the media, branch or region, thanks to proactive information sharing.	Make information available to other organisations on an annual basis, for example through coordinated participation in campaigns. The ISAC can undertake joint action during consultations or discussions on standardisation and new legislation.

"In future, ISACs will be able to act more proactively, in order to increase control over digitisation, the speed of technological developments, and shifting threats."

Step 3: Development

Setting to work

Developing capabilities costs time, energy and – in some cases – money too. It is inadvisable to develop seven capabilities all at once; indeed, tackling no more than two capabilities at a time is recommended. Ideally, the development ambition and related planning schedule should be included in the ISAC's strategy and action plan.

Beyond the model

There are other development activities outside the confines of this model that an ISAC can consider as well.

An ISAC could consider formalising its collaboration in a foundation in order to combine resources, which can help to professionalise the ISAC and build its capabilities.

Activities that go beyond the ISAC or the ISAC development model include formalising the collaboration by starting a joint sectoral CERT/CSIRT[2], automated sharing of information[3], and the purchase, analysis and (automated) processing of threat information.[4]

In future, ISACs may become more proactive by working with cyberforecasting information in order to gain more control over digitisation, the speed of technological developments and shifting threats.

The model is intended as a precursor to the next steps, although of course there are other ways to achieve the objective. Applying whatever suits your ISAC best should always be the main priority.

Further reading

- ENISA publication on cyber security behavioural aspects, 2019, https://www.enisa.europa.eu/news/enisa-news/behavioural-aspects-of-cybersecurity
- Cooperation in an ISAC | Setting to work, 2018, National Cyber Security Centre, https://english.ncsc.nl/get-to-work/cooperation/i-would-like-to-start-collaboration/sectoral-cooperation-isac
- Membership guidelines of the American Research Education Networking Information Sharing & Analysis Center (REN-ISAC), https://www.ren-isac.net/membership/MembershipDocs/REN-ISAC_Membership_Guide.pdf
- The MaGMa Use Case Framework (UCF) helps organisations to operationalise their security monitoring strategy. Management, Growth, Metrics & assessment; Use Case Framework (UCF), https://www.betaalvereniging.nl/veiligheid/publiek-private-samenwerking/magma
- Fact sheet on designing and setting up an SOC: start small and Measuring capability maturity in Security Operations Centers (SOC-CMM), https://english.ncsc.nl/get-to-work/build-an-soc
- Handboek MISP (MISP handbook) and Guide to Cyber Threat Information Sharing, NIST Special Publication 800-150, https://www.circl.lu/doc/misp/book.pdf
- Cyber threat intelligence sharing through national and sector-oriented communities, Frank Fransen & Richard Kerkdijk; Collaborative Cyber Threat Intelligence, Auerbach Publications, 2017. pp. 187-224, https://www.crcpress.com/Collaborative-Cyber-Threat-Intelligence-Detecting-and-Responding-to-Advanced/Skopik/p/book/9781138031821

2 Fact sheet on designing and setting up an SOC: start small and Measuring capability maturity in Security Operations Centers.

3 MISP handbook and Guide to Cyber Threat Information Sharing, NIST Special Publication 800-150

4 Cyber threat intelligence sharing through national and sector-oriented communities, Frank Fransen & Richard Kerkdijk; Collaborative Cyber Threat Intelligence, Auerbach Publications, 2017.

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
english.ncsc.nl
info@ncsc.nl
@ncsc_nl

January 2020