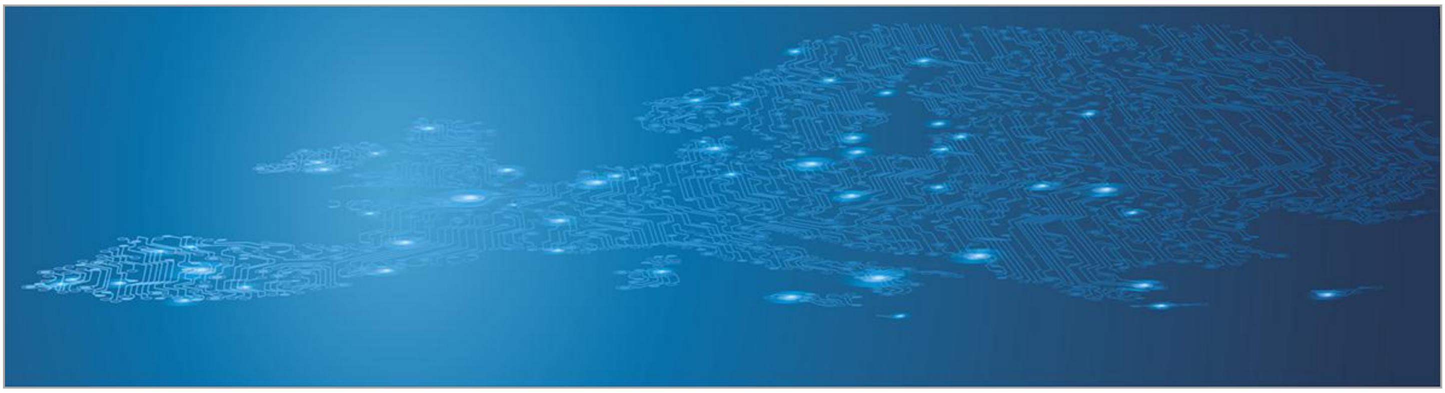


Detect, SHARE, Protect

Solutions for Improving Threat Data Exchange among CERTs

October 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector, and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Editors and Authors

- ENISA (main editor, Romain Bourgue)
- IDC (Joshua Budd, Jachym Homola, and Michal Wlasenko)
- Dariusz Kulawik, dkConsulTec (external consultant)

Contact

To contact the authors, please email cert-relations@enisa.europa.eu

For media enquires about this paper, please email press@enisa.europa.eu

Acknowledgements

We would like to thank all the teams that took part in the survey for this project. We would also like to thank those teams that provided input beyond the survey, in the form of face-to-face and telephone interviews or via further email correspondence.

We also wish to express our thanks to the contributors and reviewers of this report: Luc Dandurand (NATO Communication and Information Agency), Alexandre Dulaunoy (CIRCL), Kathleen Moriarty (EMC), Dan Tofan (CERT RO), Jan Vykopal (CSIRT-MU) and Wes Young (REN ISAC).

Acknowledgement should also be given to ENISA colleagues who contributed to this project, in particular: Rossella Mattioli, Cosmin Ciobanu and Jo De Muynck.

Legal Notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of external sources, including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Executive Summary

The ever increasing complexity of cyber-attacks requires more effective information sharing among Computer Emergency Response Teams (CERTs). **Local detection**, accompanied by trusted forms of information exchange, leads to **global prevention** of cyber-attacks. In other words, it is very beneficial for the successful identification (and subsequent handling) of an incident, if it has already been detected by CERTs sharing this information. Furthermore, effective information sharing saves time and effort in incident response and post-mortem analysis, increases synergies and aligns practices among CERTs.

Much progress has been made recently in establishing national/governmental (n/g) CERTs in Europe. All these teams, which are at different maturity levels, actively take on the job of coordinating responses to cyber-attacks. As the nature of cyber-attacks is often global, it is crucial that responses to these incidents are coordinated not only within national boundaries, but also at a cross-border level. In order for this to happen, **secure and effective information exchange and the sharing of information on such incidents** must take place.

Despite fruitful cooperation between many CERTs (n/g and others) bringing visible results in improving cyber security in EU member states (for example TI Certification or TRANSITS CERT trainings), the teams still face obstacles that work against seamless security information exchange and sharing. The key problems for effective information sharing are legal and technical barriers, as well as lack of interest from cybersecurity stakeholders in sharing information.

While trying to promote interoperability of solutions and cooperation between CERTs, improvements to information sharing must build on existing solutions and standardisation efforts in data exchange formats. A number of recent initiatives aim to streamline and make data sharing effective among CERTs[1]. These initiatives are being developed by (n/g and other sector) CERTs in Europe, by NATO, or by private companies and are driven by “cyber community” interests. Some of them have already attracted solid user communities, and they tend to be user-friendly and flexible, as they are mostly open source.

It is important to make all these approaches **interoperable**, irrespective of incident feeds, information exchange formats, or the ticketing systems used.

ENISA has identified a set of recommendations targeted to itself, the CERT community and other security actors aiming at:

- Promoting the continuity of incident feeds, which are often changed without prior notice
- Making existing tools interoperable and promoting the use of standards for data exchange
- Enhancing the functionality of existing tools as regards:
    - Interoperability
    - Correlation engines for incident analysis
    - Improved threat intelligence
    - Advanced analytics and visualisation for massive numbers of incidents
    - Automatic prioritisation

The European Union, including ENISA, can help n/g CERTs in this process, which will further facilitate the exchange among them of information on incidents.

[1] These initiatives are discussed in more detail throughout the report.

Table of Contents

List of figures

1 Introduction

1.1 Objectives and Scope

The focus of this report is on the **threat and incident information exchange and sharing practices used among CERTs in Europe**, especially, but not limited to, national/governmental CERTs. It aims at:

- Taking stock of existing communication solutions and practices among European CERTs
- Identifying the functional and technical gaps that limit threat intelligence exchange between n/g CERTs and their counterparts in Europe, as well as other CERTs within their respective countries
- Defining basic requirements for improved communications interoperable with existing solutions

This report aims at building on existing solutions and promoting achievable good practices, rather than offer unrealistic "revolutionary" solutions. It needs to be said that this is an overview of a quickly evolving domain, which necessitates frequent updates in line with the evolving environment of cybersecurity and cybercrime.

1.2 Europe's Involvement in Supporting Secure and Effective Information Exchange and Sharing

Many EU documents have stressed the importance of CERTs, especially their early warning and incident response capabilities. Most recently, a proposal for a *Directive on network and information security*[2], which accompanies the EU Cyber Security Strategy[3], addressed the topic of secure information systems. Article 9 of the proposal for the Directive states that the exchange of sensitive and confidential information shall take place through secure infrastructure.

The European Commission is empowered to adopt supplementary acts on the definition of criteria to be fulfilled by EU member states in order to be authorised to participate in the secure information system regarding the following:

a) The availability of secure and resilient communication and information infrastructure at a national level, compatible and interoperable with the secure infrastructure of the cooperation network

b) The existence of adequate technical, financial, and human resources, as well as processes for the relevant competent authority and CERT, to allow effective, efficient, and secure participation in the secure information-sharing system

1.3 ENISA's Involvement in the Area of Secure Communication and Information Sharing among CERTs

ENISA aims at supporting the process of establishing secure systems for information sharing, like the one mentioned in the draft Directive. Since 2005, ENISA has been running a programme dedicated to the capability building of national/governmental CERTs. A recent ENISA project resulted in a good

[2] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[3] Ibid.

practice guide for CERTs on honeypots for the proactive detection of IT security incidents.[4] ENISA also maintains training and exercise material focussing on enhancing the capabilities of CERTs in EU Member States (and beyond).[5] The emphasis was put on practical and applicable material about current technical and operational topics, and ENISA intends to continue maintaining and extending its CERT training library in the coming years. At the same time, ENISA is paying increased attention to the legal aspects of information sharing.[6]

One of the more in-depth studies commissioned by ENISA in recent years was *Proactive Detection of Network Security Incidents*[7]. This community-driven effort investigated proactive ways in which CERTs detect incidents targeting and affecting their constituencies, identified good practices and common mistakes, and recommended options for improvement.

ENISA also dealt with the specific topic of secure communication between CERTs and produced a report entitled *Secure Communication with the CERTs and Other Stakeholders*[8]. The focus of the earlier work was rather on communication channels (PGP, S/MIME, VPN, etc.). The 2013 project aims at a broader and more pragmatic approach by taking into consideration all collaborative tools like sharing infrastructures, messaging systems, ticketing systems, incident handling and notification systems, and so forth. These tools are hereafter referred to as communication solutions – used by CERT teams in the exchange of information between them.

1.4 Target Audience and Scope

The intended target audience for this report is primarily the national/governmental CERTs but in principle it is applicable for any kind of CERT, in Europe and worldwide. The report is tailored to be useful for both well-established CERTs and new/upcoming teams.

[4] http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-of-security-incidents-II-honeypots
[5] http://www.enisa.europa.eu/activities/cert/support/exercise
[6] http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing
[7] http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report
[8] http://www.enisa.europa.eu/activities/cert/other-work/files/secure-communication

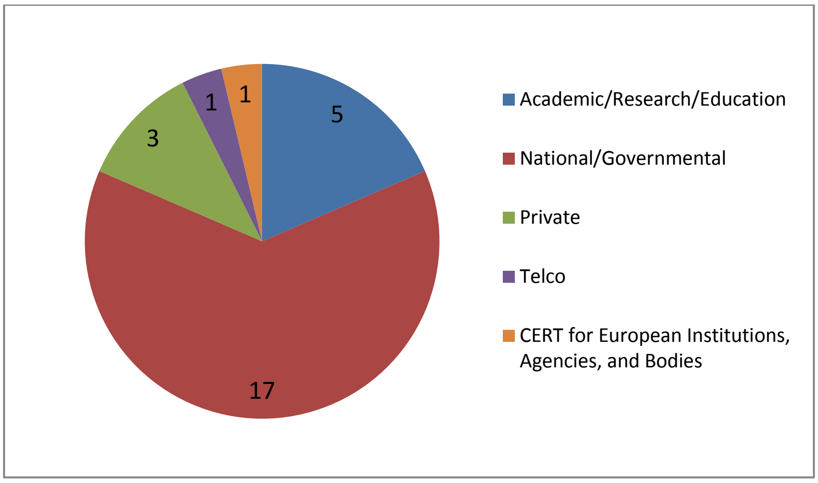
2 Overview of the Methodology

For the purposes of this report, several methodological approaches (in addition to basic desk research) were applied: surveys, interviews, and a dedicated workshop that enabled a free exchange of ideas between the interested stakeholders – national/governmental CERTs.

Survey

A survey was developed on the current communication practices of CERTs vis-à-vis other CERTs in their respective countries, their counterparts in other countries, and operators and ISPs. A total of 27 teams have responded to the survey, with the majority (63%) of them being national/governmental CERTs in Europe. While the majority of the responding teams came from EU countries, responses also came from the U.S., Asia, and the Middle East[9].

Figure 1: Completed Survey by CERT Type



Interviews

Based on the survey output, accompanying interviews were held with stakeholders in order to clarify and go beyond the replies received. These interviews were held electronically, via email correspondence, and actually in person in one case. In total, 12 interviews were conducted.

Face-to-Face Workshop

During a TF-CSIRT[10] meeting in Bucharest, a face-to-face workshop was held on 24 May 2013. At the meeting, the interim results of the project were presented to the participants (14 in total). Also, the participants presented and discussed initiatives aimed at enhancing the communication practices of CERTs.

[9] Responding teams came from: Austria, Azerbaijan, Belgium, Bulgaria, Czech Republic, European Union, Finland, France, Greece, Hong Kong/China, Japan, Latvia, Luxembourg, Netherlands, Romania, Slovenia, South Korea, Spain, Taiwan, United Arab Emirates, USA

[10] TERENA's Task Force CSIRT promotes collaboration and coordination between CERT teams in Europe. See http://www.terena.org/activities/tf-csirt/

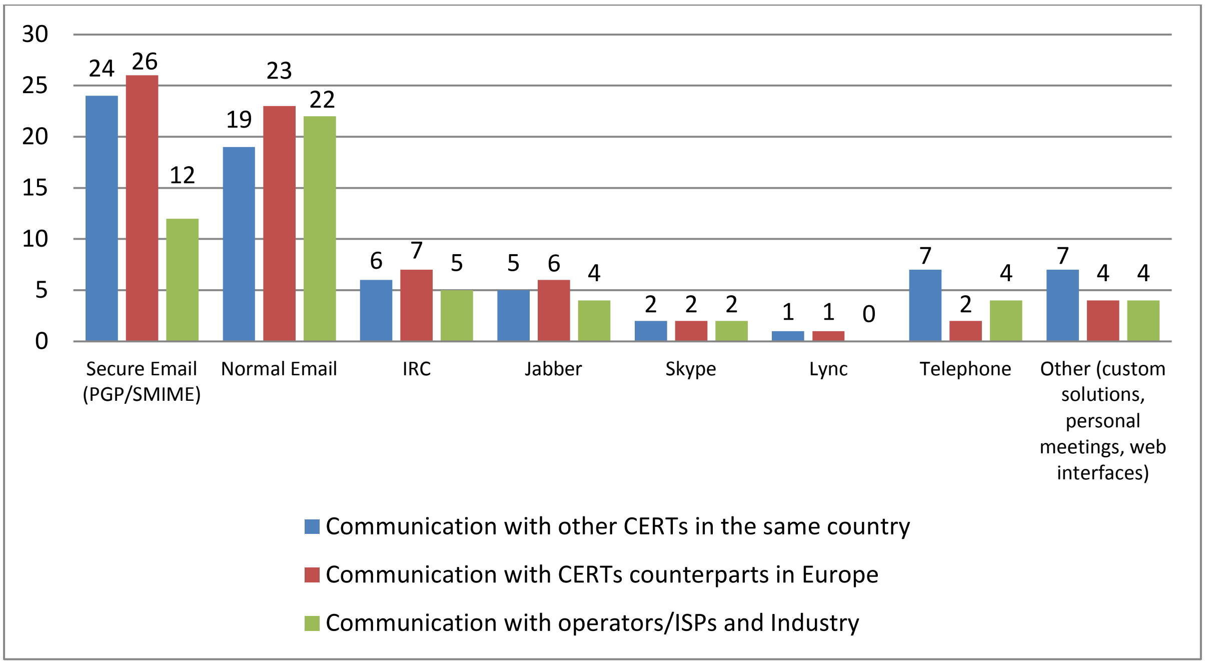
3 Findings of the Survey

This section presents the main findings of the survey on information exchange and sharing practices among CERTs. First it provides a summary of main communication solutions used by the teams, followed by identification of barriers and requirements for such effective and information exchange.

3.1 Overview of n/g CERTs' Communication Practices and Solutions

It is noteworthy that the main communication practices between n/g CERTs from different member states do not differ from those between n/g CERTs and other CERTs in the same country (see Figure 2).

Figure 2: Use of Communication Solutions among CERTs



Number of respondents: 27 CERTs

3.1.1 Secure and Regular Email

> *'Secure email is the preferred way of communicating, mainly because it is easy to use, simple, and flexible, allows for fast communication, and, most importantly, is the most common tool everyone can support.'*
>
> – One of the surveyed CERTs

Secure and/or regular email is by far the most popular communication solution used in CERTs' everyday operations.

Email communication has a few features that make it an optimal tool for sharing unstructured information between organisations. It is truly universal (everyone uses email), interoperable (it works on almost any operating system), asynchronous (users do not have to be logged in at the same time), and can carry attachment files of any type (albeit limited by size). For the purposes of secure communication, email can be encrypted, ideally by using asymmetric encryption methods.

Most of the queried CERTs have reported that they are using PGP encryption[11] for the purposes of secure information exchange within the CERT community, while S/MIME is used more rarely. Secure email with PGP is an informally adopted standard within the CERT community and the wider Internet security community in general.

While the use of secure email is common in the CERT community, both the survey and conversations with CERT representatives revealed that other stakeholders (ISPs, public administration, police, etc.) lack the culture of secure communication in general: Communication between CERTs and other parties therefore happens most often via unencrypted email.

Due to a certain degree of impracticality of secure email in everyday use, CERTs often decide on a case-by-case basis whether to send information via secure email, regular email, or another solution, such as fast and easy-to-use chat clients.

Worldwide, CERTs communicate primarily with their counterparts in other countries, but they also communicate with ISPs and system administrators, for example when a particular incident is not covered by a particular CERT. On a national level CERTs communicate most often with ISPs.

The majority of CERTs are satisfied with PGP-encrypted email as the basis for secure information exchange in their everyday operations. The incident-related sensitive information that is typically shared is only partly structured, is text-based (therefore easily compressible), and is often both machine- and human-readable. Furthermore, email as an information transportation mechanism is open and universal, which CERT experts truly appreciate.

While many CERTs admit that secure and regular email may not be quite optimal tools for information sharing in general and within the CERT community in particular, a commonly shared opinion was that any better tool would be virtually impossible to implement due to diverse requirements from different teams. However, CERTs are facing an ever increasing amount of data related to incidents, and secure email communication doesn’t scale easily. Teams reported that management of PGP- or S/MIME keys gets more and more complex as the number or recipients grows, that emails are difficult to process automatically and that they can’t cope with large data volumes or high rate of incidents due to this shortcomings. In order to reflect the changing requirements for information exchange due to large volumes and lack of common structure, some CERTs look into alternatives. It should be noted, that sharing of more data is not necessarily an improvement per se. Instead, it is important to pay attention to the quality rather than to the quantity of information.

3.1.2 Instant Messaging

The landscape of instant messaging solutions in use in the CERT community is fragmented. Solutions include (in order of popularity): IRC[12], Jabber/XMPP[13], Skype[14], and Lync[15]. No solution was found to be a clear leader in popularity; however, IRC and Jabber were generally mentioned more often than Skype and Lync.

A few interviewed CERTs stressed that, while chat clients are not absolutely crucial to their daily operations, they are indeed helpful and must be included in this guide.

[11] See http://www.imc.org/smime-pgpmime.html on PGP and S/MIME
[12] See http://www.irc.org
[13] See http://xmpp.org
[14] See http://www.skype.com
[15] See http://lync.microsoft.com

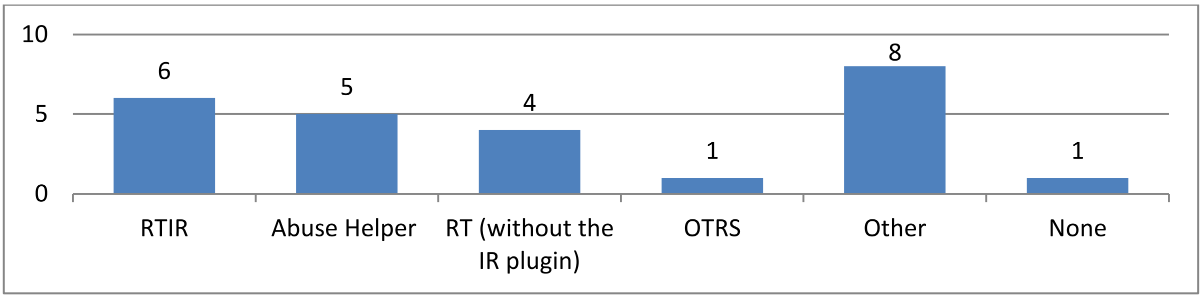
In contrast to email, IM typically requires both (or more) communicating parties to be present at their terminals at the same time so as to communicate almost instantly. Chat clients facilitate the rapid exchange of ideas and technical details, while giving the users instant feedback and a platform for an active, real-time discussion. As a communication tool, the IM family is considered to be of lower latency and less formal than email. Although solutions exist to secure instant messaging communication[16], a minority of teams uses them. The solutions in use today can be considered more as supportive rather than as primary communication channels.

3.1.3 Secure Message Boards and Closed Mailing Lists

Interviews have shown that, apart from obvious tools such as secure email and instant messaging, another class of decades-old and still very useful tools – closed Mailing List (i.e. TI-accredited CSIRTs, or ENISA N/G CERTs ML) and message boards or forums – have also proved useful in secure information sharing among the CERT community. These fora allow groups of authenticated users to share and discuss security-incident-related insights. They provide ways to communicate with a whole spectrum of trusted experts, while providing strong security mechanisms; for example, to have access to it, one needs to be invited by one established member of a given forum and to be recommended by another.

3.1.4 Incident Handling and Ticketing Systems

Figure 3: Use of Ticketing and Incident Tracking Solutions



Number of respondents: 25 CERTs

Almost all CERTs report that they are using some kind of ticketing or incident tracking system. The most popular ticketing system was found to be Request Tracker[17] (RT). Request Tracker for Incident Response[18] (RTIR) was found to be the most popular tool for incident response tracking – unsurprisingly so, as the tool is a purpose-built product for the computer security community. Another tool developed for CERTs and ISPs, AbuseHelper[19], was found to be the most popular for the purposes of automatic process incident notifications. Other solutions the interviewed CERTs use include the BMC Remedy Action Request System[20] (BMC ARS), the Open Source Ticket Request System[21] (OTRS), and MS Sharepoint[22]-based or MS Excel-based in-house ticketing systems.

RT and RTIR

[16] See OTR http://otr.cypherpunks.ca/ or http://safetyjabber.com/
[17] See http://www.bestpractical.com/rt/
[18] See http://bestpractical.com/rtir/
[19] See http://abusehelper.be
[20] See http://www.bmc.com
[21] See http://www.otrs.com
[22] See http://sharepoint.microsoft.com

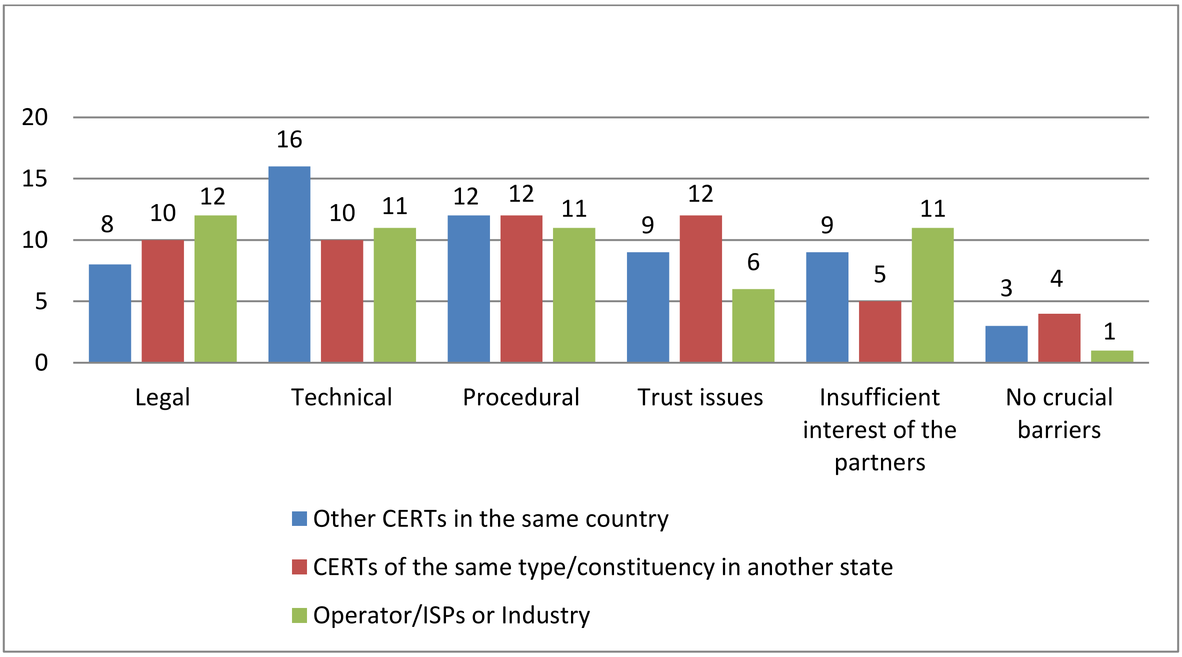
CERTs recognise and appreciate that RTIR has, in fact, been designed with the CERT community in mind, and together with that community. RT-based platforms are recognised to be working adequately for the specific purposes of CERTs. They are believed to have the most optimised workflow out of the box, are integrated with email (including the handling of the PGP security protocol), and are flexible, easily customisable, extendable, and interoperable with other systems. Multiple users are able to handle the same incident, and reports are easily generated. User interfaces include a web interface, email, a command line tool, and programmable application programming interfaces (APIs). Some teams reported having problems when handling large amounts of data related to a ticket or when using the automatic incident notification. They are now looking for alternatives.

3.1.5 Customer Relationship Management Systems

A significant majority of CERTs do not use customer relationship management (CRM) systems. Those that do, use CRM solutions delivered by Oracle, SAP, Microsoft or other parties, with no clear leader among the mentioned systems.

3.2 Barriers to and Requirements for Information Exchange and Sharing

Figure 4: Main Obstacles to More Secure and Effective Communication



Number of respondents: 22 CERTs

Technical issues were identified as the most common barrier to more effective information exchange between CERTs. These technical issues mainly concern the automated exchange of data about security incidents. Another issue mentioned was the quality of the data[23].

One solution for automated processing of incident reports is the already mentioned tool AbuseHelper. Even though, as shown in Figure 3, it is used by only five out of a sample of 25 CERTs right now, many other CERTs are also looking into using it. AbuseHelper has the potential to become

[23] In 2014, ENISA will carry out a project for good practice in this field.

the most popular tool for this purpose[24], or at least build the basis for a tailor-made in-house solution that, according also to other studies[25] many teams apply (in Figure 3, these are collated in the 'Other' category).

We have identified a consensus in the CERT community with regard to the severity of challenges in the daily operations of CERTs. Technical barriers, though being most common, are generally thought to be more easily overcome than legal issues. As for information exchange with CERTs of the same type in other states, legal barriers and trust issues are more often cited as hindering this exchange. Additionally, CERTs often cite a low level of interest among operators in sharing information they have or in acting upon the information CERTs shared with them.

3.2.1 Legal and Procedural Obstacles and Requirements

Issues around the legal and procedural aspects of information exchange between CERTs and other stakeholders were among the most frequently cited, both in the survey and especially in the in-depth interviews.

Essentially, CERTs and other similar organisations have doubts about whether a particular set of information can be shared at all, with whom, on what conditions, after what treatment, and so on. CERTs are often unsure about what sort of information can be exchanged so as not to pose legal questions regarding data protection and privacy protection. Privacy commissioners in various EU member states have a range of interpretations of how personal information is defined. For example, an IP address can qualify as personal information in one country but not in another. Categorisation is another issue in terms of which types of personal data should receive the highest level of protection. Due to such privacy questions being complex at times, extensive information sharing between CERTs and other actors is often inhibited.

According to some opinions, the legal problems do not only result from lack of harmonisation of data protection law across the EU, but also in the different interpretations of the law by different bodies.

Interviewees often indicated that these problems are even more severe than the technical challenges mentioned before, like a lack of a web portal or other means.

Many interviewees claimed that, in order to help with the issues described here, common standards should emerge in the interpretation of data protection law across the EU, at least in matters relating to cyber security incidents (which is out of scope of this particular report). For more information on the legal aspects of information sharing, see the ENISA study entitled *A Flair for Sharing – Encouraging Information Exchange between CERTs*.[26]

On the operational side, with incidents that require looking up details on entities that are responsible for URLs and IP addresses under investigation, a European forum exists that has a database of all European IPs and their corresponding owners (the Regional Internet Registry[27], or RIPE); however, the data in this registry is quite difficult to retrieve, and it can sometimes be impossible to find the entity responsible for an IP address.

[24] ENISA will further investigate how to support the community more actively in the field of automated processing of actionable information in 2014

[25] http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report

[26] http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing

[27] See http://www.ripe.net

3.2.2 Trust Issues – Barriers and Requirements

> *'The single most important requirement is trust. Trust can germinate through real-life contact and grows with regular (virtual) meeting. A secure European platform for communication can facilitate – but never replace – trust.'*
>
> – One of the surveyed CERTs

Trust issues are among the most crucial obstacles to enhanced and effective communication between CERTs and other stakeholders. Some interviewees have pointed out that, in the particular community of cybersecurity experts, trust is the single most important feature of a successful cooperative relationship.

To illustrate the consequences of a lack of trust between stakeholders, one of the interviewees noted that they had even stopped sharing security incident information with people/organisations that had committed actions that had destroyed trust between the parties, meaning that no further information was exchanged between the parties. Also, trust is undermined when only one party is active in sharing information, without getting much in return from the other party.

Situations in which trust between members of the community is diminishing or non-existent have the immediate effect of undermining the value of information shared: the size of the community. As a general observation it can be stated that the larger a sharing community is, the less valuable and less sensitive is the information and the less timely is the sharing. In other words, trust doesn't scale and needs to be paired with effective information sharing tools[28]. Protocols such as TLP allow for information to be shared in a more structured way in face-to-face communication.

3.2.3 Insufficient Interest from Partners

Within the realms of CERT-to-CERT communication, insufficient interest from partners is a very rare phenomenon. Only five of the teams responded like this.

Conversely, the in-depth interviews have confirmed the rich culture of information sharing present within the European CERT community. Typically, CERTs are not only willing to share security incident information as it happens but also to write up summary reports and share them with the community. These reports are typically very well received and appreciated within the CERT community; however, due to very heavy workloads, they are often delayed. When CERTs are handling an incident, experts focus on its mitigation and on coordination with others, and they sometimes lack the time to share reports with other CERTs. Large-scale incidents are a primary example of a situation that sparks report writing and sharing. The culture of information sharing and demand for it is definitely not an issue, but workloads are often a major inhibitor.

3.2.4 Technical Barriers and Requirements

> '*Every communication channel with each partner or type of partner CSIRT is unique. This does not scale well, and to have more fruitful, 'full-duplex', trusted engagements, standard procedures and protocols need to be established and relied upon.'*
>
> – One of the surveyed CERTs

Before moving into discussing the more technical side of issues regarding secure information exchange within the CERT community, it needs to be stated again that many interviewees mentioned that, compared with legal, procedural, and trust issues, technical deficiencies, such as the lack of a web portal or incident repository and the proliferation of communication channels, are of

[28] In 2014 ENISA will carry out a project in the area of trust building among or within communities

less significance. It is easier to find a common ground on overcoming these technical barriers than solving complicated international legal issues often pertaining to the areas of national interests and sovereignty.

Nevertheless, technical issues do exist:

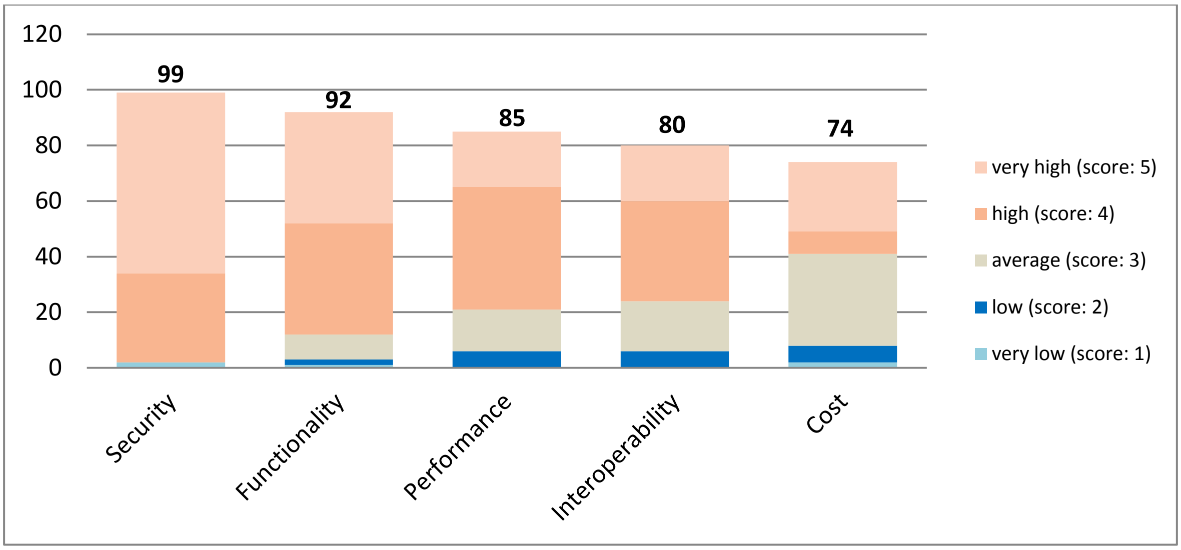
- Many CERTs appreciate receiving automated feeds from some CERTs, using them to inform their constituencies about infections; however, feeds are often found to be problematic due to:
    - format changes without prior notice,
    - timestamp/time zone issues,
    - information coming very late after the incident is noticed, which means CERTs typically work on each case separately to treat/react to the incidents,
    - data received regarding incidents contains not enough information to launch an investigation.
- Formats of regularly shared information, starting with a reasonable taxonomy of the information, needs improvement; many standards exist in the cybersecurity field, but organisations keep on doing ad hoc CSV-like exchanges.
- CERTs often lack good quality software to build up and maintain the basic database a CERT needs for a number of functions (a special kind of CRM for CERT work):
    - IP to Autonomous System Numbers (ASNs) mapping (current, historical)
    - IP to country mapping (current, historical)
    - Domain to registrar mapping
    - Contact information for all these
    - Keeping track of the quality of contacts.
- Dealing with abundant false positive detections – teams use various tools that produce varying numbers of false positives.
- Many CERTs use in-house software solutions, which they also find hard to maintain due to a general lack of software development resources. In addition, very few tools are widely adopted in the CERT community.
- Some of the incident tracking systems cannot handle large numbers of tickets.
- It may be difficult to export data from a given tracking system and link it to another system (systems compatibility issues).
- A centralised web-based service is lacking for the exchange of structured information.

Additional and more detailed technical discussions of barriers and requirements for the automated exchange of network security information can be found in two reports: *Proactive Detection of Network Security Incidents*[29] and *Proactive Detection and Automated Exchange of Network Security Incidents*[30].

When asked about priorities with regard to a potential secure European platform for communication among CERTs, surveyed teams put the highest emphasis on security aspects (confidentiality, integrity, and authenticity) when exchanging information with their peers (see Figure 5: Requirements for a potential Secure European Platform for Communication among CERTs): Functionality ranks just behind. On the other hand, cost aspects are not as crucial as technical ones, indicating that, in order to achieve the high level of security required, the teams are inclined to invest reasonable sums into effective communication solutions.

[29] http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report
[30] http://www.cert.pl/PDF/MP-IST-111-18.pdf

Figure 5: Requirements for a potential Secure European Platform for Communication among CERTs



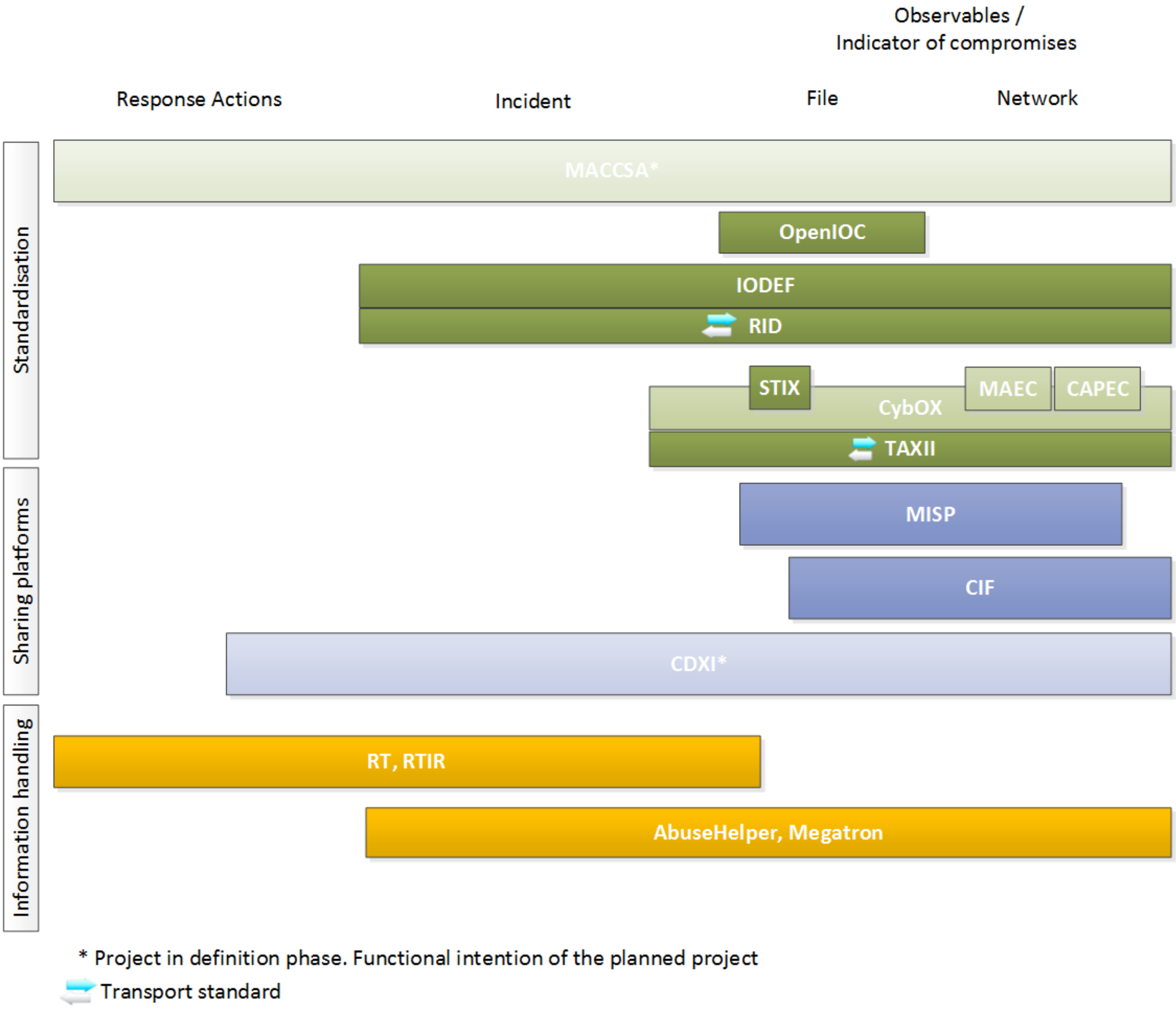
Number of respondents: 23 CERTs
Note: The total score was calculated by multiplying the number of responses for the given criterion by the ranking on a scale of 1–5.

3.2.5 Other Barriers and Requirements

The oft-quoted problem in effective information exchange is the workload, which is sometimes so heavy among CERTs that they do not have the time to write reports and share them with the community. When handling an incident, teams are often focused on its mitigation and immediate coordination with others and therefore do not always have the time to share lessons learned with other CERTs afterwards (which, from time to time, will happen after major incidents). This lack of post-processing of important incidents is considered most useful by all responding teams, alas extensive workload in day-to-day operation is a major obstacle, besides the fact that tools are not optimized to support these wrap-up reports.

4 Data Exchange Formats and Current Efforts for Secure and Effective Data Exchange

Figure 6: Mapping of Standardisation and Solutions for Response, Incident, and IoC Information Sharing



Several practices have emerged in Europe and worldwide that aim at addressing effective information exchange and sharing data about cyber incidents (as identified in the survey; see Section 3). These efforts can be considered as possible approaches to secure information exchange as envisaged by the EU Cyber Security Strategy and the draft Directive on Network and Information Security[31]. The following sections of this chapter include illustrative examples of initiatives on information exchange standards and current efforts in the area of secure and effective communication about incidents.

[31] See the Article 9 (Secure information-sharing system) of the proposed Directive. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666

INCIDENTS VS EVENTS SHARING

'Incidents' data usually contains all the information related to a security incident, including sensitive information, which cannot be easily shared. Security 'events' contain the non-sensitive metadata related to an incident. 'Events' are therefore less valuable for security analysis but are more easily shared. Tools and standards tend to be specific for one type of information (incident or event data).

Any piece of information that can be used to search for or identify potentially compromised systems is known as an indicator of compromise (IoC). These IoCs can include IP address/domain name, URL, file hash, email address, X-mailer, HTTP user agent, and file mutex. This information can be compiled into incident reports and enriched with analysis and remediation reports. Several standards exist for formatting information, however there is not a single leading one in place. However, the trend to share structured information rather than unstructured in plan emails can be observed. While, as mentioned, there is currently no single standard for data format that is generally accepted, it is crucial for an automated processing of received information! We provide an overview of existing standards below (section 4.1), followed by the summary and discussion of known challenges related to automated IoC exchanges.

Multiple initiatives exist, or are currently in development, that aim to address the aforementioned barriers (see 0) in a systematic way: CERTs still find it difficult to exchange information about (targeted) malware and attacks within a group of trusted partners or by bilateral agreement.

Despite of the trend to exchange of structured information, much of the information sharing nowadays still occurs through unstructured reports, where it is necessary, in order to process data, to manually copy & paste the information into text files that have to be parsed to be exported to (N)IDS and systems or used in log searches.

Some solutions to overcome these problems are being developed by CERTs, NATO, and private organisations, often with the participation of multiple stakeholders. In section 0, a few of them are presented that enjoy a certain degree of support in the CERT community, which have reached a good level of development, and might address the barriers presented in this report. Adopting these solutions more widely would help CERTs in forming and building larger sharing communities to exchange the benefits of previous detections and remediation efforts. This approach ultimately would lead to more confident and efficient incident response.[32]

4.1 Standardisation Efforts for Sharing Indicators of Compromise

This section is based to a large extent on the following sources: Rosella Mattioli, Information Exchange Framework for Cyber Security Incidents, Tallin University of Technology[33]; and on Chris Harrington's Sharing Indicators of Compromise: An Overview of Standards and Formats, EMC Critical Incident Response Center[34].

4.1.1 OpenIOC

OpenIOC (http://www.openioc.org/) is an extensible XML schema that enables to describe the technical characteristics of threats, an attacker's methodology, or other evidence of compromise. Originally, it was designed to enable some commercial products to codify intelligence in order to rapidly search for potential security breaches. In response to requests from across the user

[32] See the Recommendations section.
[33] http://www.07011979.org/post/26825136212/information-exchange-framework-for-cyber-security
[34] http://www.rsaconference.com/events/us13/.../sharing-indicators-of-compromise-an-overview-of

community, the company (Mandiant) has standardised and open-sourced the OpenIOC schema to allow communication of threat information at machine speed (meaning automatically). Future versions of OpenIOC will include more flexible indicators and metadata extensions to the IoC (comments, confidentiality, criticality, etc.).

The following pros and cons have been observed in relation to OpenIOC:

Pros

- Free (Apache 2 license)
- XML schema – can be extended as needed
- Three free software programs to create (IOC Editor), find (IOC Finder), and manipulate (IOC_Writer python library) OpenIOC indicators
- Full support for Mandiant products

Cons

- Limited adoption (outside of Mandiant products)
- Limited support for network-based IoCs – more suitable for file-based IoCs
- OpenIOCs not easily integrated on IDS – viewed as a 'vendor' solution
- No support for describing tactics, techniques, and procedures

Figure 7: Sample of OpenIOC document for DUQU[35]:

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="72669174-dd77-4a4e-82ed-99a96784f36e"
last-modified="2012-01-05T02:49:14" xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>DUQU (METHODOLOGY)</short_description>
  <description>Indicator for the duqu trojan. The initial duqu driver will decode and
inject a dll (marked as .pnf) into a system process (usually services.exe). The injected
dll contains another dll encoded within it's resource section which it will inject into
other processes as identified within its encoded configuruation file (another .pnf file).
This second injected dll is responsible for all backdoor/C2 communication.</description>
  <authored_by>MANDIANT</authored_by>
  <authored_date>2011-10-21T16:13:31</authored_date>
  <links>
    <link rel="caveat">Methodology</link>
  </links>
  <definition>
    <Indicator operator="OR" id="9fd46693-ee1c-4d31-b732-35bf952651e3">
      <Indicator operator="AND" id="e4deb0af-7558-498e-b953-6e70ec694767">
        <IndicatorItem id="d5b29cfe-8599-498a-b805-326273fe10c5" condition="contains">
          <Context document="FileItem"
search="FileItem/PEInfo/DigitalSignature/CertificateSubject" type="mir" />
          <Content type="string">C-Media Electronics Incorporation</Content>
        </IndicatorItem>
        <IndicatorItem id="1ca2947c-0b26-409c-93d2-28f6b364bc0b" condition="contains">
          <Context document="FileItem" search="FileItem/FileName" type="mir" />
          <Content type="string">cmi4432.sys</Content>
        </IndicatorItem>
      </Indicator>
```

[35] Source: http://openioc.org/iocs/72669174-dd77-4a4e-82ed-99a96784f36e.ioc

```
      <Indicator operator="AND" id="025d5bf1-e062-4300-a24a-e2d1c9877f1c">
        <IndicatorItem id="8a9e777b-ebbb-4494-ab05-acf39a3f6e48" condition="is">
          <Context document="DriverItem" search="DriverItem/DeviceItem/DeviceName"
type="mir" />
          <Content type="string">Gpd1</Content>
        </IndicatorItem>
        <Indicator operator="OR" id="3cfe6f4c-3276-4e8b-88d5-9b53665da358">
          <IndicatorItem id="0a704ede-840d-4075-a508-3ee5744c332f" condition="is">
            <Context document="DriverItem" search="DriverItem/DeviceItem/DeviceName"
type="mir" />
            <Content type="string">{3093AAZ3-1092-2929-9391}</Content>
          </IndicatorItem>
          <IndicatorItem id="09900e0b-8219-43dc-930b-fabf5324da4e" condition="is">
            <Context document="DriverItem" search="DriverItem/DeviceItem/DeviceName"
type="mir" />
            <Content type="string">{624409B3-4CEF-41C0-8B81-7634279A41E5}</Content>
          </IndicatorItem>
        </Indicator>
      </Indicator>
      <Indicator operator="AND" id="d0f65908-5a1a-4936-98e0-cf98ba51037e">
        <IndicatorItem id="b38d3a14-3839-4c62-ae38-3ff48b720add" condition="contains">
          <Context document="RegistryItem" search="RegistryItem/Path" type="mir" />
          <Content
type="string">HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4</Content>
        </IndicatorItem>
        <Indicator operator="OR" id="e415d391-871f-44b9-8fd3-70967644d36f">
          <IndicatorItem id="bcf49307-8362-4f05-998c-a8dd629dbb7d" condition="is">
            <Context document="RegistryItem" search="RegistryItem/ValueName" type="mir" />
            <Content type="string">CF1D</Content>
          </IndicatorItem>
          <IndicatorItem id="c13f696c-53ef-4102-b462-4fb9623f2ac5" condition="is">
            <Context document="RegistryItem" search="RegistryItem/ValueName" type="mir" />
            <Content type="string">CFID</Content>
          </IndicatorItem>
        </Indicator>
      </Indicator>

…
```

.

4.1.2 IETF Standards - IODEF & RID

The Managed Incident Lightweight Exchange (MILE) IETF Working Group focuses on data formats and transport protocols to enable the secure exchange of indicator and incident information. In this effort, the MILE working group defined two main standards for describing (IODEF) and exchanging (RID) incident information. Like all IETF standards, they benefit from the review of security, application, and transport experts.

Although the current implementations of IODEF and RID are mostly limited to internal description and local exchange of IoCs, the standards are designed to allow large scale sharing of complex incidents and more projects are implementing them or are planning to do so[36].

4.1.2.1 Incident Object Description Exchange Format (IODEF)

The Incident Object Description Exchange Format (IODEF) specification (RFC 5070, http://www.ietf.org/rfc/rfc5070.txt) defines a data representation that provides a framework for sharing information commonly exchanged by CERT teams about computer security incidents. It provides an XML representation for conveying incident information across administrative domains between parties that have an operational responsibility for remediation or watch-and-warning over defined constituencies. The data model encodes information about hosts, networks, and the services running on these systems; attack methodology and associated forensic evidence; the impact of the activity; and limited approaches for documenting workflow.

The following pros and cons have been observed for IODEF:

Pros

- IETF Open Standard defined by CERTs and for CERTs
- Enables a collaborative effort
- Vendor neutral in origin
- Flexible format (XML) allowing for extensions and the grouping of events data
- Allows for the grouping of events data

Cons

- Limited adoption
- Incident data can contain sensitive information harder to share
- High granularity that can complicate implementation

Figure 8: XML-coded IODEF document reporting an instance of the Code Red worm[37]

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- This example demonstrates a report for a very
     old worm (Code Red) -->
<IODEF-Document version="1.00" lang="en" xmlns="urn:ietf:params:xml:ns:iodef-1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:ietf:params:xml:schema:iodef-1.0">
  <Incident purpose="reporting">
    <IncidentID name="csirt.example.com">189493</IncidentID>
    <ReportTime>2001-09-13T23:19:24+00:00</ReportTime>
    <Description>Host sending out Code Red probes</Description>
    <!-- An administrative privilege was attempted, but failed -->
    <Assessment>
      <Impact completion="failed" type="admin"/>
    </Assessment>
    <Contact role="creator" type="organization">
      <ContactName>Example.com CSIRT</ContactName>
      <RegistryHandle registry="arin">example-com</RegistryHandle>
      <Email>contact@csirt.example.com</Email>
    </Contact>
    <EventData>
      <Flow>
```

[36] The Anti-Phishing Working Group is using IODEF to distribute its security information to its members. See http://siis.realmv6.org/implementations/ for a list of current implementations. See also MILE WG Wiki; http://trac.tools.ietf.org/wg/mile/trac/wiki/WikiStart.

[37] Source: RFC 5070

```
        <System category="source">
          <Node>
            <Address category="ipv4-addr">192.0.2.200</Address>
            <Counter type="event">57</Counter>
          </Node>
        </System>
        <System category="target">
          <Node>
            <Address category="ipv4-net">192.0.2.16/28</Address>
          </Node>
          <Service ip_protocol="6">
            <Port>80</Port>
          </Service>
        </System>
      </Flow>
      <Expectation action="block-host" />
      <!-- <RecordItem> has an excerpt from a log -->
      <Record>
        <RecordData>
          <DateTime>2001-09-13T18:11:21+02:00</DateTime>
          <Description>Web-server logs</Description>
          <RecordItem dtype="string">
          192.0.2.1 - - [13/Sep/2001:18:11:21 +0200] "GET
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
          </RecordItem>
            <!-- Additional logs -->
          <RecordItem dtype="url">
             http://mylogs.example.com/logs/httpd_access</RecordItem>
        </RecordData>
      </Record>
    </EventData>
    <History>
      <!-- Contact was previously made with the source network owner -->
      <HistoryItem action="contact-source-site">
        <DateTime>2001-09-14T08:19:01+00:00</DateTime>
        <Description>Notification sent to
                     constituency-contact@192.0.2.200</Description>
      </HistoryItem>
    </History>
  </Incident>
</IODEF-Document>
```

4.1.2.2 Real-time Inter-network Defense (RID)

The Real-time Inter-network Defense (RID, defined in RFC 6545[38]) was designed to transport IODEF cyber security information (and any appropriate extensions). RID is flexible enough to exchange other schemas/data models either embedded in IODEF or independent of IODEF, with a transport binding using HTTP/TLS. RID is preferred for peer-to-peer models with higher levels of security and privacy. This transport method enables increased automation over embedding the IODEF document in, for example, a secured email.

The following up- and down-sides have been observed for RID:

Pros:

- Developed, reviewed, and published by the IETF
- Benefits from the community review of security, application, and transport experts

[38] http://tools.ietf.org/html/rfc6545

- Existing open source implementations tested for interoperability
- TLS offers mutual authentication and session encryption
- Object level security (XML encryption and digital signatures applied in a standard way)

Cons:

- Limited adoption
- High granularity that can complicate implementation
- Security options can lead to high implementation costs, ROLIE (Resource-Oriented Lightweight Indicator Exchange)[39] is more suitable if high trust model is not necessary.

4.1.3 CyboX, STIX, and TAXII

The Department of Homeland Security, the National Cyber Security Communications and Integration Center, and US-CERT in the United States are at the forefront of efforts to automate and structure operational cyber security information sharing techniques on a global scale[40]:

- TAXII™, the Trusted Automated eXchange of Indicator Information
- STIX™, the Structured Threat Information eXpression
- CybOX™, the Cyber Observable eXpression

TAXII, STIX, and CybOX (all free for public use) are community-driven technical specifications designed to enable automated information sharing for cyber security situational awareness, real-time network defence, and sophisticated threat analysis.

Figure 9: TAXII™, STIX™, and CyboX™ – registered trademarks of MITRE Corporation

[39] http://tools.ietf.org/html/draft-field-mile-rolie-00

[40] The System Engineering and Development Institute (SEDI), operated by MITRE Corporation, serves as the moderator of the STIX, TAXII and CybOX communities on behalf of the Department of Homeland Security. TAXII, STIX, CybOX and their respective logos are trademarks of MITRE Corporation.

The **Cyber Observable Expression** (**CybOX**™, http://cybox.mitre.org/) is a standardised schema for the specification, capture, characterisation, and communication of events properties that are observable in the operational domain. A wide variety of high-level cyber security use cases rely on such information, including event management/logging, malware characterisation, intrusion detection, incident response/management, and attack pattern characterisation. CybOX provides a common mechanism (structure and content) for addressing cyber observables across and among this full range of use cases, improving consistency, efficiency, interoperability, and overall situational awareness.

The following pros and cons have been observed for CybOX:

Pros

- A very comprehensive list of objects to describe IoCs in detail
- Integration with CAPEC and MAEC under STIX for robust IoCs
- Vendor neutral in origin

Cons

- Integration with CAPEC and MAEC under STIX for robust IoCs
- High granularity that can complicate implementation

Figure 10: List of CybOX objects[41]

API Object	Account Object	Address Object	Artefact Object
Code Object	Custom Object	DNS Cache Object	DNS Query Object
DNS Record Object	Device Object	Disk Object	Disk Partition Object
Email Message Object	File Object	GUI Dialogbox Object	GUI Object
GUI Window Object	HTTP Session Object	Library Object	Link Object
Linux Package Object	Memory Object	Mutex Object	Network Connection Object
Network Flow Object	Network Packet Object	Network Route Entry Object	Network Route Object
Network Socket Object	Network Subnet Object	PDF File Object	Pipe Object
Port Object	Process Object	Product Object	Semaphore Object
Socket Address Object	System Object	URI Object	Unix File Object
Unix Network Route Entry Object	Unix Pipe Object	Unix Process Object	Unix User Account Object
Unix Volume Object	User Account Object	User Session Object	Volume Object
Whois Object	Win Computer Account Object	Win Critical Section Object	Win Driver Object
Win Event Log Object	Win Event Object	Win Executable File Object	Win File Object
Win Handle Object	Win Kernel Hook Object	Win Kernel Object	Win Mailslot Object
Win Memory Page Region Object	Win Mutex Object	Win Network Route Entry Object	Win Network Share Object
Win Pipe Object	Win Prefetch Object	Win Process Object	Win Registry Key Object
Win Semaphore Object	Win Service Object	Win System Object	Win System Restore Object
Win Task Object	Win Thread Object	Win User Account Object	Win Volume Object
Win Waitable Timer Object	X509 Certificate Object		

[41] Source: http://cybox.mitre.org/language/version2.0

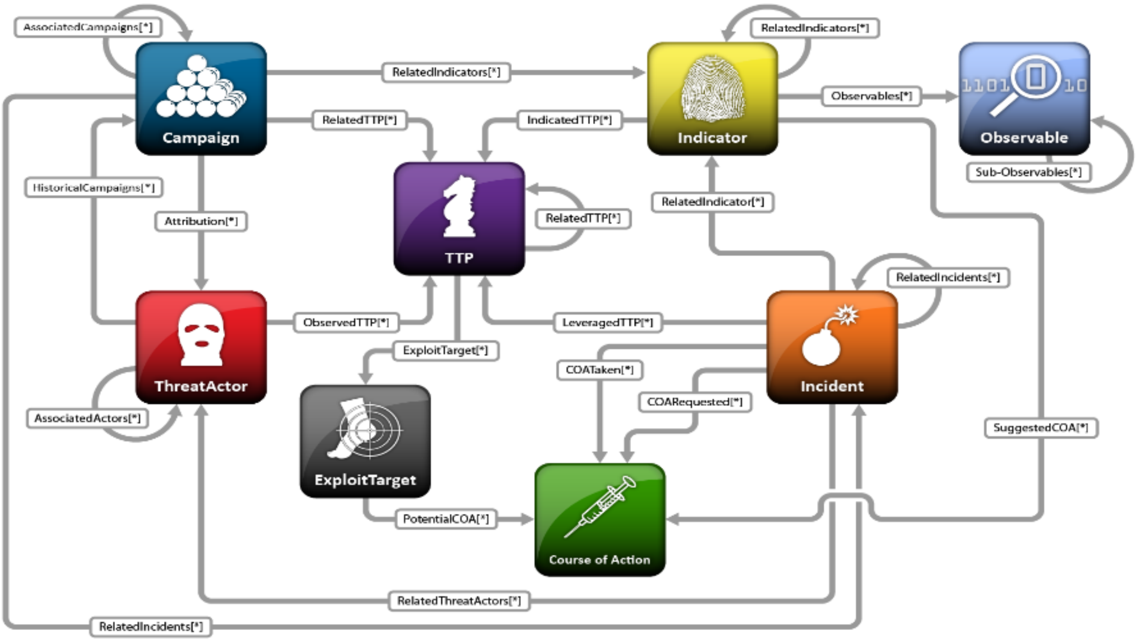
Figure 11: CybOX URIObject describing a link embedded in a referenced email[42]

```
<!-- Link URL (http://www.state.gov/public/01aff0dc/Joint_Statement.pdf) -->
<cybox:Observable id="example:observable-524048ee-9af0-4bb7-824e-52e1ce71ebd3">
        <cybox:Object id="example:object-1ba9f939-0c5a-421e-b59d-f8a6517f9018">
            <cybox:Properties xsi:type="URIObj:URIObjectType" type="URL">
<URIObj:Value>http://www.state.gov/public/01aff0dc/Joint_Statement.pdf</URIObj:Value>
            </cybox:Properties>
            <cybox:Related_Objects>
                <cybox:Related_Object idref="example:object-45ed3e11-5be1-4a7e-8f02-
25b8f74196d3"><!-- URI -->
<cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Contains</cybox:Relationship>
                </cybox:Related_Object>
                <cybox:Related_Object idref="example:object-8b319fb4-60a5-49f8-8fbc-
68eb0ea12ef0">
<!-- Email Message -->
<cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-
1.0">Contained_Within</cybox:Relationship>
                </cybox:Related_Object>
            </cybox:Related_Objects>
        </cybox:Object>
</cybox:Observable>
```

[42] Source: http://cybox.mitre.org

Structured Threat Information Expression (STIX, http://stix.mitre.org/) is a relatively recent collaborative community-driven effort to define and develop a standardised language to represent structured cyber threat information. The STIX Language is intended to convey the full range of potential cyber threat information and strives to be fully expressive, flexible, extensible, and automatable and as human-readable as possible. Any interested party can participate in evolving STIX as part of its open and collaborative community.

Figure 12: Structured Threat Information eXpresssion (STIX) v1.0 Architecture



Source: https://stix.mitre.org

Trusted Automated eXchange of Indicator Information (TAXII) is the main transport mechanism for cyber threat information represented as STIX. Through the use of TAXII services, organisations can share cyber threat information in a secure and automated manner.

Microsoft Corporation announced on July 29, 2013, that it plans to support STIX and Trusted Automated eXchange of Indicator Information (TAXII) in an article entitled *New MAPP Initiatives* on Microsoft's *BlueHat Blog*.[43]

[43] http://blogs.technet.com/b/bluehat/archive/2013/07/29/new-mapp-initiatives.aspx

4.1.4 MACCSA (Multinational Alliance for Collaborative for Cyber Situational Awareness)

(Remark: At the time of compiling this report, MACCSA is still in the early stages of development)

MACCSA is a continuation of MNE7 (Multinational Experiment 7)[44], which aims to create the conditions to enable the development, implementation, and operation of the Information Sharing Framework (ISF) for Collaborative Cyber Situational Awareness (CCSA)[45].

Organisations targeted by MACCSA include international and multinational bodies such as the EU Military Staff, Europol, NATO, the U.S., countries from Europe and Asia/Pacific, and a number of private companies such as security vendors, operators, industrial companies, and consultancies.

The ISF of MACCSA includes two main components: *information sharing model* and *information sharing management*. The information sharing model describes the means required for sharing information – proactive (push) and reactive (pull) – on alerts and warnings, best practices, and security quality management and for handling proactive artefacts.

Information sharing management focuses on ensuring the quality of the shared information. MACCSA proposes a mesh of hubs and nodes to coordinate information sharing. The model is based on existing federated secure collaboration capabilities in defence, intelligence, and industry, comprising independent entities bound together by information sharing agreements and further united by collaborative and community-centric governance authorities.

[44] http://www.federatedbusiness.org/mne7

[45] The final MNE Cyber Transition meeting took take place in Brussels on 28/29 May, hosted and supported by the European External Action Service (EEAS).

Challenges with Data Exchange Formats

'... there is no need to create new standards or specifications. The current need is to develop a system that enables the aggregation of all basic components that are common in various feeds independently from their source...'

– Rosella Mattioli, *Information Exchange Framework for Cyber Security Incidents*[46]

One outstanding issue known within the community is the considerable gap between the existence and advancement of available data feed formats and their low, scattered, or unstable adoption. Software packages developed to help CERTs deal with security incidents, such as RT/RTIR/AH etc., often do not easily enable the adoption of a range of data exchange formats. Additionally, many CERTs use different standard data formats for automatic IoC exchange.

Currently, many interested parties develop their own parsers and other software tools, which help them to deal with the incoming streams of security incident related feeds.

Another issue identified within the CERT community is the fact that, even when CERTs produce automated incident-related feeds, usually formats can change without prior notice and problems occur with timestamps/time zones or other details.

4.2 Examples of Current Efforts in Information Sharing Solutions

4.2.1 Malware Information Sharing Platform

The Malware Information Sharing Platform (MISP) has recently been released as open-source software and as a successor to the previous project, Cydefsig[47]. The Belgian Defence CERT and the NATO Computer Incident Response Capability (NCIRC) have actively developed the tool, while other teams in Europe are now participating in its testing and development. The following are among the main features of MISP:

- ***Central IoC database*** – storing technical and non-technical information about malware and attacks
- ***Correlation*** – automatically creating relations between malware, events, and attributes
- ***Storing data*** – in a structured format, allowing automated use of the database for various purposes
- ***Export –*** generating IDS, OpenIOC, plain text, and XML output to integrate with other systems (network IDS, host IDS, custom tools, etc.)
- ***Data sharing –*** automatic exchange and synchronisation with other parties and trust groups
- ***Notification –*** automatic notification using PGP
- ***Selective sharing –*** support for sharing specific attributes with specific communities

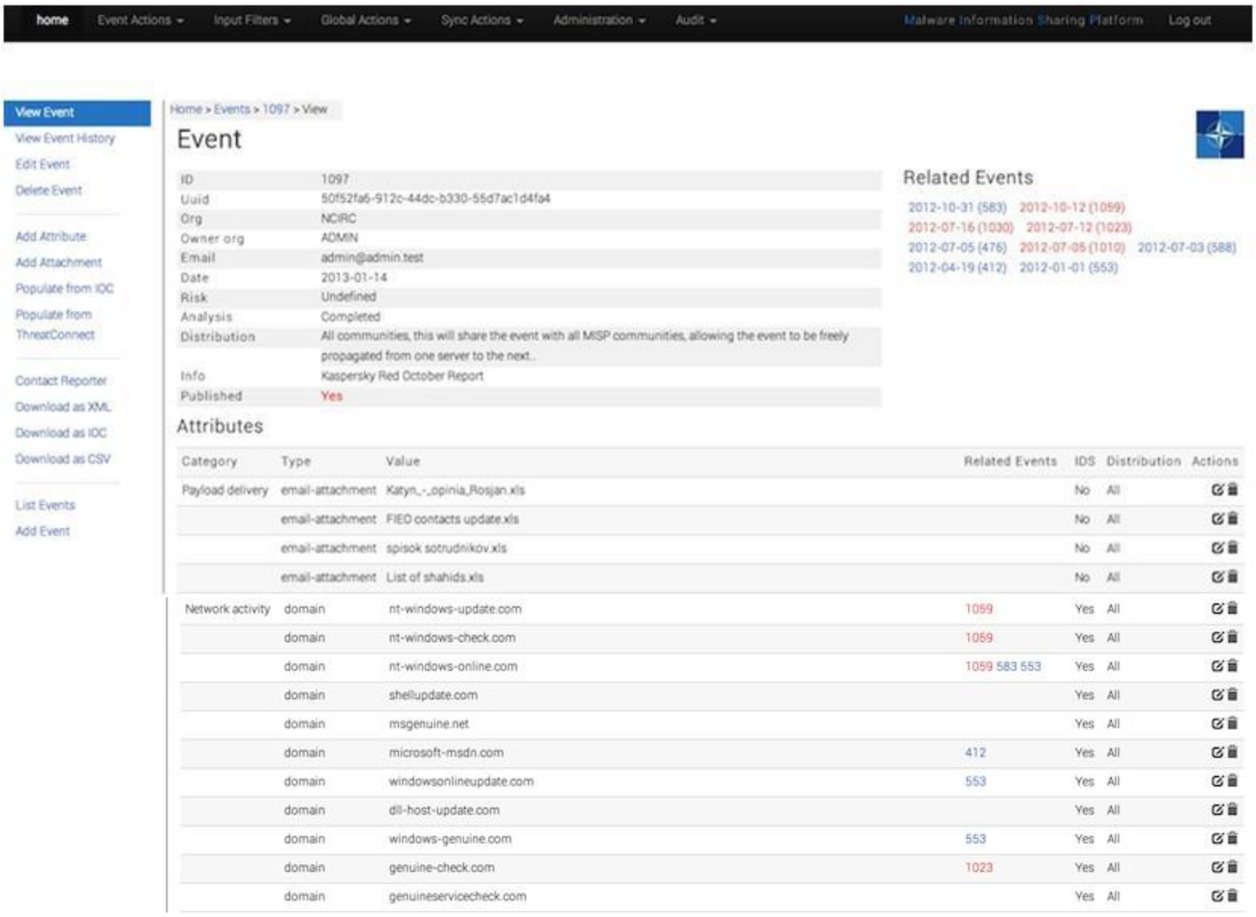
Six national/governmental CERTs have tested the MISP software. The results reveal the following:

[46] http://institutional.07011979.org/Information_exchange_framework_for_cyber_security_incidents.pdf
[47] https://github.com/MISP/MISP

- The software works well as long as the various teams are contributing.
- Automatic notification using PGP is efficient.
- Structured messages export (Snort rules or XML) works properly, but events synchronisation (merging) could be improved.
- MISP bloomfilter[48] is an implementation tool that obtains XML data from MISP and builds bloomfilter databases. The bloomfilter can be safely shared within CERTs' constituencies (e.g., Suricata NIDS and log files lookup).

The MISP user community claims to have achieved faster detection of targeted attacks, as well as improvements to the detection ratio and confidence in detected suspicions, while reducing false positives. It also avoids duplicating efforts, as it identifies quickly that other teams have already worked on handling the specific malware.

Figure 13: The Red October/Sputnik Malware as Seen in MISP[49]



Event

ID	1097
Uuid	50f52fa6-912c-44dc-b330-55d7ac1d4fa4
Org	NCIRC
Owner org	ADMIN
Email	admin@admin.test
Date	2013-01-14
Risk	Undefined
Analysis	Completed
Distribution	All communities, this will share the event with all MISP communities, allowing the event to be freely propagated from one server to the next..
Info	Kaspersky Red October Report
Published	Yes

Related Events

2012-10-31 (583) 2012-10-12 (1059)
2012-07-16 (1030) 2012-07-12 (1023)
2012-07-05 (476) 2012-07-05 (1010) 2012-07-03 (588)
2012-04-19 (412) 2012-01-01 (553)

Attributes

Category	Type	Value	Related Events	IDS	Distribution	Actions
Payload delivery	email-attachment	Katyn_-_opinia_Rosjan.xls		No	All	
	email-attachment	FIEO contacts update.xls		No	All	
	email-attachment	spisok sotrudnikov.xls		No	All	
	email-attachment	List of shahids.xls		No	All	
Network activity	domain	nt-windows-update.com	1059	Yes	All	
	domain	nt-windows-check.com	1059	Yes	All	
	domain	nt-windows-online.com	1059 583 553	Yes	All	
	domain	shellupdate.com		Yes	All	
	domain	msgenuine.net		Yes	All	
	domain	microsoft-msdn.com	412	Yes	All	
	domain	windowsonlineupdate.com	553	Yes	All	
	domain	dll-host-update.com		Yes	All	
	domain	windows-genuine.com	553	Yes	All	
	domain	genuine-check.com	1023	Yes	All	
	domain	genuineservicecheck.com		Yes	All	

[48] *A bloomfilter is a space-efficient fast data structure, conceived by Burton Howard Bloom in 1970. The set of objects is stored in hashed form, which takes up less space. Different inputs can result in a same hash output; therefore a false positive is possible when testing whether an element is present in the structure. A negative is always certain.*

[49] Source: http://www.circl.lu/files/CIRCL-MISP.pdf

The example of Red October/Sputnik[50] malware demonstrates the relationship with previous events that have similar artifacts.

European CERTs discussed the MISP initiative at the face-to-face project workshop (see Overview of the Methodology). Although not always familiar with the solution, the teams generally accepted MISP's usefulness and called for a common approach as regards a common database of incidents, while highlighting, for example, the problem of different taxonomies (in this respect, ENISA pointed to its previous work in this area)[51]. However, some scepticism was voiced regarding the likelihood of a quick agreement on common standards, let alone an agreement on solutions used. Workshop participants also called for a central database of existing ticketing systems. Overcoming the legal and political issues limiting IoC sharing may prove challenging, though.

4.2.2 Commercial Programs for Cyber Security

Microsoft, as a leading software vendor, has been active in the fight against cybercrime and, in 2010, launched the project MARS[52] (Microsoft Active Response for Security) to proactively combat botnets. The information gathered from Microsoft's botnet operations is actively shared with ISPs and CERTs.

The sharing of information on known botnet malware infections is now shared in real time with ISPs and CERTs. The new Cyber Threat Intelligence Program[52] (C-TIP) allow these organisations to have better situational awareness of cyber threats and notify people of potential security issues with their computers more quickly and efficiently.

Among the early adopters of the C-TIP cloud service are the INTECO-CERT from Spain as well as two CERTs from Luxembourg, CIRCL and the Governmental CERT of Luxembourg. C-TIP allows ISPs and CERTs to receive updated threat data related to infected computers in their specific country or network approximately every 30 seconds. Participation allows these organisations almost instant access to threat data generated from both previous and forthcoming MARS operations.

The system receives hundreds of millions of attempted check-ins daily from computers infected with malware such as Conficker[53], Waledac[54], Rustock[55], Kelihos[56], Zeus[57], Nitol[58], and Bamital[59]. This data

[50] Red October is a malware family, also known as Sputnik, which was detected in October 2012 by Kaspersky. It has been active since 2007; installations have been spotted around the globe, with diplomatic and governmental agencies targeted. The malware was usually sent by email to selected people in the respective organisations. As a cover, different office file formats have been used to transport the malware loader, using different exploits to drop the malicious content. After several stages of unpacking, the malware runs persistently on the computer, and once it successfully probes internet connectivity, it decrypts a separate file and starts to behave maliciously: it connects to a Command and Control server, awaiting new commands or downloading and executing specific malware modules. Source: https://www.circl.lu

[51] http://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/incident-taxonomy

[52] See http://www.microsoft.com/government/ww/safety-defense/initiatives/Pages/dcu-economic-crime.aspx

[53] See http://www.confickerworkinggroup.org/wiki/

[54] See http://www.symantec.com/[...]/whitepapers/W32_Waledac.pdf

[55] See http://www.microsoft.com/security/sir/story/default.aspx#!rustock

[56] See http://www.symantec.com/[...]/whitepapers/W32_Waledac.pdf

[57] See http://www.antisource.com/article.php/zeus-botnet-summary

[58] See http://www.symantec.com/security_response/writeup.jsp?docid=2012-042306-5505-99

[59] See http://www.symantec.com/security_response/writeup.jsp?docid=2010-070108-5941-99

provides valuable information that can be used by ISPs and CERTs to notify victims and help them regain control of their computers. Currently, 44 organisations in 38 countries receive these threat intelligence emails[60]. In addition to the mentioned CERTs a number of others have either signed up for the new cloud service or are in the process of signing up.

The Microsoft Active Protections Program (MAPP)[61] also needs to be mentioned. It was initially directed at security software providers, but, in the second half of 2013 it was extended to CERTs.[62] Members of MAPP receive security vulnerability information from the Microsoft Security Response Center (MSRC) in advance of Microsoft's monthly security updates. When MAPP partners receive vulnerability information early, they can provide updated protections to customers via their security software or devices, such as antivirus, network-based intrusion detection systems, and/or host-based intrusion prevention systems.

It is also worth mentioning that many anti-virus companies provides specific and highly valuable information to CERT teams on a more ad-hoc basis.

4.2.3 NATO CDXI

Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) is a system that is developed by NATO[63]. CDXI aims at serving as a repository for participants worldwide (individuals, organisations, non-NATO entities, industry, government, and academic institutions) that will automatically push and pull cyber defence data using a variety of application programming interfaces (APIs). Quality assurance of data and data confidentiality are integral to the CDXI design, and, in order to achieve the right balance of information protection (i.e., sharing with appropriate parties) and openness of the network, confidentiality and access control are implemented based on user, role, and NATO classification level.

CDXI data is structured for machine processing and automation but will also have a human-readable component. It will be integrated with cyber security appliances by means of standard APIs. To ensure a large community of adopters, NATO is considering making CDXI freely available.

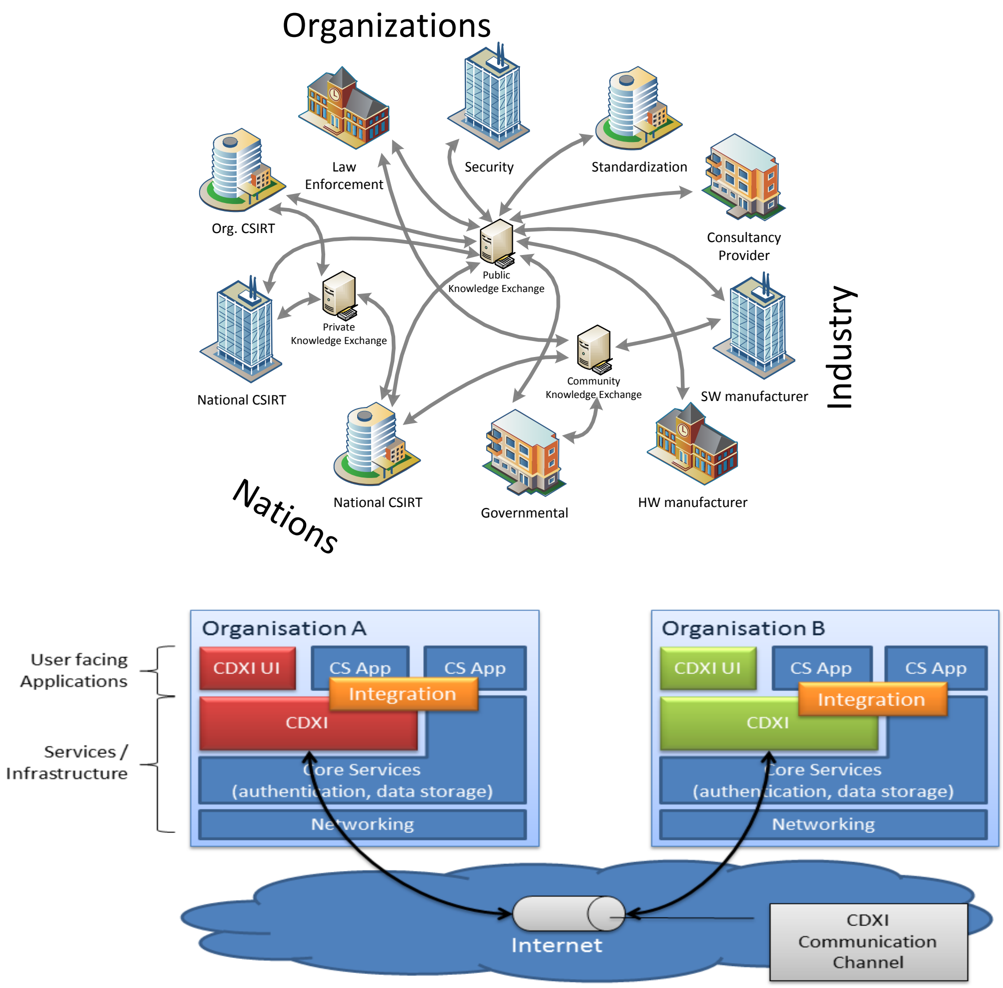
[60] Status: May 2013

[61] http://www.microsoft.com/security/msrc/collaboration/mapp.aspx#

[62] http://threatpost.com/microsoft-expands-mapp-program-to-incident-response-teams

[63] Diego Fernández Vázquez et al., “Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships”, 2012 4th International Conference on Cyber Conflict

Figure 14: CDXI targeted architecture[64]



CDXI ultimately aims at:

- Transporting cyber defence data between organisations through a resilient global infrastructure
- Feeding defence data directly into automated applications
- Providing assurance of the data's origin and quality
- Providing access controls for confidentiality
- Providing tools to collaborate on improving the data
- Enabling commercial exploitation

Among CDXI's mutually dependent benefits highlighted by its developers are:

- **Reduced costs** – adopting new standards and data sets without the need to incur further development costs, smooth deployment for all sizes and structures of organisation thanks

[64] Source: Luc Dandurand, *Cyber Defence Data Exchange and Collaboration Infrastructure (CDXI)*, an ITU-T workshop addressing security challenges on a global scale; see: http://www.slideserve.com/nalani/cyber-defence-data-exchange-and-collaboration-infrastructure-cdxi

to its modular structure, maintaining earlier investments, and the possibility to integrate previous data repositories

- **Centralised data** – storing metadata and information from various semi-structured and structured data source, open to different terminologies, and no need for the records to meet pre-defined structures or schemes
- **Faster response to incidents –** thanks to making use of the latest information
- **Support for innovation efforts** – ability to align data structures and contents with the latest developments

4.2.4 Collective Intelligence Framework

Collective Intelligence Framework (CIF) is a framework for warehousing security intelligence information in a single repository created by the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)[65]. The main goal of the project is to collect security-related data from multiple sources and provide mechanisms to effectively query, correlate, and share it. CIF evolved from the Security Event System – a project with similar goals, also developed by REN-ISAC – and is currently funded through a National Science Foundation (NSF) grant.

CIF is internally implementing IODEF, while interoperability of tools using IODEF is enforced through a scheme that is part of the Request for Comments (RFC)[66]. Adoption of IODEF means that every element of information that is a part of an incident report has well-defined semantics. The system periodically generates feeds of recent reports for every type of threat based on the means that can be used to identify a particular threat, such as an IP address, URL, or cryptographic hash. CIF periodically runs a set of data enrichment routines (analytics) on newly collected events. CIF also integrates with the Team Cymru Hash Registry service to check malware hashes[67], looks up entries in the Spamhaus[68] database, and uses the normal DNS infrastructure to extract addresses and name servers (A and NS records) for domains.

Over 200 users are on the CIF mailing list[69], including national and private CERTs, private researchers, and corporate security teams from around the world; also in developing countries the emerging equivalents of CERTs are turning to CIF to obtain information. Contrary to other information exchange platforms, which rely on various “threat languages”, CIF focuses on getting the data in the output format preferred by the user, whether it is STIX, JSON pairs, CSV, or Snort rules.

[65] http://www.ren-isac.net/
[66] http://tools.ietf.org/html/rfc5070
[67] Team Cymru Hash Registry: http://www.team-cymru.org/Services/MHR/
[68] See http://www.spamhaus.org/
[69] Status: Sept. 2013

Figure 15: CIF Architecture[70]

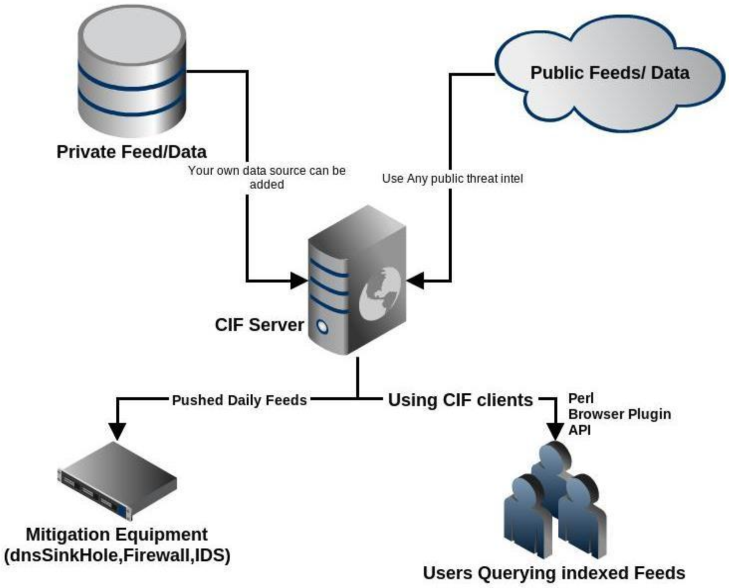
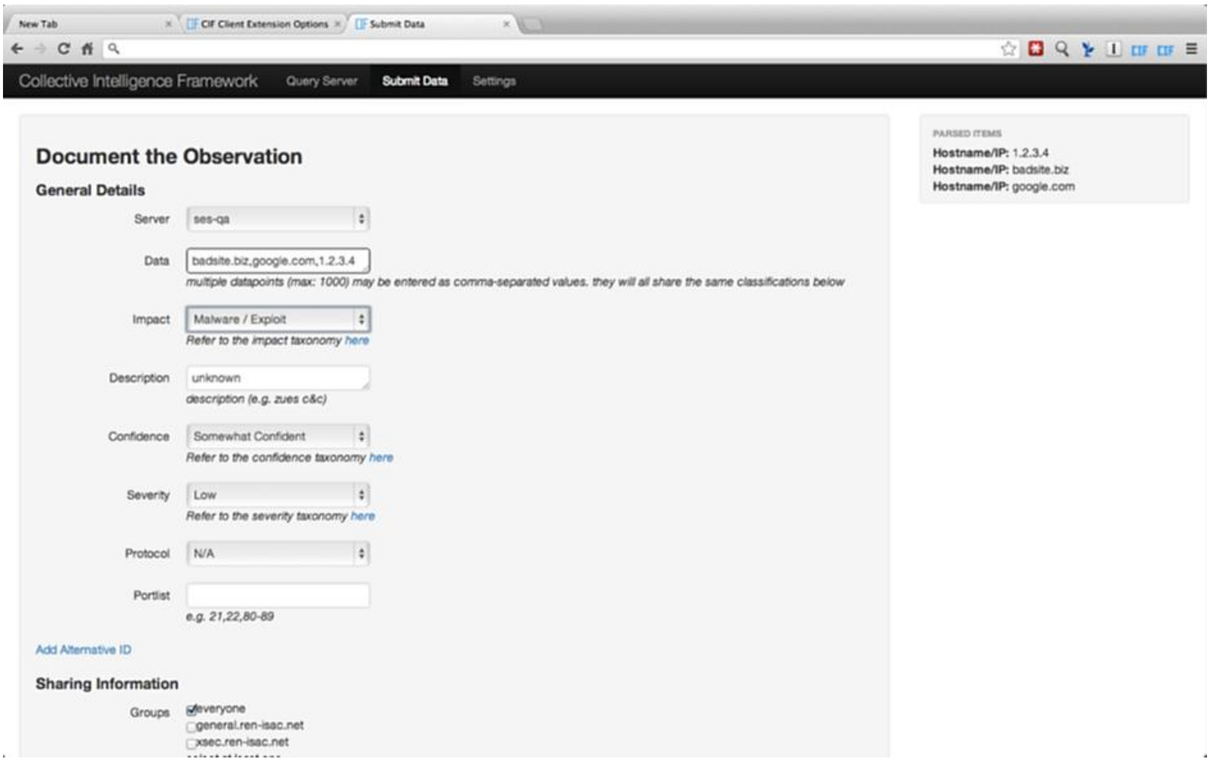


Figure 16: Submitting Data through CIF Web Interface[71]


New Tab
CIF Client Extension Options
Submit Data
Collective Intelligence Framework
Query Server
Submit Data
Settings

Document the Observation

General Details

Server: ses-qa

Data: badsite.biz,google.com,1.2.3.4
multiple datapoints (max: 1000) may be entered as comma-separated values. they will all share the same classifications below

Impact: Malware / Exploit
Refer to the impact taxonomy here

Description: unknown
description (e.g. zues c&c)

Confidence: Somewhat Confident
Refer to the confidence taxonomy here

Severity: Low
Refer to the severity taxonomy here

Protocol: N/A

Portlist:
e.g. 21,22,80-89

Add Alternative ID

Sharing Information

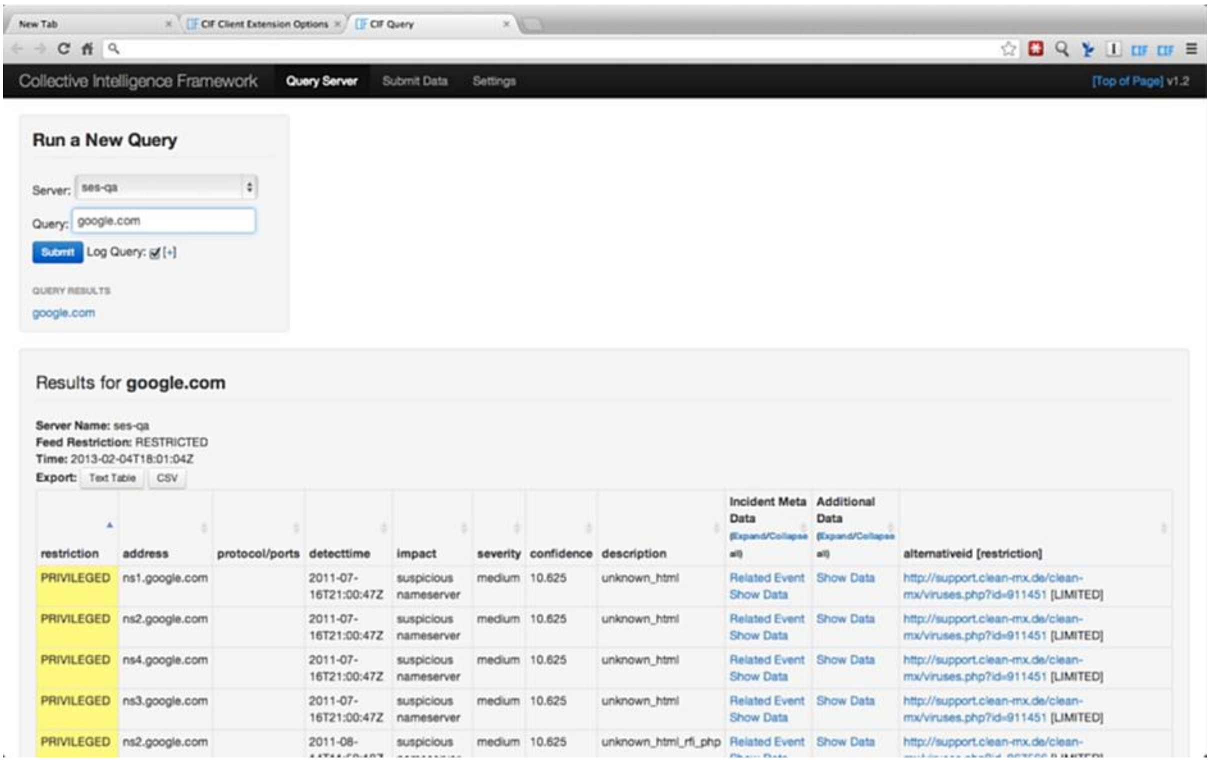
Groups:
☑ everyone
□ general.ren-isac.net
□ xsec.ren-isac.net

PARSED ITEMS
Hostname/IP: 1.2.3.4
Hostname/IP: badsite.biz
Hostname/IP: google.com

[70] Source: https://code.google.com/p/collective-intelligence-framework/

[71] Source: http://collective-intelligence-framework.googlecode.com/files/2013_MAAWG_wesyoung.pdf

Figure 17: Data Querying Through CIF Web Interface[72]



Run a New Query

Server: ses-qa

Query: google.com

Log Query: ☑ [+]

QUERY RESULTS

google.com

Results for **google.com**

Server Name: ses-qa
Feed Restriction: RESTRICTED
Time: 2013-02-04T18:01:04Z
Export: Text Table CSV

restriction	address	protocol/ports	detecttime	impact	severity	confidence	description	Incident Meta Data (Expand/Collapse all)	Additional Data (Expand/Collapse all)	alternativeid [restriction]
PRIVILEGED	ns1.google.com		2011-07-16T21:00:47Z	suspicious nameserver	medium	10.625	unknown_html	Related Event Show Data	Show Data	http://support.clean-mx.de/clean-mx/viruses.php?id=911451 [LIMITED]
PRIVILEGED	ns2.google.com		2011-07-16T21:00:47Z	suspicious nameserver	medium	10.625	unknown_html	Related Event Show Data	Show Data	http://support.clean-mx.de/clean-mx/viruses.php?id=911451 [LIMITED]
PRIVILEGED	ns4.google.com		2011-07-16T21:00:47Z	suspicious nameserver	medium	10.625	unknown_html	Related Event Show Data	Show Data	http://support.clean-mx.de/clean-mx/viruses.php?id=911451 [LIMITED]
PRIVILEGED	ns3.google.com		2011-07-16T21:00:47Z	suspicious nameserver	medium	10.625	unknown_html	Related Event Show Data	Show Data	http://support.clean-mx.de/clean-mx/viruses.php?id=911451 [LIMITED]
PRIVILEGED	ns2.google.com		2011-08-	suspicious	medium	10.625	unknown_html_rfi_php	Related Event	Show Data	http://support.clean-mx.de/clean-

[72] Source: http://collective-intelligence-framework.googlecode.com/files/2013_MAAWG_wesyoung.pdf

5 Recommendations

> *'Look at what is already there; use existing platforms for CERT cooperation; and just facilitate the needs of CERTs. Don't invent new stuff just for the sake of it, because it's fancy.'*
> – One of the surveyed CERTs

The above quote pretty much summarises the need for action in the area of exchange and sharing of information on incidents: better utilise current communication tools and practices! It is important to make tools and practices more interoperable, irrespective of which incident feeds, information exchange formats, or ticketing systems are used. After all, the core idea behind the sharing of information on incidents is that local detection, accompanied with trusted forms of information exchange, will ultimately lead to improved prevention of cyber incidents on a global scale. The probability of identifying (and subsequently handling an incident) is much greater if it is detected by several CERTs that share this information.

5.1 Recommendation 1: ENISA should facilitate the adoption of Essential Tools for the CERT Community

The sharing of information among CERTs on an efficient (automated) basis assumes that the teams first effectively handle the information on incidents internally. This requires the adoption of specific tools by CERTs that relate to ticket tracking and automated incident information processing (RTIR and Abuse Helper are among the most popular tools used by the teams). CERTs interested in working together on RT/RTIR/AH upgrades and improvements should synchronise their efforts. Whenever CERTs require new functionalities, demand arises for expert developers, a resource CERTs usually lack. CERTs can seek funding from the EU's research and technology programs for updates and upgrades.

These programmes often include, as a condition for financing, the participation of multiple parties or consortia. Such a cooperative software adaptation and improvement approach could be tested in relation to the specific needs of the CERT community, as well as being further used to create new tools if the need should surface. These efforts should be of the bottom-up type in terms of software development strategies and facilitated with top-down coordination within the community of CERTs. CERTs are encouraged to request that ENISA facilitates the adoption, coherence, and interoperability of these tools via training sessions at ENISA CERT workshops or via other arrangements.

5.2 Recommendation 2: Security information providers should improve the stability of existing incident information feeds

Many CERTs appreciate receiving automated feeds from established services (Shadowserver, Zeus Tracker, Malware Domain List, etc.) and from other CERTs to inform their constituencies about infections. However, feed formats are often changed by their publishers without prior notice. As many parties emphasise, this particular problem is even more troublesome than the fact that many feed publishers do not adhere to the standardised feed formats and create their own feed templates. CERTs have indicated that it is less problematic to create a parser for a new format of XML or CSV feed than to deal with the ever-changing feed formats.

One way to overcome these issues is the employment of “soft” tools, such as published reports, workshops, webinars, seminars, and conferences, in order to encourage improved behaviour among the feed publishers, especially:

- Wider adoption of some of the best standards of data format for the automated sharing of indicators of compromise (IODEF, STIX, OpenIOC, etc.)
- Wider adoption of 'good community citizen' behaviour, like establishing a minimal notification period for sharing feed format updates

It must be emphasised that any recommendations regarding setting and promoting better standards for automated information exchange feeds must be thoroughly discussed and supported by the community, especially by feed publishers and users (CERTs). The right platform for discussing the aspects of the continuity of feeds could be organisations and events that bring CERTs together.

ENISA will further investigate these areas and provide adequate and appropriate support for CERTs and their projects.

The previous two recommendations are natural and unavoidable, considering the state of issues with tools that help the European CERT community participants to fulfil their roles. The next few recommendations were not designed to be followed all in parallel – rather, they represent scenarios the CERT community may choose to follow. Hence, they are more of a set of alternatives, rather than a to-do list

5.3 Recommendation 3: CERTs should coordinate to enhance functionalities of existing tools for more effective data sharing within the community

As previously stated (Recommendation 1), technical barriers may present a hindrance to the adoption of essential information management tools. The same applies to information-sharing solutions.

A more crucial need than formal feed format standardisation is the enhancement of existing software tools for information sharing, processing, analysis, and presentation. It is unlikely that any commercial, non-governmental, or other organisation will create a tool that fits everybody’s need and will resolve all outstanding issues and be accepted and adopted by all CERTs and other cyber security stakeholders. It is rather safe to assume that the software tools ecosystem will continue to be fragmented, yet vibrant. It will consist of many small solutions and tools for solving specific problems. The following are among the functionalities to enhance existing tools and support interoperability in incident data sharing:

- First and foremost, interoperability for cross-hub and cross-platform sharing
- Correlation engines for incident analysis
- Advanced analytics and visualisation for massive numbers of incidents
- Automatic prioritisation features

All of these classes (and more) of software tools will have to be enhanced in order to enable CERTs to cope with the ever-increasing demands of the modern cyber security environment. However, most CERTs do not have developers working for them. Again, it is possible to access EU funds for information society projects. The actual development of enhanced tools would come from the bottom up (e.g., developers embedded at CERTs who are cooperating internationally).

ENISA will support these efforts by offering targeted training upon request from the n/g CERT community. Whenever appropriate and feasible, ENISA will actively support community driven efforts in this area.

5.4 Recommendation 4: A central trusted body at the cross-border level should develop a common incident information repository with the integration of current data exchange efforts

While CERTs are largely satisfied with the tools in use today, some see the benefits of a hypothetical new central service offering an information repository for n/g CERTs in Europe. Such a repository would include CERTs' contact information to facilitate incident detection and information correlation (DNS, ASN, and IP ranking) and a repository for past incident information, with options for sorting and filtering the database of archived information. Access to the shared incident repository should be convenient. The user could create and manage groups with other registered users and share information with those particular groups. This repository would have functionalities to send notifications based on severity or other criteria, such as IP addresses, ASNs, and ranges (constituency, country, community of interest, etc.).

In the perspective of one stakeholder:

'What could be done is to build a common attack database, or repository, with major input from CERTs – one containing the methods and characteristics attackers employ and the attack tactics and techniques they use – so that we can adapt to new avenues of attack and identify common patterns.'

However, it is widely believed that trust issues could make generating sharing practices and managing access rights to such shared repositories more troublesome than building the tool itself. A progressive approach, initially targeting useful but insensitive information (a contact repository), would facilitate the adoption of this infrastructure. In the medium term, this platform would offer brokering facilities to exchange information among existing sharing communities of n/g CERTs. A trusted organisation like FIRST, TI, or ENISA could support this service so as to encourage all n/g CERTs to join such a global sharing effort.

In 2014, ENISA will carry out a project aiming at providing better support to CERTs in the area exchanging and processing of actionable information, with the goal to, in accordance with the CERT community and as much as possible, engage in this coordination role.

5.5 Recommendation 5: Bridge Sharing CERT Communities in Europe

The 'perfect' scenario for enhancing sharing practices in the CERTs community would include building a bridging platform that would extend existing communities and broker information across these communities. Such a cross-hub exchange would require:

- Local adoption of interoperable standards of data formats (e.g. IODEF, STIX, etc.)
- The definition of diffusion policy standards (e.g., CDXI Information diffusion policy), thus enabling more complex schemes than Traffic Light Protocol (TLP)
- Coordination at international level

At the EU level, this inter-exchange effort could be entrusted to the CERT community and supported by ENISA.

In 2014, ENISA will further improve its abilities to provide active support for their key stakeholders in this area.

Annex I: Abbreviations

AH	Abuse Helper
API	Application Programming Interface
ARS	Action Request System
ASN	Autonomous System Numbers
CAPEC	Common Attack Pattern Enumeration and Classification
CDXI	Cyber Defence Data Exchange and Collaboration Infrastructure
CERT	Computer Emergency Response Team
CIF	Collective Intelligence Framework
CIRCL	Computer Incident Response Center Luxembourg
CRM	Customer Relations Management
CSIRT	Computer Security Incident Response Team
CSV	Comma Separated Values
C-TIP	Cyber Threat Intelligence Program
CybOX	Cyber Observable Expression
DNS	Domain Name System
EC	European Commission
ENISA	European Union Agency for Network and Information Security
EU	European Union
ICQ	I Seek You (wordplay)
ID	Identification
IDC	International Data Corporation
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IM	Instant Messaging
INTECO	Instituto Nacional de Tecnologias de la Comunicacion
IOC (or IoC)	Indicators of Compromise
IODEF	Incident Object Description Exchange Format
IP	Internet Protocol
IRC	Internet Relay Chat
ISA	Information Sharing Agreements
ISF	Information Sharing Framework
ISP	Internet Service Provider
JSON	JavaScript Object Notation
MACCSA	Multinational Alliance for Collaborative for Cyber Situational Awareness
MAEC	Malware Attribute Enumeration and Characterization
MAPP	Microsoft Active Protections Program (MAPP)
MARS	Microsoft Active Response for Security
MILE	Managed Incident Lightweight Exchange
MISP	Malware Information Sharing Platform
MITRE	A non-profit organisation managing federally funded research and development centres in the U.S. focusing on homeland security, defence and intelligence, federal aviation system development, and federal sector modernisation
MSN	Windows Live Messenger (currently not supported by Microsoft)

MSRC	Microsoft Security Response Center
NATO	North Atlantic Treaty Organization
MNE7	Multinational Experiment 7
NCIRC	NATO Computer Incident Response Capability
n/g CERT	National/Governmental CERT
NIDS	Network Intrusion Detection System
NS	Name Server
NSF	National Science Foundation
OTRS	Open Source Ticket Request System
PGP	Pretty Good Protection
REN-ISAC	Research and Education Networking Information Sharing and Analysis Center
RFC 5070	Request for Comment 5070 (Incident Object Description Exchange Format)
RID	Real-time Inter-network Defense
RIPE	Réseaux IP Européens (regional internet registry)
ROLIE	Resource-Oriented Lightweight Indicator Exchange
RT	Request Tracker
RTIR	Request Tracker for Incident Response
SAP	Systems Applications and Products in Data Processing
SES	Security Event System
SMS	Short Message Service
S/MIME	Secure/Multipurpose Internet Mail Extensions
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Indicator Information
TF-CSIRT	Task Force-CSIRT
TLP	Traffic Light Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
US DHS	United States Department of Homeland Security
USA	United States of America
VPN	Virtual Private Network
XML	Extensible Markup Language

Annex II: Questionnaire

Survey Overview:

- Communication practices with:
  - Other CERTs in your country
  - Other CERTs of the same type/constituency in other EU countries
  - Operator/ISPs or Industry
- Ticketing systems and CRMs
- Communication solutions

Organisation Details

Name of your organisation: ________________________________

Your name: ________________________________

Job title/position: ________________________________

Contact details (phone number, email): ________________________

What type is your CERT? For detailed definitions, see the Glossary.

□ **National**
□ **Governmental**
□ **National/Governmental**
□ **Research/Education**
□ **Other (please specify below)**

Note: The survey gives you the option of ticking several answers. Boxes are also attached below the questions for any details you wish and are able to share. Please also feel free to attach links to documents everywhere you consider suitable.

1. Please fill in the table on your communication practices.

Communication Partner	Frequency of Exchange per Type of Information	Communication Solution (check all that apply)	Your View of the Quality of This Communication (check all that apply)	Main Obstacles to More Secure and Effective Communication
Other CERT(s) in your country	*Sensitive-incident-related information* □ Daily □ A few days a week □ Once a week □ Less than once a week □ Very rarely, if at all *Vulnerability information exchange* □ Daily □ A few days a week □ Once a week □ Less than once a week □ Very rarely, if at all *Artefact information exchange* □ Daily □ A few days a week □ Once a week □ Less than once a week □ Very rarely, if at all *Alerts and warnings* □ Daily □ At least once a week □ Less than once a week □ Less than once a month □ Very rarely, if at all *Informal exchange* □ Daily □ At least once a week □ Less than once a week □ Less than once a month □ Very rarely, if at all	□ Secure Email (SMIME/PGP) □ Normal Email □ IRC □ Jabber □ Skype □ Lync □ ICQ □ Windows Live Messenger (MSN Messenger) □ Yahoo! Messenger □ IBM Lotus Sametime □ Other Comments: (specify)	□ Very good and fruitful, beneficial for both sides □ Satisfactory □ Should be extended □ Poor □ Trust barriers are impeding communication □ Mostly unilateral, lack of feedback □ Nonexistent, useless	□ Legal □ Technical □ Procedural □ Trust issues □ Insufficient interest of the partners □ No crucial barriers □ Comments: (specify)

Communication Partner	Frequency of Exchange per Type of Information	Communication Solution (check all that apply)	Your View of the Quality of This Communication (check all that apply)	Main Obstacles to More Secure and Effective Communication
CERT of the same type/constituency in another (Member) State	*Sensitive-incident-related information* □ Daily □ A few times a week □ Once a week □ Less than once a week □ Very rarely, if at all *Vulnerability information exchange* □ Daily □ A few times a week □ Once a week □ Less than once a week □ Very rarely, if at all *Artefact information exchange* □ Daily □ A few times a week □ Once a week □ Less than once a week □ Very rarely, if at all *Alerts and warnings* □ Daily □ At least once a week □ Less than once a week □ Less than once a month □ Very rarely, if at all *Informal exchange* □ Daily □ At least once a week □ Less than once a week □ Less than once a month □ Very rarely, if at all	□ Secure Email (SMIME/PGP) □ Normal Email □ IRC □ Jabber □ Skype □ Lync □ ICQ □ Windows Live Messenger (MSN Messenger) □ Yahoo! Messenger □ IBM Lotus Sametime □ Other □ Comments: (specify)	□ Very good and fruitful, beneficial for both sides □ Satisfactory □ Should be extended □ Poor □ Trust barriers are impeding communication □ Mostly unilateral, lack of feedback □ Nonexistent, useless	□ Legal □ Technical □ Procedural □ Trust issues □ Insufficient interest of the partners □ No crucial barriers □ Comments: (specify)

Communication Partner	Frequency of Exchange per Type of Information	Communication Solution (check all that apply)	Your View of the Quality of This Communication (check all that apply)	Main Obstacles to More Secure and Effective Communication
Operator/ISPs or Industry	*Sensitive-incident-related information* □ Daily □ A few times a week □ Once a week □ Less than once a week □ Very rarely, if at all *Vulnerability information exchange* □ Daily □ A few times a week □ Once a week □ Less than once a week □ Very rarely, if at all *Artefact information exchange* □ Daily □ A few times a week □ Once a week □ Less than once a week □ Very rarely, if at all *Alerts and warnings* □ Daily □ At least once a week □ Less than once a week □ Less than once a month □ Very rarely, if at all *Informal exchange* □ Daily □ At least once a week □ Less than once a week □ Less than once a month □ Very rarely, if at all	□ Secure Email (SMIME/PGP) □ Normal Email □ IRC □ Jabber □ Skype □ Lync □ ICQ □ Windows Live Messenger (MSN Messenger) □ Yahoo! Messenger □ IBM Lotus Sametime □ Other □ Comments: (specify)	□ Very good and fruitful, beneficial for both sides □ Satisfactory □ Should be extended □ Poor □ Trust barriers are impeding communication □ Mostly unilateral, lack of feedback □ Nonexistent, useless	□ Legal □ Technical □ Procedural □ Trust issues □ Insufficient interest of the partners □ No crucial barriers □ Comments: (specify)

2. What ticketing (incident tracking) system(s) are you using?

□ OTRS
□ RTIR
□ Abuse Helper
□ Other (please specify)

3. What are the main advantages of the ticketing systems you are using?

4. Are there any disadvantages of the ticketing system you are using?

□ No
□ Yes (please specify), but we are not considering switching to another ticketing system.

□ Yes, and we are considering switching to another ticketing system (please specify).

5. What CRM solutions are you using?

□ Oracle solutions
□ SAP
□ Salesforce.com
□ Microsoft Dynamics
□ RightNow
□ Other (please specify)

□ None

6. Are you using different communication solutions for exchanging information with CERTs and with other stakeholders/constituents?

□ No
□ Yes (specify below)

Please specify which (secure) solutions you use for communication with other CERTs and with other stakeholders/constituents, such as governmental bodies, telecom operators, etc.:

7. Please rate the following aspects of a secure (European) platform for communication among CERTs in terms of their importance for your CERT using a scale of 1–5 on which 1 = of very low importance and 5 = of very high importance:

- □ **Security (confidentiality, integrity, authenticity, etc.)**
  Importance ranking: □ 1 (very low) □ 2 (low) □ 3 (average) □ 4 (high) □ 5 (very high)

- □ **Interoperability (compatibility with specific information exchange standards and formats, such as IOEDF, existing solutions, etc.)**
  Importance ranking: □ 1 (very low) □ 2 (low) □ 3 (average) □ 4 (high) □ 5 (very high)

- □ **Performance**
  Importance ranking: □ 1 (very low) □ 2 (low) □ 3 (average) □ 4 (high) □ 5 (very high)

- □ **Functional (ease of use, deployment, multiple manufacturers, and support)**
  Importance ranking: □ 1 (very low) □ 2 (low) □ 3 (average) □ 4 (high) □ 5 (very high)

- □ **Cost**
  Importance ranking: □ 1 (very low) □ 2 (low) □ 3 (average) □ 4 (high) □ 5 (very high)

Comments on the needs and expectations of a secure European platform for communication among CERTs:

Thank you very much for your time!

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu