INFORMATION SOCIETIES TECHNOLOGY (IST) PROGRAMME

Proposal acronym:	**eCSIRT.net**
Proposal full title:	**European CSIRT Network**
Proposal/Contract number:	**IST-2001-37558**

Integration of Standardized Syntax and Semantics (Common Language) into CSIRT Operations

Working package:	WP 2 – Preparation Phase
Delivery:	D 2.2.1
Date of preparation:	17 May 2003

Table of Contents

1 Introduction

The eCSIRT.net project aims at improving the efficient and effective cooperation of CSIRTs which will result in a quicker response to detected security problems. Better proactive security measures that are presented as best practice and result from the collected knowledge available within the CSIRT community will reduce the overall numbers of incidents. The enabled statistics will allow to measure the level of incidents and threats existing today for the first time, as qualified information will become available.

The public presentation of incidents and vulnerabilities might be seen as something that will undermine the public confidence. But it needs to be recognized that the public confidence is already heavily impacted by the headlines regarding attacks like Code Red, Nimda, Slammer, etc. or widespread vulnerabilities like the SNMP vulnerability or any new MS Windows problem broadly discussed on the Internet. All named incidents are examples for global problems not restricted to a smaller set of organizations or directed towards a particular target but attacking the community at large. In the opposite, the availability of "true" information will result in a better understanding, and only if understanding leads to an improved security culture will users and organizations know that they need to take much better proactive steps to avoid incidents and not suffer from break-ins.

As of today cooperation among CSIRTs is not supported by techniques or well established procedures until now. The eCSIRT.net project aims to establish the necessary frameworks for the service applications based on automatic information exchange related to incidents or more specifically to CSIRT operations. Such application is far from fully established today. What is needed are standards like developed as part of ongoing activities within the IETF, namely IODEF and IDMEF, as well as the definition of advanced best practices within the CSIRT communities themselves.

1.1 Purpose of this Document

This document will examine issues related to the practical integration of formats like IODEF and IDMEF within the operation of CSIRTs. Emphasis will be given towards the technical aspects, as there will be technical borders to overcome if an automatic information exchange regarding incidents should be take up by CSIRTs.

To allow a better assessment of todays situation of CSIRTs in regard to the use and adoption of standards, these will be reviewed as well.

The document will outline concepts for practical usage and application of the available formats for automatic information exchange and discuss problems related to the take up and early adoption.

1.2 Document Structure

This document will first provide a short summary of available standards for CSIRTs within Chapter 2. This will provide the necessary background for a better understanding of the integration of automatic exchange of incident related information into CSIRT operation.

The use cases of specific interest for the eCSIRT.net project will be explained in Chapter 3, providing the foundation for any further discussion.

Applying the two exchange formats currently available for CSIRTs – IODEF and IDMEF – will be discussed in Chapter 4 from a technical point of view. Understanding the interfaces as well as operational and security issues is mandatory before options for the integration into CSIRT operations can be developed.

Based on the available approaches solutions for integration of automatic information exchange into the CSIRT operation could be developed. But as the ability of each CSIRT to apply a specific solution

clearly depends on the current state of affairs within the CSIRT, this needs to be considered as well. This is the topic of Chapter 5. Experience shows that it is important to recognize the major differences as defined by the use of tools and databases. This will allow to categorize CSIRTs into three groups, each one of them with specific challenges to overcome when integrating new means of automatic information exchange into their day-to-day operation.

The document will close with an outlook into the future and provide directions for further study and work on automatic information exchange within the CSIRT environment.

2 Standards for CSIRTs

Although the oldest CSIRT became 15 years in December 2003 – the CERT Coordination Center in Pittsburgh, PA, USA – the state of the art within the CSIRT community is still driven by only a few – mostly organizational oriented – documents like the "CSIRT Handbook" from 1998.[1] But there is an increasing interest in the automation of CSIRT related tasks. There are several reasons for this:

- Without automation CSIRTs cannot expect to get all of the interesting information or to get them in time. This is especially true for information about attacks. With fast spreading worms a CSIRT cannot rely on human alerts, as this will take too much time.
- With an increasing flood of attacks and incidents, administrators are much more concerned and needed to address the local issues instead of spending time to report incidents to their CSIRT.
- With an increasing work load CSIRTs need to safe resources and find ways to improve their operation as much as possible. This will most certainly require to remove any need to provide information stored in internal databases within manually generated emails for example and replace that by a fully integrated information exchange.
- With an increasing number of security vulnerabilities CSIRTs need to adapt approaches that allow a much better and easier presentation as well as selection of subsets for the appropriate audience.

The "players" that we need to consider for standards that could address these problems are coming from two different areas:

1. IDS vendors and practitioners are addressing the need for IDS related information exchange, mostly related to the traffic between a data acquisition component (called sensor) and a data collection component (called manager). This traffic is mostly related to single, independent packets or connections and are only later put into context. Attacks are addressed instead of incidents, which may exist of many attacks.
2. CSIRTs are concentrating not on single attacks except in relation to early warning based on reports about attacks from their constituency. (In which case they will most likely use approaches also developed by the IDS community – see above).

   CSIRTs are also planning and developing solutions to improve the exchange among CSIRTs.

   And CSIRTs are developing mechanisms for structured security advisories as well as establishing customer / constituency portals allowing more or less individual selection of the needed information.

Interestingly both groups have applied for all areas formats that are based on XML. We will in this chapter review all known approaches which have the potential for widespread adoption in the CSIRT community.

2.1 Reporting of Attacks - IDMEF

The development of a standard language to share information between intrusion detection, response and management systems began in the late 1990's within the IETF IDWG (Intrusion Detection Working Group). The core work of the group is developing the Intrusion Detection Message Exchange Format (IDMEF), which defines the XML based common language used to exchange data between parts of an intrusion detection network.

[1] There will be an updated version available at the end of 2003

IDMEF is intended to provide a standard data format which intrusion detections systems can use to exchange alerts detailing possible violations of security policy. A standard format allows the interoperation between a number of commercial, open source and research intrusion detection systems. Bringing together alerts from different sensors allows value to be added to the alerts through correlation and aggregation.

The work of the IDWG is described at http://www.ietf.org/html.charters/idwg-charter.html. Silicon Defense also maintain a version of this information at http://www.silicondefense.com/idwg/. The IDMEF data format is (currently in draft version 0.10) is available from http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-10.txt.

As alternatives there are a number of proprietary standards current used by Intrusion Detection systems to exchange data between sensors distributed across the network and a central collection point. The most wellknown one, Snort, is a popular open source IDS product. It can use a number of different output plug-ins. The standard way of a Snort sensors exchanging alerts with a central collection point is via direct communication with a SQL database, possibly encrypted over the network using stunnel. Other Intrusion Detection Systems use proprietary methods to exchange alert information. For correlating intrusion information collected from a diverse range of sensors writing support for each different IDS system would be very complicated.

Many IDSs have developed output mechanisms utilising IDMEF. Silicon Defence have developed such a plugin for Snort, enabling IDMEF alerting from Snort sensors as well.

The transport of IDMEF objects is not covered by the IDMEF standard although the IDWG has a parallel task to produce the IDMEF Exchange Protocol (IDXP) utilising the Blocks Extensible Exchange Protocol (BEEP). The IDMEF standard is however transport independent.

Potential application from a CSIRT perspective would be the analysis of trends in intrusions. This requires sampling which is carried out on as many networks as possible. This is ideally carried out by a fully automated service tuned to provide the minimum number of false positives. For any statistical analysis either the sample set must be constant, or all networks must be well matched. This is most easily carried out my making sure all collection is carried out on virgin network blocks which are put to no other use. An inclusion of a new network to the sample set which has different use patterns, or unique targets to attract attacks (such as a honeypot) would distort any resultant dataset. The use of virgin networks however only allows for the analysis the detection of widespread scanning rather than spotting trends in attack profiles against actual services.

New worms such as CodeRed, Nimda and SQL-Slammer would of been promptly and easily recognised using this method. The analysis of trends of common destination ports used in scanning gives some warning to new exploit code available in the underground (i.e an increase in ssh scanning reported from a number of disperse sensors might indicate.

Such applications make it worthwhile to consider IDMEF in a CSIRT context.

2.2 Exchange of Information about Incidents - IODEF

The Incident object Description and Exchange Format (IODEF) is the today developed by the INCH Working Group of the IETF. Previously much work was devoted to this format by the Incident Taxonomy Working Group (ITDWG) at TERENA.

IODEF is planned to be a standard format which allows CSIRTs to exchange operational information; it may also provide a future basis for the development of compatible and inter-operable tools for all kind of CSIRT related activities. This especially would allow the retrieval of statistical information across many CSIRTs, as with the IODEF format not only the syntax, but also the semantic needs to be adjusted.

As the specific problems and interpretation of the protocol itself is the topic of other documents, no further information will be provided here about the protocol, while the most important potential applications will be examined further on below.

2.3 Exchange of Information about Advisories

It is the aim of eCSIRT.net to promote and to deepen the cooperation of the participating teams in the areas of Incident handling. But furthermore a cooperation is desirable on wider fields. Almost every team must use considerable resources for the provision of an Advisory service. This is probably the most important service for the constituency of a CSIRT, if they do not suffer from an incident.

System administrators need precise and authentic information about new vulnerabilities to be able to carry out a risk assessment for his systems. The output formats orientate themselves at the needs of the constituency and they are different from team to team. Despite all differences, from the point of view of the reader, an advisory must give answers to the following questions:

- Is the advisory authentic and relevant?
- How fast do I have to react?
- Which options do I have?

Furthermore the information about vulnerabilities and threats comes from sources which are used by many teams. But many teams work simultaneously on the verification, revision, testing and if required translation of the information. In the result there is a massive duplication of the necessary work.

In order to enhance the cooperation in the production of advisories a common exchange format is needed. On this basis certain tasks can be distributed and synergies can be released.

Since the needs of the customers are different, a presentation-independent interchange format is needed. In the following sections two different approaches are introduced.

2.3.1 EISPP

A common advisory format has been developed by the participating CSIRTs within the European Information Security Promotion Programme (EISPP)[2]. The different available formats are merged in a best-practice approach into the EISPP Common Advisory Format (abbrev. EISPP). Further information about EISPP can be found under http://www.eispp.org.

The format is defined using XML, so it is possible to use a number of standard XML tools for the advisory processing. The fields and sections are formally defined as an XML DTD so that it is possible to process this advisory format automatically. A public document (EISPP Common Format v.1.2) is available which can be found on the web page mentioned before. A short description of the contents of EISPP is given in Table 1 in comparison with other formats.

2.3.2 CAIF

A further approach was proposed by the Rechenzentrum der Universität Stuttgart CERT (RUS-CERT).

Up to now, the Common Advisory Interchange Format (CAIF) project has produced a requirements document available in various formats from http://cert.uni-stuttgard.de/projects/caif. The specification of the exchange format isn't completed yet, so that a detailed comparison with EISPP is not possible. However, a comparison seems meaningful for broader considerations, so that the requirements document is taken as a base.

Just like EISPP CAIF will use the XML Document Type Definitions to formally describe their data formats.

[2] EISPP is a project fund by EU through the fifth European Framework Program within the thematic program Information Society Technologies (IST).

2.3.3 Comparison of EISPP and CAIF

The following table gives an overview of the content fields of EISPP and CAIF. The structure of the table was taken from the EISPP description.

EISPP	CAIF
Identification Data	
Issuer	
Reference Number	Advisory ID including an Issuer ID
Language	Language
Title	[Platform/Product/Protocol] Subject
Abstract	Abstract
	Date
History Data	
Version History	Revision History / Version
Update Information	
Vulnerability Classification	
Confidence Level	Confirmation
	Vendor Status
Vulnerability Category	Vulnerability Class
Attack requirements	Attack requirements
Vulnerability Impact	Impact
Attack Expertise	Probability of an Attack
Risk	Severity
System Information	
Affected Platform	Affected System
Affected Software	Affected System
Remarks	Unaffected System (optional)
Description	
Publication Context (optional)	
Technical Context (optional)	Context (optional)
Description	Description
Technical Description (optional)	
Diagnostic (optional)	Attack detection (optional)
Solution	
Solution Introduction	
Solution sections	Solution Countermeasures (optonal)

EISPP	CAIF
	Resolution (optional)
Vulnerability Identifiers and Additional Resources	
Vulnerability Id	Vulnerability Id
Additional Resources	Source
	Other Documents

At first sight it becomes clear, that the fields common in both formats predominate. This also had to be expected since they try to achieve the same objectives. But at this summary the essential differences don't immediately stand out. Besides different structures and levels of detail the different use of terminology has to be mentioned. A good example is the overall assessment of the risk (In this case the use of severity versus risk). But the problem lies more deeply and can be represented with the following questions:

- How agree to an assessment at all?
- What are the attack requirements?
- How is the probability of an attack and the possible impact classified?

Only if there is a common understanding about the assessment process and the classification of the different influence factors, the use of a common advisory format can have the desired effect. Furthermore within both formats no specification of a format or a standard naming system for affected platforms, software, etc, a so called "categorization model", is given. The use of a common scheme is prerequisite for an automated processing. The introduction and use of a common format depends substantially on the solution of these problems.

2.3.4 Conclusion

With EISPP and CAIF two candidates are available, on which foundation the cooperation between CSIRTS by the production of books can be improved. However, both approaches are still in the development phase, so that through participation in the discussion the further development can be influenced. One of EISPP Project objectives is to set up a network that would share the workload for producing Security Advisories in a co-operative way, so everybody interested in the common advisory format is invited. The CAIF project intends to become part of the IETF RFC standards development process.

2.4 Summary

One detail, almost all working groups experienced only having been already defined most of the formats, is, that it is indeed only a format. That has some advantages, as the formats are tailored towards the need for a specific interaction, but as co-operation almost always involves multiple interactions, the working groups need to forsee all such interactions, and try to put the protocol actions into the formats. The other approach would certainly be to develop new protocols, which is to be expected in the mid term.

As the standardization within the CSIRT environment is still in its infancy it is also difficult to access the real usage with its difficulties, as now the information exchange is manually and bilateral.

Certainly the lack of funding for initiatives or development work in this area is contributing to the slow speed of improvements, and adoption of available approaches. It is very difficult to overcame existing prejudices that "such solution will never scale", if no one has already made practical experiences and is able to report about it. One of the main reasons for no progress is the lack of funding for preparation and development contributed directly from the CSIRTs, as the management wants to spend the money only

on “being” a CSIRT and responding to incidents instead of investing in that area – which over time would save much more resources then.

Will concentrate on IODEF and IDMEF in this document, as eCSIRT.net focuses on responding to attacks and incidents, but the most important task is now developing “uniform categorization models” for the risk assessment and systems, an essential contribution for the further development of an Advisory Interchange Format can be made by the development of the common language for incident handling based on IODEF. As this is the task of the EISPP project, it can be expected that this project will lead to an improved co-operation and service towards partner and CSIRT constituencies for all teams that adopt the solutions developed.

3 Use Cases

The integration of any standard for the exchange of information into the CSIRT to CSIRT co-operation (and the infrastructures used for such co-operation) is only driven by real life applications. The use cases that are of interest for all CSIRTs will be presented in this chapter together with an assessment of the necessary steps to take to actually apply the available components.

3.1 Reporting towards a CSIRT

Currently the formats are not discussed in any particular context for receiving reports from the constituency. But certainly once the formats are established, there would be no reason not to make use of them in this context. Again – as we will see for other use cases – we have to consider the native application of the formats as well as helper applications allowing conversions towards or from the message formats.

One possibility would be to allow constituents to report attacks directly to the CSIRT. This will most likely be based on the IDMEF or, as an alternative, on a similar proprietary format of an IDS vendor.

In regard to IODEF a team could accept native messages as well as supporting some kind of gateway, but in the later case the main question would be, why a gateway should create an IODEF message instead of importing the data directly into any database the team uses.

3.2 Exchange between CSIRTs

The exchange between CSIRTs is very different from exchanges with constituents, as the level of expertise as well as the amount of information is concerned. Information about attacks will most certainly be exchanged between CSIRTs. But this exchange will be centred around incidents and not attacks. That means that a CSIRT will try to correlate as much as possible all information that can be attributed to the same incident.

This – by default – will include all IDMEF messages describing the attacks that a CSIRT has access to. This also means, that it cannot be anticipated to handcraft extended IODEF messages manually or even with help of a web interface.

Without the exchange of native IODEF messages the use of IODEF will therefore be very restrictive and most likely be reduced to the initial incident report.

3.3 Statistics across multiple CSIRTs

The use and exchange of statistics between multiple CSIRTs requires the establishment of a common standard of terms and classification schemes. This set of definitions, especially the classification of incidents, needs to be expressed with the IODEF syntax, as the IDMEF format is tailored towards information about attacks. Furthermore it is necessary to reach an agreement as to what kinds of incidents are contained within the scope of the format and henceforth the classification scheme.

An example here for this problem is an incident involving spam, which may be handled by some CSIRTs and not handled by others. If the statistics of various CSIRTs should be comparable and express real information, it is necessary to ensure that statistics from the various CSIRTs will be comparable to each other and will allow for meaningful aggregation into global statistics to give an overview of incident handling activity.

To ensure unambiguous incident classification, the standard should be enforced by guidelines with real world examples for most of the common incidents. All CSIRTs participating in the exchange of statistics must agree to respect these guidelines.

There are two methods of generating statistics based on the source generating them. The first method involves all CSIRTs sending IODEF objects with all the handled incidents for a given period, possibly in a sanitized version, to the clearinghouse which then proceeds to generate the statistics.

The second method involves the generation of statistics by individual CSIRTs and their submission to the clearinghouse. Both methods require an agreement on how the statistics will be submitted – whether as IODEF objects or through some other means, such as an HTML form provided by the clearinghouse.

Unfortunately, IODEF in its current form (May 2003) is not suited to the exchange of statistics. Another practical problem would be that it is not to be expected to send all the incident related information to any clearinghouse, even if this would be trusted. As usual a "need-to-know" principle would need to be adopted, making it more difficult to use the IODEF format for the exchange of statistics as sensitive data cannot always be identified with automatic approaches. Nevertheless, it is suggested that the exchanging of then sanitized IODEF objects would be more suitable and desirable. As there would be no extra effort involved, the burden on the participating team would be not that high.

Information sent by the CSIRTs should specify:

- Source (attacking) IP addresses involved in a particular incident
- The technical impact type(s) based on the assessment expressed in IODEF terms according to the specific class of the incident
- The methods (modus operandi) used in the incident once more expressed in IODEF terms

The statistics generated at the clearinghouse can then be based on combinations of the above elements for a given period.

It must be noted that IODEF does not allow for classification of institutions involved in an incident – for example, commercial or military – which is often viewed as an interesting statistic, or the most interesting after all, as the organization cannot be revealed easily.

3.4 Manual Alerting between CSIRTs

For alerts IODEF can be used, as it has enough fields to describe the circumstances that lead to an alert as needed. As the alert does not deserve as much communication as usually is involved in an incident, and as the set of information exchanged between teams is considerable smaller and not as complex, it is possible to either send IODEF as native messages or to use a web interface, collecting input to then produce an IODEF object which is then send around to all other CSIRTs. Such interface could also be established centrally and so safe some resources.

In regard to the set of information necessary for an alert the project already defined a suitable subset of IODEF, as it is even more important to be precise and concrete to allow a fast as possible information transfer towards the other CSIRTs once the team has realized the potentially dangerous situation.

4 Applying IDMEF and IODEF

4.1 Interfaces

In terms of the interface available for teams that want to use IDMEF and / or IODEF, we need to consider three different cases, based on the use cases defined and explained in the last chapter.

- **Receiving IDMEF**

  As the number of messages is so large, that all solutions that slow down the process of incorporating these messages will be disadvantaged, it is not fruitful to develop any gateway to transform IDMEF messages into other formats. This is even more true, as there is no other format that provide the same functionality and potential at this time.

  Certainly there might be format conversions necessary, most likely if messages are incorporated into databases, but then the "exchange" phase of the information has ended and the information is now further processed or stored for further processing.

- **Receiving IODEF**

  Receiving native IODEF messages will only be helpful for teams that can process these messages directly. For all other teams it would still be acceptable to receive IODEF messages, if they have either a IODEF-to-TEXT converter or if there is a gateway, that accepts IODEF messages, convert them to TEXT and forwarding them to the teams that are not yet IODEF-ready.

  While such converter could be working automatically, the converter could also provide an interface to the user. In this instance the converter would be in fact a web based form that will allow to convert all data input into an IODEF message. This is even more convenient and makes the data entry much more convenient, even without local efforts if a central web page can be utilized.

- **Sending IODEF**

  The same considerations as for receiving native IODEF messages apply to sending them.

Interestingly enough, providing one gateway for sending and receiving IODEF messages, that "translates" between the two different communities – IODEF-ready teams and the others – will be enough to allow a smooth transition and avoids that teams that need more time or resources for adopting IODEF would be excluded. This is even of advantage for the IODEF-ready teams as they do not need to handle any legacy systems or backward compatibility issues.

4.2 Operations

While the IODEF and IDMEF formats address the information exchange, each party using these formats need to consider storing this information locally. Most likely information received will need to be incorporated into databases, which means that the data format will no longer be used in order to achieve other benefits. There is basically no real possibility to not change the data model, as a team needs much more data regarding events then made available in these formats.

Another topic related to this is the triage of incoming information with already stored information. While this problem does not be a big concern for IDMEF, as the information is much more isolated and single event related, it is a problem for IODEF, when many messages are exchanged for one incident involving many hundred of compromised hosts.

To make these problem even worse, if multiple teams are involved, conflicting information might come in from multiple sources. Consider the following example:

1. Team A is sending information about Incident 321 to teams B and C

2. Team B is receiving an information, that site ABC is involved in Incident 321
3. Team C is receiving an information, that site ABC is not involved in Incident 321
4. Teams B and C are sending back their updated IODEF messages with all their information
5. Team A cannot resolve automatically the conflict between the incoming information, which requires human intervention (Team A could automatically send back an alert to the other teams, but that would not remove the need that someone needs to further research the conflict and resolves it)

A mitigation of these problems in near-time would inevitable involve some kind of protocol.

4.3 Security

The IDMEF standard relies on the communication protocol for integrity and authentication. There is a long and diverse discussion within the groups concerning the IODEF standard, in the end, only the final document will show the outcome, but it can be expected that in due course there will be no pre-requirements for any communication protocol as only an exchange format is defined.

For both formats however another approach would be to make use of XML related standards. The XML signature standard is still quite new but should offer message level integrity and authentication in the future. This has the advantage of remaining with the IDMEF message after transmission, and allowing specific sections of the XML to be signed.

As the formats are – as already indicated – only used for the exchange of information, the security problem for storing the information is of no concern for it. But the communication security needs to be maintained somehow.

Another problem obvious from the discussion in various working groups is the appropriate use of the information submitted within the formats. As long as the information can be tagged with the appropriate usage level, and as long as there are organizational policies and procedures in place, that ensure that such tags are indeed accepted and enforced, this is of no concern for the format itself.[3]

Therefore for the format privacy and non-disclosure issues can be safely ignored. Not ignored can be the following topics:

- Confidentiality – it is required that all transmitted information needs to be protected against sniffing and observing by unauthorized parties
- Authenticity – it is required that all parties can check on the authenticity of the transmitted information. This implies, that the sender of the information can be identified.
- Non-repudiation – As the authenticity of the transmitted information most likely be achieved by public key cryptography, this will at the same time ensure, that the sender cannot deny having actually send the information.

Technology is used day-to-day to solve similar problems in other application environments. This implies that either the security requirements outlined above are achieved by the application itself – the security is then embedded – or by other means achieved, usually by using a secure transport mechanism.

Depending on the final specification of the formats this means that additional efforts as well as specific solutions adding more overheads needs to be deployed.

It can only be hoped that the format specifications allow for the appropriate mechanisms to be included right away, as this would also remove obstacles in adopting the formats by teams which are concerned about the security issues.

[3] From a practically point of view it does not matter how information is transferred – as IODEF or as email – if the other team does not protect the information received or does not accept the restrictions of the sending team.

5 Integration into CSIRT Operations

While evaluating the potential take-up of the formats discussed in this report the situation of the teams must be considered as one of the main factors. Any integration of specific technical solutions into CSIRT infrastructures will depend on the actual level of sophistication. Based on a review of existing CSIRTs, three classes can be identified:

- Class A) no tools or databases are used, most likely flat files are used to store information
- Class B) proprietary tools are used to deal with some set of structured information
- Class C) standard databases and helpdesk solutions are tailored towards their needs

All of the three classes will need to be reviewed a little more detailed in order to identify any problems that might exist in regard to adopting these formats.

5.1 Type A CSIRTs – No tools or databases

Some teams do incident handling by storing information concerning incidents in (flat) text files. There are some advantages to this form, as the team is highly flexible in choosing the platform on which to work and what tools to use. Every operating system and nearly every piece of software is able to handle text files. There are a lot of tools for most of the platforms to work on these files, search for certain text strings in order to for example correlate incidents. There are the GNU tools like "grep", "sed" oder "awk", which are available as open source, so they are highly portable to nearly every kind of operating system.

On the other hand there are some drawbacks in doing incident handling with flat text files. Correlating incidents with "grep" and "awk" is a very difficult and time consuming task. One has to choose complex regular expressions when it comes to correlate more than a couple of incidents involving more than one correlation indicator.

This problem can be compensated by using scripts like shell-scripts or perl-scripts, but experience shows, that the team has to generate new scripts every now and then when it comes to correlate new kinds of incidents with new indicators. Porting the flat file incident handling system to a somewhat more experienced system like request tracker in conjunction with some sort of (perhaps SQL-) database would require a lot of work, but which has to be done only once. To be able to correlate incidents with flat files the team already had to chose some distinct, well defined format for the files, perhaps already with keywords as a preamble. So to transform those data from text file to database format, the same tools can be used, which the team does incident handling with: grep, sed, awk in conjunction with some script language like PERL or PYTHON can do the job for all of the data stored in those flat files. So the team has finally to write some scripts to change to database based incident handling and can use the experience it gathered in the past by correlating incidents with just the same methods.

5.2 .Type B CSIRTs – Proprietary tools and structured data

Some CSIRTs have developed various tools for the purpose of incident handling. In most cases incident data is stored in some database which is accessed mainly through proprietory tools, not from an elaborated application.

In order to implement an incident data exchange with the IODEF format, custom filters need to be applied for exporting IODEF documents to and importing them from the database. These filters will only be needed at the time of sending or receiving IODEF messages. Therefore the filters may be external to other tools and / or filters unless email handling is done inside these tools. Currently only a limited number of tools is available to support the creation of such filters. List of products supporting IODEF can be found at: http://www.ecsirt.org/service/documents/iodefproductlist.html.

Different problems must be considered when implementing the import and export of IODEF messages into proprietary tools based on existing databases. The most important issue is possible incompleteness of data stored in the database. Some information that is mandatory for an IODEF document may not be used in certain teams and thus may not be in the database nor can it be easily derived from other information. In this case, apart from changes in the database structure, a reconsideration of the incident handling policies will prove to be useful. On the other hand, IODEF messages may not always contain all information – certain teams put into their database (e.g. proprietary incident classification) also in the database. Obviously any extra information from the database or the IODEF document can be either discarded or stored in appropriate free text records.

Other issue related to importing and exporting data from and to IODEF messages is the specific data structure used in IODEF (e.g. nesting, linking contact and host information). The structure of databases used in proprietary tools is likely to be entirely different. It should, however, let easily derive all logical information needed to create an incident description in IODEF format. If it is not possible, then the capability of incorporating IODEF easily may be largely reduced or even none without major changes in the database structure.

5.3 Type C CSIRTs – Databases and helpdesk solutions

Longer established CSIRTs like the UKs JANET-CERT, are reviewing the established incident handling infrastructure. While their system was designed a number of years ago and has

not kept up with our workload, there are no urgent plans to replace the whole infrastructure without proper notion of what is actually going on.

Teams that review their whole installation are expected to look for a readily-deployable solution, as there is no change to stop the CSIRT service for the time of migration. It can also be expected that there is some time, when two – the old and the new – systems are operated in parallel.

This step is even more difficult for teams, as no real CSIRT enabled helpdesk solution is available. Only slowly – next month during the upcoming FIRST conference some results for an open source solution will be presented – do become some solutions available.

The communication of these teams with CSIRTs still rely on Email. This is also true for any communication with their constituency. Therefore each solution would need to consider this. Certainly Email could be used – with the proper security mechanisms – to transfer IODEF objects at nearly any location and very easily without much demanding requirements. On the other hand does the integration of IODEF via email into the helpdesk deserves many efforts and will make the helpdesk to helpdesk solution much more difficult then any direct transfer.

5.4 Summary

Given the description and evaluation above, it seems obvious that there might be only two groups with the potential to become early adoptors:

- Class B and C teams might – whenever selecting a new database – choose an existing infrastructure
- Class B and C teams might – given enough budget is available – create their own input and output filter

In any case with the help of interfaces all classes could at least participate to some degree. To make them operational, a web interface will need to be established for sending message in two – ASCII and IODEF formats – to allow sharing the information easily.

Early adaptors will be Class C teams, if they are willing and / or able to change to a new system containing / providing all functions needed. The main problem here is that there is no CSIRT Helpdesk tool available, that already incorporates these, so more effort is necessary.

Class B teams will have more difficulties, but might be the adaptors once they realize the weaknesses of their actual solutions. But they will only move if they see clearly the benefits and can actually move to another Class C solution with an IODEF-ready import and export function.

6 Outlook

The standardisation of CSIRT related activity has began. Now it is still difficult to apply very new and not well understood applications in such a sensitive environment as the CSIRT community is. On the other hand there is no reason to believe, that CSIRTs can avoid the automation of many tasks in the near future.

In addition to the concerns outlined in this report regarding to the integration of IDMEF and IODEF in the CSIRT community, it is therefore increasingly important to provide the CSIRTs with the necessary incentives to invest in their operations instead of demand only that everything needs to be invested in handling the incidents only. While the latter will result in spending less resources in the first time, a proper investment could be much more helpful to reduce the overall level of resources necessary in the mid term. As CSIRTs could greatly improve on the efficiency of their co-operation and information exchange, there are still great benefits that will result in better service and more detected and resolved compromises or incidents.

Projects as eCSIRT.net can help to research the take-up and related issues of new technologies, and in some areas help to bridge the worlds by simple integration efforts like it is planned for the upcoming work packages WP4 and WP5. Especially for WP5 a web-interface will be established to create IODEF objects based on input via some simple and easy to understand web page.