



# Report on Fourth Training Workshop

IST-2001-39118

**Training of Network Security Incident Teams Staff**

**TRANSITS**



**Deliverable no. D7**

Project Manager: Karel Vietsch

TERENA, Singel 468 D, 1017 AW Amsterdam, The Netherlands

Phone : +31 20 5304488  
Fax: +31 20 5304499  
Email: vietsch@terena.nl

Date: 16 June 2004

## CONTENTS

<b>Executive Summary</b>	<b>3</b>
<b>1. Workshop Objectives and Background</b>	<b>3</b>
<b>2. Workshop Preparations</b>	<b>4</b>
2.1. Selection of Venue	4
2.2. Choice of Presenters	5
2.3. Workshop Announcements and Selection of Participants	5
2.4. Financial Arrangements	6
2.5. Workshop Materials	6
<b>3. Workshop Delivery</b>	<b>7</b>
3.1. Participants	7
3.2. Programme	7
3.3. Experiences of Presenters and Trainees	9
3.4. Results from Feedback Forms	10
<b>4. Actions Arising</b>	<b>11</b>
<i>Annex I</i>	<i>Workshop Evaluation Form</i>
<i>Annex II</i>	<i>Fourth TRANSITS Training Workshop materials</i>

## **Executive Summary**

The fourth TRANSITS training workshop was held at the Mellingburger Schleuse Hotel in Hamburg, Germany on May 25<sup>th</sup> and 26<sup>th</sup>, 2004. As with the previous workshops, a mailing list for the participants has been set up to help them communicate with each other in future. A number of the students had been recommended to attend by colleagues who had themselves been to earlier TRANSITS workshops; it is particularly welcome to see TRANSITS being used to help expand existing small CSIRTs to make them more sustainable.

For the first time, a TRANSITS workshop was not oversubscribed, and actually the potential workshop capacity (about twenty trainees) was not fully used. Feedback received immediately after the workshop from the European CSIRT community through TF-CSIRT make the organisers believe that this was a one-off effect rather than a trend. A poll showed that there is more than sufficient interest among European CSIRTs to send their staff to TRANSITS training courses within the next twelve months. Improvements will be made in the way the future workshops will be announced.

## **1. Workshop Objectives and Background**

Increasing the proportion of European networks that have Computer Security Incident Response Team (CSIRT) services is a major part of improving the dependability of networks and promoting public confidence in the Internet. The objective of the TRANSITS project is to promote the creation of more, professional CSIRTs and the strengthening of existing CSIRTs.

Operating a CSIRT takes rare and specialist skills; currently there are only a few hundred experts in Europe who have the necessary knowledge and experience. The TRANSITS project addresses this problem by providing specialist training to staff members of new CSIRTs and new staff members of existing CSIRTs.

Before the start of the TRANSITS project, course materials had already been prepared, but these need to be edited, maintained and updated during the lifetime of the project. A try-out presentation of the course was made in January 2002 in a workshop hosted by Telia at its headquarters in Farsta near Stockholm, Sweden. After the start of the TRANSITS project in July 2002, the earlier material and the feedback from the try-out presentation of the course were taken as inputs for preparing the first edition of the course material. That work was completed in September 2002, and the result was submitted to the European Commission as TRANSITS deliverable no. D1.

During the lifetime of the TRANSITS project the course materials will be presented six times, and it is intended to spread the locations of these six training workshops over various regions in Europe. The first training workshop took place in Oegstgeest, the Netherlands, on October 31<sup>st</sup> and November 1<sup>st</sup>, 2002 and was reported on in TRANSITS deliverable no. D2. The second TRANSITS workshop was held in Warsaw, Poland, on May 27<sup>th</sup> and 28<sup>th</sup>, 2003 and was reported on in deliverable no. D3. The third workshop was held on October 30<sup>th</sup> and 31<sup>st</sup>, 2003 in San Gaudenzio near Milan, Italy and was reported on in deliverable no. D5. The

present deliverable reports on the preparations for, and the delivery of the fourth training workshop.

The course was presented using the latest version of the TRANSITS materials. A major review in early 2004 had resulted in significant changes to all modules. This second edition of the course material was submitted to the European Commission in March 2004 as deliverable no. D6.

## **2. Workshop Preparations**

The training workshop required careful preparations. The two TRANSITS project partners, TERENA (the Trans-European Research and Education Networking Association) and UKERNA (the United Kingdom Education and Research Networking Association), were both involved in this. TERENA's Karel Vietsch and Carol de Groot took responsibility for identifying a suitable location, arranging accommodation and arranging financial support to trainees if needed. UKERNA's Andrew Cormack took charge of ensuring the availability of teachers and preparing the contents of the workshop materials. The course was advertised jointly by both organisations, and Andrew Cormack and Karel Vietsch together took responsibility for the selection of trainees, asking for the advice of prominent members of TERENA's task force TF-CSIRT when needed. TERENA staff took care of having the printed workshop materials produced. Karel Vietsch and Carol de Groot installed Internet connectivity at the workshop venue.

### **2.1. Selection of Venue**

In view of the intention to spread the locations of the six TRANSITS training workshops over various regions in Europe, it was decided at the start of the project to organise the first workshop in Western Europe, the second in Central/Eastern Europe, the third in Southern Europe, and the fourth in Central/Northern Europe.

Criteria for the selection of the venue included:

- A location at a reasonable travel distance from a major international airport. Many of the workshop participants have busy diaries and it was felt to be important to keep travel time as limited as possible.
- A secluded venue with the necessary meeting rooms, hotel rooms and facilities for meals in one location. Since the training benefits strongly from personal interactions, also outside the formal sessions, it is important to make intensive use of the 48 hours that trainees and lecturers are together.
- Moderately priced accommodation. While room hire, meals for workshop participants and travel and subsistence costs of the lecturers are paid by the TRANSITS project, trainees are expected to cover their own travel and hotel costs. Some of their employers are not-for-profit organisations with limited means.

For the fourth workshop it was attractive to find a venue in the Hamburg region, so that a number of the participants would find it easy to attend the TF-CSIRT meeting and seminar that would take place in the centre of Hamburg on the two days following the workshop.

Nevertheless, because of the experiences from earlier TRANSITS training courses, much importance was attached to the criteria listed above. Big-city hotels cannot offer the right environment for the training course. Fortunately, the Mellingburger Schleuse met all the criteria while at the same time being within reasonable travel distance from Hamburg's main centre.

## **2.2. Choice of Presenters**

Lecturers were recruited from the most experienced staff members and former staff members of major professional CSIRTs. A number of members of task force TF-CSIRT have committed themselves to contribute to the TRANSITS materials and to act as teachers of course modules at a number of the training workshops. Some of the available volunteers had been co-authors of the original training course materials and/or had presented at the try-out workshop in January 2002 or the first three TRANSITS training courses.

It was therefore not difficult to find a sufficient number of very well qualified presenters. The organisers were particularly happy to find two new presenters, including Dr. Claudia Natanson, a very prominent member of the global CSIRT community and one of the original authors of parts of the training materials. The following team was chosen:

Andrew Cormack	UKERNA	United Kingdom
Stelios Maistros	GRNET-CERT	Greece
Klaus Möller	DFN-CERT	Germany
Claudia Natanson	BT SBS	United Kingdom
Jacques Schuurman	SURFnet-CERT	Netherlands

## **2.3. Workshop Announcements and Selection of Participants**

On February 13<sup>th</sup>, 2004 the announcement of the training workshop was published on the TRANSITS website ([www.ist-transits.org](http://www.ist-transits.org)). This announcement contained a course summary, an explanation of the pre-requisites, information about the time and venue and the costs, and instructions on how to apply for participation. At the same time the announcement was sent via the appropriate mailings lists to the members of TF-CSIRT, the FIRST membership and the research and education networking organisations in Europe (the TERENA membership). Four additional mailing list were used to spread the announcement: a general TRANSITS announcement list to which any interested person can subscribe to receive TRANSITS news (see [www.ist-transits.org/maillinglist.php](http://www.ist-transits.org/maillinglist.php)), and the mailing lists of participants in the first, second and third TRANSITS workshops. Reminders were sent to the same communities in the second half of March and in early April.

The following time schedule was mentioned in the workshop announcements:

8 April 2004	Deadline for sending in applications
16 April 2004	Applicants will be notified whether a place has been reserved for them at the workshop
10 May 2004	Deadline for payment of the accommodation costs and the registration fee.

Eventually, fifteen applications were received. All these applicants were well qualified to attend the training course, and were therefore accepted. All accepted candidates confirmed their participation and met the requirement of timely payment of accommodation costs and registration fee.

#### **2.4. Financial Arrangements**

As described in the TRANSITS project workplan, all trainees were expected to pay their own accommodation costs at the *Mellingburger Schleuse* as well as a (symbolic) fee of 100 euro. Participants were asked to pay these sums to TERENA no later than fourteen days before the event. This arrangement not only simplified financial administration, but it also reduced the risk of no-shows.

All participants paid their accommodation costs and fee on time, although establishing and maintaining contacts with participants in order to be certain that their payment would arrive took some time and effort from TERENA staff. However, this problem was far less substantial than on the previous three occasions.

Within the TRANSITS budget, TERENA manages funds to cover part of the travel and subsistence costs of training workshop participants from economically less-developed countries in Europe. This financial support will always cover only part of the total costs of these participants and will be limited to trainees from non-commercial, non-profit organisations. In the workshop announcements it was mentioned that such partial reimbursements of costs could be made available to participants from countries that are qualified by the World Bank as low-income economies, lower-middle-income economies or upper-middle-income economies. Only one of the participants in the fourth TRANSITS workshop applied for reimbursement of part of his costs from these funds.

Within the TRANSITS budget, UKERNA manages funds to cover the travel and subsistence expenses of the lecturers who are not UKERNA or TERENA employees. These costs will be reimbursed after the event on the basis of invoices sent by the presenters to UKERNA.

#### **2.5. Workshop Materials**

The course was presented using the latest version of the TRANSITS materials. Participants received a workshop pack containing printed copies of the slides, exercises and supporting documentation. Digital copies of these materials were provided on the workshop CD-ROM, which also included the CSIRT Handbook (with thanks to the copyright holders, Carnegie Mellon University) and a new paper on Incident Response made freely available by the US National Institute for Standards and Technology (NIST). The CD-ROM also contained RFCs relevant to CSIRT work. Each participant pack also included a copy of the book *Incident Response* by Kenneth R. van Wyk and Richard Forno (published by O'Reilly & Associates, Inc.) and a Guidance Note on writing advisories published by UKERNA. Some slides were modified immediately before the course; these were sent by email to participants later, using the workshop mailing list.

Thanks to the relatively short overland distance between Amsterdam and Hamburg it was possible for the TERENA staff to personally transport the workshop materials from the TERENA office to the workshop venue.

### **3. Workshop Delivery**

#### **3.1. Participants**

Fifteen trainees attended the course, from ten countries:

Warren Daly	HEAnet	Ireland
Aleksandar Dimeski	MARNET	FYRo Macedonia
Serge Droz	SWITCH-CERT	Switzerland
Victor Ewald	University of Amsterdam	Netherlands
Lionel Ferette	BELNET	Belgium
Frank Klein	Siemens-CERT	Germany
Detlef Lange	CERT-VW	Germany
Huw Langford	BTCERT	United Kingdom
Mally Mclane	JANET-CERT	United Kingdom
Tassos Moschos	GRNET-CERT	Greece
Matthias Oberlinner	Siemens-CERT	Germany
Daniel Staszczyszyn	CIRC/CC	Poland
Harri Sylvander	FUNET CERT	Finland
Chris Trauner	Siemens-CERT	Germany
Pieter Zaalberg	University of Amsterdam	Netherlands

Of these trainees, eleven work for existing CSIRTs and four were from organisations that are in the process of creating a new CSIRT. Three of these organisations had not participated in European CSIRT activities before. The majority of the CSIRTs represented are associated with research and education networks, but three commercial organisations and one military organisation were represented.

The lecturers came from the education and commercial sectors and had between them some 25 years of CSIRT experience.

#### **3.2. Programme**

The objectives of the training workshop were:

- to understand where CSIRTs fit into the organisation
- to understand the tasks and tools that are necessary to perform their function
- to develop and practice the skills that are needed by a CSIRT team member
- to understand the external issues (both legal and technical) that may effect the operation of a CSIRT.

The course consisted of five modules. Some of these included exercises that the trainees had to complete and discuss, while others included time for discussion among the whole class. The modules were:

- CSIRT Organisation

Describes how CSIRTs fit into their organisations; planning the CSIRT, defining the constituency of the team and gaining management authority for it, deciding the services the team will offer, working with those outside the organisation, staffing the CSIRT, funding. Trainees discussed their own organisation and how their team fits into it.

- Technical Aspects

Understanding how intruders attack systems; intruders and their motivations, network protocols and how they can be abused, operating systems and services, types of vulnerability, information gathering, breaking in, hiding traces, denial-of-service attacks. A number of exercises were used to show how these appear in practice.

- CSIRT Operations

Describes the facilities, systems and tools needed by CSIRTs to operate successfully; housing the CSIRT, equipment, e-mail, remote access, information and contacts, servers and networks, incident response plans and procedures, tracking systems. As an exercise trainees discussed and developed incident response plans for their own teams.

- Legal Issues

Looks at the areas of legislation that are likely to affect CSIRTs in their work and that team members need to be aware of; origins of computer legislation, problems, data protection, computer misuse, working with law enforcement, monitoring, evidence, European developments.

- Working with Vulnerabilities

Discusses the roles that CSIRTs may decide to play in distributing and producing information about vulnerabilities; why do vulnerabilities exist, what should CSIRTs aim to do, sources of information and how to use them, advisories – distribution, interpretation, investigation and co-ordination.

The modules were presented in parallel in two groups. In order to encourage interaction with participants not known to them earlier, trainees were divided over these groups such that if possible people from the same organisation were not in the same group, and in each group the number of participants with the same mother language was minimised.

The arrangement of the third workshop was repeated, with the module on Technical Aspects being split across the lunch break to reduce the intensity of the lengthy block of teaching. As before, this seemed to reduce the students' concerns about the volume of material being presented to them. Informal exercises were used in the modules on Operations and Organisation, which seemed to be particularly good for encouraging students to consider and discuss their own situations. As this is all done in English it requires more fluency in the language than the paper exercises, but the format should be repeated in future if groups of trainees are comfortable with it.

The time schedule of the two workshop days was as follows:

### Tuesday May 25<sup>th</sup>

Time	Group 1 in Alsterblick I + II	Group 2 in Grünes Zimmer
09.30	Welcome and introductions (Alsterblick I + II)	
10.00	Operational Issues	Legal Issues
11.30		Technical Issues
12.30	Lunch	
13.30	Operational Issues (report back)	Technical Issues
14.30	Organisational Issues	
16.30		Vulnerabilities
18.00	Close	
19.30	Dinner	

### Wednesday May 26<sup>th</sup>

Time	Group 1 in Alsterblick I + II	Group 2 in Grünes Zimmer
09:00	Legal Issues	Operational Issues
10.30	Technical Issues	
12.30	Lunch	
13.30	Technical Issues	Organisational Issues
15.30	Vulnerabilities	
17:00	Presentation and Close (Alsterblick I + II)	

**Group 1:** Droz, Melane, Moschos, Oberlinner, Staszczyszyn, Sylvander, Trauner, Zaalberg

**Group 2:** Daly, Dimeski, Ewald, Ferette, Klein, Lange, Langford

### 3.3. Experiences of Presenters and Trainees

The workshop venue worked very well and the hotel staff were supportive. Serving and eating a large meal within the hour allocated for lunch proved to be a challenge, but gave unexpected time for informal discussions. Two rooms were used for teaching sessions: both were pleasantly light and airy. There were plenty of other seating areas for individual discussions. Meals and accommodation were in the same building as the meeting rooms, so lecturers and trainees were able to talk together throughout the period of the workshop. These discussions were seen to be particularly valuable in an area such as incident response, where there is rarely a single "correct answer": one of the aims of the course is to encourage students to develop ideas that are applicable to their own CSIRT. The teaching sessions were presented in two groups of seven and eight students, with all the tutors attending one or the other session.

A wireless network was installed to cover the teaching rooms and most of the social areas. External connectivity was by an ISDN line, which may be less than most participants are used to, but was praised by one as removing a likely distraction. The network was useful for referring students to websites and documents that were mentioned in discussions. Connectivity also makes it easier for tutors, who volunteer their time, to keep in touch with their own organisations.

Every trainee was asked to fill in a feedback form during the course to rate the content and presentation of each of the modules, and the workshop organisation and venue. Written comments were also sought to help in developing the materials and organising future workshops. Marks were requested for each module for level and quantity (from 1, trivial, to 5, excessive), for usefulness, organisation, visuals and delivery (from 1, low, to 5, high). Marks on the latter scale were also requested for workshop announcements, application and selection process, pre-workshop information, meeting rooms, Internet connectivity, hotel rooms, meals and support staff. Fifteen completed feedback forms were returned. Overall the results were positive, with the modules averaging between 3.0 and 3.5 for level and quantity, 3.6 to 3.9 for usefulness. The Vulnerabilities module had slightly lower scores, between 2.8 and 3.1; the current content of this module is known to be most relevant to national co-ordinating CSIRTs, which were in the minority at this workshop. Presentation was rated highly, scoring between 3.7 and 4.3. Logistics scored between 3.6 and 4.1 and the venue between 3.4 and 3.9.

Many participants also took the time to give detailed comments on the course. Their suggestions for improving the materials and the application process will be used for future training course deliveries. General comments were positive: "thought provoking and very relevant to my work situation", "great ideas for improving our service to customers" and "best training I have been on". A number commented on the quality of discussion between students and trainers and asked for more opportunities for this type of learning.

### **3.4. Results from Feedback Forms**

Mean scores were as follows (all scores on a range from 1 to 5 – see section 3.3 for details):

<b>Module:</b>	<b>Organisation</b>	<b>Legal</b>	<b>Vulnerabilities</b>	<b>Operational</b>	<b>Technical</b>
Level	3.40	3.14	2.80	3.27	3.23
Quantity	3.00	3.07	3.07	3.40	3.47
Usefulness	3.87	3.73	2.93	3.73	3.57
Organisation	4.14	3.87	3.87	3.93	3.87
Visuals	3.87	3.73	3.67	3.80	3.73
Delivery	4.27	4.20	3.80	4.33	3.93

<b>Logistics</b>	
Announcements	3.85
Application & Selection	3.62
Pre-workshop information	4.00
Meeting rooms	3.79
Internet connectivity	3.00
Hotel	3.93
Meals	3.36
Support	4.08

#### **4. Actions Arising**

The following action items will be taken up in the TRANSITS project as a result of the experiences from the fourth training workshop:

- The course modules will all be revised in the light of comments from trainees and presenters during the course.
- The Vulnerabilities module will be extended to make it more relevant to a wider range of CSIRTs.
- The workshop documentation and application process will be reviewed in the light of comments from students.
- More opportunities for discussion will be included in future courses; these are likely to cover incident response scenarios and risk assessment – particularly successful innovations at this workshop.
- A mailing list has been created for the trainees and presenters from the course to enable discussions to continue.
- The successful and less successful aspects of this venue will be considered in the choice of venue for future workshops.