22-12-2021

Deliverable D8.5
Security Training Materials for NRENs and Constituents

Deliverable D8.5

Contractual Date:	31-10-2021
Actual Date:	22-12-2021
Grant Agreement No.:	856726
Work Package	WP8
Task Item:	Task 1
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	LITNET
Document ID:	GN4-3-21-5372A0
Authors:	Klaus Möller (DFN-CERT); Christine Kahl (DFN-CERT); Stefan Kelm (DFN-CERT); Tobias Dussa (DFN-CERT); Šarūnas Grigaliūnas (LITNET)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Abstract

This document describes the GÉANT Operational Network Security and Vulnerability Management training courses designed for network and system administrators at NRENs and their member organisations, which were developed to close the gaps in training materials identified in Deliverable D8.1.

Table of Contents

Executive Summary 1

1 Introduction 2

2 Operational Network Security Course Structure and Content 4

3 Vulnerability Management Course Structure and Content 11

4 Review Outcome 15

5 Recommendations 17

6 Further Use of the Courses 18

7 The Road Ahead: IT Forensics for System Administrators 19

8 Conclusions 22

Appendix A Surveys and Results 23
A.1 Operational Network Security Course 23
A.2 Vulnerability Management Course 38

Appendix B YouTube Viewings 43

Appendix C Course Resources 46

References 47

Glossary 48

Table of Figures

Figure B.1: YouTube viewings August 2020 to January 2021 43
Figure B.2: YouTube viewings January to June 2021 43
Figure B.3: YouTube viewings June to 9 November 2021 44

Table of Tables

Table A.1: Operating System Privacy and Security – Operating System Telemetry session: attendees 23
Table A.2: Operating System Privacy and Security – Operating System Telemetry session: survey responses 25
Table A.3: Operating System Privacy and Security – Logging and Audit session: attendees 25
Table A.4: Operating System Privacy and Security – Logging and Audit session: survey responses 27
Table A.5: Operating System Privacy and Security – File Integrity Monitoring (FIM) for detecting security incidents session: attendees 27
Table A.6: Operating System Privacy and Security – File Integrity Monitoring (FIM) for detecting security incidents session: survey results 28
Table A.7: Operating System Privacy and Security – Network First Hop Security session: attendees 29
Table A.8: Operating System Privacy and Security – Network First Hop Security session: survey results 30
Table A.9: Operating System Privacy and Security – Authentication Methods session: attendees 31
Table A.10: Operating System Privacy and Security – Authentication Methods session: survey results 32
Table A.11: Client Privacy and Security submodule: attendees 32
Table A.12: Client Privacy and Security submodule: survey results 34
Table A.13: Domain Name System (DNS) Protection submodule: attendees 34
Table A.14: Domain Name System (DNS) Protection submodule: survey results 36
Table A.15: Distributed Denial of Service (DDoS) Protection submodule: attendees 37
Table A.16: Distributed Denial of Service (DDoS) Protection submodule: survey results 38
Table A.17: Vulnerability Management Process & Standards submodule: attendees 39
Table A.18: Vulnerability Management Process & Standards submodule: survey results 40
Table A.19: Finding Vulnerabilities I – Looking into Networks submodule: attendees 40
Table A.20: Finding Vulnerabilities I – Looking into Networks submodule: survey results 42
Table A.21: Finding Vulnerabilities II – Looking into Code submodule: attendees 42
Table B.1: Training recordings: number of views, watch time and average view duration per session 45
Table C.1: Links to course resources on GÉANT and GÉANT GLAD pages 46

Executive Summary

In view of the continuously increasing importance of cyber security, during the preparation of the GN4-3 project a demand for more security trainings was expressed by the GÉANT community.

To understand where it would be most beneficial to the GÉANT community to develop additional security trainings and materials, and as the first step to preparing and delivering new training courses, Work Package 8 Security, Task 1 Business Continuity (WP8 T1) conducted a gap analysis. The gap analysis revealed that the least covered categories of trainings include operational network security, secure coding / vulnerability management, general cyber security, and forensics. Another finding of the analysis was that most of the trainings that address a specific group were aimed at security personnel tasked with handling incidents, while administrators and developers were neglected.

As a result of the findings of the gap analysis, it was decided to design the new training courses primarily for system and network administrators based on the least covered training categories.

Because of the COVID-19 pandemic, the subsequent restrictions, and the need to reduce in-person contact, it was decided to deliver the trainings as online courses. That removed the need to limit the number of participants, which usually applies to on-site trainings, and even though the trainings are of particular interest to system and network administrators, the courses were open for everyone within the GÉANT community interested in the outlined training topics.

As of November 2021, two training courses have been developed and delivered:

- Operational Network Security, and
- Vulnerability Management.

Preparation and delivery of the third training course, IT Forensics for System Administrators, is currently underway.

After completion of the first training course, an internal review was conducted to determine areas for optimising the online training sessions. The findings of this review have resulted in extensive promotional activities for the third training course; offering the course to a broader community and not only to the GÉANT community; including some interactive exercises into the sessions; and collecting feedback and requirements from attendees before conducting the final sessions about tools.

The first two new courses have received positive feedback from the attendees, and more than 700 people have registered for the third, confirming that WP8 T1 is well on its way to closing the security training gaps identified in D8.1.

1 Introduction

The importance of security and, more recently, privacy in National Research and Education Network (NREN) networks is well known. The relevance of trainings in this area is therefore widely recognised. However, as shown by the gap analysis, including interviews with NRENs, that was conducted by Work Package 8 Security, Task 1 Business Continuity [WP8_T1] as part of Deliverable D8.1 *Summary of Security Training and Awareness Campaign Materials: An Investigation and Gap Analysis of Current Security Training and Awareness Resources* [D8.1], there is an ongoing demand for more security trainings.

With reference to the above-mentioned analysis of courses and training materials currently available to NRENs, most of the security trainings (75%) are offered to technical staff. Of these security trainings, 44% do not target a specific technical group, 37% are designed for security personnel tasked with handling incidents, while only 12% are specifically designed for system and network administrators and only 7% for developers.

The gap analysis also gained a picture of the cyber-security areas that are well covered by the courses and training materials and those that are less covered. The analysis revealed that operational network security was the least covered category, as only 3% of the trainings deal with it. Slightly more trainings are available with regard to secure coding / vulnerability management, general cyber security, and forensics. Each of these three topics has a quota of 4% of the analysed training material and comprise the second least covered category of trainings.

As a result of the findings of the gap analysis, and taking into account also the interviews that were carried out with the NRENs, it was decided to design and deliver a first training course focused on operational network security for system and network administrators, as they are usually impacted by security issues at first hand. The second course to be developed was about vulnerability management, separating the secure coding aspects into different levels, also aimed at system and network administrators. The secure coding aspects were differentiated by level as Work Package 9 Operations Support, Task 2 Software Governance and Support (WP9 T2) is delivering trainings in this area specifically addressing software developers, who are probably the main target group for this topic. However, as it is still important for system and network administrators to understand and to deal with secure coding aspects in some ways, the topic was not omitted completely from the second course; only the in-depth training for software developers was considered to be covered by parallel activities in the GN4-3 project.

To close the identified gaps, the Operational Network Security training module and the Vulnerability Management training module were created, based on the experiences of and discussions with security officers and network operators, to address a number of common security risks that NRENs and their

member organisations face in their day-to-day IT operations and to strengthen the knowledge about processes and standards to mitigate some of those risks. These include:

- Authentication.
- Logging.
- Audit.
- Privacy.
- First hop security.
- Domain Name System (DNS) security.
- Protection from Distributed Denial of Service (DDoS) attacks.
- Vulnerability management.
- Vulnerability information, scanning and disclosure.
- Patch management.
- Penetration tests.
- Code audits.
- Breach and attack simulation.

Due to the COVID-19 pandemic and the subsequent need to reduce business travel and in-person contact, the original plan to deliver each training course as a two- or three-day on-site training was amended, and the courses were restructured and redesigned, with the support of the GÉANT Learning and Development (GLAD) team, into fully online training.

To allow the attendees to repeat the training sessions, and for the benefit of those who missed the course, all presented slides are available for download and further use without any restrictions. As the training sessions could only scratch the surface of some topics, the downloadable slides include additional training material and references as a starting point for users to undertake a more in-depth exploration. In addition to the slides, recordings of every session are available on YouTube. The slides and recordings may be accessed from [Security_Training].

This deliverable summarises the courses, giving, for each submodule, an overview, its delivery date, the number of attendees by session, a description of each session and links to the recording and slides (Sections 2 and 3). It also summarises the feedback that was gathered from the courses through different surveys (Section 4). The deliverable goes on to highlight some possible areas of improvement (Section 5) and opportunities for further use of the training materials developed (Section 6), and to give an overview of the third training course, IT Forensics for System Administrators, which, at the time of writing this document, has been created and delivery has begun, as Forensics also had only a 4% coverage in the analysed training material (Section 7). It ends with some overall observations and conclusions (Section 8).

Further details of attendees of the online training sessions from NRENs and member organisations by country, together with survey responses, are provided in Appendix A. Statistics on YouTube viewings are provided in Appendix B, and links to course resources are provided in Appendix C.

2 Operational Network Security Course Structure and Content

This section summarises the structure and content of the Operational Network Security course. It gives, for each submodule, an overview, the delivery date, number of attendees by session and a link to the course material, and, for each session, a description and links to the recording and slides. The overview and session descriptions are also used for the GÉANT Learning and Development (GLAD) and Security Training pages [GLAD_ONS], [Security_Training].

1st Submodule: Operating System Privacy & Security

There is no need to stress the importance of security and, as a more recent addition, privacy, in NREN networks. But while the importance of security and privacy is widely recognised, training in these areas has often been aimed at the security personnel tasked with handling incidents, while the system and network administration seems to have been neglected.

The aim of the Operational Network Security training programme is to address a number of common security risks that NRENs face in their day-to-day operations: authentication, logging, audit, privacy, first hop security, Domain Name System (DNS) security and protection from Distributed Denial-of-Service (DDoS) attacks.

Delivered on: 3–13 August 2020

Number of attendees by session: Operating System Telemetry: 91; Logging and Audit: 131; File Integrity Monitoring (FIM): 113; Network First Hop Security: 126; Authentication Methods: 110

Developed course material: https://security.geant.org/training/

Session	Content
Operating System Telemetry – configuring privacy protection in Windows 10	The session provides an insight into the telemetry mechanism Windows uses for data collection and how it can be configured to the needs of an organisation. It also explores additional ways to make Windows 10 more privacy friendly. **Recording:** https://www.youtube.com/watch?v=pwZwxnEXQAs&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=1 **Slides:** https://learning.geant.org/wp-content/uploads/Operating-system-Telemetry.pdf

Session	Content
Logging and Audit – log management and audit strategies	IT users know about log files and many of them – and not only system administrators – even regularly look at application logs, syslog entries, or Windows Eventlogs. However, without sound processes in place for analysing these logs, their value is significantly reduced. The session provides an insight into log management as well as audit strategies and some practical tips for configuring Windows & Linux logging/audit settings and understanding the need for central log collection and examination. **Recording:** https://www.youtube.com/watch?v=qAdmUOBQSA8&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=2 **Slides:** https://learning.geant.org/wp-content/uploads/Log-in-and-Audit.pdf
File Integrity Monitoring (FIM) for detecting security incidents	Detecting malicious changes to operating system files early and thoroughly is vital to the handling of security incidents. Programs to look out for such changes however are rarely used, although these have been around for a long time and their usefulness is unequivocally recognised. This seems rooted in the assumption that it is difficult and time-consuming to operate such programs properly. The session introduces the concept of file integrity monitoring (FIM) and gave practical tips to participants on how to plan and start adopting FIM in their organisation. It also includes a live demonstration of one of the latest open source FIM solutions 'Wazuh'. **Recording:** https://www.youtube.com/watch?v=tI-4tsek_5o&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=4 **Slides:** https://learning.geant.org/wp-content/uploads/File-Integrity-Monitoring.pdf
Network First Hop Security	Configuring end-user systems for accessing directly attached networks is being facilitated through use of automatic configuration protocols such as DHCP or IPv6 Router Discovery. Also, for operation on attached links, finding the corresponding link-layer address to an IP address is done using protocols such as ARP or IPv6 Neighbor Discovery. While these protocols are vital to the operation of the network, they inherit a number of security risks, which are also explored in this session, as well as ways to mitigate some security risks. **Recording:** https://www.youtube.com/watch?v=jfsmo9xsyuE&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=5 **Slides:** https://learning.geant.org/wp-content/uploads/Net-1st-Hop-Sec.pdf
Authentication Methods – how to avoid common pitfalls	Authentication is the basis for any kind of secure system. Unfortunately, it is also easy to get wrong, and getting it wrong fundamentally breaches a system's security. The session provides an overview of authentication methods and outlines the most important and relevant approaches in more detail to help participants avoid the most common pitfalls in this area.

Session	Content
	Recording: https://www.youtube.com/watch?v=BH03dRWGP2g&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=5 **Slides:** https://security.geant.org/wp-content/uploads/2021/11/2020-08-Authentication.pdf

Table 2.1: Submodule 1 – Operating System Privacy & Security

2nd Submodule: Client Privacy & Security

Examples of client software include web browsers, office programs, instant messenger applications, etc., tools which are used daily to communicate with colleagues or work on documents locally or online.

While we usually interact only with the user interface, the underlying software architecture and implementation are primary targets for attacks, on the campus or the internet.

This submodule shows how to configure securely commonly used client software to protect it against the most popular attacks and also shows how to safeguard personal information processed within these applications.

Delivered on: 21–30 September 2020

Number of attendees by session: Browser: 75; Email: 70; Instant Messaging: 49; Videoconferencing: 55; Office: 50

Developed course material: https://security.geant.org/training/

Session	Content
Browser Security & Privacy – secure surfing with fewer traces	Web-browsers have long been ubiquitous as providing a window onto the internet, with their versatility being a key factor in their success. But web browsers can also be (mis)used for tracking the activities of their users. Not surprisingly, the security of browsers and the privacy of those who use them have become one of the most important topics in information security. For Firefox and Chromium-based browsers, the session gives an introduction on how to secure them and how to avoid providing unnecessary personal data to websites or browser vendors. Participants are also shown how to avoid being tracked on their personal trail across the internet. **Recording:** https://www.youtube.com/watch?v=H3DDxa71aew&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=6 **Slides:** https://learning.geant.org/wp-content/uploads/Web-browsers-privacy-and-security.pdf
Email Security & Privacy – how to handle the most common issues	One of the oldest practical uses of the internet is email. Most of us use it on a daily basis, and email has become one of the most important tools of business. Email has also become one of the most universal and

Session	Content
	persistent sources of privacy and security headaches. The webinar gives an overview of the many challenges that email introduces and provides approaches on how to deal effectively with some of its more common issues. **Recording:** https://www.youtube.com/watch?v=GzjZMTmnksw&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=7&t=1886s **Slides:** https://security.geant.org/wp-content/uploads/2021/11/2020-09-E-Mail_Security_and_Privacy.pdf
Instant Messaging Security & Privacy – chat and more while safeguarding personal data`	From the Microsoft Messenger and Internet Relay Chat of the nineties to the more current WhatsApp and Discord, instant messengers pre-date the World Wide Web, and while the client programs have changed and gained functionality, their usage shows no sign of decline. Session participants are shown how to secure instant messenger clients and how to avoid common privacy pitfalls. **Recording:** https://www.youtube.com/watch?v=-LDe8iz9GMI&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=8 **Slides:** https://learning.geant.org/wp-content/uploads/Instant-Messaging-Security-Privacy-%E2%80%93-Chat-and-more-while-safeguarding-personal-data.pdf
An Overview of Best Practices for Videoconferencing Security & Privacy	Videoconferencing has been around for some time, but its use has increased manifold during the COVID-19 pandemic. With employees being locked down in their home offices, videoconferences have replaced business meetings and entire business trips, allowing the illusion of face-to-face interaction. This comes with the burden of an unknown impact on the privacy and confidentiality of the conversations, as well as the security of the client applications. The webinar provides an overview of security and privacy issues with popular videoconferencing clients and services and shows how to address them. **Recording:** https://www.youtube.com/watch?v=Fjq046cSCRc&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=9 **Slides:** https://learning.geant.org/wp-content/uploads/Videoconferencing-over-of-the-best-pracrtices-for-Security-and-Privacy.pdf
Office Suites – understanding privacy and security risks	Many people regularly use programs such as MS Office. Having started as simple text-editing programs, modern Office suites have turned into highly complex applications. They are available on every operating system, including mobile OSs, and are quickly evolving into cloud-based applications, allowing convenient collaboration. However, the growing complexity of these programs has introduced a number of problems related to both privacy and security. The talk gives participants an insight into common privacy issues and security risks and provides some practical tips to address them. **Recording:** https://www.youtube.com/watch?v=xJZ87mIEaH4&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=11

Session	Content
	Slides: https://security.geant.org/wp-content/uploads/2021/11/Office-1.2_PUBLIC.pdf

Table 2.2: Submodule 2 – Client Privacy & Security

3rd Submodule: Domain Name System (DNS) Protection

The Domain Name System (DNS) is one of the oldest protocols of the internet. It has proved to be capable of scaling with the tremendous growth of the internet and also of being adaptable to a variety of new applications, several of them relevant to the security of today's networks. Being a protocol from days when the internet was much smaller and thought to be safe, it has to cope with its own inherent security problems.

The module starts with an introduction to DNS, which outlines the basic security problems surrounding its operation. The following sessions deal with using the Domain Name System for network defence, like blackholing malicious domains and logging queries to infer intruder activity on the own network. The later sessions address the inherent security problems of DNS, starting with integrity protection through Domain Name System Security Extensions (DNSSEC) and concluding the course with a module on privacy protection through DNS over TLS (DoT) and DNS over HTTP (DoH).

Delivered on: 30 November – 10 December 2020

Number of attendees by session: Introduction to DNS: 99; DNS for Network Defence: 92; DNSSEC: 63; DNS Privacy Protocols: 67

Developed course material: https://security.geant.org/training/

Session	Content
Introduction to DNS and its Security Challenges – meet the problems	The Domain Name System (DNS) is one of the core services of the internet as we know it today. DNS was designed in 1983 and has been a critical part of the internet infrastructure ever since. This session give an overview of how DNS works and, crucially, what the security implications of its design and operation are. **Recording:** https://www.youtube.com/watch?v=fihRx1KcKCI&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=12 **Slides:** https://learning.geant.org/wp-content/uploads/Introduction_to_DNS_and_its_Security_Problems.pdf
DNS for Network Defence – using DNS to protect and observe	DNS is not only used for the mapping of names to IP addresses and vice versa. This session shows several use cases using information provided by DNS servers that can be used to protect the local network from malicious activities, such as SPAM or drive-by infections. This is followed by a block on monitoring DNS queries to collect information about ongoing intruder activity on an organisation's network. **Recording:** https://www.youtube.com/watch?v=VeS1krFdYG8&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=13

Session	Content
	Slides: https://learning.geant.org/wp-content/uploads/DNS_Net_Defense.pdf
DNSSEC – protecting the integrity of the Domain Naming System	Although hampered by slow adoption, DNSSEC has proved to deal effectively with the integrity problems of DNS. This module introduces the general concepts of DNSSEC and provides a practical example by implementing DNSSEC in a local zone. **Recording:** https://www.youtube.com/watch?v=dEQitN76vvo&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=14 **Slides:** https://learning.geant.org/wp-content/uploads/DNSSEC.pdf
DNS Privacy Protocols – encrypted DNS queries for privacy protection	With the integrity of DNS taken care of by DNSSEC, inspection of DNS query data has been used by various actors on the internet for both good and bad purposes. DNS over TLS (DoT) and DNS over HTTPS (DoH) have been created as ways to mitigate the latter, while unfortunately also interfering with the former. The session gives insights into the workings and configuration of DoT and DoH and explains the trade-offs organisations' network administrators have to make between security and privacy, as well as showing how some of these can be dealt with. **Recording:** https://www.youtube.com/watch?v=PhQ-Fe2niOo&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=15 **Slides:** https://learning.geant.org/wp-content/uploads/DNS-Privacy-protocols.pdf

Table 2.3: Submodule 3 – Domain Name System (DNS) Protection

4th Submodule: Distributed Denial of Service (DDoS) Protection

Distributed Denial of Service (DDoS) attacks have been the scourge of the internet over the past 20 years. Although the media attention has waned, they continue to evolve and grow in power, with botnet clients becoming easier to deploy and ever more services being exploited as multipliers for packet floods.

This module takes the participants from an overview of DDoS through details of the most common attacks and concludes with ways to detect and mitigate them.

Delivered on: 8–17 February 2021

Number of attendees by session: Introduction to DDoS Attacks: 165; Details of selected DDoS Attacks: 117; DDoS Detection: 118; DDoS Mitigation 114

Developed course material: https://security.geant.org/training/

Session	Content
Introduction to DDoS Attacks – an overview of motivation and	DDoS attacks have been around for more than 20 years now, and over this time, they have gained in power, now reaching several terabits in bandwidth, enough to knock ISPs offline. While the actual DDoS attacks

Session	Content
modus operandi of attackers	have changed very little, the orchestration of the attacks, the deployment of their components and the motives of attackers have evolved. The session give participants an overview of the attacks, the attackers, and their motivation and modus operandi. **Recording:** https://www.youtube.com/watch?v=iUOS9Io1pcU&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=16 **Slides:** https://learning.geant.org/wp-content/uploads/2021-02-08-Introduction_to_DDoS.pdf
Details of Selected DDoS Attacks – how the attacks work from a technical perspective	While DDoS attacks have become more powerful and easier to start for attackers, the technical details of DDoS attacks have been remarkably consistent over the last 20 years. This session provides participants with an in-depth view of the technical details of the most common DDoS mechanisms: amplification and reflection, and the services being exploited for them. **Recording:** https://youtu.be/z5Ig_9MviHU **Slides:** https://learning.geant.org/wp-content/uploads/DDoS-Attack-Details.pdf
DDoS Detection – how to know if you are under attack or partaking in an attack	DDoS detection may sound simple in theory, i.e., when you cannot access your systems, that means you're under attack. However, this may also happen due to technical problems or misconfigurations. And what if we want to detect attacks before falling victim to them? The session shows participants the various ways in which DDoS attacks are detected on the internet. **Recording:** https://youtu.be/uGSilJIHrUI **Slides:** https://security.geant.org/wp-content/uploads/2021/11/DDoS-Detection.pdf
DDoS Mitigation – what you can do against attacks	Mitigating a DDoS attack, especially a large-scale one, can seem like a daunting task, especially where there is a determined attacker and when several sites are affected. The session shows some simple but proven techniques to combat DDoS attacks as well as to avoid unintentionally partaking in one. **Recording:** https://www.youtube.com/watch?v=FcV9wax6Ugo&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=18 **Slides:** https://learning.geant.org/wp-content/uploads/2021-02-17-DDoS_Mitigation.pdf

Table 2.4: Submodule 4 – Distributed Denial of Service (DDoS) Protection

3 Vulnerability Management Course Structure and Content

This section summarises the structure and content of the Vulnerability Management course. As before, for each submodule, an overview, the delivery date, number of attendees by session and a link to the course material are given, and, for each session, a description and links to the recording and slides. The overview and session descriptions are also used for the GÉANT Learning and Development (GLAD) and Security Training pages [GLAD_VM], [Security_Training].

1st Submodule: Vulnerability Management Process & Standards

Vulnerabilities, in software and sometimes even in hardware, are open gates that attackers can utilise to gain access to private systems and networks. Worse, they have become a fact that IT managers and administrators have to deal with, ever accompanied by the concern that a single critical vulnerability has been overlooked which will later be exploited. Vulnerability management addresses this problem with a systematic approach to make this a reliable and reoccurring process. This module gives an overview of standards, details how to distribute security advisories among a constituency and how to plan a rollout of patches in your organisation.

Delivered on: 27 May – 10 June 2021

Number of attendees by session: Vulnerability Management: 65; Vulnerability Information: 53; Patch Management: 59

Developed course material: https://security.geant.org/training/

Session	Content
Vulnerability Management – introduction to processes and standards	The task of dealing with vulnerabilities in software, and sometimes even in hardware, has gone from an ad hoc, emergency activity to a continuous, planned task that has become one of the building blocks of reliable, secure systems and networks. This webinar gives an overview of the existing standards and covers in depth some of the key elements, such as CVE and CVSS, that will be referenced throughout the whole course on vulnerability management. **Recording:** https://www.youtube.com/watch?v=egQb8wEqODs&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=19 **Slides:** https://learning.geant.org/wp-content/u ploads/Vulnerability-Mgmt_Process.pdf

Session	Content
Vulnerability Information – how to gather and distribute security advisories to your constituency	Before one can address vulnerabilities, one needs to be aware of them: their existence, their consequences, and what to do about them. While CSIRTs and PSIRTs take care of the initial steps in researching and publishing information, the task of actually forwarding this information to the administrators responsible for vulnerable systems is something that every organisation has to deal with themselves. This webinar shows how this task can be dealt with and what information should be included in a security advisory. **Recording:** https://youtu.be/1gHquMV9_Fk **Slides:** https://learning.geant.org/wp-content/uploads/Disseminating_Vulnerability_Info.pdf
Patch Management – how to roll out and track security fixes to your systems	Patching is the name given to the process of replacing vulnerable software with a corrected version. However, the sheer number of patches that have to be applied constantly has led to the requirement to automate and track the application of patches. This webinar gives an overview of the process of applying patches and what tools can be used to automate the task. **Recording:** https://youtu.be/EJk-3vwlDs8 **Slides:** https://learning.geant.org/wp-content/uploads/Patch_Management.pdf

Table 3.5: Submodule 1 – Vulnerability Management Process & Standards

2nd Submodule: Finding Vulnerabilities I – Looking into Networks

Scanning for vulnerabilities in your organisation's network is considered one of the key aspects of vulnerability management. In this three-webinar submodule, different scanning and testing approaches are covered. From scanning the system inside out or from the outside in to simulating actual attacks (pentesting), the attendees are taken through the introductory steps of conducting and supervising scans and pentests.

Delivered on: 28 June – 13 September 2021

Number of attendees by session: Looking into the Network: 57; Network Vulnerability Scanning: 55; Penetration Tests (postponed session): 29

Developed course material: https://security.geant.org/training/

Session	Content
Looking into the Network – how to scan local systems for vulnerabilities and misconfigurations	Today's systems are so complex that it's almost impossible to run a system without vulnerabilities and misconfigurations. And although there are plenty of benchmarks, baselines, and hardening guides available, it is difficult to apply them to the local environment. This webinar introduces some of the most useful frameworks and tools for local vulnerability scanning. **Recording:** https://www.youtube.com/watch?v=XwDLv6_OO_I **Slides:** https://learning.geant.org/wp-content/uploads/VulnMgmt-Local_Vuln_Scanning-1.1_PUBLIC.pdf

Session	Content
Network Vulnerability Scanning – looking from afar	In order to stay ahead of the threats to a large infrastructure, it is crucial to maintain a clear picture of whether there are vulnerabilities in the components deployed and, if so, which ones. Scanning systems through the network is one way of gaining insight into this issue. This webinar provides an introduction to the concepts of network scanning, its benefits, and its drawbacks, as well as offering some practical examples. **Recording:** https://youtu.be/KECo-nUcPUQ **Slides:** https://learning.geant.org/wp-content/uploads/2021-06-30-Network_Vulnerability_Scanning.pdf
Penetration Tests – how does your network stand up against real attacks?	No matter how much scanning for vulnerabilities and security process evaluation is done, one question remains: Is this really enough against real attacks? Short of experiencing an attack in real life, penetration tests try to answer this question by conducting attacks in a controlled manner. This webinar gives managers and administrators an introduction to the standards and workflow of penetration tests to help in planning and supervising penetration tests carried out on their networks. **Recording:** https://www.youtube.com/watch?v=ZjS-fn2RctE&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=27 **Slides:** https://security.geant.org/wp-content/uploads/2021/11/Pentest-1.pdf

Table 3.6: Submodule 2 – Finding Vulnerabilities I – Looking into Networks

3rd Submodule: Finding Vulnerabilities II – Looking into Code

Looking for vulnerabilities in existing systems and services has become a common practice. However, vulnerability scanning covers only software packages from established sources and only those vulnerabilities that are already known. But what about vulnerabilities you do not know about yet? What about software that is developed in-house? This submodule gives an introduction to the topics of code audits and vulnerability disclosure, two main aspects of vulnerability management for software that you are responsible for. It concludes with an introduction to breach and attack simulation, a relatively new approach to assessing the risks and consequences of existing vulnerabilities in your network.

Delivered on: 14 July – 15 September 2021

Number of attendees by session: Code Audits: 39; Vulnerability Disclosure: 34; Breach and Attack Simulation (postponed session): 29

Developed course material: https://security.geant.org/training/

Session	Content
Code Audits – how to increase the quality of the code	Software without bugs or vulnerabilities does not exist. If your organisation runs software development teams, they will likely have heard of things like secure software development lifecycles and the like.

Session	Content
	This webinar introduces some basic concepts as well as tools that help developers finding bugs before the software goes into production. **Recording:** https://www.youtube.com/watch?v=EvmWRg7zOpQ&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=25 **Slides:** https://security.geant.org/wp-content/uploads/2021/11/VulnMgmt-Code_Audits-1.1_PUBLIC.pdf
Vulnerability Disclosure – letting the cat out of the bag	So you have found vulnerabilities in other people's code. Or other people have found vulnerabilities in your code. Either way, the question is: How to handle the situation? In the long run, trying to keep information about the vulnerability under wraps is unlikely to work, so this session covers some aspects and strategies of how to approach this issue. **Recording:** https://www.youtube.com/watch?v=8MWXRIV1mCM&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=26 **Slides:** https://security.geant.org/wp-content/uploads/2021/11/2021-07-16-Vulnerability_Disclosure.pdf
Breach and Attack Simulation – matching attacker behaviour with vulnerabilities	Breach and Attack Simulation (BAS) is a relatively new approach to vulnerability assessment that goes beyond simple scoring of vulnerabilities by also taking the modus operandi of adversaries into account. This webinar gives an introduction to the topic and presents some open source tools to do BAS. **Recording:** https://www.youtube.com/watch?v=bxSJEHKKkeY&list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6&index=27 **Slides:** https://security.geant.org/wp-content/uploads/2021/11/Breach_Attack_Sim-1.pdf

Table 3.7: Submodule 3 – Finding Vulnerabilities II – Looking into Code

4 Review Outcome

A number of surveys were created to gather feedback from the course attendees; details of the survey questions and the results are provided in Appendix A. Overall, the feedback was very positive. Attendees considered the training material to be up to date in most parts, and that their objectives in attending a session were usually met or at least partially met. The attendees who answered the survey would recommend the trainings to their colleagues and will likely use the knowledge acquired from the trainings for their job.

Most of the attendees work as network or system administrators, which is the group at which the trainings are aimed. The second-largest group of attendees are those who work in some kind of security-related position, for example as information security officers (ISOs) or security engineers. Most attendees were experienced or had some experience in their role; some were very experienced, while the smallest group covered those who were new to their role.

Attendees commented positively on the fact that all prepared material is available for download. (This feedback was gathered during the sessions, not as part of a survey.) Some expressed their happiness about the online training format: it enables them to participate in the trainings, as they would not be able to make business trips to join on-site events. They also expressed the hope that even if the restrictions on business travel due to the COVID-19 pandemic are lifted, any upcoming courses will be delivered as online trainings, at least in addition to on-site delivery.

Nevertheless, some areas where there might be room for improvement were also noted.

In accordance with the recommendations of the GLAD team, almost all sessions were planned to not extend beyond one hour, including the time allocated for the attendees to ask questions. This concept, together with the strategy of delivering the training sessions for one submodule within one or two weeks, seemed to work for most (see for example the Domain Name System (DNS) Protection survey, Appendix A), but there were also some notes that a deeper dive into some topics would be appreciated. Without further analysis and feedback, and due to the low number of statements in this regard, it is not possible to define a specific “in-depth” training, but some kind of training for experts might be considered as required.

As part of the surveys for the first submodule (Operating System Privacy & Security) of the first training course (Operational Network Security), attendees had the opportunity to rate the presenter’s presentation skills. No feedback noting any specific need for improvement was given, but one useful suggestion provided was for the presenters to view their own recordings and find aspects that could be optimised.

As part of one of the surveys (see Domain Name System (DNS) Protection survey, Appendix A), an evaluation was carried out to assess whether the format of the training could be changed to a collaborative format by setting up a “round table” or an “open forum” to dive into specific topics together with the attendees. However, these suggestions received little or no agreement and most attendees would prefer to proceed with the current training session setup.

The number of attendees for the second training course (Vulnerability Management) was significantly lower than for the first one. The reasons for that are unknown. Some possible explanations are:

- When the first training course began, the pandemic situation was relatively new and most organisations had just started to switch to online delivery formats for trainings, conferences and meetings, whereas at the very beginning of the pandemic such events were often simply cancelled. When the second course started, the online mode was already commonly used, and hence the second course lacked some of the shiny new glamour of the first one.

- It is possible that the second training course was of less interest or relevance than the first one. In the case of the German NREN, DFN, for example, the advisory service, which is an important part of vulnerability management for the member organisations, is well established (in place for more than 20 years) and as a lot of attendees for the first training course were from Germany, this might partly explain the lower numbers.

- It also seems that the announcement and promotion of the second course was not as good as for the first one. Therefore, it was decided to invest more time on promotional activities for the third course, IT Forensics for System Administrators (see Section 7 The Road Ahead). However, the lower number of attendees is accompanied by a lower number of completed surveys, therefore the results of the survey with respect to how attendees were notified about the training and whether any improvements could be made in this regard do not strongly indicate any specific action.

5 Recommendations

Based on the feedback received, the general concept for the training seems to be working well and should not be significantly modified for the upcoming training modules. Nevertheless, some areas for improvement have been identified.

For example, some kind of “opening out” of a session would be useful. Given that the demo in the Operating System Privacy & Security File Integrity Monitoring (FIM) session was positively received, demonstrations should be run in a session where possible. To encourage attendees to provide feedback to make the trainings more collaborative, and also to make the surveys easier to complete, additional tools (for example, Mentimeter and Poll in Zoom) should be evaluated.

Some attendees expressed the desire to know the agenda prior to the sessions (see Domain Name System (DNS) Protection survey, Appendix A). Although the “teaser” in the online announcement, promotional and registration information provides a rough overview of the content of the sessions, distributing the detailed agenda by email prior to trainings should be considered. However, as registration is per submodule or module and not per session, to avoid sending too many emails, the teaser and the agenda only could be distributed together with the information on joining a session.

Looking at the attendees per country, it seems that the training is particularly well-received in Germany and the Netherlands. Of course, the size of the target community varies by country, but it is also possible that the promotion of the training is better in these two countries than in others.

The fact that the majority of the attendees are experienced (to varying levels) might indicate that the information about the trainings is not received by people who are new in their role or that their needs are not adequately addressed. While attendees are expected to have some administration knowhow, the trainings are not specifically designed for senior administrators. The promotion for the training should therefore avoid giving the impression that senior-level administration knowledge is required in order to benefit from the training. In addition, it should be evaluated whether it is possible to announce the trainings to a broader community than was the case for the first two training courses, thereby possibly reaching more people who are new in their role. The broader communication should include the acceptance of attendees outside of NRENs or NREN member organisations, as a broad, well-educated community is a benefit for every user with legitimate interests and, due to the online format, opening up the trainings to a broader community involves no extra costs (see also Section 7 The Road Ahead).

6 Further Use of the Courses

All sessions have been recorded and are available online [YouTube_Recs], but viewing numbers are not very high. The graph of viewings (see Appendix B) indicates that the recordings are usually used in the same timeframe in which the sessions were delivered or at least in which some training sessions were delivered (the link to the YouTube page is often circulated via chat within a training session).

All the recordings are available on one YouTube page. However, the recordings do not easily or clearly show a course structure and the blog articles, which were used to promote the upcoming training modules and encourage people to register, are not optimised to allow someone who missed the online training to complete the course on their own.

A new training page was therefore designed [Security_Training] (publicly accessible since November 2021), where all training sessions are listed in course order, referencing the developed material and recordings. A similar page had already been created for the German NREN, DFN [DFN-CERT_SecTrng], and went live at the end of October 2021, and might be responsible for the small peaks of viewings at the end of October, early November 2021 (see Appendix B).

For all the advantages of making the recordings available, viewing a recording is nonetheless different from attending a live session, as:

- It is possible to ask questions at the end of a live session.
- Even if they do not see all of the other attendees, participants are aware that they are there and are available through the chat, so the live session feels like an “event”.
- Some attendees want a certificate of attendance, which is not available when using the recordings.
- Some promotion for the live sessions is not available for the recordings.

Given the findings mentioned above, it might be possible to repeat the live sessions at some point in the future, slightly adapted based on the feedback, and taking new tools and trends into account.

Once the restrictions due to the COVID-19 pandemic are over, it might also be an option to offer on-site trainings using the material already developed, as some (although not the majority) of the attendees indicated a demand for it (see Domain Name System (DNS) Protection survey, Appendix A). One option would be to host a training at a given location and accept attendees from different organisations, while another would be to organise a dedicated training for an NREN and its member organisations on-site. Further assessment needs to be carried out to decide which of these is the best option. The above-mentioned training page of the German NREN includes the option to contact GLAD if there is a need for an on-site training; as at mid-November 2021, no requests have been received.

7 The Road Ahead: IT Forensics for System Administrators

Since August 2021 the development of the third training course, IT Forensics for System Administrators, has been underway. As some restrictions due to the COVID-19 pandemic are still in force at the time of writing, and because of the positive feedback from the attendees of the previous courses, the course will be delivered as online training.

On 23 November 2021 the first of (currently) eight defined training sessions was delivered. During the remaining 2021 sessions a survey will be conducted to understand the area(s) of special interest regarding the demonstration of forensic tools, to define additional training sessions according to the gathered feedback.

Training Course: IT Forensics for System Administrators

IT forensics have become a vital part of handling security incidents, and while putting the evidence together is a job for specifically trained investigators, administrators will often be left alone with the detection of incidents, initiating an investigation and aiding investigators in the collection of required evidence. Unfortunately, many administrators are not trained in their role in a forensic investigation and have not received the necessary guidance before they are thrown in at the deep end.

This training course addresses these shortcomings with an introduction to the basic organisational steps of incident handling and forensics from the system administrator's perspective, as well as covering how to ascertain that all incidents have been detected and uncovered. Methods and tools to collect the various forms of evidence data are explained so that administrators are enabled to fulfil their role in forensic investigations.

Delivery planned: 23 November 2021 – 27 January 2022

Session	Content
Organisation	Dealing with the organisational aspects of incident handling and forensics may sound like dry paperwork far removed from the technical details of day-to-day sysadmin tasks. However, organisational preparation can help tremendously in the course of an investigation. For example, answering simple practical questions such as "Who's in charge?" or "What are we looking for?" – even "Why are we doing this?" This session introduces attendees to the basic steps of incident handling and forensic investigations, and to the principles of forensic investigations that should be adhered to for an investigation to succeed.

Session	Content
From Suspicion to Detection I and II	Someone notices “unusual system behaviour” or “suspicious network traffic” that raises the question of what to do about it. The first step in incident response is usually to ascertain whether or not the activity observed really is an incident. While there is no formal process or definition for doing so, there are many locations where possible indicators may be looked for that may eventually make an incident. Participants learn which first steps to take after a compromise has been detected.
Memory Acquisition I	Whatever the malware is doing on a computer, the code to carry out its activity has to be in the random access memory (RAM). And not only this, lots of other interesting stuff is present there, too: IP addresses of computers the malware has been communicating with, data from attacks against other systems or even exfiltrated data. By getting information directly from the storage, compromised operating system components can be bypassed. No wonder that investigating transient memory has become a hot topic in IT forensics over the last decade. Before memory contents can be scrutinised, they will have to be acquired from the computer. This webinar covers the basic principles and techniques behind memory acquisition on Linux, Windows and MacOS operating systems.
Memory Acquisition II	The previous webinar covered the basic, agnostic technique of acquiring memory through the use of kernel drivers and copying tools. However, this technique requires access to the operating system with root or administrator privileges. This webinar covers advanced techniques that will remove some of these preconditions and may in some cases be better suited for doing the job of memory acquisition.
Persistent Storage Acquisition I	If any data on a computer is to outlast a power switch or a reboot, it has to be written to persistent storage. Even cloud storage is only persistent storage on another computer. Investigating the contents of hard disks, SSDs and transportable media has been a standard operating procedure of IT forensics since the ’90s and remains so. Before storage contents can be scrutinised, they will have to be acquired from the suspect computer. This webinar covers the basic principles and techniques behind persistent storage acquisition on Linux, Windows and MacOS operating systems.
Persistent Storage Acquisition II	The previous webinar covered the basic, agnostic technique of acquiring persistent storage with raw device access and standard copying tools. However, this technique requires access to the operating system with root or administrator privileges. This webinar covers advanced techniques that will do away with some of these preconditions and might be better suited for the job in some situations.
Acquisition of Other Evidence	Are there more indicators of compromise than the contents of RAM and hard disks? Yes, of course. And it may be vital stuff that is either lost on the suspect systems due to adversary activity or was not there to begin with. One example is represented by crucial log messages that are now only present on a central loghost. Another example would be network traffic

Session	Content
	information from switches, firewalls or network IDSs that may corroborate leads that would otherwise be vague or circumstantial. This webinar introduces some of the more common forms of indicators not present on local systems and how or where to obtain them.

Table 7.8: IT Forensics for System Administrators

The training course will be extended with additional sessions to demonstrate and explain one or more commonly used tools for IT forensics such as Volatility or Autopsy, depending on the feedback from the attendees of the early sessions.

As the review of the former courses indicates, it was difficult to reach people who are new to their job. One theory is that people new to their job in the GÉANT community are not fully included in the GÉANT communication channels. Hence, it was decided to distribute the training invitations more widely, utilising, among others, existing CERT communication channels. This decision was accompanied by accepting people outside NRENs and NREN member organisations as attendees, as security is a common issue and educating people outside the GÉANT community will improve the security for the GÉANT community also.

8 Conclusions

The two new training courses, Operational Network Security and Vulnerability Management, developed to help address the security training gaps identified in Deliverable D8.1 [D8.1], were well received and have got positive feedback. At the time of writing, more than 700 people have registered for the third training course, IT Forensics for System Administrators. The training task within GN4-3 WP8 Task 1 may therefore be considered to be well on its way to accomplishing its mission to close the security training gaps identified in D8.1.

In accordance with the feedback, recommendations and the suggestions about the further use of the developed training material earlier in this document, and considering the evolving security – and, unfortunately, also malware – techniques and tools, security trainings need to be continuously adapted, even if most of the basic risks and protection mechanisms remain the same over the years, while the use of the videos (see Appendix B) suggests that the trainings need to be "live" to be of value. Continuing the training task within the upcoming GN5 project should therefore be considered. This will allow the developed training material to be kept up to date, and more "live" virtual trainings to be offered for people who missed the original training sessions. It will also allow group-specific courses to be offered, that is, on-site trainings based on the developed training material but adapted to the special needs of the group to be trained. In addition, continuing the training task in GN5 will allow more gaps to be closed: it will enable another survey or round of interviews to be conducted, both to verify that the training gaps already identified still exist and to discover any new ones, and for more trainings to be developed, delivered and made available accordingly.

Appendix A Surveys and Results

A number of surveys were created to gather feedback from the course attendees. Initially, for Submodule 1 of the first training course, a survey was run after each session. However, this was soon found to be too detailed and time-consuming, so for the next submodules and for the second training course, attendees were asked to provide feedback via a single survey for all the sessions they attended within each submodule.

The tables below provide details of the numbers of session attendees by country, and survey questions and responses, where:

- The most frequent answers are marked in **green** – comments are marked in the same colour.
- The second most frequent answers are marked in **dark yellow**.
- The number of answers is added in (brackets).

A.1 Operational Network Security Course

Attendees & Survey: Operating System Privacy and Security – Operating System Telemetry

Number of attendees: 91; **Completed surveys:** 14

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Armenia	1	Australia		Austria	
Belgium		Croatia	1	Cyprus	
Czechia		Estonia	2	Finland	2
France		Germany	52	Hungary	1
Iceland		Ireland	1	Israel	
Italy	1	Lithuania	8	Luxembourg	1
N/A	4	Netherlands	1	Poland	2
Portugal	3	Republic of North Macedonia	1	Slovenia	2
South Africa		Spain	4	Switzerland	
Turkey	3	Ukraine	1		

Table A.1: Operating System Privacy and Security – Operating System Telemetry session: attendees

No.	Question	Answer option
1	Please state your job role, i.e. are you working as a network/system administrator or in any other capacity?	Open-Ended Response Network administrator (7) System administrator (5)
2	Please let us know how you would rate your current experience regarding system and/or network administration or any other field if you mentioned it above.	- Very experienced - Experienced (8) - I have some experience (3) - I am new to it
3	In your opinion – do you think the training content is up to date?	- Yes, absolutely (14) - Yes, in most parts - No
4	Please add some further comments here.	Open-Ended Response One interesting note: "only scratched the surface"
5	In your opinion – were your objectives to attend the session met?	- Yes (14) - Partially - No - Other (please specify)
6	How likely is it that you will use the knowledge, skills and reference materials gained from this training in your work?	- Very likely (3) - Likely (9) - Unlikely - Other (please specify)
7	Would you recommend this training to your colleagues?	- Yes (13) - No
8	Any additional comments	Open-Ended Response
9	How would you describe your experience of attending this training session? Please mark all that are applicable.	- Helpful (12) - Engaging (5) - Interesting (11) - Relevant (8) - Valuable (7) - Enjoyable (4) - Dull and boring (0) - Confusing (0) - Not relevant (0) - Frustrating (0) - Disappointing (0) - Unhelpful (0) - Other (please specify) (0)
10	With reference to your trainer(s), how would you rate the following aspects: - Preparation and organisation (Excellent: 5, Good:4)	- Excellent - Good - Fair

No.	Question	Answer option
	- Subject matter knowledge (Excellent: 6) - Presentation skills (Excellent: 2, Good:4) - Ability to understand and answer questions (Excellent: 3, Good: 1) - Other (please specify) Note: Some attendees reported problems with the radio box.	- Poor
11	How would you rate this training session as a whole?	- Very Good (10) - Good (4) - Fair - Poor - Other (please specify)
12	Would you like to attend more training sessions in a similar (live online) format in the area of operational network security?	- Yes (14) - No - Other (please specify)
13	Do you have any suggestions for improvement?	Open-Ended Response

Table A.2: Operating System Privacy and Security – Operating System Telemetry session: survey responses

Attendees & Survey: Operating System Privacy and Security – Logging and Audit

Number of attendees: 131; **Completed surveys:** 28

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Armenia	1	Australia		Austria	2
Belgium	1	Croatia	3	Cyprus	2
Czechia	5	Estonia	2	Finland	3
France	1	Germany	61	Hungary	1
Iceland	1	Ireland	1	Israel	
Italy	1	Lithuania	6	Luxembourg	
N/A	6	Netherlands	2	Poland	4
Portugal	6	Republic of North Macedonia	1	Slovenia	6
South Africa	1	Spain	10	Switzerland	1
Turkey	3	Ukraine			

Table A.3: Operating System Privacy and Security – Logging and Audit session: attendees

No.	Question	Answer option
1	Please state if you are working in IT Operations.	Yes (21) No (8)

No.	Question	Answer option
2	If you are working in IT Operations, can you give us a rough estimation about the number of server systems your department is responsible for?	- less than 50 (9) - 50-200 (3) - more than 200 (7)
3	If you are working in IT Operations – how many of these systems that you are aware of have implemented log strategy? (percentage)	- up to 25% (8) - 26-50% (4) - 51-75% (1) - more than 75% (6)
4	In your opinion – were your objectives in attending the session met?	- Yes (20) - Partially (9) - No (0) - Other (please specify) (0)
5	Are there any other subjects you would like to be added to this session?	- No (3) - Useful/Not useful visualisation examples - Key Performance Indicators from Logs - focus on logs for security issues - focus on open source - Where and how to start - Real-world example of “start really small” - Windows logs centralisation - Best practices in architectural design
6	Do you think that the references and additional information provided will be of immediate use to you?	- Yes (24) - No (3)
7	Would you recommend this training to your colleagues?	- Yes (27) - No (0)
8	How would you describe your experience of attending this training session. Please mark all that are applicable.	- Helpful (19) - Engaging (12) - Interesting (25) - Relevant (17) - Valuable (15) - Enjoyable (6) - Dull and boring (0) - Confusing (0) - Not relevant (0) - Frustrating (0) - Disappointing (0) - Unhelpful (0) - Other (please specify) (too short)

No.	Question	Answer option
9	With reference to your trainer(s), how would you rate the following aspects: - Preparation and organisation (Excellent: 18, Good: 9) - Subject matter knowledge (Excellent: 22, Good: 5) - Presentation skills (Excellent: 18, Good: 7, Fair: 1) - Ability to understand and answer questions (Excellent: 18, Good: 6) - Other (please specify)	- Excellent - Good - Fair - Poor
10	How would you rate this training session as a whole?	- Very Good (21) - Good (6) - Fair - Poor - Other (please specify)
11	Do you have any suggestions for improvement?	Open-Ended Response

Table A.4: Operating System Privacy and Security – Logging and Audit session: survey responses

Attendees & Survey: Operating System Privacy and Security – File Integrity Monitoring (FIM) for detecting security incidents

Number of attendees: 113; **Completed surveys:** 17

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Armenia	1	Australia		Austria	2
Belgium		Croatia	3	Cyprus	2
Czechia	1	Estonia	1	Finland	3
France	1	Germany	52	Hungary	1
Iceland		Ireland	1	Israel	
Italy	2	Lithuania	6	Luxembourg	
N/A	5	Netherlands	2	Poland	4
Portugal	5	Republic of North Macedonia	1	Slovenia	4
South Africa	4	Spain	8	Switzerland	1
Turkey	3	Ukraine			

Table A.5: Operating System Privacy and Security – File Integrity Monitoring (FIM) for detecting security incidents session: attendees

No.	Question	Answer option
1	How important is the detection of security incidents in your daily work?	- Very Important (10) - Important (4) - Less Important (3) - Not relevant (0)
2	How likely is it that you will use the knowledge, skills and reference materials gained through this training in your work?	- Very likely (11) - Likely (6) - Unlikely - Other (please specify)
3	What was the most useful part of this training?	Open-Ended Response: - Demo (10) - the knowledge of new tools and the usage of them - The presenter's suggestions from hands-on experience. - Getting a good overview of this area - All of it
4	In your opinion - were your objectives to attend the session met?	- Yes (16) - Partially (1) - No (0) - Other (please specify) (0)
5	Any additional comments	Open-Ended Response: - Maybe also the Windows agent view to complete the picture. Hints for detecting Emotet or other current malware - Even more practical examples for FIM would be very interesting. Maybe define a standard in the DFN realm that can be used "as a default/starting-point" so that not everybody has to start from scratch.
6	How would you rate this training session as a whole?	- Very Good (14) - Good (3) - Fair - Poor - Other (please specify)

Table A.6: Operating System Privacy and Security – File Integrity Monitoring (FIM) for detecting security incidents session: survey results

Attendees & Survey: Operating System Privacy and Security – Network First Hop Security

Number of attendees: 126; **Completed surveys:** 19

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Armenia	3	Australia		Austria	2
Belgium		Croatia	5	Cyprus	1
Czechia	2	Estonia	2	Finland	3
France		Germany	54	Hungary	2
Iceland	1	Ireland	2	Israel	1
Italy	1	Lithuania	7	Luxembourg	1
N/A	5	Netherlands	3	Poland	2
Portugal	5	Republic of North Macedonia	1	Slovenia	5
South Africa	1	Spain	10	Switzerland	1
Turkey	6	Ukraine			

Table A.7: Operating System Privacy and Security – Network First Hop Security session: attendees

No.	Question	Answer option
1	Please state your job role, i.e. are you working as a network/system administrator or in any other capacity?	Open-Ended Response Network specialist/administrator (10) System administrator (2) Service Desk Specialist (2)
2	Please let us know how you would rate your current experience regarding system and/or network administration or any other field if you mentioned it above.	- Very experienced (2) - Experienced (7) - I have some experience (9) - I am new to it (1)
3	In your opinion – do you think the training content is up to date?	- Yes, absolutely (17) - Yes, in most parts (2) - No
4	In your opinion – were your objectives in attending the session met?	- Yes (18) - Partially (1) - No - Other (please specify)
5	How likely is it that you will use the knowledge, skills and reference materials gained through this training in your work?	- Very likely (9) - Likely (9) - Unlikely - Other (please specify)

No.	Question	Answer option
		→ I am already using most of the content (1)
6	Would you recommend this training to your colleagues?	- Yes (19) - No
7	Any additional comments	Open-Ended Response
8	How would you describe your experience of attending this training session? Please mark all that are applicable.	- Helpful (16) - Engaging (7) - Interesting (12) - Relevant (14) - Valuable (12) - Enjoyable (7) - Dull and boring (0) - Confusing (0) - Not relevant (0) - Frustrating (0) - Disappointing (0) - Unhelpful (0) - Other (please specify) (0)
9	How would you rate this training session as a whole?	- Very Good (14) - Good (5) - Fair - Poor - Other (please specify)
10	Do you have any suggestions for improvement?	Open-Ended Response

Table A.8: Operating System Privacy and Security – Network First Hop Security session: survey results

Attendees & Survey: Operating System Privacy and Security – Authentication Methods – how to avoid common pitfalls

Number of attendees: 110; **Completed surveys:** 9

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Armenia	2	Australia		Austria	
Belgium	1	Croatia	3	Cyprus	2
Czechia	1	Estonia	1	Finland	3
France	2	Germany	53	Hungary	2
Iceland		Ireland	1	Israel	
Italy	2	Lithuania	5	Luxembourg	
N/A	5	Netherlands	5	Poland	2

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Portugal	4	Republic of North Macedonia	1	Slovenia	1
South Africa	3	Spain	7	Switzerland	1
Turkey	3	Ukraine			

Table A.9: Operating System Privacy and Security – Authentication Methods session: attendees

No.	Question	Answer option
1	How many years of IT experience do you have?	Open-Ended Response >= 10 (7) <= 9 (2)
2	Regarding the password policy recommendations: Are they in accordance with your company strategy?	- Yes (7) - Almost (2) - No (1)
3	In your opinion – do you think the training content is up to date?	- Yes, absolutely (6) - Yes, in most parts (3) - No
4	Please add some further comments here.	Open-Ended Response - More on recent developments regarding TAN authentication codes - I think including some references to password-less (Windows Hello + FIDO 2) would be great.
5	In your opinion – were your objectives in attending the session met?	- Yes (6) - Partially (2) - No - Other (please specify)
6	With reference to your trainer(s), how would you rate the following aspects: - Preparation and organisation (Excellent: 8, Good: 1) - Subject matter knowledge (Excellent: 8, Good: 1) - Presentation skills (Excellent: 6, Good: 2) - Ability to understand and answer questions (Excellent: 7, Good: 1) - Other (please specify)	- Excellent - Good - Fair - Poor
7	This was the last session in this training module. Did you attend any of the other sessions?	- all sessions (6) - 4 sessions (1) - 2 sessions (2)

No.	Question	Answer option
8	If you attended other sessions – which one did you like the most and why?	- Network 1st Hop Security (3) because of missing experiences
9	Are you planning to attend some of the upcoming trainings?	- Yes (9) - No (0)
10	Can you suggest any changes for future training?	- The schedule is a bit weird for Spaniards, but it's OK since you have to accommodate different time zones and habits. - Maybe on some issues a little bit more detailed information. I understand that it is intended more or less as an "overview", but maybe in the future there is a chance to take a more "practical" approach to some aspects/issues.
11	Would you recommend our recorded sessions and/or the additional training material to your colleagues?	- Yes (9) - No (0)
12	Do you have any suggestions for improvement?	Open-Ended Response

Table A.10: Operating System Privacy and Security – Authentication Methods session: survey results

Attendees & Survey: Client Privacy and Security

Number of attendees by session: Browser: 75; Email: 70; Instant Messaging: 49; Videoconferencing: 55; Office: 50

Completed surveys: 32

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Armenia	7	Australia	1	Austria	
Belgium		Croatia	5	Cyprus	
Czechia		Estonia		Finland	11
France	2	Germany	129	Hungary	
Iceland		Ireland	3	Israel	
Italy	8	Lithuania	13	Luxembourg	11
N/A	30	Netherlands	40	Poland	2
Portugal	4	Republic of North Macedonia	2	Slovenia	1
South Africa	3	Spain	12	Switzerland	2
Turkey	13	Ukraine			

Table A.11: Client Privacy and Security submodule: attendees

No.	Question	Answer option
0	Please indicate which sessions of the "Client privacy and security" series you attended.	- not specified (19) - all (6)
1	Please state your job role, i.e. are you working as a network/system administrator or in any other capacity?	Open-Ended Response Network (/System) administrator (14) Security-related Job, i. e. Information Security Officer (9)
2	Please let us know how you would rate your current experience regarding system and/or network administration or any other field if you mentioned it above.	- Very experienced (5) - Experienced (12) - I have some experience (14) - I am new to it (1)
3	In your opinion – do you think the training content is up to date?	- Yes, absolutely (27) - Yes, in most parts (6) - No
4	In your opinion – were your objectives in attending the session met?	- Yes (30) - Partially (2) - No - Other (please specify)
5	How likely is it that you will use the knowledge, skills and reference materials gained through this training in your work?	- Very likely (13) - Likely (19) - Unlikely - Other (please specify) I am already using most of the content (1)
6	Would you recommend this training to your colleagues?	- Yes (31) - No (1)
7	Any additional comments	Open-Ended Response
8	How would you describe your experience of attending this training session? Please mark all that are applicable.	- Helpful (27) - Engaging (12) - Interesting (22) - Relevant (21) - Valuable (19) - Enjoyable (11) - Dull and boring (0) - Confusing (0) - Not relevant (0) - Frustrating (0) - Disappointing (0) - Unhelpful (0) - Other (please specify) (0)

No.	Question	Answer option
9	With reference to your trainer(s) how would you rate the following aspects: - Preparation and organisation (Excellent: 5, Good: 4) - Subject matter knowledge (Excellent: 6) - Presentation skills (Excellent: 2, Good: 4) - Ability to understand and answer questions (Excellent: 3, Good: 1) - Other (please specify) Note: Some attendees reported problems with the radio box.	- Excellent - Good - Fair - Poor
10	How would you rate this training session as a whole?	- Very Good (24) - Good (9) - Fair - Poor - Other (please specify)
11	Do you have any suggestions for improvement?	Open-Ended Response - Training is rather entry-level; perhaps follow-ups to delve deeper into subject matters. (1)

Table A.12: Client Privacy and Security submodule: survey results

Attendees & Survey: Domain Name System (DNS) Protection

Number of attendees: Introduction to DNS and its Security Challenges – meet the Problems: 99; DNS for Network Defence – using DNS to protect and observe: 92; DNSSEC – protecting the integrity of the Domain Naming System: 63; DNS Privacy Protocols – encrypted DNS queries for privacy protection: 67

Completed surveys: 17

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Armenia	7	Austria	9	Belgium	2
Cyprus	1	France	3	Georgia	3
Germany	125	Greece	1	Hungary	6
Iceland	1	Ireland		Israel	21
Italy	11	Lithuania	12	Luxembourg	9
N/A	42	Netherlands	38	Poland	4
Portugal	3	Republic of North Macedonia	3	Slovenia	5
South Africa	6	Spain	4	Switzerland	1
Turkey	2	Ukraine	2		

Table A.13: Domain Name System (DNS) Protection submodule: attendees

No.	Question	Answer option
0	Please indicate which sessions of the "DNS Protection" series you attended.	- all (14) - three (3)
1	Please state your job role, i.e., are you working as a network/system administrator or in any other capacity?	Open-Ended Response Network (/System) administrator (9) Security-related Job, i. e. Information Security Officer (6)
2	Please let us know how you would rate your current experience regarding system and/or network administration or any other field if you mentioned it above.	- Very experienced (6) - Experienced (7) - I have some experience (4) - I am new to it (0)
3	In your opinion – were your objectives in attending the session(s) met?	- Yes (16) - Partially (1) - No - Other (please specify)
4	How likely is it that you will use the knowledge, skills and reference materials gained through this training in your work?	- Very likely (13) - Likely (4) - Unlikely - Other (please specify)
5	How would you rate this training session as a whole?	- Very Good (12) - Good (5) - Fair - Poor - Other (please specify)
6	We are already planning the next round of training events (most likely virtual) to take place in 2021. We are seeking your views as to what will make the events more beneficial for you. Please let us know if you would like to see changes regarding the session content:	- I would like to know in advance what the agenda includes (14) - I would like an opportunity to state what is of particular interest to me in the specified area before training so that it can be covered at the event. (2) - I would like to have a follow-up event where particular subjects can be explored in greater detail (6)
7	At the moment it looks as though we shall continue with delivering virtual training sessions. Having attended some of our sessions this year, could you suggest ways to help to make sessions more beneficial for you.	- Keep the same format that we used this year: presentation (most of the allocated time) and some time for Q &A (16) - Introduce “round table” format: invite presentation from participants and include facilitated round-the-table

No.	Question	Answer option
		discussion. No (9), Yes (3) - Introduce "open forum" type of session on a dedicated subject to identify common issues, different solutions. No (4), (Yes) (7) - Use the combination of formats. No (5), Yes (3)
8	Based on your experience of attending virtual sessions this year – please share some comments regarding frequency and duration of the sessions and any changes you think we should make next year:	- Duration of each session (1 hour) is right for me (14) - I would like sessions to be longer to allow more time for Q&A, e.g. 90 min (3) - Time between each session is right for me (8) - I wish sessions were delivered with more time between each session (1)
9	When face-to-face training events become possible – in your opinion, would repeating the same modules as on-site training be beneficial to your NREN or participating organisation?	- Not sure that organising the on-site version of training will bring further benefits compared to the virtual training (11) - Yes, it will be beneficial to bring together an NREN and participating organisation at the on-site event (5)

Table A.14: Domain Name System (DNS) Protection submodule: survey results

Attendees & Survey: Distributed Denial of Service (DDoS) Protection

Number of attendees by session: Introduction to DDoS Attacks – an overview of motivation and modus operandi of attackers: 165; Details of Selected DDoS Attacks – how the attacks work from a technical perspective: 117; DDoS Detection – how to know if you are under attack or partaking in an attack: 118; DDoS Mitigation – what you can do against attacks: 114

Completed surveys: 27

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Albania	2	Armenia	1	Australia	1
Austria	20	Belgium	33	Cyprus	3
Denmark	8	Estonia	6	Finland	9
France	10	Georgia	1	Germany	202
Hungary	9	Ireland	1	Island	2
Israel	17	Italy	7	Lithuania	16

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Luxembourg	4	N/A	33	Netherlands	71
Poland	13	Portugal	4	Republic of North Macedonia	7
South Africa	9	Spain	8	Switzerland	4
Ukraine	1	United Kingdom	12		

Table A.15: Distributed Denial of Service (DDoS) Protection submodule: attendees

No.	Question	Answer option
0	Please indicate which sessions of the "DDoS Protection" series you attended.	- all (21) - three (5) - two (1)
1	Please state your job role, i.e., are you working as a network/system administrator or in any other capacity?	Open-Ended Response Network (/System) administrator (13) Security-related Job, i. e. Information Security Officer (8)
2	Please let us know how you would rate your current experience regarding system and/or network administration or any other field if you mentioned it above.	- Very experienced (4) - Experienced (14) - I have some experience (8) - I am new to it (1)
3	In your opinion – were your objectives in attending the session(s) met?	- Yes (19) - Partially (8) - No - Other (please specify)
4	How likely is it that you would recommend this training to colleagues?	- Very likely (14) - Likely (13) - Unlikely - Other (please specify)
5	How would you rate this training session as a whole?	- Very Good (12) - Good (15) - Fair - Poor - Other (please specify)
6	More training events (most likely virtual) will take place in 2021. If you would like future training to include particular subjects, please state your areas of interest below:	Open-Ended Response: - usage of GÉANT services - Identity Protection: Multi-factor Authentication and Passwordless

No.	Question	Answer option
		(FIDO2 and Windows Hello). - IPv6 security - More in-depth network security - especially at the router level - e.g. bcp38 / MANRS / RTBH, securing BGP, etc. - Infrastructure as a Service (IaaS), Firewall on Demand (FoD), Encryption - Networks Network security - Active Directory Security in University Environments Managed Anti-Virus Solutions / EDR and DSGVO - hardening websites, E2EE - Microsoft Active Directory Secure Setups and Risk of Remote Access Kerberos Mail Security - 2FA
7	Any other comments?	Open-Ended Response: (extract) - Even if training events will take place, I hope virtual attendance will remain possible. - Have presenters watch their own sessions, so they can improve.

Table A.16: Distributed Denial of Service (DDoS) Protection submodule: survey results

A.2 Vulnerability Management Course

Attendees & Survey: Vulnerability Management Process & Standards

Number of attendees: Vulnerability Management: 65; Vulnerability Information: 53; Patch Management: 59

Completed surveys: 11

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Albania	3	Armenia	4	Austria	1
Belgium	6	Croatia	1	Cyprus	1
Estonia	1	Finland	1	France	1
Germany	82	Ireland	1	Israel	3

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Italy	4	Lithuania	8	Luxembourg	4
Moldova	4	N/A	33	Netherlands	2
Republic of North Macedonia	2	Slovenia	6	Spain	5
Sweden	2	Turkey	2		

Table A.17: Vulnerability Management Process & Standards submodule: attendees

No.	Question	Answer option
0	Please indicate which sessions of the "Vulnerability Management Process & Standards" series you attended.	- all (5) - two (2) - one (4)
1	Please state your job role, i.e., are you working as a network/system administrator or in any other capacity?	Open-Ended Response Network (/System) administrator (7) Security-related Job, i. e. Information Security Advisor (2) Other (2)
2	Please let us know how you would rate your current experience regarding system and/or network administration or any other field if you mentioned it above.	- Very experienced (1) - Experienced (9) - I have some experience (1) - I am new to it (0)
3	In your opinion – were your objectives in attending the session(s) met?	- Yes (5) - Partially (6) - No - Other (please specify)
4	How likely is it that you would recommend this training to colleagues?	- Very likely (4) - Likely (7) - Unlikely - Other (please specify)
5	How would you rate this training session as a whole?	- Very Good (5) - Good (6) - Fair - Poor - Other (please specify)
6	How did you get notified about the training?	Open-Ended Response DFN/DFN Newsletter (3) Email (3) by GÉANT (3)

No.	Question	Answer option
		(recommendation) by a colleague (2)
7	Are attendees of your organisation/NREN aware that these training sessions are available?	- Yes (10) - No (1)
8	If you answered "No" to question Q8, can you suggest additional ways to notify of future training?	Open-Ended Response - no answer provided
9	More training events (most likely virtual) will take place in 2021. If you would like future training to include particular subjects – please state your areas of interest below:	Open-Ended Response - Forensic Tools - Identity - best practices to secure remote environments - Security, especially regarding critical web applications. - technical details how to harden systems and network (Linux, Windows, Firewalls) - RISK MANAGER
10	Any other comments	Open-Ended Response - thank you (4)

Table A.18: Vulnerability Management Process & Standards submodule: survey results

Attendees & Survey: Finding Vulnerabilities I – Looking into Networks

Number of attendees: Looking into the Network: 57; Network Vulnerability Scanning: 55; Penetration Tests (postponed session): 29

Completed surveys: 7

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Albania	2	Armenia	2	Belgium	7
Croatia	1	Danmark	6	France	3
Germany	79	Iceland	1	Italy	1
Lithuania	3	Luxembourg	1	N/A	10
Netherlands	8	Poland	2	Portugal	5
Slovenia	5	South Africa	2	Spain	1
United Kingdom	2				

Table A.19: Finding Vulnerabilities I – Looking into Networks submodule: attendees

No.	Question	Answer option
0	Please indicate which sessions of the "Vulnerability Management Process & Standards" series you attended.	- all (5) - two (0) - one (2)
1	Please state your job role, i.e., are you working as a network/system administrator or in any other capacity?	Open-Ended Response Network (/System) administrator (4) Security-related Job, i. e. Information Security Advisor (2) Other (1)
2	Please let us know how you would rate your current experience regarding system and/or network administration or any other field if you mentioned it above.	- Very experienced (1) - Experienced (5) - I have some experience (1) - I am new to it (0)
3	In your opinion – were your objectives in attending the session(s) met?	- Yes (4) - Partially (3) - No - Other (please specify)
4	How likely is it that you would recommend this training to colleagues?	- Very likely (5) - Likely (2) - Unlikely - Other (please specify)
5	How would you rate this training session as a whole?	- Very Good (5) - Good (2) - Fair - Poor - Other (please specify)
6	How did you get notified about the training?	Open-Ended Response DFN/DFN Newsletter/DFNCERT/Searching for DFN Data (4) Email (1) no answer (2)
7	Are attendees of your organisation/NREN aware that these training sessions are available?	- Yes (6) - No (1)
8	If you answered "No" to question Q8, can you suggest additional ways to notify of future training?	Open-Ended Response - Email to DFN partners
9	More training events (most likely virtual) will take place in 2021. If you would like future training to include particular subjects – please state your areas of interest below:	Open-Ended Response - Information Security Networks - More technical on higher level would be fine

No.	Question	Answer option
10	Any other comments	Open-Ended Response - Online format is a plus - live demo would be great - thank you

Table A.20: Finding Vulnerabilities I – Looking into Networks submodule: survey results

Attendees & Survey: Finding Vulnerabilities II – Looking into Code

Number of attendees: Code audits: 39; Vulnerability Disclosure: 34; Breach and Attack Simulation (postponed session): 29

Completed surveys: 0

Country	No. Attendees	Country	No. Attendees	Country	No. Attendees
Armenia	1	Croatia	3	Cyprus	4
Danmark	3	France	2	Germany	59
Lithuania	3	Moldova	3	N/A	7
Netherlands	3	Portugal	4	South Africa	3
Spain	7				

Table A.21: Finding Vulnerabilities II – Looking into Code submodule: attendees

Appendix B YouTube Viewings

The recordings of the sessions are available at [YouTube_Recs].

The graphs below give an overview of the number of viewings over 3 6-month periods. (Although no key is available, the graphs clearly show the pattern of viewing activity.) Details for each recording are provided in Table B.1.

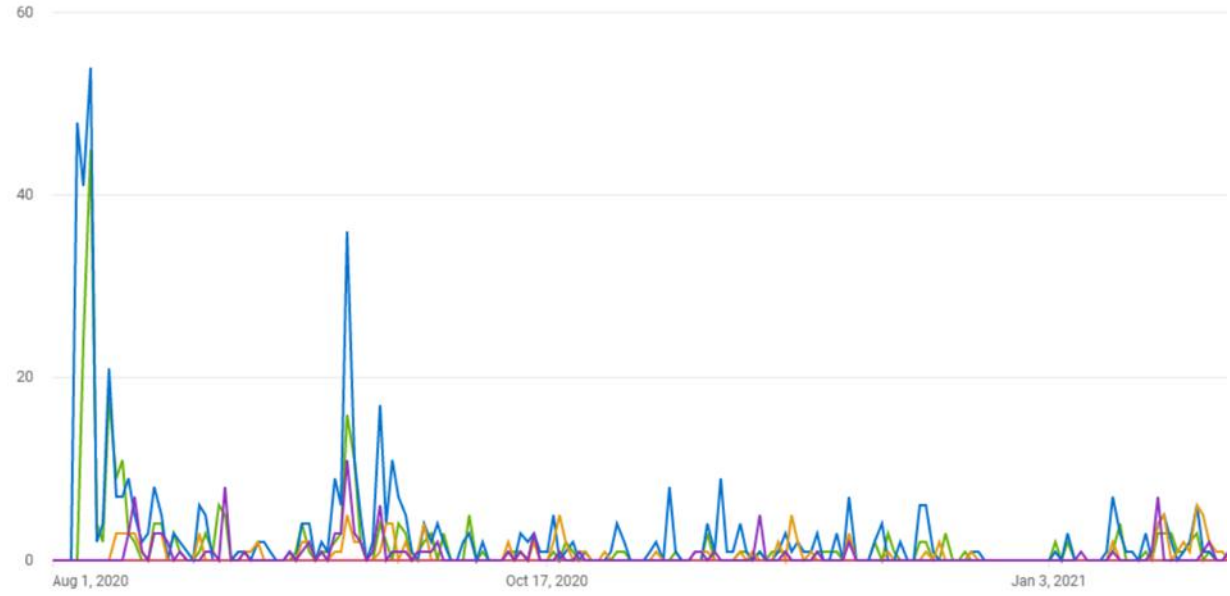

Figure B.1: YouTube viewings August 2020 to January 2021

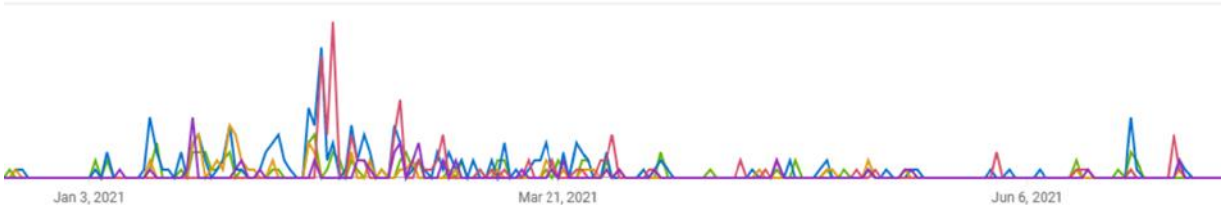

Figure B.2: YouTube viewings January to June 2021

Figure B.3: YouTube viewings June to 9 November 2021

The data about the viewings was collected on the 9th of November 2021.

Video	Number of views	Watch time (hours)	Average view duration
Operational Network Security Course			
Submodule 1: Operating System Privacy & Security			
Operating System Telemetry – configuring privacy protection in Windows 10 | 03 Aug 2020	759	78.9	0:06:14
Logging and Audit – log management and audit strategies | 5 Aug 2020	384	59.7	0:09:19
File Integrity Monitoring (FIM) for managing security incidents | 07 August 2020	97	16.7	0:10:21
Network First Hop Security | 11 August 2020	186	28.3	0:09:08
Authentication Methods – how to avoid common pitfalls | 13 August 2020	159	28.7	0:10:49
Submodule 2: Client Privacy & Security			
Browser Security and Privacy | 21 Sep 2020	114	18.6	0:09:46
Email Security and Privacy - how to handle most common issues | 23 Sep 2020	84	10.4	0:07:27
Instant Messaging Security and Privacy – chat and more while safeguarding personal data|24 Sep 2020	39	5.8	0:08:54
Videoconferencing Security and Privacy – overview of best practices | 28 Sep 2020	80	10.3	0:07:43
Office Suites – understanding privacy and security risks | 30 Sep 2020	58	9.0	0:09:16
Submodule 3: Domain Name System (DNS) Protection			
Introduction to DNS and its Security Challenges | 30 Nov 2020	59	8.8	0:08:56
DNS for Network Defence – using DNS to protect and observe | 03 Dec 2020	54	8.1	0:09:00
DNSSEC – protecting the integrity of the Domain Naming System | 07 Dec 2020	62	10.2	0:09:52

Video	Number of views	Watch time (hours)	Average view duration
DNS Privacy Protocols – encrypted DNS queries for privacy protection | 10 Dec 2020	45	4.8	0:06:23
Submodule 4: Distributed Denial of Service (DDoS) Protection			
Introduction to DDoS Attacks | 08 Feb 2021	117	9.1	0:04:39
Details of Selected DDoS attacks | 10 Feb 2021	64	9.6	0:08:59
DDoS Detection | 15 Feb 2021	41	5.2	0:07:33
DDoS Mitigation | 17 Feb 2021	39	5.2	0:08:03
Vulnerability Management Course			
Submodule 1: Vulnerability Management Process & Standards			
Vulnerability Management – introduction to processes & standards | 27 May 2021	105	17.7	0:10:06
Vulnerabiliuty Information – how to gather and distribute security advisories to your constituency | 08 Jun 2021	40	5.4	0:08:02
Patch Management – how to roll out and track security fixes to your systems | 10 Jun 2021	34	4.6	0:08:10
Submodule 2: Finding Vulnerabilities I – Looking into Networks			
Looking into the Network – how to scan local systems for vulnerabilities and misconfigurations | 28 Jun 2021	52	6.5	0:07:30
Network Vulnerability Scanning – looking from afar | 30 Jun 2021	57	11.8	0:12:26
Penetration Tests – how does your network stand up against real attacks? | 13 Sep 2021	18	2.7	0:08:59
Submodule 3: Finding Vulnerabilities II – Looking into Code			
Code Audits – how to increase the quality of the code | 04 Jul 2021	29	4.5	0:09:23
Vulnerability Disclosure – letting the cat out of the bag |16 Jul 2021	19	1.4	0:04:21
Breach and Attack Simulation – matching attacker behaviour with vulnerabilities| 15 Sep 2021	17	3.3	0:11:47
Total	**2,812**	**385**	**0:08:38**

Table B.1: Training recordings: number of views, watch time and average view duration per session

Appendix C Course Resources

The course materials were made available to the community via the GÉANT and GÉANT GLAD pages as shown in Table C.1 below.

Description	Link
Both security training courses with developed course material and recording	https://security.geant.org/training/
Operational Network Security Course	
Submodule 1: Operating System Privacy & Security	https://learning.geant.org/operational-network-security-new-for-2020-virtual-learning-with-experts-2/
Submodule 2: Client Privacy & Security	https://learning.geant.org/client-privacy-and-security-operational-network-security-new-for-2020-virtual-learning-with-experts/
Submodule 3: Domain Name System (DNS) Protection	https://learning.geant.org/domain-name-system-dns-protection-operational-network-security-new-for-2020-virtual-learning-with-experts/
Submodule 4: Distributed Denial of Service (DDoS) Protection	https://learning.geant.org/client-privacy-and-security-operational-network-security-new-for-2020-virtual-learning-with-experts-2/
Vulnerability Management Course	
Submodule 1: Vulnerability Management Process & Standards	https://learning.geant.org/domain-name-system-dns-protection-operational-network-security-new-for-2020-virtual-learning-with-experts-2/
Submodule 2: Finding Vulnerabilities I – Looking into Networks	
Submodule 3: Finding Vulnerabilities II – Looking into Code	
Recordings	
All recordings	https://www.youtube.com/playlist?list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6

Table C.1: Links to course resources on GÉANT and GÉANT GLAD pages

References

[D8.1]	Deliverable D8.1 *Summary of Security Training and Awareness Campaign Materials: An Investigation and Gap Analysis of Current Security Training and Awareness Resources* https://www.geant.org/Projects/GEANT_Project_GN4-3/GN43_deliverables/D8.1-Summary-of-Security-Training-and-Awareness-Campaign-Materials.pdf
[DFN-CERT_SecTrng]	https://www.dfn-cert.de/en/Trainings.html
[GLAD_ONS]	https://learning.geant.org/operational-network-security-new-for-2020-virtual-learning-with-experts-2/
[GLAD_VM]	https://learning.geant.org/domain-name-system-dns-protection-operational-network-security-new-for-2020-virtual-learning-with-experts-2/
[Security_Training]	https://security.geant.org/training/
[WP8_T1]	https://wiki.geant.org/display/gn43wp8/Task+1%3A+Business+Continuity [login required]
[YouTube_Recs]	https://www.youtube.com/playlist?list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6

Glossary

2FA	Two-Factor Authentication
ARP	Address Resolution Protocol
BAS	Breach and Attack Simulation
BCP	Best Current Practices
BGP	Border Gateway Protocol
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoH	DNS over HTTPS
DoT	DNS over TLS
DSGVO	Datenschutz-Grundverordnung (GDPR in English)
E2EE	End-to-End Encryption
EDR	Endpoint Detection and Response
FIM	File Integrity Monitoring
FoD	Firewall on Demand
GDPR	General Data Protection Regulation
GLAD	GÉANT Learning and Development
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IP	Internet Protocol
ISO	Information Security Officer
ISP	Internet Service Provider
IT	Information Technology
MANRS	Mutually Agreed Norms for Routing Security
NREN	National Research and Education Network
OS	Operating System
PSIRT	Product Security Incident Response Team
RAM	Random Access Memory
RTBH	Remotely Triggered Black Hole
SSD	Solid State Drive
TAN	Transaction Authentication Number

TLS	Transport Layer Security
WP8	Work Package 8 Security
WP8 T1	WP8 Task 1 Business Continuity
WP9	Work Package 9 Operations Support
WP9 T2	WP9 Task 2 Software Governance and Support