30-06-2021

Milestone M8.10 (M56)
Review of Security Training Materials

Milestone M8.10 (M56)

Contractual Date:	30-06-2021
Actual Date:	30-06-2021
Grant Agreement No.:	856726
Work Package	WP8
Task Item:	T1
Nature of Milestone:	O (Other)
Dissemination Level:	PU (Public)
Lead Partner:	DFN-CERT
Document ID:	GN43-21-20B20C
Authors:	Klaus Möller (DFN-CERT); Christine Kahl (DFN-CERT); Stefan Kelm (DFN-CERT); Tobias Dussa (DFN-CERT); Sarunas Grigaliunas (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 reports on the GÉANT Operational Network Security training course designed for network and system administrators at NRENs and their member organisations to increase their operational security knowledge.

Table of Contents

Table of Tables

1 Introduction

The importance of security and, more recently, privacy in NREN networks hardly need to be stated. But although the relevance of training on these issues is widely recognised, it has often concentrated on security personnel tasked with handling incidents, while system and network administrators have been neglected.

An Operational Network Security training module was therefore created based on experiences and discussions with security offices and network operators to address a number of common security risks that NRENs and their member organisations face in their day-to-day operations. These include:

- Authentication
- Logging
- Audit
- Privacy
- 1st Hop security
- DNS security
- Protection from Distributed Denial-of-Service attacks

The remit of GN4-3 WP8 Task 1 – Business Continuity is to prepare and conduct training courses to fill the gaps that were identified as part of the project and reported in 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].

An analysis of existing training opportunities and materials revealed that Operational Network Security was the least covered category, therefore it was decided to design and deliver the first training course focused on this topic.

Due to the COVID-19 pandemic and the subsequent need to reduce business travels and contacts, the original plan to deliver the training course as a two- or three-day on-site training was adapted, and the course restructured with the support of GLAD into a complete online training.

This report documents the course delivered, listing attendees of the online training sessions from NRENs and member organisations by country and summarising the feedback that was gathered from them through different surveys. The report also highlights some possible areas of improvement and opportunities for further uses of the training materials developed.

2 Operational Network Security Course Structure and Content

1st Submodule: Operating System Privacy & Security

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 1st Hop Security: 126; Authentication methods: 110

Session	Content
Operating System Telemetry – configuring privacy protection in Windows 10	The session provided 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 explored additional ways to make Windows 10 more privacy friendly.
Logging and Audit – Log management and Audit strategies	All 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.
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 introduced 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 included a live demonstration of one of the latest open source FIM solutions 'Wazuh'.
Network 1st 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.

Session	Content
	While these protocols are vital to the operation of the network, they inherit a number of security risks, which were also explored in this session, as well as ways to mitigate some security risks.
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 provided an overview of authentication methods and outlined the most important and relevant approaches in more detail to help participants avoid the most common pitfalls in this area.

Table 2.1: Submodule 1 – Operating System Privacy & Security

2nd Submodule: Client Privacy & Security

Delivered on: 21-30 September 2020

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

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 gave an introduction on how to secure them and how to avoid providing unnecessary personal data to websites or browser vendors. Participants were also shown how to avoid being tracked on their personal trail across the internet.
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 e-mail has become one of the most important tools of business. Email has also become one of the most universal and persistent sources of privacy and security headaches. The webinar gave an overview of the many challenges that email introduces and provided approaches of how to effectively deal with some of its more common issues.
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	Content
	Session participants were shown how to secure instant messenger clients and how to avoid common privacy pitfalls.
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 provided an overview of security and privacy issues with popular videoconferencing clients and services and showed how to address them.
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 for convenient collaboration. However, the growing complexity of these programs has introduced a number of problems related to both privacy and security. The talk gave participants an insight into common privacy issues and security risks and provided some practical tips to address them.

Table 2.2: Submodule 2 – Client Privacy & Security

3rd Submodule: Domain Name System (DNS) Protection

Delivered on: 30 November-10 December 2020

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

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 gave an overview of how DNS works and, crucially, what the security implications of its design and operation are.
DNS for Network Defense – Using DNS to protect and observe	DNS is not only used for the mapping of names to IP addresses and vice versa. This module showed 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.

Session	Content
	This was followed by a block on monitoring DNS queries to collect information about ongoing intruder activity on an organisation's network.
DNSSEC - Protecting the integrity of the Domain Naming System	Although hampered by slow adoption, DNSSEC has proven to deal effectively with the integrity problems of DNS. This module introduced the general concepts of DNSSEC and provided a practical example by implementing DNSSEC in a local zone.
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 module gave insights into the workings and configuration of DoT and DoH and explained 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.

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

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

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

Session	Content
Introduction to DDoS Attacks – An overview of motivation and modus operandi of attackers	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 off ISPs. While the actual DDoS attacks have changed very little, the orchestration of the attacks, the deployment of their components and the motives of attackers have evolved. The course gave participants an overview of the attacks, the attackers, and their motivation and modus operandi.
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 course provided 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.
DDoS Detection – How to know if you are under attack or partake in an attack	DDoS Detection may in theory sound simple, i.e., when you can't access your systems, that means you're under attack. However, this may also

Session	Content
	happen due to technical problems or misconfigurations. And what if we want to detect attacks before falling victim to them? The course showed participants the various ways in which DDoS attacks are detected on the internet.
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 course showed some simple but proven techniques to combat DDoS attacks as well as to avoid unintentionally partaking in one.

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

3 Review Outcomes

Overall, the feedback from the attendees was very positive and they considered the training material to be up to date, at least in most parts. They found that their objectives in attending a session were usually met or at least partially met. The attendees who answered the survey would recommend the training to their colleagues and will likely use the knowledge acquired from the training for their job.

Most of the attendees work as network or system administrators, which is the group the training is aimed at. 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.)

Nevertheless, some areas where there might be some 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 DNS Protection survey), 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, attendees had the opportunity to rate the presenter’s skills. No feedback noting any specific need for improvement was given, but one useful suggestion was provided 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) an evaluation was carried out to assess whether the format of the training could be changed to be a collaborative format by setting up a 'round table' or an 'open forum' to dive into specific topics together with the attendees, but these suggestions received little or no agreement and most attendees would prefer to proceed with the current training session setup.

4 Recommendations

Based on the feedback received, the general concept for the training seems to be working well and should not be modified for the upcoming training modules.

Nevertheless, some kind of 'opening out' of a session would be useful. Given that the demo in the Operating System Privacy & Security FIM session was positively received, demonstrations should be run where possible in a session.

Some attendees expressed the desire to know the agenda prior to the sessions (DNS Protection survey). Although the teaser provides a rough overview of the content of the sessions, distributing the information agenda by email prior to trainings should be considered. As registration is per submodule and not per session, to avoid sending too many emails, the teaser and the agenda should 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 advertisement for the training is better in these two countries than in others.

It should be evaluated if it is possible to announce the trainings to a broader community than is currently the case.

5 Further Use of the Course

All sessions have been recorded and are available online, but viewing numbers are not very high.

Viewing a recording versus attending a live session is different, as:

- It is possible to ask questions at the end of a live session
- Even if they do not see so 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 advertising for the live sessions is not available for the recordings.

Based on the findings mentioned, it might be possible to repeat the live sessions at some point in time, slightly adapted based on the feedback, and new tools and trends.

Once the restrictions due to the COVID-19 pandemic are over, it might also be an option to offer onsite trainings using the material developed, as some (although not the majority) of the attendees indicated a need for it (DNS Protection survey). One option would be to host a training at a given location and accept attendees from different organisations, while the other would be to organise a training for a specific NREN and their member organisations onsite. Further assessment needs to be carried out to decide which of these is the best option.

6 The Road Ahead

A second training course, Vulnerability Management, is currently underway. As the restrictions due to the COVID-19 pandemic are still in force at the time of writing, the training course is being delivered as online training.

The Vulnerability Management training consists of three submodules, with the first submodule delivered from the end of May till mid-June 2021, the second delivered in July 2021 and the third currently being planned.

A third course, which will be designed from August 2021 onwards, will focus on the topic 'Forensic', with details of the training still to be developed.

Appendix A Surveys and Results

A number of surveys were created to gather feedback from the attendees. Initially, for Submodule 1 a survey was run after each session, but this was soon found to be too detailed and time-consuming, so for the next submodules attendees were asked to provide feedback to 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).

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)

No	Question	Answer option
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) - Subject matter knowledge (Excellent: 6) - Presentation skills (Excellent: 2, Good:4) - Ability to understand and answer questions (Excellent: 3, Good:1)	- Excellent - Good - Fair - Poor

No	Question	Answer option
	- Other (please specify) Note: Some attendees reported problems with the radio box.	
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: Survey Responses: Operating System Privacy and Security – Operating System Telemetry

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 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)	- till 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: Survey responses: Operating System Privacy and Security – Logging and Audit

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-End 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-End 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: Survey Results: Operating System Privacy and Security – File Integrity Monitoring (FIM) for detecting security incidents

Attendees & Survey: Operating System Privacy and Security – Network 1st 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 1st 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: Survey Results: Operating System Privacy and Security – Network 1st Hop Security

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)
8	If you attended other sessions – which one did you like the most and why?	- Network 1st Hop Security (3)

No	Question	Answer option
		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: Survey Results: Operating System Privacy and Security – Authentication methods

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 session 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: Survey Results: Client Privacy and Security

Attendees & Survey: Domain Name System (DNS) Protection

Number of attendees: Introduction to DNS and its Security Challenges – Meet the Problems: 99; DNS for Network Defense – 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 session 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 like that 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

No	Question	Answer option
		participants and include facilitated round the table 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: Survey Results: Domain Name System (DNS) Protection

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 partake 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

Country	No Attendees	Country	No Attendees	Country	No Attendees
France	10	Georgia	1	Germany	202
Hungary	9	Ireland	1	Island	2
Israel	17	Italy	7	Lithuania	16
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 session 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)

No	Question	Answer option
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 GEANT services - Identity Protection: Multi-factor Authentication and Passwordless (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: Survey Results: Distributed Denial of Service (DDoS) Protection

Appendix B YouTube viewings

The recordings of the sessions are available on the following page:

https://www.youtube.com/playlist?list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6

Video	Number of Views	Watch time (hours)	Average view duration
Operating system Telemetry - Configuring privacy protection in Windows 10 | 03 Aug 2020	684	67,2741	0:05:54
Logging and Audit - Log management and audit strategies | 5 Aug 2020	355	53,3274	0:09:00
File Integrity Monitoring FIM for managing security incidents | 07 August 2020	82	13,3446	0:09:45
Network 1st Hop Security | 11 August 2020	167	24,4354	0:08:46
Authentication methods – how to avoid common pitfalls | 13 August 2020	143	25,7977	0:10:49
Web browsers Security and Privacy | 21 Sep 2020	94	15,9365	0:10:10
Email: Security and Privacy - how to handle most common issues | 23 Sep 2020	79	10,4184	0:07:54
Instant Messaging: Security and Privacy – chat and more while safeguarding personal data|24 Sep 2020	33	5,5476	0:10:05
Videoconferencing: Security and Privacy - Overview of best practices | 28 Sep 2020	74	9,6175	0:07:47
Office Suites - Understanding Privacy and Security Risks | 30 Sep 2020	54	8,9652	0:09:57
Introduction to DNS and its security challenges | 30 Nov 2020	48	7,7193	0:09:38
DNS for Network Defence: Using DNS to protect and observe | 03 Dec 2020	49	7,7355	0:09:28
DNSSEC session recording | 07 Dec 2020	58	10,1945	0:10:32
DNS Privacy Protocols - Encrypted DNS queries for privacy protection | 10 Dec 2020	40	4,6038	0:06:54
DDoS protection – Introduction | 08 Feb 2021	105	6,8832	0:03:55
Details of Selected DDoS attacks | 10 Feb 2021	55	8,7787	0:09:34
DDoS detection | 15 Feb 2021	33	4,2782	0:07:46
DDoS mitigation | 17 Feb 2021	30	5,1664	0:10:19
Total	**2183**	**290,0241**	**0:07:58**

Appendix C Content resources

The materials were made available to the community via the GÉANT GLAD pages.

Operating System Privacy & Security:

https://learning.geant.org/operational-network-security-new-for-2020-virtual-learning-with-experts-2/

Client Privacy & Security:

https://learning.geant.org/client-privacy-and-security-operational-network-security-new-for-2020-virtual-learning-with-experts/

Domain Name System (DNS) Protection:

https://learning.geant.org/domain-name-system-dns-protection-operational-network-security-new-for-2020-virtual-learning-with-experts/

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/

The recordings of the sessions are available on the following page:

https://www.youtube.com/playlist?list=PLELuOn8jN3IKtR40qezwfzlP5BIMPYKF6

References

[D8.1] https://www.geant.org/Projects/GEANT_Project_GN4-3/GN43_deliverables/D8.1-Summary-of-Security-Training-and-Awareness-Campaign-Materials.pdf

Glossary

DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoH	DNS over HTTPS
DoT	DNS over TLS
FIM	File Integrity Monitoring
GLAD	GÉANT Learning and Development
HTTPS	Hypertext Transfer Protocol Secure
ISO	Information Security Officer
TLS	Transport Layer Security