D4.3 - NGSOTI training experience blog post

NGSOTI Project: 101127921
DIGITAL-ECCC-2022-CYBER-03

Team CIRCL/NGSOTI

CIRCL
Computer Incident
Response Center
Luxembourg

Co-funded by
the European Union

2025-19-06

Contents

1 Experience and Key Takeaways

1.1 Disclaimer

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Words displayed in red indicate hyperlinks. These links can be clicked or viewed by hovering over the text.

1.2 Distribution and License

The document is distributed as TLP:CLEAR.

1.3 Deliverable definition

The identifier of the deliverable is **D4.3** and it adheres to the definition outlined in the grant agreement written in **bold**. **NGSOTI training experience blog post**. The description is: **Blogpost on training experience with NGSOTI how the tools were used on d4-project.org**

The training experience described in this deliverable was published on d4-project.org. Following the publication, feedback was collected from the project reviewers and incorporated into this deliverable.

2 Our Experience and Key Takeaways from Trainings within the NGSOTI EU Funded Project

We are glad to share the overwhelmingly positive outcomes and valuable insights gained from our participation in the NGSOTI (Next Generation Security Operations and Threat Intelligence) EU Funded Project. The project has been a resounding success, allowing us to engage with a diverse audience and make significant strides in cybersecurity education and training.

2.1 A Resounding Success in Numbers

Throughout the project, we conducted **13 training sessions**, reaching a total of **155 participants**. These participants hailed from a variety of professional backgrounds, including the financial and academic sectors, creating a rich and collaborative learning environment.

2.2 Tailored Training for the Financial Sector

One of our key observations was the effectiveness of providing ready-to-use training materials for professionals in the financial sector. Given the fast-paced and highly regulated nature of their work, having access to practical, immediately applicable knowledge and tools proved to be the most efficient and valuable approach.

2.3 Bridging the Gap in Academia with Hands-On Tools

In the academic sector, we identified a clear need for more practical, hands-on tooling sessions for students. To address this, our training for university students focused on Digital Forensics and Incident Response (DFIR) and Threat Intelligence, utilizing cutting-edge open-source tools such as:

- **MISP - A Threat-Intelligence Platform**
- **AIL Project (Analysis Information Leak)**
- **Kunai**
- **FlowIntel**

The engagement and feedback from students were exceptional, highlighting a strong desire for this type of practical experience.

2.4 Rethinking University Curriculums: A Call for Practicality

Our experience within university settings also brought to light several shortcomings in traditional academic approaches to cybersecurity education:

- **Lack of Practical Labs:** There is a significant scarcity of hands-on laboratory sessions where students can apply theoretical knowledge.
- **Overemphasis on GRC:** Curriculums often focus heavily on Governance, Risk, and Compliance (GRC) at the expense of practical, hands-on skills.
- **Onboarding Challenges:** We observed a learning curve for students who were not accustomed to hands-on lab environments.

These observations point to a tremendous opportunity for universities to rethink and modernize their cybersecurity curriculums. By incorporating more practical, tool-based training, we can better prepare the next generation of cybersecurity professionals for the real-world challenges they will face.

2.5 User experience and impact collection

The third objective of the training work package is to collect feedback from training to improve the future ones. The analysis of the feedback regarding the MISP training was published on Github. It uses the terms issues to track ideas and feedbacks. It describes improvements of the MISP tool based on user experience and impact.

The table below summarizes the feedback collected during MISP trainings. The start date was 16 December 2024, and the cut-off date was 19 June 2025. The user experiences described in this deliverable are based on that feedback. All feedback regarding the MISP tool gathered during trainings is tagged 'from:training' on the following link.

Issue	User experience	Impact
10321	API usability — it affects how developers consume the API and what response format they get.	If ignored, clients may receive an unexpected format.
10320	MISP administrators. It affects the stability of a MISP instance.	If ignored an MISP instance can be overload and cause stability incidents caused by unbounded API queries.
10219	In the graphical user interface, users experienced difficulty recognizing extended events.	Users were forced to click through each event, increasing effort and time needed to identify extended events.
10218	In the graphical user interface, users experienced difficulty expanding extended events.	Users were forced to remember the event ID they wanted to extend and then manually insert the event ID into their extended event.

Issue	User experience	Impact
10216	Users want to be able to seamlessly share their cache between instances, like a sync push/pull.	Users encountered limitations when sharing their cache.

The NGSOTI incident response training started with a voluntary questions in order to collect feedback from the audience:

- Round table.
- Purpose make this training useful.
- What are your area of expertise?
- What do you expect from this course?

The table below presents insights gathered from the Incident Response training. These insights were used **to improve subsequent Incident Response trainings**. The trainings were attended by groups from individual organizations and were primarily composed of security professionals. The participants generally fell into two categories: GRC personnel and operational staff. GRC participants were often managers focused on Governance, Risk, and Compliance activities, while operational staff were technical professionals such as system administrators, engineers, and SOC operators.

Topic	GRC	Operational Staff
Expectations	Policies and procedures to establish and govern SOC operations.	Practical tools and techniques applicable to day-to-day SOC operations.
Incident Detection	Collecting the information required to complete regulatory reporting forms.	Investigating affected services and implementing remediation measures.
Lessons Learned	Feedback from participants and regulators on how reporting can be avoided.	Feedback on ineffective or incorrect remediation actions.
Areas of Interest	Contractor evaluation: ensuring contractors take the necessary actions to support proper reporting when evidence is identified.	Collecting evidence correctly without compromising or destroying it.
Tooling	Identifying available tools and how metrics can support risk assessment.	Operational use of tools in SOC activities.

3 Conclusion

The NGSOTI project has been a rewarding experience. It has not only allowed us to share our expertise but has also provided us with invaluable insights into the diverse needs of the cybersecurity community. We are more committed than ever to championing hands-on, practical training and look forward to continuing to bridge the gap between theoretical knowledge and real-world application.