HORIZON 2020

Digital Security: Cybersecurity, Privacy and Trust
H2020-DS-2015-1

DS-04-2015 Information driven Cyber Security Management
Grant n° 700176

Secure Information Sharing Sensor Delivery event Network[†]

Deliverable D2.1: Interim Dissemination Report

Abstract: This report is an instrument that will allow following the awareness actions done by the project partners throughout the project. The preliminary version will report past activities and give an overview of actions the planned in the second period, while the final report will contain the list of all activities done at several dissemination level, such as papers, website, links from other reference websites, demonstrations and workshops.

Contractual Date of Delivery	31 October 2017
Actual Date of Delivery	26 December 2017
Deliverable Security Class	Public
Editor	Adam Kozakiewicz (NASK)
Contributors	All *SISSDEN* partners
Internal Reviewers	Massimiliano Aschi (POSTE)
Quality Assurance	Anna Felkner (NASK)

[†] The research leading to these results has received funding from the European Union Horizon 2020 Programme (H2020-DS-2015-1) under grant agreement n° 700176.

The *SISSDEN* consortium consists of:

Naukowa i Akademicka Sieć Komputerowa	Coordinator	Poland
Montimage EURL	Principal Contractor	France
CyberDefcon Limited	Principal Contractor	United Kingdom
Universitaet des Saarlandes	Principal Contractor	Germany
Deutsche Telekom AG	Principal Contractor	Germany
Eclexys SAGL	Principal Contractor	Switzerland
Poste Italiane – Società per Azioni	Principal Contractor	Italy
Stichting the Shadowserver Foundation Europe	Principal Contractor	Netherlands

Table of Contents

1 Introduction

1.1 Aim of the document

The document presents an overview of the dissemination and exploitation activities performed by the consortium in the first reporting period (from M1 to M18) and the plans for the second period.

1.2 Structure of the document

Section 2 provides an overview of the activities realized in the period:

- The first subsection presents the project's Internet presence – both the main project website and the social media activity.
- The second subsection focuses on the technical and scientific dissemination. This activity is expected to intensify in the second period, as the main research work package (namely WP5) has started in month 6 and only a part of the work had a chance to generate publishable results and to pass the peer-review and editorial delays so far. Still, a significant amount of dissemination activities has already been done.
- The third subsection highlights dissemination efforts oriented towards EU policy makers and suggestions emerged on future regulatory options in the area of ICT security.
- The fourth subsection focuses on the non-technical dissemination activities of the consortium – the general project presentations and other promotional activity.
- Finally, the fifth subsection presents the early exploitation activity of the consortium – namely the use of the early project results for practical goals.

Section 3 analyses the progress of the key performance indicators defined in the project proposal, based on information presented in Section 2.

Section 4 contains an update to the project's exploitation and dissemination plan. The focus of this chapter is biased towards dissemination activities, due to the fact that 1) exploitation is also explored and detailed in deliverable D2.3 "Preliminary market strategy and sustainability plan" and 2) not all planned exploitation activities can be fully described in this public deliverable (i.e. D2.1).

2 Current dissemination and exploitation activity

2.1 Website and social media

The website for the SISSDEN project was created on M2 and is now available at the following URL: https://sissden.eu. The project website includes a set of relevant elements namely: information about the project and the state of advancement, blog, project results, collaboration and contact information.

The following figure shows the upper part of the first page of the web site.

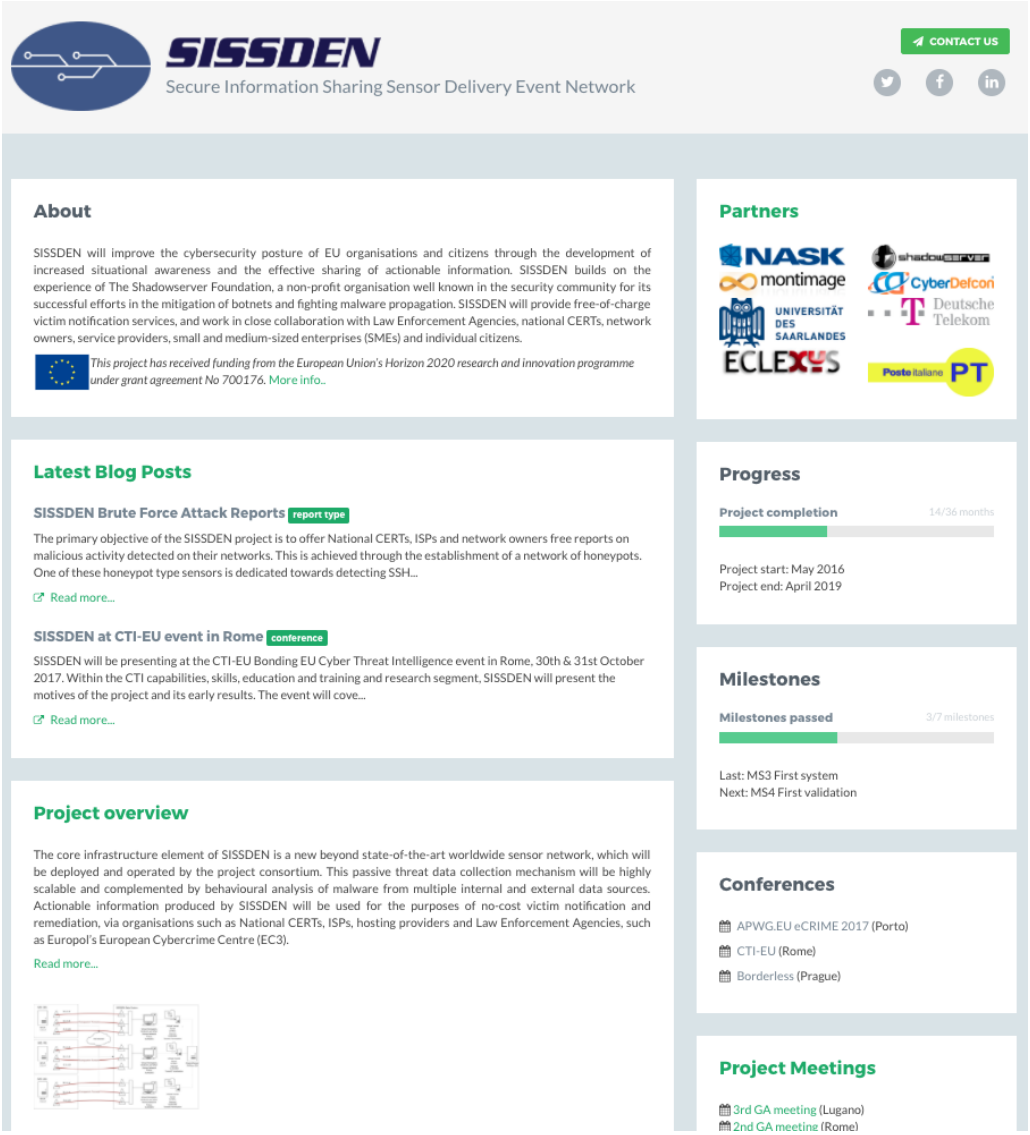

Figure 2.1: Front page of the SISSDEN website

The blog allows the partners to announce events and accomplishments. Two last blog posts that have been added are:

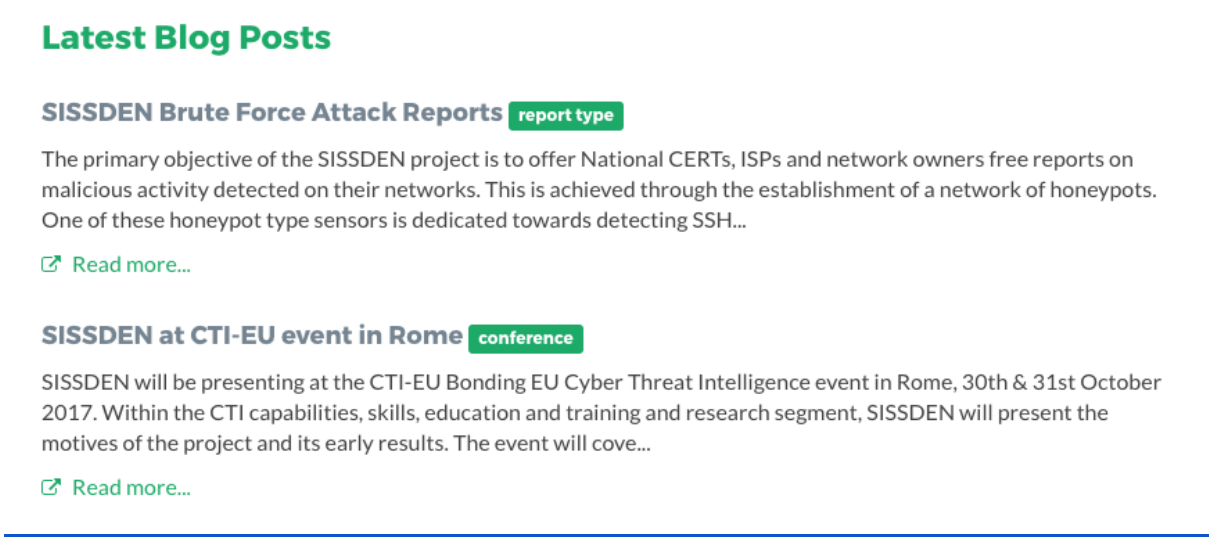

Figure 2.2: Blog section of the website

The website provides a link to the public deliverables in Google Drive. Five deliverables have been published so far.

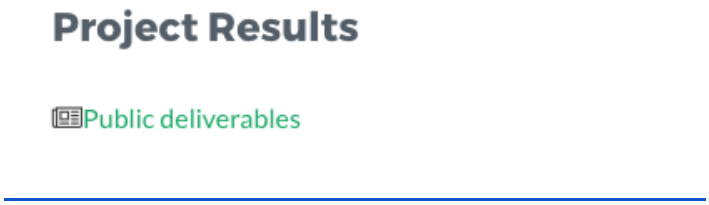

Figure 2.3: Deliverables section of the website

The website's dashboard gathers statistics on the number of visitors which is very positive. The statistics gathering was started on August 30, 2017. From August 30, 2017 to October 26, 2017 there has been 6585 accesses to the site. In the last month (October 2017, corresponding to month 18 of the project) there were 2634 accesses, as shown in the next figure.

Figure 2.4: Access statistics of the website

Moreover, three social media accounts (Twitter, Facebook, LinkedIn) have been created on M2 and are now active; all these social media accounts are linked in the upper part of the SISSDEN project website.

Figure 2.5: The SISSDEN Twitter profile

SHAD has been managing the SISSDEN Twitter account in 2017. Overall statistics since the launch of the Twitter account (June 2016) are as follows: 34 tweets, 221 followers as of 26th October 2017. We consider this to be a very positive result provided that the SISSDEN system was not fully operational for the majority of this period and is not publically accessible yet.

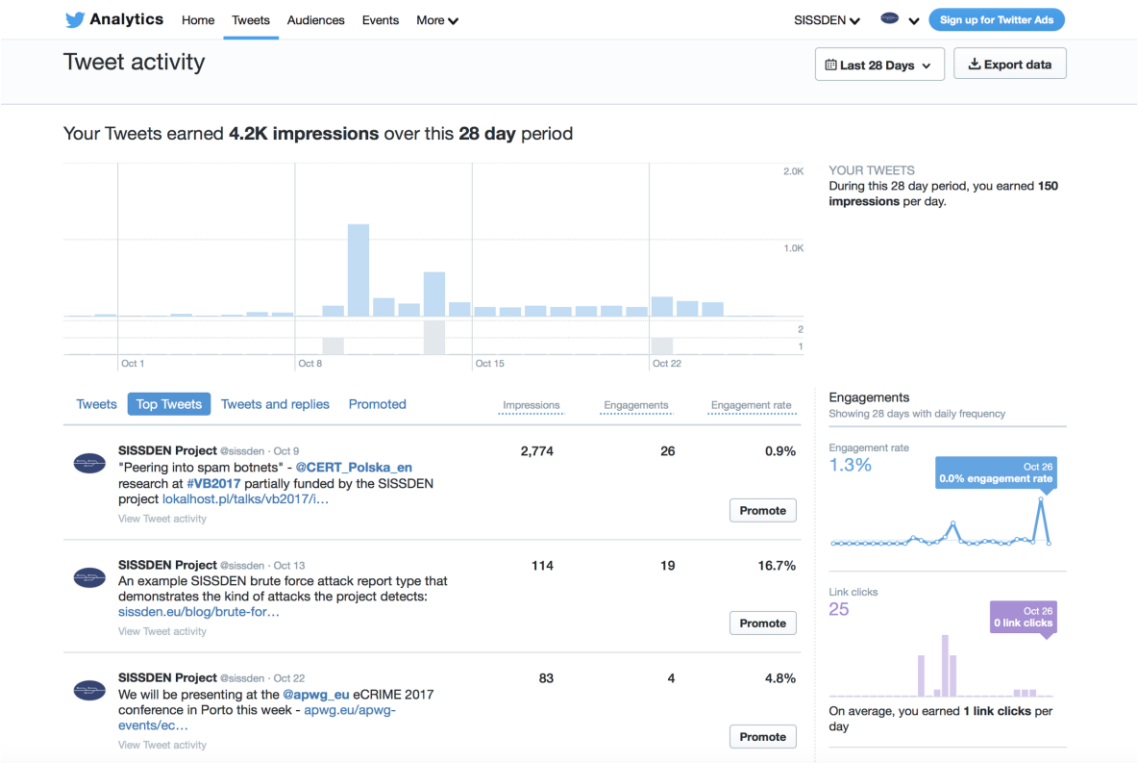

Figure 2.5: The SISSDEN Twitter statistics

CYBE has been managing the SISSDEN Facebook profile and the LinkedIn group. Currently the Facebook profile is observed by 10 people – the main website is more promoted by the consortium and clearly provides more visibility. The profile was used to publish early blog posts before the main website started offering this feature. The posts are now published through both channels.

Figure 2.6: The SISSDEN Facebook profile

The consortium's social activity will intensify in the months leading up to the Maturing System milestone (M24) in order to build interest in the opening of the platform to external users and will remain high afterwards in order to draw more users to the system.

2.2 Scientific and technical dissemination

The following section presents the current results of the project's scientific and technical dissemination efforts.

2.2.1 NASK

- Piotr Bazydło, Krzysztof Lasota, and Adam Kozakiewicz, "Botnet Fingerprinting: Anomaly Detection in SMTP Conversations", in IEEE Security & Privacy, vol. 15, no. 6, pp. 25-32, November/December 2017, doi: 10.1109/MSP.2017.4251116 (accepted for publication before M18).
- Piotr Białczak, "Dwa światy złośliwych żądań HTTP" ("Two worlds of malicious HTTP requests"), Secure 2017, 21st Conference on Telecomunications and IT Security, 24-25 October 2017, Warsaw, Poland
- Piotr Bazydło, "Pokaż mi swój dialekt a powiem Ci kim jesteś - rozpoznawanie botnetów na podstawie implementacji SMTP" ("Show me your dialect and I will tell you who you are - botnet fingerprinting on the basis of SMTP implementation"), Secure 2017, 21st Conference on Telecommunications and IT Security, 24-25 October 2017, Warsaw, Poland
- Piotr Bazydło, "Wykrywanie spamu na podstawie implementacji SMTP" ("Spam detection on the basis of SMTP implementation"), KSTiT 2017, National Symposium on Telecommunications, Information and Communication Technologies, 13-15 September 2017, Warsaw, Poland[1]
- Piotr Białczak, "Aktualne projekty badawczo-rozwojowe CERT Polska" ("Current research and development projects of CERT Polska"), Polish National Cybersecurity Centre Partners meeting, 11 October 2017, Warsaw, Poland
- Maciej Kotowicz, Jarosław Jedynak, "Peering into spam botnets", Virus Bulletin 2017, 4-6 October 2017, Madrid, Spain
- Jarosław Jedynak, Paweł Srokosz, "Use your enemies: tracking botnets with bots", Secure 2017, 21st Conference on Telecomunications and IT Security, 24-25 October 2017, Warsaw, Poland
- Paweł Pawliński, "Trying to Know Your Own Backyard (A National CERT Perspective)", FIRST Annual Conference 2017, 12-16 June 2017, San Juan, Puerto Rico
- (Lightning talk) Paweł Pawliński, "Malware configs for everyone", FIRST Annual Conference 2017, 12-16 June 2017, San Juan, Puerto Rico
- Paweł Pawliński, "Threat monitoring - a national CERT perspective", MNSEC 2017, 28-29 September 2017, Ulaanbaatar, Mongolia

[1] This presentation has a corresponding journal publication (DOI: 10.15199/59.2017.8-9.44, Piotr Bazydło and Adam Kozakiewicz "Wykrywanie spamu na podstawie implementacji SMTP" ("Spam detection on the basis of SMTP implementation"), in Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne, vol. 8-9, 2017, but only the presentation itself is officially reported, since due to an editing error the published paper lacks the required funding acknowledgement.

2.2.2 SHAD

Dedicated technical talks:

- Piotr Kijewski, David Watson, SISSDEN sensor network demo, ENISA-CTI EU, Rome, October 2017 (demo session)
- Piotr Kijewski, Building the SISSDEN honeypot sensor network, APWG.eu eCRIME, Porto, October 2017
- Piotr Kijewski, "Horizon 2020: SISSDEN" lightning talk, FIRST 2017 Conference, Puerto Rico, June 2017
- Piotr Kijewski, Lightning talk on the SISSDEN Project, NASK/CERT Polska SECURE 2016 Conference, Warsaw, October 2016 [in Polish]
- Piotr Kijewski, Jart Armin (CYBE), Presentation of the SISSDEN Project, APWG.eu eCRIME, Bratislava, October 2016

Other talks that included SISSDEN/SISSDEN related topics:

- Piotr Kijewski, "Effective Application of Threat Feeds for Victim Remediation", APWG Symposium on Global Cybersecurity Awareness Messaging, Vienna, August 2017
- David Watson, Stew Garrick, "Shadowserver: Introduction and Operational Capabilities" (included coverage of SISSDEN), Ministry of Defence Corsham, June 2017
- Piotr Kijewski, Jonathan Flaherty, SISSDEN overview at the "Understanding and effectively processing threat reports" training, AfricaCERT Training, Nairobi, May 2017
- Piotr Kijewski, "Zbieranie śmieci w sieci: przegląd działalności Fundacji Shadowserver" (included coverage of SISSDEN), OWASP Poland meetup, Warsaw, April 2017 [in Polish]
- Mark Chaffe, "Old man yells at cloud: stories of so called "big data" and "devops" (included coverage of SISSDEN), Australian Cyber Security Centre Conference, ACSC 2017, Canberra, Australia
- Jonathan Flaherty, Presentation that included SISSDEN, National Cyber Security Centre UK, London, December 2016
- David Watson, "Shadowserver: Introduction and Operational Capabilities" (included coverage of SISSDEN), Cyber Defence Alliance event, London, August 2016
- Jonathan Flaherty, Presentation that included SISSDEN, Cyber Defence Alliance, London, July 2016
- Jonathan Flaherty, Presentation on Shadowserver reports that included SISSDEN, National Crime Agency, Coventry, July 2016
- David Watson, "Shadowserver: Updates and highlights from recent activities" (included coverage of SISSDEN), Honeynet Project workshop, San Antonio, May 2016

2.2.3 USAAR

- Johannes Krupp, Michael Backes and Christian Rossow, "Identifying the Scanners and Attack Infrastructure behind Amplification DDoS attacks", 23rd ACM Conference on Computer and Communications Security, Hofburg Palace, Vienna, Austria, October 24-28, 2016
- Johannes Krupp, Mohammad Karami, Christian Rossow, Damon McCoy, Michael Backes, "Linking Amplification DDoS Attacks to Booter Services", 20th International

Symposium on Research in Attacks, Intrusions and Defenses, Georgia Tech Hotel, Atlanta, Georgia, September 18-20, 2017

2.2.4 Montimage

Sissden related demos and presentations that have been done by Montimage:

- meetings with industrial partners, Thales and Orange;
- Mobile World Congress 2016 (stand hosted by BusinessFrance); and,
- EuCNC 2017 (stand hosted by NetWorld2020-SME-Workgroup).

These events allowed Montimage to present the SISSDEN project and demonstrate its probe specifically adapted to monitor honeypot and darknet network activity.

2.2.5 Eclexys

SISSDEN technical presentation and talks performed by Eclexys during M1-M18

- Friday 10 March 2017, Swissôtel Merchant Court, Singapore:
  Conference + Networking Reception:
  "Cyber-space and Cyber-crime in Switzerland and in Europe" by Prof. Angelo Consoli, Professor and Researcher, Head of Presentation of SISSDEN principles and their background ideas, the activities and the final project objectives to an audience of 85 attendees (list can be made available upon request).
- 15 June 2017, University of Applied Science of Southern Switzerland, department of innovative technologies:
  Lesson in the frame of the executive master: "MAS ICT System, Security and Cybercrime" which started in September 2016 and will last 3 years, followed by a thesis project. More information can be found at this link:
  http://www.supsi.ch/fc/offerta-formativa/advanced-studies/mas/ict-systems-security-cybercrime.
  A full evening (4 hours lesson) was devoted to the principles and activities in the SISSDEN project.
- 17 October 2017, World Trade Center 25th year anniversary conference:
  Presentation on Cyber-crime for companies and citizens, hosted by Hotel Principe Leopoldo, Lugano.
  Discussion of the impact of malware traffic on ISP infrastructure. SISSDEN principles and solution explained.
  220 participants from top management (C-level profiles).

2.2.6 CyberDefcon

- ITU Sibiu- Romania September 2017, Cyber Security in Romania, http://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Events/2017/CYBR/Cybersecurity-in-Romania.aspx
- ENISA CTI October 2017: Bonding EU Cyber Threat Intelligence, https://www.enisa.europa.eu/events/cti-eu-event
- *Planned event - Europol (Infrastructure Security) November 2017*

2.3 Dissemination to policy makers

On invitation of the EFA political group of the European Parliament, Ninja Marnau (USAAR) was invited to speak at a hearing on potential IoT security regulation. The hearing took place in the European Parliament on June 7, 2017. Mrs. Marnau presented extensive data from SISSDEN's research on structure and prevalence of IoT botnets and IoT-focused malware. She made suggestions regarding regulatory options for the EU including liability regulation for security quality standards and mandatory patches. She also emphasized the need for legal incentives for sharing of threat-data among European companies, researchers and CERTs.

2.4 Project promotion

2.4.1 NASK

Generic promotional materials

The project logo used in the proposal was a good, but low-quality design for initial use. In September 2016 it was professionally redesigned, with color, monochrome and inverted versions in multiple formats. The new logo is available to the project participants and has been consistently used in all dissemination activities since.

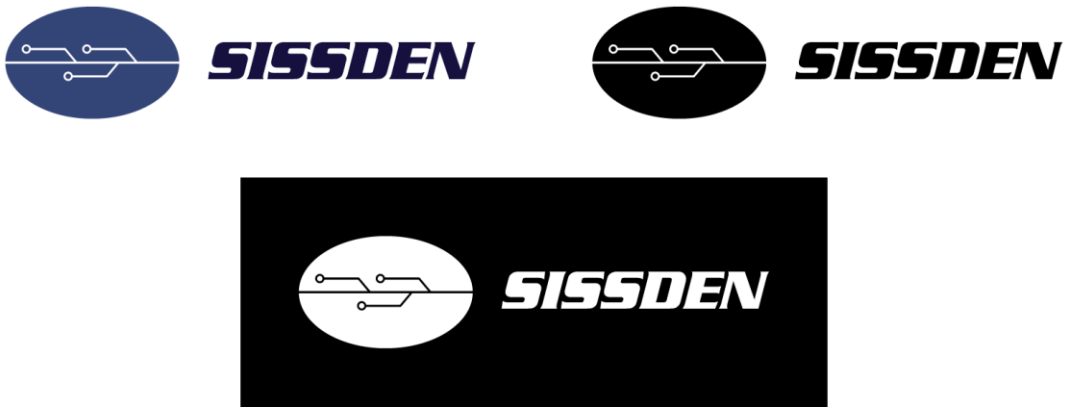

Figure 2.7: SISSDEN logo versions (normal, monochrome, inverted)

A general, high-level presentation of the project has been prepared in October 2016; it can be used as a basis for any presentations by project partners and is periodically updated. The newest version was developed for the events in the second half of October 2017. The current version is always available to partners in the project repository on Google Drive.

A roll-up poster has been designed and printed in March 2017. It has been used for a poster session during the Warsaw conference presenting the defense/security oriented work of research institutes (see section "General project presentations") and as an additional promotional element on several other occasions, e.g. the SISSDEN demo during the ENISA event in Rome. The source file is available to the consortium, so that a new poster can be made for any event if delivering the existing one proved logistically infeasible: so far this has not been necessary. A new version is being prepared currently, including information on the deployed infrastructure and updated technical information. The overlap of the contents of both posters is sufficiently small that using both in parallel at the same event would be feasible.

Moreover, NASK is currently preparing the project leaflet.

Press relations

So far two press releases were prepared by NASK (in Polish). The first one (May 2017) covered the project as a whole, stressing its utility for the security of the European network. The second one (October 2017) focused on the analytical modules prepared by NASK and was intended to promote the SISSDEN-related presentations at the SECURE conference. At the moment of writing NASK is working on a bilingual (Polish and English) press release announcing the deployment of the target platform and reaching the KPI of 100 sensors (expected before the review meeting).

One of the results of the first press release was the appearance of SISSDEN in public radio. The 18-minute long interview with Adam Kozakiewicz titled "Wirtualne garnki z miodem wabikiem na hakerów" ("Virtual honey pots a lure for hackers") was aired on May 23, 2017 at 19:10 in the science-focused Eureka series of Polskie Radio Program 1 – one of the most popular Polish radio stations (third place with 7,5% market share in the Radio Track Millward Brown results for the second quarter of 2017, 15-75 year old group). The interview was aimed at the general public interested in new technical developments, therefore the level of technical detail is relatively low. The interview is available at:
https://www.polskieradio.pl/7/5098/Artykul/1768643,Wirtualne-garnki-z-miodem-wabikiem-na-hakerow.

General project presentations

NASK has been actively promoting SISSDEN in various events. Where appropriate, detailed technical or scientific presentations were given (see previous section), while on other occasions a general presentation of the project was more appropriate, both as means of spreading the knowledge about the project and as an invitation for cooperation. Here following list reports these occasions with details on the focus and presenter involved:

- Adam Kozakiewicz, "SISSDEN – H2020 project on collection of actionable information", CESCP (Central European Cyber Security Platform) meeting, Warsaw, 27 October 2016 (general SISSDEN presentation).
- Adam Kozakiewicz, presentation of SISSDEN in the poster session of the conference „Cywilne instytuty badawcze wspierają bezpieczeństwo Polski" *(„Civilian research institutes suport Poland's security/defense")*, Warsaw, 27 March 2017.
- Adam Kozakiewicz "GDPR i nie tylko - wyzwania dla zespołów typu CSIRT" („GDPR etc. – challenges for CSIRT-type teams", NC Cyber Partners Meeting, Warsaw, 11 October 2017 (specifically referred to SISSDEN deliverable D2.2, includes a short general SISSDEN presentation).
- Adam Kozakiewicz "Secure Information Sharing Sensor Delivery Event Network", Motorola Solutions Innovation Showcase 2017, Keynote speech, Cracow, 25 October 2017 (general SISSDEN presentation).
- Piotr Bazydło "Secure Information Sharing Sensor Delivery Event Network", HIPEAC (European Network on High Performance and Embedded Architecture and Compilation) Stuttgart, 25-27 October 2017 (general SISSDEN presentation).
- Adam Kozakiewicz "Secure Information Sharing Sensor Delivery Event Network", ENISA CTI – EU Bonding Event, Rome, 31 October 2017 (general SISSDEN presentation).

2.4.2 SHAD

The promotional activities carried out by SHAD at conferences have led to a number of third parties declaring the willingness to host SISSDEN sensors. These range from National CERTs to private individuals (researchers). These volunteers are critical to building traction for the project, improve the dataset and diversity of sensor locations as well as meet declared project KPIs. Continuous outreach and dissemination activities also allowed expansion of SISSDEN report recipient base (including adding France and Bulgaria CERTs).

In addition, the SHAD outreach activities have resulted in contact being made with other EU projects operating in a similar space. For example, Piotr Kijewski was invited by the DiSIEM project[2] to sit on the External Advisory Board of that project. Data from SISSDEN for specific DiSIEM project partners could allow them to validate their SIEM research. Similarly, the RAMSES project expressed interest in providing their malware analysis capabilities to SISSDEN. Finally, the upcoming YAKSHA project that aims to establish honeypot sensors in low and middle income countries seems to be an interesting avenue for collaboration. SISSDEN will be exploring all the above potential collaboration activities.

The demo at the ENISA CTI event in Rome also met with interest of multiple event participants, hopefully opening up more collaboration paths with multiple entities in the future.

[2] http://disiem-project.eu/

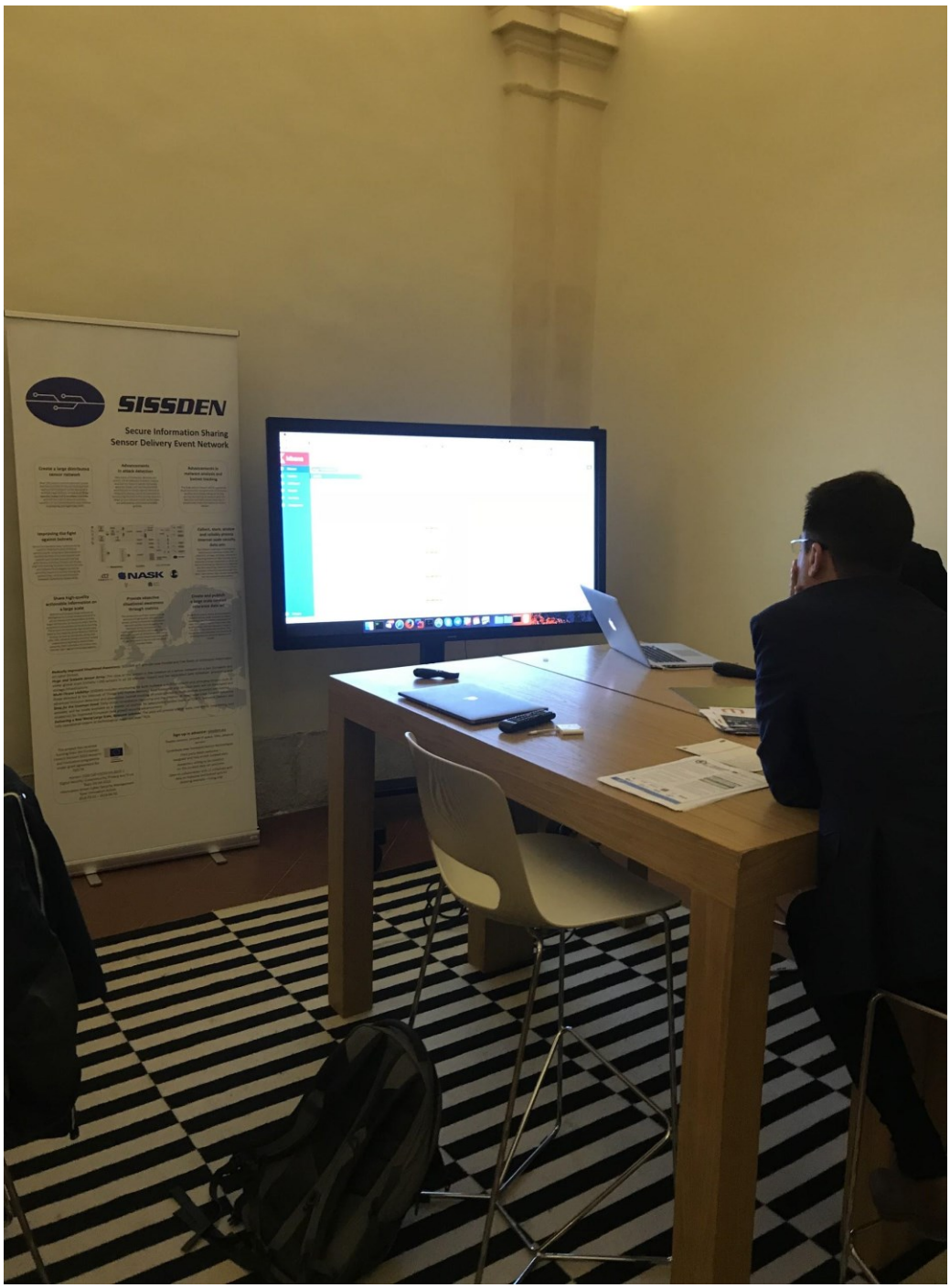

Figure 2.8: SISSDEN demo in Rome at the ENISA Bonding CTI event in October 2017

2.4.3 Eclexys

SISSDEN-related cybercrime meetings participated by Eclexys during M1-M18 are as follows:

- Friday 10 March 2017, Headquarter of StarHub (telco operator):
  StarHub Cyber Security Centre of Excellence: overview and round table.
  Round table discussing activities and new trends in traffic management and analysis for cybercrime.
- 14 March 2017, Canberra Innovation Network, Level 5, 1 Moore Street | Canberra
  Round Table and workshop with key Canberra based Cyber Security stakeholders, hosted by the Canberra Innovation Network and including key representatives of the

Australian National University, the University of Canberra and the Canberra Institute of Technology.
Discussion of the impact of malware traffic on ISP infrastructure.

2.5 Exploitation of early results

The launch of the first system in April with a small number of SISSDEN sensors has allowed for attack data to be collected on a regular basis. Since April, attacking IPs conducting brute force attacks have been reported to victims via Shadowserver's reporting system (strictly on a trial basis). The format of these new reports can be viewed on the news available at Shadowserver's Drone-BruteForce report page:
https://www.shadowserver.org/wiki/pmwiki.php/Services/Drone-BruteForce.

Additionally, for the pilot in M12 SHAD spampot sensors were deployed. The format for reports for those sensors can be found here:
https://www.shadowserver.org/wiki/pmwiki.php/Services/Spam-URL.

During the period of the project, SHAD's National CERT recipient user base has increased to over 90 National CERTs worldwide (exceeding SISSDEN expected KPIs for worldwide CERTs). Of the EU MS National CERTs, only Cyprus, which – to our knowledge – does not have a National CERT, is not on the recipient list. The number of direct recipients is now over 4000, exceeding expected SISSDEN KPIs.

Since the activation of the platform pilot in M12 (April) reports are being sent out on a trial basis. In M17 the sensor network has expanded thanks to the newly procured datacentre and has started collected data on a larger basis (with 44 sensors). By M20 we expect everything will be in place to start sending our reports on a daily basis, meaning that the SISSDEN project will achieve real impact in the security community by supplying it with a constant stream of actionable threat information.

The analysis modules developed as part of WP5 at NASK are put to direct operational use as soon as they reach sufficient maturity. First prototypes of the static malware analysis and botnet tracking tools are already used as a part of the daily operations of the team and provide vital intelligence on malware relevant to the constituency. Darknet analysis modules including an early prototype of the PGA analysis are continuously monitoring the large darknet address space available to NASK. While the results are not yet directly made available to the constituency yet, as the reliability of the data is being assessed, the outcomes already inform and guide operational activities of the team. Other modules (e.g. the SMTP dialect analysis) have also been used for this purpose, although their full-time deployment is still in the plans.

3 Key Performance Indicators

At proposal stage, SISSDEN has defined clear key performance indicators (KPIs) for the dissemination activity. The target values for each KPI were specified as end-of-project goals. The following table analyzes the progress achieved so far in each of the categories.

Dissemination tool / channel	KPI	Objective	Progress analysis
Website	Website Visits	500 monthly visits	With over 2500 visits in the last month, this KPI is fulfilled at this time.
Brochures	Number of leaflets / brochures produced	3	First leaflet in preparation, two more planned in the second phase of the project.
Conference / Journal publications	Number of peer-reviewed scientific publications	10	Due to the length of the editorial cycle and the main research work package (WP5) starting in M6, this KPI is more relevant to the second reporting period. However, with one high-quality journal paper accepted for publication, 2 peer-reviewed conference publications and several papers either submitted or in preparation the progress seems on track and the objective will likely be exceeded.
Press releases	Number of specialized press releases	6	2 press releases so far, third in preparation. The total number of press releases (any language) will probably be significantly exceeded, with the number of English language press releases close to the target.
Project showcases	Number of different demonstration videos produced	2	None so far. Following the successful demonstration during the ENISA CTI Bonding Event in Rome, the first video showcase is in early preparation stages.
Project blog	Number of posts	1 per month	The blog functionality has been recently added to the website and new posts are being submitted. The number of posts per month is not yet a valid metric, since the blog has not been operational long enough, but the objective is likely to be met or exceeded in the second reporting period. 3 posts have been published at the moment of writing with 2 more ready in the queue.
Presentations at events	Number of presentations showcasing project goals and achievements	15	Objective already exceeded, see the previous sections.

4 Dissemination and exploitation plan

The dissemination and exploitation plan of the SISSDEN project is an important activity to the consortium, including individual members' strategies designed to achieve a high level of interest in SISSDEN's aims and outputs. The effort in the initial stage of the project has focused on gaining interest and anticipation from a wide range of stakeholders. More specific details on the stakeholders identified are contained in D2.3 as part of the overall market strategy. Here dissemination activities are defined collectively as the intent is to reach a wide-ranging audience and to engage as extensively as possible. By encouraging feedback from a variety of sources, it will be possible to identify future partners and users on a large scale.

Dissemination is split into two main sectors: (i) dissemination to the scientific community (ICT Security community), to garner interest in SISSDEN results (curated reference data, knowledge and tools) within complementary research fields; and (ii) dissemination to the commercial community (Independent Systems Vendors (ISVs), investors, technology providers, SME's, public and private institutions, large Industry, CERTs, security practitioners, consultants, open source communities, etc.), to advance and promote SISSDEN capabilities and cyber threat intelligence to potential users.

In the launch campaign, M1 - M6 (milestone MS1), the start of the project was announced and further publicized via the project's website, (https://sissden.eu), as outlined above in Section 2.1 Website and Social Media. Moreover, social media accounts were created and are active (Twitter, Facebook, LinkedIn).

Now, part-way through the execution campaign (M6 to M24), all online formats are progressing well. The monitoring of visitors to the website has been encouraging to date with over 6,500 visits, representing a strong visual identity and platform for further dissemination and communication materials. For Twitter, there were 221 followers as of 26th October 2017, an indication that dissemination is progressing well and that SISSDEN is well on the way to creating an active online presence.

At this execution stage, the project is on aim to be further presented to specialized audiences from the scientific community, as well as industrial stakeholders and policy makers, with the objective of determining the stakeholders' needs and expectations. The intended medium is via conferences, scientific workshops, academic papers and scientific magazines. These aims are ongoing with strong representation in these fields by the consortium as outlined by partners' completed dissemination activities and further events planned during the latter stages of the execution phase and the final phase.

The commercial dissemination is focused on shorter, more generic but communication-driven items (web coverage, flyers, press releases, whitepapers, exhibition stands, magazines and websites aimed at security practitioners and stakeholders, etc.). These activities will become a higher priority towards the end of the execution stage M24 and continue to the end of the project and beyond.

During the final campaign, that lasts from M24 to M36 (milestone MS7), dissemination of the project results is of high importance and will be presented in different forums along with the established forums highlighted above.

The SISSDEN project has progressed a branding launch through its website (https://sissden.eu), with a visually distinctive logo and informative communications on

project progress, partner information, fact sheets, meetings, and documentation. The range of material available on the website will continue to grow as the SISSDEN project advances and its presence becomes more fully established. During the final campaign stage, and as marketing materials are created and produced, the website will be home to a range of leaflets, posters and brochures to promote the project's achievements and main outcomes in dissemination and networking events.

For SISSDEN partners the dissemination strategy is considered as a key vehicle for the possible commercialization as well as general exploitation of results. The methodology followed throughout is:

- Define what will be disseminated - the dissemination "products"
- Identify the target groups for dissemination
- Establish the appropriate source for the dissemination activities (in terms of roles and responsibilities)
- Raise public awareness about the project achievements through the most suitable means for communicating with the respective target groups.

Key Performance Indicators (KPIs) provide an effective means of monitoring progress in dissemination. The KPIs include website statistics, active event participation and quantity of publications, but also include measuring the value of the actions, that is, number of citations, number of "reads" of online materials and so on. The analysis of these KPIs will let SISSDEN partners steer dissemination to the most effective activities to obtain the highest impact and assure the project's sustainability. With the SISSDEN online presence now established these types of KPI's, during the latter stages of the execution phase, are important to meeting the desired dissemination aims.

Communication and exploiting the power of social networks is a key activity in the context of SISSDEN. The goal is to create a SISSDEN social community that will be flexible enough to engage its members during all of the project's noted periods (e.g. start of the pilot, release of tools, statistics on the results obtained). The project will engage with the identified community and carry out dissemination and exploitation objectives that include:

- Maintaining profiles in professional social networks such as LinkedIn, and Twitter. These will be used as direct communication channels with other professionals from relevant fields.
- Identifying the most appropriate social network communities that already exist in the framework of ICT Security. These communities will be approached in order to attract its members and subsequently enrich the SISSDEN community.
- The effectiveness of our actions will be presented during project management reports, and at the end of the project.

Communication activities will also target security practitioners, and be extended to the public at large. This will be achieved through communication actions to demonstrate to non-specialized audiences that SISSDEN is expected to bring added value in security, growth and job creation. It will be important, as well, to seek views from the public on the future of the European Union's policies in the area of ICT security. It is proposed that this type of inclusion and involvement will assist in the creation of a SISSDEN community consisting of people who will / may be interested in SISSDEN achievements and results.

5 Conclusion

The dissemination activity of the SISSDEN project is proceeding properly. General promotional activity exceeds the expectations set out in the project Key Performance Indicators. Scientific dissemination is also active and expected to intensify in the second part of the project, since research results are already available and growing. Exploitation of early results is ongoing. Plans for further exploitation and dissemination have been updated.