



Project Deliverable

D8.1

Internal and External IT Communication Infrastructure

Project Number	700692
Project Title	DiSIEM – Diversity-enhancements for SIEMs
Programme	H2020-DS-04-2015

Deliverable type	Report
Dissemination level	PU
Submission date	30 th November 2016

Responsible partner	FFCUL
Editor	Alysson Bessani
Revision	1.0



The DiSIEM project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700692.

Editor

Alysson Bessani, FFCUL

Contributors

Alysson Bessani, FFCUL

Ignacio Robla, ATOS

Elsa Prieto Perez, ATOS

Executive Summary

This deliverable marks the launch of the internal and external DiSIEM IT communication infrastructure. The internal infrastructure includes the establishment of mailing lists, and a file repository with version control, while the external infrastructure corresponds to the official dissemination materials and channels, including the project website. The report also describes the procedures and policies for dissemination and communication in the DiSIEM project. Furthermore, we define the means for communication to external target groups including marketing measures and communication channels.

Table of Contents

1	Introduction.....	7
1.1	Organization of the Document.....	7
2	External Dissemination and Communication.....	8
2.1	Roles and Responsibilities.....	8
2.2	Target Users.....	8
2.3	Key messages.....	8
2.4	Visual identity.....	9
2.5	Communication Policy.....	10
2.5.1	IPR conflict in publications.....	10
2.5.2	Disclosure of PU deliverables.....	10
2.5.3	Implementation of open green access.....	11
2.5.4	EU disclaimer and EU emblem.....	11
2.6	Key Performance Indicators.....	11
2.7	Communication and dissemination materials.....	13
2.8	Communication and dissemination channels.....	15
2.9	Project website.....	16
3	Internal Communication Infrastructure.....	18
3.1	Project mailing lists.....	18
3.2	Instant messaging.....	18
3.3	Tele-conferences.....	18
3.4	Project repository.....	18
4	Summary and Conclusions.....	20
	References.....	21
	Appendix: A very brief introduction to Git.....	22

List of Figures

Figure 1 DiSIEM visual identity.	9
Figure 2 DiSIEM logo and visual identity.....	9
Figure 3 DiSIEM leaflet. The leaflet is available at http://disiem-project.eu/wp-content/uploads/2016/12/DiSIEM-leaflet.pdf	14
Figure 4 Project website.	17

List of Tables

Table 1 KPI for dissemination and communication activities.....	12
Table 2 Important git commands.....	22

1 Introduction

This document describes the procedures, policies and infrastructures for dissemination and communication activities in the DiSIEM project.

Dissemination is mostly related with the knowledge diffusion to the peers, usually other researchers and organisations working in the area of the project. Typical forms of dissemination are the website, presentation at a scientific audience, etc.

Communication is aimed at non-specialists, a wider audience, including stakeholders and end-users interested in the innovations produced during the project. Typical examples of communication activities are press releases spread in general public media at the start of the project, local workshops targeted at audiences for which the action is of interest, brochures/leaflets to explain the action's work, etc.

This report focuses on the external communication and dissemination, as well as the internal communication infrastructure for the DiSIEM project. The external communication and dissemination infrastructure subsumes the means and tools for communication of the project to external target groups including conferences, marketing measures and communication channels. This includes also the definition of clear policies for using and producing communication and dissemination materials. The internal communication infrastructure of DiSIEM includes the mailing lists, tele-conference and instant message tools, and an internal file repository with version control.

1.1 Organization of the Document

This short report contains three chapters (besides this introduction). Chapter 2 describes the external communication and dissemination procedures and channels of the project. Chapter 3 describes the internal IT infrastructure of the project. Finally, we conclude and summarize the report in Chapter 4.

2 External Dissemination and Communication

In this chapter we define the main procedures, materials and channels for realizing both dissemination and communication activities during the project.

2.1 Roles and Responsibilities

As the project coordinator, FFCUL is responsible for leading the communication and dissemination task of DiSIEM. However, all partners have PMs in this WP8 and it is expected that they contribute with communication and dissemination activities of DiSIEM by raising awareness about the project within their organization and community, and giving talks in conferences and workshops about the project results. In terms of effort, we it is expected these activities take between 1-2 PMs per partner during the three years of the project.

2.2 Target Users

The dissemination and communication strategy of the project is divided in two main phases. On the first year of the project we are more interested in raising awareness about it, so communication activities will be privileged. On the second and third years of DiSIEM our focus shift more to dissemination as we expect to have already important results to disseminate.

Given this strategy, our targets will also change: at the beginning is more general audience, then we can try to reach more technical people, and finally we tend to exploitation/adopters.

2.3 Key messages

There are some key concepts and messages of DiSIEM that need to be stressed in every dissemination and communication activity. They are:

- DiSIEM is an innovation project that aims to improve the capacity of SIEMs to deal with modern/advanced persistent threats;
- DiSIEM will produce several components that (in principle) can be integrated in any existing SIEM systems;
- The project will exploit OSINT data (security feeds, indicators of compromise repositories, blogs, social networks, etc.) and machine learning techniques to detect, inform and propose actions to deal with novel threats against a cyber infrastructure;
- The project will equip existing SIEMs with the capability of evaluating diverse configurations of monitoring and protection devices, novel application-based misuse detection and secure cloud-based even archival.

2.4 Visual identity

We established the visual identity of the project, including the project logo (with variants) and templates for presentations and deliverables (used in this document). Figure 1 presents the basic iconography of the project logo.

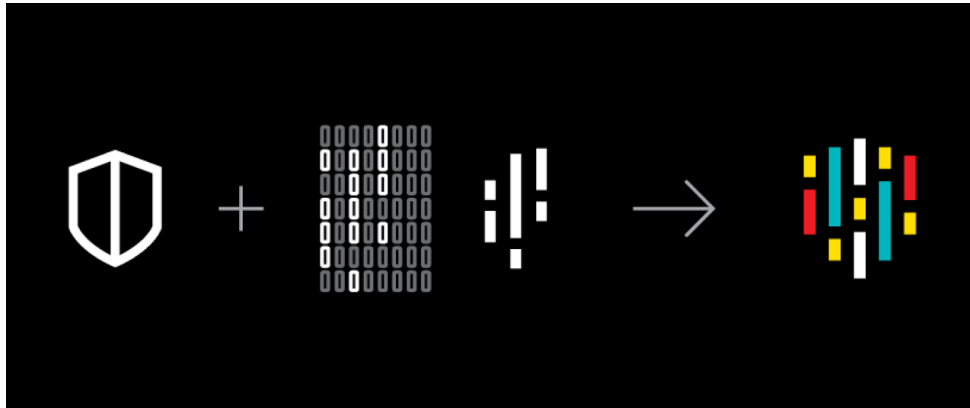


Figure 1 DiSIEM visual identity.

The project's brand was inspired by visually connecting three concepts that define DiSIEM: cyber-security (represented by a shield); data streams (represented by vertical lines with different sizes); and diversity of inputs (represented by the multi-coloring of the vertical lines).

Figure 2 presents the final project logo within the colour and backgrounds that are recommended for keeping a consistent visual identity for DiSIEM.



Figure 2 DiSIEM logo and visual identity.

All communication and dissemination activities of the project should try to comply with logo and colours defined in our visual identity. In order to preserve coherence and harmony throughout the communication, some typography was selected, and it's recommended to be used in all graphic pieces:

- Titles: Furore
- Text: Gotham

More details and logo variants are available on the project repository for the partners to inspect.

2.5 Communication Policy

The project consortium implements a publication process to ensure the quality of deliverables and of any other external publication. It ensures that the IPR (Intellectual Property Rights) of the partners are adequately verified before the dissemination of any project results.

This section defines the policy for dissemination of project results and deliverables. Some of the information in this section contains minor revisions on the plan described in Part B of the DiSIEM Grant Agreement (Section 3.2.2).

2.5.1 IPR conflict in publications

For general dissemination activities, the partners need to communicate the consortium about the dissemination **at least one week** before it is made public. In the particular case of conferences and journals, the partners should disseminate a draft of the paper before submission. In the worst case, an accepted paper must be disseminated to the consortium members at least one week before the camera-ready version is submitted.

The aforementioned communication must be done through the project mailing list (*disiem-technical*, see Section 3.1) and the draft of the paper/presentation/article must be made available on the relevant WP directory on the project repository.

Once the paper, presentation, or article is made available to the consortium, partners have the chance to review the content to identify potential conflicts with confidential information. Partners have one week to express their objection to the publication. Silence is considered a tacit approval.

2.5.2 Disclosure of PU deliverables

For official project deliverables, there will be a specific process of review before the submission to EC. This guarantees that the qualitative targets are reached with regards the technical content, the objectives of the project and adhere to

formal requirements established in the Grant and Consortium Agreements. The review process should be done in accordance with the formal review process defined in D9.1 (Project Quality Plan).

After the submission of a deliverable to the EC, the document/software package will be made available on the DiSIEM website within one week (for public deliverables). We will clearly mark each deliverable as “*Under Review*” or “*Approved*” in the website.

2.5.3 Implementation of open green access

The DiSIEM project is fully committed with open green access of publications. This means that any paper reporting work supported by DiSIEM must be published also in an open-access repository. As with several H2020 projects, we plan to have the pre-print of all papers on the Zenodo EU-funded repository [Zenodo]. The version on this repository will be linked to the project webpage.

2.5.4 EU disclaimer and EU emblem

The following statements must be added to every dissemination and/or communication item.

For presentations, blog posts or webpages:



The DiSIEM project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700692.

For papers, a shorter version suffices:

This work is supported by the European Commission through the H2020 programme under grant agreement 700692 (DiSIEM).

2.6 Key Performance Indicators

Communication and dissemination activities must be measured by key performance indicators (KPIs) defined by the consortium. These indicators are intended to demonstrate how effective communication and dissemination activities are, in terms of quantity and quality. On one hand, the quantity is measured by controlling the frequency of the communication activities. On the other hand, the quality is evaluated with the specialized research capacity demonstrated in the resulting impact.

Table 1 describes the KPI proposed in the project, which will be monitored, and specific actions will be defined accordingly.

Table 1 KPI for dissemination and communication activities.

Category	Quantitative KPIs	Qualitative KPIs (Optional)
Branding		
Leaflets	Number of leaflets produced	Type of events where the leaflets were handed out (e.g., trade fair, research conferences)
Leaflets	Number of events where leaflets were handed out	
Press releases	Number of published PR Impacts of published PR (in other media) Publication in other media (newsletters, clusters website)	
Publications		
Papers	Number of papers produced	Conference rank where the paper has been accepted
Articles	Number of published articles	
Blogs, specialized webs	Number of mentions in specialized blogs, webs of the partners	
Events		
Conferences	Number of attended third party conferences Size of audience	Type of audience
Workshops	Number of attended third party workshops Size of audience Number of organized workshops Size of audience	Type of audience
Events	Number of attended third party events Size of audience	Type of audience
Webinars	Number of organized webinars Size of audience	Type of audience
Social media		
Website	Metrics of the website, including the number of visitors, countries of the visitors, and number of downloads of dissemination files	
Social accounts	Social network metrics such as number of followers, number of tweets with @disiemproject, #DiSIEM, #disiemproject, and number of reactions in the feeds of @disiemproject account	
Face-to-face contacts		
Face-to-face contacts	Number of contacts with potential target users	Relevance of the contact with target users

Collaboration with R&D projects		
Clusters	Number of clusters to belong Number of developed activities inside the clusters	Type of collaboration
Actions with other projects	Number of actions with other projects	Type of collaboration
Mentions		
Mentions in third party media	Number of mentions to DiSIEM project in other social media (e.g., twitter, facebook) external to DiSIEM partners; Number of mentions in websites external to DiSIEM partners	

2.7 Communication and dissemination materials

We prepared seven materials for communicating the overall ideas of the project.

- **Announcement letter.** A short document informing about the start of the project.
- **Press release.** An official statement issued to disseminate to the press and partners institutions.
- **Leaflet.** Information material to raise awareness on project targets, opportunities and partners, which can be distributed via e-mail or directly in meetings/conferences. The leaflet is presented in Figure 3.
- **Short project description.** A very short introduction about the objectives and expected contributions of the project. To be included in partner's websites, booklets, etc.
- **Project presentation.** A half-hour presentation about the project that can be used by the partners in workshops, innovation boards, etc.
- **Project video.** In the next months, we plan to have promotional video of the project and one newsletter of the project each six months.

DIVERSITY ENHANCEMENTS FOR SECURITY INFORMATION AND EVENT MANAGEMENT

PROJECT KEY FACTS

Although a fundamental tool in modern Security Operation Centres, current SIEMs have many limitations on the methods and means they use to collect events, store data and report information.

The cornerstone of the DiSIEM project is the use of **scalable information extraction and machine learning algorithms** and tools to extract information from multiple data sources (monitored infrastructures, open-source intelligence, social networks, security news feeds, advisory organisations, etc.) and feed SIEMs with it for threat prediction and enhanced risk assessment, aided by probabilistic methods and advanced visualisation tools.

DiSIEM will also equip existing SIEMs with the capabilities of **evaluating diverse configurations of monitoring and protection devices, novel application-based misuse detection and secure cloud-backed long-term archival** of selected events.

The DiSIEM enhancements:

- are **compatible with all existing SIEMs** that support custom connectors and provide access to the event store.
- **can be used either individually or together** (thus broadening the project results impact scope).
- **will be validated in production environment** by three large partner organisations: an electricity utility (EDP), a lawyer services company (Amadeus) and a SIEM and security provider (AtoS).

The DiSIEM exploitation business model considers components that will be supported by partners offering services to SIEM operators (operating HR, AOCs), internally by partners operating large SIEMs (Amadeus, EDP), and by startup initiatives created primarily from the research and development partners (FFCCSA, CITY, Fraunhofer IIS).

CURRENT CHALLENGES TO SECURITY MANAGEMENT SYSTEMS

Organizations currently monitor and manage the security of their infrastructures by setting up Security Operation Centres (SOC) to make security-related decisions. A SOC obtains an integrated view of the monitored infrastructure by employing a Security Information and Event Management (SIEM) system. These are complex systems that incorporate the functionality to collect logs and events from multiple sources, correlate them and then produce summarised measurements, trends and different types of visualisations to help system

administrators and other security professionals. Despite their widespread use and the recent impressive market growth, current SIEMs still have many limitations:

1. **Their threat intelligence capacity is still in its infancy.** Consequently, they are unable to automatically recognize novel threats that may affect the monitored infrastructure, requiring considerable human intervention to adapt and react to changes in the threat landscape.
2. **They can show any "low-level" data related with the events received, but they have little "intelligence" to process this data and extract high-level information.** These low-level data are difficult to translate to high-level metrics for senior C-level managers.
3. **The data visualisation techniques are limited and rudimentary.** This can seriously impact the ability of SOCs to deal with incidents as they happen.
4. **The event correlation capabilities are as good as the quality of the events fed to it.** Imprecise events and alarms generated by imperfect monitoring devices will be taken as correct by the SIEM and the uncertainties associated with these events are never reported.
5. **They are incapable of retaining the collected events for a long duration.** This limits their use in conducting forensic investigations in the long run.

The DiSIEM project aims to address these limitations by complementing existing SIEMs with a set of components for accessing diverse data sources, feeding enhanced events to the SIEM and generating improved reports and metrics to better support the security operation centres.

DiSIEM OBJECTIVES

Instead of proposing novel architectures for future SIEMs or modifications to existing ones, the project will address the aforementioned limitations by extending current systems, already deployed in production, leveraging their built-in capacity for extension and customisation. The core idea of the project is to enhance existing SIEM systems with several diversity mechanisms, representing five main advances to the state of the art:

1. **Integrate diverse OSINT (Open Source Intelligence) data sources available on the web,** such as the NCTA National Vulnerability Database, vulnerability and patch databases offered by vendors; threat intelligence data shared by organisations; security blogs and data streams from social networks (e.g., Twitter, Facebook, LinkedIn); collaborative platforms used in the Dark Web (e.g., Pastebin); search engines and online repositories; standards-based indicators of Compromise, and many others. **This data needs to be fetched, analysed, normalised and fused** to identify relationships, trends and anomalies, hence helping in the

EXPECTED RESULTS

The main results of DiSIEM will be the design and implementation of the several components illustrated in the figure:

- **Techniques and tools for analysing, evaluating and guiding the optimal deployment of diverse security mechanisms** in the managed infrastructure, including multi-level risk-based metrics (employed in all blue boxes in the figure).
- **An OSINT-based security threat predictor** (the "OSINT Data Analysis and Fusion" box).
- **A rich set of enhanced interactive visualisations** to improve the quality of the decision support of security analysts (the "Visualisation and Analysis Tools" box).

- **A framework for deploying diverse and redundant sensors** (part of the "Diversity-Enhanced Monitoring" box).
- **A novel application-based anomaly detector** for complementing other sensors and detect frauds in application servers (part of the "Diversity-Enhanced Monitoring" box).
- **Components that allow for long-term event archival in diverse clouds** (the "Cloud-of-Clouds Event Archival" box).

By choosing the extension approach instead of developing a new SIEM or requiring changes to existing ones, DiSIEM is expected to foster innovation much faster, and to maximize the impact and business potential of its results.

METHODOLOGY

The DiSIEM project brings together research in several technologies, including machine learning, probabilistic models for security assessment, application behaviour monitoring, novel methods for data visualisation, cloud storage and security log-performance metrics. The figure below presents the five phases of the project methodology and the activities that will be carried on in these phases.

To achieve the DiSIEM objectives, a first step of the project is to study the most prominent SIEMs in detail, to assess their extensibility features. DiSIEM will identify how these features should be used and compare the extension capabilities among the SIEMs.

The first step enables the definition of a reference architecture to guide the integration of the novel components to a SIEM. This architecture will define the key components and responsibilities of the developed enhancements, ensuring they can easily work together.

In parallel with this activity, an in-depth analysis of the state of the art will be conducted in all technical areas of the DiSIEM project. This will produce detailed reports summarising the findings and defining the requirements for the new components. After this stage each component will be developed, mostly independently, leading to the production of detailed design documents that are agreed on by all involved partners. Finally, the enhanced tools and mechanisms will be implemented and integrated in the existing SIEMs.

All developed components will be internally tested and validated by each partner, by following standard testing and quality assurance methodologies employed in software development. After this phase, all components will be made available to the partners that operate SIEMs. These will define a validation plan for the components and will integrate them to their SIEMs, first on a controlled environment and then on production.

CONSORTIUM

The DiSIEM consortium brings together a unique combination of academic and industrial experts in diverse fields to realize the vision of the project.

Project Coordinator: Professor Alysson Bessani
 Departamento de Informática
 Faculdade de Ciências - Universidade de Lisboa
 Edifício C6 - Piso 3, Campo Grande - 1649-016 Lisboa - Portugal
 Email: alysson@ciencias.ulisboa.pt / Tel: +351 21 790 03 94

Figure 3 DiSIEM leaflet. The leaflet is available at <http://disiem-project.eu/wp-content/uploads/2016/12/DiSIEM-leaflet.pdf>.

All communication material will be available in the project webpage, in the "Publications and Deliverables" section.

2.8 Communication and dissemination channels

Finding the best channels for communicating and disseminating the project and its results is crucial for broadening the impact of DiSIEM. These available channels include the participation in academic and industrial events such as conferences, workshops, meetings and fairs, the press, partner's blogs and newsletters, among others. The project website (described in the next section) should be the main concentrator of all these activities.

Below we list the main channels considered in DiSIEM.

- **Project web page.** Channel to disseminate information on the project and its impact on interested parties worldwide (e.g., news such as conference talks, publications and deliverables, involved partners, links, etc.)
- **Project newsletter.** Starting at month six, we plan to summarize the main achievements of the project every three months in a newsletter to be published on the webpage and sent to interested parties.
- **Partner's blogs and newsletters.** Several partners maintain blogs, magazines and newsletters that should be used to communicate the project. To cite just some:
 - Ascent (<https://ascent.atos.net/>) (Atos Website for Technical and Research contents, designed to share with Atos partners and customers innovation and thought leadership on emerging trends in many areas. This publication is linked to the Atos scientific community in charge of identify the most innovative technological trends.
 - Twitter account: @AtosES;
 - AXIA: Atos Spain Corporate magazine (only edited in Spanish). The aim of "axia" is to reinforce Atos corporate image and effectively communicate the company's knowledge and success stories in the Information Technology market;
 - Ascent Journey: series of yearly publications, a comprehensive document from Atos where we present our predictions and vision for technology that will shape business through to the next 3 years;
 - DigitalMR blog (<http://www.digital-mr.com/blog>) and newsletter: (<http://www.digital-mr.com/archive/archives/category/Social-Media-Research-Digest/page/1>);
 - All partners also have their institutional webpages, and it is expected that these channels are used for communicating DiSIEM ideas and results.
- **Academic events.** Academic events are important for reaching the scientific audience. In DiSIEM, the dissemination activities includes the attendees of some of the top conferences in security and dependability, such as IEEE/IFIP Dependable Systems and Networks, IEEE Security & Privacy, IEEE International Symposium on Software Reliability Engineering, ACM Computer and Communication Security, USENIX Annual Technical Conference, European Symposium on Research in Computer Security and USENIX Security, to cite just some. In addition visualisation related activities will be presented in top venues such as

IEEE VIS, EuroVis, and the more security oriented IEEE Symposium on Visualisation for Cyber Security.

- **Industry events.** For the technical and industry audience, we envision the promotion of DiSIEM and its results in industry-focused meetings and fairs such as Web Summit, InfoSec, CeBIT, Cyber Security for Energy and Utilities, among others. Selected results of the project can also be presented in international industry-focused conferences about social media, such as iStrategy Conference, Social Media World Forum, Innovate, and The Social Media Strategies Summit.
- **Journals and magazines.** There are many journals and magazines that can be used for disseminating the ideas of the project. We want to have at least one paper for disseminating the overall ideas of the project in a magazine such as IEEE Security & Privacy magazine and Computer & Security. Besides that, it is expected that the partners publish some of their scientific work in high-reputable academic journals.
- **Social networks.** We recently created a twitter account [@disiemproject](https://twitter.com/disiemproject) to disseminate main the achievements of the project and as an additional tool to create a community around the project. This account is under responsibility of City, but other partners such as ATOS and FFCUL can also post using this account through the use of Tweetdeck [Tweetdeck].
- **Press.** Every partner is responsible to try to reach the (technical) press for disseminating the DiSIEM project and its results, thus broadening the audience of the communication activities.
- **Liaison with related research projects.** A final channel that we plan to explore is the possible collaborations with other H2020 projects such as SUPERCLOUD, CIPSEC, COMPOSITION, and ANASTACIA, to cite just some.

2.9 Project website

The DiSIEM project website is the most important dissemination channel of the project. FFCUL is the main responsible for building, maintaining and updating the website, which is hosted in University of Lisbon, Faculty of Sciences premises. The website is accessible since the end of October 2016 though the addresses www.disiem-project.eu, disiem-project.eu, and disiem.lasige.di.fc.ul.pt.

Figure 4 presents the initial page of the project webpage. As can be seen, the main sections of the website are:

- **The Project.** This section presents an overview of the key facts, objectives, main innovation vectors, and the methodology we want to employ.
- **News.** This section contains all the news of the project. We want to use this section also to publish short blog-like posts informing about project key results and milestones.
- **Consortium.** This section lists project partner institutions together with key persons in each one of them.

- **Publications.** This section lists, in separated sections, the scientific publications, deliverables (reports), and the communication material (e.g., leaflet, newsletters, overview documents) of the project.
- **Contact.** This last section lists the contact of all partners and means to easily contact the project coordinator.

This structure can be easily changed in case of need as the webpage is built using the Word Press content management system [Word Press].

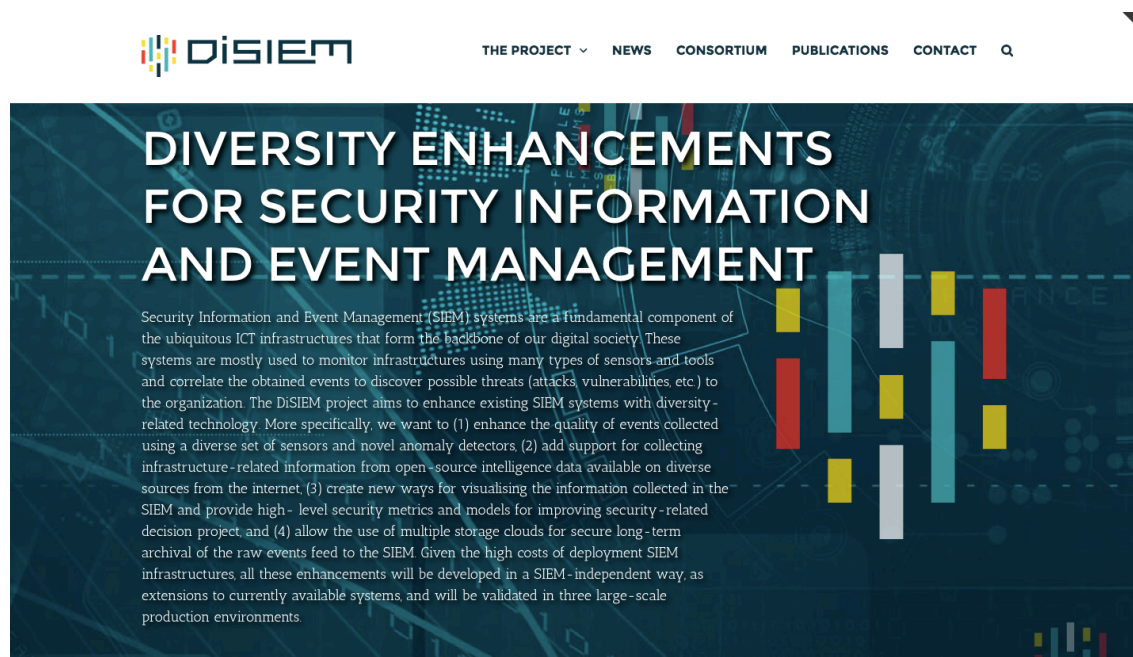


Figure 4 Project website.

3 Internal Communication Infrastructure

This chapter describes the main internal communication infrastructure of the DiSIEM project. In particular, we detail the most important infrastructures for collaboration: mailing lists, instant messaging, tele-conferences and the project file repository.

3.1 Project mailing lists

We have two mailing lists for internal communication on the project, one for technical discussions (disiem-technical@listas.di.ciencias.ulisboa.pt) and another for administrative issues (disiem-administrative@listas.di.ciencias.ulisboa.pt). Any partner can subscribe members in these lists at any time by asking the project coordinator.

3.2 Instant messaging

The project coordinating team did not defined a specific tool for instant messaging as our experience in previous project is that few people stay online in these private chat tools. Therefore, partners are using mostly Skype [Skype] for exchanging messages on real time. Other possible tools are Gtalk/Google Hangout [Hangouts]. Every person working on DiSIEM maintains its Skype and Gtalk contacts on the `contact-list.csv` file on our project repository.

3.3 Tele-conferences

Every teleconference meeting will have a host partner, whom is responsible for setting up the tele-conference (telco) system and invite the other participants. Currently we are hosting telcos using both Skype corporate [Skype] and WebEx [WebEx], but Google Hangouts [Hangouts] is also a possibility. In any case, it is expected that the host partner send the invitation to all other by email using either the project mailing list or individual emails found in the contact list on the project repository.

3.4 Project repository

For this project, we host the files with version control based on GIT. In particular, we setup a GitLab server [GitLab] on the FCUL infrastructure. This server hosts a master repository that other partners can clone in their hosts and contribute to.

The server repository can be found at <http://git.lasige.di.fc.ul.pt/root/DiSIEM> (via web), or directly through a git URL <git@git.lasige.di.fc.ul.pt:root/DiSIEM.git>. Accessing this server requires an account created at FCUL, and an explicit invitation by the project coordination. Any partner can ask access at any time by contacting the project coordinator.

The project repository is organized with the following main directories:

- **00-Project-Info.** Communication and dissemination material about the project, including the logo, leaflet, templates and other materials described in Section 2.7;
- **01-Official-Documents.** This directory contains the Grant Agreement, Submitted deliverables, Published papers and any other official documentation related with the project;
- **02-Workpackages.** Here we have one subdirectory for each work package of the project. WP coordinators must use this space as a repository for WP work;
- **03-Meetings-Telcos.** Stores information about all physical meetings and telcos done in the project, separated per year and meeting;
- **04-Other-Info.** This is directory for storing other stuff, such as general related work about the project.

If the need arises, we can change this structure for accommodating further needs.

We provide a short introduction to Git in the appendix of this report as a reference to project partners.

4 Summary and Conclusions

This deliverable described the DiSIEM internal and external infrastructure for communication and dissemination. In particular, we defined the channels, materials and procedures for executing external communication and dissemination activities in the project. Regarding the internal communication infrastructure, we describe all the fundamental elements for establishing a successful collaboration: mailing lists, telco and instant message tools, and the project repository.

With all these procedures and infrastructures set, we now have the tools and methods for communicating and disseminating the DiSIEM and its innovations.

References

[Chacon and Straub 2014] Scott Chacon and Ben Straub. Pro Git. 2nd Edition. 2014. Freely available at <https://git-scm.com/book/en/v2>.

[GitLab] GitLab open source git server. <https://about.gitlab.com/>. Accessed in November 2016.

[Hangouts] Google Hangouts. <https://hangouts.google.com/>. Accessed in November 2016.

[Skype] Skype. <https://www.skype.com/>. Accessed in November 2016.

[SVN] Apache Subversion. <https://subversion.apache.org/>. Accessed in November 2016.

[TweetDeck] TweetDeck. <https://tweetdeck.twitter.com/>. Accessed in November 2016.

[WebEx] Cisco WebEx. <https://www.webex.com/>. Accessed in November 2016.

[Word Press] Word Press Content Management System. <https://wordpress.org/>. Accessed in November 2016.

[Zenodo] Zenodo Repository. <https://zenodo.org>. Accessed in November 2016.

Appendix: A very brief introduction to Git

In the following we describe some of the basic commands for operating a command-line git tool and suggest some graphical interfaces for using git on different operating systems. Our purpose here is not to be extensive but provide some basic information for partners' non-familiar with this tool to use the repository.

Git is a version control system similar to svn [SVN] The big advantage of git is that it is distributed: a "master" repository can be cloned, modified, locally committed and latter on pushed for integrating the updates to the master repository. When compared with svn, the big difference is that updates committed to the repository are done only locally, and thus need to be pushed to the master repository (hosted at FCUL in case of DiSIEM). **Error! Reference source not found.** presents some basic commands for operating the DiSIEM repository. For more information, we refer the reader to [Chacon and Straub 2014].

Table 2 Important git commands.

Action	Command
Cloning remote "master" repository	<code>git clone git@git.lasige.di.fc.ul.pt:root/DiSIEM.git</code>
Inspect (and change) repository configurations	<code>git config -l</code> (to list configs) See other options for values
Synchronize local repository with master repository (master -> local)	<code>git pull</code>
Status of local repository	<code>git status</code>
Status of master repository	<code>git remote status</code>
Add or Update files	<code>git add, git commit</code>
Synchronize master repository with local repository (local -> master)	<code>git push origin master</code>

There are some graphical interfaces for using git, we recommend the following two for the partners less inclined to use the command line:

- <http://www.syntevo.com/smartgit/> (Windows, MacOS, Linux)
- <https://tortoisegit.org/> (Windows)
- <https://gitextensions.github.io/> (Windows)