A CIP-PSP funded pilot action
Grant agreement n°325188

Deliverable	**D4.4 Publicly Accessible Database of Botnet Metrics**
Work package Due date Submission date Revision Status of revision	WP4 Evaluating and Incentivizing Botnet Mitigation 31/07/2015 31/07/2015 Final
Responsible partner Contributors Peer reviewer	Beatriz Gallego-Nicasio Crespo (ATOS) Elsa Prieto (ATOS), Tigran Avanesov (ULUX), Jan Kohlrausch (DFN-CERT), Paolo Roccetti (EII) Jonathan P. Chapman (Fraunhofer)
Project Number Project Acronym Project Title Start Date of Project	CIP-ICT PSP-2012-6 / 325188 ACDC Advanced Cyber Defence Centre 01/02/2013

Dissemination Level	
PU: Public	X
PP: Restricted to other programme participants (including the Commission)	
RE: Restricted to a group specified by the consortium (including the Commission)	
CO: Confidential, only for members of the consortium (including the Commission)	

Version history

Rev.	Date	Author	Notes
01	02/06/2015	Beatriz Gallego-Nicasio Crespo (ATOS)	First draft
02	12/06/2015	Beatriz Gallego-Nicasio Crespo (ATOS) Elsa Prieto (ATOS)	Revision of the incentives model
03	29/06/2015	Beatriz Gallego-Nicasio Crespo (ATOS) Tigran Avanesov (ULUX), Jan Kohlrausch (DFN-CERT)	Addressing comments from peer review in section 1, 2 and 5. Finalizing sections 3 and 4.
04	14/07/2015	Beatriz Gallego-Nicasio Crespo (ATOS)	Addressing comments from peer review in sections 3 and 4.
05	17/07/2015	Paolo Roccetti (ENG)	Revising and updating section 4.2.1.
Final	17/07/2015	Beatriz Gallego-Nicasio Crespo (ATOS)	Generation of the final version

Glossary

ACDC	Advanced Cyber Defence Centre
CCH	Centralized Data Clearing House
CP	Community Platform
DAM	Data Access Manager (in the Community Platform)
FS	Financial Services
JSON	JavaScript Object Notation
WP	Work Package

Table of contents

Table of figures

Table of tables

1. Executive summary

Robust comparative cyber security metrics are a key to providing executive level management a quantifiable and measurable solution to prove the effectiveness of their implemented governance approach, and justify the return of the ever growing investments in IT security. Moreover, turning these metrics into standard available benchmarks would increase transparency, contributing to reduce market failures associated with information asymmetry, usually controlled by certain groups of stakeholders (e.g. antivirus providers). However, reputational costs associated to underperformance, e.g. in preparedness against cyber-attacks or showing weaknesses in coping with cyber threats, raise sensitivity concerns of organizations to disclose any security related information. This document compiles the metrics designed in the context of Task 4.2 “Design and production of comparative botnet metrics”, providing a specification and describing the infrastructure that has been put in place to compute them and make the results available using a specific JSON[1] format. This way, the results of the metric computations can be used for research and statistical evaluation of botnet activity, for example analysing presence in countries, ASNs or ISPs; or to populate graphical interfaces and charts to build custom dashboards for end-users.

The document also describes the work conducted in Task 4.5 “Publishing benchmarks to incentivize market actors” and proposes how to use benchmarks based on these botnet metrics to encourage market actors to share cybersecurity related information, and in particular contributing to the ACDC benchmarks. It further presents an incentives model that rewards their participation in the benchmarking activities, by publishing the results in a dashboard and highlighting, for instance, those whose efforts in fighting botnets are feeble or absent while rewarding the outstanding performers.

[1] http://json.org/

2. Introduction

2.1. *Scope and relation to other ACDC outputs*

The goal of the infrastructure described in deliverable D2.3 “Technology Development Framework
Outlining basic models for integration and delivery principles”[i] to support the ACDC operational model (see Figure 1) is to provide solutions to users to fight botnets. These solutions should make possible building up botnets occurrence and behaviour through data collection an analysis, enabling capabilities for early detection of emerging botnets.
ACDC therefore aims to improve prevention, detection and mitigation of botnets and in turn, to reduce the malicious activities supported by these botnets such as cyber-attacks, malware distribution networks or cyber spying.

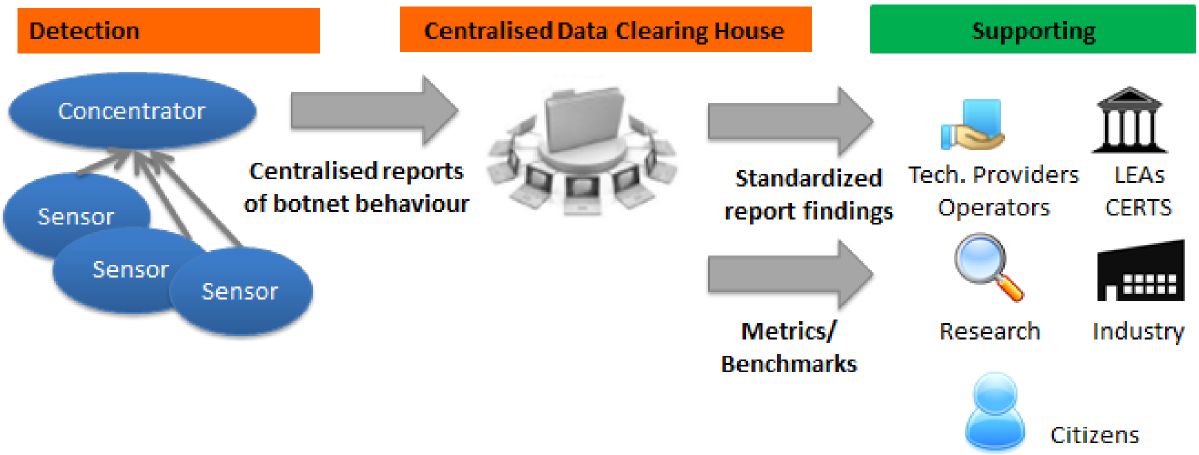


Figure 1 ACDC project anti-botnet operation model

The information about infected users, malware and its distribution services, and methods is stored in the CCH. The information comes from sensors deployed over specific infrastructures (or monitored systems) and is handled based on different trust levels and other defined criteria. Trust levels include various types like reputation, provider, source, volume, or frequency. The access to this information is managed through the ACDC Community Portal (CP), according to the type of member category, legal requirements (outlined in section 5.4.1), and other kinds of possible restrictions expressed by the owners of the information.
The ACDC CP is deployed as the single front-end to access the ACDC CCH, as well as a knowledge management and activity support tool for the ACDC community members.
One of the services offered by ACDC (called *Benchmarking-as-a-Service* in deliverable D5.2.2 “Final Exploitation Plan” to be released in M30) is meant to enable ACDC stakeholders to identify cybersecurity strengths and weaknesses and to compare, in an unbiased manner, their security status against their peers. This is (anonymous) organizations that have a similar profile. This service is built upon a set of metrics computed on the data stored in the CCH and a set of graphics and charts that provide visualization to support the benchmarking feature. The database of metrics implemented is a result of the work conducted in Task 4.2.

2.2. *Objectives of this document*

The main objective of this document is to *describe a model that contributes to the motivation of market actors in sharing cyber security related information, based on the ACDC approach and using the infrastructure provided to support it*. This high-level aim can be split into three:

- Designing and implementing a set of comparative metrics that enable ACDC stakeholders to:
    - assess botnet impact in terms of detection of incidents, geographical distribution, volume, quality of data, etc., and

    - evaluate the operation of the ACDC infrastructure that enables cybersecurity information sharing.
- Defining a set of benchmarks based on the computation of these metrics over cybersecurity related events gathered from an operational pilot infrastructure and make them available online.
- Describing the core elements to support the model in terms of building trust and a program of incentives, rewards and penalizations, necessary to motivate market actors to participate in the ACDC initiative.

2.3. Structure of the document

After this introductory chapter, the document is structured into three main chapters:

- **Section 3** focuses on the specific set of metrics that has been designed and implemented to support the benchmarking activities.
- **Section 4** describes the benchmarks and provides an overview of the different visualization tools that have been put in place to support the benchmarking activity. These tools contribute to make end-users aware, in a more convenient manner, of both the botnet impact and the results of the benchmarking campaigns run.
- **Section 5** studies how to motivate market actors to participate in ACDC benchmarking activities and to contribute to fighting botnets. The section presents a model for incentivizing market actors, defining the ACDC stakeholders that are the target group for the benchmarking service, the methodology used to identify incentives/rewards, the type of participation and the trust model behind to support it.

To close the document, section 6 outlines the main conclusions and next steps.

The document also contains four annexes:

- **Annex I** contains the questionnaire created to support the gathering of requirements from stakeholders for the metrics, benchmarking and incentivation model.
- **Annex II** contains the JSON schemata to represent metric results
- **Annex III** is a detailed specification of the metrics listed in section 3
- **Annex IV** lists the default configuration and some screenshots of the custom implementation that Atos have done of a dashboard of metrics

3. Botnet Metrics database

3.1. *Design and specification of botnet metrics*

The development of *good* cybersecurity related metrics that are meaningful, high-level, quantitative and reproducible is still a research area of interest that is present in many cybersecurity landscape analysis and proposals for future security research agendas[ii],[iii],[iv].
The design and specification of comparative botnet metrics is a work conducted in the context of Task 4.2. Metrics have been specified using a common template (see Figure 2), to harmonise their description and facilitate their publication as an available online resource.
The template also includes the specification of the algorithm to calculate the metric (*data processing* field) using pseudo-code, to facilitate the software implementation.

ID: <INTEGER>
Objectives: Brief description of the metrics and the achievements.
Data selection and Quality Criteria: Specification on which data the metric is applied. If required quality requirements can be stated that the data has to fulfil.
Data Enrichment: Here, a brief description of additional information that is relevant for the results of the metric can be stated.
Data Processing: This section provides pseudo code, intended to understand how the results are produced and what the meaning of the results is.
Data Exchange Format: For all metrics the format "eu.acdc.metrics" should be used. Only if it is inevitable, another data format should be used.
Legal Statement: Since the results are supposed to avoid any data containing personal information, no legal issues are expected. However, if a metric relies or has to include such data, a legal statement is required, indicating that the

Figure 2 Template for metric specification

The complete specification of all metrics is included a the end of this document in Annex III and it is also available online at the ACDC CP in a dedicated section called "Botnet Metrics", in order to facilitate future updates and additions of new developed metrics in a dynamic and collaborative fashion.
The metrics specified in Task 4.2 have been grouped into the following categories, oriented towards the benchmarks defined in section 4.

- **Data Quality metrics**: assess the quality of the data submitted to the CCH in terms of gaps and anomalies, taking into account that it could distort the statistical stability of the data. This category of metrics can be used to compare technologies (i.e. network sensors, malware analysis tools, spam-traps, correlation services, etc.) based on the information reported to the CCH, both in qualitative and quantitative terms.
- **Botnet Impact metrics**: assess the impact of the botnet activity in terms of distribution, by comparing incidents related to bots (unique IP-based, proxy-based, RDNS-based) per ASN, per country, per ISP-subscriber.
- **Operational metrics**: this type of metrics group focuses on evaluating volume and quality of data reported to the CCH in the context of specific pilot experiments, such as those conducted in WP3, or certain types of cybersecurity related events such as DDoS attacks, malicious URIs detected or malware samples analyzed.

3.2. *Data Quality metrics*

This set of metrics focuses on assessing the quality of the data submitted to the CCH by the different data sources in terms of gaps or anomalies in the data and the distribution.

- **Data sources per Submission Key**
  The metric aims at identifying gaps or anomalies in the data that might be caused by a failure of the data submission or the sensor.

- **Data Distribution per Submission Key**
  The metric aims at identifying gaps or anomalies in the data that pertains the distribution of reported systems. The metric computes the number of reports that are associated to ASNs and if feasible to networks. The assumption is that anomalies and gaps distort the statistical stability of the data.
- **False positives per partner**
  The aim is to determine the rate of false-positives per CCH submission key / data source. Currently, the following criteria are implemented:
  - Private IP addresses
  - Malformed reports
  - Reports that violate explicit or implicit criteria if the format definition
- **Reliable Data sources per Submission Key**
  The metric aims at identifying gaps or anomalies in the data that might be caused by a failure of the data submission or the sensor. This is achieved by computing the total number of reports from all data sources in a specific time interval whose confidence level exceeds 0.8. Data sources are unique keys that are used to submit data to the CCH. In the context of the metrics, gaps are time intervals where no reports are submitted or where the number is significantly less than the average number of reports.

The following set of metrics aim at evaluating the quality of the data submitted to the CCH by individual tools (based on the confidence level value associated to each report), the volume of data submitted and the distribution of the reports submitted (i.e. per ASN and Country).

- **Tool-based Quality Metric: Average Confidence Level.**
  The metric takes as a basis the CCH API Write Key ID, to identify the different tools submitting reports and the type of report. On the other hand, confidence levels indicate the expected quality of the reports. Thus, to determine the actual quality, the verdict should be cross-checked, e.g. by a CERT flagging reports as true or false positives after investigating them, as in the metric listed above "False positives per partner".
- **Tool-based Distribution Metric: Volume of reports per ASN, per Country**
  This metric aims at evaluating the distribution of the data submitted by tools to the CCH. The metric takes as a basis the API Write Key ID to identify the different tools submitting reports and the type of report, and the ASN/country associated with the report.
- **Tool-based Quantity Metric: Volume of reports per category**
  In order to evaluate tools with regards to their contribution to fighting botnets and cyber threats, there have also been proposed metrics that assess the volume of the information shared by tools in achieving the objective of detecting attacks, bots, botnets, etc. As an example, Annex III provides specification of metrics focusing on Attack reports and Malware reports.

3.3. *Botnet Impact metrics*

The ACDC project focuses especially on fighting against botnets. These metrics aim to help assessing the impact of botnet activities and presence (by looking at the Bots distribution) over time. The botnet metrics that fall into this category are outlined next.

- **Daily Bot IDs per country user, per ASN-IP, per partner or ISP**
  This metric's aim is to compare the number of unique bots per country, ASN-IP, ISP. To address the different population of each country the overall number is normalized with the individual population of the specific country, with the number of IPs per ASN. One condition for the data is to contain unique identifiers of bots, which unfortunately is not always the case.
- **IP-based metrics: Unique daily IPs per country user, per ASN-IP, per ISP-subscriber**

Aim is to compare the number of unique IPs per country, ASN-IP, ISP-subscriber. To address the different population of each country the overall number is normalized with the individual population of the specific country, with the number of IPs per ASN.

- **Proxy-based metrics: Daily attack events per country user, per ASN-IP, per ISP subscriber.**
  Depending on the type of attack, we can also explore comparing the impact of the attack for different ISPs and ASNs. For example, in the case of spam, one metric which is also important is the number of spam messages each bot has sent, and total number of bots.
- **RDNS-based metrics: Unique daily IPs/reports with the same second level domain per day**
  The objective of this metric is to compare the number of unique IPs and reports per second-level domain (e.g. dtag.de). This metric is useful in the cases where the ASN and the second level domain are not equivalent, this way it complements the previous metric. For example, DFN is assigned to AS680, but each university has an own network and second level domain: e.g. the university of Hamburg belongs to to AS680 but has the SDL uni-hamburg.de.

3.4. *Operational metrics*

The metrics described in sections □ and 0 are generic in the sense that they can be used to evaluate botnet activity or quality of the information shared with any specific purpose and at any time, without taking into account the specific operational context. Operational metrics permit the evaluation of the performance of the end-to-end ACDC solution performing in a particular scenario in real-time, and focusing on a set of specific scenario objectives. In the ACDC project, five experiments have been scheduled to recreate the conditions of some cyber-security typical scenarios: fast-flux domain detection (Fast-flux in short), malicious website detection and malware analysis (Websites in short), detection and mitigation of DDoS attacks (DDoS in short), detection of malicious activities in mobile devices (Mobile in short) and spam campaign analysis, prevention, and mitigation (Spam in short). Each of the scenarios focuses on certain aspects aiming at detecting and improving response against proliferation of botnets. A set of metrics have been defined to evaluate the performance of the different types of tools integrated and working together towards achieving the particular objectives of the scenario evaluated.

Full details of the scenario configuration, tools and metrics are provided in ACDC project deliverable D3.2. “Design report of each experiment”[v].

Group	Metrics
FAST-FLUX metrics	Volume of fast-flux domains detected: per TLD, per Country, per ASN Distinct IP addresses used in Fast-flux techniques (Fast-flux bots): per Fast-flux domain, per ASN, per Country Distinct C&C (Command & Control) IP addresses: per Country, per ASN
WEBSITES metrics	Number of attacks to websites detected: per ASN, per Country, per TLD Number of malicious/suspicious/vulnerable websites analyzed (identified) : per ASN, per Country, per TLD Number of bots attacking websites identified: per ASN, per Country Number of detected/analyzed malware distributed from websites Number of detected C&C IP addresses: per ASN, per Country Number of different botnets detected with malicious websites involved
DDOS metrics	DDOS Attacks Volume by Subcategory Number of total IP addresses identified as DDoS bots: per attack, per ASN, per country Number of detected C&C IP addresses: per country, per ASN Number of different botnets supporting DDoS attacks detected
MOBILE metrics	Volume of mobile events analysed per malicious activity: related to HTTP

	protocol, application events related to malware, SMS events related to spam/C&C messages, Hardware events. Volume of malicious/suspicious APKs reported Distinct mobile bots identified Distinct C&C involved in malicious mobile activities Volume of botnets related to mobile devices
SPAM	Volume of reports of spam campaigns: per country, per ASN Volume of spam campaigns detected: distributing malware in attachment, distributing malicious URL Distinct IP addresses sending spam: per ASN, per country Volume of spambots: per country, per ASN, per campaign Distinct C&C IP addresses: per Country, per ASN Volume of botnets related to spam activities Volume of malicious URLs related to spam reported: per TLD, per subcategory Volume of spam attachments reported

Table 1 Operational metrics for WP3 experiments

The metrics listed in Table 1 are strongly related to the needs of evaluation of WP3 pilot experiments, and can be considered as an example of operational metrics that can be designed. Therefore, we would not include the corresponding specification in Annex III. Nevertheless, these metrics can be easily calculated by counting reports of the categories and/or subcategories relevant in each case (e.g. eu.acdc.malicious_uri, eu.acdc.malware, eu.acdc.attack), submitted to the CCH in the specific period of study (by looking at the timestamp field in the CCH report JSON schema). Calculation is done in a similar way as metrics with ID 12, 13, 14 and 23 included in Annex III are calculated. However, the reports used as input for the metrics calculation in the context of a specific experiment should be marked to distinguish between those belonging to the experiment from the rest. During the execution of the WP3 pilot experiments, the agreement between participant partners was to include a tag in the report_category field of the JSON report schema. This tag will clearly identify reports that belong to each experiment: [DDOS], [FASTFLUX], [MOBILE], [WEBSITES], [SPAM].

Filtering per ASN, country or TLD can be easily implemented by making a selection over the meta-data that the CCH provides, associated to each report. This meta-data also follows a JSON schema that includes fields for ASN, country, TLD, domain and the exact date-time where the report was submitted to the CCH, amongst other information.

The results of the execution of the experiments and their evaluation using the metrics in Table 1 will be reported in deliverable D3.4 “Final report of running & control experiments”, to be released by M30.

3.5. Implementation: the Statistics server

The metrics described in sections □ and 0, and specified in the Annex III are computed in ACDC in a separate infrastructure, for short “Statistics Server”, and taking as input the data available in the CCH in regular intervals (by default 1 day). Figure 3 depicts an overview of the software elements that interact in order to compute metrics. On the right side, the CCH is receiving data from sensors and other components that contribute with reports about cybersecurity incidents, and offers the data to subscribers (via DAM in the CP) through XMPP protocol. On the left side, the elements that are deployed in the Statistics server interact with the CCH in two ways:

- for getting new reports stored in the CCH (through the XMPP client), and
- for submitting the results of the computation (using JSON reports of category eu.acdc.metric) by means of the CCH REST API.

The CCH JSON reports are received continuously as a stream from the CCH via XMPP and are parsed and stored in a local Postgres[1] database. This database is used as temporary storage

[1] http://www.postgresql.org/

to facilitate metric computation in the Metrics Calculation module. This module stores metrics computation results in a local MongoDB[1], which is used as a cache that avoids re-calculating metrics on every request. This way, when a request for a specific metric and time interval arrives to the Metrics Calculation module, it checks whether the corresponding values are already in the MongoDB cache. If so, the value is returned, but if it is not already present, the module posts the SQL query corresponding to the requested metric to the Postgres database. The results are stored in the MongoDB cache.

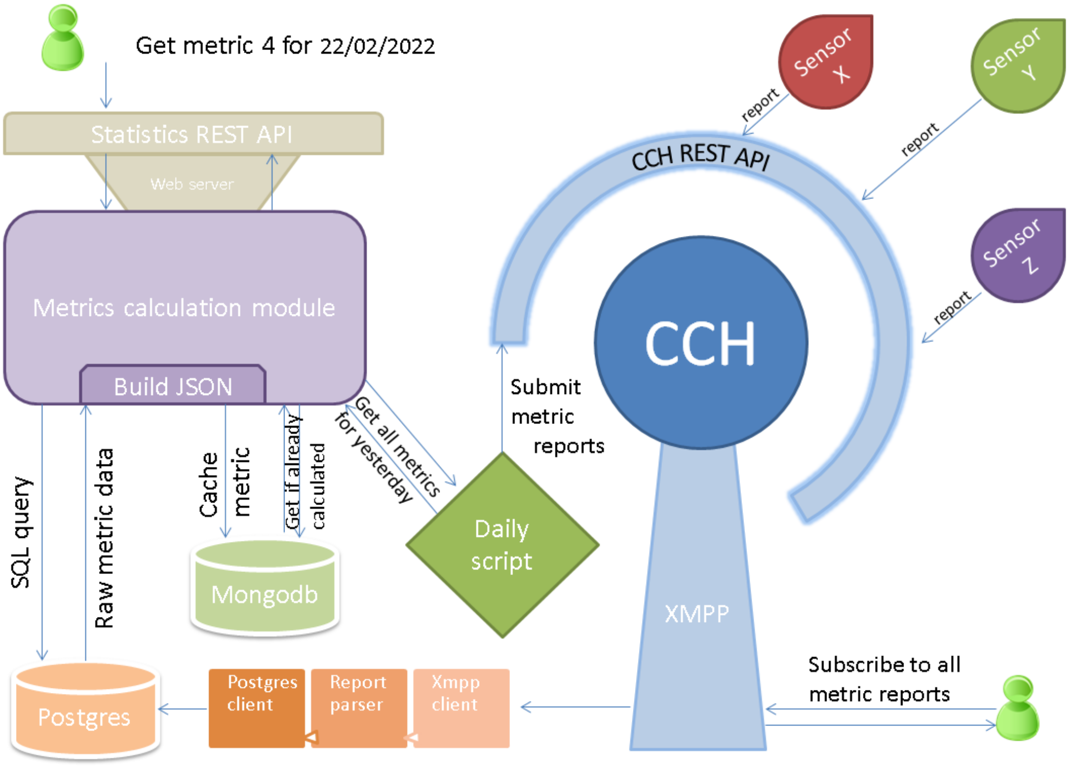


Figure 3 Infrastructure to compute metrics

The data format to represent the raw results of the computation of each metric is adopted from the Research Workflow, as described in D1.7.2 “Data Formats Specification”, and specified using the corresponding JSON schema. For convenience, the JSON schema is also included in Annex II, and an example of raw results of a metric calculation, represented using the JSON schema is displayed in Figure 4. The Research Workflow also specifies how the results of the metrics computation are submitted to the CCH and how they can be retrieved from it.

There are two ways to retrieve metric data results from the Statistics Server:

- *Via XMPP from the CCH, following the retrieval procedure established in the Research Workflow*.

Retrieving metrics raw results requires that the corresponding data sharing policies are established in the CP DAM. These policies are mandatory for any software component to get access to this type of data (i.e. eu.acdc.metric), and to regularly receive streams of reports by means of the XMPP server.

- *Directly from the Statistics Server, by means of a REST API*

This is a method to get results in a “pull mode”, especially appropriate for getting the results on demand, for example for visualization in graphical charts. The consumer of metrics results will send an HTTP request to the web service specifying the metric ID and the time frame. The web server will query the Metrics Calculation module for the

[1] https://www.mongodb.org/

requested data, which in turns checks the MongoDB cache, and returns a JSON list of records that match the request, one per day per metric.

```
{
    "report_category": "eu.acdc.metric",
    "measurement_window": 86400,
    "metric_description": "Unique IPs per Second Level Domain",
    "metric_id": 7,
    "metric_result": {
        "anonhost.DE": {
            "attack": {
                "412": {
                    "data": 1
                }
            }
        },
        "anonhost.NET": {
            "attack": {
                "412": {
                    "data": 1
                }
            }
        }
    },
    "report_subcategory": "ip_based_metric",
    "report_type": "[METRIC][RDNS_METRICS][DFN-CERT] Unique IPs per
Second Level Domain",
    "timestamp": "2015-04-07",
    "version": 1
}
```

Figure 4 Example of metric using the JSON schema

Regarding the operational metrics described in section 0, some of them have been implemented by ULUX, in the context of Work Package 3, and are currently available via https://acdc.uni.lu until the end of the project. Since the Statistics Server is based on the code developed for WP3, all the functions to calculate these metrics are available, and thus they can be used to extend the metrics in sections □ and 0 by re-enabling them in the code. Some of the operational metrics have been implemented also by ATOS to populate the SLSIEM dashboard (as described in 4.2.2). The results of the metrics computation in the SLSIEM are not shared through the CCH following the Research Workflow. This is mainly because the data used as input is limited to the data sharing policies established by Atos in the CP DAM, and thus the computations are done only over a subset of the total dataset stored in the CCH, being of no use to anyone else besides Atos.

4. Publishing benchmarks and botnet metrics

4.1. Benchmarking

Benchmarking is already well known in business and industry as a management tool for rapidly gaining reputation and increase turnover, boost profits and improve productivity.[vi]. Benchmarking helps in the following ways:

- Identifying what other business do for their success and adapting to those methods to become more competitive
- Identifying areas of excellence in the existing business, learning their success points and defining best practices, extending them to the rest of areas using training to increase productivity.
- Developing a continuous improvement plan of individual business processes, allowing their evolution to meet changing demands and requirements.

Cybersecurity-related benchmarking is a tool for business to improve their cybersecurity posture and prove compliance in an unbiased and standardized manner. The benchmarks developed in the ACDC project are a consensus achieved among partners from industry, government and academia from 14 different European countries, constituting an independent program using a commonly shared standard reporting format and APIs, which compose the initial Benchmarking-as-a-Service offering described in D5.2.2.

- **Benchmarking of Data Sources / Technologies**
  The evaluation of the information supplied to the CCH by technology providers is a key element in the trust model described in section 5.4.2 and in the definition of the incentives program described in section 5.4.3. In case the quality of the shared data is proven to be below minimum quality requirements along a predefined period of time, it may be a cause to discontinue the participation of a stakeholder in the ACDC initiative and in particular in the benchmarking activity, or to revise their conditions of participation and access mode (e.g. data access/submission quota). On the contrary, in case the information supplied is proven to be above the standards of quality, the initial access mode can be revised and promoted, as a reward to their noticeable participation. The metrics described in section □ will be used to compare data sources and specific technologies:
  - In terms of volume.
  - In terms of quality of data: by comparing confidence level of reports, distribution per country, ISP, ASN; false positives detected.
  - Per type of technology (e.g. network sensors, mobile device sensors, malware analysers, correlation technologies, etc.)
  - Per type of cybersecurity event (e.g. malware, attacks, bots, botnets, malicious URL, etc.)
- **Benchmarking to assess botnet impact (distribution)**
  By benchmarking botnet activities it is possible to assess the distribution of unique bots per country, ISP and ASN, as well as the evolution and trends over time for specific countries, ISPs or ASNs. Evaluating trends in the impact and distribution of bot presence is also a way to evaluate impact of the ACDC pilot. The metrics described in section 0 will be used to compare:
  - Distribution of bots: per Country, per ISP, per ASN
  - Trends and evolution in time
  - Impact in terms of volume of affected unique IPs, individual users
- **Benchmarking within experiments (WP3 experiments or new ones)**
  One of the objectives of the ACDC project is to demonstrate that the joint work of different technologies in fighting botnets yield better results than working in isolation. The ACDC Technology Development Framework proposes a decoupled architecture where the tools interact only by means of the information exchange through the central

data clearing house. Different technologies are integrated according to this model, each one focusing on each of the phases of the process of fighting botnets, which are Detection, Analysis, Notification, and Prevention/Mitigation. The approach tested in the ACDC project and evaluated with the support of the WP3 pilot experiment is the following. Technologies provided by the project partners are deployed and integrated, each one covering one or more of the 4 phases. In order to support the evaluation process and to enable the comparison of the performance of the technologies deployed, the metrics proposed in section 0 can be used to benchmark. For this, the quantity and quality of the information that the tools report to the CCH in the context of specific WP3 experiments or any other planned in the future (by looking at a tag included in the report_type field of the CCH JSON reports) will be measured over a pre-defined period of time.

- Quality of the data
- Volume of data
- Comparative per phases (detection, analysis, notification)
- Comparative of technologies participating

The description of the benchmarks presented above, as well as the metrics specifications which these benchmarks are based on, are available online as a dedicated “Botnet Metrics” section in the CP.

This will permit any other implementation of the metrics computation and configuration of benchmarks based on these specifications, besides the ACDC implementation done in the context of WP4.

Information is power and consequently, sharing it is done only under very specific conditions. Furthermore, publishing information about one’s performance is an even more delicate matter.

Despite the wide acceptance of the benefits of benchmarking for business health, there exists a traditional industrial reticence to share information about their performance for fear of endangering reputation or revealing too much information to competitors. On the other hand, eagerness to knowing how competitors are doing in certain areas, being proud when one is simply outstanding and having the opportunity to show off to the wider community are understandable characteristics when the business objective is to achieve and progress.

Developing a model of operation attached to the benchmark publication activity, in terms of sharing policies and access control modes, which forces participants to disclose a certain level of information while balancing their right to keep some degree of confidentiality, is critical to ensure engagement of stakeholders. Section 5.4 describes the proposal model for incentivizing market actors and details the model to govern access to benchmarks.

4.2. Reporting Dashboard

Raw metrics, as such, are usually too technical, showing figures and using statistical concepts and IT security vocabulary. By tailoring to user profiles, using custom graphic metaphors and vocabulary, the aim is to reach all types of users from technical staff or C-level management (e.g. CISO, CTO) to non-technical citizens (e.g. through National Support Centers’ websites), and satisfy each level of the information needs of each, thus offering a multitude of depth in detail.

Dashboards are graphical user interfaces that are used in ACDC to support the publication of benchmarking results. In the project there are multiple implementations of dashboards used for different purposes:

- **Project-wide evaluation of the impact of botnet activities**: compute metrics over the data stored in the CCH and focuses on evaluation of the impact of the project in fighting botnets.
- **Custom dashboards for monitoring and evaluating specific aspects**: services offered by tools that compute metrics over the data received from the CCH (and thus,

subject to the enforcement of data sharing agreements between particular ACDC parties) and focus on specific metrics and benchmarks of special interest for the dashboard owner.

Here we are going to describe one example of implementation of each of the above-listed types of dashboards.

4.2.1. Project-wide evaluation of botnet activities: ACDC Botnet Metrics in the CP

To illustrate this category we describe here the "Botnet Metrics" section of the CP. This functionality is available only for registered users and offers visual representation of the data quality and botnet impact metrics described in section 3. The metrics are computed in the Statistics Server, as described in section 3.5, and the results are accessed through a REST API interface offered by the web server running in the Statistics Server and used to populate the dashboard using different types of charts.

The information available in this section has been divided into three subsections: Technology Benchmarking, Botnet Impact Benchmarking and Cybersec Events Benchmarking. Each section provides filtering of the information based on different criteria (timeframe, ASN, API-keys, Country), depending on the kind of information made available by the Statistics Server by means of a web service API (see section 3.5).

The Technology Benchmarking subsection aims at comparing technologies that are used to submit reports to CCH. As each technology is related to one or more API-keys in the CCH, this section allows exploring the provisioning of data by different API keys. A sample of the graphs available in this subsection is shown in the figure below.

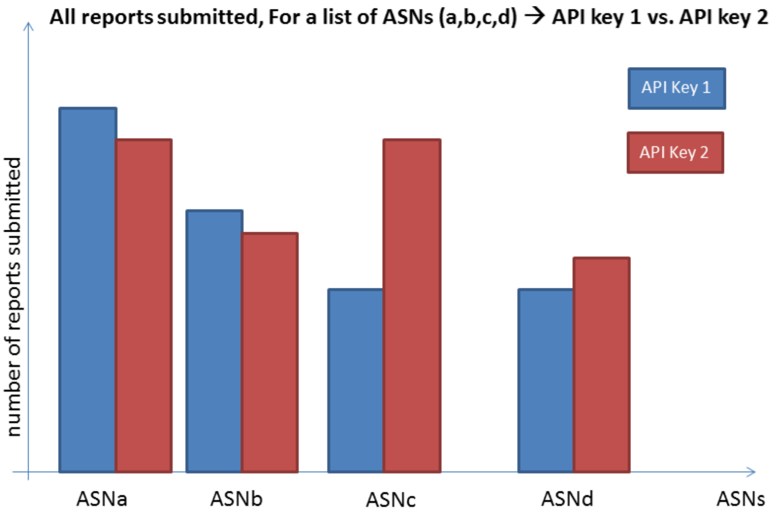


Figure 5 - Sample of Technology Benchmarking graph

The Botnet Impact Benchmarking information helps the user in assessing the impact of botnet presence (by looking at the Bots distribution) geographically along time. A sample of the graphs available in this subsection is shown in the figure below.

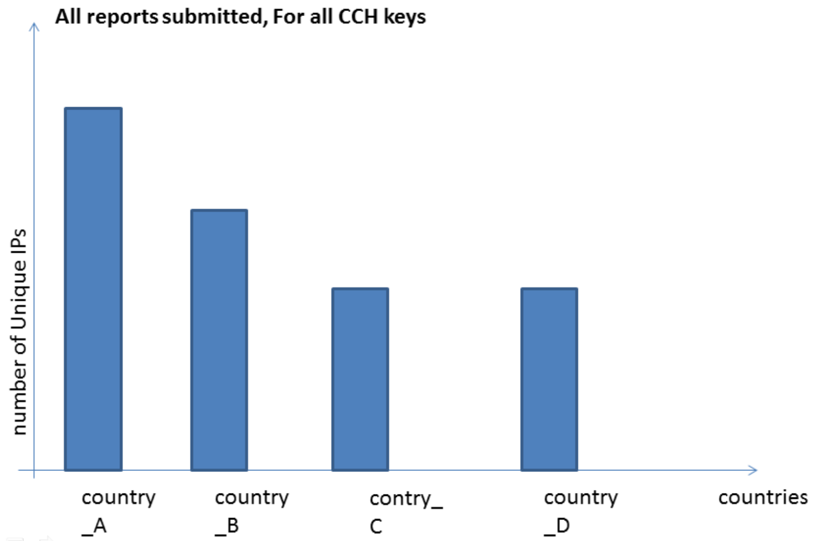


Figure 6 - Sample of the Botnet Metrics Benchmarking graph

Finally, the Cybersec Events Benchmarking subsection, allows comparing the different types of cybersecurity events reported to the CCH. A sample of the graphs available in this subsection is shown in the figure below, showing reporting trends for the different kind of DDOS attacks over time.

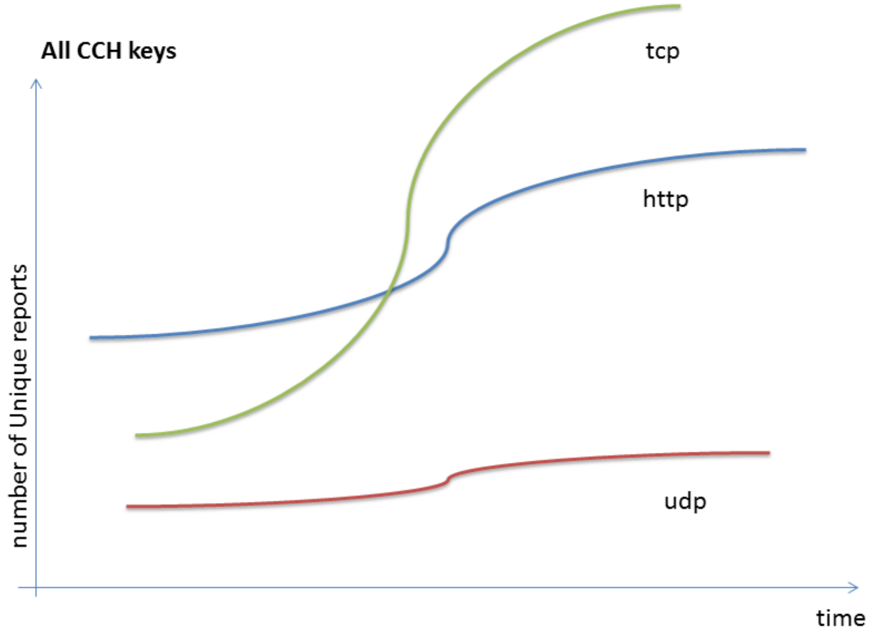


Figure 7 - Sample of Cybersec Events Benchmarking graph

4.2.2. Custom dashboard: Atos SLSIEM

Based in on Atos' graphical reporting tool and part of the Atos Service-Level SIEM (SLSIEM) component, the dashboard is a web-based GUI composed by different charts that can be organized into views, each one displayed as a web page. The dashboard views can be customized according to each end-user profile in terms of content and layout/look and feel. Access to the custom dashboard is handled by an access management module, which allows defining user-level granularity access policies, and to control the information displayed as well as the customization of graphical aspects.

A significant difference between project-wide evaluation dashboards and custom dashboards, such as the Atos one, is that the computations of the metrics are performed only over the data received from the CCH by means of the data sharing agreements established between parties participating in the benchmarking activity. Also, the metrics computed and the charts displayed respond to the particular needs of the dashboard stakeholder.

By default, six views are configured in the reporting dashboard, and a set of charts is displayed in each view:

- *Public view*: provides general information about volume of reports received by subcategory (e.g. Top 10 Attack subcategories) and by associated ASN (e.g. Attacks by source IP ASN)
- *Executive view*: this a customizable view oriented towards the profile of the stakeholder, to provide high-level information focusing on aspects of their particular interest (e.g. overall threat level, top 10 vulnerabilities).
- *Operational view*: this is a view compiling charts that provide information useful for a security administrator, in terms of the daily volume of reports received and trend over the last week, the quality of the information (e.g. average confidence level) and the correlation alarms triggered.
- *Technologies view*: this is a view that permits comparing technologies in terms of volume of reports submitted and their quality (i.e. confidence level), for the different categories of reports.
- *ACDC Experiments view*: this is a view that serves evaluating the WP3 experiments in terms of volume and quality of the reports submitted in the context of each of the 5 WP3 pilot experiments.
- *Situational Awareness view*: this view focuses on showing the distribution of cybersecurity events (i.e. reports received) by looking at the geo-location of the associated IPs.

The configuration of the views, in terms of charts and content, depends on the type of user and the information access policies applicable to them. The default configuration is outlined in Annex IV, as well as some screenshots of the different views offered by the SLSIEM dashboard.

The Atos reporting dashboard component supports metrics calculation over the data received from the CCH within the last 15 days, and the graphical interface is available online but credentials to access must be requested from Atos contact point[1]. As an additional feature, the SLSIEM dashboard can automatically generate and export PDF reports with historic data. There are various pre-configured report types on metrics per day, week, month, year or other custom periods, as long as the database is configured in the tool for storing the data for such periods of time.

[1] beatriz.gallego-nicasio@atos.net

5. Incentivizing market actors

Recent economic research has found that the infected machines of end users (zombies) are a key source of security externalities, most notably home users and small and medium-size enterprise (SME) users. In contrast to larger corporate users, these groups often fail to achieve desirable levels of protection[vii].

For decades security and risk management practitioners have been caught in discussions around the contribution of implementing a cyber-security governance framework to business value, and showing investment incentives in putting security mechanisms in place. Nowadays, cybersecurity is a top priority for many organizations and spending in IT security has increased significantly. However, higher investments require executive level management to justify the return of the investment by demonstrating the effectiveness of the implemented cyber security governance approach. A key to providing C-level a quantifiable and measurable solution to the effectiveness of their IT security is through metrics, and more broadly, by implementing a Cyber Security Metrics program. As a human way to interpret raw data, metrics provide C-level the means to quantify and measure the effectiveness of the implemented policy, strategy, programs, and invested resources across cyber security activities. Moreover, metrics permit leadership assessing the current cyber climate and, through the analysis of key trends associated with cyber security, constitute the key for leveraging future strategic decisions and investments.

There is a lack of standardization of metrics across the cyber security industry, mainly due to the privacy and sensitivity concerns of organizations to disclose any security related information. Reputational costs associated with bad results in preparedness against cyber-attacks or showing weaknesses in coping with cyber threats may end up in causing stock price and company value to drop.

Another point that contributes to the lack of standardization in cyber security metrics is the specificities of each organization's goals and infrastructures. This leads to different prioritization of the risks to cover, the assets to protect, and the mitigation strategies adopted to combat attacks. In consequence, customization of the metrics becomes necessary in order to meet the organizational needs.

A critical problem that all botnet mitigation efforts face is the lack of consistent metrics to measure the impact of countermeasures across networks and over time. The absence of metrics also undermines the incentives of market actors to act against botnets.

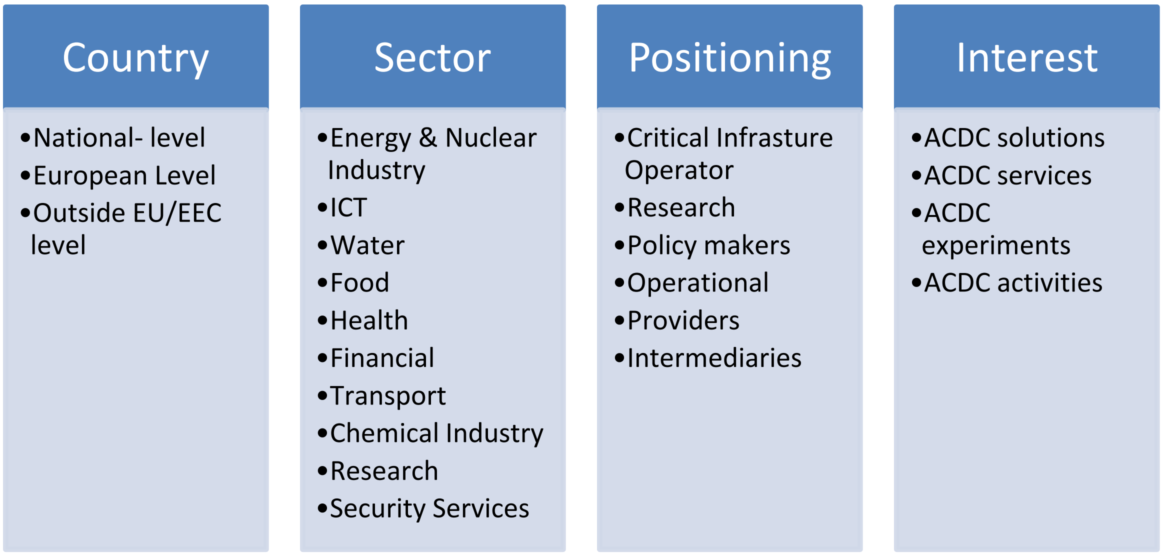
Turning these metrics into standard available benchmarks would increase transparency, contributing to reduce market failures associated with information asymmetry, usually controlled by certain groups of stakeholders (e.g. antivirus providers). However, reputational costs associated to underperformance, e.g. in preparedness against cyber-attacks or showing weaknesses in coping with cyber threats, raise sensitivity concerns of organizations to disclose any security related information. The global scale and complexity of cybersecurity calls for stakeholders to share crucial information that may lead to not only preventing attacks but also to support the development of better mitigation tools.

An incentive program to encourage the cyber security actors towards information sharing and contributing to the ACDC benchmarks (published in a dashboard) would highlight those whose efforts in fighting botnets are feeble or absent while rewarding the outstanding performers.

5.1. ACDC Stakeholders

The creation of a community of stakeholders related to fighting botnets is one of the major work lines of the ACDC project. The management of the community, the animation, and interaction is done with the support of the already introduced online tool ACDC CP. The stakeholders are categorized according to a defined criteria, ranging from the most general ones (Country and Sector), to the cybersecurity field (Positioning), down to the botnet topics that are covered by the ACDC activities (Interest). The criteria, as well as the methodology followed by ACDC to classify stakeholders, is described in full detail in the public deliverable

D6.1.1 ACDC User Profiles and Categorization[viii], here we will only introduce them briefly for the sake of understanding of the stakeholder classification displayed in the diagram in Figure 8.



Country
- National- level
- European Level
- Outside EU/EEC level

Sector
- Energy & Nuclear Industry
- ICT
- Water
- Food
- Health
- Financial
- Transport
- Chemical Industry
- Research
- Security Services

Positioning
- Critical Infrasture Operator
- Research
- Policy makers
- Operational
- Providers
- Intermediaries

Interest
- ACDC solutions
- ACDC services
- ACDC experiments
- ACDC activities

Figure 8 Stakeholder classification criteria

The *Country criterion* diversifies between national-level stakeholders and international, European-level ones, highlighting differences in the way stakeholders may interact in the community and thus, have an influence in the access to the services and the information offered. In particular this criterion determines the benchmark publication and access modes described in section 5.4.1 since national-level stakeholders may access benchmarking data through National Support Centers, while European-level stakeholders' contribution may be handled by European-wide entities such as the ACDC CCH. For stakeholders outside the EU/EEC this criterion is critical, in particular in what concerns the application of the legal requirements to the information sharing, publication of benchmarks, and the control of their access, is taken into account in the trust model attached to the incentives model, as described in section 5.4.

The *Sector criterion* is useful to know shared interests and common requirements within stakeholder groups. This way, the incentivation strategy can be tailored to them in a more effective way. This criterion also helps shaping the characteristics of the published benchmarks access mode for each particular group of stakeholders, considering for example to define a specific mode for a particular stakeholder group. The classification by sectors used in ACDC mainly derives from the ECI Directive proposal[ix] but it is not restricted to it exclusively as it introduces other sectors of relevance for ACDC, such as health or finance, as can be seen in Figure 8.

The *Position criterion* refers to the positioning of the stakeholder with respect to the cybersecurity field. Again, this criterion helps defining incentives for participation that are really attractive for that particular group of stakeholders. One remark regarding this criterion is the fact that it is a very dynamic one, since most actors in cybersecurity usually play more than a single role and their positioning may evolve over time from one to another. Policy makers include Regulation Bodies, National Governments, International Institutions, Policy Agencies and Citizen Associations. Among Providers are included Hosting providers, Technology providers and Service providers. Operational refers to Agencies, CSIRTs, Public Prosecutors, Law Enforcement Agencies (LEAs) or National and International Centers for cybersecurity/crime.

The *Interest criterion* evaluates not only the level of interest of stakeholders in ACDC offering, which clearly contributes to the incentives model definition, but also the potential involvement of stakeholders' in the ACDC activities and their contribution to ACDC services, solutions or experiments. This contribution can be either in the form of cybersecurity information shared through the CCH and possibly by participating in the benchmarking activities, or as providers of technology to be integrated in ACDC solutions. The ACDC experiments consist of a set of scenarios where the tools integrated to compose ACDC solutions are executed under pre-defined conditions, allowing the evaluation of performance and functionality of the ACDC concept end-to-end, as well as metric calculation and benchmarking. During the project lifetime, five experiments are scheduled, each one focusing on different cybersecurity aspects: fast-flux domains detection, malicious websites detection and malware analysis, detection and mitigation of DDoS attacks, detection of malicious activities in mobile devices, and spam campaigns analysis, prevention and mitigation. Other experiments can be designed and executed in a similar way to support benchmarking activities after the project ends.

5.2. Consideration of legal aspects

The ACDC anti-botnet methods, and specially the cybersecurity-related information sharing through the CCH component, require a legal assessment related to privacy concerns before the EU legal framework and the laws of selected Member States, which has been published in a public deliverable document entitled "1.8.1 – Legal Requirements"[x]. The first iteration of the assessment identified, among others, a set of recommendations that are relevant for the implementation of the incentive model described in this paper, in particular for regulating the participation in benchmarking activities and the publication of their results.

- *Classification of IP addresses as personal data*.

There is no conclusive opinion at EU level on this matter since this assessment should be done on a case by case basis and depends on the circumstances of the event. Nevertheless, this study recommends the ACDC project to follow the opinion of the Article 29 Working Party[xi] which considers that IP addresses shall be treated as personal data in almost all situations. Anonymization is the typical solution for preserving privacy for IP addresses. However, IP addresses carry utmost importance for the calculation of botnet metrics that measure botnet activities, their trends, and impact, and especially on the information derived from them (e.g. country, ASN). Full anonymization of IPs will simply make these metrics useless and only some lighter techniques such as pseudo-anonymization or truncation of the last part of the IP (i.e. the last octet in IP v4 and the last 80 bits in IP v6) would work since metrics do not necessarily need the individual IPs involved in botnet activities and can still yield significant results based on the IP ranges. This is for example the approach used by Google Analytics[xii].

- *Implementation of Article 7 of Directive 95/46/EC[xiii], with especial attention to paragraphs (a), (b), (c) and (f), including the interpretation of balance of interests between data controllers and data subjects.*

This analysis has revealed that the main legal barriers to the operation of the Centralized Clearing Data House (CCH) at EU level rely on the fulfilment of the legitimation grounds described under Article 7 of Directive 95/46/EC. In order to process personal data, controllers must first justify their data processing activities on one of the legal grounds listed in article 7 of Directive 95/46/EC. Additional obligations refer to compliance with a series of principles such as: data quality principles of fairness, lawful and limited purpose, data minimization, data accuracy, and storage limitation. In the case of ACDC, the need to fight botnets (as part of the security of the network) should be balanced against the need to protect users' confidentiality of communications. Two data processing operations should be legitimate: the sharing of personal data with the CCH and its further processing for fighting botnets. This processing will be performed by the CCH and shared with a legitimate interested party, i.e.

ISPs, webmasters and hosts. The rules of the CP together with the numb and automated character of the CCH are designed to ensure the minimal possible impact on the fundamental rights of data subjects in being taken into account. Removing the processing of personal data would diminish the capability of the CCH to a level where the purpose is no longer attainable. However, input and output data are controlled and ranked by the CP, which also enables sharing preferences and restricts access to data according to partners' legitimate interests. For instance, ISPs receiving data feeds from the CCH can only have access to information related to their own range of IP addresses, never to data relating to users that are not related to their services. This guarantees sufficient levels of confidentiality of communications and lesser invasive means on user data. This is also applicable for benchmarks and it is reflected by the access modes described in section 5.4.1.

- *National Comparative Analysis.*

The analysis of the national laws of Belgium, France, Germany, Italy, Portugal, Romania, Slovenia, Spain, and the Netherlands has revealed that most countries do not present a significant obstacle to the deployment of ACDC and its tools. The findings of this comparison were based in the text of the law and are thus subject to the interpretation of the national protection authorities. A sustainable strategy for the publication of benchmarks and the incentives model, which considers stakeholders from outside the EU/EEC (as indicated in section 5.1), should consider extending the comparative analysis of legislations and new implications it may impose in the incentivation model and benchmarking access modes.

5.3. Gathering requirements from stakeholders representatives

The process of definition of a model for encouraging stakeholders to participate in the ACDC initiative and especially, to share cyber security related data through the CCH, requires the interaction with stakeholders in order to gather requirements on the types of metrics and benchmarks that are the most interesting from their viewpoint, and to obtain knowledge on how to motivate them to participate.

A set of representatives from the stakeholder groups were interviewed and a set of requirements were collected with regards to three main categories: *metrics*, *publishing benchmarks*, and *trust and incentivation*. From the list of ACDC stakeholders (see section 5.1) three groups have been selected for conducting interviews and gathering requirements: banking, technology providers and LEAs. These three stakeholder groups represent 3 main roles in the ACDC model, with the banking acting as data provider (as infrastructure owner), the LEAs acting as data consumer and finally, the technology provider as a representative of the institutions providing the tools to be deployed in the IT infrastructure that enable the detection, analysis, notification, and mitigation & prevention phases driving the ACDC integrated process for fighting botnets.

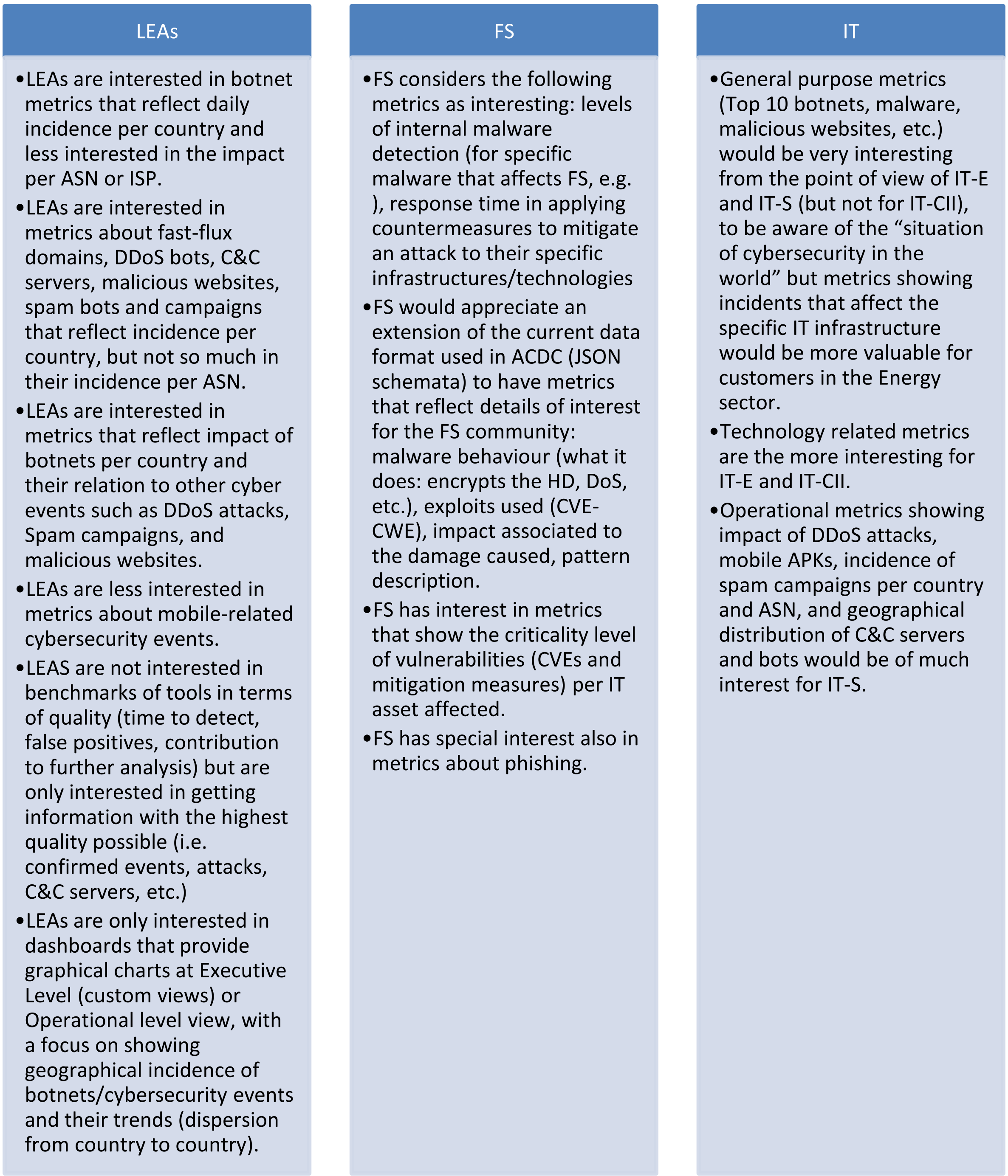
From these three groups, some representative entities have been appointed for interview, either by taking advantage of an existing relationship with some of the ACDC partners participating in this task, or because of a previously expressed willingness from the entity to collaborate in this type of activities, for instance when joining the ACDC Community.

The interviews consisted in a presentation of the project, its purpose and main assets, and a brief overview on the metrics defined in WP4 and the benchmarking activities. After the presentation, optionally, a short demo of the existing graphs and dashboard implementations available (i.e. the Atos SLSIEM dashboard and the ACDC analytics feature of the CP) was also shown to illustrate the concepts presented before. After a discussion with the interviewees, a questionnaire to get feedback on the specific aspects relevant for defining the model was shared and filled in.

The questionnaire (see Annex I) enquires about a list of pre-selected metrics, a strategy for publishing benchmarks and tools, and the elements that define the incentives model, as well as its basic operation. This material is presented to the interviewees and used to trigger discussion. The conclusions of the discussion have been analysed with the objective of extracting requirements and helping refining the draft incentives model.

In total, 8 people were interviewed: 1 representative from a LEA, 2 representatives from the FS Sector and 4 representatives from the IT Providers stakeholder category (2 IT Security Consultants specialized in the Energy Sector, 1 security manager of Critical Infrastructures and 1 IT Security Expert).

The feedback received from the questionnaire and from the discussions with interviewees helped identifying a set of requisites for the incentives model but also on the metrics presented and the visual dashboard to support benchmarking. The main conclusions are listed in the next tables, where *LEAs* stands for Law Enforcement Agencies, *FS* stands for Financial Services, *IT-E* stands for IT Security Consultants specialized in Energy Sector, *IT-CII* for the security manager of Critical Infrastructure and *IT-S* for the IT Security Expert.



LEAs

- LEAs are interested in botnet metrics that reflect daily incidence per country and less interested in the impact per ASN or ISP.
- LEAs are interested in metrics about fast-flux domains, DDoS bots, C&C servers, malicious websites, spam bots and campaigns that reflect incidence per country, but not so much in their incidence per ASN.
- LEAs are interested in metrics that reflect impact of botnets per country and their relation to other cyber events such as DDoS attacks, Spam campaigns, and malicious websites.
- LEAs are less interested in metrics about mobile-related cybersecurity events.
- LEAS are not interested in benchmarks of tools in terms of quality (time to detect, false positives, contribution to further analysis) but are only interested in getting information with the highest quality possible (i.e. confirmed events, attacks, C&C servers, etc.)
- LEAs are only interested in dashboards that provide graphical charts at Executive Level (custom views) or Operational level view, with a focus on showing geographical incidence of botnets/cybersecurity events and their trends (dispersion from country to country).

FS

- FS considers the following metrics as interesting: levels of internal malware detection (for specific malware that affects FS, e.g.), response time in applying countermeasures to mitigate an attack to their specific infrastructures/technologies
- FS would appreciate an extension of the current data format used in ACDC (JSON schemata) to have metrics that reflect details of interest for the FS community: malware behaviour (what it does: encrypts the HD, DoS, etc.), exploits used (CVE-CWE), impact associated to the damage caused, pattern description.
- FS has interest in metrics that show the criticality level of vulnerabilities (CVEs and mitigation measures) per IT asset affected.
- FS has special interest also in metrics about phishing.

IT

- General purpose metrics (Top 10 botnets, malware, malicious websites, etc.) would be very interesting from the point of view of IT-E and IT-S (but not for IT-CII), to be aware of the “situation of cybersecurity in the world” but metrics showing incidents that affect the specific IT infrastructure would be more valuable for customers in the Energy sector.
- Technology related metrics are the more interesting for IT-E and IT-CII.
- Operational metrics showing impact of DDoS attacks, mobile APKs, incidence of spam campaigns per country and ASN, and geographical distribution of C&C servers and bots would be of much interest for IT-S.

Figure 9 Feedback about Metrics

LEAs

- LEAs prefer custom benchmarks and dashboard with restricted access
- LEAs are only interested to share their information (published in benchmarks) only to other LEAs
- LEAs understand that publishing benchmarks would be beneficial to fighting botnets because enhance preparedness and prompt reaction to attacks; helps standardizing methodologies for cybersecurity incident prioritization, reporting and management; and contributes to a wider societal impact and effective awareness raising.

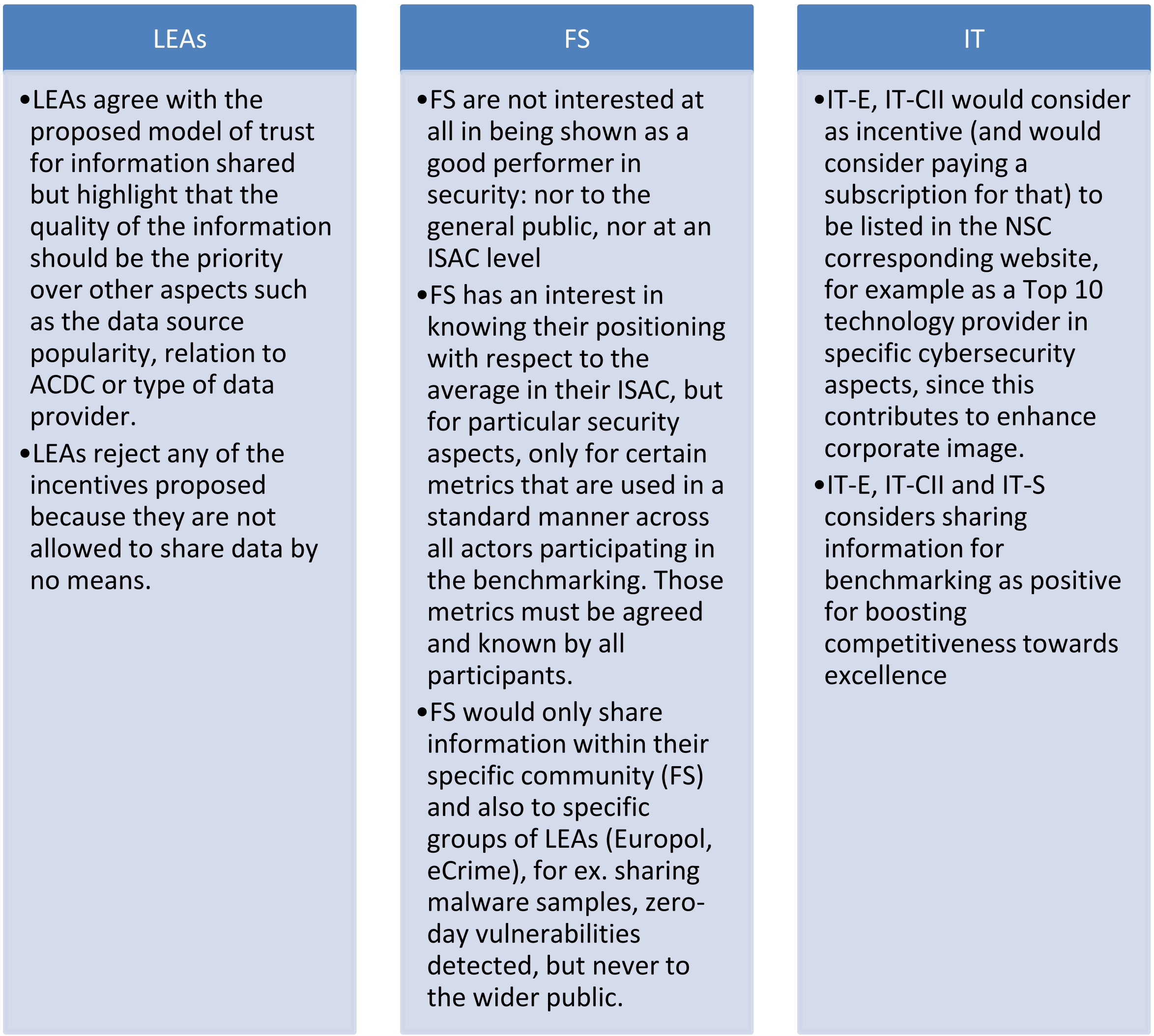
FS

- FS prefers a benchmarking service with dashboard customized to their profile, and only show charts with information relevant to their business
- FS wants to be able to filter the information displayed in the charts to adapt to their needs and particularize per user
- FS are interested in charts showing the level of risk for the specific stakeholder business (add a configurable business-criticality value to weight what is shown in the risk-gauge)
- FS has interest in comparing what is happening inside the stakeholder’s business network with regards to what is happening outside.
- FS would thank an accessible API to be able to configure the actual queries behind the charts

IT

- IT-E would be interested in any kind of cybersecurity benchmark, including sector-specific.
- IT-E, IT-CII would be interested in benchmarks of technologies, for specific categories (e.g. SIEMs, malware analysis, threat analysis, IDS/HIDS, etc.), especially in terms of quality of the information provided.
- IT-E, IT-S would be interested in benchmarks that show incidence of botnets activities (e.g. attacks, exploits) per country, per ISP.
- IT-CII would be interested in benchmarks that show incidence of botnets activities (e.g. attacks, exploits) per country and ISP, but restricted to those that are related to their business (e.g. countries and ISPs where their branches are located).
- IT-E and IT-CII would appreciate configurable alarms that automatically notify Security Manager or Administrator about specific vulnerabilities or attacks that exploit and target the technologies in the infrastructure owned by the IT-E.
- IT-E and IT-CII would be interested in contributing to benchmarks with any kind of cyber security information within the community, and certain information (vulnerabilities, attack types/patterns, malware samples) that do not contain sensitive data (or anonymised) to the general public.
- IT-E, IT-CII and IT-S would consider subscribing to access to benchmarking services based on price to get extra features such as monthly/weekly PDF reports, customization of the dashboard, and be able to participate in the benchmarking activities (to compare technologies).
- IT-E, IT-CII and IT-S would be very interested in a dashboard that allows different views, especially an Operational view and Tool benchmarking. IT-S would also appreciate a Citizen/Public view with charts showing global situation (Top 10), as a starting point and then, drill-down to get more specific charts.

Figure 10 Feedback about Publishing Benchmarks



LEAs

- LEAs agree with the proposed model of trust for information shared but highlight that the quality of the information should be the priority over other aspects such as the data source popularity, relation to ACDC or type of data provider.
- LEAs reject any of the incentives proposed because they are not allowed to share data by no means.

FS

- FS are not interested at all in being shown as a good performer in security: nor to the general public, nor at an ISAC level
- FS has an interest in knowing their positioning with respect to the average in their ISAC, but for particular security aspects, only for certain metrics that are used in a standard manner across all actors participating in the benchmarking. Those metrics must be agreed and known by all participants.
- FS would only share information within their specific community (FS) and also to specific groups of LEAs (Europol, eCrime), for ex. sharing malware samples, zero-day vulnerabilities detected, but never to the wider public.

IT

- IT-E, IT-CII would consider as incentive (and would consider paying a subscription for that) to be listed in the NSC corresponding website, for example as a Top 10 technology provider in specific cybersecurity aspects, since this contributes to enhance corporate image.
- IT-E, IT-CII and IT-S considers sharing information for benchmarking as positive for boosting competitiveness towards excellence

Figure 11 Feedback about Trust & Incentives model

5.4. Incentives Model

The model for incentivizing market actors towards achieving transparency in cyber security presented next takes as input the initial model drafted and presented to stakeholders and the conclusions and formal requisites yielded from the interviews.

There are three key enablers for stakeholders to participate in the benchmarking activities:

- establish a clear access control scheme to ensure certain level of confidentiality for participants,
- offer some attractive means to reward their participation, and
- provide a minimum level of trust to guarantee their business and reputation is not going to be harmed. For example, as a result of benchmarks showing an erroneous position because they were created using low quality data and a model for governing access to the information shared.

The following three sections describe the draft proposal of a model to govern access to the information shared, a trust model to guarantee the quality of the information and an incentives program. However, for this model to become operational, the following elements must be defined:

- Organizational structure and governance
- Operational processes
- Information structure
- Supporting infrastructure and tools

The incentives model is intended to be attached to the Benchmarking-as-a-Service offering described in D5.2.2, which according to the Sustainability Roadmap, is planned to be fully developed during the ramp-up phase. The specificities of these elements depend on the commitment and agreements reached by the ACDC consortium partners after the project ends, as explained in D5.3 “Sustainability Plan”.

5.4.1. Access to the published benchmarks

The following table (Table 2) describes a summary of the characteristics of the three modes considered in ACDC to govern access to published benchmarks for two categories of membership: free (Freemium access) and paid (Based on price). The *public/open access* mode will be available for everyone accessing the ACDC website and basically allows online access to a view showing general cybersecurity metrics over a predefined period of time. The paid mode permits accessing the metrics that compose each benchmark and their definition, amongst other things. The *restricted access (ACDC community)* mode restricts access to the members of the ACDC community and allows viewing reports specific to the sector the user belongs to. The paid mode permits conducting an assessment of the user’s own position and compare it to other members of the community in the same sector of activity (in confidential manner), and offers the possibility to publish this position to the rest of the members of the ACDC community. The *restricted access (ACDC specific communities)* works in a similar way to the ACDC membership restricted access. But in this case, the benchmarks are related to a specific community of interest (e.g. finance, mobile technology vendors, Critical infrastructure operators, ISPs, etc.). The charts are customized to their interests (e.g. specific threats, tools) and the cybersecurity relative position is shown with regards to other peers in their community of interest.

	Freemium access	Based on price[1] (in addition to Freemium access characteristics)
Public/open access	• Online access to a General Cybersecurity benchmarks dashboard view (no confidential information available)	• Access to benchmark definition and metrics specification • Downloadable PDF reports • Customization of the general dashboard view (in terms of layout, aspect and charts displayed) • Participation in the benchmarking activity in experimental mode
Restricted access (ACDC membership)	• Online access to a dashboard view with Cybersecurity benchmarks specific to my sector of activity (no confidential information available) • Use of the ACDC membership badge • Receive updates on metrics and benchmarks activities of other ACDC members	• Access to benchmark definition and metrics specification • Downloadable PDF reports • Customization of the dashboard view (in terms of layout, aspect and charts displayed) • Participation in the benchmarking activity • Private view: Assessment of my own

[1] The pricing model can adopt different forms.

		position with regards to other members of my sector of activity • Possibility of publication of my position/results to the ACDC community benchmarks • Possibility to be listed in my corresponding National Support Centre website.
Restricted access (ACDC specific communities)	• Online access to a dashboard view with Cybersecurity benchmarks specific to my peer group (user type or community) (no confidential information available) • Use of the ACDC specific community membership badge • Receive updates on metrics and benchmarks activities of other specific ACDC community members	• Access to benchmark definition and metrics specification • Downloadable PDF reports • Customization of the dashboard view (in terms of layout, aspect and charts displayed) • Participation in the benchmarking activity • Private view: Assessment of my own position with regards to other members of my specific community • Possibility of publication of my position/results in the specific community benchmarks. • Possibility to be listed in my corresponding National Support Centre website.

Table 2 Access modes for published benchmarks

The components of the table above are a proposal and other options for the pricing mode should be considered (e.g. Academic/Research, Government Institutions, SMEs).

5.4.2. Trust model for information shared

The trust model aims at ensuring a level of quality of the information shared by peers, which has a huge impact in the quality of the benchmarking service offered by ACDC. Having a reliable source of cybersecurity information to calculate metrics is critical to ensure first, the initial participation, and second, the engagement of stakeholders to the benchmarking activities over time. A trust value should be attached to the information shared through the CCH (in the same way the confidence level is currently attached to each report), which partially derives from the tool/service that provides the information and the particular institution that operates it (i.e. data source). Different trust scales can be defined but the important point is how each level is assigned to the data shared (and to the data source) first, and how a particular trust level is maintained along the operation time.

A simple trust model, where the following aspects, related to the quantity and quality of their contributions to the CCH, directly influence the trust value associated to a particular data source:

- *The confidence level of the reports sent to the CCH.* This is a mandatory attribute of the CCH report format which indicates how reliable is the information reported to the CCH. It is a float value with ranges from 0.0 (experimental) to 1.0 (confirmed by CERT/NSC/ISP) and its assignment is subject to the data provider, to the best of their knowledge. Since it is not contrasted or validated by any formal means, this value should be considered only as informative for data consumers.

- *The volume and regularity of reports sent to the CCH*. A regular and fair amount of data provision is considered, in principle, a positive aspect in trusting a data source.
- *The quality of reports provided over time*. This aspect requires an objective assessment of the reliability of the information provided, which can be done, for instance, by comparison against other reports of the same incident, against other peers (data sources) with a high trust level, or against confirmed reports (provided by CERTs, NSCs or ISPs).
- *Type of data provider (e.g.: research, industry, technology provider, CERT).* CERTs, NSCs and other government agencies could be considered more reliable than specific technology providers, in the sense that the information from technology providers can be biased due to economic/commercial agreements.
- *Relation with ACDC.* Partners of the ACDC project are considered as the most trusted parties by default, with regards to this aspect. Members of the ACDC community are not completely unknown, have been introduced to the ACDC model and have committed to a minimum involvement in ACDC activities. Some of the members can join the ACDC community with a mentor (i.e. an existing member of the community) and therefore, by default should be more reliable than those that do not join with a mentor. Within the ACDC Community there can be specific groups of interest (e.g. finance, law enforcement) working similarly to ISACs, and members of one or more of these communities of interest are considered to have a more strong involvement in ACDC activities, and thus, have a level of trust higher than those members not involved in specific communities within ACDC. Entities that have expressed a public endorsement to ACDC are also considered of a minimum level of commitment with the ACDC initiative and thus, more reliable than unknown parties, but with a less trust level than members of the community, by default.
- *Popularity as data provider.* This is an assessment related to the experience, and reflects the opinion that other participants in the benchmarking activities have with regards to the quality and the usefulness of the data provided by the data source over time. By default, popularity is set to 0.

All the above-listed aspects need to be balanced (i.e. weighed) in order to come up with a trust value associated to each particular data source. The initial values of each parameter are fixed by default and revised on a regular basis, to reflect their actual performance over time.

Procedures to monitor and assess the trust value associated to each participant are critical. They need to be defined and the necessary resources to support their implementation and operation should be put in place before the benchmarking services are offered by ACDC to the wider community outside the project.

5.4.3. Incentives program

In order to engage stakeholders in the participation in an initiative that implies disclosing (to a certain level) information valuable for business activity, it is of the utmost importance to offer very attractive reasons to join and a good loyalty strategy to keep them active. The design of a good incentives program is a task that implies analysing each of the groups of stakeholders; evaluate their interests and challenges trying to identify commonalities and differences to create custom and realistic offerings.

A set of incentives has been considered so far:

- *Know the relative cyber security ranking against my peer-group*

This could be used as a way to motivate members to enhance their performance in order to gain business reputation.

- *Tracking results over time*
  Participants to the benchmarking activities will have the possibility to track their activity along time and assess the evolution of their own results with regards to different aspects. Tracking the evolution against the results of their peers or with regards to the average should be also possible.
- *Contribute and receive information from a trusted community (ACDC stakeholders' community).*
  Data providers and data consumers would benefit from this incentive since reliable data of a decent quality level is a valuable asset in cybersecurity.
- *Transparency in the metrics used*
  Having access to the specification of the metrics used in certain benchmarks could be beneficial for understanding. It could further motivate the creation of custom implementations in corporate dashboards, e.g. for presentations to C-level management to justify investments in security.

The incentives program is very closely related to the Trust Model for information sharing described in the previous section and both are inter-dependent in the sense that higher levels of trust will be rewarded. The following rewards have been considered:

- *Gaining Positive Reputation*
  - Appear as one of the top performers in cyber-security
  - Appear as the one with the best positive evolution over time
  - Appear as one of the top data providers to the benchmarks
  - Appear as "trusted" member of ACDC
- *Preferential treatment based on contribution* (e.g. getting a discount in yearly membership rate)
  - Based in the volume of data
  - Based in the quality of the data (e.g. confirmed bot IPs and bot ID)
  - Based in the provision of rare data (e.g. C&C servers)

On the other hand, a negative evolution in the trust scale in time needs to be punished somehow. Some incentive trusts have been considered as well:

- Show any kind of underperformance in cyber-security against my peers.
- Show a negative evolution of results over time.
- Being perceived as a lurker[xiv]
- Have a limitation in the quota allowed to contribute/consume from the CCH

In the implementation of these incentives, the CP would play an important role. It could serve to animate specific communities to launch regular benchmarking campaigns focused on particular aspects, or to involve members to participate and keep them regularly updated on performance trends and evolution.

6. Conclusion

The document presented the results of Task 4.2, compiling a database of botnet metrics, describing and specifying them, that permit the analysis of the cyber-security related information shared in the CCH in terms of quality and volume. The metrics here have been grouped into three categories: data quality metrics, botnet impact metrics and operational metrics. These metrics are used to create benchmarks that permit comparing the data sources that submit data to the CCH by focusing in different aspects (e.g. volume, quality, distribution, categories of reports). Other benchmarks focus on evaluating the impact of botnet activities and allowing a temporal assessment of the presence of bots in different countries, ISPs and ASNs. Benchmarks oriented to evaluate the operation of the ACDC infrastructure in the context of experiments (e.g. WP3 pilot experiments) have been also proposed.

The document describes an implementation of an infrastructure (i.e. Statistics Server) that computes metrics for regular time intervals (by default 1 day) and makes the results available for various purposes such as the research and evaluation of botnet impact and trends, or for the visualization of these results in the form of graphical charts and end-user dashboards. The ACDC Community Portal has a dedicated section on “Botnet Metrics” to compile and explain all metrics developed and to visualize the results of the metrics computed each day in the Statistics Server using different types of graphs.

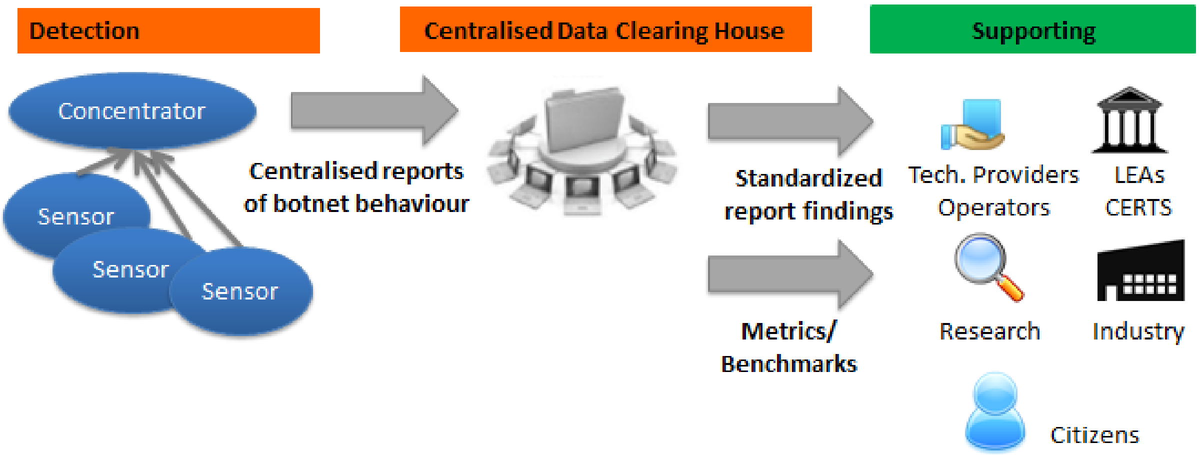
This deliverable document presented the results of the work conducted in Task 4.5 to define a model that incentivizes cybersecurity-related market actors to contribute to ACDC benchmarking activities, by sharing information with the ultimate goal of fighting botnets. The document proposes using this model to support the Benchmarking-as-a-Service proposal described in deliverable D5.2.2.

Annex I: Questionnaire

Questionnaire: Cyber Security Benchmarks and Incentives Model

6.1. *Introduction to ACDC*

ACDC (Advanced Cyber Defence Centre) is a European pilot project funded under the CIP-PSP programme[1]. The ACDC project runs over 30 months from 01/02/2013 to 31/07/2015.
ACDC aims to deploy an infrastructure of interconnected support centres across European Member States linked to a central ACDC clearing house (in short CCH). The goal of the infrastructure is to provide solutions to users to fight botnets, and to build up through data collection an analysis capability of botnets occurrence and behaviour to also provide early detection of emerging botnets. ACDC therefore aims to improve prevention, detection and mitigation of botnets.


Detection
Centralised Data Clearing House
Supporting
Concentrator
Sensor
Sensor
Sensor
Centralised reports of botnet behaviour
Standardized report findings
Metrics/ Benchmarks
Tech. Providers Operators
LEAs CERTS
Research
Industry
Citizens

ACDC unites a community of 28 organisations from 14 countries, including Internet Service Providers, CERTs, law enforcement agencies, IT providers, National Research and Education Networks (NRENs), academia and critical infrastructure operators.
More information can be found at the project website: http://www.acdc-project.eu/

6.2. *Motivation for this questionnaire*

One of ACDC services is meant to enable users (ACDC stakeholders) to not only identify cybersecurity strengths and weaknesses, but also compare, in an unbiased manner, their security status against those of their peers, this is (anonymous) organizations that have a similar profile.
The purpose of this questionnaire is to identify those benchmarks that can be useful for you, as well as to find incentive models to promote the contribution to these benchmarks.

[1] http://ec.europa.eu/information_society/activities/ict_psp/index_en.htm

6.3. Benchmarks

6.3.1. What kind of benchmarks are you interested in?

Add "X" where applicable. Multiple answers are possible.

	any kind of cybersecurity benchmarks
	cybersecurity benchmarks specific to my sector of activity
	cybersecurity benchmarks specific to my peer group (user type)
	Other (indicate below)

6.3.2. What information would you like to see reflected in the benchmarks?

Add "X" where applicable. Multiple answers are possible.

	Cyber attacks
	Malicious websites
	Vulnerable websites
	Bots
	Spam campaigns
	Botnets
	Fast-flux service networks
	ISPs / ASNs
	Countries
	Tools/technologies
	IPs
	DNSs
	Other (indicate below)

6.3.3. What information related to your organisation would you be willing to share in the benchmarks?

In the following table mark with an "X' in the white cells the kind of information you would commit to sharing for each access mode. Add as many cells as necessary. Indicate N/A if the type of information is not applicable for your type of organisation.

Information	Access mode		
	Public/open access	Restricted (Anyone in the ACDC community)	Restricted (Only to Specific ACDC communities)
Cyber attacks			
Malicious websites			
Vulnerable websites			
Bots			
Spam campaigns			
Botnets			
Fast-flux service networks			
ISPs / ASNs			

Countries			
Tools/technologies			
IPs			
DNSs			
Other (indicate below)			

6.3.4. How would you think these benchmarks should be published?

According to what indicated in the previous question, please, indicate in the cells of the following table, what access mode you consider more suitable and pricing model you would be willing to adopt. Also, indicate in the cells of the table any other characteristic you consider is missing for each of the access mode.

	Freemium access	Based on price[1] (in addition to Freemium access characteristics)
Public/open access	Online access to a General Cybersecurity benchmarks dashboard view (no confidential information available)	N/A
Restricted access (ACDC membership)	Online access to a dashboard view with Cybersecurity benchmarks specific to my sector of activity (no confidential information available) Use of the ACDC membership badge Receive updates on metrics and benchmarks activities of other ACDC members	Access to benchmark definition and metrics specification Downloadable PDF reports Customization of the dashboard view (in terms of layout, aspect and charts displayed) Participation in the benchmarking activity Private view: Assessment of my own position with regards to other members of my sector of activity Possibility of publication of my position/results to the ACDC community benchmarks Possibility to be listed in my corresponding National Support Centre website.
Restricted		

[1] The pricing model can adopt different forms.

access (ACDC specific communities)	Online access to a dashboard view with Cybersecurity benchmarks specific to my peer group (user type or community) (no confidential information available) Use of the ACDC specific community membership badge Receive updates on metrics and benchmarks activities of other specific ACDC community members	Access to benchmark definition and metrics specification Downloadable PDF reports Customization of the dashboard view (in terms of layout, aspect and charts displayed) Participation in the benchmarking activity Private view: Assessment of my own position with regards to other members of my specific community Possibility of publication of my position/results in the specific community benchmarks. Possibility to be listed in my corresponding National Support Centre website.

6.4. How do you value the metrics proposed in the following subsections

6.4.1.1. Operational metrics

The operational metrics permit the evaluation of the performance of the end-to-end ACDC solution performing in a particular scenario in real-time. In the ACDC project, five experiments have been scheduled to recreate the conditions of some cyber-security typical scenarios: fast-flux domains detection (Fast-flux in short), malicious websites detection and malware analysis (Websites in short), detection and mitigation of DDoS attacks (DDoS in short), detection of malicious activities in mobile devices (Mobile in short) and spam campaigns analysis, prevention and mitigation (Spam in short). Each of the scenarios focuses on certain aspects aiming at detecting and improving response against proliferation of botnets. A set of metrics have been defined to evaluate the performance of the different types of tools integrated and working together towards achieving the objectives of each experiment.

Moreover, the ACDC project focuses especially in fighting against botnets. Therefore, in addition to the experiment-specific metrics, there have been developed a set of metrics that evaluate the impact of botnets activities in the world along time.

NOTE: Rank each metric according to your interest from 1 to 5, being 1 the less valuable and 5 the most valuable.

Botnet Metrics	Interesting? (Y / N)	Value (1-5)
Absolute count: Count of total number of infected IP addresses per country per day		
Absolute count: Count of total number of infected IP addresses per ISP (Internet Service Provider) per day		
Normalized count: Count of total number of infected IP addresses per country per day, normalized by total number of Internet subscribers		
Normalized count: Count of total number of infected IP addresses per country per day, normalized by total number of Internet subscribers		
Indexed time series across sources: Number of infected IP addresses aggregated by country per day, normalized by total number of Internet subscribers, indexed across multiple sources		
Indexed time series across sources: Number of infected IP addresses aggregated by ISP per day, normalized by total number of Internet subscribers, indexed across multiple sources.		
Ranking (borda count): Borda count is an aggregation of multiple rankings based on the normalized metric for different sources (count of infected IP address per country/ISP per day, normalized by total number of Internet subscribers)		

Fast-flux Metrics This experiment aims at the detection and mitigation of domains that implement fast-flux techniques in order to support botnet infrastructures.	Interesting? (Y / N)	Value (1-5)
Number of fast-flux domains detected per TLD (top level domain)		
Number of fast-flux domains detected per Country		
Number of fast-flux domains detected per ASN		
Number of total IP addresses used in Fast-flux techniques (Fast-flux bots) per Fast-flux domain		
Number of total IP addresses used in Fast-flux techniques (Fast-flux bots) per ASN		
Number of total IP addresses used in Fast-flux techniques (Fast-flux bots) per Country		
Total number of detected C&C (Command & Control) IP addresses per Country		
Total number of detected C&C (Command & Control) IP addresses per ASN		
Total number of different botnets detected related to Fast-flux domains.		

DDoS (Distributed Denial of Service) experiment Metrics This experiment aims at the analysis of attacks and mitigation of botnets used to perform DDoS attacks.	Interesting? (Y / N)	Value (1-5)
Total number of DDoS attacks detected		
Total number of DDoS attacks analyzed		
Number of total IP addresses identified as DDoS bots per attack		

Number of total IP addresses identified as DDoS bots per ASN		
Number of total IP addresses identified as DDoS bots per country		
Total number of detected C&C IP addresses per country		
Total number of detected C&C IP addresses per ASN		
Number of different botnets supporting DDoS attacks detected		

WEBSITES experiment Metrics This experiment aims at the detection and mitigation of malicious websites used to support main botnet activities like malware distribution and illicitly Internet activity like phishing, and identity theft. Identification of botnets used to attack and compromise websites**.**	Interesting? **(Y / N)**	Value (1-5)
Number of attacks to websites detected per ASN		
Number of attacks to websites detected per country		
Number of attacks to websites detected per TLD		
Number of bots attacking websites identified per ASN		
Number of bots attacking websites identified per country		
Number of suspicious websites analyzed per ASN		
Number of suspicious websites analyzed per country		
Number of suspicious websites analyzed per TLD		
Number of vulnerable websites analyzed per ASN		
Number of vulnerable websites analyzed per country		
Number of vulnerable websites analyzed per TLD		
Number of analyzed malware distributed from websites		
Number of detected C&C IP addresses related to malicious websites per ASN		
Number of detected C&C IP addresses related to malicious websites per country		
Number of different botnets detected with malicious websites involved		

MOBILE experiment Metrics This experiment aims at the detection and mitigation of botnets affecting mobile devices.	Interesting? **(Y / N)**	Value (1-5)
Number of suspicious mobile events analysed per malicious activity		
Number of Network events related to HTTP protocol (malicious URI - Uniform Resource Identifier) analyzed		
Number of Application events related to malware		
Number of SMS events related to spam		
Number of SMS events related to C&C messages		
Number of Hardware events related to malicious activities		
Number of APKs analysed		
Number of suspicious/malicious APKs detected		
Number of total mobile bots identified		
Number of detected C&C involved in malicious mobile activities		
Number of different botnets detected with mobile devices involved		

SPAM experiment Metrics This experiment aims at the detection and mitigation of spam botnets used as infection channels and as a vehicle of a lot of botnet activities.	Interesting? **(Y / N)**	Value (1-5)
Total number of detected spam per country		
Total number of detected spam per ASN		
Number of single IP addresses sending spam per ASN		
Number of single IP addresses sending spam per country		
Total number of detected spambots per country		
Total number of detected spambots per ASN		
Total number of detected spambots per campaign		
Total number of detected C&C IP addresses per Country		
Total number of detected C&C IP addresses per ASN		
Total number of detected botnets related to spam campaigns		
Number of spam campaigns detected distributing malware in attachment		
Number of spam campaigns detected distributing malicious URLs		
Total number of URLs analysed per TLD		
Total number of (malicious) URLs sent by spambots		
Total number of attachments analysed		

6.4.1.2. Technology-related metrics

To enable the comparison of the performance of the technologies deployed, some metrics have been defined to evaluate, along a pre-defined period of time, the quantity and quality of the information that the tools report to the CCH. The quality of the information reported by the tools is evaluated **in comparison to events confirmed** by CERTs and NSCs. It is evaluated the false positives and true positives but also the delay in detecting true positives.

The technologies are also assessed in their contribution to the joint work of fighting botnets and detecting, analysing and preventing cyber threats. To measure that contribution, there have been proposed metrics that assess the relevance of the information shared by tools in achieving the objective of detecting attacks, bots, botnets, etc.

Technology-related Metrics	Interesting? **(Y / N)**	Value (1-5)
Total detected confirmed attack (by subcategory: DoS, abuse, compromise, etc.)		
Total detected confirmed Bots (by subcategory: spam bot, fast flux bot, DDoS bot)		
Total detected confirmed C&C servers		
Total detected confirmed Fast-flux domains		
Total detected confirmed Malicious URIs		
Total detected confirmed Vulnerable URIs		
Total detected confirmed Malware samples		
Total detected confirmed Botnets (by subcategory: p2p, c&c, etc.)		
Total detected confirmed Spam campaigns		
Delay (in milliseconds) in detecting a confirmed attack (by subcategory: DoS, abuse, compromise, etc.)		
Delay (in milliseconds) in detecting a confirmed Bot		
Delay (in milliseconds) in detecting a confirmed C&C server		
Delay (in milliseconds) in detecting a confirmed FF domain		
Delay (in milliseconds) in detecting a confirmed Malicious URI		
Delay (in milliseconds) in detecting a confirmed Vulnerable URI		
Delay (in milliseconds) in detecting a confirmed Botnet (by subcategory: p2p,		

Technology-related Metrics	Interesting? **(Y / N)**	Value (1-5)
c&c, etc.)		
Delay (in milliseconds) in detecting a confirmed Spam campaign		
Total wrongly detected attacks (by subcategory: DoS, abuse, compromise, etc.)		
Total wrongly detected Bots (by subcategory: spam bot, fast flux bot, DDoS bot)		
Total wrongly detected C&C servers		
Total wrongly detected Fast-flux domains		
Total wrongly detected Malicious URIs		
Total wrongly detected Vulnerable URIs		
Total wrongly detected Malware samples		
Total wrongly detected Botnets (by subcategory: p2p, c&c, etc.)		
Total wrongly detected Spam campaigns		
% Contribution to detecting attacks (by subcategory: DoS, abuse, compromise, etc.)		
% Contribution to detecting Bots (by subcategory: spam bot, fast flux bot, DDoS bot)		
% Contribution to detecting C&C servers		
% Contribution to detecting Fast-flux domains		
% Contribution to detecting Malicious URIs		
% Contribution to detecting Vulnerable URIs		
% Contribution to detecting Malware samples		
% Contribution to detecting Botnets (by subcategory: p2p, c&c, etc.)		
% Contribution to detecting Spam campaigns		

6.4.2. Dashboard

The ACDC dashboard is an online tool that supports the publication of benchmarking results. The ACDC dashboard aims at tailoring to user profiles, using custom graphic metaphors and vocabulary to reach all types of users from technical staff or C-level management (e.g. CISO, CTO) to non-technical citizens (e.g. through National Support Centers websites), and satisfy each level of information needs. The dashboard is a web-based GUI composed by different charts that can be organized into views, each one displayed as a web page. The dashboard views can be customized according to each end-user profile in terms of content and layout/look and feel. Access to the custom dashboard is handled by an access management module, which allows defining user-level granularity access policies, and control the information displayed as well as the customization of graphical aspects.

As an illustration of the graphical metaphors available in the Atos reporting dashboard, a screenshot showing a sample view page with different types of charts is depicted in Figure 12.

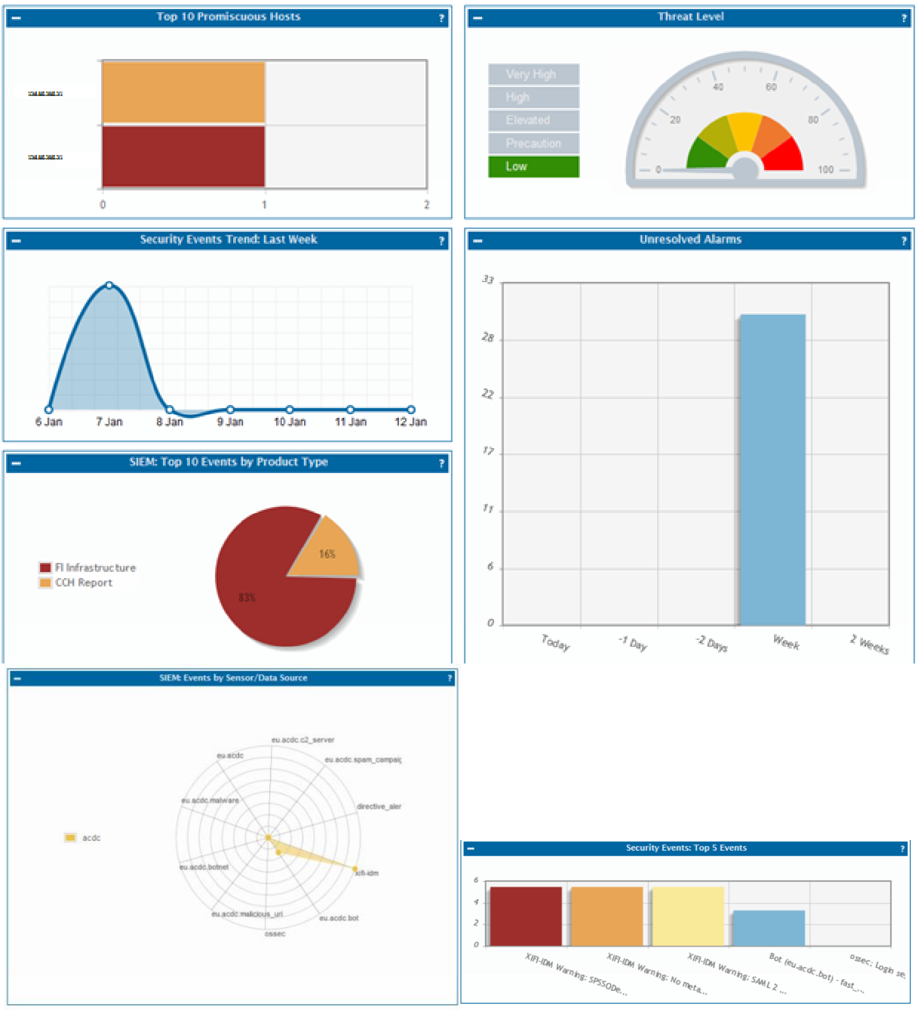


Figure 12 A reporting dashboard view page with some sample charts

Please, mark with an 'X' the charts from the left column that are relevant, from your view point, for each of the dashboard views listed in the other columns. Multiple options are possible.

Chart type	Executive (C-level) View	Operational View	Tool benchmarking view	Citizen (NSCs) view
Overall Threat Level				
Last Cyber Sec Events				
Cybersec Events Trend				
Last Incidents occurred				
Incidents Trend				
Top 10 Malicious URIs				
Top 10 Vulnerable URIs				
Top 10 Malware Exploits				
Top 10 Vulnerabilities				
Top 10 C&C Servers				
Top 10 Fast-flux domains				
Top 10 Security Events by Type				
C&C Servers by Countries				
Attack Sources by Countries				
Malicious Websites by Countries				
Average Confidence Level of Reports				
Top 10 Promiscuous Hosts				
Top 10 Hosts with Multiple Events				
Malware Exploits ID (identifier)				
Vulnerabilities ID				
Destination TCP/UDP Ports				
Attacks by Subcategories				
Malicious Websites by Subcategories				
C&C Servers by Subcategories				
Top 10 Tools on Bots detection				
Top 10 Tools on C&C Servers				

detection				
Top 10 Tools on Fast-Fllux Domains Detection				
Top 10 Tools on Malicious URI Detection				
Top 10 Tools on Vulnerable URI Detection				
Top 10 Tools on Malware Detection				
Top 10 Tools on Botnets detection				
Top 10 Tools on confidence level of information shared				
Others (list below)				

6.5. Trust and Incentives

6.5.1. The trust level of the information used to calculate metrics should be determined based on the following factors:

Add "X" where applicable. Multiple answers are possible.

	The confidence level of the data source (e.g: data sensor feeding into the CCH)
	The level of contribution (e.g: amount of shared information)
	The quality of the information provided over time
	Type of data provider (e.g: research, industry, technology provider, CERT)
	Relation with ACDC: Community membership
	Relation with ACDC: Community endorsement
	Relation with ACDC: Community of interest (e.g. ISAC[1]s) within ACDC
	Popularity as Data Provider (other's perception)
	Other (indicate below)

6.5.2. What would be a valuable incentive for you to share information for metrics?

[1] ISAC - Information Sharing and Analysis Center

Add "X" where applicable. Multiple answers are possible.

	Know the relative cyber-security ranking against my peer-group
	Contribute and receive information from a trusted community (ACDC community)
	Transparency in the metrics used
	Transparency in the enforcement of participation rules
	Being displayed in the dashboard as one of the top performers in cyber-security
	Being displayed in the dashboard as one of the top data providers
	Being displayed in the dashboard as a one of the trusted members of ACDC
	Obtain a preferential treatment or reward (e.g. free upgrade in the access mode, custom benchmarks reports, etc.) based on high quality data contribution
	Other (indicate below)

6.5.3. What kind of incentive trusts[1] could prevent you from participating?

Add "X" where applicable. Multiple answers are possible.

	Having displayed in the dashboard any kind of underperformance in cyber-security against my peers.
	Having displayed in the dashboard a strong underperformance in cyber-security against my peers.
	Being perceived as a lurker[2] within the ACDC community
	Other (indicate below)

6.5.4. Why do you think publishing benchmarks could be beneficial for fighting botnets and cybersecurity in general?

Add "X" where applicable. Multiple answers are possible.

	Boosting competitiveness towards excellence
	Collaboration to enhance preparedness and prompt reaction to attacks
	Standardization of methodologies for cybersecurity incident prioritization, reporting and management
	Wider societal impact and more effective awareness raising
	Other (indicate below)

[1] Incentive trust definition: http://en.wikipedia.org/wiki/Incentive_trust

[2] Lurker definition: http://en.wikipedia.org/wiki/Lurker

6.5.5. *Please insert, if you wish, further comments in order to enrich your answers.*

Annex II: Metric Schema in JSON format

```
{
   "title": "ACDC dataset for aggregated or correlatied data",
   "description": "This is the schema for aggregated data that is intended to be used by the research
workflow and workflows devoted to WP4. It is important to note, that data format must not contain
any data that is directly related to a person.",
   "properties": {
      "report_id": {
         "title": "Report ID",
         "description": "The ID of the report in the CCH. This will be set by the CCH and is thus
overwritten on import.",
         "type": "string"
      },
      "report_category": {
         "title": "Report category",
         "description": "The category of the report. This links the report to one of ACDC's schemata.
This report category has the format 'eu.acdc.metric",
         "type": "string"
      },
     "report_subcategory": {
         "title": "Report subcategory",
         "description": "The subcategory of the report. This is used to categorise different types of
similar reports that have mostly the same fields. It is defined as an enum in the schema of the report
category.",
         "type": "string",
        "enum": ["quality_metric", "ip_based_metric", "event_based_metric", "other_metric"]
      },
      "report_type": {
         "title": "Report type",
         "description": "The type of the report. This is a free text field characterising the report that
should be used for a human readable description rather than for automatic processing. As a rule of
thumb this should not be longer than one sentence.",
         "type": "string"
      },
      "timestamp": {
         "title": "Starting date of the measurement window",
         "description": "The timestamp details the starting date of the measurement windows. All
reports whose original timestamp (This can for example be when an attack occurred, when a
malware hosting was observed, or when a compromise took place according to log files.) falls into
the period of the measurement window (timestamp, timestamp + measurement_window) are
covered by the report.",
         "type": "string",
         "format": "date-time"
      },
      "reported_at": {
         "title": "Time of the report's submission",
         "description": "The timestamp when the report was submitted to the CCH. This will be set by
the CCH and is thus overwritten on import.",
         "type": "string",
         "format": "date-time"
      },
     "measurement_window": {
         "title": "Time frame of measurement",
         "description": "Time frame of measurement in seconds",
         "type": "integer",
         "minimum" : 0
      },
     "metric_id": {
        "title": "ID of Metric",
        "description": "ID of Metric, all metrics are summarised and specified in an external
document.",
         "type": "integer"
     },
     "metric_result": {
        "title": "Result of Metric",
        "description": "Resulting data (unstructured) of application of metric",
        "type": "object"
     },
     "metric_description": {
         "title": "Description of the metric.",
         "description": "Detailed description of metrics. This field complements the report_type if a
more specififc or additional decription is intended.",
         "type": "string"
      },
      "version": {
         "title": "Version of the format",
         "description": "The version number of the data format used for the report.",
         "type": "integer",
         "enum": [1]
      }
   },
   "required": ["report_category", "report_type", "timestamp", "measurement_window",
"metric_id", "metric_result", "version"]
}
```

Quality metrics: Data sources per Submission Key

ID: 15

Objectives: The metric aims at identifying gaps or anomalies in the data that might be caused by a failure of the data submission or the sensor. This is achieved by computing the total number of reports pertaining all data sources in a specific time interval. Data sources are unique keys that are used to submit data to the CCH. In the context of the metrics, gaps are time intervals where no reports are submitted or where the number is significantly less than the average number of reports.

Data selection and Quality Criteria: This metric is applied to all data sources (CCH keys) that submit data to the CCH. Since this metric is used to assess the data quality, no quality criteria are expected

Data Enrichment: -

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for api_key _id, report_category in LIST_CCH_SUBMISSION_KEYS,
LIST_REPORT_CATEGORIES:
   RESULT[api_key_id, report_category] =
number_of_reports_that_match(key, category, MEASUREMENT_WINDOW)
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric

Legal Statement: No person related information are contained.

Quality metrics: Data Distribution per Submission Key

ID: 16

Objectives: The metric aims at identifying gaps or anomalies in the data that pertain the distribution of reported systems. The metric computes the number of reports that are associated to ASNs and if feasible networks. The assumption is that anomalies and gaps distort the statistical stability of the data.

Data selection and Quality Criteria: This metric is applied to all data sources (CCH keys) that submit data to the CCH. Since this metric is used to assess the data quality, no quality criteria are expected.

Data Enrichment: -

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for all api_key_id, report_category:
   for asn in LIST_ASN:
      RESULT[asn, api_key_id, report_category] =
number_of_reports_that_match(asn, MEASUREMENT_WINDOW)
```

Data Exchange Format: eu.acdc.aggregation_type: metric

Legal Statement: No person related information are contained.

Comparative metrics: Daily BotIDs / country user

ID: 17

Objectives: Aim is to compare the number of unique bots per country. To address the different population of each country the overall number should be normalised with the individual population of the specific country.

Data selection and Quality Criteria: This metric requires a unique bot ID in the data. Therefore, only data sources are applicable that comprises such identification.

Data Enrichment: -

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for all api_key_id, report_category:
  for country in LIST_COUNTRIES:
     RESULT[country,report_category, api_key_id] =
number_of_unique_botIDs_that_match(country_of(source_IP) is in country) /
population(country)
```

Data Exchange Format: eu.acdc.aggregation / aggregation_type: metric

Legal Statement: No person related information are contained

Comparative metrics: Daily BotIDs / ASN-IP

ID: 18

Objectives: Aim is to compare the number of unique bots per ASN To address the different population of each country the overall number should be normalised with the individual number of IP addresses within the ASN.

Data selection and Quality Criteria: This metric requires a unique bot ID in the data. Therefore, only data sources are applicable that comprises such identification.

Data Enrichment: -

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for all api_key_id, report_category:
  for ASN in LIST_ASN:
     RESULT[ASN,report_category, api_key_id] =
number_of_unique_botIDs_that_match(country_of(source_IP) is in ASN) /
ips(ASN)
```

Data Exchange Format: eu.acdc.aggregation / aggregation_type: metric

Legal Statement: No person related information are contained

Comparative metrics: Daily BotIDs / partner or ISP

ID: 19

Objectives: Aim is to compare the number of unique bots per country.

Data selection and Quality Criteria: This metric requires a unique bot ID in the data. Therefore, only data sources are applicable that comprises such identification.

Data Enrichment: -

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for all api_key_id, report_category:
  for partner_id in LIST_PARTNER:
     RESULT[partner_id,report_category, api_key_id] =
number_of_unique_botIDs_that_match(country_of(source_IP) is in partner)
```

Data Exchange Format: eu.acdc.aggregation / aggregation_type: metric

Legal Statement: No person related information are contained

IP-based metrics: Unique daily IPs per country user

ID: 2

Objectives: Aim is to compare the number of unique IPs per country. To address the different population of each country the overall number should be normalised with the individual population of the specific country.

Data selection and Quality Criteria: This metric applies only for IPv4 addresses in the data. Per default, all reports that contain a source IPv4 address are considered by this metrics. Moreover, the metric should be computed for each submission_key separately. If required a blacklist comprising known benign scanners could be applied before the metric is computed.

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for all api_key_id, report_category:
    for country in LIST_COUNTRIES:
     RESULT[country, report_category, api_key_id] =
number_of_unique_IPs_that_match(country_of(source_IP) is country) /
population(country)
```

Data Exchange Format: eu.acdc.aggregation / aggregation_type: metric

Legal Statement: No person related information are contained

IP -based metrics: Unique daily IPs per ASN-IP

ID: 1

Objectives: Aim is to compare the number of unique IPs per asn. To address the different population of each country the overall number should be normalised with the individual population of the specific country.

Data selection and Quality Criteria: This metric applies only for IPv4 addresses in the data. Per default, all reports that contain a source IPv4 address are considered by this metrics. Moreover, the metric should be computed for each submission_key separately. If required a blacklist comprising known benign scanners could be applied before the metric is computed.

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for all api_key_id, report_category:
    for ASN in LIST_ASN:
     RESULT[ASN, report_category, api_key_id] =
number_of_unique_IPs_that_match(country_of(source_IP) is country) /
population(country)
```

Data Exchange Format: eu.acdc.aggregation / aggregation_type: metric

Legal Statement: No person related information are contained

IP -based metrics: Unique daily IPs per ISP-Subscriber

ID: 3

Objectives: Aim is to compare the number of unique bots per country. To address the different population of each country the overall number is normalised with the individual population of the specific country.

Data selection and Quality Criteria: This metric applies only for IPv4 addresses in the data. Per default, all reports that contain a source IPv4 address are considered by this metrics. Moreover, the metric should be computed for each submission_key separately. If required a blacklist comprising known benign scanners could be applied before the metric is computed.

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for all api_key_id, report_category:
    for partner_id in LIST_PARTNERS:
     RESULT[partner_id, report_category, api_key_id] =
number_of_unique_IPs_that_match(country_of(source_IP) is country) /
population(country)
```

Data Exchange Format: eu.acdc.aggregation / aggregation_type: metric
Legal Statement: No person related information are contained

Proxy-based metrics: Daily events per country user

ID: 4

Objectives: Depending on the type of attack, we can also explore compare the impact of the attack for different ISPs, countries, and ASNs. For example, in the case of spam, one metric which is also important is the number of spam messages each bot has sent, and total number of bots.

Data selection and Quality Criteria: The metric requires the selection of specific attacks or report types such as spam related reports. Moreover, the metric should be computed for each submission_key separately.

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for all api_key_id, report_category:
  for country in LIST_COUNTRIES:
    RESULT[country, report_category, api_key_id] =
number_of_unique_Reports_that_match(country_of(source_IP) is country) /
population(country)
```

Data Exchange Format: eu.acdc.aggregation / aggregation_type: metric
Legal Statement: No person related information are contained

Proxy-based metrics: Daily events per ASN-IP

ID: 5

Objectives: Depending on the type of attack, we can also explore compare the impact of the attack for different ISPs. For example, in the case of spam, one metric which is also important is the number of spam messages each bot has sent, and total number of bots.

Data selection and Quality Criteria: The metric requires the selection of specific attacks or report types such as spam related reports. Moreover, the metric should be computed for each submission_key separately.

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for all api_key_id, report_category:
  for ASN in LIST_ASN:
    RESULT[ASN, report_category, api_key_id] =
number_of_unique_Reports_that_match(country_of(source_IP) is country) /
ips(ASN)
```

Data Exchange Format: eu.acdc.aggregation / aggregation_type: metric
Legal Statement: No person related information are contained

Proxy-based metrics: Daily events per ISP Subscriber

ID: 6

Objectives: Depending on the type of attack, we can also explore compare the impact of the attack for different ISPs, countries, and ASNs. For example, in the case of spam, one metric which is also important is the number of spam messages each bot has sent, and total number of bots

Data selection and Quality Criteria: The metric requires the selection of specific attacks or report types such as spam related reports. Moreover, the metric should be computed for each submission_key separately.

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for all api_key_id, report_category:
  for partner_id in LIST_PARTNERS:
    RESULT[partner_id, report_category, api_key_id] =
number_of_unique_Reports_that_match(country_of(source_IP) is country) /
ips(partner)
```

Data Exchange Format: eu.acdc.aggregation / aggregation_type: metric

Legal Statement: No person related information are contained

RDNS-based metrics: Unique daily IPs with the same second level domain (e.g. dtag.de) per day

ID: 7

Objectives: Aim is to compare the number of unique IPs per second-level domain

Data selection and Quality Criteria: This metric applies only for IPv4 addresses in the data. Per default, all reports that contain a source IPv4 address are considered by this metrics. Moreover, the metric should be computed for each submission_key (api_key_id) separately. If required a blacklist comprising known benign scanners could be applied before the metric is computed.

Data Enrichment: -

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
DOMAIN_LIST = ()     # list of unique second level domains
RESULT = []          # hash key=second level domain, value number of
unique IPs

for domain in DOMAIN_LIST:
  sdl = retrieve_sdl(domain)
  for all api_key_id, report_category:
    RESULT[sdl, report_category, api_key_id] =
sum_of_unique_ips_matching(sdl, report_category, api_key_id)
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric

Legal Statement: No person related information are contained.

RDNS-based metrics: Unique daily events/reports with the same second level domain (e.g. dtag.de) per day

ID: 22

Objectives: Aim is to compare the number of reports per second-level domain.

Data selection and Quality Criteria: This metric applies only for IPv4 addresses in the data. Per default, all reports that contain a source IPv4 address are considered by this metrics. Moreover, the metric should be computed for each submission_key (api_key_id) separately. If required a blacklist comprising known benign scanners could be applied before the metric is computed.

Data Enrichment: -

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
DOMAIN_LIST = ()     # list of unique second level domains
RESULT = []          # hash key=second level domain, value number of
unique IPs

for domain in DOMAIN_LIST:
  sdl = retrieve_sdl(domain)
  for all api_key_id, report_category:
    RESULT[sdl, report_category, api_key_id] =
sum_of_reports_matching(sdl, report_category, api_key_id)
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric
Legal Statement: No person related information are contained.

Tool-based: Quality Metric – Average Confidence level

ID: 8

Objectives: This metric aims at evaluating the quality of the data submitted by tools to the CCH, based on the confidence level value associated to each report. The metric takes as a basis the API Write Key ID, to identify the different tool submitting reports and the type of report.

Data selection and Quality Criteria: This metric is applied to all data sources (CCH keys) that submit data to the CCH. Since this metric is used to assess the data quality, no quality criteria are expected.

Data Enrichment: By using the mapping between API Write Key ID and the key owner, associated report category and potentially the tool

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for key in LIST_CCH_SUBMISSION_KEYS
   RESULT[key] = Avg (confidence_level_of_reports_that_match(key,
MEASUREMENT_WINDOW))
     RESULT[category] = Avg
(confidence_level_of_reports_that_match(category, MEASUREMENT_WINDOW))
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric
Legal Statement: No person related information are contained.

Tool-based: Distribution Metric – Volume of reports per ASN

ID: 9

Objectives: This metric aims at evaluating the distribution of the data submitted by tools to the CCH. The metric takes as a basis the API Write Key ID, to identify the different tool submitting reports and the type of report, and the ASN associated to the report.

Data selection and Quality Criteria: This metric is applied to all data sources (CCH keys) that submit data to the CCH. Since this metric is used to assess the data quality, no quality criteria are expected.

Data Enrichment: By using the mapping between API Write Key ID and the key owner, associated report category and potentially the tool.

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for key in LIST_CCH_SUBMISSION_KEYS
   RESULT[key] = number_of_reports_that_match(key,
asn_of(source_ip),MEASUREMENT_WINDOW))
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric

Legal Statement: No person related information are contained.

Tool-based: Distribution Metric – Volume of reports per Country

ID: 10

Objectives: This metric aims at evaluating the distribution of the data submitted by tools to the CCH. The metric takes as a basis the API Write Key ID, to identify the different tool submitting reports and the type of report, and the country associated to the report.

Data selection and Quality Criteria: This metric is applied to all data sources (CCH keys) that submit data to the CCH. Since this metric is used to assess the data quality, no quality criteria are expected.

Data Enrichment: By using the mapping between API Write Key ID and the key owner, associated report category and potentially the tool.

Data Processing:

```
   START_TIME = current_date at 0:00:00
   MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
   for key in LIST_CCH_SUBMISSION_KEYS
      RESULT[key] = number_of_reports_that_match(key,
country_of(source_ip),MEASUREMENT_WINDOW))
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric

Legal Statement: No person related information are contained.

Quality metrics – Notification phase: Reports per ASN

ID: 11

Objectives: This metric aims at calculating the percentage of reports that tools send to the CCH, and that are suitable for notification by the corresponding ASN. That is reports with confidence level > 0.8. The metric takes as a basis the API Write Key ID, to identify the different tool submitting reports and the type of report.

Data selection and Quality Criteria: This metric is applied to all data sources (CCH keys) that submit data to the CCH. Since this metric is used to assess the data quality, no quality criteria are expected. For the duration of the WP3 experiments, the list of ASNs of interest should be restricted to those participating in ACDC.

Data Enrichment: By using the mapping between API Write Key ID and the key owner, associated report category and potentially the tool.

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for key in LIST_CCH_SUBMISSION_KEYS
   for asn in LIST_ASN_IN_ACDC
      RESULT[key, asn] = number_of_reports_that_match(key, asn,
conf_level>0.8,MEASUREMENT_WINDOW)) / number_of_reports_that_match(key,
MEASUREMENT_WINDOW))
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric
Legal Statement: No person related information are contained.

DDOS metrics – DDOS Attacks Volume by Subcategory

ID: 12
Objectives: The aim is to know the volume of reports of category eu.acdc.attack, subcategory dos.*, per type of DDoS attack, for each unique target IP. The metric takes as a basis the API Write Key ID, to identify the different tool submitting reports and the type of report.
Data selection and Quality Criteria: This metric is applied to all data sources (CCH keys) that submit data to the CCH. The quality criteria would be based on the confidence_level value of the reports, that must be > 0.8 (that is, suitable for notification)
Data Enrichment: By using the mapping between API Write Key ID and the key owner, associated report category and potentially the tool.
Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for key in LIST_CCH_SUBMISSION_KEYS
   for dos_subcat in [tcp,udp,dns, http,..]
   RESULT[key,dos_subcat] =
number_of_unique_dst_ip_reports_that_match(key, dos_subcat,
conf_level>0.8,MEASUREMENT_WINDOW))
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric
Legal Statement: No person related information are contained.

MALWARE metrics –Volume per Day

ID: 13
Objectives: The aim is to know the volume of reports of unique malware samples (i.e. category eu.acdc.malware) sent to the CCH per day. The metric takes as a basis the API Write Key ID, to identify the different tool submitting reports and the type of report.
Data selection and Quality Criteria: This metric is applied to all data sources (CCH keys) that submit data to the CCH. The quality criteria would be based on the confidence_level value of the reports, that must be > 0.8 (that is, suitable for notification).
Data Enrichment: By using the mapping between API Write Key ID and the key owner, associated report category and potentially the tool.
Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for key in LIST_CCH_SUBMISSION_KEYS
   RESULT[key] = number_of_unique_malware_reports_that_match(key,
conf_level>0.8,MEASUREMENT_WINDOW))
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric
Legal Statement: No person related information are contained.

MALWARE metrics – Mobile Malware Volume per Day

ID: 14
Objectives: The aim is to know the volume of reports of unique malware samples (i.e. category eu.acdc.malware) sent to the CCH per day detected in mobile devices (using the optional field ‘mime_type’ = 'application/vnd.android.package-archive' of eu.acdc.malware reports). The metric takes as a basis the API Write Key ID, to identify the different tool submitting reports and the type of report.

Data selection and Quality Criteria: This metric is applied to all data sources (CCH keys) that submit data to the CCH. The quality criteria would be based on the confidence_level value of the reports, that must be > 0.8 (that is, suitable for notification).

Data Enrichment: By using the mapping between API Write Key ID and the key owner, associated report category and potentially the tool.

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for key in LIST_CCH_SUBMISSION_KEYS
   RESULT[key] = number_of_unique_mobile_malware_reports_that_match(key,
conf_level>0.8,MEASUREMENT_WINDOW))
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric

Legal Statement: No person related information are contained.

Quality metrics – false positives per partner

ID: 20

Objectives: The aim is to determine the rate of false-positives per CCH submission key / data source. Currently, the following criteria are implemented:

- private IP addresses
- malformed reports
- reports that violate explicit or implicit criteria if the format definition

Data selection and Quality Criteria: This metric is applied to all data sources (CCH keys) that submit data to the CCH.

Data Enrichment:

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
RESULT[api_key_id] = 0
for report, api_key_id in LIST_UNIQUE_IPs, LIST_CCH_SUBMISSION_KEYS
   if ip.report in set(PRIVATE_IP_ADDRESSES):
      RESULT[api_key_id] += 1
          continue
     if JSON(report_category) does not match schema:
      RESULT[api_key_id] += 1
      continue
     if JSON(report) violates format properties:
          # further specification required
      RESULT[api_key_id] += 1
      continue
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric

Legal Statement: No person related information are contained.

Quality metrics: Reliable Data sources per Submission Key

ID: 21

Objectives: The metric aims at identifying gaps or anomalies in the data that might be caused by a failure of the data submission or the sensor. This is achieved by computing the total number of reports pertaining all data sources in a specific time interval whose confidence level exceed 0.8. Data sources are unique keys that are used to submit data to the CCH. In the context of the metrics, gaps are time intervals where no reports are submitted or where the number is significantly less than the average number of reports.

Data selection and Quality Criteria: This metric is applied to all data sources (CCH keys) that submit data to the CCH. Since this metric is used to assess the data quality, no quality criteria are expected.

Data Enrichment: -

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for api_key_id, report_category in LIST_CCH_SUBMISSION_KEYS,
LIST_REPORT_CATEGORIES:
   RESULT[api_key_id, report_category] =
number_of_reports_that_match(key, category, MEASUREMENT_WINDOW) and
(confidence_level(report) > 0.8
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric

Legal Statement: No person related information are contained.

Quality metrics: Number of reports per Attack subcategory

ID: 23

Objectives: The metric aims at identifying gaps or anomalies in the data that might be caused by a failure of the data submission or the sensor. This is achieved by computing the total number of reports per attack subcategory and CCH submission key.

Data selection and Quality Criteria: This metric is applied to all data sources (CCH keys) that submit data to the CCH. Since this metric is used to assess the data quality, no quality criteria are expected.

Data Enrichment: -

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for api_key_id, report_subcategory:
   RESULT[api_key_id, report_subcategory] =
number_of_reports_that_match(key, report_sub)
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric

Legal Statement: No person related information are contained.

Quality metrics: Number of reports per Attack subcategory counted by unique IP

ID: 24

Objectives: The metric aims at identifying gaps or anomalies in the data that might be caused by a failure of the data submission or the sensor. This is achieved by computing the total number of reports per attack subcategory and CCH submission key.

Data selection and Quality Criteria: This metric is applied to all data sources (CCH keys) that submit data to the CCH. Since this metric is used to assess the data quality, no quality criteria are expected.

Data Enrichment: -

Data Processing:

```
START_TIME = current_date at 0:00:00
MEASUREMENT_WINDOW = (START_TIME, START_TIME + 86400 sec)
for api_key_id, report_subcategory:
   RESULT[api_key_id, report_subcategory] =
number_of_reports_that_match_and_have_unique_ips(key, report_sub)
```

Data Exchange Format: eu.acdc.aggegation / aggregation_type: metric

Legal Statement: No person related information are contained.

Annex IV Atos SLSIEM dashboard

Dashboard view	Charts	Chart Description
Public	Top 10 cybersecurity event categories	Pie chart showing the top 10 categories of reports in terms of volume (for the last 15 days)
	Attacks by subcategory	Pie chart showing the top 10 subcategories of attack reports in terms of volume (for the last 15 days)
	Malicious Websites by subcategory	Pie chart showing the top 10 subcategories of Malicious URI reports in terms of volume (for the last 15 days)
	Botnets by subcategory	Pie chart showing the top 10 subcategories of botnet reports in terms of volume (for the last 15 days)
	C&C servers by subcategory	Pie chart showing the top 10 subcategories of C&C server reports in terms of volume (for the last 15 days)
	Bots by subcategory	Pie chart showing the top 10 subcategories of bot reports in terms of volume (for the last 15 days)
	Top 10 botnets	Bar chart showing the top 10 most reported botnets (for the last 15 days)
	Top 10 Malicious URI	Bar chart showing the top 10 most reported Malicious URIs (for the last 15 days)
	Top 10 Spam Campaigns	Bar chart showing the top 10 most reported Spam Campaigns (for the last 15 days)
	Top 10 C&C servers	Bar chart showing the top 10 most reported C&C servers (for the last 15 days)
	Top 10 Vulnerabilities	Bar chart showing the top 10 most reported Vulnerabilities (for the last 15 days)
	Top 10 Fast-flux domains	Bar chart showing the top 10 most reported Fast-Flux domains (for the last 15 days)
	Attacks by Source ASN	Pie chart showing the top 10 most reported ASNs associated to attacks (for the last 15 days)
	Malicious URI by ASN	Pie chart showing the top 10 most reported ASNs associated to Malicious URIs (for the last 15 days)
	Bots by ASN	Pie chart showing the top 10 most reported ASNs associated to Bots (for the last 15 days)
	C&C servers by ASN	Pie chart showing the top 10 most reported ASNs associated to C&C servers (for the last 15 days)
	Malware exploits IDs	Tag cloud chart showing the most reported malware exploit IDs
	Vulnerabilities IDs	Tag cloud chart showing the most reported Vulnerability IDs
Executive	Cybersecurity events threat level	Gauge chart showing the overall threat level, taking into account that each event (report) has associated a threat level based on the type of report category and confidence level
	Correlation alarms Risk level	Gauge chart showing the Correlation Risk level, taking into account that each alarm triggered by the SLSIEM correlator has associated a risk level based on the type of alarm category, confidence level and other parameters
	Top 10 malicious URIs used in Attacks	Bar chart showing the top 10 most reported URIs used in attacks (for the last 15 days)
	Top 10 malicious URIs	Bar chart showing the top 10 most reported malicious URIs (for the last 15 days)
	Top 10 Vulnerabilities	Bar chart showing the top 10 most reported vulnerabilities (for the last 15 days)
	Top 10 Vulnerable URIs	Bar chart showing the top 10 most reported Vulnerable URIs (for the last 15 days)
	Top 10 Attack sources	Bar chart showing the top 10 most reported IPs used as source of attacks (for the last 15 days)
	Attacks by ASN	Pie chart showing the top 10 most reported ASNs associated to attacks (for the last 15 days)

	Top 10 C&C servers	Bar chart showing the top 10 most reported C&C servers (for the last 15 days)
	Top 10 Malware exploits	Bar chart showing the top 10 most reported Malware exploit IDs (for the last 15 days)
Operational	Last cybersecurity events	Temporal Linear chart, showing the trend of volume of reports received from the CCH within the current day
	Cybersecurity events trend: last week	Temporal Linear chart, showing the trend of volume of reports received from the CCH for the las 7 days
	Cybersecurity events by data source	Radar chart showing the report categories with the highest volume (for the last 15 days)
	Top 5 cybersecurity events	Bar chart showing the top 5 most reported event categories and subcategories (for the last 15 days)
	Average confidence level by report category	Bar chart showing the average confidence level of all reports received form the CCH (for the last 15 days)
	Correlation: last incidents	Temporal Linear chart, showing the trend of volume of alarms triggered by the correlator within the current day
	Correlation: incidents trend last week	Temporal Linear chart, showing the trend of volume of alarms triggered by the correlator for the las 7 days
	Correlation: top 5 incidents	Bar chart showing the top 5 most triggered alarm types (for the last 15 days)
	Top 10 promiscuous hosts	Bar chart showing the top 10 host IPs used as a destination of multiple incidents (report categories) (for the last 15 days)
	Top 10 hosts with multiple events	Bar chart showing the top 10 host IPs used as source of multiple incidents (report categories) (for the last 15 days)
	Destination TCP ports	Tag cloud chart showing the most used TCP ports in reports
	Destination UDP ports	Tag cloud chart showing the most used UDP ports in reports (for the last 15 days)
Technologies	Top 10 tools detecting Malware	Bar chart showing the top 10 tools in terms of volume of malware reports submitted with confidence level >=0.5
	Top 10 tools detecting Malicious URIs	Bar chart showing the top 10 tools in terms of volume of Malicious URI reports submitted with confidence level >=0.5
	Top 10 tools detecting C&C servers	Bar chart showing the top 10 tools in terms of volume of C&C server reports submitted with confidence level >=0.5
	Top 10 tools detecting Fast-Flux domains	Bar chart showing the top 10 tools in terms of volume of Fast-Flux domain reports submitted with confidence level >=0.5
	Top 10 tools detecting Spam Campaigns	Bar chart showing the top 10 tools in terms of volume of Spam Campaigns reports submitted with confidence level >=0.5
	Top 10 tools detecting Attacks	Bar chart showing the top 10 tools in terms of volume of Attacks reports submitted with confidence level >=0.5
	Top 10 tools detecting Vulnerable URIs	Bar chart showing the top 10 tools in terms of volume of Vulnerable URIs reports submitted with confidence level >=0.5
	Top 10 tools detecting Botnets	Bar chart showing the top 10 tools in terms of volume of Botnet reports submitted with confidence level >=0.5
	Top 10 tools detecting Bots	Bar chart showing the top 10 tools in terms of volume of Bot reports submitted with confidence level >=0.5
	Top 10 tools by number of confirmed reports	Bar chart showing the top 10 tools in terms of volume of reports submitted with confidence level = 1.0
	Top 10 tools by number of High-Level reports	Bar chart showing the top 10 tools in terms of volume of reports submitted with confidence level > 0.7 and < 1.0
	Top 10 tools by number of Medium-Level reports	Bar chart showing the top 10 tools in terms of volume of reports submitted with confidence level >=0.5 and <=0.7
ACDC Experiments	DDOS: Reports by Tool	Bar chart comparing tools in terms of the volume of reports associated to the DDOS experiment

	DDOS: Average Confidence Level by Report Category	Bar chart comparing categories in terms of the average confidence level of reports associated to the DDOS experiment
	DDOS: Average Confidence Level of Reports by Tool	Bar chart comparing tools in terms of the average confidence level of reports associated to the DDOS experiment
	WEBSITES: Reports by Tool	Bar chart comparing tools in terms of the volume of reports associated to the WEBSITES experiment
	WEBSITES: Average Confidence Level by Report Category	Bar chart comparing categories in terms of the average confidence level of reports associated to the WEBSITES experiment
	WEBSITES: Average Confidence Level of Reports by Tool	Bar chart comparing tools in terms of the average confidence level of reports associated to the WEBSITES experiment
	FAST-FLUX: Reports by Tool	Bar chart comparing tools in terms of the volume of reports associated to the FAST-FLUX experiment
	FAST-FLUX: Average Confidence Level by Report Category	Bar chart comparing categories in terms of the average confidence level of reports associated to the FAST-FLUX experiment
	FAST-FLUX: Average Confidence Level of Reports by Tool	Bar chart comparing tools in terms of the average confidence level of reports associated to the FAST-FLUX experiment
	MOBILE: Reports by Tool	Bar chart comparing tools in terms of the volume of reports associated to the MOBILE experiment
	MOBILE: Average Confidence Level by Report Category	Bar chart comparing categories in terms of the average confidence level of reports associated to the MOBILE experiment
	MOBILE: Average Confidence Level of Reports by Tool	Bar chart comparing tools in terms of the average confidence level of reports associated to the MOBILE experiment
	SPAM: Reports by Tool	Bar chart comparing tools in terms of the volume of reports associated to the SPAM experiment
	SPAM: Average Confidence Level by Report Category	Bar chart comparing categories in terms of the average confidence level of reports associated to the SPAM experiment
	SPAM: Average Confidence Level of Reports by Tool	Bar chart comparing tools in terms of the average confidence level of reports associated to the SPAM experiment
Situational Awareness	Geographical Distribution of Cyber Security Events: Scanning Hosts, Malicious Hosts, All	World map where the IPs associated to cyber security events (reports received from the CCH) are geo-located.
	Geographical Distribution of C&C servers: by subcategory	World map where the IPs associated to C&C server reports are geo-located.
	Geographical Distribution of Attack Servers: by subcategory	World map where the IPs reported as source of attacks are geo-located.
	Geographical Distribution of Bots: by subcategory	World map where the IPs associated to bot reports are geo-located.

Table 3 Default configuration of the SLSIEM dashboard

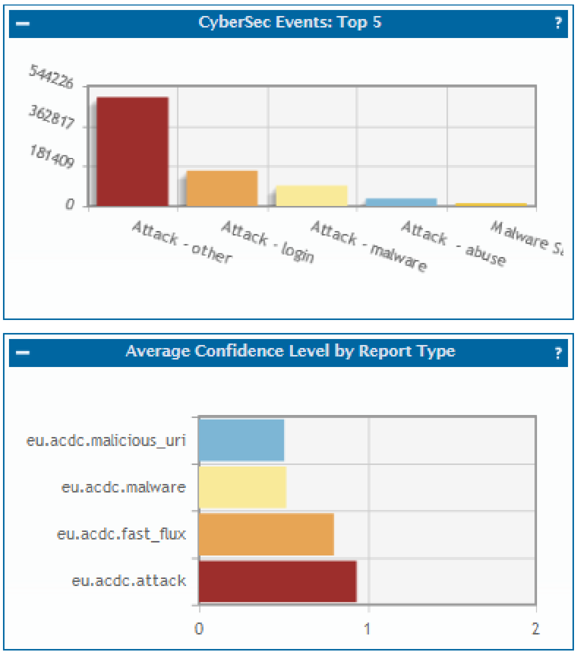


Figure 13 Sample charts form the Operational view

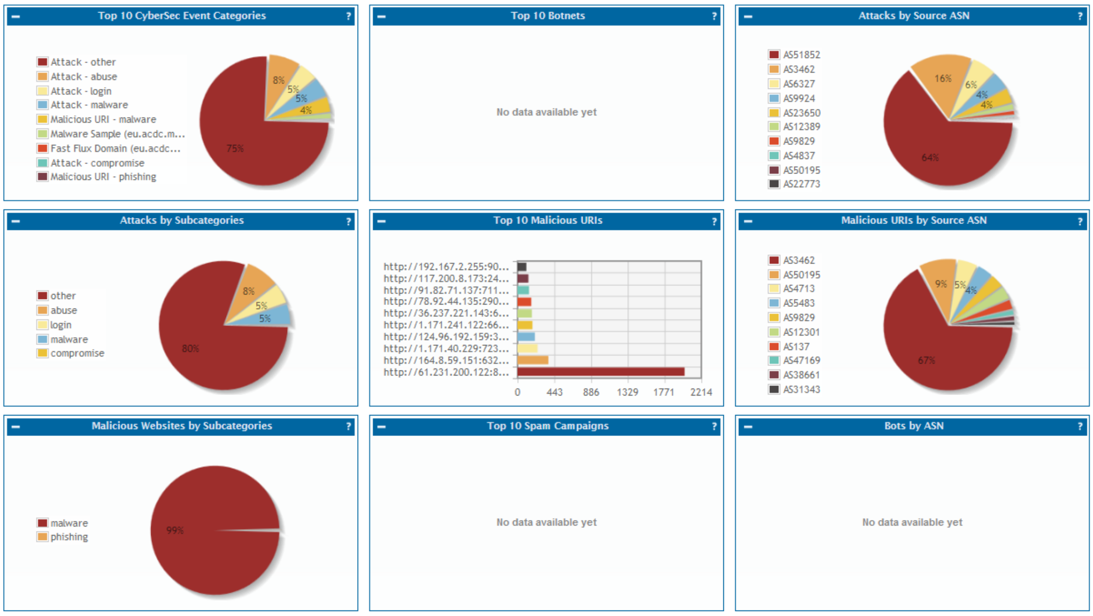
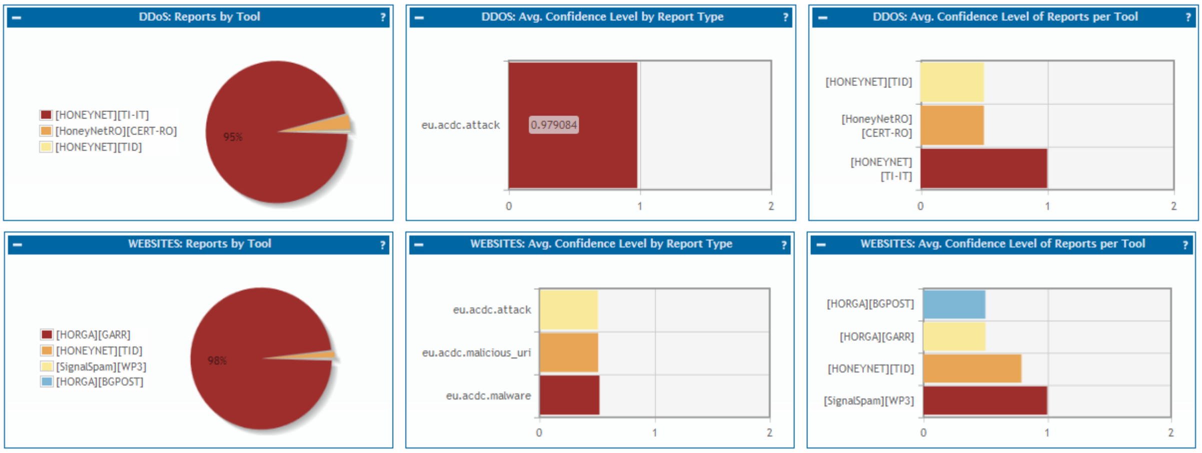


Figure 14 Sample charts from the Public View



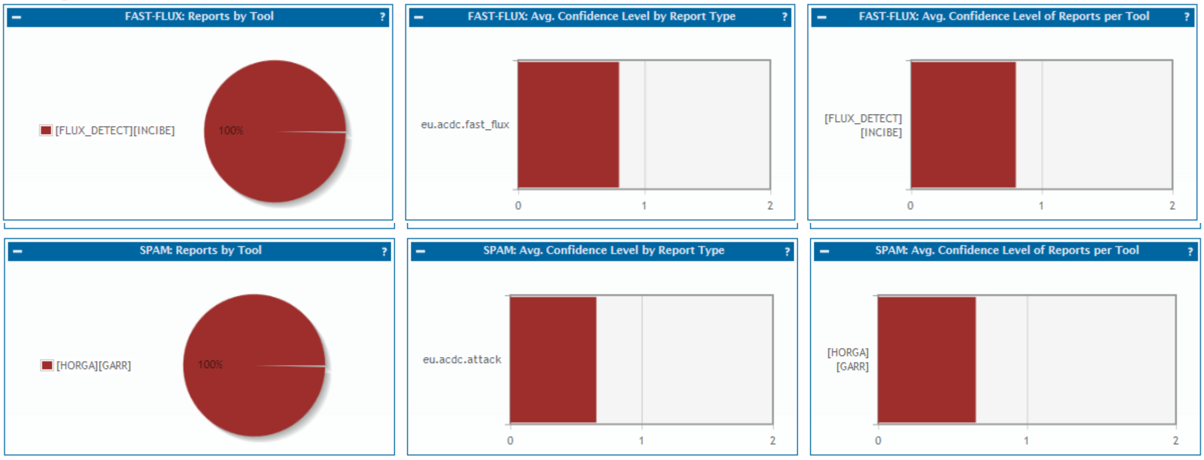
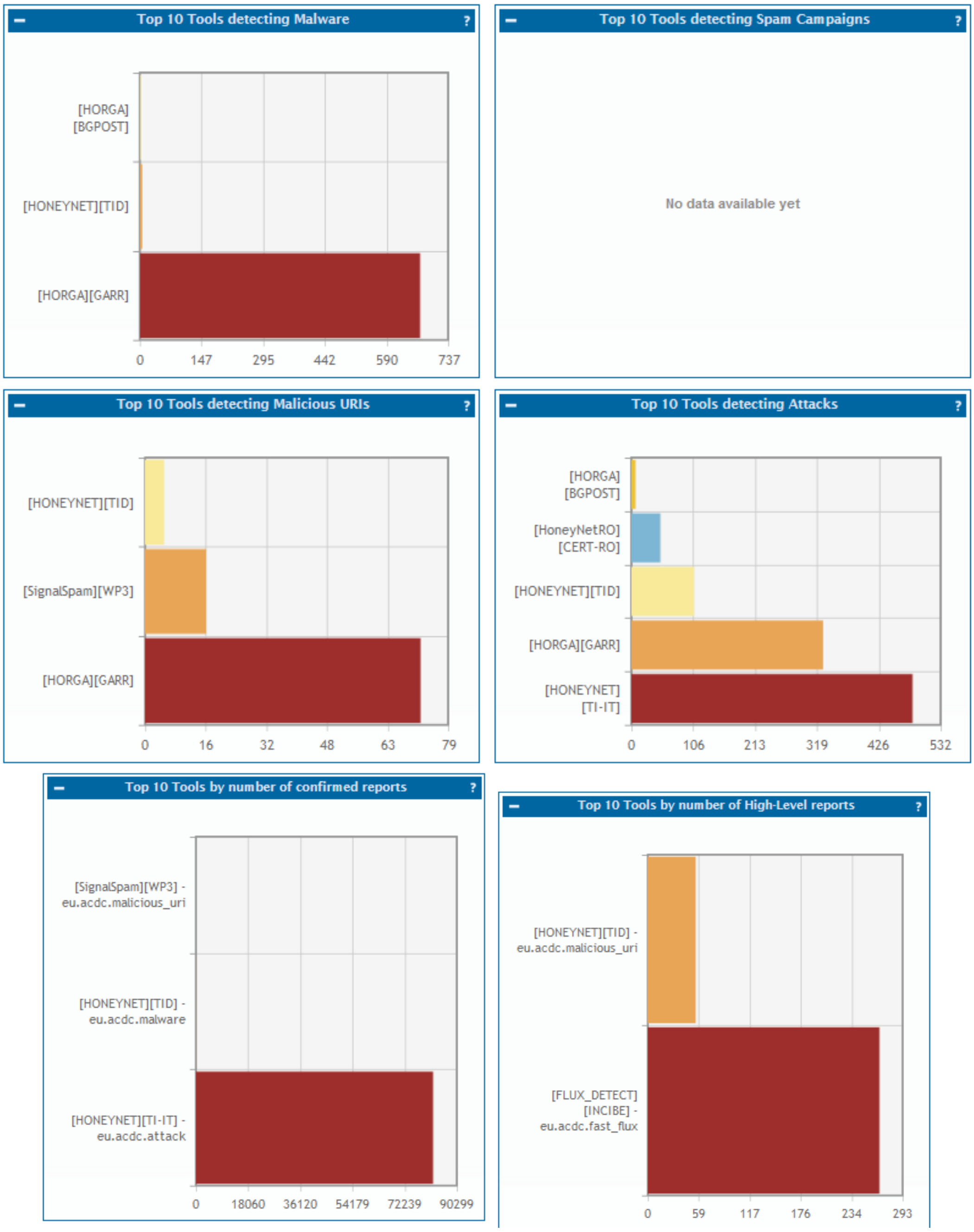


Figure 15 Sample charts from the ACDC Experiments view



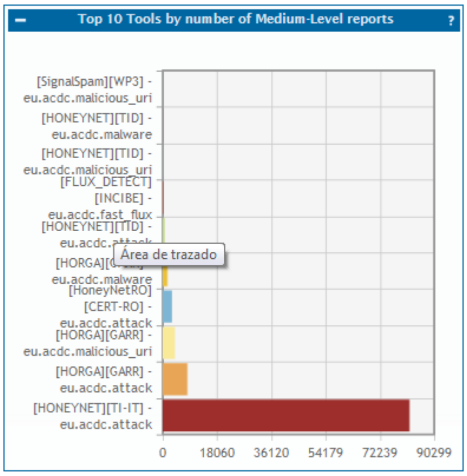
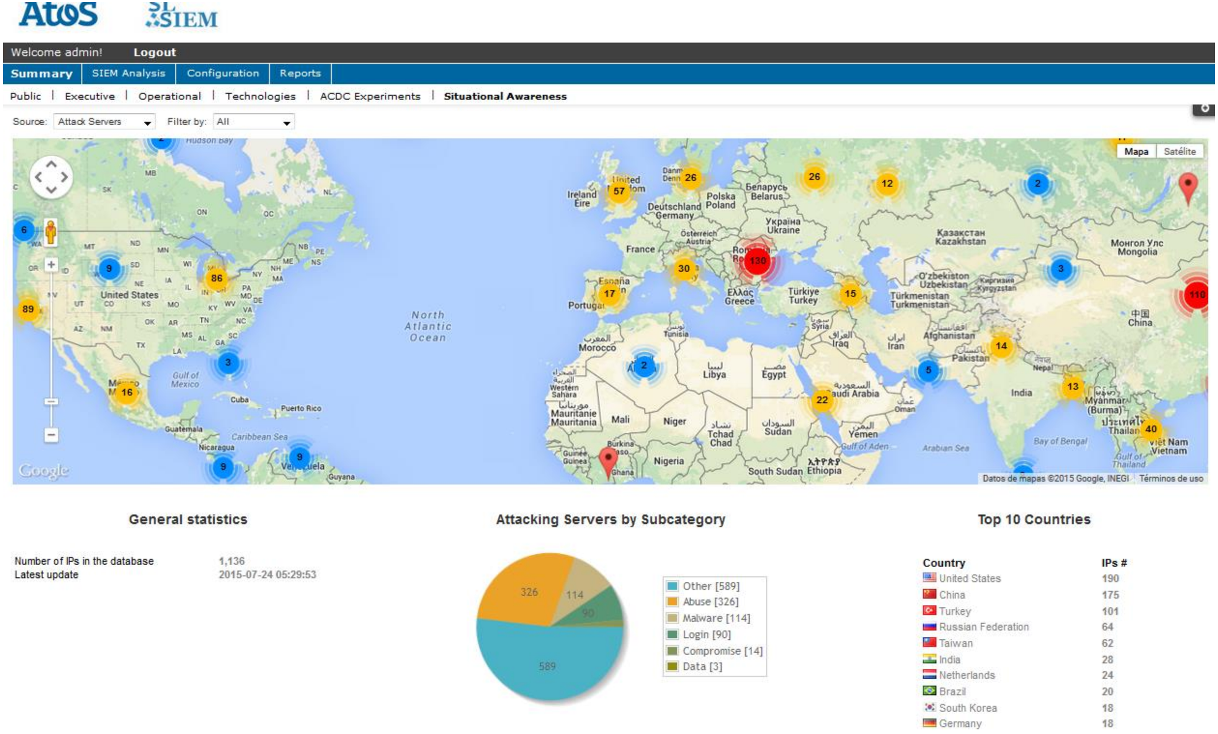


Figure 16 Sample charts from the Technologies View



General statistics

Number of IPs in the database	1,136
Latest update	2015-07-24 05:29:53

Top 10 Countries

Country	IPs #
United States	190
China	175
Turkey	101
Russian Federation	64
Taiwan	62
India	28
Netherlands	24
Brazil	20
South Korea	18
Germany	18

Figure 17 Sample from the Situational Awareness View

7. References

[i] ACDC consortium (2014). D2.3.: Technology Development Framework outlining basic models for integration and delivery principles. Available online at http://www.acdc-project.eu/wp-content/uploads/2014/11/ACDC_D2.3_Technology_Development_Framework.pdf

[i] See US GAO (2007). Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats. United States Government Accountability Office. Available online at http://www.gao.gov/new.items/d07705.pdf

[ii] NIS PLATFORM WORKING GROUP 3 (WG3) (2014). State of the art of Secure ICT Landscape

[iii] CAPITAL Project consoritum. (2014) Initial set of research activities listed to meet gaps. Available online at: http://www.capital-agenda.eu/files/Deliverables/CAPITAL_D3%201_v1%205_30_10_2014.pdf

[iv] ERCIM (2014) Whitepaper on cyber-security and privacy research. Available online at: http://www.ercim.eu/news/386-ercim-white-paper-on-cyber-security-and-privacy-research

[v] ACDC consortium (2014). D3.2.: Design report of each experiment.

[vi] http://www.benchmarkindex.com/improving-business-performance.htm

[vii] See US GAO (2007). Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats. United States Government Accountability Office. Available online at http://www.gao.gov/new.items/d07705.pdf

[viii] ACDC consortium (2014). D6.1.1 ACDC User Profiles and Categorization. Available online at http://www.acdc-project.eu/wp-content/uploads/2014/11/ACDC_D6.1.1_ACDC_User_profiles_and_categorization.pdf

[ix] COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 8/12/2008. Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[x] ACDC consortium (2014). D1.8 Legal Requirements. Version 1. Available online at http://www.acdc-project.eu/wp-content/uploads/2014/11/ACDC_D1.8.1_Legal_Requirements.pdf

[xi] European Commission. Article 29 Data Protection Working Party. Available online at http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

[xii] Google (2015). IP Anonymization in Google Analytics. Available online at https://support.google.com/analytics/answer/2763052?hl=en

[xiii] European Comission. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[xiv] http://en.wikipedia.org/wiki/Lurker

Statement of originality:

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.