**DiSIEM Meeting 18-20 October 2017**

* Presentation of all the partners
* 10 deliverables submitted
* Everyone should have a well-defined idea of their components
* Review in 5 months (no dates so far)
* Agenda of the 3-day meeting

**WP8: Exploitation - Alberto (Atos)**

* DiSIEM Intermediate Business Plan/ Exploitation report (M18)
* DiSIEM Final Business Plan/ Exploitation report (M36)
* Exploitation Roadmap

**1. Identification of exploitable items** (completed): Exploitable items have been already identified. A fiche has been sent to each partner to fill out with the main information.

**2. Market analysis:** (ongoing) it will be updated for the next months of the project (SWOT, can be extended to PEST if partners are familiar with it)

**3. Business model (ongoing):** e.g., CANVAS or any other well-known model

**4.** **Exploitation strategy (ongoing):** Individual and/or joint exploitation

* Two deliverables in WP8 due to the end of the project.
* Commercial vs Non-commercial exploitation:
  + DiSIEM as a whole or DiSIEM components, services around DiSIEM, brand
  + Knowledge, training, standardization, proof of concept, re-use of other results
* There are 9 components, 4 services and 3 pilots. There was a question about the threat predictor (EDP) and the threat analyser (FFCUL) on what are the differences between them, as they seem to be similar. Alysson said that the threat analyser is more research oriented than the threat predictor, both using different methodologies.
* SIEM Market = US$ 4.54 billions
* Do we go for an **exploitation of each component or for several joint components?** An initial version of the business model will be done for each pilot.
* We should **emphasize the impact of the project over SMEs** as this is something checked by the EU Commission.
* Does it make sense to do the canvas for non-commercial exploitation? No!
* What about for open-source components?... Not sure, it is possible to propose freemium where basic features of a component are provided for free, but the user has the possibility to upgrade for a paid premium version with more features and functionalities.
* **Alberto will send the ToC to some partners to get help with the deliverable**. First contribution (CANVAS, joint-CANVAS) is expected for December (before holidays). Second contribution (if needed) will be expected by mid-January. Final version of the document will be ready by the beginning of February.
* Alberto suggests that we should focus in what we are going to provide in DiSIEM that is not already in the market.
* **Alberto will share templates of CANVAS, IPR, PEST, SWOT, etc. There is no template for non-commercial exploitation**
* Modularity is the best strategy to develop components for DiSIEM.

**Dissemination - Alyson, Pedro (FFCUL)**

* Visual identity – Leaflet (300 already printed)
* Website – more news, video (Alysson is planning to make a video about DiSIEM)
* Social media – twitter, linkedIn (a twitter account will be created for DiSIEM as well as a linkedIn page)
* Publications 🡪 **We need more papers!** FFCUL is working on 5 technical papers, others?
* Talks on conferences
* Workshops in a well-known conference (e.g., DNS) in 2018 it will be in Luxembourg in June.
* FFCUL proposes to organize 2 machine learning competition. Not many venues that allow this kind of events.
  + 1st competition to be submitted in IEEE WCCI’2018 🡪 collocated IJICNN, FUZZ-IEEE, IEEE-CEC (July 2018, Brazil), results in D8.5 (M36)
  + 2nd one not yet planned.
  + Supervised learning problem, labelled training data set with tweets, unlabelled testing data set with tweets. Unsupervised learning problem, unlabelled data set… Anonymization to be considered, also issues if the user deletes the tweet, Can we keep it in our local DB?

**WP5 Visual Analysis Platform – Phong (CITY) and Fraunhofer**

* User Behaviour Analytics – Behaviour-based Fraud & Threat Detection
* Current results: users with repetitive behaviour, users with diverse behaviour
* New features have been added to the visualization platform: selected sessions are displayed in the timeline, relative and absolute timeline for the sessions is displayed, comparison with past activities.
* D5.1 has been released. It presents architecture and initial designs of the visualization platform.
* Data set currently used is not from the pilots
* **Need more clarification from the network analysis with Atos**
* Fraunhofer presented its model: Visualisation of individual user behaviours based on their actions 🡪 it creates a pattern on the user behaviour. Actions are encoded from inside out and then, they are aggregated. There is a notion on time in the sequence but not in the visualised model.
* Advanced Modelling of User Behaviour 🡪 Modelling with LSTMs. They can predict the right action 60-70% of the cases. They claim that they can easily predict the bad actions. Preliminary tests have been performed with Amadeus datasets (85% of coincidences).

**WP3: Security Metrics**

* 2 ongoing deliverables
* T3.1 survey on metrics has been shared among partners (July). It is very important that industrial partners fill the questionnaire. Security metrics are available in the Gitlab.
* Splunk is a good way to compute risks, and it considers different types of events, it computes risks per assets, but it does not consider dependencies as Qradar does.
* FFCUL approach is to compute risks by assets in each layer bottom-up. They have decided to use incidents and nor events with variables in vulnerabilities, dependencies and incidents. Events have too many false positives. Final score is normalised to 0-100
* **FFCUL has a DB with incidents and an application showing the vulnerabilities, dependencies, risks, and assessment values**. Parameters can be customised.
* **It is possible that Atos include information about the threat score in D3.1 about security metrics.**
* Diversity metrics for DiSIEM (City) 🡪 Decide by asking: what are they for?
* Assessment: Efficacy of diverse defence layers (IDS, Antivirus, Firewalls…); trade-off between false positive and false negative rates. CITY compares models using a technique that takes the distribution of one model and makes a prediction.

**WP4: OSINT data fusion and analysis (FFCUL)**

* Outputs: D4.1 ongoing, 2 MsC Thesis, 3 case studies set-up, 1 paper submitted (rejected), 2 papers to submit to DSN’2018
* Is tweeter useful? 🡪 out of 6,623 vulnerabilities, we found tweets referring 73 (1.1%) before publication
* **Current approach of FFCUL: Convolutional Neural Network (CNN). Results show the approach is promising.**
* FFCUL and EDP assessment component to reduce the rate of false positives. IP collector from different blacklists, **they are using Arcsight but it can be adapted to any other SIEM**. Precision of the solution is 1.2% smaller than the paid cybersecurity tools, 3% bigger than the public and private blacklists. It considers historical incidents.
* Presentation of our tool: Context-aware Intelligence Integrator. Alyson said that it will be probably **difficult to provide all the input data** we expect to have from them, but probably **some of the data is possible to obtain**. Olivier asked how they could help Atos in the assessment process, and I said that it would be important that they give us a feedback on the heuristics and scores used for the training process.
* FFCUL is concentrated in classifying the information coming from Tweeter but they are not working on filtering this information to feed our component. **They do not use JSON format**, therefore it will be necessary to go further for them in order to provide the input data in the format we require. This is not an easy task, and Alysson is not confident that it could be provided.
* In addition, CITY asked me what is the meaning of our score, **how it can help users to make the right decision?**. What is it good or bad for us, and how we define the good and bad scores? How reliable the score will be? **What does it measure: importance, severity, any other aspect? 🡪 I guess it measures relevance of the input data**

**WP6: Infrastructure Enhancements**

**T6.1: Enhanced monitoring applications (Amadeus)**

* Development of several components, identify deviations, enhancement in storage, monitoring and detection.
* Partial results from 6.1 to 6.3 (due date Sept 2018)
* Dual engine: behavioural (training and prediction) and rule (expert knowledge, OWASP rules)
* D6.2 (prototype) 🡪 proof-of-concept M24 (sept 2018)
  + OWASP CRS integration
  + Test unsupervised modules
* Components can be shared as a service, or as a software. This needs to be defined
* **Do we need to validate the components with other partners from the consortium? e.g., Atos components need to be validated in Amadeus infrastructure and vice versa?**
* Amadeus wishes to share it in Git but this is something to be checked and probably not feasible.

**T6.2: Diversity related components (CITY)**

* Alert filter, traffic input labelling
* Assessment is done over the labelled traffic
* Showing in the dashboard if things are getting better or not, results, etc.
* Diverse IDS Alerts (Snort, bro, Suricata) 🡪common fields found
* Comparison of Suricata City rules against other IDSs and rulesets.

**T6.3: Cloud storage (FFCUL)**

* In general SIEMs are not able to retain the collected events for long period of times, some zero-day vulnerabilities take up to 320 days to be discovered. **For forensics it could be useful to use the cloud to store old events.**
* SLICER – Safe Long-term Cloud Event aRchival is the component developed by FFCUL
* SIEMs based on relational databases (ArcSight, OSSIM) use a logger components to keep events since relational DB do not scale. Events are collected and kept for 3 months and 6 months in the logger. SIEMs based on NoSQL approach (SL-SIEM, SPlunk, Elastic Stack) keep events in the core engine.
* **Events are compacted in blocks every hour and indexed. For each block of events a key is generated to encrypt it and store it in different clouds.** In order to decrypt the block, it is necessary to recover it from at least two clouds.
* Avoid downloading data 🡪 Indexing could be a good solution. Queries are constrained (no SQL queries are possible).
* **Options being evaluated:** (1) No using indexing at all; (2) using bloom filters (storing sets of IPs, ports, users, etc that are going to be stored and indexed. Here we do not store all the information from the events but only those fields we need); (3) text-based indexes (Apache Lucene). Next steps focuses in evaluating the 2 last options, there is already a prototype that simulates each solution and they are evaluating their performance and false positives.
* The idea here is, instead of downloading the whole block with all data of events, we will download the index containing the data we require.
* **The approach seems to be useful for forensics analysis but not for real time analysis**

**1st AB Meeting (Part B)**

Part A: Ethical and Business (Meeting in London)

* Jane Rachel
* Sergio Sá

Part B: Technical (Meeting in Nice)

* Marc Dacier
* Piotr Kijewski
* Innovation Action (TRL 7 or higher)
* Proposed enhancements: Diversity monitoring, Visualization, Cloud storage, and OSINT integration.

**Questions and answers**

* Does the project aim at working on an enterprise environment or on a university environment, or any kind of environment? 🡪Environments are not the problem, the SIEMs are already deployed, we want to improve detection, visualisation and other features of current SIEMs
* The proposed enhancements are for the SIEM or the SOC? 🡪 probably the SOC
* How to take into account the diversity enhancements for different SIEMs 🡪 In the dashoboard, a tab can be created as an add-on for the SIEM.
* **Is XL-SIEM open-source? Do you plan to sell components individually or jointly? 🡪 It is a non-commercial tool built on top of an open source SIEM, but it is not open-source. Atos can propose some licenses to use the tool. Not yet done**
* Do you consider the environment while assigning scores in the assessment done for WP3? For instance, if a vulnerability is assessed high on a machine connected to the network, it should not be high if that machine is isolated. 🡪 EDP redefines the scoring depending upon the environment.
* Do you use probability in the scores? 🡪 No
* It is easier to assess the past activities than current or future ones. **In WP3, are you using metrics to measure the ROI?** 🡪 Yes, it is taken into account. Here, I am not sure, how can they measure return on investment with qualitative values? The metrics are not considering financial losses, therefore, ROI or any other similar metric won’t be possible to evaluate.
* **How can we be good in predictions using events from the past?** It is not possible to predict an attack is going to happen if we have never seen it. 🡪 True, we cannot predict an attack only from past events, but we can be good at identifying the useful information that can help in the analysis. Based on the past, we can know who is knocking the door
* **How do you differentiate what is a general conversation from what it is relevant for a threat in Tweeter for instance?** 🡪 To be confirmed, the work is done by a student, neither Ana, nor Alysson could answer the question.
* **Trustworthiness is very difficult to evaluate.** It is very blurry; it is not a very precise science. There is a danger that in collecting IP addresses we can blacklist everything.
* **What is the novelty of the threat score module?** 🡪 Integrating information from OSINT and the infrastructure to evaluate their pertinence.
* **Do we know other organizations outside SIEM developers that are using STIX in their components?** An example can be MIST; it is open source and can be useful to see how we can integrate our work into what they do.
* Why developing new visualisation tools if we can use Kibana or any other available from the market? 🡪 Most of them highlight events as suspicious when they really are not. In DiSIEM we want to reduce false positives.
* **Talking about visualisation, why should I believe it will work**? How can you ensure that if there is something to be seen, I will see it? It is not just the dashboard; it is also detecting bad guys. 🡪 Not easy to ensure that, since they are predictions, and as such, we are not 100% sure of the final results.
* What the AB is missing is the argument when visualisation is better instead of analytically formulating it?
* The Skeptic tool presented by Amadeus is very much promising.
* For the approach presented by City, how do they deal with data they have missed? 🡪 Investigating past events in historical data to see what we have missed in the analysis that has let the event happen…
* **The Cloud approach is fine if we want to avoid dependability issues, but for the price arguments, it does not make sense.** It is less expensive for a company to have its own data center to store the data, if we make the calculation of how much a company must pay for 1TB of storage in a year it will be much more expensive than having that stored internally.

**Conclusions:**

* 10 deliverables already released; 16 other deliverables ongoing, most of them prototypes.
* Next steps: finish first version of the project, integrate them with SIEMs, dissemination and communication activities.

**Recommendations from AB**

* **Publishing** what we are doing in top conferences. It is always easier for reviewers to see with better eyes the work that has been peer-reviewed and already published.
* Much of the research work is very interesting; it would have been helpful to present **concrete examples** from the real world where these solutions can be applied.
* Within one year, the consortium has done a lot of things for DiSIEM. The presentation was nice, it shows nicely the individual efforts but **it is important to make it clear that** **it’s been integrated**. For the review, it is important to make an effort to show the modules are being developed to be integrated together and not just as standalone modules.
* For the review it should be important to show demonstration of the tools being developed within the project.
* A report from the AB comments and recommendations will be sent soon.

**Management – Next meetings, deliverables**

* D9.2 has been done by FFCUL with 52 identified risks and a description and assessment of them. Medium risks are mostly related to integrating components in ArcSight since this SIEM is very closed and difficult to integrate visualization improvements and other aspects. At this stage of the project, Alysson does **not see any dangerous risk, most of them are Low, and some others medium but nothing to worry about**.
* There will be **2 reviews for the project**, one in February 2018 (**M18**) and the other at the end of the project (**M36**). Some of the risks described in D9.2 should be revised and update it. We will have some telcos to do that.
* **A technical and financial report need to be done by M18**. We will receive a document to account the financial report in which every partner needs to justify every euro already spent.
* **The 1st review will be in the middle of April, probably the week of 16-18 April** (we have 60 days after the first half of the project to do the review). The next DiSIEM EB meeting will be done before this date. Not all components will be able to be presented. Normally the review is in Brussels, unless we have a demo to show which justifies why we do not want to do the review in Brussels.
* We need to decide which components we will show in the review, which demos will be ready to be shown. **One or two people per partner must assist**.
* **Next meeting to be done in March in Germany - Fraunhofer (tentative dates: 21-23/03 or 14-16/03)**🡪 WP8 is very important for this meeting.
* Several **deliverables** will be delivered by the **end of February**. 3 weeks before the deadline deliverables should be sent for internal review, partners will have one week to send their feedback, then corrections are taken into account, and the document is delivered 3 days before the deadline.
  + **Atos is the reviewer of D3.1** (security metrics). One person that is not participating in the document should review it. Probably Rodrigo???
  + D3.1 (Metrics)🡪 Atos, FHG (deadline 20-11) 🡪 To be delivered end of November
  + D3.2 (Metrics) 🡪EDP, FHG (deadline 7/02/18) 🡪 To be delivered end of February
  + D4.2 (OSINT implementation)🡪Amadeus, City (deadline 7/02/18) 🡪 To be delivered end of February
  + D8.3 (Exploitation)🡪 DigitalMR, FFCUL (deadline 7/02/18) 🡪 To be delivered end of February
* Last part of the meeting concentrated in providing more details of the Marie Curie Funding.

**Next Steps to do:**

* Zayani is interesting in having more information about the Network-based Anomaly detector, the features used in the analysis, the dataset and main results obtained. In addition, he asked if the sensor has been developed using Java, and if we are planning to have a standalone component or include it in the SIEM. I promised him to send him more information about the sensor as soon as possible. We can probably get some data from the results obtained in ZoneSec.
* Phong (City) needs to know what kind of data we are going to provide for visualization. But more importantly, why do we need to send that data to the visualization module. We need to justify the reason why it is needed and then, it will be needed to provide datasets for different sensors, so that they do their treatment. Do we have other sensors besides Snort? Which ones?
* One important thing City asked, is if we are going to work in the development of the visualisation module using our data, since we have 20 PMs in WP5 and it will be difficult to justify that enormous amount of work by only providing datasets. I guess, we will focus most of our effort in T5.4 (SIEM Integration), there is no deliverable for this task, and there is no information in the GA about the PMs per task per partner. We only see PMs per WP per partner.
* Ana gave some remarks to the paper about SIEMs, she will send a paragraph to be added in Sec 2.
* Ilir also sent feedback of the journal paper. Everything seems to be fine, after integrating the remarks, the paper will be sent for review.
* Ilir wants to propose a telco to discuss about T6.2. He will contact us in the following days. Their objective is to obtain traffic from different IDSs from Atos. He asked if the datasets we have are the logs produced by Snort, or by the XL-SIEM.