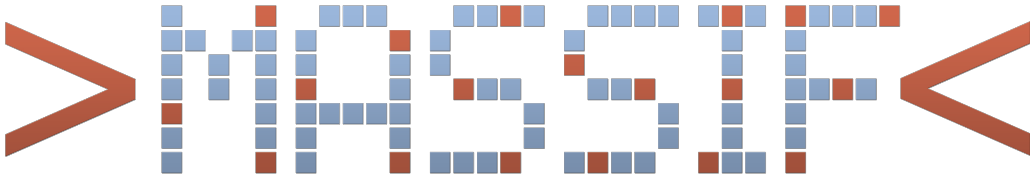

MAnagement of Security information and events in Service InFrastructures

MASSIF
FP7-257475

D1.2.1 - Research and Roadmapping Report Year 1

Activity	A1	Workpackage	WP1.2
Due Date	Month 12	Submission Date	2011-10-15
Main Author(s)	Roland Rieke (Fraunhofer), Elsa Prieto Perez (ATOS) Herve Debar (IT), Saïd Gharout(FT)		
Contributor(s)	Valerio Formicola (CINI), Andrew Hutchison (T-systems SA)		
Version	v1.0	Status	Final
Dissemination Level	PU	Nature	R
Keywords	R&D Management, Coordination of Activities, Technology Roadmapping		
Reviewers	Elsa Prieto Perez, Pedro Soria-Rodríguez (ATOS) Claudio Soriente (UPM)		

Part of the Seventh
Framework Programme
Funded by the EC - DG INFSO

Version history

Rev	Date	Author	Comments
V0.8	2011-09-29	Roland Rieke (SIT)	review version
V0.9	2011-10-03	Roland Rieke (SIT)	comments of reviewers integrated
V1.0	2011-10-15	Elsa Prieto (Atos)	final review and official delivery

Glossary of Acronyms

Abbr	Abbreviation
AB	Advisory Board
BoD	Board of Directors
BSCW	Be Smart - Cooperate Worldwide
CSS	Cascading style sheets
DoW	Description of Work
EB	Executive Board
EC	European Commission
EU	European Union
FIA	Future Internet Assembly
FP7	Seventh Framework Programme
KO	Kick-Off
LoI	Letter of Interest
MASSIF	MAnagement of Security information and events in Service InFrastructures
MSS	Managed Security Service
MSSP	Managed Security Service Provider
PMC	Project Management Commitee
PU	Public Usage
R&D	Research & Development
RSS	Really Simple Syndication
SIEM	Security Information and Event Management

Executive Summary

The goal of technology roadmapping in MASSIF is to ensure that the outreach of the MASSIF results beyond the project as well the influence of outside trends on MASSIF are appropriately addressed. This includes an assessment of the MASSIF approach and directions in light of the technology environment and the investigation of its consequences. MASSIF will continue this roadmapping task throughout the duration of the project, in order to guide the research and development work of MASSIF.

As a means of choice, in the initial phase of MASSIF work groups mutually reviewed the technical concepts of the individual activities and developed a blueprint of the MASSIF architecture. Furthermore, based on the results of the scenario work package MASSIF developed important recommendations concerning security, event processing, trustworthiness and compiler technologies to be used as guidelines for further work in the project.

In terms of activity co-ordination the project has established a close interaction through regular meetings and workshops, complemented by regular voice- and video-conferences.

In terms of technology roadmapping, the MASSIF project has in its first year:

- Refined the goals, deliverables and architecture in terms of detailed contribution by each partner
- Communicated about, and positioned, the project in a wide variety of forums in Europe and beyond
- Researched, collated and confirmed details of the research challenges and emerging trends relating to Security Information and Event Management systems
- Constituted an advisory board to the project, composed of leading industry and domain experts who are well positioned to guide the project and ensure relevant and quality outcomes

Based on these diverse activities, and through steady and consistent co-ordination of all activities, the project is on-track in terms of timing and technical progress.

Preliminary findings and outcomes indicate that the MASSIF project can play a valuable role in achieving its goal of advancing Security and Event Management Capabilities and in strengthening the ability of organisations and enterprises to thwart the rapid growth and seriousness of information security threats and attacks.

Contents

List of Figures

List of Tables

1 Introduction

The MASSIF project aims to create a next generation Security Information and Event Management (SIEM) environment, and does this through the development of applied security techniques. To test the depth and breadth of these techniques several scenarios were selected, and these span both information and cyber-physical environments. In particular the following scenarios were identified: *a*) Mobile payment system, *b*) Olympic games infrastructure management, *c*) Managed security services provision, *d*) Dam wall monitoring and control environment.

The document is structured to focus on two overall aspects of the project:

a) Co-ordination of activities and

b) Technology roadmapping activities

Co-ordination of activities. In terms of activity co-ordination the process of conducting the project is reported on. This provides the reader with insight into the dynamics and modus operandi of the project consortium. In the first year of the project it has been essential to effect procedures for facilitating technical discussions and resolving technical conflicts, as well as for ensuring integration and interoperability of MASSIF results.

Technology roadmapping activities. In terms of technology roadmapping, this document considers:

The goals of MASSIF and progress to date. An architecture working group led by Hervé Debar from Institut Téécom, acting as technical director of the project, has been established and has contributed to the project progress in relevant areas. The *proposed architecture has been validated* by the project and will be refined further on an as-needed basis. This effort will continue in the project under the scopes of the testing and validation and integration work packages in order to enhance the architecture description as modules are developed.

Techology guidelines. Based on the requirements defined in the scenario deliverable [7], a set of *techology guidelines* for the design and development of next generation SIEM platforms has been identified.

The outreach and dissemination activities relating to MASSIF. This activity has aimed to ensure that the communication of results, and influence of outside trends, is appropriately addressed. This has also included *regular exchange with related projects*.

Details of the research challenges and *emerging trends* relating to SIEM systems. Within the project consortium there is ongoing assessment of the MASSIF approach, and direction, in light of the technology environment and its consequences.

Through studying the details of the MASSIF project progress, in its process and technical dimensions, it is evident that the consortium has quickly settled and started to work constructively to achieve the goals of MASSIF. The achievements of the first twelve months are aligned with intended project progress, and no significant risks to continued progress are envisaged.

In Section 2 a “Report on regular R&D management” is presented; Section 3 provides a “Report on Coordination of Activities” after which Section 4 gives a “Report on Technology Roadmapping”. In Section 5, a “Conclusion” is drawn and the progress is summarized and assessed.

2 Report on regular R&D Management

This section shows the activity performed on the project internal technical management during the first year. The main objectives of this task were:

- To seek for a common technological approach.
- To align the technical work with the objectives in the Description of Work (DoW) [6].
- To check regularly the progress of technical activities.
- To early identify difficulties or problems for the normal course of the technical work.
- To prevent isolated developments.
- To keep the consortium informed about the status of the technical work.

In principle this activity was within the scope of Project Management Committee (PMC) [5], as main technical consortium body. However it was considered that the participation should be extended by including not only the board of directors and the activity leaders, but also the work package leaders.

During the Kick-off meeting it was agreed to call teleconferences (called R&D teleconferences)monthly. The initial technical range of these teleconferences (related to activities 2,3,4 and 5) was also extended to bring some pertinent information from non-technical activities (those within WP1.1 - project management- , WP6.1 - dissemination- and WP6.2 -exploitation) in order to provide the participants a complete view of the project progression. The following list summarizes the dealt topics:

- Work packages progress.
- Progress of ongoing deliverables (M3, M6, M12) and quality issues.
- Need for public version of deliverables and confidentiality issues.
- MASSIF requirements.
- MASSIF architecture definition (see also Chapter 3.1)
- Integration of MASSIF components.
- Collaboration and joint activities with other groups, projects and initiatives (see also Chapter 4.2.1)

- Actions and procedures with regard to the advisory board (see also Chapter 4.4)
- Preparation of reporting activities, including internal midterm reporting and the first period reporting.
- Preparation of additional meetings.
- Preparation of the first project review.

The following table summarizes these teleconferences:

Date	Description
2010-12-14	First R&D telco Progress status of running WPs: WP1.2, WP2.1, WP3.1, WP3.2, WP3.3, WP4.3, WP5.1, WP5.3, WP6.1, WP6.2, and WP1.1. Need for a session on architecture. Need for a scenarios session. Progress of deliverables due in M3.
2011-01-11	Progress status of running WPs: WP2.1, WP3.1, WP3.2, WP3.3, WP4.3, WP5.1, WP5.3, WP6.1, WP6.2, and WP1.1 Preparation of the WP3.2 meeting in Madrid. Confidentiality of D3.2.1 and D3.2.2. Preparation of EB meeting in Darmstadt. Cooperation with DEMONS project.
2011-02-01	Progress status of running WPs: WP2.1, WP3.1, WP3.2, WP3.3, WP4.3, WP5.3, WP6.1, WP6.2, and WP1.1 Discussion on MASSIF architecture. Midterm activity and effort reporting (M6).
2011-03-01	Progress status of running WPs: WP2.1, WP3.1, WP3.2, WP3.3, WP4.3, WP5.1, WP5.3, WP6.1, WP6.2, and WP1.1 Progress of deliverables due in M6 Discussion on MASSIF requirements vs Scenario requirements. Discussion on MASSIF architecture.
2011-04-05	Progress status of running WPs: WP3.1, WP3.3, WP4.3, WP5.1, WP5.3, WP6.1, WP6.2, and WP1.1 WP2.1 post mortem and closing. Key issues arisen during the EB meeting in Darmstadt. EU-Canada Future Internet Workshop. Participation in EFFECTS+ clusters and contributions to FIA roadmapping. Cooperation with VIKING project.
2011-05-10	Progress status of running WPs: WP1.2, WP3.1, WP3.3, WP4.1, WP4.2, WP4.3, WP5.1, WP5.3, WP6.1, WP6.2.

Date	Description
2011-06-06	Progress status of running WPs: WP2.3, WP3.1, WP3.3, WP4.1, WP4.2, WP4.3, WP5.1, WP5.3, WP6.1, WP6.2, and WP1.1 Discussion on test and evaluation strategies. Preparation of the A4 KO meeting in Darmstadt Advisory Board feedback to architecture and requirements EFFECTS+ Workshop on Models
2011-07-12	Progress status of running WPs: WP2.3, WP3.1, WP3.3, WP4.1, WP4.2, WP4.3, WP5.1, WP5.3, WP5.4, WP6.1, WP6.2 Preparation for the first project review Discussion on integration Effort, activity reporting (M12) and first periodic report Preparation for the EB meeting in Naples.
2011-09-16	Misuse case selection for the first project review (cancelled due to poor-quality teleconference)

Table 2.1: Teleconferences

All teleconferences were written up and records were kept in the project internal repository (BSCW) following the indications of the Quality Plan (D1.1.1).

3 Report on Coordination of Activities

3.1 Architecture Working Group

3.1.1 Architecture rationale

During the MASSIF kick-off meeting in October 2010, several partners had architectural aspects for a MASSIF platform in mind and reflected them in the presentations of their contributions. The fact that the project does not have a deliverable related to the architecture of the MASSIF platform was discussed. Such an architecture is important for ensuring that partners share a common vision of the production of the project, know where and with whom they should be prepared to integrate and test, and what interfaces and information they are consuming, producing and offering. The project then decided to establish an architecture working group led by Hervé Debar from Institut Téécom, acting as technical director of the project. A first draft of this architecture, typically a rough sketch, was planned for and included in deliverable D3.2.2, also under the responsibility of IT. Since this deliverable included an analysis of common data formats, hence interfaces, it provided a suitable vehicle to include such a preliminary architecture.

During the project R&D teleconference meeting in Month 5 of the project, a first advancement of the architecture work was reported and partners provided feedback. It was decided to have an architecture session during the March 2011 EB meeting in Darmstadt, and to request all partners interested in the task to provide their vision of the architecture as inputs to the discussion. 6 inputs were received from partners, showing a difference of orientation between partners. This difference highlighted the fact that proposals were either considering data gathering and transport, or data analysis and decision support. These being the main functions of a SIEM environment, leads to the conclusion that this difference in opinions in fact truly and appropriately reflects the contributions and expertise of the partners, provided that these two layers are appropriately interfaced. This meeting was then used to raise consensus on the various issues that need to be solved in order to achieve proper integration, and in particular major event stream interfaces. The decision of the project was the definition of a more complete architecture, presented in the following section, and included in this deliverable as the best vehicle to disseminate the project vision.

3.1.2 MASSIF architecture

Figure 3.1 presents a high-level overview of the MASSIF architecture, inserted within a monitored environment (whose components and data streams are represented in *green* in the figure). The architecture is separated in two parts, a data acquisition and analysis layer detailed in this figure, and a central platform

detailed in Fig. 3.2 (represented in *grey* in the figure).

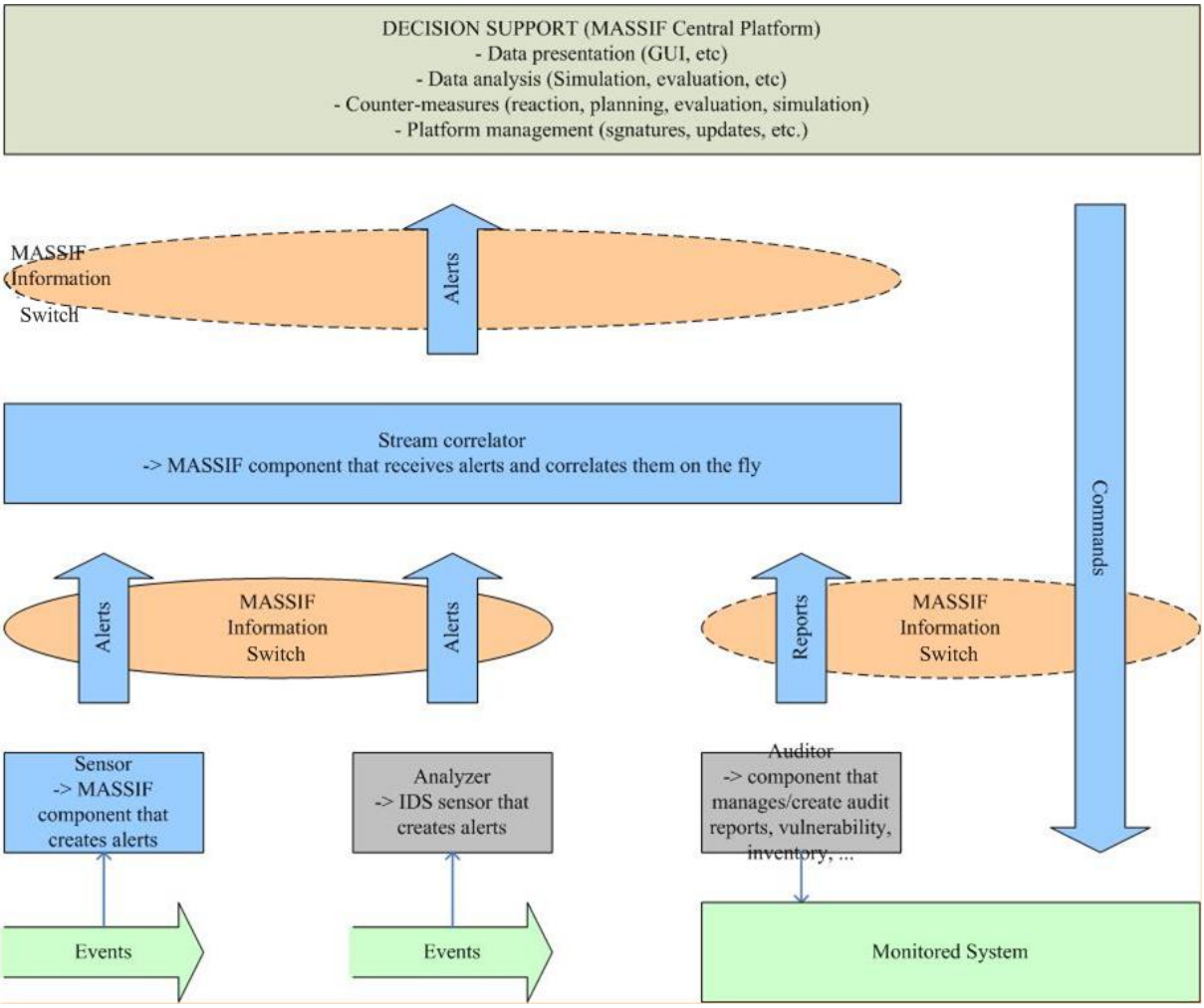

Figure 3.1: MASSIF Architecture Overview

The *blue* boxes are representations of MASSIF components and data streams. One can separate data streams in three categories:

Alerts are elements of information that represent a phenomenon of interest, typically an attack symptom. They are generally generated after being triggered by the action of a user of the monitored system, manifesting itself by the capture of some pattern within an event stream. Events streams are described in deliverable D3.2.1, and they can be generated either by components developed within the project, or by external intrusion detection systems.

Reports are elements of information that represent the state of the monitored system. They do not correspond to events generated in response to user requests, but rather to the maintenance of the monitored system, such as vulnerability analysis reports.

Commands are elements of information that are sent back by the MASSIF platform to the monitored system. The main purpose of these commands as envisioned within the project is threat mitigation.

The following components are considered within the MASSIF architecture:

Sensor is a MASSIF component that generates alerts. Within the scope of the MASSIF project, this covers the components that are detecting attacks against business processes.

Analyzer is an external component that generates alerts. Within the scope of the MASSIF project, this covers security-related components such as intrusion detection sensors, firewalls, web-application firewalls, antivirus, etc.

Auditor is an external component that generates audit reports related to vulnerabilities, inventories, maintenance operations, etc.

Stream correlator is a high-performance correlation engine to correlate alerts on the fly, using pre-specified queries to limit the stream of information reaching the central platform.

During the MASSIF March 2011 EB meeting in Darmstadt, FFCUL introduced the notion of the *MASSIF Information Agent (MIA)*, acting as a gateway to the MASSIF platform (cf. Fig. 3.1). This notion is in fact compatible with most SIEMs in the market, which require a mediation between the monitored environment and the central platform. This MIA will be the focus of the project's effort related to Activity 5, resilience and high volume data gathering.

Figure 3.2 represents a more detailed view of the architecture of the central massif platform. The monitored system and the three information streams (alerts, reports and commands) are represented at the bottom of the picture, while the graphical user interfaces for operators and management of the MASSIF platform are represented on top. This figure focuses on the needs of the project. Other components may appear in SIEM platforms, such as databases or archival servers, that are not relevant in the context of the project and have been ignored.

The MASSIF central platform is organized around two key components, information management and analysis on the left-hand bottom-up side, and countermeasures on the right-hand, top-down side:

Decision Support System has in charge the management of alerts and diagnosis. It is traditionally the component in charge of alert correlation in current SIEM platforms. Within MASSIF, it has in charge the management of alerts until a proposal for reaction can be offered to the operator. As such, it interacts with the following components:

Alert correlator The central alert correlator is in charge of analyzing and correlating alerts. It may use similar technologies to the stream correlator developed and presented in the previous figure.

System Simulator is in charge of analyzing the impact of alerts on the monitored system. It receives hypotheses related to possible decisions and evaluates them.

Attack simulator is in charge of analyzing the impact of attacks on the monitored system. It receives hypotheses related to possible decisions and evaluates them. It can also proactively report about potential attack opportunities; this activity is triggered by tasks directly submitted by operators.

The Decision Support System provides reports to the operators, which in turn request tasks for further analysis. One of these tasks is the submission of decisions to the Threat Mitigation System.

All three side components interact with the management GUI to receive threat models, attacker models and correlation rules.

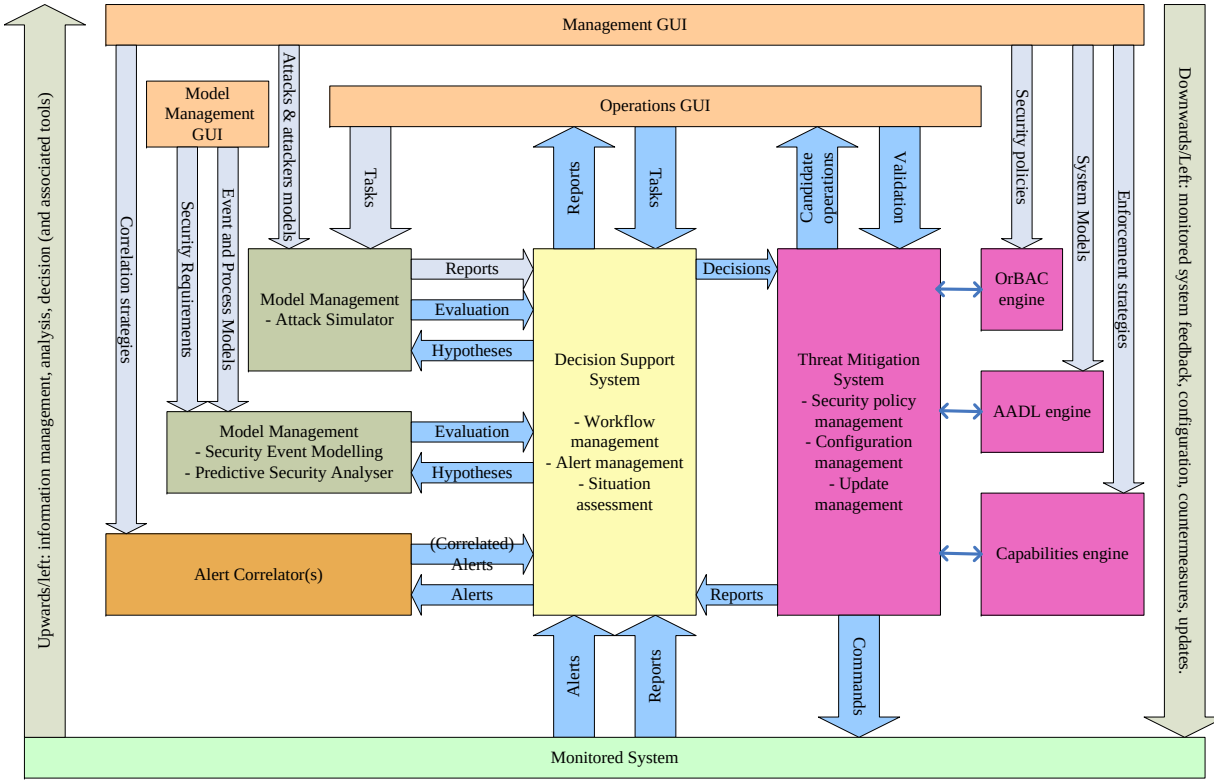

Figure 3.2: MASSIF Platform Architecture

Threat Mitigation System has in charge the application of decisions proposed to the operator by the decision support system. This includes managing the security policy of the monitored system in order to evolve it and align it with the current threats. As a consequence, it is also managing some aspects of the configuration of the monitored system as well as managing updates such as new intrusion detection signatures or system patches. As such, it interacts with the following components:

OrBAC engine (Organization-Based Access Control) is a modern security policy engine evolved from the Role-Based Access Control (RBAC) paradigm. It is used for modeling and managing the security policy of the monitored environment. The project will be using a Python-based implementation.

AADL engine (Architecture Analysis and Design Language) is a standard from the automotive industry (see deliverable D3.2.1). It is used to model system dependencies and threat propagation.

Capabilities engine describes the capabilities of the enforcement components available within the monitored system. Such description may be implemented using for example M4D4 (see deliverable D321).

The three side components also interact with the management GUI to receive security policies,

system models and enforcement strategies.

As one can see from the figure, the interactions between the Threat Mitigation System and the three side components are not fully specified yet. This will be the work carried out in WP 5.2.

This proposal has been validated by the project and will be refined further on an as-needed basis. This effort will continue in the project under the scopes of the testing and validation (WP2.3) and integration (WP5.3, WP5.4) work packages, and we will continue to enhance the architecture description as modules are developed.

3.2 Results from Language Definition and Mapping

The work package on language definition and mapping, while short-lived in the project, has a strong relationship to the coordination and impact of the project. The last decade has witnessed the development of a large number of data formats related to logs, events and alerts generation. This large number of formats is a consequence both of the need for monitoring tools and monitoring information, but also of the difficulty to converging towards a simple definition of the information that needs to be communicated from sensors and log providers to management platforms. This has a significant impact on MASSIF as promoting a set of easily understandable data formats would go a long way into improving the reach of SIEM technologies.

By and large, we can separate them in two broad categories, the general purpose formats and the specialized formats.

General purpose formats The general purpose formats mostly represent the point of view of the event consumer, generally a Security Event and Information Management (SIEM) system. Examples of these formats are IDMEF and IODEF from the IETF, but also the Common Intrusion Detection Framework (CIDF) or the Common Event Format (CEF) from Arcsight. Their specification is often large, as they try to acquire information from multiple heterogenous sources and normalize it. They structure and model the information, which helps defining what the detected event means, and what the circumstances are. They are thus believed to be complex to implement and are not widely adopted by event producers because of this added complexity. They also induce an overload in data transfer, as they tend to use more space to organize the information they manipulate. Also, they aim at easing the data interpretation issue, which is not an advantage for sensor vendors.

Specialized formats The specialized formats represent efforts by intrusion detection sensor vendors to communicate the diagnosis (attack) information to other components. Examples of these specialized formats are all the ones developed by vendors and developers (snort, bro, modsecurity, etc.), or the Cisco Security Device Event Exchange (SDEE), a more global effort from the network intrusion detection community. These formats are usually quite simple, and they tend to be compatible with the syslog protocol, acting as a general transport mechanism for SIEM systems. However, the vendors do not make commitments to the format, and this requires SIEM vendors to interpret many specifications and adapt their translation layers every time a new software release. They also tend to use shortcuts, such as signature identifiers; this means that the event message is not self-contained, and must be associated with the knowledge of the configuration of the sensor which generated it in order to be fully interpreted. However, this requires keeping sensor configuration and event collector knowledge base synchronized, which may be hard.

This section analyzes the Intrusion Detection Message Exchange Format (RFC4765) and proposes leads for the development of a second version of the format that improves the usability and the interoperability of intrusion detection and prevention systems. IDMEF was initially started as a research interoperability effort by DARPA at the end of 1998 and was stable around 2003, even though the final RFC was published only in 2007. Unfortunately, the software security market evolved significantly during this period, as well as the threat landscape. This has significantly lessened the impact of IDMEF. At the same time, experience and feedback have been provided by the community, up to a point where a second version of the standard could be developed to make it much more useful for the community.

We have identified the following important features of IDMEF V1 that bear more detailed analysis.

Message type segmentation The IDMEF format separates the notion of heartbeat from the notion of alert. This helps reduce the confusion between messages types and objectives. Note however, that the creation of the CorrelationAlert and ToolAlert subclasses introduced confusion, but not for the same reason. The ToolAlert is in fact too specialized and narrow to usefully represent the variety of malware and attack tools available today and its specification should be relegated to users and product developers. The CorrelationAlert, on the other hand, is useful in SIEM platforms, for local information modeling and exchange. It relies on alerts, can reuse some components of them, but should be a different message. At the same time, the Heartbeat message could be expanded to include additional information on the sensor configuration. This capability is currently possible via the AdditionalData construct, but its use should be clarified.

Strong typing IDMEF V1 was designed as an UML class diagram model, which enables strong typing of attributes. Typing helps reducing ambiguity, but requires programmers to follow the specification accurately. As such, it is not robust to message alteration. While this is useful to ensure message integrity, it is also a strong constraint as implementors faced with new kinds of information that do not fit the existing types will either abuse them or omit interesting information. As much as strong typing is useful, it should be reserved to the most common objects, and associated to easily implementable extension mechanisms.

Definition of common objects and object types The IDMEF data model showed that there were many common objects being manipulated by SIEM environments that could be included in alerts. Machines are hosts for sensors as well as targets and origins of attacks. These machines can be identified in many different ways, depending on the capabilities of the sensor which is monitoring them. For example, the web server identifies client machines, either by name or IP address, but does not identify itself. A network-based sensor will only capture IP addresses as they appear in the packet. Thus, the same client machine could appear under different identifies regardless of format. This problem cannot be solved by the data format, so the constraints imposed by IDMEF on the description of these components should be relaxed to simplify message manipulation.

Referencing system The IDMEF V1 format includes a referencing system that enables identification of entities by a simple token. This ability exists for many components of IDMEF, such as the analyzer or the node. This creates the ability to exchange entity information by reference within a message, thus saving time and space, especially if a given component is repeatedly included in messages. In practice though, this feature seems not to be used, as implementors focus on simple identifiers that are easily within their reach (such as IP addresses). They could duplicate the information, but they do not. Also, maintaining coherence is not taken into account. IODEF V1 also includes a referencing system, the primary target being the ability to anonymize component information; two

entities exchanging information can preserve their proprietary view of said component while ensuring that they identify it with a reference that is translated from one to the other and vice-versa. This referencing capability must be part of a newer message format design, and it in fact encompasses the needs of many formats, making it a generic tool that can be homogenously standardized across several standard formats.

Extensibility IDMEF was designed to be extensible. This is important in the information security domain, as we cannot foresee what the new attack and defense mechanisms will be, and what kind of information detection and prevention systems will need to represent in order to model and configure the capabilities of these tools. Unfortunately, the solution proposed in IDMEF V1 (the AdditionalData mechanism) is difficult to implement, and it does not integrate well with the DTD, which is the normative reference. Moving to an XML schema and focusing on a single, XML-based extension mechanism would make it easier to use. An alternative design would be to include extensions as sub-schemas opaque XML blogs whose internals could be validated by an on-line mechanism. The provider of the data must then put the associated schema online. This would offer an additional degree of freedom to vendors; the most successful sub-schemas could then be made available to the community by IANA as additional standard representations of components.

Complexity and XML Using an XML-based representation of the information is often considered complex and costly. While widely accepted in the web services domain, it is only reluctantly used in the information security area. The most used formats today in this domain are one-liner formats, often using a ”key=value” pair mechanism, as exemplified by the web servers Common Log Format (CLF), syslog or iptables logs. Yet, the expressiveness of XML formats over binary or textual (e.g. syslog) representations may outweight the complexity drawback, especially since these one-liners are severely limited in size (a couple of thousand bytes), which may be insufficient to carry the information needed in an alert. Another typical limit is encodings, which pushes vendors towards awkward representations that alert consumers have difficulties parsing and understanding. In order to be more widely accepted though, it would be extremely useful to associate the best of both worlds, XML and one-liners. In addition to an XML representation, IDMEF V2 should be easily derived into a textual line-oriented representation akin to serialization, which would ensure that both the more explicit XML messages and the one-liner strings would convert easily into one-another. This dual, synchronized representation would preserve the interests of both event producers (using the one-liner format as less expensive to transmit smaller amounts of information) and event consumers (prefering the more complex XML to keep aggregated the overall incident, alert or attack information). Yet, both should share the same keys and encodings, to facilitate programmatic manipulations.

We are looking into the possibility to join additional fora for diffusion of this work. An Internet Draft of what could be IDMEF V2 is currently in the works at Télécom SudParis and might be submitted for discussion an the IETF meeting in Taipei in November.

3.3 Input from deliverable D2.3.1 evaluation plan

The results of MASSIF project need to be evaluated in order to verify their conformance to the requirements and their usability for the use case-scenarios defined in MASSIF deliverable D2.1.1 [7]. The

Evaluation Plan deliverable provides strategies to evaluate MASSIF platform according to the requirements of the four application scenarios described in D2.1.1: Olympic Games, Money Transfer Service, Managed Enterprise Service Infrastructure and DAM Critical Infrastructure. The evaluation should concern specific features as well as the entire system. The evaluation scope is limited to the criteria from the perspectives of end-users (scenarios providers). It does not address the detailed criteria or tests to be used by the developer in order to evaluate all the new features and functionalities that will be introduced by MASSIF project. The specified criteria will first serve as a guideline for MASSIF developers in order to take into account the expectations of the scenario providers. They will also be used to evaluate MASSIF platform, in the third year of the project, by the end-users. D2.3.1 proposes to base the specifications of evaluation criteria on recommendation of recognized international standards. The methodology we propose is based on two series of standards which are complementary:

- ISO/IEC9126 [4] standards for product quality in software engineering;
- ISO/IEC14598 [3] standards for software product evaluation in information technology.

The deliverable describes the objectives of the evaluation and defines the generic template for the evaluation criteria. It also defines the list of criteria. The first set of criteria is common to the four scenarios and the second set is specific to each scenario. The deliverable describes how MASSIF platform will be evaluated as an entire system. It discusses various approaches from centralized platform to distributed platform. It defines logical and physical entities needed to evaluate MASSIF features such as workload generator and attack Injectors. Some of these features can be evaluated by the end-users (e.g. scenario providers), some other features are only accessible to the developers. Finally the deliverable provides the platform testing plan, that developers should execute prior to the user validation, to check that all the expected functionalities are implemented correctly. It also specifies a list of tests to be executed by MASSIF partners in order to verify the conformance of MASSIF platform to D2.1.1 [7] requirements. These tests are classified in four categories: (1) Security, (2) Event Processing, (3) Trustworthiness, (4) Compiler technologies.

4 Report on Technology Roadmapping

4.1 MASSIF Technology Guidelines

Based on the requirements defined in deliverable D2.1.1 [7] for the four scenarios in MASSIF, a set of recommendations that should guide the design and development of next generation SIEM platforms has been identified. These desired features of future SIEMs will apply in MASSIF as far as possible. They will help the development activities within the project in keeping a tighter connection with the scenarios, and overall give MASSIF a stronger sense of focus. The recommendations can be found below divided in four topics: security, event processing, trustworthiness, and compiler technologies. In what follows, we revisit these recommendations.

4.1.1 Guidelines concerning security

Besides issues like dependability, redundancy or fault tolerance, the analysis of the above-mentioned scenarios unveils the need for security-related analysis features of the envisioned SIEM platform. These features go beyond what is currently supported by existing solutions, which lack capabilities for modelling incidents at an abstract level, possibly referring to process definitions. From the stated limitations of existing SIEM solutions, the following requirements have been identified with regard to the introduced scenarios:

- Correlation across layers of security events, from network and security devices as well as from the service infrastructure such as correlation of physical and logical event sources. This is due to the variety of systems issuing inputs that can give insights to security only when combined. An example is the off-site monitoring and the on-site management of the dam's configuration.
- Multi-level security event modelling that will enable to provide a holistic solution to protect the respective infrastructures. The Olympic Games Scenario stipulates that it would be of interest to understand the effects of technical events on the user or process level of the system.
- Analysis of malicious behaviour using attack graphs. Many of the security issues mentioned in this document originate from complex malicious actions or patterns of actions (e.g. the laundering of money in the mobile money transfer scenario or the misuse case of *Low and Slow* attacks in the Olympic Games infrastructure).
- Predictive security monitoring that allows to counter negative future actions, proactively- As stated in deliverable D2.1.1 [7], there is a crucial demand for early warning capabilities. Moreover,

the limitations with regard to the Managed Enterprise Service point to the fact that dealing with unknown or unpredictable behaviour patterns is not sufficient in current SIEM solutions.

- Modeling of the events and their relation to other, possibly external, knowledge. A basic precondition of prediction and simulation as well as of attack analysis is the proper representation of the security requirements and any relevant information about the system as well as any knowledge about the actual and possible behaviour. When reasoning under incomplete information it is not only decisive to properly gather and describe the information available, but it is also required to develop novel methods based on discernibility, probability or plausibility in order to reason about uncertainty.
- Securing the evidence progressed by the MASSIF components. D2.1.1 states the misuse case of a sensor compromise, showing that it is vital to be able to trust the information that is received, when using events from sensors like those deployed to monitor the dam or other critical infrastructures.

4.1.2 Guidelines concerning event processing

According to the descriptions of the requirements, the recommendations for the next generation event correlation engine can be summarized as follows:

- Real-time: The system must process input data at high rate and provide meaningful results with soft real-time requirements.
- Scalability and elasticity: The engine should be capable of handling high input rate and optimize the amount of resources based on the actual load. In other words, the system should monitor both input loads and vital parameters, such as CPU utilization, in order to adjust the amount of resources, i.e., provision more resources during peak load times and decommission them during valley load periods.
- Handling streaming and stored data. The engine should allow to process and correlate both streams of events and stored relations (i.e., information stored in a database).
- Multiple-sources: The engine should be able to aggregate, abstract and correlate heterogeneous events from multiple sources at different levels of the system stack.
- Pre-defined correlation rules and correlation rule wizard: The engine should be shipped with a set of predefined correlation rules to identify well-known attacks. However, it should also support easy and intuitive creation of user-defined rules.

4.1.3 Guidelines concerning trustworthiness

The analysis of the scenarios' requirements in MASSIF D2.1.1 indicates that the following key contributions would improve the general resilience and trustworthiness aspects of the next generation SIEMs:

- Resilience of the infrastructure. The infrastructure should be highly resilient under attack, concurrent component failures, and unpredictable network operation conditions.

- Security of event flows. The event flows should be protected, from the collection points through their distribution, processing and archival.
- Protection of the nodes. The designed mechanisms should offer flexible and incremental solutions for node resilience, providing for seamless deployment of necessary functions and protocols. These mechanisms should take into consideration particular aspects of the infrastructure, such as edge-side and core-side node implementations.
- Timeliness of the infrastructure. The infrastructure should provide for (near) real-time collection, transmission and processing of events, and ensure the corresponding reliable and timeliness generation of alarms and countermeasures when needed. Similarly, and in particular from D2.1.1 requirements, suggests that features for forensic support should satisfy the following requirements:
- Data authenticity. Security event data contents, as well as additional/added information related to data origin and destination must be the reliably stored.
- Fault and intrusion-tolerant stable storage. The stable storage system on which data for forensic use will be persisted must be tolerant both to faults and to intrusions.
- Least persistence principle. With respect to sensitive data, only information which is actually needed should be persisted to stable storage (most of the data should be processed in real-time and thrown away).
- Privacy of forensic records. Forensic evidence related to security breaches will be made available only to authorized parties.

4.1.4 Guidelines concerning compiler technologies

An analysis of the requirements which have been identified for the four MASSIF scenarios in D2.1.1, suggests that the data gathering level of a next generation SIEM solution must provide efficient implementation and/or support for a number of features, especially the following related to the data collection and parsing:

- Heterogeneity support. The data gathering level must have the ability to deal with a large number of highly heterogeneous data feeds.
- High degree of adaptability. This will allow seamless integration of new types of security tools/probes, to improve the capabilities of the SIEM.
- Peak handling. The volume of events to be collected and processed per unit of time can occasionally increase resulting in load peaks. The data collection layer should be able to handle such peaks and to propagate relevant events to the SIEM core platform without loss of information.
- High degree of expressiveness. The parsing logic and related languages must allow effective processing of virtually any type of security relevant event.
- Support for fast and reliable development. Simple technique/tools must be available, which will make it possible to implement, deploy, and integrate new parsers and collectors in a relatively short time and at a relatively low cost. In particular, the need for hand coding of the probes should be limited to a minimum, as it results in an error prone as well as time consuming procedure.

- Generality and platform independence. The parsing/processing logic (and code) should be as much as possible decoupled from the specific characteristics of the data format and related technologies.
- Distributed processing. Whenever possible (and convenient), the data collection and parsing layer should implement parsing, filtering, and correlation functions at the edges and/or at intermediate nodes, i.e. nodes located along the path to the core SIEM correlation engine.

4.2 Outreach of MASSIF results

In order to meet to the impact creation objective, MASSIF has been developing clustering and networking activities. These activities had the main purpose to strengthen the collaboration between MASSIF and several R&D projects and initiatives to identify possible cooperation opportunities and common interests.

4.2.1 Bilateral and multilateral activities with other R&D projects

Project Effectsplus

Effectsplus[1] (or EFFECTS+) is a FP7 Coordination and Support Action across a large spectrum of R&D activity in the ICT Framework Programme that relates to the twin requirements of Trust and Security (T&S), and their constituent concepts and components. Effectsplus activity focuses on two major areas:

- The clustering of Trust and Security projects from ICT theme (especially those of Call 5). This aims at bringing together short, medium and long term trust and security challenges, reducing fragmentation and creating synergies among the projects.
- The Future Internet roadmapping. This relates to the development of a research roadmap for Trust and Security Research on the Future Internet.

MASSIF has been playing an active role in the Effectsplus technical clustering activities. **MASSIF leads the "Systems and Networks" cluster** and also participates in the "Services and Clouds" cluster, in relation to "Provisioning for Security, Trust, and Identity" and "Assurance and Compliance" areas.

The clustering kick-off event (Brussels (Belgium), March 29th-30th 2011) [1] served not only for presenting MASSIF to the involved R &D projects (main objectives, vision and foreseen results), but also for identifying common technical issues & possible collaborations. This first meeting raised up the high commonalities with the VIKING project. As a result a close relationship was established, as reported in Section 4.2.1.

For the second clustering event (Amsterdam(Netherlands), July 4th-5th 2011) [2], MASSIF organized a technical workshop on Models (cf. Section 4.3.2) for the "Systems and Networks" cluster. This workshop resulted in some new plans for multilateral collaborations between projects as shown in Table 4.1.

To a lesser extent MASSIF also participated in the technical workshop on Software Assurance and Trust for the "Services and Cloud" cluster.

[1] http://www.effectsplus.eu/

Jesús Villasante the head of the Trust and Security Unit in the EU Directorate General Information Society and Media (DG Infso) participated in the meeting. He confirmed that his unit will support these clustering activities.

Further clustering events are planned for 2012. MASSIF will continue partaking in these cooperation activities.

Lead: Collaborating projects	**Area of common interest**
R. Rieke, G. Bjoerkman: MASSIF, VIKING (*already started*)	SCADA, critical infrastructures, cyber security modelling
A. Lioy: PoSecCo, ENDORSE	Privacy
A. Lioy: PoSecCo, ASSERT4SOA, MASSIF	Service modelling
I. Kotenko: MASSIF, ANIKETOS, PoSecCo, Hydra, WSAN4CIP, ASSERT4SOA	Analytical attack modeling and security evaluation (SNDS2012)
R. Baldoni: Comifin, MASSIF, VIS-SENSE, SYSSEC, ANIKETOS, WSAN4CIP	Systems Arch., CEP, modelling platforms, monitoring large systems, pattern detection, privacy preserving
N. Papanikolaou: ANIKETOS, ENDORSE, POSECCO, MASSIF(to be confirmed), COMIFIN	Policy, (a) theoretical aspects (b) applications

Table 4.1: Multilateral collaborations within the Effectsplus “Systems and Networks” cluster

Project VIKING

On April 27 the VIKING[2], MASSIF and SecFutur FP7 projects met at Fraunhofer SIT in Darmstadt to discuss synergies between these projects in a sub-cluster meeting under the Effortplus initiative. Gunnar Bjoerkman, the project coordinator of VIKING, presented the VIKING project with special focus on the modeling aspects which are of interest for MASSIF. Roland Rieke and Julian Schütte presented the MASSIF project with a focus on the predictive security analysis and the planned event modeling component. This also led to VIKING coordinator to become member of the advisory board.

There seems to be synergies between VIKING and MASSIF in the area of IT architecture, attack modelling and impact analysis. Fraunhofer is especially interested in how the architecture and attack models are merged. The VIKING and KTH (Royal Institute of Technology) work is interesting for MASSIF and there are plans to organise a common meeting at KTH to present and discuss the work done in VIKING/KTH on a more detailed level.

The meeting of projects VIKING, MASSIF and SecFutur is a first successful result of the Effectsplus clustering initiative and was helpful to prepare targeted material for the modelling workshop of the Systems and Networks Cluster in Amsterdam (cf. Section 4.3.2).

[2] http://www.vikingproject.eu

Project DEMONS

The FP7 project DEMONS[3] was identified at the very beginning of MASSIF, as one close project in terms of functionality. The participation of France Telecom in both consortiums and the good relationship of Atos with Telefonica (project DEMONS coordinator) led to a first contact aiming at a joint collaboration.

DEMONS envisions building a novel cooperative network monitoring and mitigation system based on a completely decentralized, application-aware, privacy-preserving, multi-jurisdictional monitoring infrastructure. Such an infrastructure will provide the detection, reporting and mitigation mechanisms needed to combat not only today's threats, but also those of tomorrow. DEMONS aims to realize this infrastructure by applying novel distributed systems technologies and leveraging their native scalability and fault tolerance characteristics.

On September 9, France Telecom presented the MASSIF project to DEMONS consortium during the DEMONS meeting in Paris.
MASSIF and DEMONS will try to intensify the cooperation in the second year of the project. They aim to organize a joint workshop in 2012.

Project SecFutur

Carsten Rudolph, the project coordinator of SecFutur[4] presented work done in Fraunhofer on Trusted Computing and TPM which is used in the embedded systems building blocks within the SecFutur project on April 27 at the VIKING, Massif and SecFutur meeting. Roland Rieke also had a meeting with the SecFutur partner SEARCH-LAB in Budapest on May 30th. Because one of MASSIF's scenarios, namely the DAM critical infrastructure, is connected to cyber-physical systems, the MASSIF team is interested in SecFutur's experience in this area, specifically w.r.t. the work done in task 5.1.4.

Project Hydra

The Hydra[5] project is an FP6 Integrated Project that developed middleware for Networked Embedded Systems. The Hydra middleware allows developers to incorporate heterogeneous physical devices into their applications by offering easy-to-use web service interfaces for controlling any type of physical device. Hydra incorporates means for Device and Service Discovery, Semantic Model Driven Architecture, P2P communication, and Diagnostics. Hydra enabled devices and services can be secure and trustworthy through distributed security and social trust components of the middleware. The MASSIF team will leverage Hydra's context-aware security and event processing capabilities for the work on security event modelling in WP4.1. Julian Schütte, a former member of the Hydra team, communicates this knowledge to the MASSIF project.

[3] http://fp7-demons.eu/
[4] http://secfutur.eu/
[5] http://www.hydramiddleware.eu/

Project Esukom

The ESUKOM[6] project aims to develop a real-time security solution for enterprise networks that works based upon the correlation of metadata. A key challenge for ESUKOM is the steadily increasing adoption of mobile consumer electronic devices (smartphones) for business purposes which generate new threats for enterprise networks. ESUKOM focuses on the integration of available and widely deployed security measures (both commercial and open source) based upon the Trusted Computing Group's IF-MAP specification. The MASSIF and Esukom teams will exchange their findings and expertise.

Project FI-WARE

FI-WARE [7] (Future Internet WARE) is the cornerstone of the Future Internet PPP program[8], a joint action by the European Industry and the European Commission. As main objective, FI-WARE is expected to deliver a novel service infrastructure, building upon certain elements or enablers that offer reusable and commonly shared functions making it easier to develop Future Internet applications in multiple sectors. Among its various functionalities, there is a work line on monitoring and control mechanisms, which is close to MASSIF in scope. The participation of Atos in both projects led to some preliminary contacts with FI-Ware in order to seek for joint cooperation opportunities. Though the current technology readiness level of MASSIF developments is not sufficient to include them as part of the enablers portfolio, later stages could evolve in better and satisfactory opportunities for cooperation or exploitation.

Project SESERV

SESERV[9] (Socio-Economics SERVice for European research projects)coordinates the work on Future Internet socio-economics (SE. It aims at studying the socio-economic aspects on Future Internet research by considering the different viewpoints and interdependence of multidisciplinary domains (research, economics, humanities, law, etc). Though SESERV is not properly a technical project, it expresses another angle of the Future Internet that cannot be underrated. MASSIF participated in SESERV survey based on its tussles analysis methodology by bringing forward new stakeholders, scenarios and how these stakeholders interact within these scenarios. The resulting reports by SESERV are expected to be a valuable input for future exploitation activity in MASSIF.

4.3 Research Challenges and Emerging Trends

The vision of the Future Internet, where multiple services are transparently and seamlessly mixed, already created a paradigm which promises to largely enrich our ability to create new applications and businesses within this new environment. But this paradigm also enables new possibilities for threats and scales up the risks of financial and also physical impact. In many cases, the information itself will be

[6] http://www.esukom.de/
[7] http://www.fi-ware.eu/
[8] http://ec.europa.eu/information_society/activities/foi/index_en.htm
[9] http://www.seserv.org/

the essential product which deserves to be protected, in the Internet of Things however, real and virtual Cyber-physical resources deserve our attention.

4.3.1 Management of Security Information and Events in Future Internet

During the technical discussions at the MASSIF Executive Board Meeting in Darmstadt (March 2011) the consortium came to the conclusion that the evolving internet provided new questions for SIEM deployments. Therefore there was ground for MASSIF to contribute to the Future Internet Research Roadmapping.

Besides MASSIF, Fraunhofer SIT is involved in the projects SecFutur and ASSERT4SOA. As a summary of the positions of these projects, Fraunhofer submitted a short paper on "Challenges for Trust and Security in Future Internet Infrastructures" to the FIA Roadmapping Open Workshop on March 31st 2011. This paper stated that *"the Future Internet shall support a trust infrastructure with inherent support for trust areas (...). Trust areas could be used to augment SIEM systems with their own security mechanisms. Furthermore, SIEM in the Internet could also be deployed as cloud type services"*. The paper was accompanied by a presentation describing the changes that the future internet will need to take into account, challenges and gaps to be addressed and new approaches or technologies to overcome these.

Furthermore, MASSIF provided input to the Effectsplus Trust and Security Research Roadmapping. Figure 4.1 summarizes MASSIF's position.

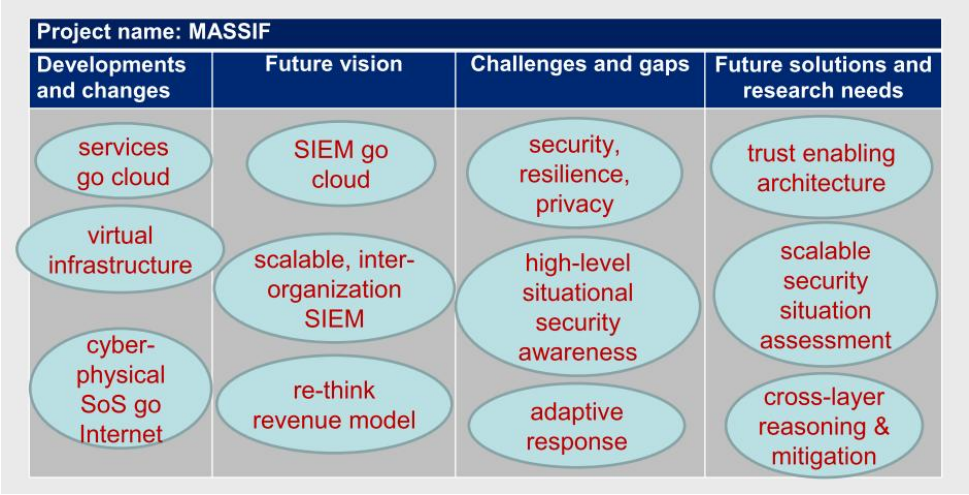

Figure 4.1: MASSIF map for FIA roadmapping

In the following we will outline the key issues mentioned in Figure 4.1 in more detail.

Changes and Developments

Security Information and Event Management (SIEM) is a key concept to identify security threats and mitigate their malicious impact. Traditional SIEM deployment occurs *within* a corporate infrastructure

or it is provided by an external service provider. In such a Managed Enterprise Service Infrastructure, which is typically based on a managed IT outsource environment where events from multiple sources are collected centrally, it is also generally the case that SIEM deployment is within the realm of the provider organization and that events only pass via internal customer or service provider links. However, the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) paradigms are driving a complete re-think of the models whereby organizations deploy and manage their own infrastructure for many aspects of their computing needs.

Furthermore, Future Internet SIEM has to address the connection of *Cyber-Physical Systems (CPS)* via the Internet which extend existing critical infrastructures and form totally new types of planet-scale coaction structures.

Vision

The drive to use IaaS and PaaS paradigms implies a need to consider the implications for *deployment of SIEM in the cloud*. Following this trend, organizations could avoid Capex investments to deploy their own analysis modules, through contracting an Opex based SIEM service based on a fixed or variable monthly fee. Through the likely shift of SIEM service provision, from stand-alone organizational environments to a shared cloud processing facility, there are opportunities to make inter-organisational analyses. This in itself raises many issues in terms of *ensuring privacy and integrity of the events* of any particular company, while still gaining the benefit of being able to spot cross-company trends. The *security of a cloud based service is also critical*, and a likely stepping stone towards Public based services is that Private cloud services, from reputable large service providers, will be the preferred deployment model. In this mode, service providers have full oversight and control over event processing, while customers benefit from a lower cost, on-demand, scalable service.

Challenges

Most important, by its very nature, the SIEM itself in a hostile and unpredictable environment is a potential target for an attacker. To prevent for example the interception or blocking of SIEM event feeds, an Internet based SIEM cloud type service would have to provide quality of service guarantees to *ensure reliable and timeous arrival of security event information* from the sensors. The debate on *Internet net-neutrality* could also refer here since there could be a case for expediting *control traffic* such as SIEM event feeds.

Ideally, the SIEM system should be able to analyze upcoming security threats and violations in order to trigger remediation actions even before the occurrence of possible security incidences. Therefore, new process and attack analysis and simulation techniques are needed in order to be able to relate security relevant events and evaluate them with respect to given security requirements.

The emerging trend for the use of meshed wireless communication to connect *cyber-physical systems* to critical infrastructures and to the Internet as a whole also has to be addressed in Future Internet and Internet of Things (IoT) SIEM. This large scale connectivity, not only of sensors but also of actuators, enables totally new types of remote attacks against critical services and infrastructures with *potentially very high impact and Societal cost*. Novel adaptive response technologies are therefore needed to enable anticipatory impact analysis, decision support and to provide impact mitigation by adaptive configuration of countermeasures such as policies.

Solutions and implied RTD needs

The project MASSIF addresses these challenges within its main research activities.

The vision of creating a next-generation Security Information and Event Management environment drives the development of an architecture which provides for *trustworthy and resilient collection of security events* from source systems, processes and applications.

A number of novel inspection and analysis techniques are applied to the events collected to provide *high-level situational security awareness*, not only on the network level but also on the service level where high-level threats such as money laundering appear. An *anticipatory impact analysis* will predict the outcome of threats and mitigation strategies and thus *enable proactive and dynamic response*.

Finally, the balance between the amount of processing, normalization, aggregation and analysis at *edge collectors* of an SIEM system, and the work done at the central *nerve centre* are also topics which have to be re-considered in the context of an Internet type deployment of an SIEM system. A scalable distribution of acquisition and parallel processing, and seamless function-splitting between core engines and edge collectors, like the one MASSIF develops is an first important step in this direction.

In essence though, the evolving Internet provides many new questions for SIEM deployment, and from an SIEM perspective reinforces the importance of having an Internet with security and possibly differentiated service for *high priority* and *trustworthy* control traffic such as the events from an SIEM. The commercial models also change since a *service fee* needs to evolve to scale up/scale down and pay-per-use models. The MASSIF project is already addressing many issues which we have identified to be needed in the Future Internet vision which we have presented in this section.

4.3.2 MASSIF Models w.r.t. Models in other FP7 Projects

The vision of the Future Internet heralds a new environment where multiple services are transparently and seamlessly mixed and exchange information, giving rise to new capabilities. This paradigm largely enriches our ability to create new applications and businesses but also enables new possibilities for threats and scales up the risks of financial and also physical impact.

Various projects in the ICT Framework Programme are currently using **Models** of different kinds in order to assess upcoming security and privacy challenges and mitigation strategies w.r.t. their possible impact.

MASSIF organized a workshop on July 4th-5th 2011 within the Effectsplus activity of Systems and Networks cluster, which aimed to provide a forum for discussing the different approaches of FP7 projects in this area. The projects were invited to contribute their activities w.r.t:

- Security Incident Models providing Qualitative and Quantitative Security Measurements (base measures and derived measures to audit and monitor complex distributed systems in FI)
- Models of Security and Privacy Requirements and Policies for FI
- Enterprise Architecture Models for Security Analysis
- Society Models for Social Impact Analysis
- Models of Security and Privacy issues in Cyber-Physical Systems, Smart Grids and other Critical Infrastructures

- Security by Design - Models on Resilience and Trust (e.g. use of trust anchors to provide a trusted backbone infrastructure)
- Models on Security and Privacy issues in Cloud Computing

The aim of the workshop was to identify possible areas of collaboration among projects w.r.t. concrete models which are publicly available and re-usable in related projects as well as to identify gaps between existing approaches and promising areas for future research.

Presentations at the Models Workshop

The following list gives an overview of the presentations at the workshop:

- Roland Rieke (MASSIF): Objectives of the Effectsplus Systems & Networks Cluster Workshop on Models
- Igor Kotenko (MASSIF): Analytical attack modeling and security evaluation in MASSIF
- Teodor Sommestad (VIKING): Enterprise Architecture Models for Security Analysis
- Mats B-O Larsson (VIKING): Virtual City Simulator (ViCiSi)
- Domenico Presenza (ASSERT4SOA): Ontologies in ASSERT4SOA
- Federica Paci (NESSoS, SecureChange): Managing Security and Changes throughout the whole System Engineering Process
- Antonio Lioy (PoSecCo): PoSecCo models
- Steffen Peter (WSAN4CIP, TAMPRES): Assessment models to Improve the Usability of Security in Wireless Sensor Networks
- James Davey (VIS-SENSE): Multi-Dimensional Clustering for the Purposes of Root-Cause Analysis
- Mark McLaughlin (ENDORSE): Introducing the ENDORSE Privacy Rules Definition Language
- Roberto Baldoni (CoMiFin): Collaborative Security for Protection of Financial Critical Infrastructures: The Semantic Room abstraction model

The MASSIF presentation focussed on the aspect of analytical attack modelling and security evaluation in MASSIF. Igor Kotenko (SPIIRAS) presented the Attack Modelling and Security Evaluation Component (AMSEC) and the key elements of architectural solutions proposed by MASSIF. These are

- Using security repository (including system configuration, malefactor models, vulnerabilities, attacks, scores, countermeasures, etc.)
- Effective attack tree generation techniques
- Taking into account as known as well as new attacks based on zero-day vulnerabilities

- Using Anytime algorithms for near-real time attack subgraph (re)generation and analytical modelling
- Stochastic analytical modeling
- Combined use of attack graphs and service dependency graphs
- Calculation metrics of attack and security countermeasures (including attack impact, response efficiency, response collateral damages, attack potentiality, attacker skill level, etc.)
- Interactive decision support to select the solutions on security measures/tools by defining their preferences regarding different types of requirements (risks, costs, benefits) and setting trade-offs between several high-level security objectives

Results of the Models Workshop

Besides the multilateral collaborations initiated by this event which are reported in Section 4.2.1 the following Effectsplus supported Systems & Networks cluster activities have been suggested:

- Classification (overview) of areas covered by the presented models (interactively edit a table on Effectsplus web-site)
- Joint paper (e.g. FIA book), or workshop: European perspective (survey) of models on security, privacy, trust
- Followup S&N cluster meeting on specific aspects of multilateral project cooperations (Feb. 2012, HP-labs, Bristol)
- Participation in Cyber-Security and Privacy EU Forum CSPEF 2012
  (Berlin 24.-25.4.) with Demonstrations and Tutorials

4.4 MASSIF Advisory Board

In an attempt not to lose track of the most innovative trends on the security information event management field, the Annex I proposed the establishment of a group of experts called “Advisory Board” (AB) that would guide the project progress. This section describes all aspects related to the participation of this group during the first year of the project.

4.4.1 Terms of participation

The participation of the advisory board in the project is described by means of a Terms of Reference (ToR) document, which is also included in the Appendix (cf. Chapter 6). This document describes the possible roles of a member, including the following aspects:

- To provide guidance to the project to application areas (Scenario requirements, security event processing, process models, attack simulation or resilience framework).

- To provide input and feedback to the MASSIF technology roadmap (related to this very document).
- To provide input and feedback to the MASSIF requirement specification.
- To provide input and feedback to the MASSIF components development.
- To provide guidance regarding ethics, privacy and compliance.
- To provide a linkage with other initiatives and groups of interest.

The members of the AB are not expected to satisfy each single role, but their participation is customized and formalized by means of a Letter of Interest (LoI) sent to Atos as MASSIF coordinator. This LoI is not binding, as the relationship is based on mutual interest.
The contact to possible new members is not only task of the coordinator. On the contrary, a successful cooperation is expected when it is related to specific fields of knowledge. Therefore MASSIF partners can identify potential members of the AB, though the final decision on membership relies on the approval by the Board of Directors.

In general terms Advisory Board members are expected to provide regular feedback to the MASSIF material issued by the consortium (deliverables or short descriptions). Nevertheless this participation can be intensified if there is particular interest of members on specific aspects, areas or concepts of the project.

4.4.2 Constitution

The MASSIF advisory board was constituted at the beginning of the project. It currently consists of the following members:

- Marco Hauri from ASCOM.
- Reijo Savola from the Technical Research Centre of Finland (VTT).
- Professor Urs E. Gattiker, Ph.D. from CyTRAP Labs GmbH.
- Luis Tarrafeta from S21SEC.
- Ferdinando Campanile from Synclab.
- Craig Gibson from Bell Canada.
- Gunnar Bjoerkmann from ABB AG, also coordinator of the FP7 project VIKING.
- Mario D'Angelo, Carlo Mogavero, Cinzia de Monte, Francesco Finelli and Dalia Paulillo from Telecom Italia (Tilab).

The first three individuals were contacted at the proposal phase of MASSIF by Atos and Fraunhofer and their are included in the AnnexI. After the Kick-Off meeting (in October 2010) they were asked to re-confirm their involvement in the project.
The rest were involved by MASSIF partners according to different interests. EPSILON contacted

S21SEC and Synclab. S21SEC can provide some guidance about particular aspects of public administrations. Additionally S21SEC is also a producer of Intrusion Detection Systems and SIEM and as such it can provide another point of view wrt the one of the SIEMS in MASSIF (OSSIM/ Prelude). In turn Synclab can benefit MASSIF with additional information about Business process monitoring
CINI contacted Bell Canada during the Canada-EU Future Internet Workshop 2011 [10] in order to take into account additional requirements related to telecom and SCADA use cases (not covered in MASSIF scenarios). CINI also contacted the Tilab members, who joined the advisory board at the end of the first year.
Finally, Fraunhofer-SIT contacted ABB during the EFFECTS+ KO cluster meeting in relation to modeling aspects in the project VIKING which could be of interest for Activity 4 (Even-driven process models and attack simulation).

4.4.3 Report of performed activity

The following list summarizes the participation of the advisory board members in the project.

Participation to the A4 meeting in Darmstadt

On June 27th 2011 an A4 meeting was held at Fraunhofer-SIT premises in Darmstadt (Germany). Though the scope was focused on developments under this activity, the agenda included a devoted session for the advisory board participation. Marco Hauri (Ascom) participated in such session where the project and A4 activities were presented. As part of his recommendations Mr. Hauri stressed the need for clarification of some concepts for the sake of the project understanding, such as the applicability of results and the interconnection and dependency between project activities. Additional comments pointed out the interdependency between policies and attack trees and the need for acceptance criteria at the evaluation phase. Finally there were additional discussion about the term “intelligent SIEM” to avoid misunderstanding of the MASSIF achievements.

Participation to the EB meeting in Naples

On September 14th 2011 a new EB Meeting was held at CINI premises in Naples (Italy). The agenda included a large session for the advisory board where the preliminary results on the following topics were presented (see Section 4.1 for further information)

- Deployment and evaluation
- Scalable event processing engine
- Event Collection, parsing and propagation
- Security Event modelling
- Predictive Security Analyser

[10] http://www.futureinternet-internetdufutur.nrc-cnrc.gc.ca/eng/index.html

- Attack modelling, simulation and risk evaluation

Representatives from Telecom Italia (Dalia Paulillo, Mario D'Angelo), Bell Canada (Craig Gibson) and Sync Lab (Ferdinando Campanile, Luca Lopresti) attended such session . Feedback from this session pointed out the need for wider scopes in event management systems, including wireless, wire line, video or mobile applications. Another point brought forward was the need for correlation in real time of behaviors from one system against activities in other systems.

Feedback to architecture and requirements

Ad-hoc material related to the architecture and scenarios was delivered by email to the advisory board members to collect, refine, and supplement the consortium vision on MASSIF solutions. As a result we received questions and answers related to the Generic Event Translator(GET) platform and the resilience framework, as long as new use cases for GSM-based attack to synchrophasors.

Internet of Service (IoS) collaboration day

To promote the International Collaborations and provide testimonials on these, the EC has organized a workshop at the Collaboration meeting in Brussels 28-29 September 2011. CINI was invited to join this workshop and give a talk on the experience in North America with the project MASSIF. CINI presentation focused on the results of the collaboration with Bell Canada within the context of the MASSIF project. The detailed agenda and the presentation are available on the IoS Web site.

Future Internet Assembly book

As a possible follow-up of the International Cooperation meeting held in Brussels on Sep 28 and 29, the FIA care takers are planning the production of a chapter dedicated to International Cooperation, to be included in the next FIA book, to which CINI and Bell Canada have been invitated to contribute.

4.4.4 Future Actions

The participation of the Advisory Board is expected to continue during the second year, starting in October 2011. MASSIF consortium will seek for new opportunities to involve the AB members. In the short term a meeting with Gunnar Bjoerkman from ABB and Fraunhofer is scheduled on October 11th 2011 to discuss the recent results of MASSIF and collect some comments in the dam scenario which is closely related to the SCADA scenarios in VIKING project. In the mid term there are also opportunities of participating at the next MASSIF EB Meeting in March 2012 in Caen (France) and in the first MASSIF workshop (around March-April 2012).

5 Conclusion

In reflecting on the first twelve months of the MASSIF project, there has been a significant amount of activity, interaction and progress in all areas.

As with any project, the first year has been about “Establishment” and “Initiation” of the project, to ground the various work-packages and the collaborating teams. In this document the key points relating to progress in technical, organizational and operational activities has been reported. The overall architecture within which the various work-packages will be delivered has matured in the course of this period; work-package and R&D reporting patterns have been established; preliminary deliverables have been completed and an overall guidance has been achieved with the appointment of an ”Advisory Board” to guide the project.

Based on internal assessment at the most recent MASSIF Executive Board meeting in September 2011, the unanimous view of the consortium is that appropriate progress has been made against what was planned. In terms of project outputs, the committed deliverables have been completed and there has also been a strong drive to connect with other European Union and security domain initiatives, to ensure that there is a sharing (and testing) of results amongst peer researchers, and also that latest and emerging trends are also considered as the MASSIF project progresses.

The purpose of the efforts overall, and the commitment of the consortium participants, is to ensure that MASSIF results in significant outcomes which are relevant and effective in combating cyber-attacks – both in information systems (as per the MASSIF scenarios on mobile payments, Olympic games infrastructure and managed security services deployment) and cyber-physical systems (as per deployment in respect of the MASSIF scenario of a dam with control valves etc). Based on the efforts to date, there is good momentum and progress to ensure that the MASSIF project can achieve this goal.

Bibliography

[1] Frances Cleary. Effectsplus 1st cluster event. Technical report, Waterford institute Of Technology, March 29th-30th 2011.

[2] Frances Cleary. Effectsplus 2nd cluster event. Technical report, Waterford institute Of Technology, July 4th-5th 2011.

[3] ISO/IEC. *Information technology - Software product evaluation - Part 1: General overview*. International Organization for Standardization, April 1999.

[4] ISO/IEC. *Software engineering - Product quality - Part 1: Quality model*. International Organization for Standardization, June 2001.

[5] Elsa Prieto. *D1.1.1 Quality Plan*. FP7-257475 MASSIF European project, December 2010.

[6] MASSIF project consortium. *MAnagement of Security information and events in Service InFrastructures - Annex 1*. FP7-257475 MASSIF European project, April 2010.

[7] MASSIF project consortium. *D2.1.1 - Scenario requirements*. FP7-257475 MASSIF European project, March 2011.

6 Appendix A

6.1 MASSIF Advisory Board

6.1.1 The Advisory Board role

The mission of the Advisory Board (AB) is to ensure that the MASSIF consortium appropriately addresses the influence of outside trends on their work. The following aspects are considered when applicable:

- Provide guidance to the project to application areas.
- Provide input and feedback to the MASSIF technology roadmap.
- Provide input and feedback to the MASSIF requirement specification.
- Provide input and feedback to the MASSIF components development.
- Provide guidance regarding ethics, privacy and compliance.
- Provide a linkage with other initiatives and groups of interest.

6.1.2 Advisory Board Membership

The Advisory Board consists of industry, academic and users stakeholders in the field of security information event management. The participation is formalized through the signature of a Letter of Interest (LoI).

Members of the Advisory Board participate on a voluntary basis. There is no contractual obligation to the consortium, but mutual interest to cooperate and exchange ideas. Nevertheless it is understood that a successful collaboration relies on active participation.

Candidates to the Advisory Board can be proposed by any partner of the consortium justifying the scope of participation and how this participation can help MASSIF to achieve its objectives. However official membership is approved by the Board of Directors of MASSIF, this is the project coordinator (Atos), the scientific coordinator (Fraunhofer), the technical coordinator (Institut Telecom, and the exploitation coordinator (Atos). The Board of Directors can also revoke this membership when the collaboration with a member is considered not satisfactory for MASSIF.

6.1.3 Participation in the Advisory Board

This participation is expected to be performed along the whole project duration (36 months, up to September 2013).

In general terms Advisory Board members will be involved in each MASSIF milestone to get regular feedback. MASSIF partners will decide by mutual consent what information will be shared.

According to MASSIF planning, the milestones will occur around the following dates:

- MS2 – September 2011
- MS3 – March 2012
- MS4 – September 2012
- MS5 – December 2012
- MS6 – March 2013

MASSIF wishes to interfere minimally with the members quotidian responsibilities. Thus the foreseen work load will be limited.

Atos, as MASSIF coordinator will manage the general communication between the Advisory Board and the consortium. All communication between MASSIF and the Advisory Board is done in English as lingua franca.

Nevertheless this participation can be intensified if there is particular interest of members on specific aspects, areas or concepts of the project. In this case, direct communication between the interested parties can take place in order to prevent formalities that could hamper the exchange of ideas.

Advisory Board members can be invited to consortium meetings and workshops. There is a limited budget for advisory board expenses that could cover fewer travels along the project lifetime, if AB members needed so. MASSIF consortium decides how to distribute this amount; therefore every request will be evaluated.

To be consistent with the principles of economy, efficiency and effectiveness required by the EC, MASSIF will cover up to 1000 euros per travel. MASSIF will try to follow a principle of equity by paying one travel per member when so required. Atos as coordinator, following its internal policies for these cases, will reimburse the payment to the advisory board member.

The activity between the Advisory Board and MASSIF consortium will be reported in public deliveries D1.2.x.