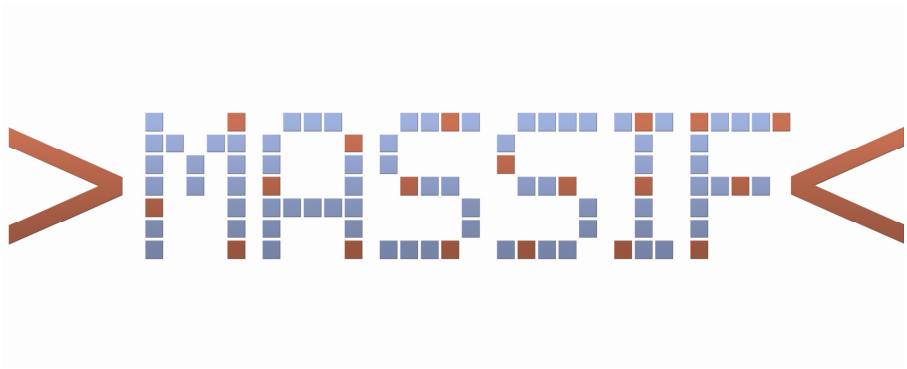
WHITE PAPER




# *Enhancing Security and Trustworthiness with Next-Generation Security Information and Event Management*

June 2012

MASSIF is a project co-funded under contract FP7-257475 of the Seventh Framework Programme of the European Union

SEVENTH FRAMEWORK PROGRAMME

## Foreword

Security Information and Event Management (SIEM) is a discipline, which many organizations include in their information security processes nowadays, and for which numerous solutions exist in the market [1] . MASSIF (*"MAnagement of Security information and events in Service InFrastructures"*) [2] is a project developing a new generation of SIEMs operate at multiple layers and offer reliability and flexibility features not found today in commercial SIEMs.

This document is divided into four parts discussing the problem statement, the basic solution to the problem statement, the solution offered by MASSIF, the market opportunities for MASSIF and finally the conclusions.

For disambiguation, any Security term appearing in the text is referred to its definition within the "Glossary of Key Information Security Terms"[3] from the National Institute of Standards Technology (NIST).

## Problem Statement

The vision of the Future Internet [4] , where multiple services are transparently and seamlessly mixed, already created a paradigm which promises to greatly 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 the essential product which deserves to be protected, in the Internet of Things however, real and virtual Cyber-physical resources deserve our attention.

> *"It seems unarguable that the key challenge facing modern ICT is the management of a transition from systems comprising many relatively isolated, small-scale elements to large-scale, massively interconnected systems that are physically distributed yet must remain secure, robust, and efficient." [5]*

In spite of the fact that technical security solutions are deployed, there are numerous instances of processes or transactions being compromised. It is sometimes said that "what you cannot measure, you cannot manage". Cyber Security is an area of great global focus, yet it is both hard to manage and arguably even harder to measure. In order to provide high-level situational security awareness, a next-generation Security Information and Event Management environment is thus needed, which should provide an architecture for trustworthy and resilient collection of security events from source systems, processes and applications. In addition, an anticipatory impact analysis should enable us to predict the outcome of threats and mitigation strategies and thus enable proactive and dynamic response.

## The Basic Solution: the SIEM.

The management of events and incidents is one of the cornerstones for any service. Security Information and Event Management (SIEM) is a key concept to identify security threats and mitigate their malicious impact. SIEM technology provides two major functionalities: log management and compliance reporting (called also Security Information Management (SIM)); and real-time monitoring and incident management (called also Security Event Management (SEM)). Most companies require a deployment supporting both functionalities, but the priorities and required capabilities of these two functions vary.

The SIEM market [1] is maturing and very competitive, and in a broad adoption phase where several vendors can meet the requirements of a typical customer. The set of common functionalities present in most available products is quite large, even though there are often differences in the actual performance of those functionalities.

SIEMs have evolved over the last years to adapt to new challenges in IT security management and in light of new threats. Yet the current solutions show some constraints. We mention the following:

- Inability to interpret data from the higher layers such as service view or the business impact view.

- Dependency on centralized correlation rules processed on a single node, making scalability difficult, creating bottlenecks and single points of failure.
- Incapability of providing a high degree of trustworthiness or resilience in event collection, dissemination and processing, thus becoming susceptible to attacks on the SIEM systems themselves.
- Inability to encompass ICT infrastructures with global deployment, since they normally consider events from single organizations.
- Lack of reaction to identified attacks.
- Non-existent or limited security analysis capabilities.

## MASSIF

## Project Introduction

MASSIF stands for *"MAnagement of Security information and events in Service InFrastructures"*. MASSIF is a collaborative research project co-funded under the European Commission's FP7 ICT Work Programme 2009 (FP7-ICT-2009-5) [6] . It is aligned with the objective ICT-5-1.4 - Trustworthy ICT.

The MASSIF Consortium, led by Atos, consists of twelve partners from six European countries (France, Germany, Italy, Portugal, Russia, and Spain) and South Africa. The MASSIF consortium includes all important groups needed to reach its objectives, and relevant industry partners to ensure that the results are integrated in the value creation chain. It consists of four industrial use case providers (Atos, France Telecom, T-Systems South Africa and Epsilon srl), two Open Source SIEM providers (AlienVault and 6cure), and six scientific research organizations (Consorzio Interuniversitario Nazionale per l'Informatica, Fraunhofer – SIT, Fundaçao da Faculdade de Ciencias da Universidade de Lisboa, St.Petersburg Institute for Informatics and Automation of Russian Academy of Science, Institut Mines-Télécom, and Universidad Politécnica de Madrid).

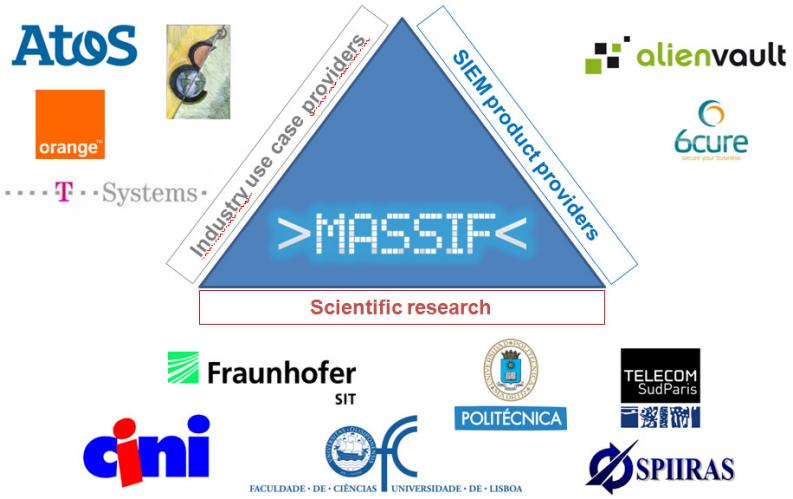



**Figure 1: MASSIF consortium**

## MASSIF solution

The main objective of MASSIF is to address the aforementioned limitations of event management solutions and to achieve a significant advance in this area. The project target is to provide a next-generation SIEM framework for service infrastructures, offering the following key features and differentiators:

- Multi-domain: Clear decoupling between the target (monitored) and SIEM (monitoring) systems, for minimal impact on the observed infrastructure, and adaptation to varying target/SIEM system combinations.
- Cross-layer correlation of security events from network and security devices and service infrastructure such as correlation of physical and logical event, and multi-level security event modelling that provides a holistic solution to protect the service infrastructures.

*MASSIF provides a next-generation SIEM offering multi-domain, cross-layer correlation, reaction capability and resilient operation.*

- Predictive security monitoring that enables proactive fighting of attacks by predicting future critical states in the monitored process.
- Reaction capabilities through countermeasures selection based on an ontology-driven approach.
- Resilient operation against faults and attacks of incremental severity, maintaining availability, integrity and confidentiality.

## Requirements-driven System Approach

In the MASSIF approach, business processes, applications and infrastructures of four industrial use cases were the starting points for analysis of the solution, resulting in a set of design and technical implementation guidelines for advanced SIEMs [7] . The understanding of MASSIF guidelines also implies meeting a set of key objectives:

- Scalable data acquisition and collection of vast amounts of events from diverse and geographically spread nodes.
- Distributed and near real-time aggregation, dissemination and processing of events.
- Scalability and elasticity of correlation, across integrated and distributed engine implementation alternatives.

*The MASSIF solution also meets other objectives such as high availability, high scalability and high elasticity.*

## Key Architectural Advantages

The MASSIF SIEM system also benefits from an architectural concept [8] based on the following points:

- A topology following the WAN-of-LANs model [9] and laid down as a logical overlay over the target system, so as to preserve legacy but allow seamless integration of the monitoring and monitored systems -- possibly across different and wide-scale administrative domains.
- Modular and adaptive structure, achieved by: (i) using modular functions and protocols, to be re-used by different instantiations of the architecture; (ii) concentrating all functions in configurable conceptual devices which act as the nodes of the overlay.

*MASSIF architectural definition benefits from a modular, adaptative and resilient structure laid down as a logical overlay over the target system*

- Information flow in the overlay implemented as a secure and real-time event bus, modelled essentially as a producer-consumer SCADA-like system upstream, with low-bandwidth commands downstream.
- Resilience improvement based on: securing the information flow; making the dissemination infrastructure itself resilient; protecting crucial processing units with incremental resilience strategies relying on hardware and software based alternatives; and differentiating between edge-side of the SIEM (at the monitored system) and its core-side configurations.

## Key Components

MASSIF is a set of technologies and tools for SIEMs delivered as a combined standalone system [8] . While the primary exploitation focus is on this system as a whole, its components or sub-modules also offer exploitable benefits in terms of products or services. Representing SIEM technology enhancements, the components contribute to the MASSIF SIEM or can be applied in standalone combinations.

## Gap Analysis and Solution Development Process

The following flow represents the approach adopted in MASSIF, consisting of seven steps:

1. Definition and characterization of the four industrial scenarios within the project:
   i) the management of the Olympic IT infrastructure,
   ii) a mobile phone based money transfer service,
   iii) managed IT outsource services for large distributed enterprises, and
   iv) an IT system supporting the control of a dam as an example of a critical infrastructure.
2. Identification of technological gaps derived from the analysis of the scenario requirements.
3. Design of the MASSIF SIEM architecture addressing those gaps.
4. Implementation of the individual components of the MASSIF SIEM complying with the identified guidelines and architecture design.
5. Integration of single components to build the MASSIF SIEM.
6. Adaptation of MASSIF SIEM to the four use case industrial scenarios.
7. Validation of the solution on the project scenarios.

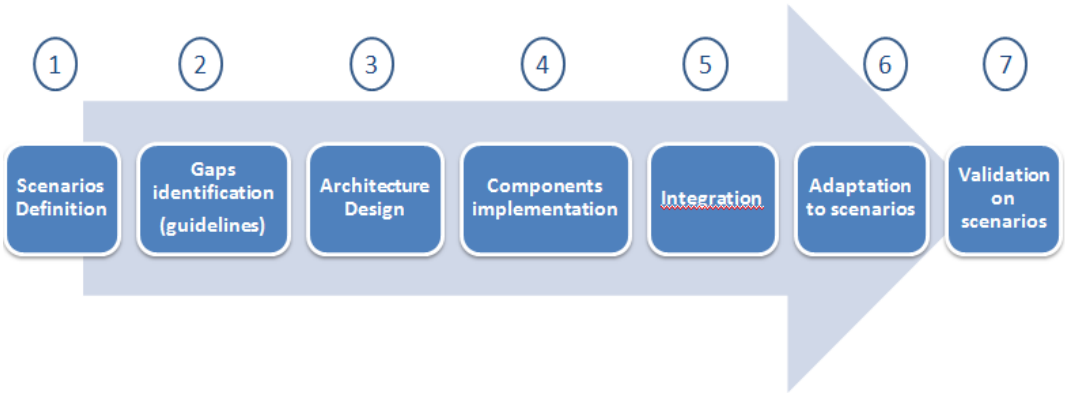



**Figure 2: MASSIF approach**

In spite of a sequential appearance, some of these steps can overlap in time owing to the needs of the project. At the time of the release of this document, the project completed the initial three stages and is entering a mature phase of components implementation, while taking the first steps towards the integration of the components and the adaptation of MASSIF SIEM to the four industrial scenarios.

Furthermore, it is expected that some MASSIF innovations and components can be integrated into the open source SIEMs, OSSIM and Prelude, contributing to the improvement of their existing versions available in the market.

## MASSIF market opportunity

In terms of exploitation actions, we differentiate between joint and individual exploitation. The joint exploitation plan is focused on an integrated system adapted to different industry sectors at the end of the project. Our goal is to provide a proof of concept solution showing how to improve significantly the current state of the art of SIEM systems. In order to demonstrate the usefulness of the generic platform on a real life case, four industrial scenarios serve as basis for the final demonstration and validation. Nevertheless the applicability of MASSIF could be extended to other likely scenarios.

The individual exploitation plans are developed by each of the consortium partners. The content and goal of these plans varies notably from partner to partner. This is not contradictory in any way, as the visions and “short vs. long term” planning are different among partners and can also evolve during the project lifetime. Furthermore, the type of organization (SME, large companies, academia or research centers) and

the complementary initiatives between partners will guide the exploitation planning of the partners in terms of market (or niche) segmentation and positioning.

In the initial MASSIF exploitation plan [1] , the consortium devised three complementary exploitation channels.

- The *business* exploitation apect, based on seeking opportunities for creating new business opportunities from the results of the project (MASSIF SIEM or MASSIF components).
- The *knowledge* exploitation aspect, related to the acquisition and transfer of new knowledge also linking with other technical or scientific communities.
- The *public* exploitation aspect, related to the citizens' benefit, even though this is considered as a very indirect channel in general terms.

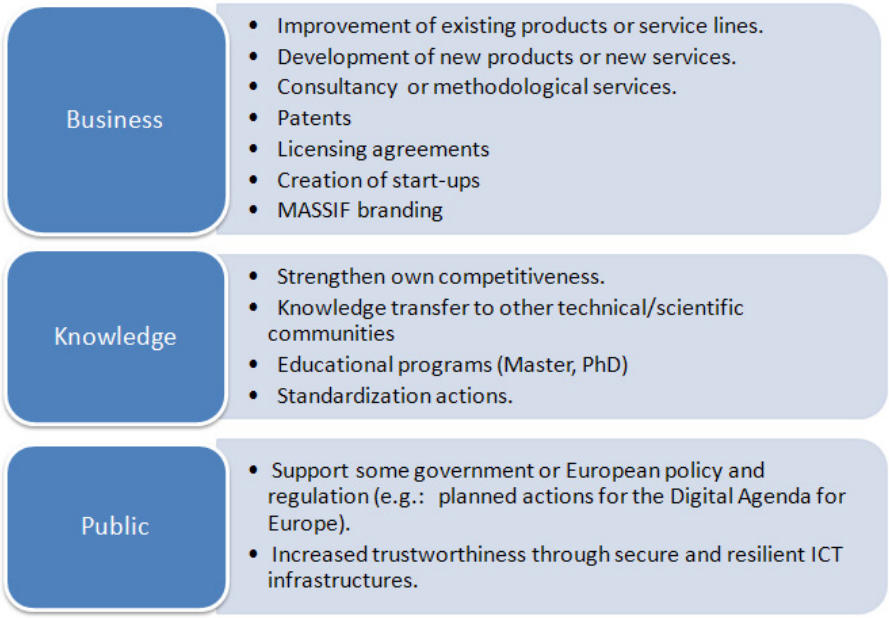



**Figure 3: MASSIF exploitation areas**

## Conclusions

SIEMs have evolved over the last years to adapt to new challenges in IT security management and in light of new threats. MASSIF is the natural evolution of such adaptation, addressing the key issues that are starting to pose the next challenges to IT security administrators and CISOs.

As it proceeds to enhance security and trustworthiness, MASSIF is set to deliver, in 2013, a next generation SIEM offering:

- Multi-domain capabilities
- Cross-layer correlation
- Predictive security monitoring
- Reaction capabilities
- Resilient operation
- Scalability
- Elasticity
- Distributed operation

Industrial commercialization of MASSIF will be available in the form of services and products from different project partners. Other exploitation channels are also possible.

## References


[1] MASSIF consortium. "D6.1.2 – Exploitation plan". September 2011.

[2] MASSIF project website. http://www.massif-project.eu

[3] National Institute of Standards Technology. *"Glossary of Key Information Security Terms"*. February 2011. http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

[4] Alvarez, F.; Cleary, F.; Daras, P.; Domingue, J.; Galis, A.; Garcia, A.; Gavras, A.; Karnourskos, S.; Krco, S.; Li, M.-S.; Lotz, V.; Müller, H.; Salvadori, E.; Sassen, A.-M.; Schaffers, H.; Stiller, B.; Tselentis, G.; Turkama, P.; Zahariadis. *"The Future Internet. Future Internet Assembly 2012: From Promises to Reality. Series: Lecture Notes in Computer Science"*. Vol. 7281,Subseries: Information Systems and Applications, incl. Internet/Web, and HCI,. (Eds.) 2012. http://www.springer.com/computer/communication+networks/book/978-3-642-30240-4

[5] S. Bullock., D. Cliff. *"Complexity and Emergent Behaviour in ICT Systems"*. October 2004. http://www.hpl.hp.com/techreports/2004/HPL-2004-187.pdf

[6] European Commission. Community Research & Development Information Service. ICT homepage. http://cordis.europa.eu/fp7/ict/home_en.html

[7] MASSIF consortium. "D2.1.1 – Scenario requirements". March 2011.

[8] MASSIF consortium. "MASSIF Architecture Document". April 2012.

[9] P. Verissimo, N. Neves, and M. Correia. "*The middleware architecture of MAFTIA: A blueprint"*. In Proceedings of the IEEE Third Survivability Workshop, pages 157–161, October 2000.

[10] Alienvault. "OSSIM, the Open Source SIEM". http://communities.alienvault.com/community

[11] Prelude. "Homepage". http://www.prelude-technologies.com/


## Glossary of Acronyms

| | |
|---|---|
| CINI | Consorzio Interuniversitario Nazionale per l'Informatica |
| CISO | Chief information security officer |
| FFCUL | Fundaçao da Faculdade de Ciencias da Universidade de Lisboa |
| FT | France Telecom |
| ICT | Information and Communication Technologies |
| IT | Institut Mines-Télécom |
| LAN | Local Area Network |
| MASSIF | MAnagement of Security information and events in Service InFrastructures |
| NIST | National Institute of Standards Technology |
| OSSIM | Open Source Security Information Management |
| SCADA | Supervisory Control And Data Acquisition |
| SIEM | Security Information Event Management |
| SP | Security Probes |
| SPIIRAS | St.Petersburg Institute for Informatics and Automation of Russian Academy of Science |
| UPM | Universidad Politécnica de Madrid |
| WAN | Wide Area Network |


***Contact Data:***

*For more information please, visit our web page: http:www.massif-eu.project*
*Or contact us at: Pedro Soria-Rodriguez, Atos. pedro.soria@atos.net*