# Challenges for Advanced Security Monitoring – The MASSIF project

Roland Rieke[1], Elsa Prieto[2], Rodrigo Diaz[2], Hervé Debar[3], Andrew Hutchison[4]

[1] Fraunhofer Institute SIT, Darmstadt, Germany
[2] Atos Research & Innovation, Spain
[3] Institut Télécom, France
[4] T-Systems, South Africa

**Abstract.** 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 at 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.*

*Research Challenges and Emerging Trends.* The vision of the Future Internet already created a paradigm which promises to largely enrich our ability to create new applications and businesses within this new environment. However, this enables new 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. *Security Information and Event Management (SIEM)* is a key concept to identify security threats and mitigate their malicious impact. A SIEM system collects and examines security related events and provides a unifying view of the monitored systems' security status. There are a number of highly regarded SIEM solutions available commercially, and most SIEM solutions have the ability to identify, collect and correlate security events from a heterogenous ICT environment including end-user devices, servers, network elements and various security appliances such as firewalls. The main constraint of current systems is the restriction of SIEM to infrastructure, and the inability to interpret events and incidents from other layers such as the service view, or the business impact view, or from a viewpoint of the service itself. Furthermore, there are a number of other constraints such as the inability of systems to consider events from multiple organisations (thus identifying security threats that are emerging from one entity but yet to affect other entities), or the ability to provide high degrees of trustworthiness or resilience in the event collection environment (thus ensuring the non-repudiation of the event source). A further issue is the scalability of current solutions, to provide comprehensive posture of the environments under consideration when considering global deployment of ICT infrastructure. Current solutions depend largely on centralised rule processing with the constraint that single nodes process the full event traffic, bounding the capacity of the system to the capacity of a single node. Here, we consider challenges for advanced SIEM systems, which are derived from the analysis of four industrial domains: (i) the management of the Olympic Games information technology infrastructure; (ii) a mobile phone based money transfer service, facing high-level threats such as money laundering; (iii) managed IT outsource services for large distributed enterprises; and (iv) an IT system supporting a critical infrastructure (dam). The project MASSIF (http://www.massif-project.eu/), a large-scale integrating project co-funded by the European Commission, addresses these challenges. The vision of creating a next-generation SIEM environment drives the development of an architecture which provides for trustworthy and resilient collection of security events from source systems, processes and applications.

*Approach & Key Results.* MASSIF combines a wide set of innovations in different areas to progress beyond the state of the art in SIEM technology. *Cross-layer correlation* of security events from network and security devices and service infrastructure, and multi-level security event modelling will provide a holistic solution to protect the service infrastructures of the Future Internet. *Predictive security monitoring* will enable to fight attacks proactively by predicting their future actions. The SIEM infrastructure will be protected against accidental (e.g. node crashes) and malicious failures (e.g. intrusions) with leading edge innovations in high availability and Byzantine fault tolerance. The former will enable to provide continuous availability of the SIEM in the face of accidental failures, by tolerating them and reintegrating failed components in an online non-disruptive manner. The latter will protect against intrusions and specific attacks to the SIEM infrastructure. The SIEM infrastructure will be holistically protected with unforgeability that will guarantee the authenticity of generated, processed and stored events, which will enable use of stored events as evidence for criminal/civil prosecution of attackers. 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, such as the MASSIF architecture develops is an important first step in this direction.

In essence though, the evolving Internet provides many new questions for SIEM deployment, and from a 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 as necessary in the Future Internet vision which we have presented here.