Contribution ID: **65** Type: **Presentation**

Log and reporting architecture for achieving compliance in distributed and multitenant infrastructures

Description of the work

Although the distributed computing models and virtualization technologies have introduced substantial benefits, the fact that both physical and software resources can be geographically distributed and shared by different users, even from different administrative domains, has heightened the common security and regulatory issues of traditional IT infrastructure. Most important initiatives on security compliance, including CSA (Cloud Securtiy Alliance) and ENISA, emphasizes the importance to certify the resource offering to the common security standards, including ISO27002, PCI-DS and audit framework such as SAS-70 II and the need to have specific audit event, log and report management mechanisms providing the evidence of adherence to the reference security and/or regulatory framework. In this presentation we will describe an architecture of a SIEM (System Information and Event Management) based, scalable and flexible system which can be deployed in a variety of distributed and virtualized infrastructure and which provides the following capabilities: collection in a secure way of audit messages from different nodes (and in different format) of the distributed infrastructure, normalization of them in a standard an common format independent from the source, application of security police over the normalized messages and (in case of events that may require corrective actions or other types of responses) generation of alert, summary of data in reports in conformity with ISO 27k, PCI-DSS and HIPAA. The proposed solution allows defining security controls and generate alerts and report on a perimeter or a per-tenant basis. These controls are mainly related to: user authentication, access to resources, attacks from unknown or untrusted sources, attacks/infections at network/host level, operations on services (suc as install, invoke, remove, terminate), system corruption and hardware failure, access to sensitive data, geolocalization of data, data retention/transfer/deletion.

Wider impact of this work

The presentation delves into what has been traditionally an IT problem and which has been exacerbated in the area of distributed and virtualized infrastructure in a real-life business, that is the compliance to regulations and security certification standards.
In this context, the proposed and standard based solution provides key capabilities for the security management in this type of infrastructure, while accomplishing the most important requirements of scalability, failover and high-performance.
Adopting such a solution may help to overcome one of the most difficult barrier for organizations considering moving to a distributed and virtualized infrastructure.

Printable Summary

Addressing compliance to security certification standards such as ISO27002, PCI-DSS and to EU directives on data privacy is more and more revealing to be a key factor in the adoption of distributed and virtualized computing model in the real-life business. In this context, logging, monitoring, auditing and reporting practices, while transcending the compliance regimes, represent the primary instrument of assurance for security manager and auditors that compliance objectives are being met or, if not fully met, then progressively improved.
The aim of this presentation is to provide an overview of impelling requirements coming from most common security certification standards and regulation, and then to present an architecture of a logging and reporting component that aim at supporting infrastructure providers to achieve compliance objectives.

Primary author: Mrs BONELLI, Lucia (Engineering Ingegneria Informatica spa)

Co-authors: Mr MANIERI, Andrea (Engineering Ingegneria Informatica spa); Mr IMMEDIATA, Angelo (Engineering Ingegneria Informatica spa); Mr LUZZI, Antonio (Engineering Ingegneria Informatica spa); Mrs GIUDICIANNI, Luisa (Engineering Ingegneria Informatica spa)

Presenter: Mrs BONELLI, Lucia (Engineering Ingegneria Informatica spa)

Track Classification: Virtualised Resources: challenges and opportunities (Michel Drescher: track leader)