Security Monitoring in the Cloud: An SLA-Based Approach

3 Author(s)

Valentina Casola ; Alessandra De Benedictis ; Massimiliano Rak

View All Authors

Abstract:
In this paper we present a monitoring architecture that is automatically configured and activated based on a signed Security SLA. Such monitoring architecture integrates different security-related monitoring tools (either developed ad-hoc or already available as open-source or commercial products) to collect measurements related to specific metrics associated with the set of security Service Level Objectives (SLOs) that have been specified in the Security SLA. To demonstrate our approach, we discuss a case study related to detection and management of vulnerabilities and illustrate the integration of the popular open source monitoring system Open VAS into our monitoring architecture. We show how the system is configured and activated by means of available Cloud automation technologies and provide a concrete example of related SLOs and metrics.

Published in: Availability, Reliability and Security (ARES), 2015 10th International Conference on

Date of Conference: 24-27 Aug. 2015

INSPEC Accession Number: 15539352

Date Added to IEEE *Xplore*: 19 October 2015

DOI: 10.1109/ARES.2015.74

ISBN Information:

Publisher: IEEE

Keywords

IEEE Keywords
Monitoring, Security, Computer architecture, Measurement, Servers, Automation, Protocols

INSPEC: Controlled Indexing
system monitoring, cloud computing, contracts, public domain software, security of data

INSPEC: Non-Controlled Indexing
cloud automation technologies, security monitoring, SLA-based approach, monitoring architecture, signed security SLA, security-related monitoring tools, open-source products, security service level objectives, SLO, vulnerability management, open source monitoring system, OpenVAS

Author Keywords
Security Service Level Agreements, Cloud security monitoring, vulnerability monitoring, Open VAS

Authors

Valentina Casola
Dipt. di Ing. Elettr. e Tecnol. dell'Inf., Univ. of Napoli Federico II, Napoli, Italy

Dipt. di Ing. Elettr. e Tecnol. dell'Inf., Univ. of Napoli Federico II, Napol, Italy

Alessandra De Benedictis
Dipt. di Ing. Elettr. e Tecnol. dell'Inf., Univ. of Napoli Federico II, Napol, Italy

Massimiliano Rak
Dipt. di Ing. Inf., Second Univ. of Napoli, Aversa, Italy

Related Articles

Cloud Computing Security: From Single to Multi-clouds
Mohammed A. AlZain; Eric Pardede; Ben Soh; James A. Thom

Security as a Service Using an SLA-Based Approach via SPECS
Massimiliano Rak; Neeraj Suri; Jesus Luna; Dana Petcu; Valentina Casola; Umberto Villano

Insider Threats to Cloud Computing: Directions for New Research Challenges
William R Claycomb; Alex Nicoll

From system-centric to data-centric logging - Accountability, trust & security in cloud computing
Ryan K. L. Ko; Markus Kirchberg; Bu Sung Lee

S2Logger: End-to-End Data Tracking Mechanism for Cloud Data Provenance
Chun Hui Suen; Ryan K. L. Ko; Yu Shyang Tan; Peter Jagadpramana; Bu Sung Lee

Design and Realization of Modbus Protocol Based on Embedded Linux System
Dao-gang Peng; Hao Zhang; Li Yang; Hui Li

An Autonomous Agent Based Incident Detection System for Cloud Environments
Frank Doelitzscher; Christoph Reich; Martin Knahl; Nathan Clarke

Security evaluation of open source clouds
Sasko Ristov; Marjan Gusev

Cloud computing: Survey of different utilization techniques
Uday Moghe; Prashant Lakkadwala; Durgesh Kumar Mishra

Designing SCIT architecture pattern in a Cloud-based environment
Quyen L. Nguyen; Arun Sood