International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.3, No.2, April 2014, pp. 99~108
ISSN: 2089-3337

SOCaaS: Security Operations Center as a Service for Cloud Computing Environments

Fahad F. Alruwaili*, T. Aaron Gulliver*
* Department of Electrical and Computer Engineering
University of Victoria, PO Box 1700, STN CSC
Victoria, BC V8W 2Y2, Canada
Email: fruwaili@uvic.ca, agullive@ece.uvic.ca

Article Info

Article history:

Received Feb 19th, 2014
Revised Mar 25th, 2014
Accepted Apr 10th, 2014

Keyword:

Security Operations Centre (SOC), Security Incident and Event Management (SIEM), Threats, Cloud Security Services, Service Level Agreement (SLA), Cloud Governance.

ABSTRACT

The management of information security operations is a complex task, especially in a cloud environment. The cloud service layers and multi-tenancy virtual architecture create a complex environment in which to develop and manage an information security incident management and compliance program. This paper presents a novel security operations center (SOC) framework as a service for cloud service providers and customers. The goal is to protect cloud services against new and existing attacks as well as comply with security policies and regulatory requirements. The SOCaaS design is based on multi-governance and defense in depth models and fits within the multi-tenancy cloud services. A SOCaaS provider is a trusted entity that collects event and system logs from cloud systems to ensure proactive incident management and compliance with regulations. The proposed approach provides better managed services for customers wanting to outsource their information security operations to attain reliable, transparent, and efficient cloud security and privacy.

Corresponding Author:

Fahad F. Alruwaili
Department of Electrical and Computer Engineering
University of Victoria, PO Box 1700, STN CSC
Victoria, BC V8W 2Y2, Canada
Email: fruwaili@uvic.ca

1. INTRODUCTION

Cloud computing resources are delivered on-demand as a service for customers over the internet. They can be constructed from multiple interconnected components such as virtualized hardware, operating systems, services and tools, platform components, and customizable software application [1]. This increases the complexity of cloud security services and their management. Thus, new techniques must be developed to provide efficient and reliable security for cloud computing environments [2].

When cloud computing service models were first developed, the focus was on performance, convenience, on-demand deployment, and functionality. Conversely, topics such as confidentiality, integrity and availability (CIA) were given low priority [3]. However, in [4] the authors show that there are significant costs associated with cyber attacks due to lost productivity, revenue and customer trust. In addition, a survey on the global state of information security [5] found that the financial losses, and lost intellectual property and company reputation as a result of cyber attacks can be substantial. Table 1 shows the results of a 2011 survey of 450 senior IT and business decision-makers on cloud adoption and trends by the Cloud Industry Forum (CIF) [6]. This shows that the top 4 issues in the cloud environment are data security at 64%, data privacy at 62%, and cloud availability and reliability.

Cloud services are delivered via the internet and are accessible anywhere, anytime. Thus these services are open to cyber attacks. In this paper, a security operation centre as a service (SOCaaS) is proposed for cloud service providers and customers to provide information security assurance and event management. It is based on the aggregation of events and logs from cloud security devices and systems. The infrastructure layer as a service (IaaS), platform layer as a service (PaaS), and software layer as a service (SaaS), typically have security devices deployed by the cloud provider. For example, a security device for intrusion detection and prevention can be embedded in each cloud layer [7]. It is expected that service providers will employ multiple security devices such as firewalls, identity management, proxy servers, antivirus software, encryption devices, and network analyzers. These security devices report events to the SOCaaS as the main source of data. The events are stored in a relational database for threat detection and analysis purposes. Events are gathered via SOCaaS system agents deployed in each cloud security device. The SOCaaS system aids cloud service providers in improving the reliability, performance, and accuracy of their security devices. The long term goal of SOCaaS is to support business and government organizations in migrating their application software, operating system platforms, and infrastructure to robust and secure cloud computing environments.

Table 1. Cloud Industry Forum Cloud Adoption and Trends Survey 2011 [6]

What are your most significant concerns, if any, about the adoption of cloud in your business?

Only asked of respondents who either currently use cloud or will do at some point in the future	Total	No. employees Fewer than 20	20-200	More than 200
Data security	**64%**	62%	61%	68%
Data privacy	**62%**	68%	61%	60%
Dependency upon internet access	**50%**	53%	58%	42%
Confidence in the reliability of the vendors	**38%**	32%	38%	41%
Contract lock-in	**35%**	30%	43%	30%
Cost of change/migration	**32%**	27%	35%	33%
Contractual liability for services if SLA's are missed	**31%**	16%	38%	33%
Confidence in knowing who to choose to supply service	**28%**	27%	29%	28%
Confidence in the vendors business capability	**24%**	16%	25%	26%
Confidence in the clarity of charges (ie will they be cheap on-prem)	**22%**	16%	26%	21%
Lack of business case to need cloud service	**21%**	11%	27%	22%
Base	**323**	73	112	95

The SOCaaS framework developed here is based on information security management [8], and computer security [9] models, both of which are described in detail in the next section. In addition, this framework conforms to the recommendations outlined by the Cloud Security Alliance (CSA) in category#7 [10]. CSA category#7 provides guidelines on the design and deployment of information security and event management services for cloud based networks, infrastructure and applications.

2. THE SOCaaS CONCEPT

The SOCaaS information security management model employs the best practices recommendations described below:

- *Information Security Management Model* [8]

  The SOCaaS framework is based on an information security management model where multiple system components are connected to all security devices in the cloud provider infrastructure and application domain. These devices are managed based on a predefined set of rules and policies shared with and agreed upon by the cloud customers. The SOCaaS obtains logs in the cloud provider domain, analyses, and correlates them in order to detect threats and predict uncertain events.

- *The Cloud Security Model*
  Straub [9], proposed a computer security model which is based on deterrence theory adopted from the discipline of criminology [11]. This security model has three layers. Within the SOcaaS framework, the first layer is a deterrents layer which employs policies defining acceptable and unacceptable behaviour in the cloud environment. Figure 1 shows this as the first layer on the left, with the other layers being prevention and detection of cloud abuse. The second layer prevents violations of rules and policies and cloud abuse. The third layer detects any deviations from these rules and cloud abuse through continuous monitoring and system audits. The goal is to discourage abuse of the system. Cloud abuse is defined as unauthorized and deliberate misuse of the cloud infrastructure by individuals and/or processes.

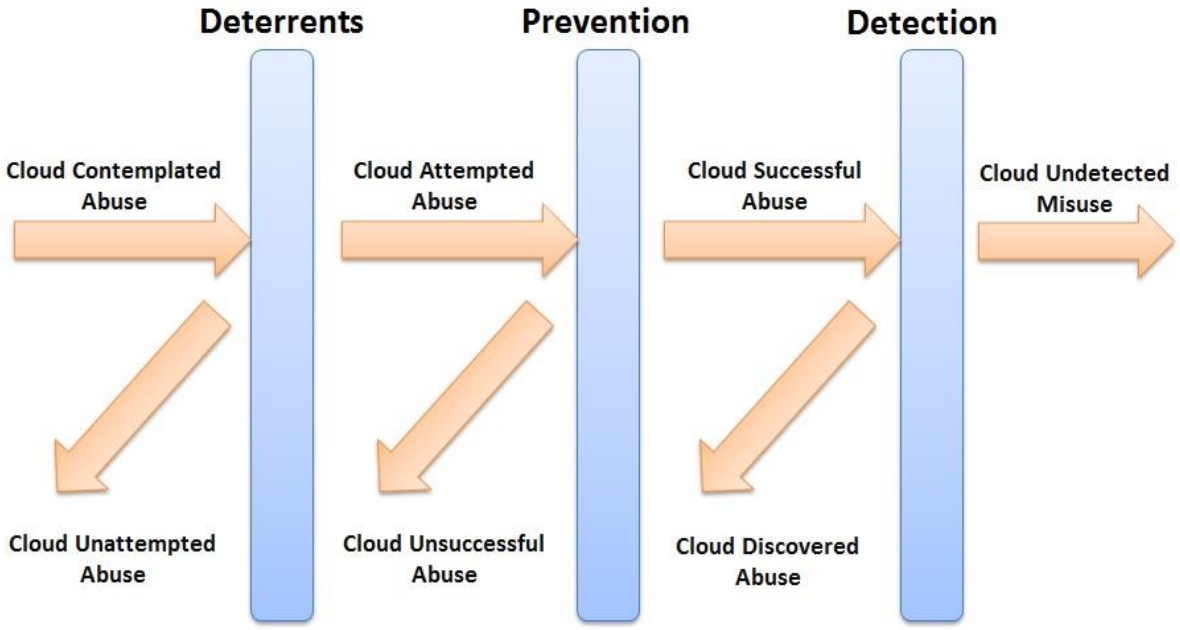

Figure 1. The cloud computer security model.

3. RELATED WORK

Establishing a security operations centre (SOC) in a cloud environment is a new approach to providing information security and event management to cloud services. The Cloud Security Alliance (CSA) [2] professionals and researchers have introduced the concept of Security-as-a-Service (SECaaS) to cloud services. They developed a set of requirements, and discussed implementation considerations and concerns. However, the recommendations provided did not specify a specific model to implement SOC in a cloud computing environment.

Probst et al. [12] suggested an automated evaluation of cloud security mechanisms and their efficiency. The focus was on evaluating access control and intrusion detection systems, which is just a part of the overall cloud risk management and assessment process. Further, their approach is limited to the cloud computing infrastructure.

In [13] the authors discussed the suitability of security-as-a-service (SaaS) for critical cloud information infrastructure services. They proposed a model to integrate traditional security solutions into a cloud infrastructure. However, their model only provides a high level description and does not provide any details of the implementation of the SOC in the cloud infrastructure or application layer.

Marty [14] presented a cloud logging framework and guidelines to provide a proactive approach to logging. This approach provides proactive information and system logging to ensure that the data needed for forensic investigation is available. While this is considered a main component of a SOC, it is limited to post event and reverse engineering analysis.

In [15], the authors introduced SECaaS using a service oriented architecture (SOA) to allow cloud customers to have more control over hosted services. A user-centric approach was employed to allow users to choose security services and monitor the status of their applications and data in the cloud environment. However, their architecture is limited to access control settings and some security settings in the chosen cloud service model (IaaS, PaaS, or SaaS).

Montesino et al. [16] reviewed security controls recommended by known standards such as ISO/IEC 27001 and NIST SP 800-35. They determined that 30% of the controls can be automated. They proposed a security information and event management (SIEM) framework to automate these security controls. They did not consider the application of their framework to the multi-layer/multi-tenancy architecture of a cloud computing environment. Further, 70% of the security controls are excluded which may leave the cloud environment vulnerable to attack.

4. OBJECTIVES

The aim of this paper is to devise a robust cloud security information and event management system. The SOCaaS is based on the aggregation of events from cloud security devices and applications. The collected events and system logs will be analyzed against an up-to-date cyber intelligence database to identify matching or relevant patterns. The SOCaaS oversights the security devices provided by cloud service suppliers. Periodic reports will be distributed to provide in depth comments and reports based on an analysis of this data, Forensic investigation should be conducted to identify threats affecting the cloud provider/customer. Note a single security device (e.g., a firewall), has limited information and thus may fail to detect and/or prevent cyber attacks. The goal here is not to expose deficiencies in the internal information security management of a cloud provider, but rather to leverage best practices in security operations and event management within the cloud community.

It is assumed that cloud service providers will allow the SOCaaS provider to deploy SOCaaS agents in their security devices for the purposes of collecting system events. It is also assumed that cloud service providers will allow the SOCaaS system to respond to an event that might require a change in a security device. The advantage for providers is an increase in public trust, service quality, and cloud service adoption. This is achieved by allowing customers to employ SOCaaS to oversee their hosted cloud services and provide real time security assurance.

5. SECURITY OPERATION CENTRE AS A SERVICE (SOCaaS)

This section first provides a definition of cloud events, the SOCaaS operational process is then disccused, and finally the proposed SOCaaS framework is described .

a. Event Definition

Cloud events can be classified into the following categories:

- *Violation of compliance policy:* detection of a violation of a defined set of rules (e.g. a user used a 128 bit encryption link instead of a 256 bit link to access a given cloud resource).
- *System configuration change:* an alert of a change in the configuration settings of cloud servers, applications, software, storage, or network components (e.g., auto-backup has been rescheduled from daily to once a week which can be a normal or unacceptable change based on the rules in the SOCaaS event database and/or the cloud security device/system).
- *Service vulnerability:* detection of a weakness in a cloud service that has been exploited to gain unauthorized access.
- *Compromised identity:* detection that personal information has been misused and/or stolen. (e.g. the credentials of a cloud user with access from a given location are used to access cloud services from a different location).
- *Data breach:* detection of a disclosure and/or data leak (spill) of sensitive, protected, or confidential cloud information by an unauthorized individual or process.
- *User Activity:* detection of user access to unauthorized virtual resources or has logged in a prohibited hours. Events can be triggered if a user exceeds his/her network or processing defined utilization permit. In addition, events can be triggered if a user tried to install unauthorized software application.
- *Attacks:* detection of a network attack such as distributed denial of service (DDoS), or web based attack such as SQL injection.

- *Malware infection:* detection of malware such as a virus, worm, or Trojan that slows cloud applications, corrupts system files, consumes cloud storage by self-replicating, or installs a backdoor for unauthorized access.

The event categories above are non-exhaustive. Detailed event definitions, categorization, and prioritization, must be developed and agreed upon by the cloud customers, service providers, and SOCaaS monitoring entity.

b. SOCaaS Operational Process

The key to an effective security operations centre is the event detection and analysis timeframe (i.e., time to detect, analyz, and repond). The faster the detection and analysis process, the better and more effective the SOCaaS system will be. The number of false positive and false negative events should also be kept low to ensure SOCaaS detection accuracy.

Figure 2 presents the timeline from event detection to response decisions, event research and analysis, and reporting. For example, the SOCaaS system detects a distributed denial of service (DDoS) attack against cloud customer 'A', which is a web server. After the initial correlation analysis, the system responds to block all active connections initiating the DDoS attack. If needed, the system can annotate the event for further investigation. Then the advanced event research and forensic analysis traces back to the origin of the attack. Finally, the corresponding patterns are used to update the system threat database, and the final report is distributed.

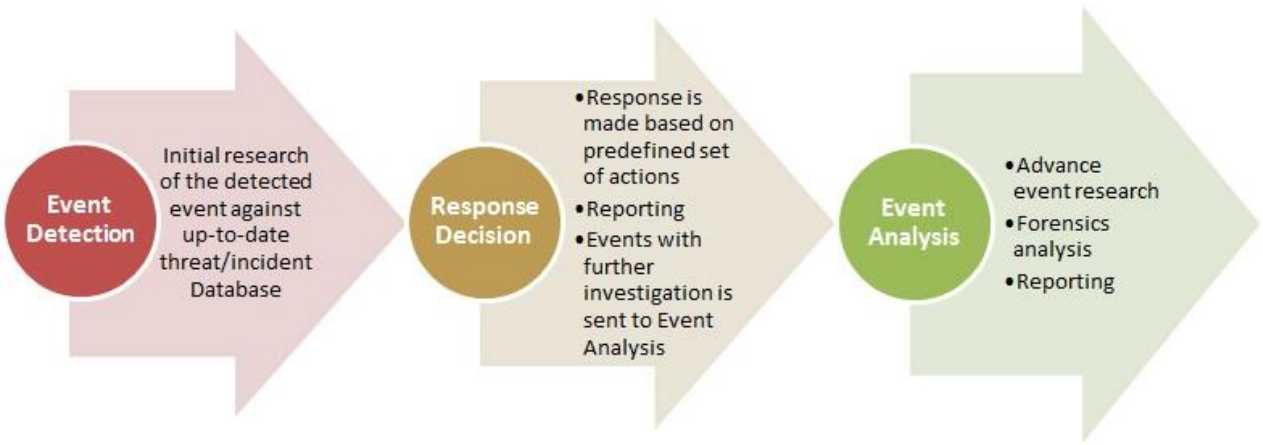

Figure 2. The SOCaaS operational process timeline.

c. SOCaaS Framework

The proposed Security Operation Centre as a Service (SOCaaS) framework is designed to provide comprehensive information security and event management for all cloud devices and applications. The correlation of all events and logs aggregated from all the security devices increases the likelihood of detecting and preventing attacks and threats compared to events and logs aggregated from one or few devices. This framework not only provides comprehensive cloud protection but also, assists in enforcing compliance and policy requirements. On demand event reports are provided for auditors from cloud service providers and customers in order to assess the process. Compliance and audit reports can also be used by external auditing agencies to verify adherence to regulatory standards and requirements, and for certification purposes. Law enforcement agencies can use these reports when events are classified as criminal (e.g., identity theft, credit card fraud, investment fraud, and phony eServices) [17].

The SOCaaS framework consists of nine modules which are described in the following sections.

i. System Agent (SA)

The system agent (SA) is a virtual application installed in-line with cloud services and/or a hardware appliance placed in front of or behind a physical server, network component, i.e., firewall, IDS/IPS, identity management, routers and switches, and storage controllers. The SA is responsible for monitoring and capturing logs (e.g., system logs, application logs, user profile and activities, security logs, and directory service logs), and sends them in real time to the system event management (SEM) module.

The SA can perform certain changes to the security device as a response to an event. Therefore, the SA must have system level privileges to manage the security devices and applications. The SA is flexible in the sense that it can be configured to filter unwanted traffic or processes. However, it is light in the sense that it has no impact on the performance and availability of the cloud security devices.

ii. System Agent Manager (SAM)

The system agent manager (SAM) is responsible for the deployment, maintenance, and discharge of SA agents in the cloud infrastructure and software. It also manages SA agent configuration settings and monitors the connectivity between an SA and SEM.

iii. System Event Managment (SEM)

The system event management (SEM) collects, correlates, and analyzes events and logs from the security devices, system and applications, and respond accordingly. The SEM has the following components:

- *Events and Logs Database (ELD):*

  The events and logs database (ELD) acts as a repository for all events and logs sent by the system agents. It is updated in real time and has a mirrored ELD backup as a contingency in case of failure.

  Events are categorized (e.g. based on defined rules), and stored in a suitable format based on a unified taxonomy. This allows analysts to easily retrieve and group events based on their category.
- *Event Correlation (EC):*

  The event correlation (EC) module is a key system component as it is used to detect events not previously noticed. It uses the information stored in the ELD to derive meaningful results. The correlation results are evaluated against an event knowledge base (EKB) to identify relationships and detect threats. For example, an event in the ELD that a cloud user attempted to log into a cloud web server more than five times could correspond to a 'brute force' login attack in EKB.
- *Event Knowledge Base (EKB):*

  The event knowledge base (EKB) is an online threat knowledge base for cloud providers and the customer infrastructure, platforms and software services. It preserves data from previous known and zero day events. The EKB is shared globally among cloud providers, antivirus vendors, and research institutions to maintain the highest level of cloud security. It contains symptoms that match certain event(s) along with the recommended countermeasures and/or responses.
- *Event Analysis (EA):*

  The event analysis (EA) module allows security analysts to perform advanced research on events. Some events need further explanation and investigation to provide additional details. Other events require long periods of time (e.g., days or weeks) before launching an attack. Therefore, advanced analysis and correlation functions can be employed to understand the source and motivation of certain event.

iv. Event Response (ER)

The event response (ER) module provides appropriate responses according to predefined rules. Typically, requests are sent automatically to the SAs to configure the cloud devices according to the recommend countermeasures. In the case of an event that needs in depth analysis, an analyst will determine the response the first time, and add this action as a response for similar events in the future.

v. Integration Agent (IA)

The integration agent (IA) ensures the operational compatibility of any legacy cloud security devices with SOCaaS system. Any security system, device, or application not integrated with the SOCaaS system does not participate in the event generation, detection, and analysis process. In fact, this can pose a threat to cloud services since any attack or compromise to that device or system will virtually be undetected. Thus, it is essential that the integration agent be used during the development process and prior to cloud customer platform migration to the cloud.

vi. Compliance and Audit Checking (CAC)

The compliance and audit checking (CAC) module regularly checks for compliance with security policies to ensure they are enforced and operational. The CAC continuously scans all security devices and reports any events deemed to be non-compliant with regulatory requirements and customer SLA agreements. For example, if a cloud customer is hosting an online payments system, it must ensure the cloud provider complies with payment card industry data security standards (PCI-DSS) [18].

vii. Security Assessment (SAss)

The security assessment (SAss) module determines what risks are inherent to which cloud assets. As part of the security assessment, vulnerability and stress assessments are conducted regularly on every cloud system or service to determine its survivability against any a malicious event. This process is done for both existing cloud services and services under development. The SAss is an automated periodic assessor. It ensures that the necessary cloud security controls are adequately integrated into each cloud service of every customer as per SLA and regulatory requirements.

viii. Physical Security Monitoring (PSM)

The physical security monitoring (PSM) module enables cloud customers to monitor their critical or sensitive information processing facilities. It enables the SOCaaS system and cloud customers to measure the readiness of the facility to an emergency event (i.e., electrical failure, communication failure, temperature and ventilation failure, fire, and floods), as per recovery requirements. The PSM is connected to the physical access controls and sensors such as motion detectors to document unauthorized individuals entering a facility.

ix. Reporting

Reporting is integrated into every SOCaaS module given above. All event reports are aggregated to the central reporting module. The correlation of these reports provides a representation of all phases of the events. It also provides event summaries with forecasts to assist management personnel in making informed decisions on future projects.

Cloud customers and service providers can be granted access to the reporting module based on contractual agreements. Law enforcement authorities can also access reports and forensic analysis if criminal activity has occurred.

Every connection between the SOCaaS system and a service provider domain is encrypted using encryption keys of a suitable length. For instance, events sent from an SA to the ELD are encrypted using a virtual private network (VPN), i.e., point to point tunnelling protocol (PPTP) and IP Security (IPSec) protocol configuration. The Traffic between the SOCaaS system and a cloud provider must be protected against unauthorized interception and attacks such as a man-in-the-middle attack which can result in the systems being compromised.

6. DISCUSSION

In this section, we discuss the advantages of the proposed SOCaaS framework and how it achieves the objectives identified in Section 4.

The proposed framework improves the ability of a cloud organization to rapidly detect, analyse, and respond to malicious events. It can also assist in ensuring cloud providers and customer cloud security event management and meet regulatory compliance requirements. This system also provides information which can aid in making informed decisions on future software, applications, and infrastructure development.

The SOCaaS system can be operated by a trusted third party to manage cloud provider security devices and appliances. The trusted SOCaaS party will possess the best practices in operating and supporting different security operation centre platforms. This provides the security assurance and transparency demanded by cloud customers. Delegating a third party to monitor and manage cloud provider security systems encourages cloud providers to increase investment in service functionality and security [19]. The SOCaaS entity operating as a business interest will invest in well trained security personnel and adopt established SOC operational and analytic procedures. These procedures will be aligned with cloud provider's and customer's business requirements. It should also establish an organizational relationship and have regular meetings with cloud service providers and customers. This facilitates productive discussions and information sharing which can aid in updating service level agreements and regulatory compliance requirements. It can also support customer software development and vulnerability assessment.

The proposed framework combines people (i.e., SOC managers, security engineers, event analysts, and security system and device administrators), SOC platforms (i.e., event management technology), processes and procedures to provide event monitoring, detection, correlation, and response to all cloud

security events. Physical surveillance is also incorporated. An important advantage of SOCaaS is that it can detect malicious events that a single information security application or one layer of security devices may fail to recognize. Monitoring of all cloud services and processes through the collection of cloud security system events and logs enables efficient and effective event analysis and response on a 24/7 basis.

The approach presented in this paper complements existing cloud security systems. Different from existing solutions, the proposed SOCaaS framework is the first to employ a multilayer security model in order that fits with the cloud multi-tangency model, i.e., the fundamental architectural aspect of cloud computing services. It incorporates all security devices in the cloud provider domain. The integration agent ensures security devices are compatible with the SOCaaS SEM module. All cloud security systems (i.e., physical and virtual security devices and applications), participate as the main sources of data for the SOCaaS system, thus ensuring cloud data assurance.

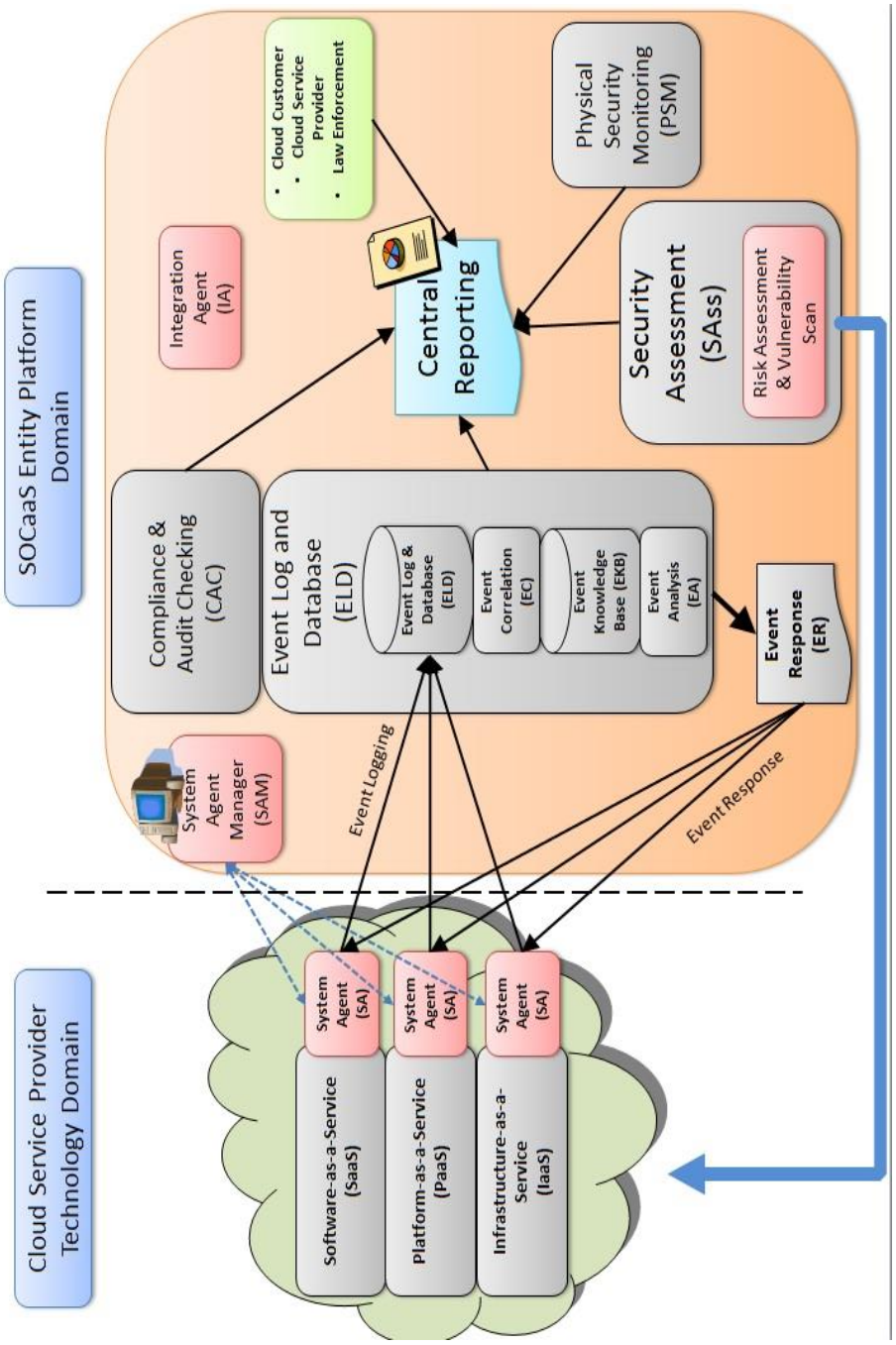

Figure 3 The System Operations Center as a Service (SOCaaS) system architecture.

7. CONCLUSION

Adopting proper cloud security information and event management (SIEM) is essential to the success of cloud service providers' and customers' information assurance. The number and sophistication of malicious events will surely increase. Therefore, it is critical that information security practitioners and researchers contribute to solving cloud information security and privacy issues [20-22].

The proposed SOCaaS framework is based on a multi-layer security model which fits the architectural complexities of a cloud environment. This framework enables trusted entities to establish a security operation centre (SOC) to monitor and manage cloud service provider security appliances, applications, and software. In accordance with cloud customer SLA, policies and regulatory requirements, the SOCaaS framework provides security assurance for critical and sensitive cloud services. It is based on the correlation of events collected from security devices with an event and threat intelligence database. This correlation along with advanced event analysis and forensics assists in detecting and protecting against threats to the cloud systems. The ongoing risk assessment to cloud assets ensures security controls are in place to withstand any external or internal threats. Detailed reporting and event summaries with are delivered to all personnel, including management, to aid in making informed decisions.

The Federal Risk and Authorization Management Program (FedRAMP) recently proposed legislation to force cloud service providers to undergo third party assessment organization (3PAO) evaluation. This is required to meet the minimal security requirements outlined by the Federal Information Security Management Act (FISMA) [23-26]. This legislation will encourage cloud service providers to invest in a secure and reliable cloud infrastructure. We predict that organizations providing security assessment and security operations will be established in the near future. The proposed framework will increase customer confidence and trust in adopting cloud services as it will reduce losses (of data, monetary, and reputation), and increase the return on information security investment (protecting cloud services against known threats and unforeseen events).

REFERENCES

[1] J. Meszaros, "Towards security management in the cloud utilizing SECaaS," *Proceedings WSEAS International Conference on Cloud Computing*, Austria, November 2012.

[2] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0," *Cloud Security Alliance*, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, 2011.

[3] S. Hiroyuki, A. Kanai, and S. Tanimoto, "A cloud trust model in a security aware cloud," *IEEE/IPSJ International Symposium on Applications and the Internet*, pp. 121-124, 2010.

[4] Symantec Corporation Technical Report "State of Enterprise Security," *Symantec Corporation*, http://www.symantec.com/content/en/us/about/presskits/SES_report_Feb2010.pdf, 2010.

[5] PWC, "Global State of Information Security Survey," *Price Waterhouse Coopers (PwC)*, http://www.pwc.com/es_CO/co/publicaciones/assets/global-state-of-information-security-survey-2011.pdf, 2011.

[6] Cloud Industry Forum, "Cloud UK: Adoption and Trends," *Cloud Industry Forum*, http://www.cloudindustryforum.org/downloads/whitepapers/cif-white-paper-1-2011-cloud-uk-adoption-and-trends.pdf, 2011.

[7] F. F. Alruwaili and T.A. Gulliver, "CCIPS: A Cooperative Intrusion Detection and Prevention Framework for Cloud Services," *International Journal of Latest Trends in Computing*, Vol. 4, No. 4, pp. 151-158, December 2013.

[8] T. Finne, "A conceptual framework for information security management," *Elsevier Computers & Security*, Vol. 17, pp. 303–307, 1998.

[9] D.W. Straub, "Deterring computer abuse: The effectiveness of deterrent countermeasures in the computer security environment," *Dissertation, Indiana University Graduate School of Business*, 1986.

[10] Security as a Service Working Group, "Defined categories of services 2011 version 1.0," *Cloud Security Alliance*, https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_7_SIEM_Implementation_Guidance.pdf, October 2011.

[11] A. Blumstein, J. Cohen, & D. Nagin, "Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates," Assembly of Behavioural and Social Sciences (US). *National Academy of Sciences Panel on Research on Deterrent and Incapacitative Effects*, Washington DC, pp. 431, 1978.

[12] T. Probst, E. Alata, M. Kaaniche, V. Nicomette, & Y. Deswarte, "An Approach for Security Evaluation and Analysis in Cloud Computing," *Safecomp*, France, September 2013.

[13] B. Niekerk, & P. Jacobs, "Cloud-based security mechanisms for critical information infrastructure protection," *IEEE International Conference on in Adaptive Science and Technology*, pp. 1-4, November 2013.

[14] R. Marty, "Cloud application logging for forensics," *ACM Symposium on Applied Computing*, pp. 178-184, March 2011.

[15] M. Hussain, & H. Abdulsalam, "SECaaS: security as a service for cloud-based applications," *ACM Conference on e-Services and e-Systems*, Kuwait, April 2011.

[16] R. Montesino, S. Fenz, & W. Baluja, "SIEM-based framework for security controls automation," *Information Management & Computer Security*, Vol. 20, No. 4, pp. 248-263. 2012.
[17] E. Casey, "Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet," *Elsevier Inc, Academic press*, 2011.
[18] Payment Card Industry (PCI), "Data Security Standard - Requirements and Security Assessment Procedures," *Payment Cards Industry Security Standards Council*, Version 1.2.1., July 2009.
[19] S. Hiroyuki, A. Kanai, and S. Tanimoto, "A cloud trust model in a security aware cloud," *IEEE/IPSJ International Symposium on Applications and the Internet*, pp. 121-124, 2010.
[20] P.S. Pawar, M. Rajarajan, S. Krishnan Nair, and A. Zisman, "Trust model for optimized cloud service," *Springer Trust Management VI IFIP Advances in Information and Communication Technology*, Berlin, Vol. 374, pp. 97-112, 2012.
[21] M.L. Kaufman, "Can public-cloud security meet its unique challenges?," *IEEE Security and Privacy*, Vol. 8, No. 4, pp. 55-57, 2010.
[22] "Top Threats to Cloud Computing. March 2010," *Cloud Security Alliance*, https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, Last viewed (10-04-2014).
[23] "Third Party Assessors (3PAO)," *The Federal Risk and Authorization Management Program (FedRAMP)*, http://cloud.cio.gov/fedramp/3pao, Last viewed (04-04-2014).
[24] M. Kozlovszky, M. Trocsik, T. Schubert, and V. Póserné, "IaaS type cloud infrastructure assessment and monitoring," *IEEE International Convention on Information and Communication Technology Electronics and Microelectronics*, pp. 249-252, 2013.
[25] "Information Security," *Federal Information Security Management Act (FISMA)*, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf. Last viewed (15-03-2014).
[26] D.E. Issa, "Federal Information Security Amendments Act of 2013'" *Library of Congress*, http://thomas.loc.gov/cgi-bin/bdquery/z?d113:h.r.1163:/. Last viewed (01-02-2014).

BIOGRAPHY OF AUTHORS

Fahad F. Alruwaili is a faculty member at computer science department at University of Shaqra, Saudi Arabia. He works as information security and computer networks consultant with over nine years of practical and administrative experience. He earned his BS degree in Computer Engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2002. In 2008, he achieved his MS degree in Computer, Information, and Network Security with first class honour from DePaul University, Chicago USA. In 2011, he received his first class honour in his second MS in Information Systems and Technology from Claremont Graduate University, Los Angeles USA. He is currently working on his Ph.D. degree in University of Victoria, the Department of Electrical and Computer Engineering, Canada. He has research interests in technical and theoretical views of cloud security and privacy.

T. Aaron Gulliver received the Ph.D. degree in Electrical Engineering from the University of Victoria, Victoria, BC, Canada in 1989. From 1989 to 1991 he was employed as a Defence Scientist at Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic positions at Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999 and is a Professor in the Department of Electrical and Computer Engineering. In 2002, he became a Fellow of the Engineering Institute of Canada, and in 2012 a Fellow of the Canadian Academy of Engineering. His research interests include security, cloud and grid computing, information theory and communication theory, algebraic coding theory, and cryptography.