Chapter 5
Security Information and Event Management Implementation Guidance

Yushi Shen
Microsoft Corporation, USA

Ling Wu
EMC² Corporation, USA

Yale Li
Microsoft Corporation, USA

Shaofeng Liu
Microsoft Corporation, USA

Qian Wen
Endronic Corp, USA

ABSTRACT

This chapter is about guidance and implementation prepared by the Cloud Security Alliance (CSA) Security as a Service (SecaaS) workgroup, which is made up of users and practitioners in the field of information security. In preparing this implementation guide, input has been sought from experts throughout Europe, the Middle East, and the United States. A lot of professional judgment and experience are applied in the architecture, engineering, and implementation of a Security Information and Event Management (SIEM) guide to ensure that it logs the information necessary to successfully increase visibility and remove ambiguity, surrounding the security events and risks that an organization faces. By providing SIEM as a service under SecaaS, the provider has to be able to accept log and event information, customer information and event feeds, and conduct information security analysis, correlation, and support incident response. By providing flexible real-time access to SIEM information, it allows the party consuming the SIEM service to identify threats acting against their environment cloud. This identification then allows for the appropriate action and response to be taken to protect or mitigate the threat. The simple step of increasing visibility and removing ambiguity is a powerful tool to understanding the information security risks that an organization is facing.

DOI: 10.4018/978-1-4666-4801-2.ch005

OVERVIEW

Purpose

This chapter provides guidance on how to evaluate, architect and deploy cloud based services providing SIEM services to both enterprise and cloud based networks, infrastructure and applications. The guidance addresses the leveraging of cloud based SIEM services in support of cloud environments, both public and private, hybrid environments and traditional non-cloud environments. While this document addresses SIEM as a cloud service, it does not preclude a hybrid environment for enterprises that have traditional SIEM deployments where the SIEM cloud service supplements.

Intended Audience and Document Organization

The target audience is primarily IT security managers, technical architects and systems managers that are responsible for monitoring and auditing their organization's infrastructure and applications. SIEM data can be used for both general monitoring, as well as security monitoring and auditing (Laundrup & Schultz, 2011). In addition to technical staff, other staff such as IT generalists, auditors and compliance managers may benefit from the understanding of higher level contents. Finally, reasonable technically aware C-level board members such as CTOs, CISOs, and CIOs can find this a useful reference, in providing an overview of cloud based SIEM services, and the areas that need to be considered, if they are to implement and consume such a service.

This chapter is arranged in such a way that the content becomes more technical in nature as the sections progress. The subsequent sections are organized as follows:

- **Requirements:** This section is intended as a high level overview of SIEM functions and implementation options. It addresses several key functionalities for which SIEM can be leveraged. The section is to also touch on less traditional deployments, which can be implemented in specific markets, where regulatory or other compliances require it. The intended audience includes executives and the senior leadership responsible for IT and security operations, compliance officers, and other decision makers within the enterprise. The material is written for executive level discussions, and indicates a baseline for best practices on the implementation and design of security services in the Cloud.
- **Architectural Implementation:** This section details the considerations and concerns that should be part of the decision-making conversation, whether by an architecture team, auditing team, or within the context of a purchase decision. The section is written for those who are implementing, integrating, or performing a technical evaluation of cloud based SIEM. This section is also well suited for auditors, to help them understand typical services and capabilities that may be implemented for cloud based SIEM deployments.
- **Technical Implementation:** This section discusses in high technical detail those items described in the previous two sections. This material is written for system architects, designers, implementers and developers, and includes guidance for the implementation of secure Cloud-based implementation of the subject.
- **References and Links:** This section contains links to trusted sources of information regarding SIEM and Security-as-a-Service, and references used in the creation of this document.

Scope

This guide covers generic (non-industry specific) implementations only at this time. While some