The 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
24-26 September 2015, Warsaw, Poland

SIEM approach for a higher level of IT security in enterprise networks

Prof. Dr. K.-O. Detken [1], T. Rix [1], Prof. Dr. C. Kleiner [2], B. Hellmann [2], L. Renners [2]
[1] DECOIT GmbH, Fahrenheitstraße 9, detken/rix@decoit.de, https://www.decoit.de
[2,3] University of Applied Sciences and Arts of Hanover, Ricklinger Stadtweg 120, D-30459 Hanover,
carsten.kleiner/bastian.hellmann/leonard.renners@hs-hannover.de, http://www.hs-hannover.de

The threat of cyber-attacks grows up, as one can see by several negative security-news from companies and private persons. [7] Especially small-and-medium-sized enterprises (SME) are in focus of external attackers because they have not implemented sufficient security strategies and components for their networks yet. Additionally, tablets, smartphones, and netbooks changed the requirements of IT security rapidly. Today, there are several security components (e.g. anti-virus-system, firewall, and intrusion detection system) available to protect enterprise networks; unfortunately, they work independently from each other – isolated. But many attacks can only be recognized if logs and events of different security components are combined and correlated with each other. This possibility is offered by a security information and event management (SIEM) system. But nowadays these systems are very complex and expensive in deployment and maintenance ([12]). The SIMU project, funded by the BMBF [6] and presented in this paper, offers several features of a SIEM system with better handling and more efficient use in the SME environment.

Keywords: SIEM, open source, IF-MAP, CBOR, IDS, network security

I. INTRODUCTION

SIEM systems are seen as an important component of company networks and IT infrastructures. These systems allow to consolidate and to evaluate messages and alerts of individual components of an IT system. At the same time messages of specialized security systems (firewall-logs, VPN gateways etc.) can be taken into account. However, practice showed that these SIEM systems are extremely complex and only operable with large personnel effort. Many times SIEM systems are installed but neglected in continuing operation.

SIEM systems are typically not suitable for the use in SME environments, mainly because of the following reasons:

a. High costs for installation and maintenance because new components (collectors) of IT infrastructure have to be installed, configured and maintained.
b. High costs for the operation due to the necessity of extensive expert knowledge for the policy and rule definition as well as for the correct analysis and the right interpretation of the output of SIEM systems.
c. Deficient scalability to small-and-medium-sized networks

Therefore the main goal of the SIMU project is the development of a system, similar to SIEM, which significantly improves IT security in a corporate network without making great effort. In addition to its simple integration into IT infrastructures of SME and its easy traceability of relevant events and processes in the network, it is to be realized without great effort of configuration, operation and maintenance. On the functional level SIMU works like common SIEM systems, which means it monitors processes and events within the corporate network and automatically detects situations of interest. It can thereby provide high-level information and even initiate proactive measures in near real-time, significantly improving security. [5]

The remainder of this paper is structured as follows. The next section II provides an introduction into SIEM systems and our understanding of SIEM. Subsequently, section 0 covers the architecture of the SIMU project. In section IV a workflow demonstration is described to clarify our approach for a SIEM-like system. The final section V gives concluding remarks and an outlook on the next steps and future lines of research.

II. SIEM DEFINITION

The term security information event management (SIEM), which has been coined by Mark Nicolett and Amrit Williams of Gartner in 2005 [4], describes the product capabilities of gathering, analyzing and presenting information from network and security devices.

Although the acronyms SIM, SEM and SIEM are often used within the same context, the term SIEM correctly is a combination of security information management (SIM) and security event management (SEM). The first area, SIM, provides long-term storage, analysis and reporting of log data. The second area, SEM, deals with real-time monitoring, correlation of events, notifications and console views. [3] Both areas can be combined differently to set-up a SIEM system.

In detail, SIEM technology thereby provides near real-time analysis of security alerts, which have been generated by network hardware and applications. SIEM can be used as software, appliance or managed service, and is also applied to log security data and generate reports for compliance purposes. The objective of SIEM is to help companies respond to attacks faster and organize mountains of log data. A key focus is to monitor and help managing user and service privileges, directory services and other system configuration changes, as well as providing log auditing and review and incident response.

A complete SIEM system consists of different modules, which have to support the following functionalities:

a. **Event correlation:** save, archive, normalize, and correlate log-files to a common data-basis for further analysis.
b. **Situation detection:** surveillance of the network condition and detection of unwanted and unexpected situations. This can include configuration management, signature based matching, or anomaly detection techniques.
c. **Identity mapping:** assigning network specific information, like IP/MAC addresses, to real identities, e.g. the actual user.
d. **Key performance indication:** measurement of the IT security by central analysis of asset details regarding security information.
e. **Compliance reporting:** continuous check on the IT compliance (e.g. integrity, risk, effectiveness) of an enterprise and comparison to the real situation.
f. **Application programming interface (API):** adaptation of legacy security systems and offering of a generic interface for the integration of arbitrary devices or systems.
g. **Role based access control:** central view of all events (big picture) of an enterprise under consideration of different responsibilities.

Not all available SIEM systems of the market cover all features equally ([12]).

III. SIEM Architecture of SIMU

The SIMU project implements architecture quite similar to typical SIEM systems. Figure 1 depicts an overview of the components, which can roughly be divided into two layers:

a. The **SIMU collectors and flow-controllers**, which are responsible for data collection and enforcement.
b. The **SIMU engine**, which includes the central data and knowledge storage, the data correlation, aggregation, and visualization of data, as well as protocol interfaces.

The communication between the layers and the components is mostly realized by using the IF-MAP protocol.

A. *SIMU-Engine*

The SIMU engine is the processing and presenting component of the architecture. It is composed as follows:

a. **irond:** The central communication point, implementing the MAP-Server as defined by the IF-MAP specification. Alternative approaches have been suggested in literature ([11]) but those imply the disadvantage of using a proprietary format instead of IF-MAP, see section B below.
b. **VisITMeta:** IF-MAP graph persistence (with respect to the history of the data) and visualization of graph data. [9]
c. **Detection Engine:** detection of relevant situations using a graph pattern matching approach on the basis of the data provided by the VisITMeta data service part.
d. **CBOR-Proxy:** RFC 7049 defines the Concise Binary Object Representation (CBOR), a data exchange protocol, which focuses on multiple design goals including small code, message size, and extensibility. In this architecture CBOR is used as an alternative to SOAP/XML, and helps to address performance problems and to facilitate the usage of IF-MAP enabling the application in small bandwidth scenarios.
e. **IO-Tool (Interconnected-asset ontology):** extends the database with further asset information of the network infrastructure to enable a correlation later on.
f. **SIMU-GUI:** graphical user front-end for the administrator. Presents analysis results and incidents as well as mechanisms for incident management, such as detailed information views or a ticketing system, in an understandable manner.

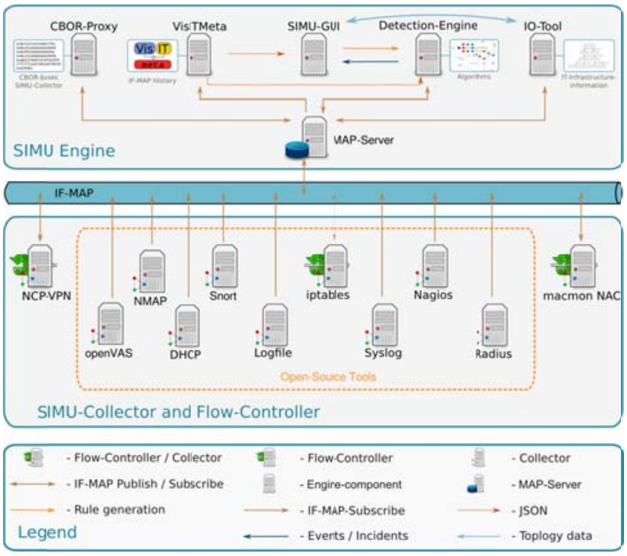


Figure 1: SIEM architecture of the SIMU project

B. *IF-MAP*

The Interface for Metadata Access Points (IF-MAP) is an open standard, client-server based protocol for sharing arbitrary information across different entities, specified by the Trusted Computing Group (TCG). Its intended purpose was to enable network devices to share sensitive security information with the goal of integrating arbitrary tools (like NAC solutions, firewalls, IDS, etc.), thus easing their configuration and extending their functionality. However, it turns out that IF-MAP can also provide benefit to other use cases that do not have anything to do with network security. That is why the TCG decided to separate the use case independent base protocol (current version 2.2[13]) from the use case dependent metadata specifications. This ensures that new metadata specifications can easily be developed without touching the base protocol spec.

The base specification defines the two roles – client and server – and three different operations: publish, search and subscribe to distribute and access information. In addition, the basic data model is defined, consisting of *identifiers* (entities) and *metadata*, which can be attached either to the identifiers directly or connect two identifiers as a kind of relationship, called *link*. Thereby, an undirected information graph originates.

The separated specification for network security [14] adds the definition of standardized metadata for the network security domain (an example graph is given later in this paper in section IV covering the workflow demonstration). Hence, IF-MAP can provide the following benefits:

- Integration of existing security systems by a standardized, interoperable network interface
- Avoidance of isolated data silos within a network infrastructure
- Extended functionality of existing security tools (for example automatic responses on detected intrusions, identity-based configuration of packet filters)
- No vendor lock-in

C. *Collector and flow controller components*

Flow controller and collectors are the typical components and services in a network infrastructure. They collect information or manage the network behavior. Several clients have been adopted to support the integration into an IF-MAP environment, i.e. providing their information in the IF-MAP data model or using information from the MAP-Server for their decisions. The following client collectors have been implemented for the architecture of SIMU (as also shown in Figure 1):

a. **DHCP collector:** extracts metadata of actual IP leases from the lease file.
b. **RADIUS collector:** delivers metadata regarding user logins and the user itself (groups, authority).
c. **Syslog collector:** delivers metadata regarding the status of arbitrary syslog clients - hosts and services (e.g. CPU load or false logins).
d. **Nagios collector:** publishes extracted metadata from Nagios regarding the status of hosts and services (i.e. availability of the network).
e. **Snort collector:** translates Snort alerts into IF-MAP metadata.
f. **Nmap:** Network Mapper integration into the IF-MAP environment. Detects devices, server, services, etc.
g. **OpenVAS:** Publication of the scan results obtained by the vulnerability scanner. Allows for periodic or regularly triggered scans and can automatically respond to requests for investigation.
h. **Log-file collector:** generic collector for analysis of arbitrary log-files and translation of the log information in IF-MAP metadata.
i. **Android collector:** delivers metadata regarding the status and behavior of the smartphone (e.g. firmware, kernel, build number, traffic on different network interfaces, CPU load).
j. **LDAP collector:** manages a connection to the directory service and delivers according IF-MAP metadata.

Furthermore, the architecture includes the following flow-controller components, which partly may also have collector functionality:

a. **iptables:** can perform automated enforcement by adapting the firewall rules and informs about operated reactions.
b. **macmon NAC:** publishes different information about connected devices in the network (e.g. authorization of well-known devices, their location in the network), and further device characteristics (e.g. operating system, ports).
c. **NCP-VPN:** delivers several relevant metadata about the VPN users, such as authorization, IP address, data throughput, and connection time. Furthermore, automated enforcement is possible on the VPN layer.
d. **OpenVPN:** alternative, SSL-based VPN solution with similar features.

IV. WORKFLOW DEMONSTRATION

The following example setup and scenario is used to clarify the collaboration of the different tools as well as to further illustrate the individual task. The network infrastructure for the demonstration scenario is shown in Figure 2. Irond is running as a central MAP-server (MAPS) and several MAP-clients (MAPC) provide information regarding the overall network state: Typical services like a RADIUS server for the network access control, a DHCP server and according lease information, or a mail-server. Additionally, security relevant components are available like a Nmap scanner and an OpenVAS client, which periodically scan the network and publish information about identified devices, services, and vulnerabilities. A snort IDS monitors the network traffic and raises critical alerts.

The gathered information is persisted by the data service component of VisITMeta. The connected detection engine uses this information to analyze the network situation and detects malicious conditions. The found incidents are communicated towards the SIMU-GUI, which presents a general overview regarding the incidents and the network situation. More detailed information can be displayed, i.e. on the basis of the VisITMeta visualization of the MAP graph itself (cf. [9]). The SIMU-GUI additionally manages the incidents raised by the detection engine in form of a ticketing system paving the way for further handling. Previously presented visualization tools (e.g. [10]) are too complex for the less skilled operators in SME and also lack the integration of a ticketing system to further simplify the security incident management workflow for a SME.

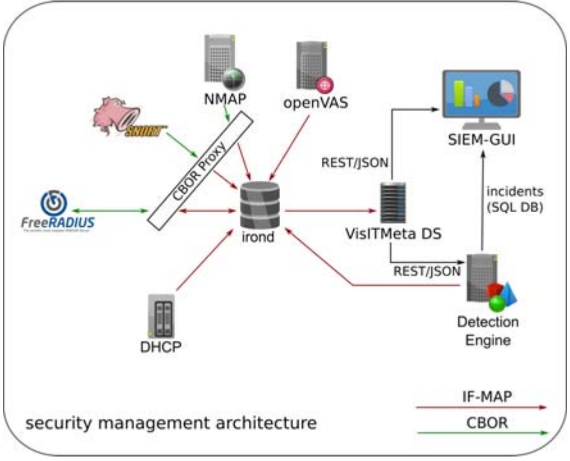


Figure 2: Management architecture of the demonstration

The communication of some MAP-clients has been realized using the CBOR-Proxy to take advantage of the more compact data representation – it does not affect the fulfilled tasks.

Subsequently, the individual demonstration steps will be described and Figure 3 illustrates the resulting IF-MAP graph. The initial situation is as follows:

- The RADIUS server manages the network access based on its configuration and the company policy.
- The detection engine is equipped with rules that detect malicious patterns, e.g. brute force login attacks or Snort alerts in correlation with vulnerable targets.

The SIMU-GUI is used by an administrator to monitor the network status and react on incidents. The demonstration itself consists of the following activities:

1. The Nmap client identifies a running SSH server.
2. OpenVAS detects a vulnerability in the version of the SSH server.
3. Later, an employee is authenticating successfully at the RADIUS server and gains access to the company network.
4. Snort monitors network traffic and detect attack patterns from the authenticated client's IP address.
5. The detection engine correlates the detected attack with the information that the server is actually vulnerable to these kinds of attacks (provided by the vulnerability scanner).
6. A resulting incident is created due to correlation and communicated towards the SIMU-GUI.
7. Due to its severity (a service that is actually vulnerable to the specific attack), the detection engine additionally creates metadata about the incident to enable automated enforcement, preventing further harm.
8. The RADIUS server consumes the metadata and consequently blocks the user access. A report about the enforced action is published.
9. The administrator sees the (high-level) alert reporting and can react appropriately. The provided and attached information (exactly which metadata led to the alert creation) allow for a targeted analysis.
10. After the incident has been handled appropriately, the client can be reintegrated into the company network and the employee can follow his regular work.

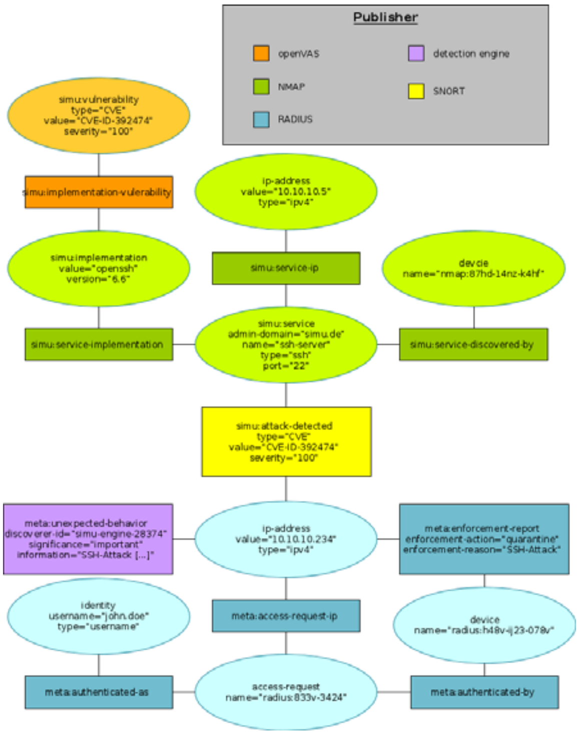
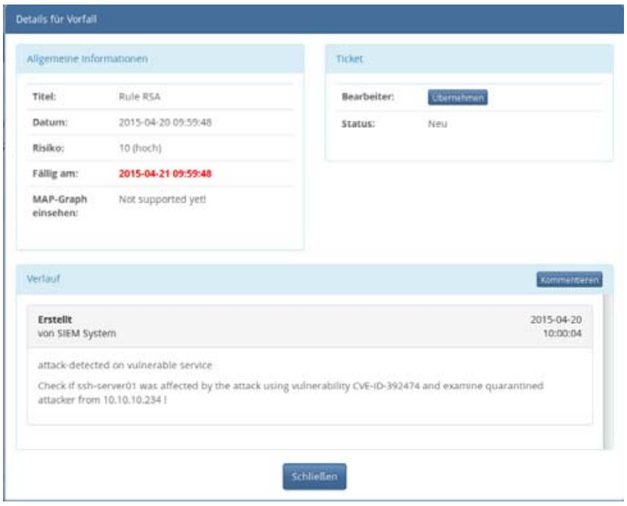


Figure 3: IF-MAP graph of the workflow demonstration

The administrator's viewpoint is further highlighted in Figure 4, which shows an excerpt of the information provided by the SIMU-GUI. In particular, the detailed report of the generated incident is displayed.

The incident describes the detected situation and the recommendation informs the user of already performed steps (i.e. the request for an automated enforcement) and proposes next steps along with further information about the specific situation.


Details für Vorfall

Allgemeine Informationen

Titel: Rule RSA

Datum: 2015-04-20 09:59:48

Risiko: 10 (hoch)

Fällig am: 2015-04-21 09:59:48

MAP-Graph einsehen: Not supported yet!

Ticket

Bearbeiter:

Status: Neu

Verlauf

Erstellt
von SIEM System
2015-04-20
10:00:04

attack-detected on vulnerable service

Check if ssh-server01 was affected by the attack using vulnerability CVE-ID-392474 and examine quarantined attacker from 10.10.10.234 !

Figure 4: Incident report of the SIMU-GUI

The administrator is thereby enabled to properly investigate and perform actions. The SIMU-GUI can be further used to assist the administrator to track his movements and time spent applying the integrated ticketing functionality. The gathered information can be used for later assessment of the incident as well as the response.

This demonstration shows how different open source tools can be used to build a SIEM-like system that detects and treats anomalous and malicious behavior in near real-time. Different, heterogeneous data sources allow for complex and precise situation definition and the user-friendly GUI enables easier security management.

The (optional) extension, CBOR proxy, allows the deployment in environments with bandwidth or resource limited scenarios. It also shows how open source tools, developed by different vendors, collaborate by leveraging TCG technologies, especially the IF-MAP protocol.

V. Conclusions

SIEM systems are complex solutions and consist of different modules, security components, and interfaces. Thus, high installation and service efforts are associated with the use of such systems. As a consequence, these kinds of systems are still not used in small-and-medium-sized enterprises (SME). The developed system in the SIMU project focusses on the SME scenario and targets an easier implementation strategy.

The use of the IF-MAP protocol enables an integration of different information from multiple security components on the same data format. Already implemented clients and open architecture facilitate the inclusion of typical networking devices and services, reducing the management and investment efforts. This is further supported by the general focus on open-source solutions.

The data collection in one common data format allows easily performed correlations to detect malicious behavior and undesirable situations. Additionally, the SIMU system enables automatic reactions, e.g. alerts or enforcements, to prevent attacks in the enterprise infrastructure.

Eventually, the complete system thereby improves security management, especially in SME environments.

Acknowledgment

The authors give thanks to the BMBF [6] for the financial support as well as all other partners involved into the research project SIMU for their great collaboration. The project consists of the industrial partners DECOIT GmbH, NCP engineering GmbH, macmon secure gmbh, and the research partners Fraunhofer SIT, and University of Applied Sciences and Arts of Hanover.

References

[1] K.-O. Detken, T. Rossow, R. Steuerwald: *SIEM-Ansätze zur Erhöhung der IT-Sicherheit auf Basis von IF-MAP*. D.A.CH Security 2014: Bestandsaufnahme, Konzepte, Anwendungen und Perspektiven, ISBN 978-3-00-046463-8, Hrsg. Peter Schartner u. Peter Lipp, syssec-Verlag, Graz (Österreich) 2014

[2] K.-O. Detken, J. v. Helden, B. Hellmann, T. Rossow, R. Steuerwald, A. Steffen, D. Dunekacke: *Near Real-time Security with Open Source Tools*. IF-MAP scenario demonstration on the RSA conference in San Francisco with the partners DECOIT GmbH, University of Applied Sciences in Rapperswil and University of Applied Sciences and Arts in Hanover, 24.-28. February, Moscone Center, USA 2014

[3] Amir Jamil: *The difference between SEM, SIM and SIEM*. Blog, 29th July 2009

[4] Amrit Williams: *The Future of SIEM – The market will begin to diverge*. Blog, 1st January 2007

[5] SIMU project website: *http://www.simu-project.de*. Last request on 11th February 2015

[6] Federal Ministry of Education and Research: *http://www.bmbf.de/en/index.php*

[7] M. Shahd, M. Fliehe: *Fast ein Drittel der Unternehmen verzeichnen Cyberangriffe*. BITKOM-Pressemitteilung vom 11. März 2014, CeBIT, Hannover 2014

[8] H. Birkholz, I. Sieverdingbeck, K. Sohr, C. Bormann: *IO: An interconnected asset ontology in support of risk management processes*. IEEE Seventh International Conference on Availability, Reliability and Security, Page 534-541, 2012

[9] V. Ahlers, F. Heine, B. Hellmann, C. Kleiner, L. Renners, T. Rossow, R. Steuerwald: *Replicable security monitoring: Visualizing time-variant graphs of network metadata*. Joint Proceedings of the 4th Int. Workshop on Euler Diagrams (ED 2014) and the 1st Int. Workshop on Graph Visualization in Practice (GViP 2014), edts.. Jim Burton, Gem Stapleton u. Karsten Klein, number 1244 in CEUR Workshop Proceedings, p. 32-41, Melbourne, 2014

[10] E. Novikova, I. Kotenko: *Analytical Visualization Techniques for Security Information and Event Management*. 21st Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), 2013, IEEE Computer Society, p. 519-525

[11] I. Kotenko, O. Polubelova, I. Saenko: *The Ontological Approach for SIEM Data Repository Implementation*. 2012 IEEE International Conference on Green Computing and Communications (GreenCom), IEEE Computer Society, p. 761-766

[12] K. Kavanagh, M. Nikolett, O. Rochford: *Gartner Magic Quadrant for Security Information and Event Management*, 2014

[13] http://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_specification

[14] http://www.trustedcomputinggroup.org/resources/tnc_ifmap_metadata_for_network_security