Research Paper Management

Security Information and Event Management

Eva Kostrecová

Helena Bínová

ABSTRACT

The importance of IT security grows year by year. Cyber-attacks are getting more sophisticated, less detectable and our only option is to make the defense stronger and stronger. These attacks are executed from various places in the world and the nature of the Internet itself predicts their global impact. To be successful in detection of such attacks, we need to utilize every possible source of information. The useful source of information is represented by log files that are generated by every major application, service or component of system. For analysis and management of these log files we can use much kind of tools. One of them - Security Information and Event Management (SIEM) - is the subject of this contribution. SIEM is an inseparable part of every information system, which contains sensitive (client) data and can provide one layer of defense, for example zero-day threat detection and immediate alerting. These abilities are inseparable part of every modern security system.

KEYWORDS Information Security, Log Files Management, Security Monitoring

INTRODUCTION

The first thing we need to know is what Security Information and Event Management (SIEM) is? In general, security information and event management is a combination of the formerly disparate product categories of SIM (security information management) and SEM (security event management). SIEM technology provides real-time analysis of security alerts generated by network, hardware and applications. SIEM solutions come as software, appliances or managed services, and are also used to log security data and generate reports for not only compliance purposes but also for detecting a potential threat.

1.SIEM definition

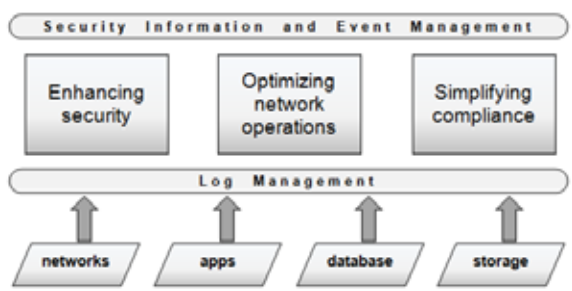
The term Security Information Event Management, coined by Mark Nicolett and Amrit Williams in 2005 describes the product capabilities of gathering, analyzing and presenting information from:

- network and security devices;
- identity and access management applications;
- vulnerability management and policy compliance tools;
- operating system;
- database and application logs;
- external threat data.

A key focus is to monitor and help manage user and service privileges, directory services and other system configuration changes as well as providing log auditing and review and incident response.[1]

We can see visualization of main activities and resources for SIEM in figure 1.

Fig. 1.Main activities and resources for SIEM



Source: authors

It is evident from the picture that log management is crucial part of the SIEM system. Without complete logs from various systems we are not able to fully understand the characteristics and behavior of some special or potentially dangerous event.

2 SIEM capabilities

Let's have a closer look at the main capabilities of SIEM solutions:

- ***Data aggregation:*** SIEM solutions aggregate data from many sources, including network, security, servers, databases, applications, providing the ability to consolidate monitored data to help avoid missing crucial events;
- ***Correlation:*** SIEM looks for common attributes, and links events to gather into meaningful bundles. This technology provides the ability to perform a variety of correlation techniques to integrate different sources, in order to turn data into useful information;
- ***Alerting:*** SIEM provides the automated analysis of correlated events and production of alerts, to notify recipients of immediate issues;
- ***Dashboards:*** SIEM tools take event data and turn it into informational charts to assist in seeing patterns, or identifying activity that is not forming a standard pattern;
- ***Compliance:*** SIEM applications can be employed to automate the gathering of compliance data, producing reports

that adapt to existing security, governance and auditing processes;

- ***Retention:*** SIEM solutions employ long-term storage of historical data to facilitate correlation of data over time, and to provide the retention necessary for compliance requirements.

3 SIEM importance

Now we understand what SIEM is capable of. But why is it necessary to have it? IT environments are growing even more distributed, complex and difficult to manage, making the role of security information and event management technology more important than ever. We are going to present some reasons to use SIEM:

- The size and complexity of today's companies is growing exponentially, along with the number of IT personnel to support them. IT Operations are often split among different groups such as the network operations center, the security operations center, the server team, desktop team, etc., each with their own tools to monitor and respond to events. This makes information sharing and collaboration difficult when problems occur. A SIEM can pull data from disparate systems into a single pane of glass, allowing for efficient cross-team collaboration in extremely large companies.

- New attack vectors and vulnerabilities are discovered every day. Firewalls, intrusion detection system, intrusion prevention system and anti-virus solutions all look for malicious activity at various points within the IT infrastructure, from the perimeter to endpoints. However, many of these solutions are not equipped to detect zero-day attacks. A SIEM can detect activity associated with an attack rather than the attack itself.

- A forensics investigation can be a long, drawn-out process. Not only must a forensics analyst interpret log data to determine what actually happened, the analyst must preserve the data in a way that makes it admissible in a court of law. By storing and protecting historical logs, and providing tools to quickly navigate and correlate the data, SIEM technologies allow for rapid, thorough and court-admissible forensics investigations. Since log data represents the digital fingerprints of all activity that occurs across IT infrastructures, it can be mined to detect security, operations and regulatory compliance problems. Consequently, SIEM technology, with its ability to automate log monitoring, correlation, pattern recognition, alerting and forensic investigations, is emerging as a central nervous system for gathering and generating IT intelligence.

- Advanced persistent threats have been in the news a lot, with many experts claiming they were responsible for the high-profile breaches at RSA (security firm, named after the initials of its co-founders - Ron Rivest, Adi Shamir, Len Adleman), Lockheed Martin and others. An advanced persistent threat is generally defined as a sophisticated attack that targets a specific piece of data or infrastructure, using a combination of attack vectors and methods, simple or advanced, to elude detection. In response, many organizations have implemented a defense in depth strategy around their critical assets using firewalls, intrusion detection system andintrusion prevention system at the perimeter, two-factor authentication, internal firewalls, network segmentation, anti-virus, etc. All of these devices generate a huge amount of data, which is difficult to monitor. A security team cannot realistically have eight dashboards open and correlate events among several components fast enough to keep up with the packets traversing the network. SIEM technologies bring all of these controls together into a single engine, capable of continuous real-time monitoring and correlation across the breadth and depth of the company.

CONCLUSIONS

The importance of IT security grows year by year. Cyber-attacks are getting more sophisticated, less detectable and our only option is to make the defense stronger and stronger.

These attacks are executed from various places in the world and the nature of the Internet itself predicts their global impact. To be successful in detection of such attacks, we need to utilize every possible source of information. The useful source of information is represented by log files that are generated by every major application, service or component of system. SIEM can provide one layer of defense, for example zero-day threat detection and immediate alerting. These abilities are inseparable part of every modern security system, but getting the right SIEM solution for any company is not as easy as buying a new piece of hardware. Many aspects have to be considered, a lot of people involved and a quite amount of money spent. But finally, you can receive in SIEM a reliable tool to support IT security.

RNDr. Eva Kostrecová, Ph.D. is an university tutor of Forecasting and IT security at Faculty of Management, Comenius University in Bratislava, Slovakia.During hercareershe workedin managerial positionsingovernmentasdirector ofData center-a budgetary organizationof the Ministry ofFinance of the SlovakRepublic, butalsoin the internationalprivate sectorandmultinationalcorporations.She teachesInformation Securityand-Cybercrime at Faculty of Electrical Engineeringof the Slovak TechnicalUniversity inBratislava, Expert SystemsandComputing-for managers, lecturesin French,at the Faculty ofManagement at Comenius Universityin Bratislava,and Economic andTechnical toolsuseful for police practiceatthe Police AcademyinBratislava. She is the authorandco-author ofseveralprofessional publicationsfocusing oncybercrime, information securitymanagementanddata processing.

Ing. Helena Bínová, Ph.D. is an university tutor at Czech Technical University Prague. From 1979 to 2003 she was Project Manager at Keramoprojekt Praha, P.M. Konsorcium, DUFF and from 2003 she is Managing Director and Project Manager at

A.R.D. CENTRAL, s.r.o.From 2009 - to date she is Researcher & Assistant Professor, Czech Technical University in Prague, Faculty of Transportation Sciences, Head of the Intermodal Transport and Logistics Laboratory and member of the executive team of the EU project Transatlantic Dual Master's Degree Program in the frame of EU-U.S. Atlantis programme. She is the author or co-author of 3 books/university textbooks and 57 articles. She is the author or co-author of 12 research projects and grants.

REFERENCES

1. http://www.infotech.com/research/it-vendor-landscape-plus-storyboard-security-information-event-management | 2. BEJTLICH, R.: The Tao of Network Security Monitoring: beyond intrusion detection. Addison-Wesley, 2005, ISBN 0-321-24677-2 | 3. FRY, Ch. & NYSTROM, M.: Security Monitoring. O'Reilly Media Inc., First Edition, 2009, ISBN 978-0-596-51816-5 | 4. STEDRON, B.: Forecast for Artificial Intelligence, FUTURIST (USA), March-April 2004, pp.24-25, ISSN 0016-3317 | |