

ISO/IEC JTC 1/SC 27
IT Security techniques
Secretariat: DIN (Germany)

Document type: Working Draft Text

Title: WG4_N0244_Text_2nd_WD_27044_20130827

Status: As per resolution 25 (contained in SC 27 N12740) of the 14th SC 27/WG 4 plenary meeting, held in Sophia Antipolis, France, 26 April 2013, this document is circulated for review and comment to WG 4 experts, National Bodies and liaison organizations of SC 27/WG 4.

PLEASE submit your comments on the hereby attached document via the SC 27 e-balloting website at: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27> by the due date 2013-10-17.

Secretariat's note:

This request for comments is also concurrently being circulated as WG 4 document N0244 for test purposes ONLY as part of the WG 4 Livelink trial via the Working Group Consultation application accessible at: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4>

For the test purposes the National Bodies and liaison organizations of SC 27/WG 4 are kindly invited to send their responses to the hereby attached document via the above-mentioned WG 4 Working Group Consultation application.

Any responses received are greatly appreciated and will be taken into account when assessing the trial results and preparing a report for consideration at the next SC 27 Heads of Delegation meeting in Incheon, Republic of Korea, 24th October 2013.

Date of document: 2013-08-27

Source: Editors

Expected action: COMM

Action due date: 2013-10-17

No. of pages: 1 + 1 + 15

Email of secretary: krystyna.passia@din.de

Committee URL: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

ISO/IEC JTC 1/SC 27/WG 4
Security controls and services
Secretariat: SABS (South Africa)

Replaces: N 75

Document type: Request for comments

Title: Text 2nd WD 27044 - Text for ISO/IEC 2nd WD 27044, Information technology – Security techniques – Guidelines for security information and event management (SIEM)

Status: As per resolution 25 (contained in SC 27 N12740) of the 14th SC 27/WG 4 plenary meeting, held in Sophia Antipolis, France, 26 April 2013, this document is circulated for review and comment to WG 4 experts, National Bodies and liaison organizations of SC 27/WG 4.

A Working group consultation will be created for submissions to this request. Submissions should be sent directly via the SC 27/WG 4 commenting website at <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4> before the action due date.

Please note that due to unforeseen circumstances, the results of this request for comments will not be available one month before the meeting in October 2013.

A request for review and comment will be issued in parallel by SC 27 as SC 27 N12677.

Date of document: 2013-08-27

Source: Editors

Expected action: COMM

Action due date: 2013-10-17

No. of pages: 1 + 15

Email of secretary:

Committee URL: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4>

ISO/IEC JTC 1/SC 27 N **12677**

Date: 2013-08-27

ISO/IEC WD 27044.2

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: DIN

Information technology — Security techniques — Guidelines for security information and event management (SIEM)

Élément introductif — Élément central — Élément complémentaire

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

D:\ISO\isomacroserver-prod\temp\DOCX2PDFISOTC\DOCX2PDFISOTC.Iliadmin@srvweb23_93\15850748_1.doc STD Version 2.1c2

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

[Indicate the full address, telephone number, fax number, telex number, and electronic mail address, as appropriate, of the Copyright Manager of the ISO member body responsible for the secretariat of the TC or SC within the framework of which the working document has been prepared.]

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

Page

| | |
|---|----|
| Foreword | iv |
| Introduction..... | v |
| 1 Scope | 1 |
| 2 Normative references | 1 |
| 3 Terms and definitions | 1 |
| 4 Abbreviated terms | 2 |
| 5 Overview..... | 2 |
| 5.1 Structure of this international standard | 2 |
| 5.2 Relations with the other ISO/IEC standards/guidelines | 3 |
| 5.2.1 Overview..... | 3 |
| 5.2.2 SIEM within the application of ISO/IEC 27001/27002 | 4 |
| 5.2.3 SIEM in context with ISO/IEC 27033 | 5 |
| 5.2.4 SIEM in context with ISO/IEC 27035 | 5 |
| 5.2.5 SIEM in context with ISO/IEC 27037 | 5 |
| 5.2.6 The application of ISO/IEC 27039 for SIEM | 5 |
| 5.3 SIEM elements and process | 5 |
| 5.4 Architectural concepts of SIEM systems..... | 6 |
| 5.4.1 Agent based SIEM | 6 |
| 5.4.2 Agentless SIEM..... | 6 |
| 6 SIEM functionalities | 6 |
| 6.1 Basic SIEM functionalities..... | 6 |
| 6.1.1 Information/event collection | 6 |
| 6.1.2 Information/event normalisation..... | 6 |
| 6.1.3 Information/event correlation..... | 6 |
| 6.1.4 Alerting | 7 |
| 6.2 Extended SIEM functionalities | 7 |
| 6.2.1 Information/event storage | 7 |
| 6.2.2 Analytic and investigative capabilities..... | 7 |
| 6.2.3 Provision of digital evidence..... | 7 |
| 6.3 General correlation principles | 7 |
| 6.3.1 Simple correlation | 7 |
| 6.4 Cross correlation of security events/information | 8 |
| 6.5 Cross correlation with security and non security related information/events | 8 |
| 6.6 SIEM and information security policy management..... | 8 |
| 6.7 SIEM in virtual and cloud environments | 8 |
| 6.8 Reporting..... | 9 |
| 6.9 Auditing | 9 |
| 7 SIEM Selection | 9 |
| 7.1 Selection and evaluation criteria | 9 |
| 7.2 Technical criteria | 9 |
| 7.3 Organisational criteria | 9 |
| 8 Implementation guidelines | 9 |
| 9 Operational Guidelines | 9 |
| Bibliography..... | 10 |

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27044 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

Introduction

[editors note: to be written in the before CD ...contributions welcome]

Information technology — Security techniques — Guidelines for security information and event management (SIEM)

1 Scope

This International Standard provides guidelines to assist organizations in preparing to deploy Security Information and Event Management Processes/Systems. In particular, it addresses the selection, deployment and operations of SIEM.

This International Standard is intended to be helpful to:

- a) An organization in satisfying the following requirements of ISO/IEC 27001:2005:

Editor's note: Before FDIS check on ISO/IEC 27001 and 27002 new releases

- The organization shall implement procedures and other controls capable of enabling prompt detection of and response to security incidents;
- The organization shall execute monitoring and review procedures and other controls to properly identify attempted and successful security breaches and incidents;

- b) An organization in implementing controls that meet the following security objectives of ISO/IEC 27002:2005:

- To detect unauthorized information processing activities;
- Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified;
- An organization should comply with all relevant legal requirements applicable to its monitoring and logging activities;
- System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model;

Editor's note: To be expanded to reflect 27033, 27035, 27039 etc. in clause 5.1.

An organization should recognize that deploying SIEM is not a sole and/or exhaustive solution to satisfy or meet the above-cited requirements. Furthermore, this International Standard is not intended as criteria for any kind of conformity assessments, e.g., Information Security Management System (ISMS) certification, IDPS services or products certification.

2 Normative references

[Editors note: To be added, if applicable, contributions welcome]

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

security information and event management

SIEM

process in which electronic data is first aggregated, sorted according to specific categories and subsequently correlated

Note to entry: The intent is to both reveal information security relevant incidents and to prioritize such information for further action.

3.2

SIEM process

To be added and updated

3.3

SIEM system

software application or appliance automating a SIEM process including collection, normalization, correlation and storage

3.4

correlation

creation of context between independent events and information previously collected near real time and normalized in superordinated categories

3.5

Intrusion Detection and Prevention System

IDPS

an Intrusion Detection System (IDS) and an Intrusion Prevention Systems (IPS) are software applications or appliances that monitor systems for malicious activities. An IDS focuses only on alerting on the discovery of such activity while IPS has the potential to prevent some intrusions upon detection. A single system combining both IPS and IDS is often referred to as a Intrusion Detection and Prevention System.

[ISO27039, 2.18]

3.6 Firewall

FW

type of security barrier placed between network environments – consisting of a dedicated device or a composite of several components and techniques – through which all traffic from one network environment traverses to another, and vice versa, and only authorized traffic, as defined by the local security policy, is allowed to pass

[ISO 27033 Part1 3.2.12]

4 Abbreviated terms

SIEM security information and event management

5 Overview

5.1 Structure of this international standard

5.2 Relations with the other ISO/IEC standards/guidelines

5.2.1 Overview

This International Standard is intended to complement other standards and documents which give guidance on the investigation of, and preparation to investigate, Information Security Incidents. It is not a comprehensive guide, but lays down certain fundamental principles which are intended to ensure that tools, techniques and methods can be selected appropriately and shown to be fit for purpose should the need arise.

This International Standard also intends to inform decision-makers that need to determine the reliability of digital evidence presented to them. It is applicable to organizations needing to protect, analyze and present potential digital evidence. It is relevant to policy-making bodies that create and evaluate procedures relating to digital evidence, often as part of a larger body of evidence.

This International Standard describes part of a comprehensive investigative process, which includes, but is not limited to, the application of the following standards

ISO/IEC 27037: Guidelines for the Identification, Collection, Acquisition and Preservation of Digital Evidence.

This describes the means by which those involved in the early stages of an investigation, including initial response, can ensure that sufficient potential digital evidence is captured to allow the investigation to proceed appropriately.

ISO/IEC 27038: Specification for digital redaction.

In some circumstances material which is found during various phases of the investigation must not be disclosed. In these cases, redaction may be required.

ISO/IEC 27040: Storage security.

Security mechanisms can affect ability to investigate by introducing obfuscation mechanisms. They should be considered prior to and during the conduct of an investigation. They can also be important in ensuring that storage of evidential material during and after an investigation is adequately prepared and secured.

ISO/IEC 27041: Guidance on Assuring the Suitability and Adequacy of Investigative Methods. 29

It is important that methods and processes deployed during an investigation can be shown to be 30 appropriate. This document provides guidance on how to provide assurance that methods and processes meet the requirements of the investigation and have been appropriately tested.

ISO/IEC 27042: Guidelines for the Analysis and Interpretation of Digital Evidence. 33

This describes how methods and processes to be used during an investigation can be designed and implemented in order to allow correct evaluation of potential digital evidence, interpretation of digital evidence and effective reporting of findings.

ISO/IEC 27043: Guidance on Investigation Principles and Processes.

This defines the key common principles and processes underlying the investigation of incidents and provides a framework model for all stages of investigations.

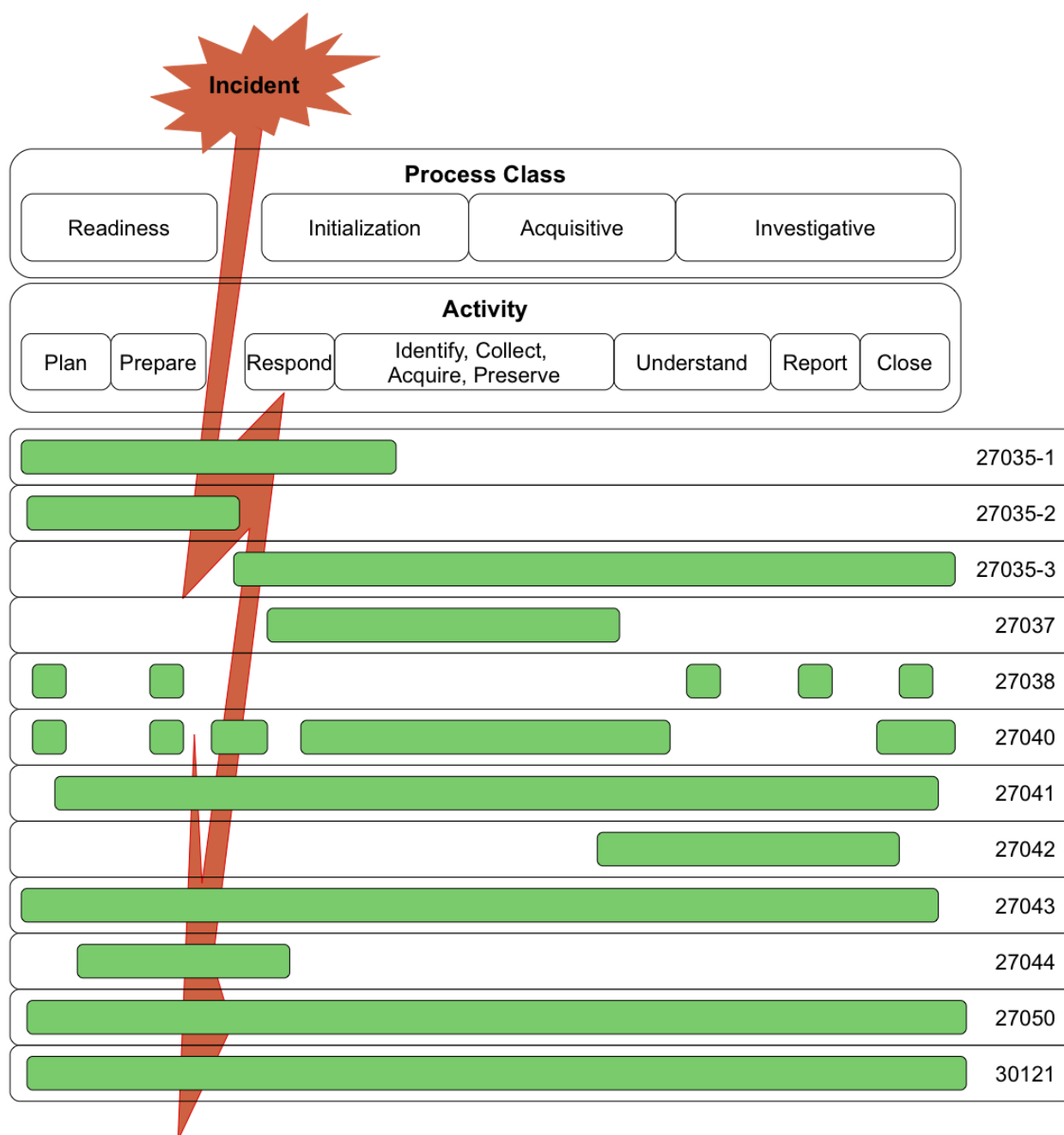


Figure 1 – Incidents and Investigations

The standards listed above are mapped onto this sequence, showing where each is most likely to be directly applicable. It is recommended, however, that all should be consulted prior to, and during, the planning and preparation phases.

5.2.2 SIEM within the application of ISO/IEC 27001/27002

Further SIEM can be seen to support the implementation of an ISMS described in ISO/IEC 27001 and by supporting controls from ISO/IEC 27002. The following aspects are in support of ISO/IEC 27001/2:

[editors note : to be expanded, due to the expected imminent publication of the new versions of 27001/2, this section will be completed after the FDIS ballot hopefully passes]

5.2.3 SIEM in context with ISO/IEC 27033

[editors note : to be expanded, contributions welcome]

5.2.4 SIEM in context with ISO/IEC 27035

[editors note : to be expanded, contributions welcome]

5.2.5 SIEM in context with ISO/IEC 27037

[editors note : to be expanded, contributions welcome]

5.2.6 The application of ISO/IEC 27039 for SIEM

ISO/IEC 27039 defines guidelines for the selection, deployment and operation of Intrusion Detection and Prevention Systems.

SIEM not only allows to correlate IDPS data, such as source IP, destination IP, event name, timestamp etc. with other risk assessment data such as, vulnerability assessment data, to allow for more accurate alerting and reduction of false positive alerts.

By means of (cross) correlation SIEM is also often able to detect security breaches, especially if those are not pattern related, but e.g. can be deducted from behavioural abnormalities or creating context between independent events/information.

In this context SIEM can greatly aid in defining more granular alarms than a pure IDPS as well as adding further visibility and monitoring capabilities.

5.3 SIEM elements and process

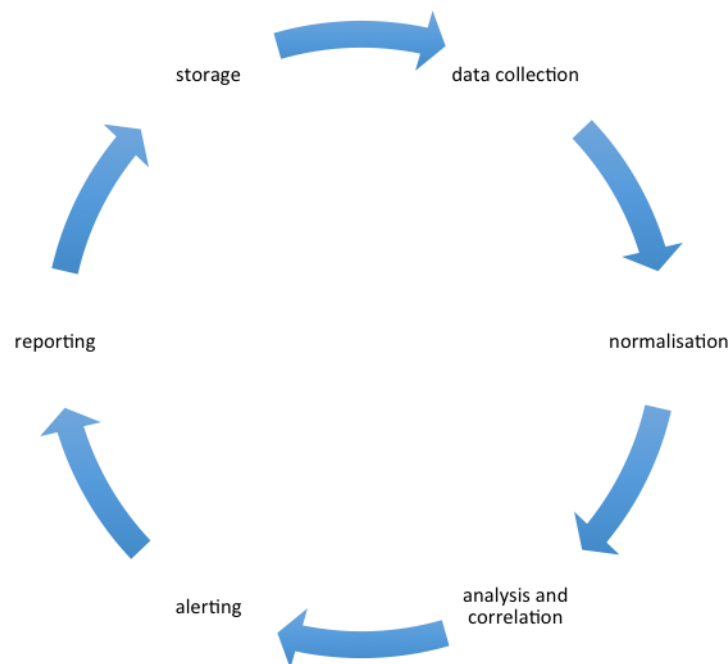


Figure 2 - SIEM elements/processes

Figure 2 illustrates the relationship of the individual SIEM elements/processes the execution order.

5.4 Architectural concepts of SIEM systems

There exist various distinct concepts for the implementation of SIEM. These are illustrated in the diagram in

Figure 3 - Architectural concepts of SIEM systems

5.4.1 Agent based SIEM

Some SIEM systems, especially older ones, require the deployment of a software agent to collect data from server and applications and any non syslog data source.

While agent based SIEM has grown to be largely unpopular due to the added effort and possible performance issues they create, they have the advantage that they additionally allow security and information data to be filtered prior to being transmitted at the source. This is useful in environments with limited network bandwidth, or systems that do not permit the configuration of a push delivery or pull retrieval of the system's log files.

5.4.2 Agentless SIEM

The vast majority of modern SIEM systems are agentless, meaning that log files can be collected by a sensor and forwarded to collection without the deployment of a local agent on the respective system.

6 SIEM functionalities

6.1 Basic SIEM functionalities

6.1.1 Information/event collection

In order to perform any of the subsequent functionalities a SIEM process or tool must first aggregate all electronic records (log files) of the connected systems. The value that SIEM may provide is greatly based on the variety and completeness of the data collected. However, depending the intended use and focus of the SIEM process / tool as well as the available technical and human resource it may be advisable to exercise caution in the amount and type of data collected.

6.1.2 Information/event normalisation

As log files may be labelled differently depending both on their technical origin as well as the vendor of the application from which the log file may be collected from it is necessary to sort collected data under common categories.

For example while e.g. a firewall vendor A may label a category "event type" another may label the same category "event name", an application may merely label it "event" etc.

As the value and efficiency of subsequent correlation functions are greatly depending on speed and accuracy it is necessary to sort varying category labels into common labelled categories the SIEM process/tool will use to proceed.

6.1.3 Information/event correlation

Once normalized information and events can now be correlated according to simple, cross or advanced correlation rules.

A major part of a SIEM system implementation is the definition and customization of such correlation rules (see also section).

6.1.4 Alerting

Based on the correlation results a variety of alerts can be generated, depending on the tool not only on a SIEM management screen, but also via text message and e-mail etc.

6.2 Extended SIEM functionalities

6.2.1 Information/event storage

As outlined in section 6.1 a SIEM system will collect the raw log files from multiple connected sources and normalize the raw logs.

A SIEM system should allow for a variety of storage options for both raw logs as well as normalized logs, as it enables not only analytic and digital evidence functionalities and aid in the compliance to standards and policies requiring the preservation of log files.

6.2.2 Analytic and investigative capabilities

When organizations review and redesign security policies and processes the analysis of extended SIEM log history may be extremely helpful as such review will allow conclusions based on documented facts.

Hence a decision to e.g. address a security problem via a redesign of processes or processes, or by adding additional security measures may be significantly more precise and efficient then without the use of such information.

Modern SIEM tools offer a variety of search capabilities and trend reports to aid organizations in such efforts.

Observing local legislature it is also possible to analyse user behaviour as well as conduct detailed investigations of security breach and attack data documented in these log libraries.

6.2.3 Provision of digital evidence

As outlined above the investigation of security breaches and attack data via analysis of log files collected in a SIEM will greatly aid in identifying the exact course of such event as well as the identification of sources involved. In order to use such data as digital evidence the stored normalized logs are not sufficient but will certainly require the actual raw logs along with a irrefutable proof of chain of custody. In this context again local legislature is to be observed as described in ISO/IEC 27041. However, while SIEM systems are certainly capable to aid in the investigation it cannot be expected that these electronic records may be automatically accepted in a legal environment.

6.3 General correlation principles

The paramount functionality of any SIEM process/system is the ability to correlate the collected data according to predefined correlation rules.

In general the following correlation principles are most common.

6.3.1 Simple correlation

A simple correlation may be defined as the mere sorting of normalized data e.g. by predefined categories such as source, destination, event name, event count and time stamp etc. without the addition of further correlation parameter.

EXAMPLE The event count 4 over a timeframe of 3 minutes with the event name “failed log on” from a single source IP may just point to a user, who has forgotten his password. If the event count is 400 in the same time frame from the same source, with the same event name the probability of a brute force attack seems extremely high.

It should be noted in this context that the identification of this hypothetical brute force attack was not based on an attack pattern but via the correlation of behavioural electronic data.

6.4 Cross correlation of security events/information

The term cross correlation is defined by comparing and analysing not only via sorting normalized data, but to possibly add further parameter available both in log files defining events as well as log files from device and application residing configurations and information.

EXAMPLE An IDPS alert on a network based attack is triggered as the IDPS sensor has identified the network based attack pattern. This alert is fed into the SIEM system, which also has the log file of a vulnerability assessment of the same day, which states that the targeted destination IP is not vulnerable to this particular attack.

With this information available the possible high level alert from the IDPS may be downgraded to a mid level or even low-level alert.

6.5 Cross correlation with security and non security related information/events

Modern SIEM systems are not only capable of analyzing and correlating information and events from security tools, but essentially from any log file source and format.

This allows the advanced cross correlation of even non IT or application security system related information to analyse or even detect security breaches from events, that outside of the context would seem perfectly secure and acceptable.

EXAMPLE The log file of a physical door entry system records the legitimate departure of a user from a building, car park etc. The log file of an ERP system records the legitimate log on of the same user with proper username and password.

Both events viewed singularly will most likely not trigger any alerts from their respective logs as they are permitted and not in violation of any obvious safeguards. However, if the timestamp of the log on to the ERP is e.g. 30 minutes later than the time stamp of the physical access control system the probability of a security breach seems rather high, especially if the said ERP system may not be reachable remotely.

6.6 SIEM and information security policy management

As security policies in organizations are ideally aligned to ever changing business requirements they are prone to be regularly reviewed and adapted.

Additional factors may be changing regulatory compliance requirements as well as changing technical parameter.

Subsequent decisions can be of immense strategic and financial impact and hence tend to require an adequate amount of scrutiny and precision in planning and implementation.

With historical SIEM data already collected and at hand these objectives can be achieved swiftly and effectively.

Also in determining and monitoring compliance to a security policy or regulatory standard a SIEM process/system can be

6.7 SIEM in virtual and cloud environments

An organisation may be confronted with the objective to move to a virtualised FW system or possibly outsourcing an entire data centre.

6.8 Reporting

6.9 Auditing

7 SIEM Selection

7.1 Selection and evaluation criteria

7.2 Technical criteria

7.3 Organisational criteria

8 Implementation guidelines

One factor determining the successful implementation of a SIEM tool is the adequate allocation of storage space for both types of data.

9 Operational Guidelines

Bibliography

Log Management functionality