PREDRAG ŠKUNDRIĆ
Ibis-instruments,
Tošin bunar 272
Belgrade, Serbia,
E-mail: predrag@skundric.com

UDC 004.383.2.056.53

Original research article
Received: 15th October 2019
Accepted: 15th November 2019

VANJA KORAĆ
Mathematical Institute SASA,
Knez Mihailova 36/III,
Belgrade, Serbia,
E-mail: vanja@mi.sanu.ac.rs

ZORAN DAVIDOVAC
Mathematical Institute SASA,
Knez Mihailova 36/III,
Belgrade, Serbia,
E-mail: zorandavidovac@mi.sanu.ac.rs

# IMPLEMENTATION AND MANAGEMENT OF SECURITY INFORMATION AND EVENT MANAGEMENT TOOLS IN INFORMATION SYSTEMS THROUGH THE MSSP MODEL

## ABSTRACT

*This paper presents a solution which can be applicable to most small and medium companies having to deal with cyber threats and a lack of staff who would be in charge of the safe management of the infrastructure, whilst also delivering with acceptable costs. The aim of this paper is to create the general initial architecture of a SIEM solution, with the goal of positioning it as a MSSP system for the centralised collection and analysis of system records collected from various forms. Through a general overview of the solution, which comprehends a detailed analysis of connecting components, the management of security information and events tools in information systems is shown as a MSSP model. Additionally, the advantages and disadvantages related to the suggested solution are given.*

**KEYWORDS: MSSP, MANAGED SECURITY SERVICE PROVIDER, PROCESSING SYSTEM RECORDS, COLLECTING SYSTEM RECORDS, SIEM.**

We have been witness, in the more recent past, to various types of attacks on information systems of different organisations. When we say "different", we really mean it in the fullest sense of the word. The attacks are no longer related only to large corporations such as oil companies, water-supply systems, pharmaceutical companies, etc.; nowadays, attacks can be expected even by the smallest business entity. Regardless of their level of protection, it can be said that the common denominator of all systems is separate management consoles, which prevent not only an integrative monitoring of the system, but also a detailed analysis of the any attacks that have occurred, that is to say, a correlation of system records from a large number of systems with the goal of decreasing false positive detections. Solutions which enable all of these activities are called SIEM, which is, in fact, an acronym of the English term Security Information and Event Management. The importance of such systems can be seen from the following example: after performing an illegal activ-

ity, the perpetrator would try to cover his tracks, because traces of whatever happens on the OS are left in logs. It is possible to do a backtrace based on the logs and identify, though forensic analysis, who it was that performed the illegal activity. Considering the fact that attackers try to erase log files as well while covering their tracks, it is recommended that the logging take place on special log servers so that the attacker is unable to delete the files. This is precisely why the already mentioned SIEM (Security Information and Event Management) solutions or log management systems exist in large corporations, to collect logs, so that even if the attacker erases the logs, they have already been forwarded to the log management system. It is vital to point out that with these management systems it is extremely important to carefully configure the synchronisation of the logs with log management. If the synchronisation time is poorly defined, a malevolent attacker can take advantage of that delay and, if he makes a malicious script which deletes the logs on a local computer during the "defined synchronisation period", the log will never reach log management and the alarm will not be activated (Korać and Prlja 2018).

From this, it can be concluded that tracking system records from a single place does not represent a luxury, rather that it is, in fact, obligatory for every business system.

When it comes to achieving a safe work environment, notable efforts have been present on a global level for some time (NIST directive, GDPR, international standards ISO27001, ISO27552, etc.). Aside from the global approach, local efforts have also been made to secure a safe business framework by adopting relevant legal regulations (Law on Information Security, Law on Protection of Personal Data, etc.), as well as relevant accompanying documents (Strategy for the Development of Information Security, Decision on Minimum Information System Management Standards for Financial Institutions, etc.).

All the aforementioned legal regulations essentially represent the "transfer" of business requirements into a legal framework, which enables a heightened level of security.

This paper does not comprise an evaluation of the complete set of needs of information security in the technological sphere; the focus is, instead, on the segment concerning the implementation of SIEM solutions through MSSP models.

The solution presented here can be applicable for most small and medium companies having to deal with both cyber threats and a lack of staff who would be in charge of the safe management of the infrastructure, whilst also delivering with acceptable costs.

The aim of this paper is to create the general initial architecture of a SIEM solution, with the goal of positioning it as a MSSP system for the centralised collection and analysis of system records collected from various forms. The paper is subdivided into the following topics:

description of the MSSP and a general overview of the solution,

a detailed analysis of connecting components,

advantages and flaws of the MSSP approach.

The paper will not deal with the implementation of the necessary network resources regarding the equipment and licences needed by the provider of the hardware infrastructure nor the client for whom the monitoring of system records would be performed. The paper will show, instead, evaluations of specific SIEM solutions.

## MANAGE SECURITY SERVICE PROVIDER – DESCRIPTION

Before moving on to the actual description of the solution, it is necessary to explain the exact meaning of the term Managed Security Service Provider (MSSP). The MSSP is, in fact, a provider of IT services that enables an organisation to track and manage information security in a particular manner, which can facilitate virus and spam mail blocking, break-in detection, management of firewall devices, and virtual private network (VPN)

management. The MSSP can also manage system changes, modifications and upgrades (Rouse 2018).

An organisation can manage all aspects of its IT security functions either separately or by sending them to a MSSP. The MSSP usually provides a certain level of continuous tracking of the entire information security of an organisation/company, vulnerability risk assessment, threat notification and similar activities.

After reviewing the Serbian market, it can be concluded that the majority of companies in this area are small and medium enterprises (hereinafter: SME – Small and Medium Enterprises). The main trait, when it comes to information security, of this type of business organisation is a lack of expertise in the sense of information security, but also a lack of funds or very small sums allocated for the development of information security as a whole.

Regardless of whether a company is big or small, the initial risks in terms of business are identical. Malicious users attack organisations regardless of their size, but exclusively on the basis of the manner in which they can take advantage of the victim. If this axiom and the previous statement are combined, it can be concluded that small and medium enterprises are in a far worse position than big ones, while the attack vectors remain the same.

Upon observing the systems with SIEM, it can be fairly easily concluded that the already mentioned business entities run even greater risks than big companies.

If the needs of business entities are observed while analysing, at the same time, the challenges placed before the MSSPs by conducting empirical research, the summed up results can be seen in the following table:

| Service | On-premise | MSSP |
|---|---|---|
| Monitors system records and network communication | × | × |
| Helps achieve the necessary goals of information security | | × |
| Enables a 24x7 analysis | | × |
| Stores system records outside of the organisation seat in the safest way possible | | × |
| Provides security intelligence and expertise as part of the service | | × |
| Provides DR and BCP mechanisms as part of the service | | × |
| Provides predictable costs | | × |
| Provides flexible licensing according to the current needs of the organisation | × | |
| Requires initial infrastructure investment by the organisation | × | |
| Requires infrastructure upgrade investment | × | |
| Requires staff investment | × | |

## GENERAL SOLUTION DIAGRAM – ARCHITECTURE

The following segment will show a general solution, with a special overview of its architecture.

The application and management of tools of security information and events management (SIEM) enables MSSPs to quickly collect and review event logs, correlate events and generate alerts for familiar threat and incident patterns for managed networks.

Emphasis is placed on the technically best solution needed to cover the largest number of scenarios as well as the possibility of rapid di-

saster recovery. Also, this chapter will show the minimal configuration which can meet the minimal users' needs, although it would not provide the necessary redundancy level or quick recovery in the case of a problem.

An initial configuration is based on All-in-one IBM Security QRadar devices. So as to achieve the greatest efficiency and increased scalability, for users and also for future system expansions, the suggestion is to use a virtualisation platform. With the arrival of version 7.3.x, all the virtualisation platforms are supported, including Microsoft Hyper-V platform, i.e. KVM. As VMWare is the most widespread virtualisation platform, the said platform will be used for the creation of a solution; one should also bear in mind the fact that the said model can easily be applied on other platforms as well.

The technically superior and safest solution for the implementation of a system with wide accessibility is the implementation of the VMWare cluster platform. For this, it is necessary to provide two identical hardware servers which will be located in the virtualisation cluster.

On the mentioned severs, an installation of All-in-one (hereinafter: AiO console) consoles for IBM Security Qradar will be performed. In order to reduce initial expenses for small MSSP providers, it is suggested that every user have his own AiO console for processing system records. This way, the simplest administration per user will be enabled, with the possibility of upgrading the system and increasing capacities in accordance with the demands of the users and implemented MSSP support package.

On the location, a necessary number of system record collectors (event collectors) would be installed, as well as flow collectors.

Aside from the initial console, the IBM Security Qradar's portfolio also includes two additional modules:

IBM Security QRadar Vulnerability and Risk module, and

QNI (Forensic module).

The first module will not be taken into consideration here, because there are significantly

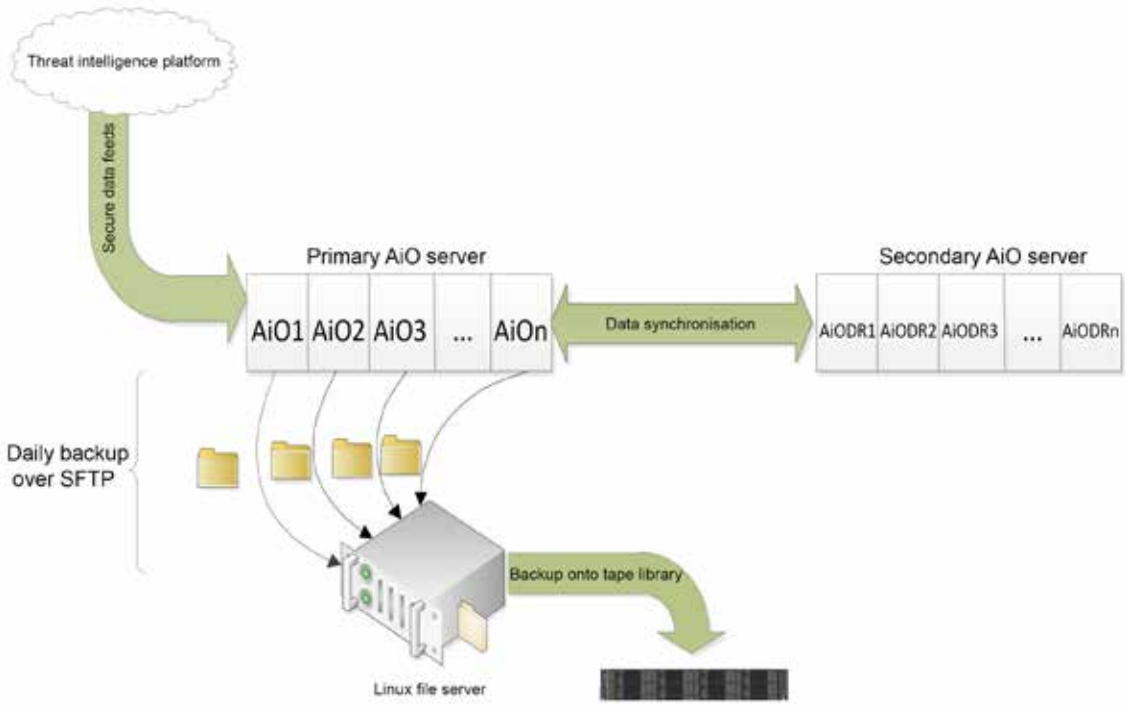


Fig. 1

less costly and probably better solutions which are exclusively intended for system vulnerability testing.

The forensic module will not be taken into consideration either, because of the high initial implementation costs (a separate physical device is needed), but also a significant increase in network traffic between the client's infrastructure and the AiO console. It would be appropriate to take into consideration both of those modules when it comes to the implementation of solutions which would be completely within the infrastructure of the user.

With the implementation of the AiO console as a threat intelligence platform, the licence also provides the IBM X-Force Security feed. Should it be necessary, there is the possibility of implementing additional security feeds, either commercially produced or open source types, which are based on STIX and TAXII communication formats or through specific API calls.

| Description | Values |
|---|---|
| Maximum capacity | 200,000 FPM<br>5,000 EPS |
| Memory | 64 GB 8x 8 GB 1600 MHz RDIMM |
| Storage | 9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 4.9 TB usable (RAID 6) |
| Dimensions | 29.5 inches deep x 17.7 inches wide x 2.4 inches high |
| Included components | Event Collector<br>Event Processor for processing events and flows<br>Internal storage for events and flows |

In order to provide an adequate level of backup, it is necessary to configure a FTP server on the CentOS platform for more permanent data storage of users' systems. Every user system should have a separate folder for storing system records. Retention of logs/system records on AiO devices would be for up to 6 months, while the records would be kept on a backup server for up to 2 years. Aside from retention, system configuration per user would also be stored for the same period of time. The listed backup processes would be performed automatically at least once a day, and more often manually, should it be necessary, depending on system activities. As with the AiO servers, the backup servers should also be kept in a high accessibility regime (Fig. 1).

In accordance with the legal regulations and demands of the ISO27001 standard, it is necessary to provide disaster recovery as well, i.e. recovery in cases of a disaster occurring on the primary site. For this reason, it is necessary to provide tape backup for system records, as well as system configurations. In order to optimise the time taken, the tape backup would use a tape library device which would enable the management of a number of tapes at the same time. Every user would have the required number of tapes based on the internal procedures of the user and the potential of the organisation that provides the MSSP services.

As a third level of security against system failure, it is necessary to provide replication of primary data on a DR location. It is possible to achieve this by transferring the infrastructure onto a remote location, which would require redundancy from the company providing the hardware resources for the implementation of the MSSP service.

In the second case, it is necessary to provide a disaster recovery licence for the AiO component of the system.

For all the systems mentioned, it is necessary to provide rapid communication links.

For a minimal, though insufficiently safe configuration, it is necessary to provide the following:

A server on which the AiO console, as well as a Linux backup server would be installed.

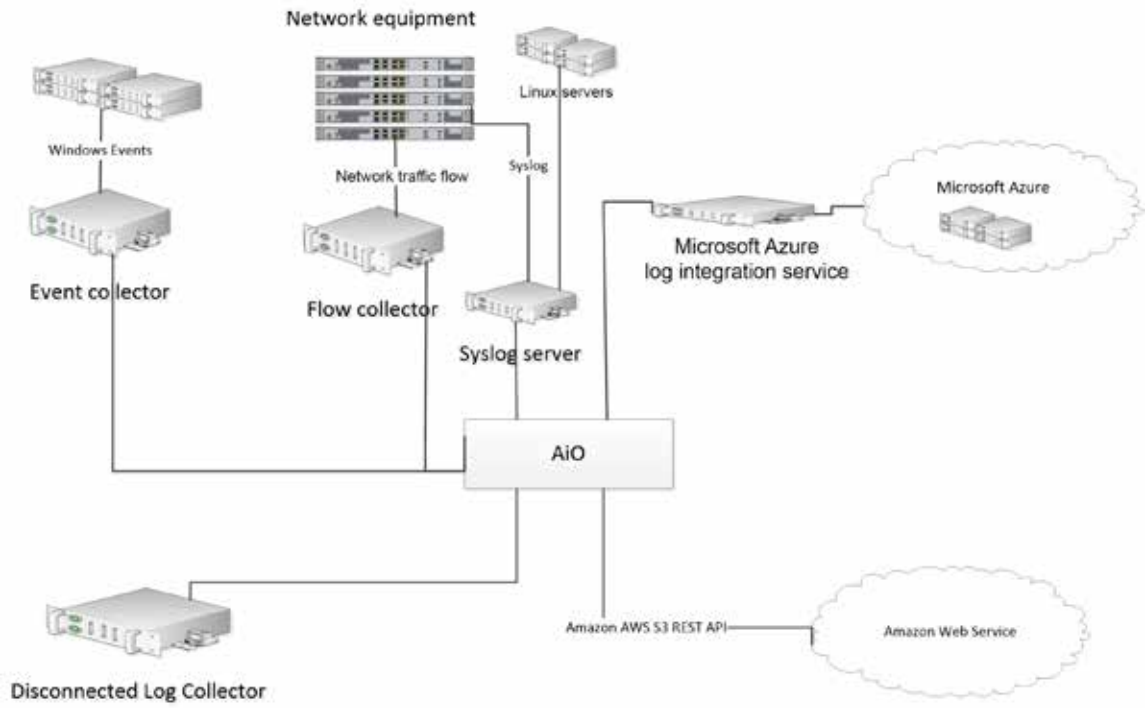


Fig. 1 Noah work vineyard. Fresco from monastery Decani. Gallery of frescoes, Belgrad.

This configuration does not allow for the option of restoring from tapes, or the long-term storage of system records. Additionally, another big risk that should be mentioned is the fact that there is no option which would enable high accessibility for the system. All of this means that in case of unforeseen events, such as a system failure or works on the system, users would not be able to access contracted services. Since local data collection is enabled, the user would be able to perform the collection, but not the evaluation of collected system records until the system is fully restored.

Based on empirical experiences, the quantity of EPS and Flow records for users ranked in SIEM environments can easily be handled by configurations which support up to 5,000 EPS, i.e. 200,000 FPM.

As for the dimensions of the system, the basic model used would be the AiO console IBM QRadar 3105 (IBM Knowledge Center 2019). This console is intended for small and medium-sized implementations. A description is provided in the following table.[1]

Should every user opt for the said console, it would be necessary to also increase, for the listed values, hardware demands for the said system.

A downside of these solutions is the exponential increase of needs for IOPS capacities for the storage of collected records.

## A DETAILED CONFIGURATION OF THE AIO COMPONENT AND CONNECTIONS TO DIFFERENT ENVIRONMENTS

In order to collect system records from users' equipment, it is necessary to install systems for system record collection on the users' side.

In order to access his own AiO console, the

1 https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.8/com.ibm.qradar.doc/c_hwg_3105_allone_base.html

user would use the fixNAT access. It is also necessary to stress the fact that it is recommended that local accounts be used for accessing the system, without integration with the existing access rights management systems located on the user's side.

The image below provides an example of the implementation with a user who has all the aforementioned systems and a much diversified infrastructure, which is split between an on-premise installation and a cloud environment.

In this particular case, it is necessary to obtain licences for the following systems:

AiO console,

Event collector,

Flow collector.

It is necessary to point out here that for the Event and Flow collector only Node licences should be obtained, while the quantity of EPS/ Flow records is defined exclusively via the AiO console.

## CONCLUSION

The MSSPs can provide real value to organisations of all sizes, by offering them the visibility needed in their environment as well as the possibility to fulfil the demands of legislative regulations, implemented standards and, probably most importantly, the demands of their work. Along with the particular solution presented here, there is always the possibility of upgrading such solutions in accordance with the needs of particular business activities with additional systems, such as a solution for vulnerability testing and analysis. That is to say, they can be scaled in accordance with the needs of the implemented systems.

* * *



## BIBLIOGRAPHY

**Rouse, M. 2018**
Managed security service provider (MSSP), Searchitchannel, 2018, https://searchitchannel.techtarget.com/definition/MSSP

**Korać, V., Prlja, D. 2018**
Targeting Cyber Threats by Recognizing Active and Passive Malicious Attack Techniques and Protecting Information, *Archaeology and Science* 14: 103-114.

**IBM Knowledge Center 2019**
QRadar 3105 (All-in-One), IBM, 2019.
https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.8/com.ibm.qradar.doc/c_hwg_3105_allone_base.html

## REZIME
## PRIMENA I UPRAVLJANJE ALATOM ZA BEZBEDNOSNE INFORMACIJE I DOGAĐAJE U INFORMACIONIM SISTEMIMA U VIDU MSSP MODELA

**KLJUČNE REČI: MSSP, PROVAJDER UPRAVLJANJA BEZBEDNOSNIM INFORMACIJAMA, OBRADA SISTEMSKIH ZAPISA, PRIKUPLJANJE SISTEMSKIH ZAPISA, SIEM, UPRAVLJANJE BEZBEDNOSNIM DOGAĐAJIMA.**

Ovim radom obuhvaćeno je kreiranje opšte inicijalne arhitekture SIEM rešenja koji je koncipiran kao MSSP model za centralizovano prikupljanje i analizu sistemskih zapisa prikupljenih sa različitih formi. Dat je opšti prikaz rešenja, prikazana je detaljna analiza povezivanja komponenti u predloženom rešenju i istaknute su prednosti i mane MSSP pristupa. Prikazane su evaluacije određenih SIEM rešenja, a fokus je postavljen na tehnički najbolje rešenje koje pokriva najveći broj scenaria i poseduje mogućnost brzog oporavka od katastrofe. U ovom radu je prikazano kako najbezbednije rešenje za implementaciju sistema sa visokom dostupnošću tako i jedna minimalna konfiguracija koja može zadovoljiti minimalne korisničke zahteve, ali neće obezbediti neophodan nivo redudanse i brz oporavak u slučaju problema. Ono što treba napomenuti jeste da se ovakva rešenja mogu nadograđivati u skladu sa potrebama poslovnih aktivnosti sa određenim dodatnim sistemima (analiza i testiranje ranjivosti) i skalirati u skladu sa potrebama implementiranih sistema.