Overview of Security Information Management (SIM)

Last Updated : 16 Sep, 2021

Not in only IT organizations, but for all type of organizations data is the source of power to their organization. Data is undeniably one of the most powerful assets in this digital age. Business organizations gather and store a huge amount of information from their customers. Such as user data, how often they purchase something, what things are purchased together, payment data, health care information and a lot more.

This information helps the business organizations to see trends, behavior analytics of customers and many insights can be deduced from the data with some systems by observing the pattern in the massive amount of data.

Apart from the storage of customers' information, business organizations need to store their employee data, trade secrets/strategies, ongoing project documentation and other essential information confidentially. And they need to make sure that all the data and information are secured.

And with the advancement of technology, many malicious activities happen digitally that threaten the growth and existence of businesses. That is why the security of information must be ensured by real-time management. This is where security Information Management (SIM) plays its crucial part. So, in this article we will discuss about this Security Information Management.

Security Information Management :

Security information management is a process of gathering, monitoring and investigating log data in order to find and report suspicious activities on the system. This process is automated by security information management systems or tools.

Log data is nothing but a file that collects and stores whatever happens in the system. The files (records) have information about system activities such as running applications, services, errors that occurred. So that is what security log data is.

With security log files, one can know the IP address of the system, MAC or internet address, login data and status of the system. If such details fall on bad guys, they might use the details destructively. This is one of the major reasons behind the birth of security information management.

But, **Where does SIM obtain log data from?**

Well, the log data is collected from various sources like firewalls, intrusion detection systems, antivirus software, proxy servers, file systems, etc. So based on the data gathered from all sources, security information is monitored and maintained.

Thus, this is what and how the SIM system does its job. Security management is categorized into three segments. One of them is SIM. Another one is SEM (Security Event Management) which deals with real-time monitoring and alerting the admins whenever it detects certain events occurring in the network activity. The last one is the fusion of SIM + SEM = SIEM (Apparently the abbreviation stands for Security Information Event Management). These days, businesses prefer the power-packed fusion of SIEM tools majorly.

What exactly SIM systems do ?

- SIM systems keep track and show the activity analytics of the system events as they happen.
- They then translate events data gathered from many resources into a general and simplified format. Usually, the data is translated into an XML file.
- SIM systems collect and coordinate data from various resources in such a way that helps administrators to recognize the real threats and false positives on the system. False positives mean events that seem to be a major threat but in reality it’s not a threat.
- As soon as suspicious activities occur, the SIM tool responds to the event by sending alerts to administrators of organizations and by generating reports and graphical representations such as charts and graphs.

The reports generated by SIM systems are typically used to :

1. Detect unauthorized access as well as modifications to files and data breaches.
2. Identify data trends that can be leveraged potentially by business organizations for their progression.
3. They are also used to identify network behavior and assess performance.

The SIM tool (system) acts as a software agent which sends the reports about the events to the centralized server. By which admins are updated about the reports. That's all about Security Information Management.

Comment | More info | Advertise with us

Next Article >

Integrating Risk Management in SDLC | Set 1

Similar Reads

Principle of Information System Security : Security System Development Lif...

INTRODUCTION: The Security System Development Life Cycle (SSDLC) is a framework used to manage the development, maintenance, and retirement of an...

7 min read