Understanding Security Event Management

Last Updated : 23 Nov, 2022

Security Event Management :

SEM stands for Security Event Management. As the name implies, SEM is the process of managing the security events happening across the network of an organization. This process is automated by SEM systems (tools).

What are security events?

Security events are activities of systems or software running on a computer network of the organization. These events are recorded in files one after the other as they occur. Those files are called event logs.

Since event logs are generated on each system of the network, they are then transported into a centralized location with the help of protocols such as Syslog and SNMP.

Working of SEM tools :

SEM tools identify, gather, organize the log events in a centralized location and represent them in visual formats such as graphs and charts for the security team of an organization to easily understand what is happening and what happened in their organization's systems connected in a common network.

By analyzing the log events in real-time, SEM tools do the following.

- Detects threats/vulnerabilities and bad actors like ransomware in the network.
- Automatically responds to incidents in real-time. Such as log off users, block an IP address on firewalls, killing an ongoing process, etc.
- Reports compliance in the network.

Need of SEM tool :

In the modern era; with the advancement of technology, numerous innovations solve significant problems and make things more convenient and comfortable than ever.

Along with that, some people exploit the technology maliciously for their own good or someone's downfall. So keeping crucial data within the organizations securely and confidentially has become a challenge.

Hence, organizations need to protect their data and resources proactively before someone sneaks in digitally. Without accessing the systems connected in a network within an organization, it's almost impossible for invaders to sneak in and get their hands on crucial data and resources.

That is one of the most important reasons for organizations to monitor and keep track of the activities going on all the systems of their organizations connected in a common network.

And manually keeping track of the ongoing activities across the network of numerous systems is impossible. Even if it's done manually by increasing the workforce, what happens next is the inefficient use of resources, wasting a huge amount of time and money on the additional workforce. So the pitch-perfect solution for such a significant scenario is Automation.

Benefits of SEM :

1. **Confidentiality** –
   SEM ensures that no unauthorized person gets access to the data and resources of an organization through the network. If someone sneaks in and gets unauthorized access, then the SEM tool will notify the security team and also take the necessary action to prevent the access instantly.
2. **Integrity** –
   Data and resources remain the same as left by the authorized person. No unauthorized person can modify any data and use resources while the SEM tool is in charge.
3. **Availability** –
   Access to certain data and resources for authorized users are available for a

4. **Non-Repudiation –**
   Whoever gets access, makes modifications and/or just being in the network are known and noted by SEM tools. This ensures that the information is passed between the authorized sender and receiver appropriately.

These benefits appease the organizations that use SEM tools by total security.

The combination of SEM and SIM(Security Information Management) tools is known as SIEM tools which are used widely these days to deliver unified solutions of Security Information and Event Management.

Comment | More info | Advertise with us

Next Article
Understanding Application Performance Management (APM)

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

Difference between Hardware Security and Software Security