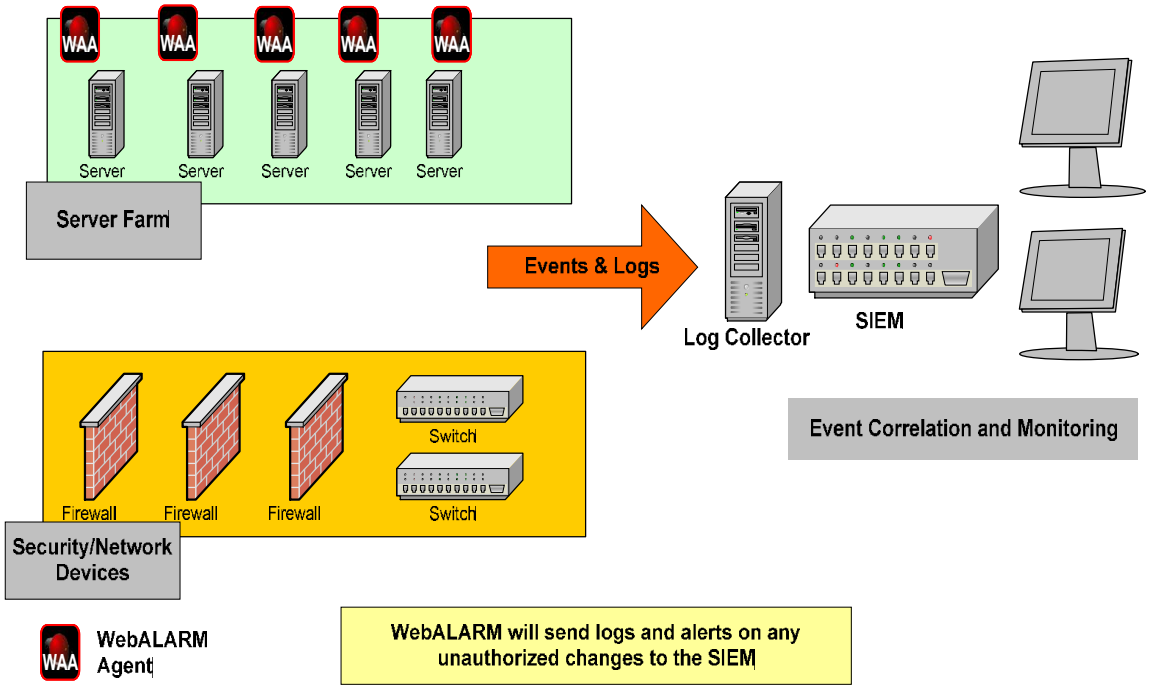
WebALARM

Integrating with SIEM for Real Time Visibility in Threats Detection and Management

In most organizations, one of the key components deployed for threats detection and management is by using a log management tool or SIEM systems. An organization may either setup a security operation center (SOC) infrastructure itself using these tools or outsource the monitoring to an SOC outfit. The traditional log management tools are mainly used to collect and store logs for analysis but they don't provide the intelligence needed for real-time security. The real-time security intelligence is usually provided by the SIEM systems. However there is an inherent weakness in this traditional log management or SIEM systems as that they do not provide the visibility on changes to files and data. This means that organizations end up missing critical information or alerts on potential threats and compromises at the file and data layer.

These weaknesses can be fully mitigated using WebALARM to complement their SIEM or Log Management systems. WebALARM combines existing security event analysis with additional view on data integrity without compromising on intelligence, performance and scalability. With WebALARM, companies will have a security solution they need to fully monitor threats at all levels; respond to threats quickly while maintaining continuous compliance.



WebALARM is readily integrated to most SIEM thus enabling companies to monitor activities in real time via a central console and act upon events of interest. As WebALARM provides alerts only when there is unauthorized changes to the files and data, it automatically reduces the amount of false positives that is usually generated from any monitored devices or servers. Thus enabling security analysts to respond appropriately in near real time to real security events and protect the confidentiality and integrity of the companies' IT infrastructure.

By integrating WebALARM and SIEM, the customers will gain an unparalleled visibility of threat management to its IT infrastructure while benefiting from WebALARM's file integrity and protection capabilities. As a key solution provider for file integrity monitoring and protection, we recognize that understanding changes in the IT environment plays a critical role in ensuring data integrity and security. Having the ability to identify events that lead to change, determine how it happened and whether it is a threat and then act accordingly is critical in protecting an organization's IT infrastructure.

Product Features:

1. Remote Administration

Agent and Console concept allows users to configure the agent only via the console, which can be installed local to the agent or remotely.

2. Multiple User Accounts

WebALARM promotes the use of multiple user accounts with explicitly assigned permissions to support multiple users.

3. SNMP / Email / Sound Alerts

Beyond SIEM and Log Management alerting capabilities, WebALARM can generate independent alerts when unauthorized modification of a monitored file has been verified. The agent can be configured to send out a SNMP trap message, an email notification or run a program in the form of a batch file or shell script.

4. Quick Response Time

WebALARM uses an integrity monitoring engine that performs real-time surveillance on user selected files/folders and able to instantly detect file modification with 100% accuracy.

5. Login Security

The Admin user is able to restrict user access to a range of IP addresses making it difficult for a foreign host within the internal network to pose as a valid host.

6. Backup Copy Monitoring

The Backup folder contains the backup copies of the monitored files/folders that are used by the agent for automatic restoration.