WHITEPAPER
FOR
eNlight SIEM

Table of Contents

1 Introduction to eNlight SIEM

SIEM (security information and event management) use has boomed in the previous two decades significantly, driven generally by complex and requesting compliance prerequisites such as Payment Card Industry Data Security Standard (PCI DSS) and Sarbanes–Oxley (SOX), as well as the requirements of occurrence reaction groups for danger management. As appropriation expanded, enterprises rapidly realized the esteem of the SIEM in giving and leveraging "threat intelligence"—giving perceivability into known dangers happening around the world and the capacity to distinguish and track potential dangers as they happen. This situational awareness permits enterprises to identify attacks sooner, and, as a result, take action to minimize the impact of today's progressed threats.

Security Information and Event Management (SIEM) solutions provide enterprises with network security insights and real-time monitoring for network gadgets, frameworks, and applications. Utilizing SIEM arrangements, IT administrators can mitigate sophisticated cyber assaults, recognize the root cause of security incidents, monitor user activity, obstruct data breaches, and, most importantly, meet administrative compliance requirements. The IT framework of any enterprise includes network devices (routers, switches, firewalls, etc.), frameworks (Windows, Linux, etc.), and business-critical applications that create a huge amount of log information. This log data can give effective experiences and network security insights into user behaviors, network anomalies, system downtime, policy infringement, inside dangers, etc.

As the volume of log data is large, manually evaluating it to meet your IT security standards is impossible. Manually monitoring and analysing logs in real time is impossible. As a result, exploiting log data requires automation, which is where SIEM solutions come in.

This Whitepaper is intended to give details and issues that IT administrators encounter with managing terabytes of data and solution which eNlight SIEM provides solutions to overcome this problems.

2 Architecture

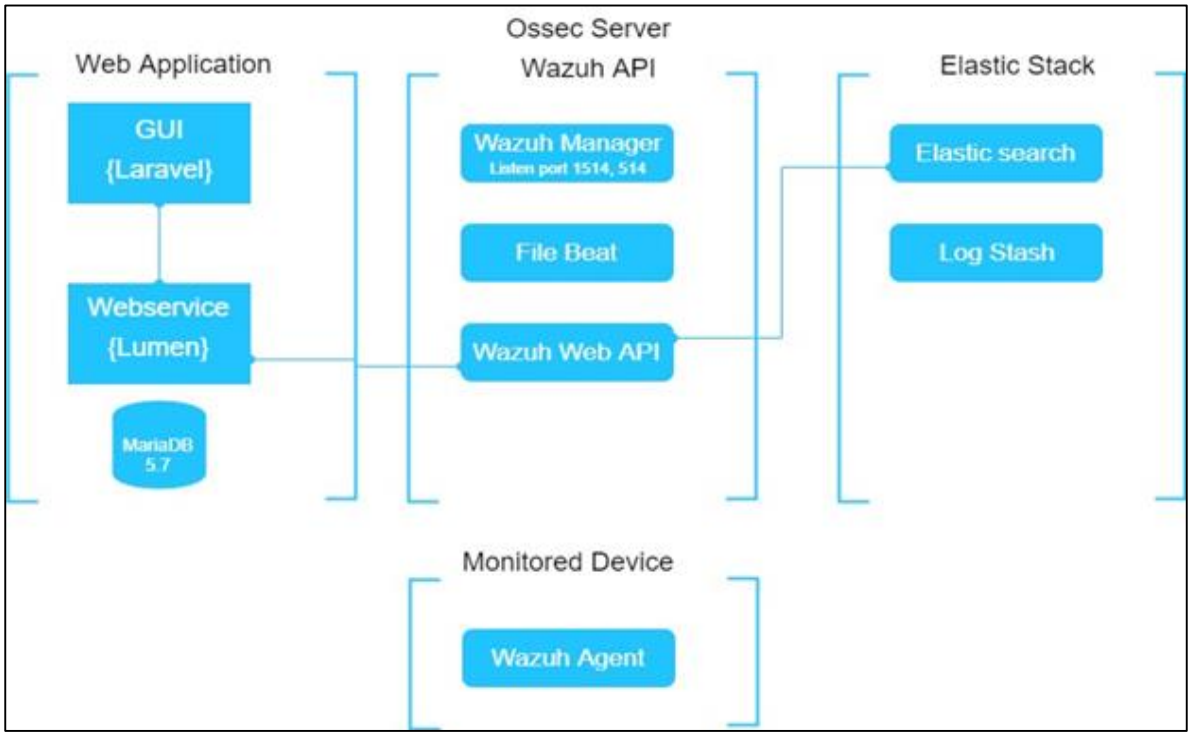

Figure: Product Architecture

3 Why eNlight SIEM?

In today's business environment, IT infrastructure is considered the lifesaver of any organization, both large and small. And, keeping the IT infrastructure secure from dangers has ended up a troublesome task for IT personnel. Log data that's produced by network frameworks, devices, and applications could be a gold mine that can help organizations keep their network secure from all arrange dangers; that is, as it were in case the log data is monitored and analyzed in real-time.

Organizations require tools that can determine important, significant data, and security insights from the log information. Checking and analyzing log data isn't a one-time process that will secure your network. It should be a continuous process in which the log information is collected, checked, and analyzed in real time at a central location.

Security Information and event management (SIEM) solutions have entered the showcase to supply security intelligence and robotize overseeing terabytes of log information for IT security. SIEM solutions screens network systems, devices, and applications in real time, giving security insights for IT experts to mitigate dangers, connect occasions, recognize the root cause of security occurrences, and meet compliance requirements.

eNlight SIEM is foremost cost-effective software in the market. It allows organizations to automate the whole process of overseeing terabytes of machine-generated logs by collecting, analyzing, looking, reporting, and archiving data from one central location.

IT security experts can presently relieve dangers, conduct log measurable examination, screen user activity, and comply with distinctive compliance administrative bodies by employing a single tool. The eNlight SIEM gives organizations total visibleness into their network infrastructure to keep their networks secure from dangers in real time.

4 Features

Following are the features of eNlight SIEM:

4.1 Log Analysis

eNlight SIEM has the capability to aggregate logs from heterogeneous sources (Windows frameworks, Unix/Linux systems, applications, databases, switches, switches, and other gadgets) at a central location. Universal log collection is a critical requirement for ventures looking out to deploy a SIEM solution. The advantage of the eNlight SIEM's universal log collection feature is that enterprises will be able to collect and analyze any log information organize from any source. Application or system problems, misconfigurations, attempted and/or successful malicious operations, policy violations, and other security and operational issues can all be detected using eNlight SIEM rules.

4.2 Log Forensics

eNlight SIEM makes forensic investigation exceptionally simple with its effective log search functionality and right away creates forensic reports based on the search comes about. It provides two distinctive log search capabilities, the Basic Search and the Advanced Search. Group search and range searches can also be conducted by utilizing Fundamental search. eNlight SIEM's Advanced Search has much more sophisticated look capabilities, but holds the ease of fundamental search.

4.3 IT Compliances

With eNlight SIEM, administrators can gain superior experiences into security threats and meet regulatory compliance necessities by monitoring and analyzing log data from the network framework. It provides some of the vital security controls to become compliant with industry guidelines and directions. The eNlight SIEM allows clients to customize the existing out-of-the-box compliance reports to meet their specific internal review necessities. It too allows IT administrators to produce modern compliance reports to comply with the modern regulatory acts, which may request compliance within the future.

4.4 Intrusion Detection

eNlight SIEM checks the monitored frameworks searching for malware, rootkits and suspicious peculiarities. They can identify hidden records, cloaked processes or unregistered network listeners, as well as irregularities in system call responses. In addition to specialist capabilities, the server component uses a signature-based approach to intrusion detection, utilizing its standard expression engine to analyze collected log data and explore for indicators of compromise.

4.5 Incident Reponses

Incident response is an organizational procedure that enables security teams to limit security incidents or cyber-attacks, as well as avoid or mitigate harm. When certain conditions are met, eNlight SIEM provides out-of-the-box dynamic responses to perform various countermeasures to meet dynamic hazards, such as restricting access to a system from the risk source. eNlight SIEM can also be used to remotely run commands or system queries, identify indications of compromise (IOCs), and assist with other live forensics or occurrence response duties In addition, incident response enables teams to deal with the attack's aftermath—recovery, patching security gaps disclosed by the attack, forensics, communication, and analysis.

4.6 File Integrity Monitoring

By safeguarding sensitive information and facilitating real-time file integrity monitoring (FIM), the eNlight SIEM assists enterprises in meeting their compliance requirements. Security professionals can now centrally track all changes to their files and folders such as when records and folders are created, accessed, seen, wiped, edited, renamed, and so on using the eNlight SIEM's record judgment monitoring functionality. eNlight SIEM keeps tabs on the file system, recognizing changes in content, rights, ownership, and file attributes that need to be addressed. It also recognizes the people and apps that created or modified the files.

4.7 Container Security

Security insight into hosts and Dockers containers is provided by eNlight SIEM, which monitors their activities and detects threats, vulnerabilities, and anomalies. Users may monitor images, volumes, network configurations, and running containers using the eNlight SIEM agent's local integration with the Dockers engine. It constantly gathers and analyses precise runtime data. For example, alerting for advantaged mode containers, vulnerable programs, a shell operating in a container, changes to specified volumes or photos, and other potential threats.

4.8 Cloud Security Monitoring

eNlight SIEM uses integration modules to pull security information from well-known cloud providers such as Amazon AWS, Sky Blue, and Google Cloud, allowing it to monitor cloud infrastructure at an API level. It also provides principles for evaluating the setup of your cloud environment and quickly identifying flaws.

4.9 Dashboards

eNlight SIEM systems is driven by dashboards, which assist IT managers in taking fast action and making the best decisions in the case of network anomalies. Data on security must be provided in a way that is intuitive and user-friendly. IT administrators can customize the dashboard to include and view only the security data they need. The security data is displayed in simple graphs and charts, and the IT administrator can look deeper down into the data and perform a root cause evaluation in minutes.

4.10 Reports

The security reports generated by eNlight SIEM are used by IT managers to make choices. The reports generated are precise and accurate. It include a number of pre-built security and compliance reports that may be created in minutes and scheduled for a specific time/day. Security reports are well-designed, and the data is well-organized. Administrators can use the custom report builder to develop security reports to match their internal security requirements. This custom report builder is adjustable, and allows IT administrator to add or remove certain security criteria while creating the custom report.

5 Conclusion

Security threats to businesses are always increasing, and businesses must ensure that their networks are sufficiently protected. By securing the network with real-time log analysis against data breaches and current cyber threats, eNlight SIEM can provide huge security benefits to the firm. In any event, the eNlight SIEM is one that is simple to implement, cost-effective, and satisfies all of your IT security requirements with a single device.