SIEM Architecture & Implementation

Reading

1h

Status | Incomplete

Introduction

In the previous reading, you learned the fundamentals of SIEM technology. In this reading, you will learn how to put together and implement a SIEM system and how to select the right SIEM that matches the needs of your organization.

Reading

SIEM Architecture

As you know from the previous reading, SIEM is an integrated security solution that can identify, analyze, and respond to any potential threats. The architecture of SIEM is composed of several key components, all of which collaborate with one another to present a complete perspective of the security posture of an organization. These components of SIEM architecture have been explained below:

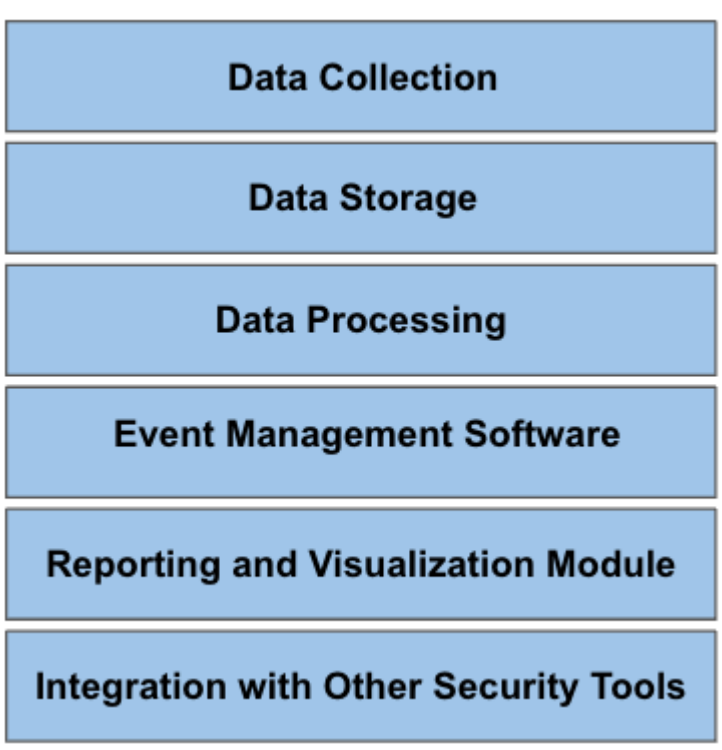

Figure 1: Components of SIEM Architecture

- **Data collection:** devices and systems that create data relevant to security, such as firewalls, intrusion detection systems (IDS), and logs from servers and applications are included in the data collection category. Logs of system activity, network traffic, and security events might be among the data that are collected.
- **Data storage:** in order to keep the collected security data safe and sound, a protected database or data storage system is utilized. It is important that the data storage system be able to manage massive volumes of data and give quick access to the

data so that it may be analyzed.

- **Data processing:** software that processes and analyzes the data acquired for security purposes is referred to as "data processing." This component incorporates correlation and alerting engines, which perform data analysis to recognize potential threats and generate alerts as a result.
- **Event mManagement software:** software that controls the events that are created by the analytic process, including correlation, prioritizing, and escalation, is referred to as event management software. This component contributes to the reduction of false positive alerts and assists in the prioritization of security events depending on the severity of the incident as well as its possible impact.
- **Reporting and visualization module:** software that creates reports and offers visualizations of security-related data for the purpose of analysis and evaluation is referred to as the reporting and visualization module. Because of this component, security teams are able to swiftly gain an understanding of the current state of their security posture and identify areas in which they may make improvements.
- **Integration with other security tools:** SIEM systems can be integrated with other security tools in order to provide a comprehensive view of an organization's security posture. These other security tools include IDS, intrusion prevention systems (IPS), firewalls, and threat intelligence feeds.

A holistic view of an organization's security posture, the ability to effectively identify and respond to security threats, and the ability to maintain compliance with security and regulatory standards are all provided by a SIEM architecture. This architecture has been appropriately built to help any organization to protect their assets and respond effectively and efficiently.

> ⚠ Read the following article to get an in-depth understanding of SIEM architecture: SIEM Architecture: Technology, Process and Data.

As you read, focus on the following:

- Key components of SIEM architecture and its capabilities
- Types of SIEM implementation on the basis of organizational business needs

SIEM Implementation – Key Considerations

Selecting the right tool for your needs is always a challenge, and here we are talking about the SIEM which integrates all logs generated from all those tools. Even though you should consider many factors, there are some industry standards that should guide you when selecting the right SIEM for your organization; some are as follows:

- **Correlation and analysis:** select a system that can do real-time correlation and analysis of security events in order to identify possible threats and security issues, and then go with that solution.
- **Incident response:** choose a product that already incorporates incident response features, such as automated response workflows, playbooks, and reporting, into its core offering.
- **Integration:** ensure that the solution you choose is compatible with the other security measures you already have in place, such as firewalls, IDS, and vulnerability scanners.
- **Data coverage:** choose a solution that protects all relevant sources of security data, such as network devices, servers, apps, and cloud infrastructure, rather than one that only protects some of these areas.
- **Alerts and reporting:** choose a system that enables you to effectively respond to possible threats and security events, and make sure that it gives you the ability to customize alerts and offers extensive information.
- **Threat detection:** choose a system that has advanced capabilities for detecting threats, such as behavioral analysis, machine learning, and threat intelligence.
- **Data collection:** pick a solution that can collect logs from all the key sources you need to keep an eye on.
- **Data analysis:** make it a point to verify that the solution offers real-time analysis, correlation, and warnings.
- **Compliance:** give some thought to a system that has the potential to assist you in satisfying regulatory standards and security best practices, such as PCI-DSS, HIPAA, and SOC 2.
- **Scalability:** choose a system that can grow with your company to support increased data quantities, sources, and security requirements. This is an important consideration when selecting a solution.
- **Vendor reputation:** pick a provider who has a track record for providing excellent service to their customers, coming out with innovative products, and being dependable.
- **User-friendliness:** pick a provider that has a simple user-friendly interface, easy navigation, and customizable dashboards.
- **Cost:** think about the whole cost of ownership, which should include things like licensing, maintenance, and support.

Choosing a SIEM system that is not only comprehensive but also efficient and affordable is not a simple task. In most situations, we conduct proof-of-concept (POC) research and write test cases in order to carry out a direct comparison. You will go over most of these factors and discuss the pros and cons and dependencies, and also what must-haves or good to have of any specific organization. That also includes, should they have open source or buy expensive commercial products?

Key Takeaways

- SIEM architecture has several different components, such as event management software, reporting and visualization modules, etc.. These components interact with each other to present a holistic view of the security posture of an organization.
- SIEM architecture and implementation varies from organization to organization depending upon the specific business needs of the organization.
- When selecting the SIEM that fits the business needs of your organization, it is recommended to consider the industry standards established for SIEM implementation.

Conclusion

Now that you understand the basics of SIEM and SIEM architecture, you will move on to a check your understanding activity to help you develop your understanding of SIEM technology even further.

✓ Mark Completed

Previous
Introduction to SIEM Systems

How well did this activity help you to understand the content?

Let us know how we're doing

W08D2

Tue Aug 13

W08D2 Schedule »