TechBridge
Making the World Smarter

# tbSIEM

## WHITE PAPER

# Contents

# 1. Introduction

Cyber-attacks are becoming more common, with a serious IT breach making headlines every other day. Attackers constantly look to exploit any gap in IT systems, applications and hardware. One of the key security approaches to prevent and combat attacks is to identify and respond to security events in real-time to minimize the damage. Security Information and Event Management Software (SIEM) allows security teams to keep on top of security alerts in real-time. In this article we will outline what a SIEM solution is, its importance and its benefits.

# 2. SIEM Overview

Security Information and Event Management (SIEM) is security software that gathers log security data from diverse sources, categorizing and analyzing security alerts in near-real time. SIEM combines security information management –meaning long term storage, analysis and reports on log data –with security event management, which monitors the system in real-time, correlating events and generating alerts.

The platform uses correlation rules and statistical algorithms to extract actionable information from events and log entries. Key features of a SIEM security solution include:

1. **Visibility in Near-real Time:** Uses visual consoles as dashboards to provide an overall view of the security system.

2. **Data Consolidation:** Manages log events of data streaming from various sources.

3. **Correlation of Events:** Uses Boolean logic rules to add context and intelligence to raw data.

4. **Automated Security Event Alerts:** Analyzes indicators of compromise and sends alerts, notifying issues in real time.

## 2.1. Why Is It So Important?

The reason an organization needs a SIEM solution to monitor the systems and report suspicious activities is that the amount of data an average organization generates nowadays is too much to handle manually.

For instance, Gartner considers a SIEM system as small if it has up to 300 event sources, with events generating at 1,500 events per second. Large SIEMs handle thousands of event sources, generating more than 25,000 events per second. The key ability of a SIEM is to filter through all the data and prioritize security issue alerts, making security more manageable.

Log management sits at the core of SIEM functions; as the more diversified types of logs from more disparate sources feed the SIEM system, the more it generates actionable reports. This capability allows SIEM to correlate relevant events by cross-referencing logs from different sources against correlation rules.

**The following are three of the main reasons that organizations need a SIEM solution:**

**1. Detecting Incidents**
A SIEM solution detects incidents that otherwise can go unnoticed. This technology analyzes the log entries to detect indicators of malicious activity. Moreover, since it gathers events from all sources across the network, the system can reconstruct the attack timeline to help determine its nature and impact. The platform communicates recommendations to security controls –for example, directing a firewall to block the malicious content.

**2. Compliance with Regulations**
Companies use SIEM to meet compliance requirements by generating reports that address all logged security events among these sources. Without a SIEM, an organization need to manually retrieve log data and compile the reports.

**3. Incident Management**
A SIEM improves incident management by allowing the security team to identify an attack's route across the network, identifying the compromised sources and providing the automated mechanisms to stop the attacks in progress.

## 3. Best Practices for Successful SIEM Implementation

- **Establish the Scope and Requirements**
  Know exactly what activities and logs you want your SIEM to monitor. This includes choosing if you want to implement your SIEM as an on-premise software or a hosted or managed service.

  Next, you should get a clear picture of the requirements for your SIEM, including the use cases for your particular industry. In addition, you should take note of compliance requirements, comparing them with the candidate SIEM solutions you are considering. Some vendors offer built-in features that support specific compliance requirements, including auditing.

- **Customize Correlation Rules**
  The core value of SIEM stems from applying correlation rules that can flag security events that otherwise go unnoticed. For instance, a correlation rule that says that if there are

several failed logins from the same IP in a given timeframe followed by a successful login, a brute force attack may be in progress. While SIEM software comes with its own set of built-in rules, you can customize it to your needs by removing false positives or creating new rules.

- **Do a Test Run First**
  A pilot run in a section of the infrastructure is a good way to test the new deployment. This stage provides the proof of concept, and the potential ROI for the system. However, it is important that this test subset represents the wider system context to allow for identifying flaws and vulnerabilities in security policies.

  During this test run, collect as much data as possible to allow for a clear picture of how the system would run. Of course, it is not always possible to collect data from every single source across the organization. In this case, you should prioritize sections dealing with the critical systems and sensitive data.

- **Have an Incident Response Plan in Place**
  A SIEM provides near real-time monitoring and alerts for IT threat detection, allowing for a rapid response to a myriad of security events. However, the organization should leverage SIEM features by implementing a detailed, hands-on Incident Response Plan.

  This comprehensive protocol should cover issues such as distributing the responsibilities and tasks in the event of a data breach or attack, prioritizing and documenting the event, and delegating who will be responsible for communicating the breach to stakeholders and relevant authorities. A well-laid incident response plan provides the exact steps and guidelines for the security teams to follow when an attack occurs, saving time and minimizing mistakes resulting from ad-hoc responses.

- **Update Your SIEM System Continuously**
  Since attackers are constantly improving their methods and techniques, the SIEM needs to remain a step ahead. You should periodically test your SIEM, modelling potential attacks and evaluating the SIEM reaction. Simulating attacks can help you to refine the SIEM configuration by tweaking the correlation rules, policies and procedures to keep ahead of malicious attackers.

## FOR MORE INFORMATION

### About TechBridge

TechBridge is the World's leading Product & Solutions Company. Data Center Applications, Collaboration and Real Time Communication. DC Management and Monitoring, Disaster Management, Security, Collaboration and Cloud. Its market-leading Network Modernization, Unified Communications, Mobility and Embedded Communications solutions enable customers to quickly capitalize on growing market segments and introduce differentiating products, applications and services. We are an expert and leader in Government Solutions, Smart City Solutions, Data Centers and Large Enterprises. We do custom applications also, as per the customer requirements.

### Certificates:-

**ISO 9001**


**ISO 27001**


**ISO 20000**


**CMMi L3**


**ISO 15408-1**


**PinkVERIFY**


**Mail us at**: sales@tech-bridge.biz

**Address:-** TechBridge Consultancy Services LLP
326, Tower B3, Spaze iTech Park, Sector-49, Sohna Road, Gurgaon-122018, Haryana