Penta's IT Risk Solutions Portfolio

WHITE PAPER

Guide to SIEM Solutions

What is a SIEM?

It could all start with a tiny incident that goes unnoticed. A phishing link sent to a new employee, a social engineering call to a director's PA, a USB plugged into an unattended PC in the lobby, an unpatched server running old software, or an outdated network printer that is exposed to the internet. The next thing you know, you're hit with a wide-scale ransomware attack or data breach causing massive financial losses, decreased customer trust, and other irreparable damages.

There is no doubt that cybercrime has been on a steep rise over the last two decades, and it has grown in complexity and sophistication making it one of the top risks to mitigate for any organization.

To counter this ongoing complexity and novelty at scale, cybersecurity professionals turn to advanced software that monitors and analyses telemetry and logs from IT infrastructures in real-time to detect irregularities and patterns that could signal real threats. This type of solution is referred to as a Security Information and Event Management (SIEM) system, and it is considered a critical component of any cybersecurity ecosystem, and an essential compliance tool.

SIEM solutions have been around for more than a decade and they have been evolving rapidly to keep up with the increasingly complex and challenging cyber risk landscape.

How does a SIEM system work?

A SIEM system works by collecting and ingesting security event logs from various data points including servers, workstations, software applications, storage, network traffic, in addition to network and security devices. The SIEM then normalizes this data which typically comes in different formats and structures, and then analyses it in real-time. It then correlates the data to detect suspicious activities and incidents that could represent actual threats and assesses their potential severity and impact.

SIEM systems help automate the processing and handling of large volumes of data from multiple sources in a way humans cannot possibly achieve, while leveraging external sources of knowledge on threat intelligence. Machine learning and artificial intelligence add another layer of effectiveness to SIEM systems, enabling them to analyze large datasets to detect anomalies that are not previously known as threat signals, or evaluate things like the behavior of internal users to detect insider threats.

The human element still plays a critical role in a SIEM setup, which is typically integrated through the role of a Security Operation Centre (SOC), where teams of cybersecurity professionals receive the alerts about

potential threats, investigate such incidents in context, determine the right course of action and respond in real time.

All the logs captured in a SIEM system are stored for set periods of time for regulatory compliance reasons and to conduct further analyses when needed.

SIEM Acquisition and Deployment Options

SIEM is essentially a software solution that can be acquired and deployed in three different ways:

On-premises SIEM

With an on-premises SIEM solution, you would acquire the software, hardware and resources and deploy the system within your own IT infrastructure. The advantage of this approach is having full control over the deployment and keeping the data in-house. However, this approach also means that you are fully responsible for maintaining and managing the system which typically requires a lot of resources. A common problem with this type of implementation is alert fatigue, where your internal teams are flooded with a barrage of alerts that could be false positives but require further investigation to find out. This option also tends to have the highest Total Cost of Ownership (TCO) compared to the other routes.

Cloud-based SIEM

In the case of a cloud-based SIEM, the solution is subscribed to as a pay-as-you-go service, which alleviates the hassle of acquiring and setting up software and hardware, thus reducing up-front costs. In this approach the cost depends on combinations of variables such as volume, resources, number of devices, or data velocity. Very often with Cloud-based SIEM, log data is stored and processed outside the premises which can be a challenge for many when it comes to compliance. Another key challenge with cloud-based SIEM is that it still requires a lot of resources and expertise to monitor the system, respond to alerts, and expand the system to handle new cases.

Managed SIEM

In a managed SIEM approach, the SIEM solution is acquired as a managed service provided by a professional third party that is experienced in implementing and operating SIEM systems and handling threat detection and response. The managed SIEM solution includes both the SIEM system and the professional services bundled together as a custom package. This is to differentiate it from third party professional services that are acquired separately to help support a new or existing on-premise or cloud-based SIEM deployment, especially when it comes to comparing costs. While there is generally less control in this approach, the advantages are lower costs and less need to hire internal resources, making it more accessible to a wider segment of businesses to reap the benefit of using a SIEM system without having to go through the hassle of purchasing it or managing it.

What is the best approach to follow?

The best choice of SIEM implementation depends on many factors such as the scope of monitoring, your own priorities and requirements, regulatory compliance requirements, the capacity and experience of your internal security teams, and of course the budget restrictions.

In the case of most SMEs, the scope of monitoring is smaller, internal teams are smaller and less capable, and the budgets are typically lower, which makes a pay-as-you-go cloud-based SIEM or a managed SIEM the

ideal approach. While in the case of larger enterprises, the monitoring scope is generally much wider, internal teams are bigger and more capable, and budgets are higher, which makes an on-premises SIEM or a full-on cloud-based SIEM the more ideal approach.

Nevertheless, even large enterprises may be better off going with a managed SIEM solution as field data suggests. According to leading IT research and advisory firm Gartner, many companies indicate that they are seeking external service support for their SIEM deployment, or that they plan to acquire that support in conjunction with a SIEM product. Many indicate a lack of internal resources to manage a SIEM deployment, a lack of resources to perform real-time alert monitoring or a lack of expertise to expand a deployment for new use cases.

Gartner predicts the demand for managed SIEM services to continue to grow as more customers face 24/7 monitoring requirements and implement use cases that require deeper SIEM operational and analytics expertise.

Therefore, in most cases, a managed SIEM approach remains a sensible option for all types and sizes of companies that have a limited budget and lack a dedicated team of in-house security experts to deploy and manage a SIEM solution and respond to the high volume of alerts it is likely to generate.