ManageEngine
Log360 Cloud MSSP

An MSSP's **cloud-SIEM business guide**

The **why, what,** and **how** of discovering a cloud-based SIEM solution

www.manageengine.com/cloud-siem/

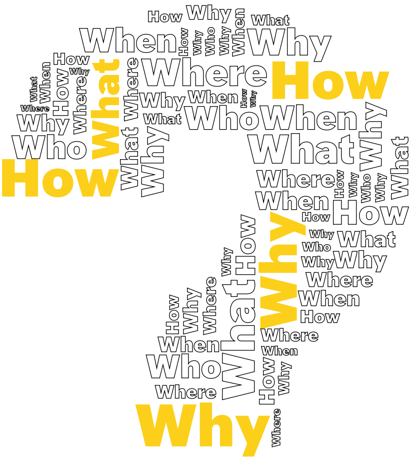

Table of content

5 reasons you need a cloud-SIEM solution as an MSSP

5 ways you can capitalize on the current MSSP market with a cloud SIEM

5 boxes your cloud-based SIEM should check for your MSSP needs

As an MSSP, you might face continual and shifting operational, technical, and commercial demands. Adapting to the ever-evolving technological landscape in cyberspace requires not only scaling management capabilities but also efficiently handling existing client needs—a task that can be daunting.

This involves deploying skilled professionals adept at sifting through intricate security logs identify attack patterns and manually respond to various threat scenarios, all while managing vast amounts of data across multiple client environments. While the human element in security operations remains invaluable, one must ask: Is a hands-on approach to SIEM always the most efficient method?

In this business guide, we'll explore the possibilities of conventional SIEM alternatives for meeting the demands for instantaneous scaling, adapting to voluminous data inflows, and evolving to address emerging threats.

5 Reasons

why MSSPs need a cloud SIEM solution

To deploy a full-fledged SIEM for our clients, we need to address issues of unwanted log storage, additional compliance regulations, and high maintenance costs. The challenge is increasingly difficult with a tight pool of cybersecurity talent. Many organizations currently can't hire for all their needs.

Scaling made easy

In addition to common operational tasks being streamlined, you can enjoy the bandwidth of expanding your client base by providing multi-tenant capabilities without worrying about deployment issues. This fast tracks the process of getting a new client up and running. A cloud-based SIEM also facilitates geographical expansion by leveraging data centers in multiple locations, ensuring that data residency, and latency requirements are met.

Effortless access control

With role-based access control features, you can define and enforce granular permissions for users and administrators.This helps maintain data privacy, optimize performance, and facilitate efficient log management across multiple customer profiles, all from a single, intuitive console.

Reduce your log storage spending

A cloud SIEM can automatically adjust to handle the increased load without requiring manual intervention or hardware procurement. Organizations deploying a more cost-effective cloud SIEM can easily expand their log storage capacity as their needs grow, without having to invest in additional hardware, or worry about running out of physical storage space.

Effective client management

Organizations can utilize a centralized platform for managing logs from various sources. This not only streamlines log storage, but also simplifies log retrieval and analysis, making it easier to identify security incidents.

Ease of set up and maintenance

Cloud-native solutions enable quick, hassle-free deployment which extends to cloud SIEM solutions as well. This saves a considerable amount of time. SIEM solutions hosted in the cloud enable MSSPs to focus more on security monitoring and threat detection rather than infrastructure maintenance.

5 ways you can capitalize on the current MSSP market with a cloud SIEM

Capitalizing on the MSSP market depends on the technical features the solutions offer and might directly impact on the growth of your business. What are some of the market-differentiator features that you can look for in your cloud SIEM?

CASB visibility

A CASB provides critical visibility into user-cloud interactions, enabling enterprises to enforce policies, and extend security controls seamlessly to the cloud. By identifying shadow applications and their users, CASB enhances threat detection, ensuring that MSSPs can effectively safeguard their clients' data and networks.

Complete AWS logging

AWS logging is a crucial addition to cloud SIEM for MSSPs due to its wealth of data access insights. AWS CloudTrail logs, S3 server access logs, and Elastic Load Balancing (ELB) access logs record data access and contain details of each request, such as the request type, the resources specified in the request, the time and date the request was processed, the request path, and traffic volume. These logs provide comprehensive details on data access patterns, security audits, and misconfigurations.

Effective compliance reporting and alerting

With new compliance regulations coming up regularly, organizations are expected to be up to date with them during audits. Your SIEM should be able to provide compliance reports, retain log data over long periods, and monitor for violations to ensure your client meets all regulatory standards.

Incident management

Incident management is paramount for MSSPs using a cloud SIEM as it ensures a methodical approach to identifying and resolving security incidents. A SIEM's incident management capabilities ensures that you handle any security incident of interest methodically and with ease.The process of assigning security incidents to help desk technicians and tracking tickets is streamlined to effectively address and prioritize support issues.

Rule-based threat detection

By building rule-based alerts and leveraging a powerful correlation engine, MSSPs can swiftly detect malicious activities within their clients' networks. The Correlation engine allows a SIEM solution to identify known threats and indicators of compromise by comparing incoming events and logs against a predefined set of rules. With features like these in place, security teams are promptly notified of security incidents, accelerating incident response.

5 boxes

your cloud based SIEM should check for your MSSP needs

SIEM buyers face challenges that span from ensuring the platform scales efficiently across diverse client infrastructures, to evaluating the adaptability for varying levels of service customization. To address how your business can stand out commercially, here are five key pointers:

Multitenancy

The multi-tenant support that cloud-based SIEMs provide is a critical feature for MSSPs. This allows multiple client organizations (tenants) to be served concurrently with data segregation which maximizing resource usage and operational efficiency.

Operational efficiency

You can enhance the efficiency of your SIEM with built-in maintenance, updates, and patches handled by the cloud provider. This reduces the time and resources that the MSSP must allocate to these tasks, allowing them to focus on core security monitoring and incident response.

Profitable ROI

Cloud SIEMs do not require high-end computing resources, since the onus is on the cloud service provider to ensure that their infrastructure accommodates the computing requirements of every organization. Cloud SIEM solutions bring you enterprise-class service at a lower cost. With subscription-based models, MSSPs have a clearer picture of their expenses, helping in budgeting and financial forecasting.

Maximum SIEM service uptime

High availability and disaster recovery are often built into cloud solutions. By choosing a SIEM with reduced downtime such as Log360 Cloud, MSSPs can consistently deliver services to their clients, maintaining trust and reducing potential revenue loss.

Secure data transmission and storage

When choosing a cloud SIEM, an MSSP must prioritize secure data handling to guarantee the integrity, confidentiality, and availability of the data. These factors directly impact the MSSP's service quality, reliability, and overall business success. This can otherwise cause severe financial and reputational ramifications for the MSSP and its clients.

Security is not a one-size-fits-all and your solution should acknowledge this. ManageEngine Log360 Cloud MSSP addresses this through its client-specific dashboards and dedicated technician assignment, ensuring a personalized, tailored approach to every client's unique security landscape. The centralized client management console not only amplifies efficiency, but also fortifies data security and privacy.

Log360 Cloud MSSP's 99.9% monthly uptime is backed by its service-level agreement to ensure uninterrupted service is more than just a promise, it's a reality. Features designed specifically for a competitive MSSP market, strike the perfect balance between advanced technology and user-centric design. If you want to enhance the operational efficiency, and build unwavering trust with your clients, Log360 Cloud MSSP is the right solution.