Trustwave®

Understanding Managed Security Services Provider Offerings

The array of services offered by Managed Security Service Providers (MSSPs) continues to grow, often now including a SIEM offering. In this brief guide, we'll define the most common SIEM offerings to help you determine which is the best fit for your organization.

Security Information and Event Management

(SIEM; pronounced "sim" or "seem")

SIEM is a software tool that collects alert and logs data from potentially hundreds of elements in the environment, including security tools, network devices, computing systems and applications. SIEM aggregates this data, making it easier for security operations teams to correlate alerts and identify potential incidents.

Effectively thwarting threats, however, requires security professionals to properly configure the SIEM, as well as to interpret and act upon the data it collects. That's where the following three services come in.

Managed SIEM

Managed SIEM services help organizations operate and manage the complexities of their SIEM. Like similar services for firewall or Endpoint Detection and Response (EDR) tools, it helps customers manage their SIEM tool and may include alert monitoring and light investigation of security incidents. But most managed SIEM services fall short of addressing the end-to-end operational aspects required to get the full value out of a SIEM.

SOC-as-a-Service

SOC-as-a-Service (SOCaaS) is typically means the vendor assumes ownership of the infrastructure and product licensing. This can be a turn-key solution for smaller organizations that have neither a SIEM nor a Security Operations Center (SOC). Companies simply direct all SIEM data to their provider, who assumes responsibility for correlating alerts, interpreting the data, and identifying security problems amid the numerous false positives. In many cases, SOCaaS refers to a traditional Managed Security Services Provider (MSSP) model, where the provider monitors its own threat detection software.

Co-Managed SOC

Properly configuring and monitoring a SIEM can get complex. To get maximum value from their SIEM investment, many companies choose to partner with a provider with experience in best practices, templates, and proven configurations. SIEMs work best when accompanied by a closed-loop process, where the results of each alert investigation are used to tune the SIEM, creating highly optimized results over time. With a Co-Managed SOC approach, the provider not only helps monitor, triage, and investigate alerts, but also continuously tunes and optimizes the SIEM along with conducting reviews of security policy and architecture to improve security maturity. trial.

Learn more about Trustwave's Co-Managed SOC offering.
Visit **trustwave.com**

www.trustwave.com