Sagenet
CONNECT | MANAGE | PROTECT

WHITE PAPER:

Sizing-up SIEM-as-a-Service

Is a Fully Managed SIEM Solution the Right Choice for Your Organization?

Tulsa | Washington, D.C. | Atlanta | Chicago | Philadelphia
866.480.2263 | www.sagenet.com

SIEMasaServiceWP090519

SageNet

CONNECT | MANAGE | PROTECT

EXECUTIVE SUMMARY

According to the Cost of a Data Breach Report from the Ponemon Institute, it took 197 days on average for an organization to identify a cybersecurity incident in 2018, up from 191 days in 2017. It took 69 days on average to contain a data breach, up from 62 days the year prior. The average total cost of a data breach was $3.86 million, up from $2.62 million in 2017.

Common sense would suggest that the cost and impact of an incident increase with the time required to discover it. The Ponemon report confirms this idea. For organizations that identified a data breach in less than 100 days, the average cost was $3.11 million compared to $4.21 million for those that took 100 days or more.

Unfortunately, insider attacks, zero-day exploits and advanced persistent threats are increasingly difficult to detect. With lengthy “dwell times” in compromised systems and networks, cybercriminals are able to steal more sensitive data.

Security information and event management (SIEM) solutions can aid in the rapid detection of security incidents. SIEM helps organizations overcome two of the primary impediments to rapid incident response — an overwhelming amount of security event data and an insufficient number of skilled personnel to analyze it. However, SIEM systems are also complex to configure and manage, which can limit their value.

This whitepaper discusses the challenges associated with detecting cyberattacks and how SIEM can accelerate incident response. It also explains how a managed SIEM service can bring the benefits of SIEM to organizations with limited in-house resources.

SIFTING THROUGH THE CLUES

It’s easy to see why many cyberattacks go undetected. While attacks almost always leave clues, often they are buried in log files and alerts that go unnoticed. In fact, so many alerts are generated in the typical environment that IT teams simply can’t keep up.

In a 2018 Imperva survey, 27 percent of IT professionals said their security operations center (SOC) receives more than a mllion security alerts each day. Fifty-five percent receive more than 10,000 alerts daily. Almost half (47 percent) spend more than four hours each day simply dealing with security alerts.

Because of the sheer number of alerts coupled with the high volume of false positives, 57 percent of survey respondents said they were forced to fine-tune their alert policies to reduce the noise. Thirty percent admitted to ignoring certain categories of alerts, while 4 percent turned off alert notifications altogether.

In a recent IDC survey, 53 percent of IT professionals said they devote too much time to routine operations and incident investigations to improve security response. One-third (33 percent) said they struggle to keep up with the security workload and describe themselves as "constantly firefighting."

HOW SIEM CAN HELP

SIEM systems apply data analytics to the monumental task of sifting through security alerts. Security data is collected from a wide range of systems from across the organization, including servers, network devices, and security software and hardware. This data is forwarded to a central system, where it is inspected and analyzed in near real time.

SIEM doesn't just filter through the noise — it takes full advantage of all the data generated by various sources. While a single piece of information viewed in isolation has limited value, data collected from multiple systems and viewed holistically can reveal trends and patterns. SIEM systems use statistical correlation to identify relationships between the data points, which are then compared to profiles of normal system conditions in order to spot anomalies.

IT teams gain greater visibility and the ability to analyze alerts in context. A single management interface makes it easier to investigate security incidents and weed-out false positives. Best-in-class SIEM solutions also provide root-cause analysis of potential threats to enable responses triggered by risk level.

The Value of Security Automation

Automated security tools such as SIEM can help reduce the cost of a data breach. According to a 2018 Ponemon study, the average total cost of a data breach is 35 percent lower for organizations that have fully deployed security automation compared to those that have not.

THE TCO OF SIEM

While SIEM provides many benefits, deployment of an onsite solution is a lengthy, complex project. The system must be configured to aggregate, normalize and correlate data from various sources and to separate serious threats from false positives. If it's not set up properly, SIEM can overwhelm IT teams with more alerts.

The complexity of SIEM is reflected in its total cost of ownership (TCO). According to a recent Ponemon Institute study, the initial purchase price of the software represents just 25 percent of the total SIEM cost, with installation, maintenance and staffing making up the remaining 75 percent.

The survey also found widespread dissatisfaction with SIEM. While 84 percent of respondents said SIEM is important, very important or essential to their incident respondent processes, only 48 percent were happy with the actionable intelligence they get from their SIEMs. This dissatisfaction is linked to the complexity of the SIEM solution — 75 percent of respondents said that configuring SIEM required significant or very significant effort.

Another common complaint is that SIEM is too "noisy" — 54 percent of respondents said their SIEM generates too much low-level data and too many alerts. Seventy percent want their SIEM to generate fewer alerts that are more accurate, prioritized and meaningful, while 71 percent want to automate certain SIEM-generated tasks so that response teams can focus on priorities.

THE VALUE OF SIEM

Large enterprises were the early adopters of SIEM systems, which were primarily used for regulatory compliance. As a result, commercial SIEM platforms typically cost $20,000 to $50,000 or more, plus another $30,000 to $50,000 for compute and storage infrastructure. They are also complex to implement, requiring 120 hours or more at a cost of approximately $100,000 for engineering services.

Open source solutions have become available in recent years, providing a lower-cost alternative for small to midsize businesses looking to accelerate threat detection and incident response. However, open source tools also require significant time and expertise to implement and manage, and organizations may quickly outgrow their limited features.

Many organizations are turning to managed SIEM services to reduce costs and simplify SIEM deployment and management. A managed SIEM solution can be implemented quickly for faster time-to-value, and scaled as the environment grows and needs change. Typically, managed SIEM is offered as a monthly operational expense, giving organizations enterprise-class features without a large capital outlay. Organizations can access security data, reports and alerts, typically through a web-based portal.

Perhaps the greatest value of managed SIEM is derived from ongoing administration and maintenance. Rather than hiring and training security personnel, organizations rely on the expertise of third-party professionals who have access to up-to-date threat intelligence. When all costs are factored in, organizations can expect to pay $115,000 to $200,000 anually for managed SIEM compared to more than $230,000 for a traditional on-premises solution.

SageNet's Managed Security Operations Services

SageNet's Managed Security Operations Services include enterprise-class SIEM software in a private, hosted environment. Customers gain access to automated alerting, SageNet's custom ISO-based alerts, and ongoing tuning and maintenance by the SageNet team. SageNet's SOC-as-a-Service solution includes managed SIEM plus 24x7 security event monitoring and investigation, security analyst and engineer review, and escalation.

CONCLUSION

It can take weeks or months to detect a security breach, and the longer it takes the greater the cost of the incident. SIEM can help organizations identify threats faster by cutting through the noise created by too many security alerts.

However, implementing and managing SIEM is a costly and resource-intensive proposition. Few organizations have the time or expertise to configure a SIEM system to collect security data from across the environment and analyze it in context. Once the system is in place it requires ongoing administration and monitoring.

Managed SIEM services can simplify this process and help organizations take full advantage of SIEM capabilities. Organizations gain a cost-efficient, cloud-based service that enables them to quickly detect and respond to cyberattacks.

ABOUT SAGENET

SageNet is passionate about trusted connections. The company believes that by creating, discovering and nurturing trusted connections with its customers, associates and community, SageNet enhances the world that connects us all.

As a leader in managed network and cybersecurity services, SageNet connects, manages and protects technologies and devices across the enterprise. SageNet's collaborative approach provides peace of mind and systems-confidence that empowers an organization to focus on its core mission.

The company offers world-class service and support via its three US-based 24/7 Network Operations Centers (NOCs) and Security Operations Centers (SOCs), geographically-diverse teleports, a central National Logistics Center, multiple data centers, and a nationwide field service organization.

With a three-decade track record in managed services, SageNet boasts a long-term customer base that includes the nation's largest retail, healthcare, financial, utilities and energy organizations. SageNet manages communications at more than 220,000 endpoints. Headquartered in Tulsa, SageNet has regional offices in Washington, D.C., Atlanta, Chicago and Philadelphia.