Top 5 SIEM challenges for the midmarket

SIEM is like clockwork—it needs constant "winding"

For every dollar you spend on SIEM, you need another three dollars to manage it.

- Requires full-time security experts
- Complex to deploy and operate
- High and unpredictable costs
- Lengthy time to extract value
- High customization to meet compliance needs
- Slow reporting
- Cost/security tradeoff
- Alert fatigue

For a decade, Security Information and Event Management (SIEM) tools have represented the gold standard in enterprise security. SIEMs offer a single pane of glass for an entire organization's security posture, monitoring logs, aggregating data, and providing alerts to security staff. When integrated with a team of experts into a Security Operations Center (SOC), a SIEM functions like a finely-tuned clockwork watch.

But like clockwork, a SIEM requires constant "winding" and maintenance—staff to monitor alerts, staff to customize the SIEM tool, staff to update definitions and maintain security in the face of evolving threats. This complexity means SIEM may not be the best fit for mid-market companies.

SIEM challenges include:

Need for full-time security engineers

SIEM tools need active, continuous tuning to ensure that you are getting actionable results. A SIEM generates thousands of alerts and notifications which must be acknowledged, investigated, and, if they are attacks, defeated and remediated. Managing a SIEM and the associated agents and log sources is a full-time job, which requires several full-time trained security engineers.

Complexity to deploy and maintain

A SIEM has a long deployment cycle, varying from 3 to 6 months, with a high risk of failed deployments. A long and labor-intensive deployment cycle means high upfront costs, and an extended period during deployment where security is not actually in place. Furthermore, filtering algorithms, correlation rules, and parsing from new event

AWN CyberSOC Advantages

- Concierge Security Engineer who understands your business risks
- Predictable cost through fixed monthly subscription
- Improved security posture with actionable results
- Turnkey solution delivers value within 60 minutes

sources need constant tuning and updating to perform against new threats, increasing the ongoing costs of a SIEM.

Cost of associated data

For a SIEM to be effective, it needs a high volume of security data from every possible source, in real time. Of course, this high-velocity flood of data creates an enormous demand for speed and bandwidth, imposing additional hardware and maintenance costs. Furthermore, SIEM usage can be unpredictable. To maintain security, a SIEM solution must be architected to meet the highest possible volume of incoming events. The best practice is to double infrastructure estimates to provide necessary headroom, but this imposes a serious additional cost burden.

Trade-offs between security capabilities

A SIEM needs the full set of logs from a variety of sources in real time. Each of these requirements imposes a different requirement on architecture: depth, breadth, and speed. A majority of SIEM vendors use the same engine for collection, correlation, search and reporting. However, this means that reporting may be slow, limited to recent data, or unable to cover the full breadth of sources.

Gap between SIEM functionality and actual security.

Once a SIEM solution is in place and performing to its benchmarks, it is tempting to think that the job is complete. However, that is not the case. The ability to perform a search does not automatically provide security. Instead, security teams need to have a clear understanding of possible attacks, and subscribe to a wide range of ongoing updates to a variety of threat intelligence data, in order to make effective use of the SIEM tool.

What you need is a SOC-as-a-Service

SOC-as-a-Service is a managed detection and response solution that avoids all of these challenges and provides prompt, actionable, and affordable security to the midmarket. Arctic Wolf Network's CyberSOC combines a proprietary SIEM with the people and process needed for effective threat detection and response. It uses cloud infrastructure and a scalable, security-optimized architecture to enable immediate deployment and break the tradeoff between security depth, breath, and speed. And it provides the security expertise that IT-staff in mid-market companies sorely need, to identify advanced threats that can impact their business.

ARCTIC WOLF

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com