Top 5 SIEM challenges for the midmarket

SIEM is like a bike, needs constant pedaling...

Security Information and Event Management (SIEM) is a great tool that can protect your organization, when implemented well. SIEM is believed to be a core foundation to build a Security Operation Center (SOC). Its popularity is despite the fact that there are no major regulations suggesting to use SIEM.

Challenges of SIEM:
• Need full time resources
• Complex to deploy and operate
• High and unpredictable costs
• Failed promises in deployment
• Reporting is painfully slow
• Trade-off between cost and security posture
• Security is not searching
• SIEM alone is not enough

However, SIEM is like a bike that needs constant pedaling while looking out for traffic and people. In fact, it is an uphill biking that stops when you stop pedaling. Security is a complex problem to solve, but SIEM makes it even harder. Let’s examine why SIEM can be a bad choice for mid-market companies.

Full time engineering resources

SIEM needs active 24x7 monitoring. It generates thousands of alerts and notifications that need to be acted-on or acknowledged. You would need highly skilled resources with deep security expertise. Managing a SIEM, agents, and log sources is a full time job that needs dedicated resources.

Complexity

Security is a hard problem to solve, but SIEM makes it even harder. SIEM has a long deployment cycle that leads to many failed deployment projects. The rules, algorithms, and agents need constant tuning, updating, and managing. SIEM generates a large volume of alerts and notifications. It requires 24x7 just to look at SIEM alerts. In addition to SIEM, you need to have prevention and response strategy.
Benefits of an AWN CyberSOC:
- A concierge Security Engineer who understands your IT & business
- SOC-as-a-Service operational in 60 minutes
- Managed detection and response
- Improved security posture
- Protect breaches through early detection and quick response
- Predictable OpEx through fixed monthly subscription
- Threat and vulnerability management
- Security compliance monitoring

Cost
SIEM needs 3Vs of security data namely volume, velocity, and variety. The quality of alerts are based on the volume of data pumped into it from a variety of sources, in real-time. So this creates a big data problem quickly with SIEM on how to manage the 3V’s of the data. There is a cost associated with each of the 3V’s making SIEM unpredictable and potentially much more expensive over time. Also, as a best practice, many vendors design a factor of safety of 2x to deploy SIEM. It means that you are paying for redundancy upfront. This makes SIEM more expensive to acquire in addition to the hefty support and maintenance fee for every year of operation.

Over-promise, under-deliver
SIEM needs all of the logs (depth) from a variety of log sources (breadth) in real-time (speed). A majority of the SIEM vendors use the same engine for collection, correlation, search, and reporting. You often need to trade-off between the breadth, depth, and speed of data collection. It means that you need to trade-off between cost and security posture. The reporting is painfully slow and works only on short term data.

Security is not searching
SIEM does the correlation and analysis of events to detect anomalies and threats in real-time. This needs normalization and categorization of security events from disparate devices. Doing multiple searches does not help you with threat detection. You actually need to know what you are searching for which beats the purpose of anomaly detection.

What you need is a SOC-as-a-Service
A cyber security operation center (SOC) provides you with an end-to-end security focused on threat detection and management. SOC-as-a-Service is a security service delivered as a managed detection and response (MDR). This service removes the burden of figuring out as to what is the best methodology or technology for threat detection and response capability. AWN™ CyberSOC delivers security operations center (SOC)-as-a-Service focused solely on threat detection and cyber security incident response. AWN CyberSOC has all the necessary human and machine intelligence to collect, aggregate, correlate, analyze, report, and store your security data in real-time to detect & respond to threats instantly.

Arctic Wolf redefines the economics of security
Arctic Wolf Networks is redefining the economics of security through an affordable, turnkey SOC-as-a-Service solution that deploys in less than 60 minutes. With a designated Concierge Security Engineer™, a proprietary cloud-based SIEM, 24x7 monitoring, incident response, vulnerability scans, and a tailored escalation & ticketing process, AWN CyberSOC provides an end-to-end security monitoring at a fraction of a cost of a security engineer.

Despite significant investments in network and application security, many companies continue to experience costly and damaging security breaches. A SOC-as-a-Service managed security model augments the current network security tools with continuous monitoring, detection and response for threats.