

To SIEM or Not to SIEM

For every dollar you spend on SIEM, you need another 3X to manage it.

Modern businesses operate under constant cyberattack. Cybercriminals of every type continually launch ransomware, viruses, phishing, and denial-of-service attacks that threaten your computer systems and network infrastructure. That puts your IT and security teams always on defense, without the time and expertise to proactively detect and respond to advanced threats. And when you are on defense, just a single mistake can lead to devastating results.

Organizations of all sizes are at risk, and need to protect intellectual property, personal identifiable information, and other sensitive data from being compromised or stolen. For instance, the much-publicized cyberattacks of 2017 include the Equifax breach, where the personal data of 145 million people was stolen, and ransomware attacks such as WannaCry and Petya that targeted more modestly-sized firms across the globe.

To ensure data and sensitive information always remain safe, companies need to develop cutting-edge security strategies that use a security information and event management system (SIEM). A SIEM is a core technology of a security operations center (SOC) commonly understood as a dedicated team of security experts using a diverse range of advanced tools to thoroughly monitor a company's systems and network infrastructure for attack threats, including those of malicious insiders. Unfortunately, neither SIEMs nor SOC fit within the budgets and means of many companies, at least not when they need to buy an entire solution and staff it themselves.

This whitepaper takes a deep dive into the pitfalls of SIEMs, and describes several alternate strategies that ensure the same level of security while limiting downside risk.

Why Do You Need a SIEM?

Security information and event management (SIEM) software is a foundational component used in a SOC. It is a collection of tools that provide a combination of security information management (SIM), also known as log management, and security event management (SEM), also known as the correlation engine. By integrating these two capabilities, a SIEM offers actionable intelligence derived from a high volume of diverse log data collected from various endpoints (laptops, desktops, servers), security devices (firewalls, intrusion detection/prevention services), applications, databases, and network elements (switches, routers).

SIEM Features:

- Collects and aggregates log data
- Parses logs to output structured events
- Correlates events for further analysis
- Enables collaboration among security operators, analysts and incident handlers

What a SIEM Can Do:

- Search and filter based on source/destination IP addresses, users, event type
- Tell who did what, where, and when with pre-defined correlation rules for known attack vectors
- Generate audit-quality log reports for compliance

What a SIEM Can't Do:

- Identify unknown (zero-day) attacks for which correlation rules do not exist
- Prioritize attacks based on human intelligence and intuition
- Manage itself without constant care and feeding by security experts

A SIEM serves as the nerve center or the “single pane of glass” for security, allowing the SOC team to monitor events and prioritize incidents across a company’s entire IT infrastructure. Implemented properly, a SIEM is part of the set of security controls that Verizon’s Data Breach Investigations Report identified as capable of stopping 97% of attacks. However, implementing a SIEM is not for every organization. It is costly, complex, and time consuming. What’s more, a half-implemented SIEM can be even worse than none at all.

What to Watch Out for: SIEM Risks and Downsides

A SIEM can be a powerful tool to detect cyberattacks and insider threats if it is well architected, fully implemented, and finely tuned. But a SIEM’s success depends on much more than selecting the correct piece of software. It also relies on the skillset of those who continuously manage it, as well as the best practices used to do so. For companies with limited budgets and staff with limited security skills, implementing a SIEM from the ground up can be a poor strategic choice for reasons that include performance, cost, staffing and resource requirements, and others.

Required! Full-Time Security Staff

A SIEM depends on full-time dedicated security engineers from the moment planning begins. This is true regardless of what type of SIEM is used; an on-premises SIEM, cloud SIEM, managed or a co-managed SIEM, all have the same requirement. In fact, experts estimate that for every dollar spent on a SIEM tool, companies spend three times as much managing it.

The planning phase includes several steps. Here is where you define security objectives and design security architecture. You also need to identify security devices, Internet of Things (IoT) devices, laptops, business critical servers, databases, and applications from which log data will be collected. During this phase, you determine the business-critical network segments that need to be monitored, and build parsers to convert all log data to structured data, which can then be filtered based on fields. Each step requires engineering expertise.

The security engineers’ role only increases during actual operations. They continually build and refine correlation rules that subscribe to the latest threat intelligence data, which helps identify the latest attack vectors. In general, operating a SIEM on an ongoing basis requires two or three security operators (level-1), security analysts (level-2) and incident responders who take actions to contain and mitigate threats.

When a SIEM is in place, it generates thousands of alerts per day, the great preponderance of which are false positives—alerts that are mistakenly identified as threats. Security engineers must sift through this confusing clutter and determine which alerts require investigation. Many that are investigated, in fact, require no immediate action, but others will represent ongoing attacks that require full attention and rapid remediation.

To optimize the SIEM—and detect anomalous behavior and identify the latest zero-day attacks—user and entity behavior analytics (UEBA), machine learning, and additional threat intelligence feeds (via subscription) can be layered on the base SIEM product at additional costs. Nonetheless, these alerts must still be analyzed by a human engineer to sort out false positives from high-priority alerts.

In fact, a typical security analyst takes about an hour to acknowledge and act on eight to ten security events. An organization with two-hundred users may produce an average of one-hundred critical alerts per day—enough to completely occupy two full-time security experts. What’s more, an additional expert is required to update and manage the SIEM, agents, reports, and security integrations.

Complexity Wherever You Look

Every stage of SIEM implementation imposes its own layer of complexity.

Deployment: A SIEM is known for its long deployment cycles, and only functions effectively when connected to sufficient information sources. While an initial deployment may sound simple—i.e., just connect the SIEM to raw log sources and run searches over the resulting log corpus—it rapidly grows more challenging. Once your team deploys agents and activates normalization engines that convert raw logs into structured data, unanticipated mis-categorizations are common. Deployment cycles can run up to 12 months, and failed deployments are not infrequent. The upshot? During this entire extended deployment period, your company is not fully protected by its new SIEM.

Administration: A SIEM requires constant tuning. This goes for rules, algorithms, and agents. Rules must be regularly updated, and vendors frequently issue patches and updates for device and endpoint software. Each time this happens the agent needs to match the supported version or risk getting thousands of false positives.

Operations: A SIEM generates a large volume of alerts and notifications. It requires 24x7 monitoring and response to efficiently and promptly process all notifications. Major breaches, such as the Target breach, have occurred despite SIEM alerts. In Target's case, the security team had become overwhelmed, the SIEM dashboard was too full of notifications, and indicators of a serious attack went unnoticed.

Now add misconfiguration or version interoperability problems between your SIEM and your devices, and false positives increase by thousands. In this situation, companies generally ignore alerts and notifications until the false positive issue is completely fixed, but this leaves them vulnerable.

Costs Can Escalate

Variety, volume, velocity: SIEMs perform best when they have real-time access to multiple high-volume data sources. However, delivering this data rapidly imposes additional costs. SIEM vendors typically charge on a consumption-based model that accounts for the variety of devices from where log data is consumed, or the volume/velocity of log data as measured in events-per-second. These variety- or volume/velocity-based pricing models force companies to balance the protection and visibility they desire against their available budget.

Because of separate costs associated with data volume, velocity, and variety, these SIEM pricing models are unpredictable. Indeed, the number of devices and volume of logs can grow substantially over time, which locks you into greater expenses in the future.

Over-engineered, over-priced: SIEM pricing revolves around log data consumption. While such data already sees spikes during certain periods of the day or certain seasons of the year, during an incident or attack your system may generate two to three times its ordinary volume of data. The best practice, therefore, is to design a SIEM that can handle at least twice its ordinary workload.

A SIEM Product Includes:

- Collector pricing, based on number of event sources, or volume of events/second
- Parsers for each event/log source—devices, systems, applications, databases
- A sample set of correlation rules that need refining
- Sample compliance reports that need to be customized
- Limited threat-intelligence data—malicious IP addresses, URLs, etc.

At an Additional Cost:

- More device/log sources for greater volume of log data
- User and entity behavior analytics
- Additional threat intelligence feeds—Snort signatures, CnC sites, Tor network sites, compromised devices/accounts

Such over-engineering, although necessary to keep your SIEM from failing during times of attack, imposes high costs. When you adopt a SIEM, you often pay for the level of security you need on your company's worst day—but you pay for it for every day your SIEM is in operation.

Unpredictable costs: SIEM vendor estimated pricing is just that—an estimate. Over time, the number of logs and volume of collected data varies considerably as devices change, patches are released, and new systems are added to the network. This makes medium-term budget planning exceedingly difficult and often much costlier than originally expected.

Underperformance Is All Too Common

Multi-tasking: A SIEM is constantly multi-tasking. It requires the full set of logs from a variety of log sources in real time, and a majority of SIEM vendors use the same engine for log ingestion, correlation, analysis, searching, and reporting. If you use the same engine for all functions, the different functions interfere with one another. For example, performing a search or running a report pauses collection and other non-critical functions. This is one reason why in-house SIEMs are unable to deliver their full functionality at full performance at an acceptable price point.

Fork-lift upgrades: Typically, your SIEM vendor supplies hardware, and sells different classes of hardware to ingest, parse, and analyze/correlate a maximum capacity of log data. When you reach max capacity, you need to perform a fork-lift upgrade to the next-higher capacity SIEM platform. This can be very expensive, doubling or tripling the cost of your original SIEM.

Painful reporting delays: A SIEM is designed to analyze real-time data from across a network's devices. It can detect anomalies and threats quickly, but reporting is usually defined as a non-critical function, and performed on only one or two weeks of data.

In addition, SIEMs usually deliver poor reporting performance. Dedicated log management tools are required for quarterly reporting, and multi-year reports necessitate a third-tier architecture, such as a big-data security analytics product.

Frequent false positives: because a SIEM is so carefully calibrated, a minor change in the configuration of agents or log sources typically generates a large volume of false positive reports. This consumes staff time and resources.

In the End: An Incomplete Solution

While a SIEM provides a great foundation for cybersecurity, it fails to provide organizations with a truly holistic solution.

Security is more than search: A SIEM requires normalized and categorized security event data from disparate devices to successfully correlate and analyze events in real time, and detect anomalies and threats. Forensics analysis can be performed faster with alert data that is categorized by alert type—failed logins, malware executable, malicious URL, command-and-control traffic, etc. In addition, it demands specialized security expertise and insight to identify threats that can bypass traditional defenses.

Raw vs structured data: Log data in the form of raw syslog records can be readily ingested by a SIEM. This raw data, however, needs to then be parsed and converted to structured data that can be analyzed by a correlations rules engine.

Forensic investigation and compliance reporting requires both raw and structured data. SIEM vendors often focus on just one of these categories, leaving them lacking in the other. The result? Many popular SIEM products can't perform effective forensics and reporting on raw data.

Open-source solutions: open-source SIEM tools may appeal to budget-conscious organizations. However, patches and updates don't generally occur on a regular schedule in an open-source environment. That can leave unpatched and known vulnerabilities in your security solution, and expose companies relying on an open-source SIEM to potential attacks.

Marketplace risks: Some SIEMs have open APIs, which means anyone can build and post security applications to their online marketplaces. These apps are often untested or uncertified, and don't represent a recommended security practice.

A SIEM Alone Is Not Enough

You can overcome some of these challenges by investing vast amounts of time and money into a SIEM. But for nimble, budget-constrained organizations—which is most organizations these days—that isn't a viable option.

Even when a SIEM is fully working and optimized, the sophisticated and evolving attacks of today's threat landscape make a SIEM on its own not enough to combat present and future attacks. To do so effectively, you need a SOC with 24x7 network security monitoring.

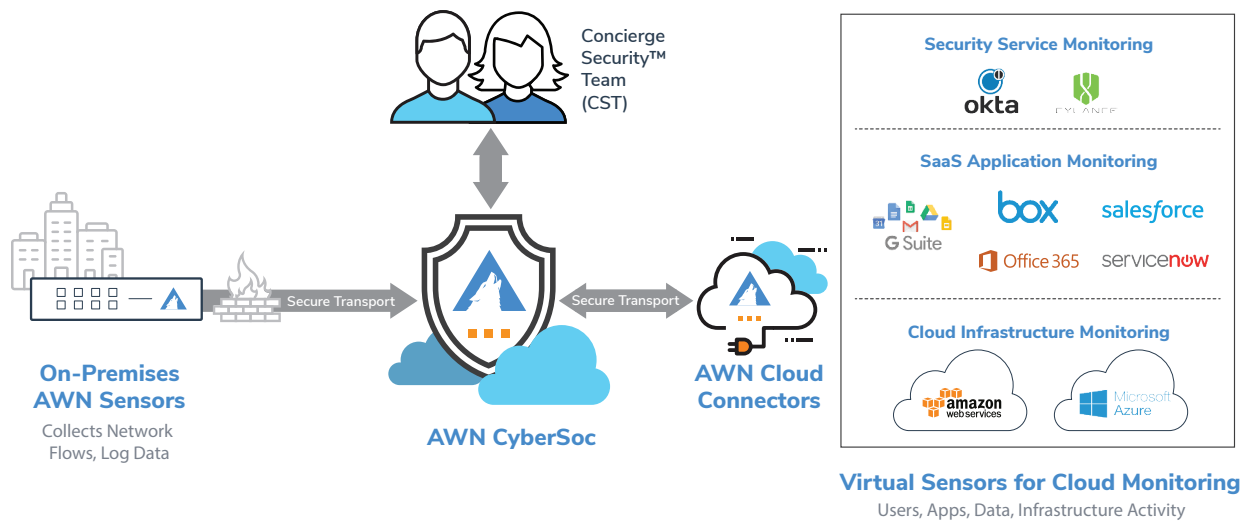
Building a SOC, however, is complex, costly, and time consuming. In addition to purchasing and deploying your own SIEM, you also need to train and develop an expert security team and implement strategic security processes.

SOC-as-a-service: A SIEM is a powerful tool. But it cannot deliver security on its own, and it is often too expensive and too demanding a choice for an organization with a limited budget for in-house security expertise. Fortunately, there are affordable solutions that combine people, processes, and technology in a single offering to meet the full set of security needs.

SOC-as-a-service delivers comprehensive, end-to-end security for companies on limited budgets. It enables you to out-source your needs while enjoying the benefits of a security service focused on threat detection and incident response. Plus, it's an affordable alternative for many organizations since it doesn't require investment in additional hardware, software, or staff. Easy to deploy and manage, it offers the people, process and technology needed for running a SOC.

PEOPLE	PROCESS	TECHNOLOGY
• Named security team • Security expertise on your IT-team • A virtual SOC analyst and trusted advisor	• Standard operating procedures and service level agreements • Escalate incidents via trouble tickets • Bi-weekly and monthly reports	• External vulnerability scans • Managed detection and response • Compliance reports

AWN CyberSOC™ Service



Arctic Wolf Networks offers the industry-leading SOC-as-a-service that protects your IT infrastructure and resources wherever they reside, including on-premises, cloud infrastructure and SaaS applications. The AWN CyberSOC™ Service can be deployed in less than 60 minutes, and offers:

- **Concierge Security™ team** named per customer, who customizes security policies based on your business specific needs, and provides scheduled reports on open/closed incidents, unpatched vulnerabilities, and top attack sources and targets.
- **Predictable pricing** that does not change based on the number of log sources or the volume of log data ingested. Our pricing is simply based on the number of employees, the number of servers, and the number of customer sites.
- **Hybrid-AI** uses human-assisted machine learning to provide 10 times better threat detection with 5 times fewer false positives than a typical SIEM. It uses machine scale efficiency in a cloud-based multi-tenant architecture to process an unlimited number of logs.



CONCIERGE SECURITY™ TEAM

- Named primary contact
- Phone/email/text support
- Understands your network infrastructure
- Proactive threat hunting
- Forensics analysis



THREAT TRACKING AND ALERTS

- 24x7 network monitoring
- Log storage and analysis
- Tailored communication and escalations
- Defined SLAs and SOPs
- Recommended actions
- Compliance controls monitoring

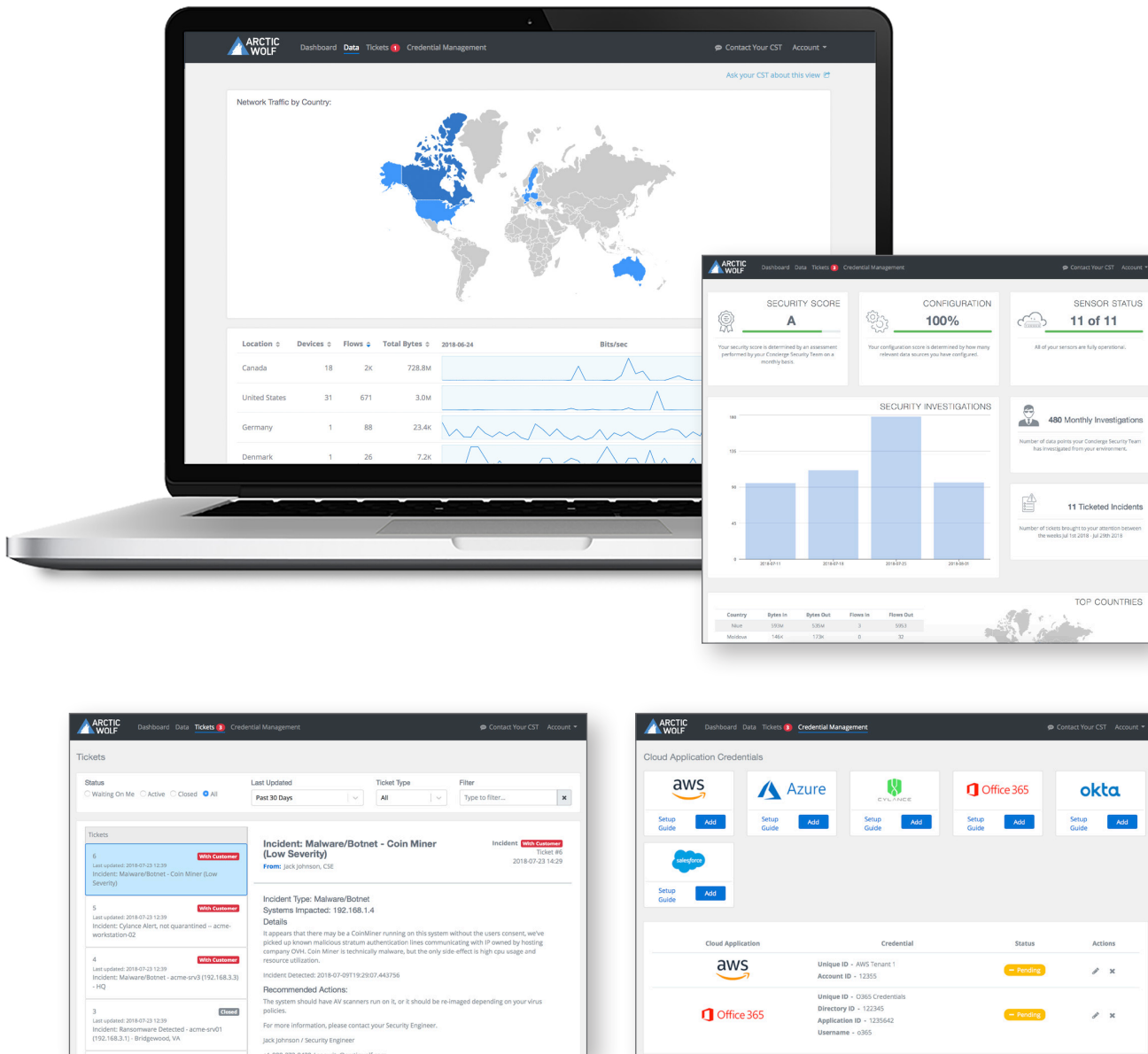


BEST-OF-BREED TECHNOLOGIES

- Deploys in less than 60 minutes
- Cloud-based multi-tenant SIEM
- Real-time threat intelligence
- External vulnerability scans

Arctic Wolf Networks' SOC-as-a-service redefines the economics of security. AWN CyberSOC service is anchored by Concierge Security™ teams and includes 24x7 monitoring, custom alerting, and incident investigation and response. There is no hardware or software to purchase, and the end-to-end service includes a proprietary cloud-based SIEM, threat intelligence subscriptions, and all the expertise and tools you need for a fully comprehensive security solution. For more information about AWN CyberSOC, please visit arcticwolf.com.

AWN CyberSOC Customer Portal



©2018 Arctic Wolf Networks, Inc. All rights reserved. Arctic Wolf Networks, AWN and the Arctic Wolf Networks logo are trademarks of Arctic Wolf Networks, Inc. in the United States and/or other jurisdictions. Other names used in this document are for identification purposes only and may be trademarks of their respective owners.



SOC2 Type II Certified

Contact us

arcticwolf.com
1.888.272.8429
info@arcticwolf.com

