TOP 5 SIEM BEST PRACTICES



Though ubiquitous in information security today, the term SIEM (security information and event management) was coined by Gartner in 2005—just 16 years ago! Since the scope of this article is to suggest best practices, it will not go into depth of what SIEMs can and should do. As security professionals might tell you, it's not what the tool claims to do ("You'll see the rats scurry away once you turn on the light!") but rather how thoughtfully it is implemented, the extent to which it is mastered, and how it is leveraged.

Here are five best practices for SIEM users:

1. Clarity of strategy—more money more value? Not quite

The appeal of managed security services (MSS) and "security in a box" seems too good to be true. After all, who wouldn't want to meet compliance requirements through a single purchase?

Let's use the fictitious Acme Corp. as an example. Acme's chief information security officer (CISO) mandates that the company must decide upon, install, and maintain a SIEM to meet compliance requirements. Perhaps this is what the board demands, and showing timely results is priority number one. Moreover, the CISO stays up at night thinking about their next audit and a lack of visibility into their environment. With this kind of pressure, a conveniently managed, do-it-all monitoring solution sounds perfect.

A fictitious security vendor, Miracle Security, makes a compelling case to Acme. Miracle claims that its OOTB (out of the box) SIEM solution will provide the analytics, alerting, and compliance reporting

Acme requires. On top of that, Miracle will add its MSS (third-party security support) and administrative support to maintain the platform. However, what the CISO and the security team don't realize is that this "administrative" support might mean that Miracle is the only ones with the knowledge and capabilities to access and troubleshoot the backend—for an additional fee.

Acme's CISO is sold and informs the security team that the security operations center (SOC) will cooperate with Miracle to stand up and leverage Miracle's proprietary SIEM, cleverly named "Magic."

A massive initial effort is undertaken across the enterprise to ingest every possible data source into Magic. The mentality is: more is better—more data sources, more visibility, more alerts, and more investigations.

Once Magic is deemed "operational," it has hundreds of data sources of differing types. The SOC has a handful of analysts who have varying levels of familiarity with Miracle, but ultimately they have not been sufficiently trained on how to improve Magic or the countless complex features Miracle pitched in its sales proof of concept (POC).

Alerts begin to flood the SOC. Most, if not all, are low-fidelity. Miracle's MSS complies with its service level agreement (SLA) to raise alerts regardless of accuracy so the organization does not lose "visibility." Also, any time Magic has a critical backend issue (which was conveniently not discussed as a possibility in the POC), Acme must open a support ticket to an overseas team that can take hours or even days to remedy. Analyst burnout becomes common.

And the worst part is that Acme is locked into a two-year contract with Miracle.

While the above example is fictitious and perhaps may even seem extreme, the reality is that numerous security teams believe that spending a significant amount on technology and services will somehow mature the organization overnight.

Sometimes, great things really are free.

2. "Show me the metrics!" (quality over quantity)

To underscore the above, security teams also often fall into "the metrics trap," and for good reason. Leaders must continually and consistently present metrics to stakeholders. Metrics in and of themselves are not negative things. In fact, quite the contrary. Metrics are invaluable**—but rarely measured correctly in the context of, "what will make our security team more effective?"** The motive behind presenting metrics may often lose sight of this and, as a result, become increasingly muddled.

A discussion of metrics is needed because, practically speaking, they are often what drive SIEM implementation and design. Rather than asking, "How many alerts are we generating?" the fundamental question must be, "Are we creating high-fidelity alerts regardless of quantity?" The former focuses on quantity, while the latter focuses on quality.

While the above may sound self-evident to seasoned security professionals, the reality of many SOCs is that this mentality simply does not happen**.** If it did, "alert fatigue" would be far less common than it is today. Simply searching for literature on "SOC alert fatigue" generates numerous articles specific to the topic written by prominent security vendors.

What often prevents security teams from making the shift from quantity to quality is uncertainty—both in terms of visibility and job security.

The mentality often is: It's better to have an abundance of disparate, disjointed visibility than a smaller, high-fidelity amount, right? (The answer is no.)

Moreover, many security leaders fear turning off the hose due to optics—or organizational metrics. How can one say they are doing their job when the alert count went down 80 percent last quarter? Never mind that analysts can now conduct end-to-end investigations with high-fidelity, intelligence-rich indicators of compromise (IOCs) and experience massive professional growth in the process—leaders must still be prepared to explain these changes in "metrics."

In short, security teams need the requisite foresight and maturity to understand that the quality of data (and analytics) in the SIEM must take precedence over visible quantity.

3. Total ownership

Executive leaders, perhaps more than anyone else, understand that risk cannot be transferred. In the example of Acme Corp., I intentionally highlighted that Acme committed to a services contract with an outside vendor for alert analysis and backend administration. While this might seem like the safest and most convenient path forward for many teams, the reality is that the more that control is removed from the security team, the more the team will experience operational friction during both day-to-day and crisis situations.

In addition, the less control the security team has over the data sources that the SIEM requires to be effective, the more difficult it will be to create high-fidelity alerts. In the example I used above, Acme stood up its SIEM with a massive initial effort, which was followed by a "set it and forget it" approach. While this is not always the case, it is often the path of least resistance for many organizations when standing up a SIEM because it is seen as a one-time cost. However, the reality of effective SIEM implementation is that it must be treated as a lifelong commitment, not simply an upfront cost. Too often, security teams realize this too late and are trapped in binding contracts or without the requisite access or personnel to succeed.

Realistically, the security team may not have full control over every asset within the SIEM. However, they should be granted the requisite control and access needed through a shared platform. This could be a security orchestration, automation, and response (SOAR) solution, or even as simple as remote access with limited privileges. Without this, it is impossible to effectively improve the quality of data ingested by the SIEM.

Finally, the security team must own the SIEM as the subject matter experts (SMEs) of the product. Ultimately, the SIEM is the security team's responsibility and the closer the center of control is to the team, the more autonomy and confidence they will experience when leveraging the product.

4. Ingest judiciously (know when to say no)

In a hurried effort to turn the lights on, Acme ingested data sources into its SIEM at a massive scale. The mentality appeared to be one of catch-up, where the faster Acme could claim to stakeholders that it had "full visibility" of the environment, the more secure it would be. Even if a security leader in the organization suggested pumping the brakes and instead focusing on whether the data ingested was high-fidelity, it is quite possible they would have been overridden. However, security leaders of all levels are paid to lead—and this means knowing the right path forward and **when to say no**.

Simply put, Acme's approach was a recipe for SIEM disaster.

A more prudent approach may have been for Acme to master its own island first. The security team could have ingested and mastered their immediate IT ecosystem, using it as a proving ground for the team. Starting from the inside out at an incremental pace will ensure that the SOC does not experience burnout and can grow in both confidence and capabilities at a more manageable level.

Once you are successfully able to manage the basics you can extend your security operations center purview to other critical servers like the mainframe, which run core business applications and commonly don't have the same security continuous monitoring they require.

No artist begins a masterpiece by throwing every color of paint on the canvas and attempting to salvage it afterward. They are masterfully thoughtful, intentional, and creative in how they build their vision.

It's the same with a security team and their tools.

5. Learn by doing

Finally, the best way to leverage any SIEM solution is simply to **master it.** Note this is not the same as "use it," as even a bot can leverage a modern graphical user interface (GUI)-based SIEM in some way.

With the advancement of security tools in recent years, many of them can perform manual and repeated functions in a security analyst's job. This is not simply a SIEM phenomenon. SOAR, endpoint detection and response (EDR), and IT service management (ITSM) platforms all attempt to streamline manual processes as much as possible and present analytics in an easily digestible format. These are all good things that make security teams more effective.

However, any tool is only as effective as its user. SIEMs require regular care and maintenance—and upgrades, when appropriate. Security teams cannot expect to passively reap the benefits of a SIEM without actively seeking to master it. This is how a SIEM can quickly become a deprecated and irrelevant tool in the security team's budget, rather than one integral to enterprise security.

A SIEM is more effective with one "power user" than ten passive users who expect it to simply present data and alerts for triage. It is the responsibility of every member of the security team to become a power user, rather than expect one or two individuals to assume this role.

These are just five principles that can help your organization successfully implement a SIEM solution (if it chooses to do so) in the most prudent manner possible. To learn more about how BMC can help your organization integrate your "backbone of the enterprise" into the SIEM with a tailored and strategic approach, visit the BMC AMI Security web page.