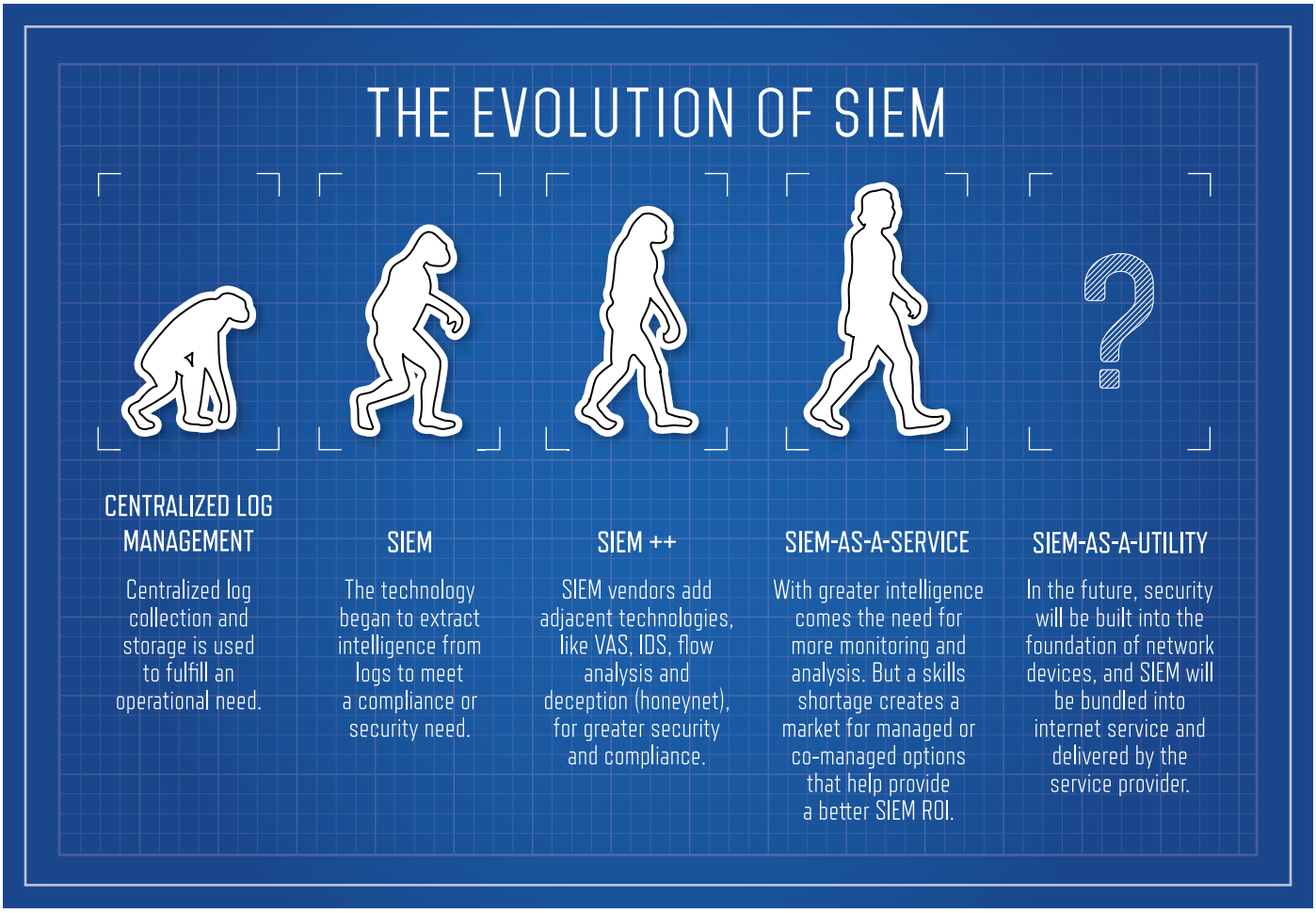
CHOOSING THE RIGHT SIEM SOLUTION FOR YOUR NEEDS

EventTracker
Actionable Security Intelligence by Netsurion

While there is little doubt that SIEM solutions are critical for compliance, security monitoring or IT optimization, it is getting harder for buyers to find the right product for their needs, especially given the number of solutions available and the different options for implementation (e.g., software, hardware, cloud, outsourced and co-managed).

Choosing the wrong solution can be expensive, arduous to maintain, and difficult to staff for constant monitoring, which is why many SIEM installations end up as shelfware.

SIEM solutions, in reality, are optimized for different use-cases and one size never fits all. In fact, the evolution of SIEM and Log Management has seen a shift from using solutions for just collecting logs and meeting compliance regulations, to being a core part of the network security infrastructure.



The good news is that with the number of potential solutions to choose from, if you do your homework, you will find a solution that meets your requirements. So how do you cut through all the vendor claims and hype to select the right solution for your environment and needs?

Define Your Requirements

First, you need to know your requirements. This might seem obvious, but cannot be overstated. Particularly in complex areas such as IT security, buyers can make the mistake of eliminating the ideal solution accidentally because they had tunnel-vision for a preconceived solution instead of first articulating the preferred business outcomes. Look at your requirements in depth and figure out your needs before heading to procurement.

Keeping your objective in mind, consider these areas when drawing up requirements:

Collection – What data sources do you need to log? Do you need real-time collection? Do you need to collect all data or a subset?

Storage – Do you need to archive everything? How long do you need to store data? How long do you need to keep data online?

Compliance – What compliance regulations do you need to meet? Do they require specific functionality, such as regular monitoring, alerting and the ability for automatic remediation? What sorts of reports will you be required to produce?

Analysis – How will you use your data once collected – for legal forensics, detecting threats in real-time, isolating attacks or incidents, or for compliance audits?

Reporting – What sort of reports do you need? Do you want the ability to customize reports?

Personnel – Do you have the expertise on-staff to most effectively use the solution? Or will you need assistance in platform administration, data analysis and ongoing tuning?

Other Considerations – Do you need multi-user access? What level of access should they have?

Choosing the wrong solution can be expensive, arduous to maintain, and difficult to staff for constant monitoring.

Consider Implementation

Once you identify your requirements, educate yourself on the implementation options and features available.

Appliance vs. Software-based Solution – When deciding between an appliance and a software solution, consider the following:

- Redundancy: To protect your valuable IT infrastructure, you will need to calculate a 1xN relationship of live appliances to back-ups. If your appliance breaks down and you don't have a spare, you have to ship the appliance and wait for a replacement. With software, if your device breaks down, you can simply install the software on existing capacity in your infrastructure, and be back up and running in minutes versus potentially days.
- Scalability: With an appliance solution, although it is turnkey, you need at least one device to get started, and it has a maximum capacity before you have to add another appliance at a high price. With a software solution, you can scale incrementally – one IT infrastructure device at a time.
- Single sign-on: Integrate easily with Active Directory or LDAP; same username/password or smartcard authentication.
- Storage: What retention period is best for your logs? Weeks? Months? Years? With appliances, it's dictated by the disk size provided. With software you decide or can use network-based storage.

Scalability – This should be thought of as multi-dimensional, encompassing the following:

- Collection: This is a multi-step process. Receiving an event is not the only part of the process. Events must be processed and data committed to storage, and these activities consume system resources. It is advisable to look at how vendors define scalability for all three activities.

- Storage: Scalability is evident in not just storage size but also how easy it is to move data between online and off-line storage, as well as retrieve and process records. And what happens to archiving when the system gets temporarily overloaded? Do the events get cached or lost?
- Analysis/Reporting: This important aspect of scalability is often ignored. A system might process 10 million events per minute, but if it takes 10 hours to run a query, you are probably not getting a scalable or viable solution.

Co-managed SIEM services enable security and risk management leaders to maximize value from SIEM and enhance security monitoring capabilities, while retaining control and flexibility. (How and When to Use Co-Managed SIEM | Gartner | April 2017)

Services - The increasing complexity of the threat landscape has spawned more complex security technologies to combat those threats. Thus, the importance of the "human element" is more critical in security management discussions than ever before. Today, the choices are either to procure security technology, and hire and train adequate internal resources to use them effectively, or outsource to a provider that is experienced with the selected technology.

There are two models for SIEM-as-a-Service:

Outsourcing/MSSP: Outsourcing security allows organizations to affordably leverage expertise that may not be available internally, but at the cost of losing control. Many providers offer cookie-cutter, one-size-fits-all solutions, which may not meet your specific needs.

Co-Sourcing/Co-Managed: In this model, the provider does the technology-specific heavy lifting and leaves a specific organization's network independent, allowing remediation to be performed by the in-house team. Organizations can also customize the solution and keep data on your premises. Some vendors offer their own co-sourced offerings, while others have a third party manage their software.

SIEM technology delivered as a service offers the opportunity to simplify and reduce the time to implement, administer, maintain and scale, while reducing licensing complexity, compared with on-premise versions.

(Innovation Insight for SIEM as a Service | Gartner | February 2017)

Conduct an Evaluation

After you make your short list, be sure to conduct an evaluation. Without an evaluation you are dependent on the vendor to give you correct information. One of several things can happen during implementation if you don't know what you're getting:

- The solution is unable to scale to your requirements
- The add-ons kill you on budget
- Excessive false positives are generated
- The analysis engine is too complicated to tune and you fail to detect a real threat

- Once you gain experience with the product and tune it to meet evolving objectives, you find the architecture inflexible
- Deployment is a nightmare and professional services are not in the budget
- The features and functionality you really need are hard to use, while the capabilities you were most impressed with, you never actually needed to use

Before your evaluation, be sure to put together your cross-functional SIEM project team that will eventually be a part of the implementation process. Members may include stakeholders from your organizations' legal, operations, HR, compliance and security departments. They can help you define the goals, scope and use cases of the deployment.

Once you've gone through the evaluation process, you should have gotten a feel for the kind of support you should expect to get. Will you be struggling to make it work or helped through the deployment and management process? If you choose to use a SIEM-as-a-Service model, you will hopefully not have any issues. But if you choose to just purchase the software and run it yourself, there's more to consider regarding support and maintenance.

For instance, if you need a new report, will your vendor work with you to develop this? What if you need a custom correlation rule or if you have a new data source that the vendor does not support? Or, what if you have a looming audit and need your vendor's guidance through the process? Ask the vendor these questions. A trusted provider will be willing to give you value-added services without breaking your budget - this can often mean the difference between a good and a great project.

At the end of the day, if you understand your problems, requirements and drivers, and do your due diligence, you should be on your way to a successful project with a product that is optimized for your business problem.

For more information about EventTracker's services, visit EventTracker.com/contact

EventTracker
Actionable Security Intelligence by Netsurion