dlt.com

WHITE PAPER

# SIEM: Value, Compliance, and Innovation

*Written by Don Maclean*
*Chief Cyber Security Technologist*

DLT® | LogRhythm®

# SIEM: VALUE, COMPLIANCE, AND INNOVATION

Conventional wisdom says that demonstrating ROI in cybersecurity is difficult, even impossible.

In real estate, only three things matter: location, location, location. If only cybersecurity were that simple. Even so, it is possible to boil this complex field down to three main elements:

***1) Is it worth the money?***

Does it minimize the true cost of ownership, in both real and hidden costs?

***2) Compliance***

Does this system facilitate compliance, and stay up-to-date with changing requirements?

***3) Foundation + Innovation***

Are the basics solid and reliable? Does the company innovate constantly, as the enemy does?

Let's take a look at security information and event management (SIEM) technology, and explore how these considerations come into play.

## *IS IT WORTH THE MONEY? WHAT IS THE TCO?*

Conventional wisdom says that demonstrating ROI in cybersecurity is difficult, even impossible. CISOs must supposedly rely only on hypothetical scenarios: "This is the horrendous breach that might have happened without this system." Hypotheticals, especially those lacking corroboration, such as an actuarial table, rarely convince those who control the purse strings.

It makes sense, then, to look at total cost of ownership (TCO). If two systems perform similar functions, but one has a much lower TCO, a security professional has a tangible, quantifiable reason to switch products—especially if the alternative is easy to install. SIEM products have notoriously high TCO. Some can take up to two years to master; others "come with an engineer," and many need extensive customization to be effective. Here are some key TCO factors in a SIEM:

### EASE OF USE

Ease of use is not just a matter of convenience. In the tense moments following a breach, every second counts. If an analyst has to wade through complex reports, wrestle with a complex and antiquated user interface, or resolve apparent duplication of data elements such as times and dates, response simply begins to take too long.

Learning a product-specific language or syntax is still necessary for many SIEM offerings, even in 2019. A rich, straightforward Graphical User Interface with powerful dashboards and intuitive workflow can make a significant difference in response times, optimize analyst workloads, minimize training time, and ease personnel transition in shops with high staff turnover.

### TRAINING REQUIREMENTS

Many security programs—especially in the public sector—experience high turnover, and finding well-trained qualified replacements is difficult. Once hired, security analysts wear many hats, and must learn multiple systems quickly. Training is necessary and beneficial, but time and money for training are limited. The need for enablement on multiple technologies can also prove challenging. A SIEM that does not require a Ph.D. to learn and operate makes current staff more effective, and lets future staff get up to speed quickly.

### DEPLOYMENT AND OPERATION

Cybersecurity is a complex endeavor, and cybersecurity systems can be hard to deploy; however, deployment should not require a three-month engineering engagement by the vendor or a third party. Your in-house staff should be able to deploy a SIEM, not only to reduce up-front costs, but also to ensure familiarity with the details of its implementation and configuration.

Some SIEMS have specific infrastructure requirements from other vendors. This approach allows for the use of in-house systems but can also complicate troubleshooting when each vendor points to others as the cause of the problem.

True high-availability and redundancy are also essential for protection. A favorite tactic of an attacker is first to attack the security systems themselves. The attack might disable a system stealthily using a known exploit, or take the form of a distributed denial-of-service (DDoS) attack to distract or disable security systems.

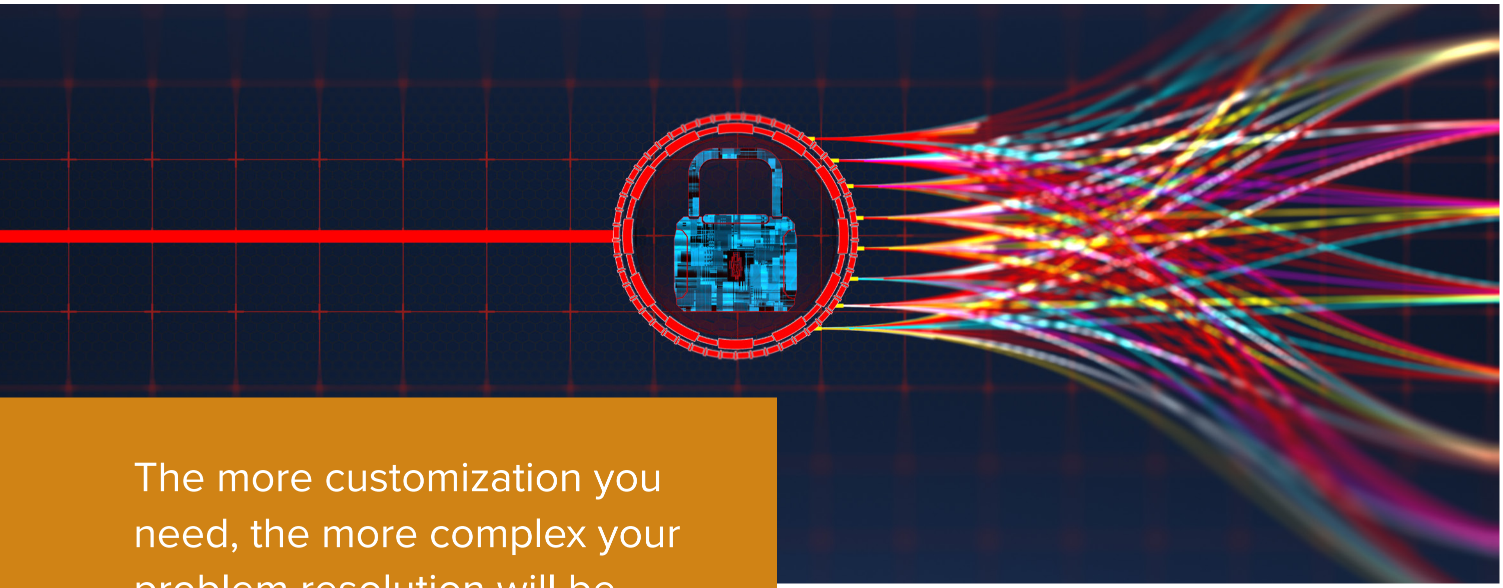
Since the worst time for security tools to fail is during an attack of this type, look for a robust platform that provides resiliency, redundancy, and high-availability. Consider a switch if your current vendor cannot meet this fundamental requirement.

Be careful of upgrades that involve a migration in lieu of an upgrade. Look for self-packaged installers that don’t disrupt major systems. Once installed, a SIEM needs to provide up-to-date content such as compliance reports that match current regulatory and legal requirements. More importantly, it must be reliable. Your security staff has better things to do than monitor problems popping up from “red light” health checks.

Scalability is also key. How often have you heard the phrase, “It worked fine in the lab”? Lab demos and proofs of concept (POCs) are great and essential first steps, but make sure your solution can scale up without additional cost to your production environment. Trust vendor statistics, but verify with real users.

Finally, look carefully at the system requirements like cores, memory, and storage. If you are running an on-premise operation, steep resource requirements could mean costly capital expenditures. If your systems run in the cloud, CPU, memory, and other resources all come at a per-hour or per-minute cost.

# SIEM: VALUE, COMPLIANCE, AND INNOVATION



The more customization you need, the more complex your problem resolution will be.

### TECH SUPPORT

When trouble arises you need help immediately, especially if an attack is in progress. Imagine being in a bank during a robbery and calling 911 - only to hear some horrible music while waiting for the "next available operator" who, of course, "values your business." As absurd as this scenario sounds, it represents the events during a cybersecurity incident. Fast, reliable technical support is a crucial element for a SIEM solution.

Technical support must be fast, effective, and easy to reach. For many government agencies, it must also be provided by U.S. citizens on U.S. soil—a feature only a few vendors can offer.

Technical support is a stressful occupation, however, so look into the vendor's turnover rates. Will a different analyst answer the phone each time, or will you reach someone who already knows your system and understands the problem that needs immediate resolution? Do you have to describe the incident from the beginning each time you call, or do the analysts document and share information effectively?

### DATA ACQUISITION AND CORRELATION

SIEMs correlate data from multiple sources to facilitate threat detection, response, and forensics. Customizing correlation rules is critical to useful correlation, but creating those rules, and ensuring that one rule neither duplicates nor nullifies another, is essential. Too often, SIEM offerings make rule creation difficult and fail to optimize their execution.

Before a SIEM can correlate data, it must provide a means for collecting and parsing. While most SIEMs come with a set of parsers for standard data sources, you may have to request or create a custom parser or collection module if you are using a unique or legacy system. The more customization you need, the more difficult problem resolution will be.  The vendor's tech support staff may not know the details of your specialized parser, and you will have to make sure the tech support staff is up to speed on the specifics.

## COMPLIANCE

In government security shops, compliance is king—as well as a resource hog. It is common to see compliance work consuming 70 percent of a security budget—money that could go to procuring technology or supporting a larger or more expert staff. Support for compliance regimes, then, is a critical element of any security tool, particularly a SIEM.

The venerable Risk Management Framework (RMF) and the Defense Information Assurance Risk Management Framework (DIARMF) dominate the landscape. These take shape in the form of NIST security control requirements, which are spelled out in SP800-53 and periodically updated along with the RMF. In fact, NIST released a major update to the RMF in late 2018, and plans to publish a completely new compendium of SP800-53 in the summer of 2019.  Can your SIEM stay current with these updates? Does it have a mechanism, preferably a simple one, to accommodate future updates?

The RMF and DIARMF are not the only compliance games in town, though. In May 2017, Executive Order 13800 mandated the use of the "other framework," namely the Cybersecurity Framework (CSF) promulgated in 2014. The CSF control set correlates closely with the RMF controls in 800-53.  Does your SIEM support it? The catchy-titled Health Insurance Portability and Accountability Act (HIPAA) also includes a healthy set of cybersecurity requirements. Again, does your SIEM provide reports or other artifacts in support of this regime?

## SECURITY = FOUNDATIONS + INNOVATION

Imagine a beautiful house, filled with the most expensive furniture and decorated by the world's most prominent interior designer. Now imagine that house on a cracked and rickety foundation. A stunning mansion becomes worthless.

Cybersecurity technology is not so different. It has two main dimensions: foundational systems that deal with common, known vulnerabilities and innovative technologies that stay ahead of the bad, but agile actors. The best cybersecurity systems play in both worlds, maintaining solid capabilities for mundane, but essential tasks while constantly innovating in response to new challenges.

> **To be truly useful, a SIEM must have rock-solid basics: fast data acquisition, normalization, correlation, stone-code reliability, and ease of use.**

SIEM solutions started as foundational technology. In the beginning, they were little more than repositories for log files, but they soon began to ingest many other types of data from a much wider range of sources. Normalizing and correlating the data was the obvious next step, but turning data into actionable information is the primary purpose of a SIEM.

To be truly useful, a SIEM must have rock-solid basics: fast data acquisition, normalization, correlation, stone-cold reliability, and ease of use. These features are "table stakes," but they become truly valuable when innovative technology can use them to stay ahead of the enemy.

Does your SIEM vendor exploit the latest machine-learning and artificial intelligence methods to identify and remediate threats? Does the user behavior and analytics

# SIEM: VALUE, COMPLIANCE, AND INNOVATION

To be effective, SIEM must minimize cost of ownership through ease of use.

approach truly identify bad behavior, or does it simply generate a swath of false positives, which your staff either ignores or wastes time investigating?

## *SUMMARY*

A SIEM is a critical piece of technology for providing end-to-end threat lifecycle management and maintaining a solid cybersecurity posture. To be effective, it must minimize cost of ownership through ease of use. Its resource requirements must be as low as possible, but it must be fast and reliable. The company must back its offering with rapid and robust technical support. The system must not force you into no-win upgrade decisions, but instead provide for modernization and innovation that will enable you to stay abreast of changing compliance requirements and remain a step ahead of the adversary.

For more information, contact DLT at **sales@dlt.com.**

dlt.com

DLT®

Accelerating Public Sector Growth for Technology Companies