CYBERSHARK™

CYBERShark WHITE PAPER

# 10 COMMON PITFALLS TO AVOID WHEN EVALUATING SECURITY INFORMATION MANAGEMENT (SIM) SOLUTIONS

Security is everyone's concern, but it’s our business.

WWW.CYBERSHARKINC.COM

# CONTENTS

1

# EXECUTIVE SUMMARY

Choosing a security information management (SIM) solution can be a confusing, challenging process for today's security-conscious organizations. Worse yet, companies often lack the insight needed to make sound choices in a SIM solution – one that will protect their valuable assets today and in the future, and do so cost effectively. Whether talking about SIM, security event management (SEM), or the catchall phrase security information and event management (SIEM), companies know that the objective is to secure corporate data and ensure regulatory compliance. So regardless of the terminology, companies are faced with a daunting task in determining which SIM technology is appropriate for the information security issues they are trying to resolve.

The good news is that there are plenty of SIM solutions on the market. A recent count showed 28 vendors claiming they do some aspect of SIM. In addition, some vendors have multiple products, so companies can find themselves considering 100 different solutions. The downside, however, is that
unless companies understand very specifically what to look for in a SIM solution, they can take on greater total cost to operate (TCO) than necessary for their environment, and more importantly, can come up short in protecting their valuable data and maintaining compliance.

This paper can help companies searching for a SIM solution to narrow their options and assist in determining which technology is the right one for their IT environment and security objectives. The following list of 10 pitfalls organizations make when choosing a SIM product can help prevent companies from making these same costly errors, which can lead to unnecessary security risks, complex implementations, user challenges, a lack of scalability, hidden costs, and more. This list of pitfalls is by no means all-inclusive, but offers useful information that can aid in making the right decision in a SIM solution.

# PITFALL 1:

## Misunderstanding security obligations and needs.

Companies are often confused about the difference between a logging product and a SIM solution, and do not know if they need a SIM solution or if a logging product will be sufficient. This confusion often begins with the typically complex regulatory guidelines, leading to misunderstandings about security requirements. For example, most regulations specifically state that logs must be preserved. As a result, many companies believe that by implementing a logging strategy they can meet their security objectives. However, most of the regulations also require some level of real-time monitoring and incident response. For instance, many believe that Requirement 10 of the Payment Card Industry Data Security Standard (PCI DSS) only requires logging. Yet the requirement states, "Track and monitor all access to network resources and cardholder data."

Many assume the "monitor" portion of the requirement means logging, but because the standard exists to protect cardholder data before it is compromised, real-time monitoring is necessary. Logging, on the other hand, only deals with "after-the-fact" forensics and cannot prevent intrusions while they are happening.

So companies typically need both log management and real-time monitoring. Investing in two products from two different vendors, with each product delivering entirely separate functionality such as logging and real-time threat identification, ultimately requires more IT and budgetary resources to implement and manage than an integrated solution.

A single, integrated platform, such as CYBERSHARK, will provide the logging needed initially, yet also provides real-time threat identification and remediation. With a solution that allows companies to turn on the functions as they can afford and manage them, organizations can better meet compliance obligations and effectively plan for a more secure environment.

# PITFALL 2:

## Choosing a product based on broad promises  rather than architecture details

When comparing SIM solutions, companies should take the time to investigate individual features, which vary greatly from product to product. Take correlation, for example. Many vendors claim their products do extensive correlation, when they actually offer minimal correlation at best. Therefore, companies should research such claims. Organizations must ask important questions such as the following when evaluating a SIM solution, for a better understanding of what the product really offers:

### How extensive are the collectors?

A SIM solution is only as good as the information it collects. Vendors should not only offer broad support for the security feeds they import, but also extensive analysis of that data. Yet logging products often do very little or nothing at all to analyze the events being created. This can result in attacks going undetected and data subsequently being exposed.

### How strong is the analysis of the data?

Though vendors may claim that they “correlate data,” questions remain as to the degree of correlation. When performed effectively, correlation enriches data, taking the raw information, sifting through it, and presenting a prioritized list of risks that need to be investigated or eliminated.

### How does the product mitigate or remediate threats?

ASIM solution should provide the means to an end. It should not only be effective at identifying threats, but should also provide reliable guidance and a sound framework for responding to those threats.

### What type of correlation is being performed?

Many SIM products offer simplistic analysis of security events, such as determining the number of invalid logon attempts to a protected server. Although this can help in identifying some of the more common attacks, it fails to provide any assistance in uncovering the most dangerous threats, such as low and slow attacks that can penetrate and obtain protectedinformation.

### How easy is it to write custom correlation rules that are effective in protecting particular environments?

Every enterprise is different, so individualized protection is crucial. In most cases, SIM products either do not offer customized rule creation or creation of these rules is cumbersome and ineffective. Rules- based correlation is extremely important in ensuring that a security posture is as tight as reasonably possible.

# PITFALL 3:

## Choosing a product that will not scale to meet future needs.

Most companies evaluate a SIM solution based on how they need to deploy it today, but fail to consider how the product will need to evolve down the line. In addition, vendors often estimate the size of a company's deployment based on a subset of the events that will be used during the proof of concept (POC) trial. During the POC, the vendor scales the system to minimize initial costs and offers an attractive deal. Then, when the system is moved into deployment, the customer unfortunately finds the performance unacceptable. To rectify this situation, the customer has one of three choices:

1. Add more technology from the vendor to achieve the desired performance: **This can be expensive and time consuming, since a modification of the entire deployment architecture may be required.**

2. Add hardware that was never proposed **This will greatly increase the cost of the deployment.**

3. Rip and replace the product with another solution. **This can discredit the decision makers who recommended the solution in the first place. Additionally, this adds significant cost and time to the road to a secure environment.**

**Products should not only scale vertically to eliminate the potential consequences noted above, but also horizontally. As attack vectors increase and become more sophisticated, more and more security-related information needs to be analyzed. Adding additional devices due to a lack of solution scalability is one problem, but needing to add different types of security information such as data-level or physical security can create an entirely new type of challenge for products that are not architected properly. Products must be able to address both types of scaling issues to effectively meet security and budgetary goals. Due to these and other issues, companies should thoroughly map out their security strategy prior to any purchase decisions. They should also insist that vendors show what the hardware requirements will be when all required devices are hooked into the SIM solution. The vendor should be able to provide some guarantee that their estimates are accurate, to eliminate any unexpected requirements following deployment. Vendors should also be able to explain how new collectors can be added for devices without native support.**

**Companies should also expect the vendor to demonstrate how easy it is to add non-perimeter type device events into the SIM solution. Companies should focus on products that already offer integration points to systems such as database monitoring, configuration management databases (CMDBs), helpdesk systems, vulnerability scanners, and so on, since they have already shown support for a broader range of security-type information.**

**By choosing a product that will scale as needs scale, companies can maximize their investments while minimizing any hidden costs. Protecting a SIM investment once a decision is made can help achieve security and compliance objectives while strengthening thecore business.**

# PITFALL 4:

## Selecting a product that fails to collect and correlate enough information to achieve the desired security goals.

SIM started out as a way to reduce false positives primarily with IDS/IPS and firewalls. Then SIM expanded to include other perimeter devices. But as the perimeter solidified, criminals found new, innovative ways to gain access to data. Now, many different types of security information are required to achieve the same level of security previously achieved by simply analyzing firewall logs.

When evaluating a SIM solution, companies should choose a product that not only can handle the voluminous amounts of traditional security events, but can also collect, interpret, and alert on all types of events occurring across the enterprise. As attack vectors become more sophisticated and criminals improve on stealth tactics, more analysis is required across more sources in order to secure enterprise wide data. For example, unauthorized access to information is a growing issue that IT departments face today. Therefore, SIM solutions must regularly collect new types of events to accurately assess the threats facing critical data. However, this requires more than simply analyzing perimeter data or database activity. The solution must analyze both to get an accurate picture of what is going on within the network. Once a criminal uses aggressive methods to penetrate the network perimeter, they can easily access the critical application layer data when inside. Looking only at perimeter events may not detect the intrusion. Once inside, nothing will trigger the unauthorized access alert if a valid user id/password combination is used, which the criminal could have obtained either through the brute force network intrusion or through social engineering.

A solution that looks at both perimeter events and database activity provides the level of granularity needed to thwart data loss. By collecting all types of security data – from the perimeter to the core – companies can uncover both low and slow attacks as well as the more blatant security attacks.

# PITFALL 5:

## Focusing on the compliance checkboxes and not the security.

With the many detailed, complex security regulations pressing organizations for compliance, companies often find themselves focusing on the line items in the regulations rather than the security objectives underlying them. In fact, many companies spend hundreds of thousands of dollars trying to meet their compliance mandates and yet still leave their data exposed. This is especially true for companies governed by more than one regulation. Regulations can contradict one another, plus typically offer detailed instructions in some areas with more general instructions in others. So trying to determine which measure should be taken to meet which control can cause confusion and frustration. However, all of the security standards were created for one purpose: to secure the environment and to protect the elements within that environment. Companies should focus on security. If a company dedicate resources to securing their environment, using the mandates as a guideline, then compliance will follow.

Logging serves as a great example here. Too many times companies will implement a logging strategy since it is the most clearly spelled out in the regulations. Yet at the same time, they ignore the greater importance of real-time threat identification and remediation. Then, when a breach occurs, they are surprised that they were vulnerable and even more surprised when fines are levied. Again, it is important to remember that the purpose of the regulation is to secure that data. Of course, part of the regulation is concerned with “after-the-fact” forensics to analyze security events. However, the regulation and the governing bodies are more concerned with preventing the breach from occurring in the first place. Doing one without the other is not enough. By focusing on security and not simply the regulation, companies can increase their security posture and comply with regulatory mandates.

# PITFALL 6:

## Focusing on the symptom rather than the cure.

1. As discussed earlier, assuming that data retention and logging are enough to meet security and regulatory objectives.

2. Assuming that threat identification is sufficient.

Identifying threats against the network and the information held within is only the first step in achieving a secure environment. Without question, being able to quickly identify threats, and in real time, is a necessity. However, choosing a product that also offers help with stopping the attack is just as important as identifying the risk. Security is about securing an organization's assets, not simply knowing when they are exposed and under attack. By focusing on both identification of threats as well as stopping them, companies can ensure a more secure environment with less compromises while achieving all of their security compliance objectives.

# PITFALL 7:

## Choosing a product that can only be leveraged by a few individuals.

In most cases, SIM products are used by multiple people in different settings. Some companies have network operations centers (NOCs) with operators dedicated to monitoring the network infrastructure. Others also have security operations centers (SOCs) that are specifically tasked with managing the enterprise’s security posture. Some companies use a combination of both.

The challenge is to ensure that any SIM product deployed can be leveraged in many different settings and can accommodate many different skill levels. Companies should evaluate a SIM solution carefully, balancing ease of use with the right level of data collection and sophisticated analysis to secure the enterprise.

Ease of use is important, but companies should be cautious if it seems to be the fundamental benefit offered by the SIM solution, since important functionality might be lacking. Conversely, a product that provides all the details and workflow needed to address security concerns yet comes with a steep technology learning curve can stifle usability while failing to support rapid response. Instead, companies should only consider products that offer both ease of use for the front line operators but provide the important tools needed for the security analysts to ultimately resolve security issues.

Evaluation criteria should include how the product looks from an operator’s point of view. The ability to easily diagnose problems once they have been identified is also imperative. The SIM solution should offer dashboards that are easy to produce and understand. The reporting mechanisms within the product should produce the high-level summaries needed while at the same time offering the level of detail required for the backend support. Once deployed, companies must be able to utilize the product across different roles within the organization as well as gain value for different departments.

All of these functions must be considered during the evaluation of any SIM product. By choosing a product that can be utilized by many different people within the organization, companies can maximize their investments.

# PITFALL 8:

## Buying the wrong size SIM for your environment.

SIM solutions come in varying degrees of scalability, performance and feature sets. Selecting a SIM vendor that does not offer flexible SIM options in order to ensure you get a proper 'fit' for your environment can be a very costly pitfall. Larger, more complex networks, such as ones that employ a dedicated Security Operations Center (SOC), will have different goals and requirements than a smaller organization or single business unit. To ensure that you get a SIM solution that is the optimal size for your environment and budget, you should consider these questions:

1. How many security and network devices will we want to integrate into our SIM?
2. What level of scalability do we require in the short term ANDthe long term?
3. What types of correlation and reporting are we looking to obtain?
4. What level of compliance reporting is required?
5. How many resources do we have to dedicate to our SIM program?
6. Do we need a plug and play solution or can we dedicate more time to deployment and customization?
7. How much budget do we have to dedicate to a SIM program this year?

Organizations must keep in mind why they are deploying the solution in the first place: security. Ease of deployment is irrelevant if the solution does not meet the requirements of the organization.

In achieving all of their security compliance objectives. good SIM vendor will be able to provide either software or appliance solutions tailored to address your requirements.

If your SIM solution is not sized properly, one of two consequences occurs:

1. If insufficient in power and capabilities, the solution will not properly collect and analyze all critical data, exposing the enterprise and risking noncompliance.
2. If you buy more than you need, you will waste valuable budget and resources on an overly sophisticated solution.

# PITFALL 9:

## Not accurately considering total cost of ownership (TCO).

During POC trials, vendors project how many servers and what kind of budget might be required to make the SIM product fully operational. Often, six months later, the product is not performing as expected, so the vendor suggests one of two options

### 1. Buy additional appliances or software to balance out the workload.

### 2. Purchase bigger hardware or additional databases to better distribute the load.

If the original product underperforms, organizations either fail to meet their security and handle the workload, but rather, will benefit from securing details on how it will accomplish this. After determining the initial cost, it is crucial to project out how the product will scale both vertically (that is, increasing events per second) and horizontally (meaning, different types of data such as application, database, configuration, and so forth). By ensuring future needs are considered and factored into the SIM investment, in addition to meeting current objectives, companies can keep costs low and still maintain the level of security required, now and in the future.

# PITFALL 10:

## Choosing a SIM vendor rather than a SIM partner.

In choosing a SIM technology and making an investment in time and money, it is important to select the right technology – but equally important to select the right company. Companies should make sure the SIM vendor seems like the right fit, and by all means should ask for references to contact with similar business needs. Organizations will gain from knowing whether the company will stand behind their product and their services. Knowing a company's renewal rate is important as it is a very good measure of customer satisfaction. It also makes sense to find out what other products the company sells. Most important, companies should carefully assess the level of commitment and expertise dedicated to addressing unique SIM needs.

CYBERShark: PROTECTING DATA, ENSURING COMPLIANCE
Evaluating SIM solutions can be a difficult process, especially when engaging with companies with limited experience in the SIM industry or that are not prepared to thoroughly respond to every question about how the solution might work in a particular environment and on a specific budget. This is where CYBERShark– the company that pioneered SIM in 1999 – can help. Today, CYBERShark delivers the most comprehensive security decision support available, backed by its two powerful, flexible SIM platforms. CYBERSharks' patented technologies – SIEM Storm and SIEM Storm – offer an easy yet innovative approach to managing security information from the perimeter to the core, regardless of the business size or security team. These robust, streamlined SIM solutions help centrally collect and manage security and network data to enable rapid identification and response to threats while addressing compliance challenges. Here is how BlackStratus can help companies avoid suffering the consequences of the 10 pitfalls made when evaluating a SIM solution.

# CONCLUSION:

## ENTERPRISE-CLASS INFORMATION MANAGEMENT

CYBERShark security and compliance platform, the industry's most robust Security Information Management software solution, transforms huge volumes of disparate, security-related data into understandable, actionable intelligence. Built on a highly-scalable n-tier architecture, the platform enables large organizations with complex networks to centrally gather, analyze, and accurately report on security events and risk posture. By identifying and enabling a rapid response to threats and providing an auditable compliance framework, CYBERShark helps protect valuable data and address a myriad of regulatory challenges.

## FLEXIBLE POWERFUL AND AFFORDABLE SIM AND LOG MANAGEMENT APPLIANCES

Easy to deploy and use, CYBERShark features advanced correlation technologies and real-time monitoring for rapidly identifying and prioritizing threats. Add to that comprehensive log collection, documentation and storage and organizations can now cost-effectively meet compliance demands while enhancing their overall security posture. With flexible deployment options, CYBERShark accommodates any size networking environment.

Making a hasty or misinformed decision in a SIM solution can result in negative consequences in security stature, compliance, and cost of ownership. Companies need to move through the evaluation process equipped with the knowledge that will help them make the right decision for their unique information security challenges and goals. By being proactive, asking all the right questions, and ultimately making an informed decision when selecting a SIM solution, companies can protect their valuable data, meet regulatory requirements, and stay within their information security budgets today and tomorrow.

# ABOUT CYBERSHARK

CYBERShark is a pioneer of security and compliance solutions deployed and operated on premise, in the cloud or “as a Service" by providers of all sizes, government agencies and individual enterprises.

Through our patented multitenant security information and event management (SIEM) technology, CYBERShark delivers unparalleled security visibility, prevents costly downtime, and achieves and maintains compliant operations at a lower cost to operate.