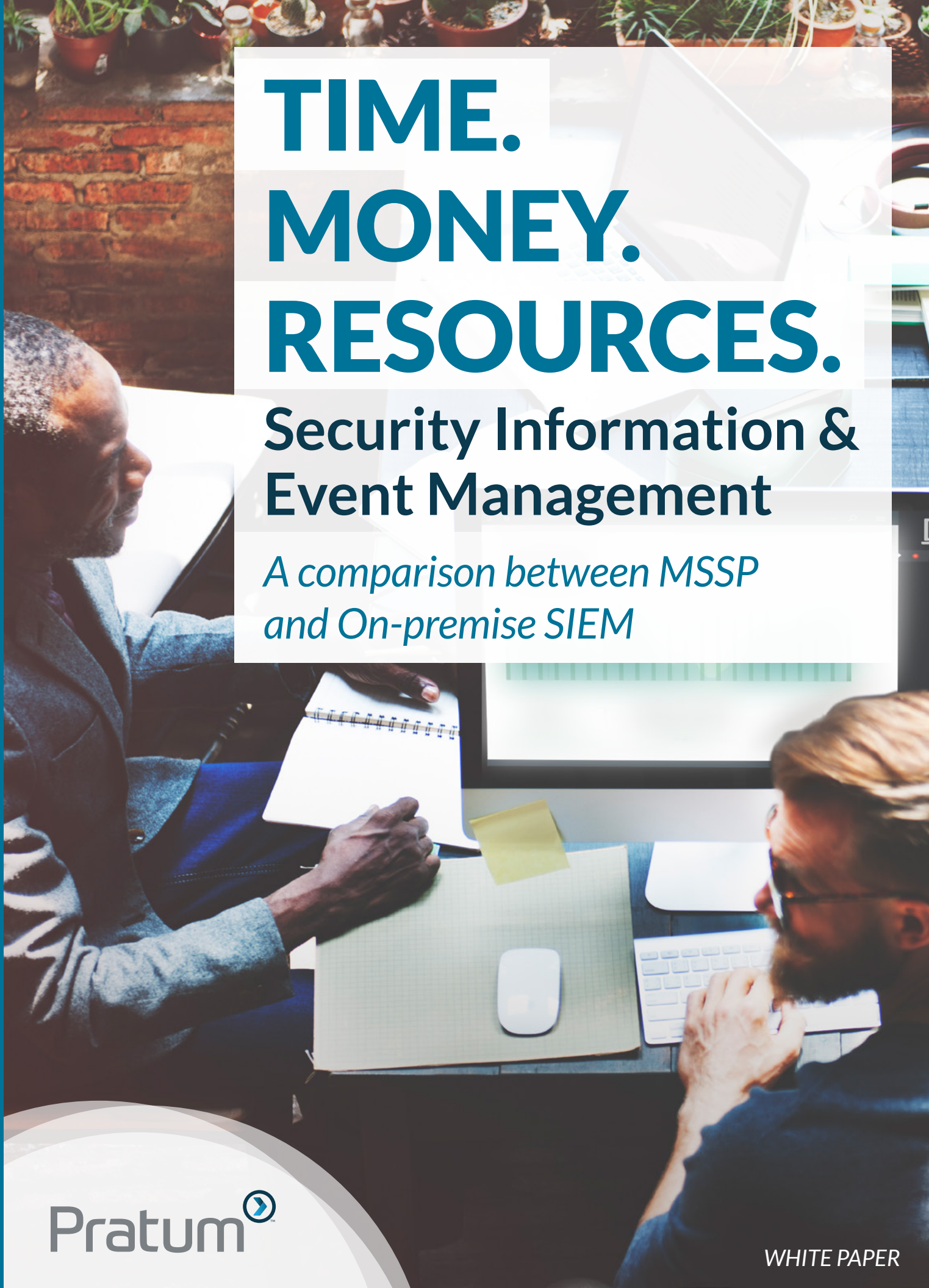

TIME. MONEY. RESOURCES.

Security Information & Event Management

A comparison between MSSP and On-premise SIEM

Pratum

WHITE PAPER

Introduction

The importance of using SIEM to its full potential

A properly implemented security information and event management (SIEM) solution will draw attention to hacker warning signs and alert an organization as suspicious activity occurs within its network.

SIEM is an essential component in a comprehensive security operation, and it is not something that should be simply implemented then forgotten. It is an element of the security program requiring constant attention. As cyberattacks evolve, the continual monitoring of network activity becomes exceedingly important.

When successfully implemented, SIEM is one of the most efficient ways of identifying and responding to security threats. SIEM can also be a great resource for understanding technology and business environments, monitoring performance and availability, diagnosing issues and reporting on network activity.

SIEM Technology

SIEM software ranges from out-of-the-box to fully customizable. Some softwares emphasize simplicity, making it easy for the user to operate but lacks necessary security features. Other software can be difficult to manage due to complexity, but has the capability of creating advanced alerts and running valuable reports.

When operating on-premise, it is important to have a software that is understood and enjoyed by technology and security staff. An underutilized SIEM is a waste of money and may leave you with a false sense of protection.

SIEM Engineers and Analysts

Understanding Roles and Responsibilities

Deciding between a managed security services provider (MSSP) and on-premise SIEM solution can be daunting. Gaining a basic understanding of the responsibilities of SIEM Engineers and Analysts will help your organization to establish its best approach to security monitoring.

The Human Element

Technology is great for correlating and consolidating mounds of data into manageable portions, but without human involvement the data is useless. Analysts help decipher between critical alerts, false positives, and everything in-between. Each incident must be addressed, and that responsibility rests on the shoulders of security professionals.

Adding security monitoring responsibilities to an employee's existing work load is a common mistake made by first-time on-premise SIEM operators. This increased responsibility often results in an employee's underperformance of their collective job responsibilities. The underestimation of the demands of security monitoring leaves an organization scrambling for additional resources at the most inopportune time.

If you are considering bringing SIEM on-premise, be prepared to allot the necessary resources to ensure its success.

When considering on-premise SIEM, ask yourself these questions.

Do we have employees who could handle the new SIEM responsibilities?

If so, do they have enough time in their schedules to do it properly?

If not, are we prepared to hire additional employees for this role?

An Analyst's Average Day

Take a minute to review the following roles to decide if your team is prepared for the responsibilities.

24x7 Security Alerting

Critical events often occur off hours, as many attacks originate from latenight hackers and nation states with differing times zones. Full coverage requires analysts to provide 24x7x365 on-call response.

Parser Performance

Parsers pull information from logs to allow for customized rule creation. Analysts build new parsers for devices that are not initially supported by the SIEM solution and modify existing parsers to properly assign attributes to the millions of log events that are processed each day.

Rule Creation and Modification

Analysts create new rules and modify existing ones to ensure alerts trigger only when needed. It is exceedingly important to properly address false positive alerts, as they can cripple response times and decrease monitoring efficiencies.

Maintain the Configuration Management Database

Due to employee turnover and device upgrades, organizations regularly add and remove devices from SIEM. Analysts are responsible for managing these changes and ensuring that monitoring is accurate. It is also important for analysts to maintain and document the evolving list of security threats.

Communication with Security and Technology Teams

Analysts are communicators; they working with security and technology teams to minimize and help eliminate risk associated with discovered incidents.

Making your decision, and what it means for your security future

A well designed and executed SIEM strategy will help prepare your organization to recognize and react to security threats. A poorly implemented SIEM approach will leave your organization exposed to attack with the inability to properly respond to incidents. It is important to understand your options and make your selection according to your organization's needs and abilities.

On-premise SIEM

Some organizations opt to purchase an out-of-the box solution, and others take on the task of organizing a comprehensive SIEM team with highly trained engineers and analyst. Most organizations exploring the idea of on-premise management are somewhere in the middle. They understand that the less-involved, out-of-the box solution is likely lacking the necessary configurations to properly monitor all network activity, but an all-inclusive on-premise SIEM solution complete with fully developed SIEM software, a team of analysts and engineers, and 24x7 support is over budget.

As displayed in the cost benefit analysis on *page 9* of this paper, there are numerous upfront costs with on-premise SIEM. In order to ensure a healthy return on investment it is important to commit to a long-term on-premise program. It is also advised to have complete support from all technology and security team members to ensure successful deployment and ongoing maintenance of an on-premise solution.

What you will need

Before taking on the task of managing SIEM internally, review the following list to make sure you have the minimum requirements.

TIME: Thoroughness & Dedication

Sifting through hundreds of alerts per day can be extremely laborsome, requiring hours of attention. A large portion of time is devoted to actively managing the SIEM and reviewing the information generated from it. Regardless of an analyst's efficiency, these tasks take time.

MONEY: Capital and Operating Expenditure Funds

SIEM software and maintenance licenses are costly. And the underlying infrastructure to operate SIEM requires high performance servers and resources including CPU, memory, virtual and physical servers, and storage requirements, which all come with hefty price tags. Storage arrays and NAS servers require their own management and must be large enough to support retention span requirements.

RESOURCES: Expert Security Analysts

Each security alert delivered by SIEM software warrants an investigation and response. This includes identifying false positives, modifying and adding rule logic, and reacting to incidents. These tasks require the expertise of security analysts who have a solid understanding of the multitude of event types, devices, rule logic, and the SIEM's underlying configuration.

"There are no out-of-the box SIEM solutions that are truly out-of-the box ready for security monitoring. Networks are too unique and complicated to rely solely on default rules, filters, and reports. Every on-premise solution will require adjustments and continuous modification."

Steve Healey, C|EH
Pratum, Chief Technology Officer

MSSP SIEM

The MSSP selection process can be difficult, but to make it easier here are three basic principles you must consider: effectiveness, collaboration, and value. Finding a managed SIEM provider with each of these attributes is important in setting the foundation for your security monitoring future.

Effectiveness

Effectiveness is about finding an MSSP that specializes in SIEM and excels at providing quality service. This involves some research on your part. You need to get an idea of the amount of experience the MSSP has with security monitoring and their policies and procedures for reacting to security incidents. Here are some things to consider in your initial conversations with prospective MSSPs.

Can they make recommendations on which devices and systems to monitor?

SIEM relies on accurate information to generate alerts and correlate data, the more information that is received the better the alert. A security service provider must assist with identifying which systems, applications, and devices to monitor.

Can they ensure that your monitored devices are appropriately configured?

SIEM doesn't just require data, it requires the right types of data. It is imperative that SIEM analysts identify the data being received and ensure it is configured with accurate audit policies.

Do their analysts tune rulesets regularly, or does this require a separate professional services fee?

Every SIEM is only as good as its rule engine and the analysts who run it. Ask the provider if they custom tailor rules for each organization or if they use a standard ruleset for everyone. Ideally, the provider will not only be adjusting and tuning the thresholds for rules but also frequently modifying and creating new rule definitions without charging extra.

It is worth noting that a large number of providers charge a professional services fee to perform customizations. This typically requires that all customizations be performed at once, as opposed to ad hoc adjustments. Try to avoid this type of MSSP, as these charges can add up quickly.

Can you contact their support team for help with creating rules and reports or with questions pertaining to generated alerts?

You will have questions throughout the SIEM process. Be sure your MSSP is available to help you along the way.

Do they actively respond to false positives and enhance the rule logic, or simply dismiss/disable them?

It is always recommended to identify false positives and exclude them from rules, thereby ensuring that only valid incidents trigger alerts. If false positives and other unwanted noise are not addressed, there is a higher probability of missing legitimate incidents. However, if a rule is completely disabled, there is no way for it to trigger during real threats. Therefore, rules that create unwanted noise should not simply be disabled but modified to exclude that noise.

Collaboration

Once an organization hires an MSSP, they must work together. It is important to select a partner that is collaborative and helpful. Even though the MSSP will handle the bulk of the SIEM responsibilities, clients must react to security alerts as they are generated.

Prior to making your decision, it is important to contact references from the MSSP's existing client base. If possible, request to speak with a reference that aligns within a relevant industry.

Questions to ask the MSSP's references:

Are you satisfied with the effort your SIEM provider delivers?

Does your provider respond swiftly and without reservation?

Are the analysts knowledgeable when responding to alerts?

Are you being bombarded with false-positive alerts?

Are you receiving help with creating custom rules and reports?

Value

When comparing the prices between SIEM providers, make sure to compare the services as well. Pricing can be misleading when the statements of work are not equal. The goal should be to find a managed SIEM that provides a great value for the price. It is not about hiring the cheapest provider or the most expensive, but rather finding one that fits organizational needs and is committed to security.

Cost comparison between an on-premise SIEM solution and Pratum's managed SIEM

Industry Standard SIEM Cost Benefit Analysis

Cost Comparison Based on 200 Monitored Devices.

On-premise Solution	
Year One Costs	
Software License Purchase	$ 45,000
Software Maintenance	$ 13,500
Initial Software Installation *(8 hours)*	$ 325
Initial Software Configuration and Tuning *(160 hours)*	$ 6,501
Daily Log Review *(4 hours/day)*	$ 42,255
Threat research, rule, and alert development *(2 hours/day)*	$ 21,128
System Maintenance, Patching, Tuning, Backup, Reporting *(10 hours/month)*	$ 4,877
Total Year One Costs	**$ 133,586**
Year Two Costs	
Software License Purchase	$ 45,000
Daily Log Review *(4 hours/day)*	$ 42,255
Threat research, rule, and alert development *(2 hours/day)*	$ 21,128
System Maintenance, Patching, Tuning, Backup, Reporting *(10 hours/month)*	$ 4,877
Total Year Two Costs	**$ 76,883**
Year Three Costs	
Software License Purchase	$ 45,000
Daily Log Review *(4 hours/day)*	$ 42,255
Threat research, rule, and alert development *(2 hours/day)*	$ 21,128
System Maintenance, Patching, Tuning, Backup, Reporting *(10 hours/month)*	$ 4,877
Total Year Three Costs	**$ 76,883**
Total In-house System Cost	**$ 297,106**

Pratum Managed SIEM	
Year One Costs	
Software License Purchase	$ 0
Annual Cost of Monthly MSSP Fees	$ 69,600
Total Year One Costs	**$ 69,600**
Year Two Costs	
Annual Cost of Monthly MSSP Fees	$ 69,600
Total Year Two Costs	**$ 69,600**
Year Three Costs	
Annual Cost of Monthly MSSP Fees	$ 69,600
Total Year Three Costs	**$ 69,600**
Total Managed SIEM Cost	**$ 208,800**

Labor Calculated at $40.63/hr. ($65,000 salary plus 30% for taxes and benefits)

29% Savings with Pratum's Managed SIEM, Totaling $88,306 in 3 Years

Which one will you choose? *(You may only select one.)*

- ◯ On-premise SIEM
- ◯ Managed SIEM

You've made a decision, now what?

Now that you have made your decision you will need to make a few more plans in order to develop a complete security program.

If you are going with an On-premise solution

You will want to establish a relationship with a 3rd party information security company to contract any future breach investigations or other security services that arise.

If working with a Managed SIEM

Make sure to fully understand all of the provider's service offerings. They may provide additional security services that will benefit your organization's security program. Also, be prepared to audit their services from time to time. Trust, but verify.

Pratum
pratum.com

Pratum solves information security challenges based on risk, not fear. Our goal is to enable every client to securely use technology to meet their business objectives. We strive to transform security fears into confidence. With an intentional approach to shifting the security culture within an organization, Pratum helps clients develop information security programs that positively impact business decisions.

sales@pratum.com