Managed Security Monitoring

Version 1.4
Released: July 25, 2016

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051
info@securosis.com www.securosis.com

Author’s Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Securosis blog, but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

This report is licensed by IBM Security.

Copyright

Managed Security Monitoring

Table of Contents

Use Cases

Many security professionals feel the deck is stacked against them. Adversaries continue to improve their techniques, taking advantage of plentiful malware kits and botnet infrastructures. Continued digitization at pretty much every enterprise means everything of interest is on a computer system somewhere. Don't forget the double whammy of mobile and cloud, which democratizes access without geographic boundaries, and takes the one bastion of control, the traditional data center, out of your direct control. Are we having fun yet?

Of course the news isn't all bad — security has become very high profile. Getting attention and resources can sometimes be a little *too* easy — life was simpler when we toiled away in obscurity moaning that senior management didn't understand or care about security. That's clearly not the case today, as you get ready to present the security strategy to the board of directors. Again. And after that's done you get to meet with the HR team trying to fill your open positions. Again.

Getting attention and resources can sometimes be a little too easy — life was simpler when we toiled away in obscurity moaning that senior management didn't understand or care about security. That's clearly not the case today, as you get ready to present the security strategy to the board of directors.

In terms of fundamentals of a strong security program, we have always believed in the importance of security monitoring to shorten the window between *compromise* and *detection* of compromise. As we said in our recent SIEM Kung Fu paper:

> *Security monitoring needs to be a core, fundamental, aspect of every security program.*

There are many different concepts of what security monitoring actually is. It certainly starts with log aggregation and SIEM, although many organizations are looking to leverage advanced security analytics (either built into their SIEM or using third-party technology) for better and faster detection. But that's not what we want to tackle in this paper. It's not about *whether* to do security monitoring, it's a question of *the most effective way* to monitor resources.

Given the challenges of finding and retaining staff, the increasingly distributed nature of data and systems that need to be monitored, and the rapid march of technology, it's worth considering whether a managed security monitoring service makes sense for your organization. Under the right circumstances a managed service presents an interesting alternative to racking and stacking another set of SIEM appliances.

Drivers for Managed Security Monitoring

We have no illusions about the amount of effort required to get a security monitoring platform up and running, or what it takes to keep one current and useful, given the rapid adaptation of attackers and automated attack tools in use today. Many organizations feel stuck in purgatory, reacting without sufficient visibility, yet without time to invest to gain that much-needed visibility into threats. A problematic situation, and often the initial trigger for discussion of managed services. Let's be a bit more specific about signs that it's worth considering managed security monitoring.

- **Lack of Internal Expertise:** Even having people to throw at security monitoring may not be enough. They need to be the *right* people — with expertise in triaging alerts, validating exploits, closing simple issues, and knowing when to pull the alarm and escalate to the incident response team. Reviewing events, setting up policies, and managing the system, all require skills that come with training and time with a security monitoring product. This is not a skill set you can just pick up anywhere. Compounding the issue is the challenge of security talent management. There is no dispute that finding and keeping talented people is hard — so if you don't have sufficient expertise internally, that's a good reason to check out a service alternative.

> Even having people to throw at security monitoring may not be enough. They need to be the right people

- **Scalability of Existing Technology Platform:** You might have a decent platform, but perhaps it can't scale to what you need for real-time analysis, or has limitations in capturing network traffic or other voluminous telemetry. And organizations still using a first-generation SIEM with a relational database backend (yes, they are still out there) face a significant and costly upgrade to modernize the system. With a managed service offering, scale is not an issue — any sizable provider is handling billions of events per day and scalability of the technology isn't your problem… so long as the provider hits your SLAs.
- **Predictable Costs:** To demonstrate our mastery of the obvious, the more data you put into a monitoring system the more storage you need. The more sites you want to monitor and the deeper visibility you want, the more sensors you need. Scaling up a security monitoring environment can quickly become costly. One advantage of managed offerings is predictable costs. You know what you're monitoring and what it costs. You don't face variable staff costs, nor do you have to deal with out-of-cycle capital expenses for new applications.

- **Technology and Operational Risk Transference:** You have been burned by vendors promising the world without delivering much of anything. That's why you are in this predicament and considering alternatives. Selecting a managed service becomes effectively an insurance policy to minimize your technology investment risk, because the provider is on the hook to deliver the functionality to which they committed. Similarly, if you are worried about your ops team's ability to keep a broad security monitoring platform up and running, you can transfer operational risk to a provider who assumes responsibility for uptime and performance — so long as your SLAs are structured properly (we're making that point again because it's important).
- **Geographically Dispersed Small Sites:** Managed services also interest organizations which need to support many small locations without a lot of onsite technical expertise. Think retail and other distribution-centric organizations. This presents a good opportunity for a service provider which can monitor remote sites.
- **Round the Clock Monitoring:** As security programs scale and mature, some organizations decide to move from an 8-hour/5-day monitoring schedule to round-the-clock. Soon after that decision they realize the difficulty of staffing a security operations center (SOC) 24/7. A service provider can leverage a 24/7 staffing investment to deliver service to many customers.

Of course you can't outsource thinking or accountability, so ultimately the buck stops with the internal team, but under the right circumstances managed security monitoring services address skill and capabilities gaps.

Favorable Use Cases

The technology platform used by the provider should be at least equal to an in-house solution, as many providers use commercial monitoring platforms for their managed services. This is a place for significant diligence during procurement, as we will discuss later in this paper. There are a few use cases where managed security monitoring makes a lot of sense, including:

> If you have a ton of network and security devices, but lack the technology or people to properly monitor them, managed security monitoring can help.

- **Device Monitoring & Alerting:** The driver for this use case is scaling and skills. If you have a ton of network and security devices, but lack the technology or people to properly monitor them, managed security monitoring can help. These services are generally architected to aggregate data on-site and ship it to the service provider for analysis and alerting, though a variety of different options are emerging for where the platform runs and who owns it. Linchpins of this use case include a correlation system to identify issues, a means to find new attacks (typically via a threat intelligence capability) and a bunch of analysts who can triage and validate issues quickly, and then provide actionable alerts.

- **Advanced Detection:** With increasing attacker sophistication it can be hard for an organization's security team to keep pace. A service provider has access to threat intelligence, presumably multiple clients across which to watch for emerging attacks, and the ability to amortize advanced security analytics across customers. Additionally, specialized (expensive) malware researchers can be shared across many customers, making those resources more feasible than for a single organization.

- **Compliance Reporting:** Another no-brainer for a managed security monitoring alternative is basic log aggregation and reporting — typically driven by a compliance requirement. This isn't a complicated use case, so it fits service offerings well. It also gets you out of the business of managing storage and updating reports when a requirement or mandate changes. Your provider should take care of all that for you.

- **CapEx vs. OpEx:** As much as it may hurt a security purist, buying decisions come down to economics. Depending on the funding model and your organization's attitude toward capital expenses, leasing a service may be a better option than buying outright. Of course there are other ways to turn a capital purchase into an operational expense, and we're sure your CFO will have plenty of ideas on that front, but buying a service can be a simple option for avoiding capital expenditure. Obviously, given the long and involved process to select a new security monitoring platform, you need to make sure the managed service meets your needs *before* economic considerations come into play — especially if there's a risk of Accounting's preferences driving you to spend big on an unsuitable product.

There are plenty of other situations where managed security monitoring makes sense which have nothing to do with those nice clean buckets. We have seen implementations of all shapes and sizes, and we need to avoid overgeneralizing. But most implementations fit these general use cases.

Unfavorable Use Cases

Of course there are also situations where a monitoring service may not fit well. That doesn't mean you cannot use a service if you have extenuating circumstances, typically a staffing and skills gap. But services generally don't fit these situations well:

- **Dark Networks:** Due to security requirements, some networks are dark, meaning no external access is available. These are typically highly sensitive military and/or regulated environments. This is problematic for a security monitoring service because the provider cannot access the customer network. If you really need to address a skills gap in such an environment, you need to consider contracting for a dedicated onsite resource, and either buying a security monitoring platform yourself or leasing one from a provider.

- **Highly Sensitive IP:** On networks with particularly valuable intellectual property, providing access to external parties is usually a non-starter. Examples include highly proprietary designs and other content that would be very valuable to a competitor or other external entity. SaaS has made remarkable inroads for very sensitive business functions including finance, sales, and human resources, but there are still reservations and limitations. Exactly which types of information are deemed highly sensitive is organization-specific and remains a moving target.
- **Large Volumes of Data:** If your organization is very large and has a ton of logs and other telemetry for security monitoring, this can challenge a service offering that requires data to be moved to a cloud-based service — particularly network forensics and packet analytics. In this case an on-premise monitoring service will likely be the best option. Note the new hybrid offerings which capture data and perform security analytics on-premise using resources in a shared SOC. We'll discuss these hybrid offerings later in this paper.

As with the favorable use cases, these unfavorable cases are strong indicators but not absolutes. It all depends on your specific requirements, your ability to invest in technology, and the availability of skilled resources. These generalizations offer a head start for considering a managed security monitoring service.

As with the favorable use cases, these unfavorable cases are strong indicators but not absolutes. It all depends on your specific requirements, your ability to invest in technology, and the availability of skilled resources.

Selecting a Service Provider

Let's say you went through the use cases and decided to move toward a managed security monitoring service. Awesome! That was the easy part. Now you need to figure out what kind of deployment makes sense, and then do the hard work of actually selecting the best service provider *for you*.

That's an important distinction to get straight up front. Vendor selection is about *your* organization. We know it can be easier to just go with a brand name. Or a name in the right quadrant of the analyst chart to pacify senior management. Or the cheapest option. But none of those might be the best choice for your requirements. So the selection process requires an open mind, and doing the work. You may end up with the brand name or the cheapest one. But you'll know you found the best fit.

The selection process requires an open mind, and doing the work. You may end up with the brand name or the cheapest one. But you'll know you found the best fit.

Deployment Options

The deployment decision comes down to two questions:

1. **Ownership:** Who owns the security monitoring platform? Who buys it? Is it provided as part of a service, or do you need to buy it up front? Who is responsible for maintenance? Who pays for upgrades? What about scaling up? Are you looking at jumping onto a multi-tenant monitoring platform, property of your service provider?

2. **SOC Location/Operations:** There are various aspects of defining SOC location. Where does the monitoring console reside? And were do the staff sit? In many cases, that's the same place but managed security monitoring provides flexibility such that the platform, including collection and analytics happens on customer premise, but triage and initial analysis happens in a service provider's SOC. Then there are the technical nuances: Is the central repository and console on your premises? Does it run in your service provider's data center? Does it run in the cloud? There are also staffing nuances to define, including: Who fields the operational staff, especially if some part of the platform will run at your site?

Per the chart below, the options depend on how you answered the questions above:

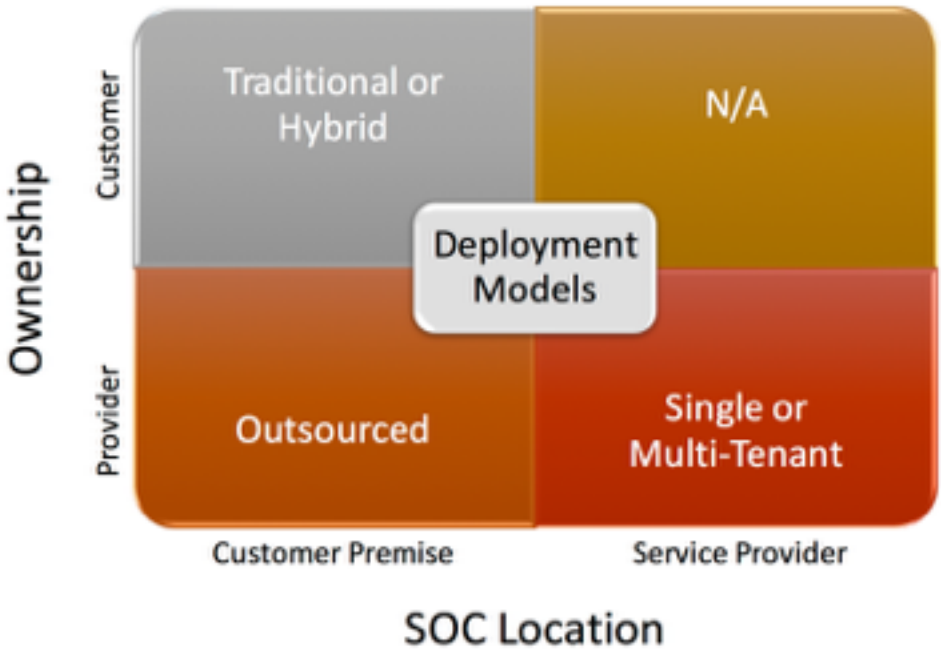
1. **Traditional:** The customer buys and operates the security monitoring platform. Either way the monitoring platform runs on the customer premises, staffed by the customer. This is not managed security monitoring.

2. **Hybrid:** The customer owns the monitoring platform, which resides on-premise, but the service provider manages it. Alternatively the provider might buy the platform and lease it back to the customer monthly, but that doesn't affect operations. The provider handles alerts and is responsible for maintenance and system uptime.

3. **Outsourced:** The service provider owns the platform that resides on the customer's premises. Similar to the hybrid model, the provider staffs the SOC and assumes responsibility for operations and maintenance.

4. **Single-tenant:** The service provider runs the monitoring platform in their SOC or the cloud, but each customer gets its own instance, and there is no commingling of security data.

5. **Multi-tenant:** The service provider has a purpose-built system to support many clients within a shared environment, running in their SOC or the cloud. The assumption is that application security controls are built into the system to ensure customer data is accessible only to authorized users, but that's definitely something to check as part of your due diligence.



Selecting Your Provider

We could probably write a book about selecting (and managing) a security monitoring service provider, and perhaps someday we will. But for now here are a few things to think about:

- **Scale:** You want a provider who can support you now and scale with you later. Having many customers roughly your size, as well as a technology architecture capable of supporting your plans, should be among your first selection criteria.
- **Viability:** Similarly important is your prospective provider's financial stability. Given the time and burden of migration, and the importance of security monitoring, having a provider go belly up would put you in a precarious situation. Many managed security monitoring leaders are now part of giant technology companies so this is less of an issue. But if you are working with a smaller player make sure you are familiar with their financials.
- **Technology Architecture:** Does the provider use their own home-grown technology platform to deliver the service? Is it a commercial offering they customized to meet their needs as a provider — perhaps adding capabilities such as multi-tenancy? Did they design their own collection device, and does it support all your security/network/server/database/application requirements? Where do they analyze and triage alerts? Is it all within their system, or do they run a commercial monitoring platform? How many SOCs do they have, and how do they replicate data between sites? Understand exactly how their technology works so you can assess whether it fits your use cases and scalability requirements.
- **Staff Expertise:** It's not easy to find and retain talented security analysts, so be sure to vet the folks the provider will use to handle your account. Obviously you can't vet them all, but understand the key qualifications of the analyst team — things like years of experience, years with the provider, certifications, ongoing training requirements, etc. Also make sure to dig into the organization's hiring and training regimens — over time they will need to hire new analysts and quickly get them productive to deal with industry growth and inevitable attrition. You don't want to have the bulk of analysts on your account being n00bs learning on your dime.
- **Industry Specialization:** Does this provider have many clients in your industry? This is important because there are many commonalities to both traffic dynamics and attack types within industries, and you should leverage your provider's familiarity. Given the maturity of most managed security offerings, it is reasonable to expect a provider to have a couple dozen similar customers in your industry.
- **Research Capabilities:** One reason to consider a managed service is to take advantage of resources you couldn't afford yourself, which a provider can amortize across many customers. Security research and the resulting threat intelligence are good examples. Many providers have full-time research teams investigating emerging attacks, profiling them, and keeping their collection devices up to date. Get a feel for how large and capable a research

team a provider has, how their services leverage their research, and how you can interact with their research team to get the answers you need.

- **Customization:** A service provider delivers a reasonably standard service — leveraging a core set of common features is key to profitability. That means you might get less customizability with a managed offering. Or customization might be expensive. Some providers may protest, but be very wary of offers to deeply customize their environment just for you, because it's hard to make that model work at scale.

- **Service Level Agreements:** Finally make sure your Service Level Agreements (SLAs) provide realistic assurances. Look for a dedicated account team, reasonable response times, clear escalation procedures, criteria for scope expansion and contraction, and firm demarcation of responsibility before you sign anything. Once the deal is signed you have no leverage to change terms, so use your leverage during courting to make sure your SLAs reflect the way you do business.

You may also want to consider taking the service for a spin as part of your selection process. Start small, collecting data from a handful of devices and running through the use cases driving your purchase. With a service offering it is as much about the interface and user experience as anything else, but be sure to test their alerting process, as well as escalation procedures for when the provider doesn't meet your SLAs.

With a service offering it is as much about the interface and user experience as anything else, but be sure to test their alerting process, as well as escalation procedures for when the provider doesn't meet your SLAs.

Checking References

There are at least two sides to every story. We have seen very successful security monitoring engagements across customers large and small. We have also seen train wrecks. Of course the customer can be as responsible as the service provider when things go off the rails, but ultimately it's your responsibility to perform sufficient due diligence when selecting a provider to learn the good, the bad, and the ugly.

That means talking to both happy and unhappy customers. Obviously a provider is unlikely to introduce you to *their* disgruntled customers, but they are always happy to find happy customers who chose them over another provider. Leverage all the vendors competing for your business to assemble a set of both positive and not-so-positive references for potential providers.

Specifically, dig into a few areas:

- **Deployment & Migration:** Make sure you understand the process to move to this provider's platform. How will they deploy collectors? Can they import existing security data? What kind of project management oversight governs deployment and cutover? These are key questions to bring up during reference calls. Ask for a very specific migration plan up front.

- **Responsiveness:** What kind of experience have customers had getting alerts and investigating issues? Have the analysts been helpful? Do they provide enough information to perform your own investigation? When the bad guys come knocking you won't have time to fuss with bureaucracy or side issues. You'll need the data, and to get your investigation moving, so your provider must not hinder that process. Build responsiveness metrics into your agreement, along with escalation policies and penalties for violations.
- **Expertise:** Do they know what they are talking about? Did they do a bait and switch with the analysts monitoring customer networks? How precise and accurate are their alerts? Everything looks great during the sales cycle, but you want to make sure their A team (or at least their B+ team) is working your account on a daily basis.
- **SLA Violations:** Not everything goes well. Learn how the provider deals with issues. Are they responsive? Do they work until the problem is solved? Have they been sued for breach of contract by other customers? This is where discussions with former clients can be very useful. There is usually a reason they are *former* clients, so find out. The provider should offer a standard SLA for you to review.
- **Account Management:** How does the relationship evolve over time? Is the account rep just there to sell you more services? Does the provider check in periodically to see how things are going? Do they take your feedback on product shortcomings and feature requests seriously? A service provider is really a partner, so make sure this provider actually *acts* like a partner to their customers.

Mismatched Expectations

As when an on-premise security monitoring implementation goes awry, the root cause can usually be traced back to mismatched expectations. With a monitoring service always keep in mind what the service does, and don't expect it to be something it's not. Don't count on deep customization or deep off-menu capabilities, unless they are agreed to up front.

As when an on-premise security monitoring implementation goes awry, the root cause can usually be traced back to mismatched expectations. With a monitoring service always keep in mind what the service does, and don't expect it to be something it's not.

Using a service provider for security monitoring can help provide resources and capabilities you don't have in-house. That said, you need to perform due diligence to ensure you have both the right choice, and the right structure in place, to manage them.

Summary

Given the skills gap and how hard it makes finding personnel to effectively monitor a security environment, along with infrastructure's rate of technological change, managed security monitoring services are becoming much more interesting to organizations of all sizes. Additionally, many service providers can make much greater investments in threat intelligence and infrastructure than typical enterprises.

> As with an on-premise, customer-owned security monitoring platform, this is not *set it and forget it* technology. The goal is to spend less time and money caring for it, and to better leverage the service provider's platform investments across many customers.

As with an on-premise, customer-owned security monitoring platform, this is not *set it and forget it* technology. The goal is to spend less time and money caring for it, and to better leverage the service provider's platform investments across many customers. For suitable use cases, with realistic expectations, our research shows that security monitoring can provide significant value and agility for organizations without the skills or inclination to manage a monitoring platform in-house.

Yet buying a monitoring service remains fraught with difficulty. Significant diligence is required to ensure the service will meet requirements and keep pace with technology change. You also need to take care in crafting Service Level Agreements (SLAs) that protect your organization, ensuring the provider is responsive and keeps the monitoring platform current.

To wrap up we offer a reminder: a monitoring service does not shift accountability. Keep the inevitable handoffs and escalations in mind as operational processes are defined and implemented with the service provider; because ultimately your internal team is still responsible to detect, investigate, and remediate attacks.

If you have any questions on this topic, or want to discuss your situation specifically, feel free to send us a note at info@securosis.com.

About the Analyst

Mike Rothman, Analyst and President

Mike's bold perspectives and irreverent style are invaluable as companies determine effective strategies to grapple with the dynamic security threatscape. Mike specializes in the sexy aspects of security — such as protecting networks and endpoints, security management, and compliance. Mike is one of the most sought-after speakers and commentators in the security business, and brings a deep background in information security. After 20 years in and around security, he's one of the guys who "knows where the bodies are buried" in the space.

Starting his career as a programmer and networking consultant, Mike joined META Group in 1993 and spearheaded META's initial foray into information security research. Mike left META in 1998 to found SHYM Technology, a pioneer in the PKI software market, and then held executive roles at CipherTrust and TruSecure. After getting fed up with vendor life, Mike started Security Incite in 2006 to provide a voice of reason in an over-hyped yet underwhelming security industry. After taking a short detour as Senior VP, Strategy at eIQnetworks to chase shiny objects in security and compliance management, Mike joined Securosis with a rejuvenated cynicism about the state of security and what it takes to survive as a security professional.

Mike published The Pragmatic CSO <http://www.pragmaticcso.com/> in 2007 to introduce technically oriented security professionals to the nuances of what is required to be a senior security professional. He also possesses a very expensive engineering degree in Operations Research and Industrial Engineering from Cornell University. His folks are overjoyed that he uses literally zero percent of his education on a daily basis. He can be reached at mrothman (at) securosis (dot) com.

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **Primary research publishing**: We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.

- **Research products and strategic advisory services for end users**: Securosis will be introducing a line of research products and inquiry-based subscription services designed to assist end user organizations in accelerating project and program success. Additional advisory projects are also available, including product selection assistance, technology and architecture strategy, education, security management evaluations, and risk assessment.

- **Retainer services for vendors**: Although we will accept briefings from anyone, some vendors opt for a tighter, ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients, we maintain our strict objectivity and confidentiality requirements. More information on our retainer services (PDF) is available.

- **External speaking and editorial**: Securosis analysts frequently speak at industry events, give online presentations, and write and speak for a variety of publications and media.

- **Other expert services**: Securosis analysts are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users. Clients include large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.

Additionally, Securosis partners with security testing labs to provide unique product evaluations that combine in-depth technical analysis with high-level product, architecture, and market analysis. For more information about Securosis, visit our website: <http://securosis.com/>.