



Security Management 2.5: Replacing Your SIEM Yet?

Version 1.91

Released: February 1, 2014

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 Systems



www.ibm.com/security

IBM provides the security intelligence to help organizations protect their people, data, applications and infrastructure. IBM operates one of the world's broadest security research and development organizations. IBM manages and monitors 15 billion security events every day for nearly 4,000 clients around the world and holds more than 3,000 security patents. For more information on IBM security, please visit: www.ibm.com/security

Copyright

This report is licensed under Creative Commons Attribution-Noncommercial-No Derivative Works 3.0.



<http://creativecommons.org/licenses/by-nc-nd/3.0/us/>

Security Management 2.5

Table of Contents

Introduction	4
Changing Needs	6
Platform Evolution	9
Revisiting Requirements	12
Evaluating the Incumbent	16
The Decision Process	20
The Selection Process	26
Negotiation	30
Migration	32
Conclusion	36
About the Authors	37
About Securosis	38

Introduction

Security Information and Event Management (SIEM) systems cause a lot of controversy among security folks. They are a cornerstone of every enterprise security program but SIEM continues to generate many complaints and elicit considerable angst among the folks we talk to. Two years ago we published [“SIEM 2.0: Time to Replace your SIEM?”](#)¹ based on conversations with organizations wanting more from their investment. They wanted better scalability, easier deployment, the ability to monitor business applications ‘up the stack,’ and more integration with enterprise systems such as identity.

Enterprises needed to analyze more types of data, from more sources, with more and better analysis capabilities, to keep pace with advanced attackers. They needed to “do more with more,” so SIEMs needed to grow as well.

Over the past couple years customer demands have accelerated, along with platform evolution to address them. When we wrote our SIEM 2.0 paper we thought we were discussing a mature market, but the innovation we saw in second-generation SIEMs using purpose-built data stores turned out to be the tip of an iceberg. Enterprises needed to analyze more types of data, from more sources, with more and better analysis capabilities, to keep pace with advanced attackers. They needed to “do more with more,” so SIEMs needed to grow as well. Despite solid platform upgrades from a number of SIEM vendors, the requirements have grown faster than some vendors could respond. Sadly but not surprisingly, security vendors falling

behind marketed “advanced capabilities” which were really the same old pig in a new suit — resulting in further chagrin and disappointment.

Whatever the reasons here we are two years later, listening to the same tales of woe from customers looking to replace their SIEMs (again) in hopes of finally being able to meet new requirements. You might feel like Bill Murray in *Groundhog Day*, reliving the past over and over again, but this round is different. The requirements have changed! Really! The original architects of early SIEM platforms could not have envisioned the kinds of analysis required to detect modern attacks designed to evade SIEM systems. Attackers are thinking differently, causing defenders to rip up the old playbooks and critically evaluate their old tools for a chance to keep up.

Advanced malware attacks are now the major driver of security product evolution, but you cannot really detect advanced attacks based on file signatures, so you need to mine data for security information in a whole new way. Cloud computing and mobile devices further complicate matters by disrupting existing technology infrastructure. And the collection and analysis of these and many other data streams (including

¹ <https://securosis.com/Research/Publication/security-management-2.0-time-to-replace-your-siem>

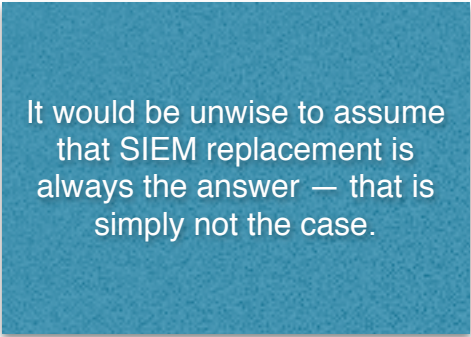
full packet capture) are bursting the seams of current SIEM products. It doesn't stop with security alerting either. Other organizations, from IT Operations to Risk to Business Analytics, also want to mine security information for new ways to streamline operations, maintain availability, and optimize everything.

Given the rapid evolution we have seen in SIEM/Log Management over the past 4-5 years, product obsolescence is a real concern. The negative impact of using a product that has not kept pace with technical evolution and customer requirements must not be trivialized. This pain becomes more acute in the case of a security incident where the SIEM did not collect the necessary information — or worse failed to detect the threat at all. Customers spend significant resources — both time and money — on the care and feeding of SIEM platforms. If they don't see value commensurate with their investment they will move on again — searching for better, easier, and faster products. It is reasonable, and often inevitable for customers to question whether their incumbent offering makes sense moving forward.

Additionally, firms increasingly consider managed services and third-party security operations providers to address internal skills and resource shortages. Many firms simply lack the internal expertise to detect advanced threats. This skills gap promises to reshape the landscape of security management, so we will begin with these factors to set the stage for our 'how-to' guide on selecting a SIEM.

This paper will walk you through the entire process — from soup to nuts — of evaluating, selecting, and deploying a SIEM. We will offer pragmatic advice on how to get it done based on years working through this process as both consumers and vendors of SIEM technology. The process is not always painless, but we are certain it will help you avoid foundering on bad technology and inter-office politics.

Despite the title of this paper, it would be unwise to assume that SIEM replacement is always the answer — that is simply not the case. After this analysis you might actually feel better about your original SIEM purchase, with a plan to increase usage and make it a success. But you owe it to yourself and your organization to ask the right questions and to get answers. It is time to slay the sacred cow of your substantial SIEM investment, and to figure out your best path forward.



It would be unwise to assume that SIEM replacement is always the answer — that is simply not the case.

Changing Needs

Organizations' needs and requirements for security management have changed a lot over the last three years. The reasons customers list for SIEM failures are different too. Below are the main discussion points when we speak with enterprise customers, and the big picture reasons currently motivating SIEM users to seek alternatives.

- **Malware/Threat Detection:** Malware is by far the biggest security issue enterprises face today. It drives many of the changes rippling through the security industry, including SIEM and security analytics. SIEM is designed to detect security events, but malware is designed to be stealthy and evade detection. You may be looking for malware, but you don't always know what it looks like. You hunt for anomalies that kinda-sorta look like they could be an attack, or just odd stuff that might be an infection. The days of simple file-based detection are gone, at least for the simple malware 'signature' based detection techniques of a few years ago. You need to detect new and novel forms of advanced malware, which requires adding different data sources to your analysis and observing patterns across many — possibly new — event types. You also need to leverage emerging security analytics capabilities to examine data in new and novel ways. Even if we do all this, it might not be enough. This is why feeding third-party threat intelligence into the SIEM is becoming increasingly common — so organizations can watch for attacks seen by others.
- **Cloud & Mobile:** As firms move critical data into cloud environments and offer mobile applications to employees and customers, the *system* to protect now encompasses devices and use cases outside the classical corporate perimeter, changing the scope of infrastructure to monitor. Compounding this issue is the difficulty of monitoring mobile devices, many of which you do not fully control... without effective tools to gather telemetry and metrics. Even more daunting is the lack of visibility (basically log and event data) into what's happening within cloud service providers. Some providers simply *cannot* provide infrastructure logs to customers because their event streams combine events from all customers. Sometimes they cannot provide network logs, because there is no 'network' to tap in a virtualized network environment, so existing data collectors are useless. In other cases the cloud provider is simply unwilling to share their full event picture, and device monitoring might be contractually prohibited. The net result is that security monitoring and event analysis must be tackled in a fundamentally different fashion. This typically involves collecting the

You need to detect new and novel forms of advanced malware, which requires adding different data sources to your analysis and observing patterns across many — possibly new — event types.

events you can gather (application, server, identity, and access logs) and massaging them into your SIEM. For Infrastructure as a Service (IaaS) environments, look at adding your own cloud-friendly collectors into the flow of application traffic.

- **General Analytics:** Much more information is available from IT systems than just security events. This is definitely useful but it cuts both ways — some event analysis platforms are set up for IT Operations **first**, with security and business operations teams as secondary customers piggybacking off that investment. Analysis, reporting, and visualization must be both accessible to a wider audience (including security), and optimized to perform true correlation and analysis.

What Customers Really Want

These example use cases reflect the business drivers for action. The bullet points represent high-level motivations but don't tell the whole story — they fail to capture why so many current platforms fail to meet expectations. We need to take a more technical look at requirements to understand why problems are frequent and serious enough for customers to consider jettisoning current solutions, re-evaluating requirements and deficiencies, and going through a whole new SIEM deployment.

Deeper Analysis Requires More Data

To address the use cases above, especially malware analysis, more data is required. That means more event volume — such as capturing and storing full packet streams, at least briefly. It also means more data types — such as human-readable data mixed with machine logs and telemetry from networks and other devices. It includes complex data types — such as binary and image files — which are difficult to parse, store, and even categorize. And it means we cannot afford to scrub, sanitize, and squeeze the data we already collect into neat little containers.

The Need for Better and More Flexible Analysis

Simple correlation of events — who, what, where and when — is insufficient for security analysis today. Not only because those attributes are insufficient to distinguish bad from good, but also because analysis approaches are fundamentally evolving. Many organizations want to profile normal traffic and usage — baselines help understand how systems are being used, and detect anomalies which might indicate misuse.

There is considerable fragmentation in how customers use security management products and services — some choose to leverage SIEM more for real-time alerting and analysis, while others want to combine many different views to create a big picture. Some customers want fully automated threat detection while others want more interactive *ad hoc* and forensic analysis. To make things even harder for vendors, today's hot analytical methods could very well be irrelevant a year or two down the road. Many customers want to make sure they can update analytics as requirements develop — making optimized hard-wired analytics a liability rather than an advantage.

Simple correlation of events — who, what, where and when — is insufficient for security analysis today. Not only because those attributes are insufficient to distinguish bad from good, but also because analysis approaches are fundamentally evolving.

The Velocity of Attacks Requires Threat Intelligence

When we talk about threat intelligence we are not just thinking of things like IP reputation or ‘fingerprint’ hashes of malware binaries. Those features are widely used but threat intelligence is much more than that. Some intelligence feeds look at social connections and credit histories of customers connecting to retail sites. Some services ‘scrape’ known hacker sites for indicators of pending DoS attacks. Others highlight specific botnet C&C actions that identify infected systems **within** your networks. You can also analyze uploaded binary files and images to profile malware, and then search for those indicators within your environment. But these custom feeds do *not* come in `syslog` format. They are generally from third parties, and typically require integration into the SIEM; as well as analytic, alerting, and reporting adjustments to take advantage of them.

This creates another problem for security event notification: if event capture increases by a factor of 10 while accuracy remains the same, false positives increase tenfold. As SIEM architectures scale, filtering and analysis must become much faster and more accurate to avoid overwhelming already overworked security personnel.

The Volume of Data Demands Enhanced Speed, Scale, and Accuracy

When you collect more data from more sources the volume of information to parse, manage, and inspect grows dramatically — even exponentially. The scale of SIEM clusters continues to increase rapidly to accommodate additional data, and the data and equipment dedicated to SIEM continue to grow substantially faster than other IT functions. This creates another problem for security event notification: if event capture increases by a factor of 10 while accuracy remains the same, false positives increase tenfold. As SIEM architectures scale, filtering and analysis must become much faster and more accurate to avoid overwhelming already overworked security personnel.

The Skills Gap Requires Better Automation and Efficiency

Co-sourcing SIEM capabilities with third-party Security Operations Centers (SOCs) — sharing SIEM monitoring and/or management with a service provider — or even fully outsourcing is increasingly common; many organizations find it a necessity. Large firms continue to face challenges in staffing, training, and retaining security operations teams. Security is a growing problem across all industries, so demand is growing faster than the small pool of talented SIEM operators and security experts.

As one of our readers pointed out: “If you have the resources to invest in a SIEM, you might as well invest in various open-source ‘big data’ technologies.” Many customers have turned to big data systems to supplement their SIEM platforms. But the key limitation is not funding — it is finding the talent to architect big data solutions and further develop security analysis scripts and policies embedded in SIEM. In some cases you are re-creating SIEM functions by writing data collectors and analysis code. Customers are embracing big data infrastructure and capabilities — both directly in-house and through third-party SOC and SIEM vendors. But firms outside the security business often prefer to outsource or engage third parties to fill the gaps as SIEMs go through this period of change. The shift toward using big data to fill SIEM gaps underscores the need to “do more with more” as we discussed above, but again the gating factor is often talent.

Platform Evolution

This section discusses the evolutionary changes in SIEM, focusing on the evolution of underlying platform capabilities to meet customer demands. As we mentioned above, it is all about doing more with more data. The change in these platforms over the past few years has been mostly under the covers. It is not sexy, but the architectural evolution was necessary for the platforms to scale and handle the needed analyses moving forward. The problem is that most folks do not appreciate the boatload of R&D required to enable platforms to receive a proverbial brain transplant. We will start with the major advancements.

It is all about doing *more with more data*. The change in these platforms over the past few years has been mostly under the covers. It is not sexy, but the architectural evolution was necessary.

Architectural Evolution

To be honest, we downplayed the importance of SIEM's under-the-hood changes in our [previous paper](#)². The “brain transplant” was *the* significant change that enabled a select few vendors to address the performance and scalability issues plaguing the first generation of platforms built on RDBMS. For simplicity's sake we skipped over the technical details of how and why, but it is now time to explore that evolution.

The fundamental change is that SIEM platforms are no longer based on a massive central service. By leveraging a distributed approach — using a cooperative cluster of many servers independently collecting, digesting, and processing events — policies are distributed across multiple systems to more effectively and efficiently handle load. If you need to support more locations or pump in a bunch more data, just add nodes. This sounds like big data because essentially it is — several modern SIEM platforms are based on big data technologies.

The result is parallel event processing resources deployed ‘closer’ to event sources, faster event collection, and systems designed to scale without massive reconfiguration. This architecture enables different deployment models and better accommodates distributed IT systems, cloud providers, and virtual environments — which increasingly constitute the fabric of modern technology infrastructure. The secret sauce making it all possible is distributed systems management. It is easy for a vendor to say “big data”, but much harder to scale heavy-duty security analysis. Later, when we get to proof-of-concept testing and final decision-making, we will discuss substantiating vendor scalability claims.

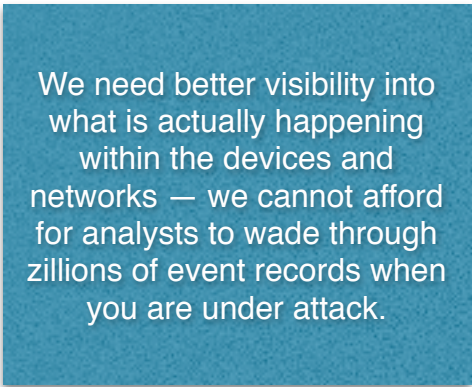
² <https://securosis.com/Research/Publication/security-management-2.0-time-to-replace-your-siem>

The important parts, though, are the architectural changes to enable scaling and performance, and support for more data sources. Without them nothing else matters.

Serving Multiple Use Cases

The future of security management is not just detecting advanced threats and malware, although that is the highest-profile use case. We still need to get work done *today*, which means adding value for operations, as well as for compliance and security. This typically involves analyzing vulnerability assessment information so security teams can ensure basic security measures are in place. You can analyze patch and configuration data similarly to help operations teams keep pace within dynamic — and increasingly virtual — environments. We have even seen operations teams detect application DoS attacks through infrastructure event data. This kind of derivative security analysis is the precursor to allowing risk and business analytics teams to make

better business decisions by leveraging data collected from the SIEM — redeploying resources, taking applications offline, etc.



We need better visibility into what is actually happening within the devices and networks — we cannot afford for analysts to wade through zillions of event records when you are under attack.

Enhanced Visibility

Attackers continually shift strategies to evade detection, increase efficiency, and maximize the impact of attacks. Historically one of SIEM's core value propositions has been an end-to-end view, enabled by collecting all sorts of different log files from devices all around the enterprise. Unfortunately that turned out to be insufficient — log files and NetFlow records rarely contain enough information to detect or fully investigate attacks. We need better visibility into what is actually

happening within the devices and networks — we cannot afford for analysts to wade through zillions of event records when you are under attack.

Three technical advances together provide much better visibility into the event stream. In no particular order they are more and better data, better analysis techniques, and better visualization.

- **More and Better Data:** The ability to collect application events, as well as *full* network packet capture — not just metadata — and other sources that taxed older SIEM systems has provided the foundation for this deeper analysis. In many cases the volume or format of the data was incompatible with the underlying data management engine, driving this advancement.
- **Better Analysis:** New data sources enable more detailed analysis, longer retention, and broader coverage; improved capabilities combine to provide better depth and context for analysis.
- **Better Visualization:** Enhanced analysis, combined with advanced programmatic interfaces and better visualization tools, substantially improves the experience of interrogating the SIEM. Old-style dashboards with simplistic pie charts and bar graphs have given way to complex data representations that much better illuminate trends and highlight anomalous activity.

These improvements might look like simple incremental improvements to existing capabilities, but together they provide dramatically better visibility.

Decreased Time to Value

Another common need mentioned by SIEM buyers is for platforms to provide value without major customization and professional services. They want platforms to address their needs *right out of the box*. Customers are tired of buying SIEMs that function more like toolkits than platforms, and then needing to invest significant time and money in professional services to build a custom SIEM system tailored to their particular requirements. SIEMs have actually gotten much better at this, but with the rapid evolution of the market it does not always *feel* like it. As we mentioned earlier, collecting an order of magnitude more data requires a commensurate jump in analysis capabilities to avoid drowning in a sea of alerts.

The same math applies to deployment and management — monitoring many more types of devices and analyzing data in new ways means platforms need to be easier to deploy and manage simply to *maintain* the old level of manageability. The good news is that SIEM platform vendors have made significant investments to support more devices and smooth installation and integration, which means less custom work is required.

With new data sources and enhanced visibility, the competitiveness of a platform can be determined by the simplicity and intuitiveness of its management interface, and the availability of out-of-the-box policies and reports which make use of the new data types. But given the need for increasingly sophisticated analysis, and the lack of folks able to perform it, organizations need a way to kickstart analysis functions. This can make the biggest difference in time to value for new platforms.

Hybrid Deployments and Streamlined Integration

Very few firms are actually in the business of delivering security, so many leverage third parties to either manage an on-premise SIEM from a remote location or run the SIEM at an off-site Security Operations Center. These deployment models enable a handful of experts to help set up and manage a SIEM, and provide expert policy development and analysis unavailable in most organizations.

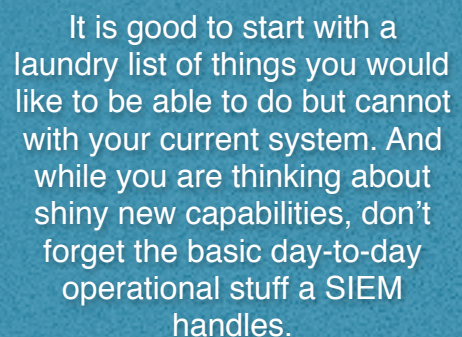
Several interesting hybrid deployment models are appearing. One uses a managed service to do the first level of alerting and validating alerts. The internal team *also* collects and manages overlapping data within its own monitoring and analysis platforms, for forensic analysis and more advanced uses of security data. This allows the organization to allocate its skilled staff to *real* issues, leaving simple alert reduction and initial analysis to a commodity security monitoring provider.

We also see hybrids leveraging external intelligence feeds to alert internal SoC staff to potential trouble. These intelligence sources provide a much broader set of indicators to drive analysis or tune monitoring, based on what is happening out in the wild. That kind of data is not available internally before attacks hit. It is an excellent way to benefit from the misfortune of others who have already been targeted by emerging attacks.

Revisiting Requirements

Given the evolution of SIEM technology and the security challenges facing organizations, it is time to revisit the underlying requirements and use cases driving investment. This is an essential part of the evaluation process. You need a fresh and critical look at your security management environment to understand what you need today, how it will change tomorrow, and what kinds of resources and expertise you can harness — without being constrained by your current situation. Some requirements may not have changed much — such as ease of management and compliance reporting — but the way you use these systems has probably changed dramatically.

That is our way of saying it is good to start with a laundry list of things you would like to be able to do but cannot with your current system. And while you are thinking about shiny new capabilities, don't forget the basic day-to-day operational stuff a SIEM handles. Finally, you need to consider what is coming down the road in terms of business challenges and resulting security issues over the next couple years. None of us has a crystal ball, but critical business imperatives should give you a basis for figuring out how things need to change.



It is good to start with a laundry list of things you would like to be able to do but cannot with your current system. And while you are thinking about shiny new capabilities, don't forget the basic day-to-day operational stuff a SIEM handles.

A Fresh Start

Some organizations choose to take a fresh look at their security management infrastructure every so often, while others have the need thrust upon them. For instance if your organization was breached or infected by malware and your SIEM platform failed to detect it, you need to take a critical look at your security management environment. The current platform may be adequate or it might be a dog — and you personally might not have even chosen it — but your success is linked to how well your platform meets requirements, now and moving forward. If things go south blaming your predecessor for choosing a mediocre SIEM won't save your job.

You also need to face the fact that other groups within the organization have differing needs for the SIEM. Operations only cares that they get the metrics they need, compliance teams only care about getting their reports, and business executives care about meeting their corporate objectives, all of which may be different from what's important to security. Use this opportunity to roll up your sleeves and figure out what *you* need.

To find the best path forward, compare priorities when you selected the incumbent platform against current priorities. This should illuminate how requirements have changed over time. To be more specific, compare the reasons you bought the system against your current spending drivers. The differences should help identify where you need the most work.

It's All about Me!

Setting requirements is all about you, right? It's about what *you* need to get done. It's about how *you* want to work. It's about what *you can't do* — at least easily — today. Well, not quite. We jest to make a point: you need to start with a look inward at what your company needs, rather than getting distracted by what's on the market today. This requires taking a look at your organization and the other internal teams that use the SIEM. Once your team is clear about your own requirements, start to discuss requirements with external influencers. Assuming you work in security you should consult ops teams, business users, compliance, and perhaps the general counsel. Ask about their requirements, and whether and how they have changed. This should confirm the priorities you established earlier and set the stage for enlisting support if you decide to move to a new platform.

The key drivers for SIEM — improving security and efficiency, and supporting compliance — remain the same, and none of them has gotten easier. The scale of the problem has grown, so if you have been standing still without adding new capabilities... you actually lost ground. To catch up you need to make sure correlation and monitoring work better, and use threat intelligence to help you figure out what to look for.

Increasingly SIEM platforms “monitor up the stack” — collecting additional data types including identity resources like users and groups, database activity monitoring, application logs, and configuration data. The additional data helps isolate infrastructure attacks, but you cannot afford to stop there. As attacks target higher-level business processes and the systems that automate them, you need visibility beyond core infrastructure. So your security management platform needs to detect attacks in the context of business threats. Don't forget about advanced forensics — it would be foolish to count on blocking every attack. So you will probably rely on your security management platform to help [React Faster and Better](#)³ with incident response.

You might also be looking for a more integrated user experience across a number of security functions to improve efficiency. For example you might have separate vendors for change detection, vulnerability management, firewall and IDS monitoring, and database activity monitoring. You may be wearing out your swivel chair switching between all those consoles, so simplification through vendor consolidation could be a key driver as you revisit requirements. Don't get hung up on what you have — figure out what you need now and moving forward. Do a little thinking about what would make your life much easier, and use those ideas to develop your requirements. You may not get everything you want — it might not be possible — but you won't know unless you check.

³ <https://securosis.com/Research/Publication/react-faster-and-better-new-approaches-for-advanced-incident-response>

The Platform

The other half of this analysis process, after organizational needs, is considering the technical impediments currently preventing your platform from meeting requirements. What you have might be perfectly suited for 2008, but that doesn't make it useful today. Here you need to delve into the functionality gaps in your current platform. To start off we will list the most frequently mentioned platform deficiencies, with questions to spotlight the relevant issues:

- **Advanced Detection:** Are you able to detect attacks in a timely fashion, or are you running down false positives most of the time? Changes in attacker behavior require the SIEM to adapt accordingly. It might be attack detection, fraud, system misuse, probing, or even data exfiltration, but advanced detection has emerged as a key enterprise priority. Customers *need* their platforms to either detect attacks as they happen or provide quick identification — within minutes — of system compromise. To keep pace with changing attack tactics, advanced detection requires new event sources, analyzed using more advanced queries. Some platforms build baselines to define what's 'normal', and then set activity thresholds relative to them, alerting when activity deviates. Some combine multiple event types (using threat models) to help identify what *should not* be happening. Still others map externally sourced threat intelligence to look for attack patterns recorded elsewhere. Regardless of the specific approach, the state of the art for threat detection has changed from simple 'good' or 'bad' analysis of metadata to more complex behavioral and risk-based analysis to detect attackers who are proficient at evading detection.
- **Scalability:** As IT systems grew, and you added mobile and cloud services to your supported services, you likely more than doubled the quantity of data pushed into your SIEM — in theory at least. Did your SIEM keep pace with that expansion and continue to perform admirably? Are you still trying to get budget for a bigger server and more storage? It's not like the amount of data you need to analyze will ever be *lower* than it is today, so make sure the architecture of any platform you choose can keep pace.
- **Forensics and Analytics:** The concept of drilling down into an event almost seems quaint now that most platforms provide pre-defined aggregated views of user, event, or server activity, pulling this information together automagically. If you are manually looking through log files or enriching existing records to fill out the full activity picture, you should know 2007 called and wants its SIEM back. We don't always know which specific indicators to watch to detect advanced attacks, so forensic analysis is still a key requirement. But forensics keeps changing. The challenge should not be gathering the data or trying to link it together, but instead how to make sense of the information at your disposal in a structured fashion to accelerate identification of the root cause of any attack. Built-in usage profiles for activity baselining are essential, as are advanced query facilities for quick and easy ad hoc analysis.

If you are manually looking through log files or enriching existing records to fill out the full activity picture, you should know 2007 called and wants its SIEM back.

- **Compliance:** Does your platform have all the compliance reports you need built in? Are they good enough that you don't need to do major customization and polishing for audits? How many reports do you need to build from scratch? Many customers tell us outright that their SIEM/LM platform is essential for compliance reports, and without it audits simply fail to occur. You already have enough to do — spending a lot of time building large numbers of reports from scratch adds insult to injury. Building custom reports is a lot of work, and a user interface that makes this easy is very useful, but wouldn't it be better if you don't need to write them at all?
- **Ease of Management:** How easy is it to manage your platform? To archive older data? To roll out new collectors? How about adding new use cases or customizing correlation rules? Are policy management screens easy to use, or do they consist of 500 checkboxes you don't fully understand? A huge amount of time is wasted managing difficult platforms, which is ridiculous for technology in use for over a decade. Obviously if you switch platforms you will need to accept some sunk costs to install and configure event collectors for various devices and servers. But that cost may be worthwhile if you can cut day-to-day management overhead while increasing functionality.
- **Integration:** In the old days the complaint was that vendors did not support all the devices in the organization. Now we hear more about difficulty integrating new event sources. Cloud monitoring, threat analytics, non-`syslog` events, and different intelligence feeds — all drive demand for streamlined integration to get value from additional data faster.
- **Vendor viability:** Did you buy a product from an early leader who has since hit hard times? Did the product roadmap go off into the weeds? Vendor fortunes change dramatically, and shortly after we last discussed this issue (in our [SIEM 2.0](#)⁴ paper) several SIEM/LM vendors were acquired by big IT companies. The good news is that creditors are much less likely to shutter the larger acquirers — the bad news is that they might not understand (or care) what you need, or devote sufficient resources to keeping platforms current. Either way you should assess your vendor's ongoing viability and ability to deliver on its roadmap to ensure it lines up with what you need going forward.

The good news is that creditors are much less likely to shutter the larger acquirers — the bad news is that they might not understand (or care) what you need, or devote sufficient resources to keeping platforms current.

⁴ <https://securosis.com/Research/Publication/security-management-2.0-time-to-replace-your-siem>

Evaluating the Incumbent

Customers grumble about their current products and services. It's human nature. As we have discussed, there is reality behind user complaints about SIEM. Many factors are in play. Tremendous growth in event collection driven by new devices and applications. The need to collect nearly every event type in hopes of having the critical bits to detect and block the next attack, whatever it might be. The demand for real-time response. Let's not forget the need for detailed high-performance forensics, compliance reports for non-technical audiences, or detailed operational reports for IT. SIEM customers face a daily yin/yang battle — between automation and generic results; between efficiency and speed; between easy and useful. Again, dissatisfaction is to be expected — the problem is to figure out when dissatisfaction has become a need for change.

SIEMulation

To illustrate why customers go through the re-evaluation process, here are excerpts from customer conversations:

Customer #1: “We had some data leakage a couple years ago; nothing serious, but it was a partner who discovered the issue. It took some time to determine why we did not see the activity with SIEM and other internal security systems. Needless to say our executive team was not happy, and wanted us to justify our security expenditures. Actually it was more like, ‘Why did we not see this? What the hell are we paying for?’ Our goal is to be able to get detection working the way we need it to work, and that means full packet capture and analysis. As you know, that means a lot more data, and we need longer retention periods as well.”

Customer #2: “We upgraded from log management to SIEM two years ago in order to help with malware detection and to scale up general security awareness. The new platform is supposed to scale, but we don't actually know if it does scale yet because we are still rolling it out. Talk to me again in a couple years — I ought to have it done by then.”

Customer #3: “I want security analytics. I *have* systems to measure supply chain efficiency. I have business risk analysis systems. I want the same view into operational and security risk, but I can't blend the analysis capabilities from these other platforms with the SIEM data. Our goal is to have the same type of analysis everywhere, and eventually a more unified system.”

To evaluate your current platform you need to consider the issue from two perspectives. First look critically at how well the existing platform addresses your current and foreseeable requirements. Second look at the evolving use cases we described earlier and weigh the impact of a newer platform on operations and deployment — both good and bad. Just because another vendor offers more features and performance does not mean you should replace your SIEM. The grass is not always greener on the other side.

Just because another vendor offers more features and performance does not mean you should replace your SIEM. The grass is not always greener on the other side.

Sizing the Incumbent

The first step in the evaluation process uses the catalog of requirements you built earlier to assess how well your current SIEM platform satisfies them. This means spelling out each business function, how critical it is, and whether the current platform gets it done. You will need to discuss these questions with stakeholders from Operations, Security, Compliance, and any other organizations which participate in SIEM management or take advantage of it. You cannot afford to make this decision in a vacuum, and lining up support early in the process will pay dividends later on. Trust us on this.

Operations is generally the best judge of whether the platform is easy to maintain and the complexity of implementing new policies. Security will have the best understanding of the product or service's alerting and forensic auditing capabilities. Compliance can judge suitability of reports for audit preparation. An increasingly common contributor is risk and/or data analysts who mine information and help prioritize allocation of resources. Each audience provides a unique perspective on the criticality of particular functions and the effectiveness of the current platform.

At this point you have already examined your requirements so you should understand what you have, what you want, and the difference between them. In some cases you will find that the incumbent platform simply cannot meet a hard requirement, which makes the analysis easy. In other cases the system works perfectly, but is a nightmare in terms of maintenance and care & feeding for system or rule changes. Performance may be less than ideal, but it is not always clear what that really means, because *any* system could always be faster when investigating a possible breach. It may turn out the SIEM functions as designed but lacks the capacity to keep up with all the events you need to collect, or takes too long to generate actionable reports.

We reiterate the importance of staying focused on critical items to avoid “shiny object syndrome” driving you to the pretty new thing, perhaps ignoring a cheap dull old saw that gets the job done.

Act like a detective to collect these tidbits of information, no matter how small, to build the story of the existing SIEM platform in your environment. This information will come into play later when you weigh options, and we recommend using a format that makes it easy to compare and contrast issues.

Security, compliance, management, integration, reporting, analysis, performance, scalability, correlation, and forensic analysis are all areas you need to evaluate in terms of revised requirements. Prioritizing existing and desired features helps

streamline the analysis. We reiterate the importance of staying focused on critical items to avoid “shiny object syndrome” driving you to the pretty new thing, perhaps ignoring a cheap dull old saw that gets the job done.

Next you will evaluate other SIEM solutions. At this point you have documented your requirements and rationally evaluated your current SIEM platform to determine what’s working and what isn’t. All other options will be measured against the existing platform’s strengths and weaknesses. As you evaluate new platforms you can *objectively* figure out whether it is time to move on and select another platform. At this point no decision has been made. You are doing your homework — no more, no less.

You face two major difficulties during this phase. First, you need a deep understanding of SIEM solutions in order to dig in and determine what other SIEM providers legitimately deliver and what is marketing fluff. Second, you cannot exactly compare apples to apples. Some new platforms offer advantages because they use different data models and deployment options, which demands careful analysis of how a new tool can and should fit into your IT environment and corporate culture. Start by addressing common user complaints and associated solutions to highlight differences in function, architecture, and deployment.

Yardsticks

The most common complaints we hear include: the SIEM does not scale well enough, users need more and better data, the product needs to be easier to use while providing more value, and users need to react faster to investigate the types of attacks happening today.

- **Scale:** With the ever-growing number of events to monitor, it is simply not enough to buy bigger and/or more boxes to handle exponential event growth. Some SIEM vendors tried to segregate reporting and alerting from collection and storage to offload processing requirements, to enable tuning each server to its particular role. This was followed by alternative deployment models where a log management function collected data to meet scalability needs, delivering a heavily filtered event stream to the SIEM to reduce analysis load. But that is a band-aid rather than a long-term solution. New platforms address many of the architectural scaling issues, with purpose-built data stores providing fully distributed processing. These platforms can flexibly divide event processing, correlation, reporting, and forensic analysis. For more information on SIEM scaling architectures see our [Understanding and Selecting a SIEM/Log Management](#)⁵ paper.
- **Analysis:** The clear trend is to collect more and more types of data, from more types of applications and devices. Most platforms collect data from an increasing number of devices, but many fail in two areas. First, they have failed to climb out of the network and server realms to monitor applications in more depth. Second, they are having trouble with things that don’t fit neatly into an existing format like NetFlow or `syslog`. Coupled with poorly executed correlation and enrichment, this produces data of limited value for analysis and reporting — which defeats the purpose of a SIEM in the first place. For example you might need to collect a binary file or pull data from social media. The data format is non-standard and the important aspects of an application event or SQL query must be interpreted within the context of the application, requiring a deep understanding of what it does and

⁵ <https://securosis.com/research/publication/white-paper-understanding-and-selecting-siem-log-management>

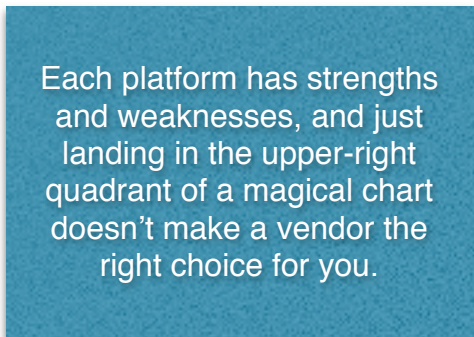
why. These events may not look suspicious under a typical correlation analysis, but if you examine the original transaction and dig into the actual query you might find SQL injection. Better data means both broader data collection options and more effective analysis of collected data within the context of business processes.

- **Simplicity:** This term encompasses many elements: automation of common tasks, real centralized management, better visualization, and streamlined analytics which don't require a PhD to interpret. Rules that ship out of the box are traditionally immature and mostly useless, as if written by tech companies with little understanding of your particular requirements — which they are. Automated reporting and alerting features got a black eye because they returned minimally useful information, requiring extensive human intervention to comb through thousands of false positives. The tool was supposed to help — not create even more work. Between better data collection, more advanced analytics, and easier policy customization, the automation capabilities of SIEM platforms have evolved quickly. Centralized management is not just a common interface for several unconnected products. To us centralized management means analysis and reporting of events across the enterprise, the ability to distribute rules from a central policy manager, *and* the capability to tune rules on an enterprise basis. Most products cannot do this, but in distributed environments where you want to push processing closer to the point of attack, you need it. Useful visualization — not just shiny pie charts, but real graphical representations of trends, meaningful to the business — can make decisions easier.
- **Modern Architecture:** Collection, followed by moving the data to a central location, aggregation, normalization, correlation, and then processing, is an antiquated SIEM model. That worked great in 2002, but not so much nowadays. Newer SIEMs inspect events and perform some preprocessing prior to storage to enable near-real-time analysis closer to the event source as well as post-correlation analysis. And many forms of analysis require more advanced queries and substantial data preprocessing to provide statistical references and activity models. These actions are computationally expensive so these advances are predicated on an advanced product architecture and appropriate deployment model. This requires SIEM deployment (analysis, correlation, etc.) to be pushed closer to — or into — 'collector' nodes.

The Decision Process

By this point you appreciate the (likely large) gap between **what you need** and **what you have**, so now dip your toes in the water to see what other vendors offer. But how? You need to figure out which vendors are worth investigating as possible alternatives. Much of defining evaluation criteria and screening potential candidates involves wading objectively through vendor hyperbole to see what each offering *actually does* vs. drug-induced optimism in the marketing department. As technology markets mature (and SIEM is fairly mature), the base capabilities of the platforms converge, making them all look alike. Complicating the issue, vendors converge on similar messaging regardless of actual features, making it increasingly difficult to differentiate between platforms.

Given your unhappiness with your current platform (or you wouldn't be reading this), you need to distill what a platform does and doesn't do, as early in the process as you can. Make no mistake — there are significant differences!



Each platform has strengths and weaknesses, and just landing in the upper-right quadrant of a magical chart doesn't make a vendor the right choice for you.

We divide vendor evaluation into two phases. First we will help you define a short list of potential replacements. Maybe you use a formal Request for Proposals or Information (RFP/RFI) to cull the 15 companies left in the space down to 3-5. You will see soon enough why you can't run 10 vendors through even the next evaluation stage, so you need a way to narrow down the field to get started. At the conclusion of the short list exercise you will test one or two new platforms during a proof of concept (PoC), which we will detail. We don't recommend skipping directly to the PoC, by the way. Each platform has strengths and weaknesses, and just landing in the upper-right quadrant of a

magical chart doesn't make a vendor the right choice for you. And the RFP process usually unearths items you had not considered, so the process is valuable for its own sake.

It is time to do your homework. All of it. Even if you don't feel like it.

The Short List

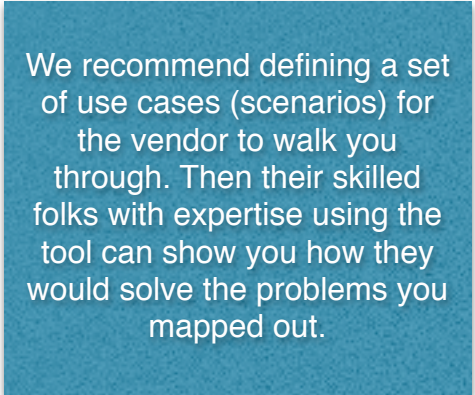
The goal at this point is to whittle the list down to 3-5 vendors who appear to meet your needs, based on the results of the RFIs or RFPs you sent out. The answers should quickly disqualify a few who lack critical capabilities. The next step, for the surviving vendors, is to get a better sense of products and companies.

Your main tool at this stage is the *dog and pony show*. The vendor brings in their sales folks and sales engineers (SEs) to tell you how their product is awesome and will solve every problem you have. Of course they won't be ready (unless they read this paper as well) for the intensity of your KGB-style interrogation. You

know what is important to you, and you need confidence that any vendor passing through this gauntlet to the PoC can meet your requirements.

Let's talk a bit about tactics for getting the answers you need, based on deficiencies with the existing product (from your earlier platform evaluation). You need detailed answers at these meetings to objectively evaluate any new platform. You don't want a 30-slide PowerPoint walkthrough and generic demo. Make sure the challenger understands your expectations ahead of the meeting so they have the right folks in the room. If they bring the wrong people cross them off. It's as simple as that — it's not like you have time to waste.

We recommend defining a set of use cases (scenarios) for the vendor to walk you through. Then their skilled folks with expertise using the tool can show you how they would solve the problems you mapped out. This forces them to think about **your** problems rather than their scripted demo and shows off capabilities that will be relevant to you, instead of the smoothness of the folks staging the demo. You don't want to buy from the best presenter — you want to identify the product that best meets your needs, and that means making the vendor convince you their product can do what **you** need.



We recommend defining a set of use cases (scenarios) for the vendor to walk you through. Then their skilled folks with expertise using the tool can show you how they would solve the problems you mapped out.

Here are a few scenarios to help you set up these meetings. Prioritize this list based on your own needs, but this should get you 90% of the way through narrowing down the list.

- **Security:** Your first scenario should focus on security. That's what this ultimately boils down to. You want to understand how they would detect an attack based on their information sources and how they configure rule sets and alerts. Make it detailed but not ridiculous. Simplify your existing environment a bit and run them through an attack you saw recently. This is a good exercise for seeing how the data they collect solves a major use case: quickly detecting an emerging attack. Have the SE walk you through setting up and customizing a rule. Use your own scenario to reduce the likelihood of the SE using a pre-built rule. You should really understand how the rules work — you will spend a lot of time configuring and maintaining your rules, so it's useful to see how easy it is for their SE to create new ones.
- **Compliance:** Next you need to understand how much automation is available for compliance. Ask the SE to show you the process of preparing for an audit. And no, showing you a list of 2,000 reports called "PCI X.X" is not sufficient. Ask them to produce samples for a handful of critical reports you rely on to see how closely they hit the mark — it's easy to quickly spot the difference between reports developed by an engineer and those created by an auditor. You need to understand where the data comes from, and hopefully they have a demo data set to generate reports from. The last thing you want is to learn that the reports didn't pull from the right data sources, two days before an audit.

- **Integration:** In this part of the discussion delve into how the product will integrate with your existing IT stack. How does the platform pull data from your identity management system? CMDB? Learn about their process for data collection. Are the connectors pre-built and maintained by the vendor? How would you use custom connectors? Can you build those yourself via an SDK, or does all customization require expensive professional services? What about collecting threat feeds and integrating alerts with other products? You want to fully understand what kind of citizen the SIEM will be in your IT neighborhood, so don't leave any questions unanswered.
- **Forensics:** Vendors throw around the term *root cause analysis* frequently, rarely substantiating how tools work through an incident. The SE should literally walk you through an investigation based on their sample data. Yes, you will test this yourself later during the PoC, but get a feel for the built-in tools and how they can be used by the SE, who should really know how to use the system.
- **Scalability:** If your biggest issue is a requirement for more power, you will want to know — at a very granular level — how each challenger solves the problem of scalability given the tsunami of data collected. Dive into their data model and deployment architectures, and have them tell stories about their biggest implementations. If scalability is a problem for the incumbent you will know how big the system needs to get, and understand whether a proposed architecture passes the sniff test.
- **Additional Data Types:** Collect application data and build some rules. The SE should walk you through the entire process: how they look at a data schema, setting up the collector, and creating a few rules to leverage the new data. You aren't looking for empirical correctness but you need to know whether unnatural acts are required to support additional data types. The less work required to get data in and get value from it, the better off you are.

Depending on your requirements and your platform evaluation, you may need to go through other areas with each vendor. This list only covers the major items — adjust and add scenarios for your own priorities.

This type of meeting could be considered cruel and unusual punishment. But you need this level of detail before you commit to actually testing a product or service.

This type of meeting could be considered cruel and unusual punishment. But you need this level of detail before you commit to actually testing a product or service. Remember, this evaluation happened because the incumbent failed to get it done. Shame on you if you don't ask every question to avoid making the same mistakes again. Don't worry about making the SE uncomfortable — this is their job.

And don't expect to get through a meeting like this in 30 minutes. You will likely need a half-day minimum to work through all these scenarios. That's why you will probably only bring 3-5 vendors in for these meetings. You will be spending days with each product during proof of concept, so try to disqualify products that won't work before wasting much time on them. This initial meeting can be a painful investment of time — especially if you realize early that a vendor won't make the cut — but it is worth doing anyway. You can thank us later.

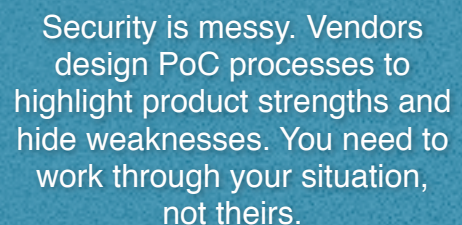
After you finish the ritual humiliation of vendor sales teams you will have a very good idea of which products or services might fit. But that's not enough, so you also need to get hands on with the systems and run each through its paces for a couple days. The next step in the process, the Proof of Concept (PoC), is the most important. If you took part in selection of the incumbent product you will be better off this time. You didn't know anything back then. Now you know what works — and more importantly what doesn't — and your evaluation will be better for it.

Security Ballet

With luck you have narrowed down your list to a couple good candidates. If one or two more meet your initial requirements that is no bad thing, but it makes the PoC process longer and a bit bloodier. The proof of concept is where sales teams smell blood, and vendors bring their best and savviest to bear. They raise doubts about competitors. They highlight how their product was selected over competitors at major accounts. They have phone numbers for customer references handy. For now forget all that. **You are running this show, and the PoC needs to follow your script, not theirs.**

Most SIEM vendors want to start by pushing you through a 3-5 day evaluation of their technology on their terms, with their guy driving. They like to airdrop tuned appliances or servers in, with their demo all prepared. You pick a few key use cases, and then the SE stands the product up and runs through them — they say it's easy because all their customers do the same thing. They like to bring in a defined set of activities for each day and end the test with a good idea of how their technology works. It looks like a well-rehearsed version of the *Nutcracker*, where each participant precisely executes their assigned task. Everything quick and painless — just like security, right?

Wrong! Security is messy. Vendors design PoC processes to highlight product strengths and hide weaknesses. We know this from first-hand experience — we have built them for vendors in past lives. You need to work through your situation, not theirs. Find the warts now — not while responding to an incident. It is bizarre that some vendors get scared by an open PoC process, but their goal is to win the deal, so they put a lot of sweat into scripting a process so it goes smoothly. But smooth sailing is not the point! The vendor will always say they can do 'it' — regardless of what exactly 'it' might be. Your job is to find out how well — or badly — they actually perform.



Security is messy. Vendors design PoC processes to highlight product strengths and hide weaknesses. You need to work through your situation, not theirs.

Before you start a PoC we recommend establishing evaluation criteria based on your requirements and use cases from earlier in this process. Your criteria don't need to be complicated. Your requirements should spell out the key capabilities you need, with a plan to further evaluate each challenger based on intangibles such as set-up/configuration, change management, customization, user experience/ease of use, etc. *Before you start, have your team assess your current platform against the criteria as a baseline.*

We recommend investing in screen capture technology. It is hard to remember exactly what each tool did and how — especially after you have worked a few unfamiliar tools through the same paces. So capture as much video as you can of the user experience — it will come in very handy as you reach the decision point.

Without further ado, let's jump into the PoC.

Driving the PoC Bus

One advantage of testing security management products is that you can actually monitor production systems without worrying about blowing them up, taking them down, or adversely impacting anything. So do that. Pull data from your firewalls, your IDS/IPS systems, and key servers. Not all devices, of course, but enough to get a feel for how to set up the collectors. The point is to run things according to your needs, with your data, alerting on your policies. Remember that *you* drive the bus, and don't get taken for a ride. You will also want to configure a custom data source or two and integrate with your directory store to see how that works. Actually run through the full configuration and bootstrap the system in your environment.

If compliance is your key requirement use PCI as an example. Start pulling data from your protected network segment. Pump that data through the PCI reporting process. Is the data correct and useful to everybody interested? Are the reports comprehensive? Will you need to customize them for any reason? How easy is that? You need to answer these kinds of questions during the PoC.

Pay attention to visualization and user interface. Security systems are not only used by security professionals. A configurable UI makes it easier for a wider audience of users to contribute to and benefit from the SIEM platform. Configure some dashboards and see the results. Mess around with reports a bit. Tighten the alert thresholds. Does the notification system work? Will alerts work in a timely fashion at enterprise volumes? Is the information in the dashboards and reports useful? These are all things you need to check as part of kicking the challengers' tires.

Run a Red Team

Run a simulated attack against yourself. We know actually attacking production systems would make you very unpopular with the ops folks so set up a lab environment. Virtual environments are perfect for this — use the same base images for each vendor. The situation should be as realistic as possible. Have attackers breach test systems with attack tools. Have your defenders try to figure out what is going on as it's happening. Does the system alert as it should? Will you need to heavily customize rules? Can you identify the nature of attacks quickly? Does their super-duper forensic drill-down give you the view you need? The clock is ticking — how easy is it to use the system to search for clues?

Obviously this isn't a real incident so you can take some editorial liberties, and that's fine. You want a feel for how the system performs in near-real-time. If an attacker is in your systems, will you find them? In time to stop or catch them? Once you know attackers are in, can you tell what they are doing? A red team exercise as part of the PoC will help determine that.

Hopefully nobody died in the process, but you want to evaluate both successes and failures of the PoC in terms of your priorities.

The Postmortem

Hopefully nobody died in the process, but you want to evaluate both successes and failures of the PoC in terms of your priorities. When you finish a red team exercise you should have a bunch of data that nicely illustrates what the attack team did — and perhaps what the defense team didn't do as well as they could have. This is a learning experience for everyone, and real attack scenarios provide a good indication of the value of these platforms. Knowing a tool will hold up in the heat of battle goes a long way toward giving security and operations teams

confidence when they go live. Now ask, "How does it compare to our existing product for comparable functions?" This should help determine a contender's suitability for your business.

You cannot fully test scalability during a PoC so focus on the stuff you can see, feel, and touch. That's the user experience, and there is no better way to distill out the effectiveness of a challenger than to stage an attack. Your team should grade each candidate while memory is fresh and perceptions are raw. After spending a week or two with another product they won't remember what they liked and didn't about earlier ones — another reason screen grabs are handy.

Lather, Rinse, Repeat

You will probably test more than one product or service, so you get to do it all again. Given the resource-intensive nature of the testing process, you probably cannot put more than a couple products through a comprehensive PoC, but use the same scenarios for each. Consistency helps make the challenge fair and comparisons more meaningful.

Now you have all the information you need to make a decision, so it is time to figure out what to do, and to gather data to substantiate your choice for the internal sales process. You can use the grades and videos you collected for each competitor — especially to make the case for a new platform, if that's what you decide. There is method to our madness.

Given the resource-intensive nature of the testing process, you probably cannot put more than a couple products through a comprehensive PoC, but use the same scenarios for each. Consistency helps make the challenge fair and comparisons more meaningful.

The Selection Process

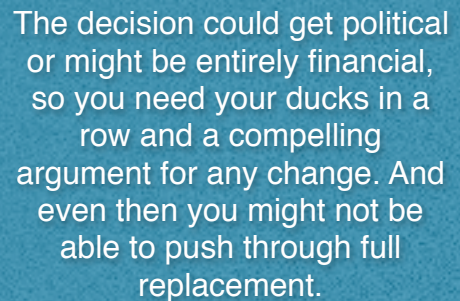
With vendor evaluations in hand, you are ready to make your decision, right? The answer is both ‘yes’ and ‘no’. You probably know what direction you want to go, but now you have to go through a structure process to ensure everyone else is on board. We know the importance of this decision — you are here because your first attempt at this project wasn’t as successful as it needed to be. After the vendor evaluation process you are in a position to distinguish innovative technologies from pigs wearing fresh lipstick.

Now you need to see which vendor is actually the best fit. Successful decision-making on SIEM replacement goes beyond vendor evaluation — it requires evaluating yourself too. It is important to differentiate between the two because you cannot make the best choice without taking a long hard look at yourself, your team, and your company. This is an area where many projects fail, so we will break the decision down to ensure you can make a good recommendation and feel comfortable with it.

But vendor selection is more complicated than simply matching needs against capabilities. The output of our Security Management 2.5 process is not really a decision — it is more of a recommendation. The final decision will likely be made in the executive suite. That’s why we focused so much on gathering data, preferably quantitative — you will need to defend your recommendation until the purchase order is signed, and likely afterwards.

Defensible Position

We won’t mince words. This decision generally isn’t about objective or technical facts — especially because most of you reading this have an incumbent, who typically has important relationships with heavies inside your shop. The decision could get political or might be entirely financial, so you need your ducks in a row and a compelling argument for any change. And even then you might not be able to push through full replacement. In that case the answer might be to supplement — you still aggregate the information currently being collected by the existing platform because it’s already in place, but then you feed portions of the data and collect new data sources using the new platform to perform advanced analysis, reporting, and forensics across the enterprise. The cost of running both makes this scenario unacceptable for many organizations, but if your hands are tied on a full replacement, this kind of creative approach is worth considering.



The decision could get political or might be entirely financial, so you need your ducks in a row and a compelling argument for any change. And even then you might not be able to push through full replacement.

But that is still only the *external* part of the decision process you need to sell to management. In many cases the (perceived) failure of the existing SIEM may be self-inflicted. So you also need to evaluate and explain the causes of that failure, with assurance that you can avoid them this time. If not your successor will be in the same boat in another 2-3 years. So before you put your neck on the chopping block and advocate for change — if that is what you decide — it is time for deep introspection.

Looking in the Mirror

First let's make sure you really re-examined the existing platform in terms of your original goals. Did they adequately map your needs at the time? Did you fail to anticipate any requirements? Did some of the things you thought were important back then end up being unimportant? How have your goals changed over time? Be honest! Do not let ego get in the way of doing what's right, and take a hard and fresh look at the decision to ensure you don't repeat previous mistakes. Did you kick off this process because you were pissed at the original vendor? Or because they got bought and seemed to forget about the platform? Do you know whether the incumbent is *capable* of satisfying your requirements? If yes, what would it take to get there? Is it a question of throwing professional services at the issues? Is there a fundamental technology problem?

Yes, the new generation of platforms requires less expertise to keep operational, but don't be naive — no matter what any sales rep says, you cannot simply set and forget a SIEM system.

Did you assess the issues critically the first time around? If there was a skills gap on your side, have you successfully addressed it? Are your folks in a better position to build and maintain the selected platform moving forward? Are you looking at a managed service to take that concern off the table? If it was a resource problem, do you now have enough staff for proper care and feeding? Yes, the new generation of platforms requires less expertise to keep operational, but don't be naive — no matter what any sales rep says, you cannot simply set and forget a SIEM system. *Whatever* you pick will require expertise to deploy, manage, tune, and analyze reports. These platforms are not self-

managing — by a long shot.

Your choice is no simple matter of black vs. white, but the merit of your argument (and your commitment) to replace the incumbent platform will become clear when you need to sell it to management. Some of you may worry that management will see the need for replacement as “your fault” for choosing the incumbent, so be sure you have answers to those questions, and that you aren't falling into a self-delusional trap. You need your story straight and motivations clear. Bring a straightforward and honest assessment of what is going right and wrong, so you are not caught off-guard when asked to justify changes and new expenses.

Setting Expectations

Revisiting requirements provides insight into what you need a security management platform to do.

Remember, not everything can be Priority #1, which is why you picked and prioritized the top three must-have use cases.

If you love some new features of the challenger, will your organization leverage them consistently? Firing off alerts faster won't help if your team takes a week to investigate each issue, or cannot keep up with the

increased workload. The new platform's ability to look at application and database traffic doesn't matter if your developers won't help you understand normal behavior to build the rule set. Fancy network flow analysis can be a productivity sink if your DNS and directory infrastructure is a mess and you can't reliably map an IP to a user.

Does your existing product have too many features? Some organizations simply cannot take advantage of (or even handle) complex multi-variate correlation across the enterprise. Do you need to aggregate logs because organizational politics, or your team's resources or skill set, prevent you from getting the job done otherwise? This might be a good reason to outsource or use a managed service. It's less about being 'right' and more about being honest, so you don't land you in the hot seat again.

Is it realistic to think you can deploy a common rule set across your enterprise? All these extra capabilities

Don't expect people or politics to change just because the organization gains the ability to monitor across the enterprise. Having a technical capability doesn't mean you will have agreement on whether or how to use it.

are great, and we recommend central management and reporting to ensure consistency, but all too often companies delegate IT maintenance down to each division, and it takes an act of Congress to get them in the same room — much less to agree on policy. Don't expect people or politics to change just because the organization gains the ability to monitor across the enterprise. Having a technical capability doesn't mean you will have agreement on whether or how to use it. Don't forget the realities of your organization either. Will people regard this whole project as snooping or unwelcome interference? That could seriously impede project success, so you may need to actively manage expectations.

If you kicked off this effort because the existing SIEM missed something and that resulted in a breach, can you honestly say the new platform *would* (not *might*) detect that attack? Was it really because you were just missing some data that would have enabled detection, or was the failure more systemic? We have certainly seen high-profile breaches result in tossing the old and bringing in the new (someone has to pay, after all), but make sure you address the real cause of the problem. And make sure you evaluate the right tool. If you were compromised by a persistent attacker you might be looking at the wrong technology. Maybe you really need full packet capture. Maybe not, but shame on you if you don't at least ask yourself.

Economics

Even when introspection and expectations line up, economic reality might not. IT groups need to tackle more responsibilities with tightening budgets, and that trend is not changing. So you need to weigh the cost of getting the existing product functional against replacing it. Even if you want to stack the deck against the incumbent, don't forget the time and money to train folks on the new tool — or professional services to migrate your existing rules, data sources, and data. If you managed to get some of that done during proof of concept that's great, but there is certain to be more as you move toward full deployment.

Sure, the new platform may do a lot more, but at what cost? If essential reports do not get produced, or you find yourself running on what feels like a deprecated platform, you still need to account for purchase, maintenance, deployment, customization, and training on the new thing. Make sure you consider *total* and not merely *procurement* cost. Even OpEx was real money last we checked.

Documentation

The end goal is a recommendation, so you need to document what you think and then present it to the folks with the money. You may not always be in the room when decisions are made so your documentation must clearly articulate the reasons for change. We normally structure that artifact of the decision process in a consistent way.

- **Requirements:** Tell them what you need and who said you need it. Compliance and security requirements come from different groups, so make sure these dependencies are referenced.
- **Current product evaluation:** What works and doesn't with the existing solution within the context of your requirements, both now and as requirements evolve.
- **Challenger assessment:** Summarize the work you did to find the next platform. Which vendors did you disqualify and why? What did you learn in the proof of concept? Which competitor came out on top? How did that competitor stack up relative to the incumbent?
- **Cost estimate:** What would it cost to move to the new platform? How much is capital expense and what fraction is operational? What kind of investment in professional services would be required? How does that differ from making incremental improvements to the incumbent, and what functionality are you sacrificing in the move?
- **Migration plan:** If you ultimately decide to replace the SIEM, what will the migration look like? How long will it take? Will the migration entail disruption of any services? Will you be more exposed to attack, and if so for how long? You need all these answers before you pitch to the powers that be. Not a Gantt chart — that comes at the end — but enough to answer the tough questions.
- **Recommendation:** Your entire document should be building to this point, where you put the best path down on paper. If it is a surprise to your audience you did something wrong. This is about telling them what they already know and making sure they have an opportunity to ask any remaining questions.

But when you make your recommendation the decision is far from done. Now you have to negotiate with the new vendor (or the incumbent) and get sign-off from senior management. This is when your process is most vulnerable. Negotiations around price and services could be challenging. Additionally, an incumbent losing the deal will act desperately to save it. Challengers will do likewise if they think you are staying put or choosing a competitor.

Negotiation

You made your decision and kicked it up the food chain — now the fun begins. Well, fun for some people, anyway. For the first half of this discussion we will assume you have decided to move to a new platform and offer tactics for negotiating for a replacement platform. But some organizations decide not to move, using the potential switch for negotiating leverage. It is great to stay with an existing platform, so long as you have done the work and know it can meet your requirements. We wrote this paper for the people who keep telling us about their unhappiness, and how evolving requirements have not been met. But after asking all the right questions, if the best answer is to stay put, that's clearly a less disruptive choice.

Replacement Tactics

For now, though, let's assume your current platform won't get you there. Now your job is to get the best price for the new offering. Here are a few tips to leverage for the best deal:

- **Time the buy:** Yes, this is Negotiation 101. Wait until the end of the quarter and squeeze your sales rep for the best deal to get the PO in by the last day of the month. Sometimes it works, sometimes it doesn't, but it's worth trying. The rep may ask for your commitment that the deal will, in fact, get done that quarter. Make sure you can deliver if you pull this card.
- **Tell the incumbent they lost the deal:** Next get the incumbent involved. Once you put in a call letting them know you are going in a different direction they will probably respond. Not always, but generally the incumbent tries to save the deal. And then you can go back to the challenger and tell them they need to do a bit better because you got this great offer from their entrenched competition. Just like buying a car, to use this tactic you must be willing to walk away from the challenger and stay with the incumbent.
- **Look at non-cash add-ons:** Sometimes the challenger can't discount any more. But you can ask for additional professional services, modules, boxes, licenses, whatever. With new data analytics, your team might lack some in-house skills for a successful transition — in which case the vendor can help. Remember, the incremental cost of software is zero, zilch, nada — vendors can often bundle in a little more to get the deal when pushed to the wall.
- **Revisit service levels:** Another non-cash sweetener could be an enhanced level of service. Maybe it's a dedicated project manager to get your migration done. Perhaps it's Platinum support, even if you pay for Bronze. Given the amount of care and feeding required to keep any security management platform tuned and optimized, a deeper service relationship could come in handy.

- **Dealing with your boss's boss:** One last thing: be prepared for your recommendation to be challenged, especially if the incumbent sells a lot of other gear to your company. This entire process has prepared you for that call, so just work through the logic of your decision once more, making clear that your recommendation is best for the organization. But expect the incumbent to go over your head — especially if they sell a lot of storage or servers to your company.

Negotiating with the Incumbent

Until the process reaches a conclusion, sticking with the incumbent will remain on the table. So it is good to know how to *leverage* both sides for a better deal. Dealing with an incumbent who doesn't want to lose business adds both complexity and opportunity to the decision: price cuts may entice you, management, or the CFO to prefer a particular player. Customers need to be prepared for vendor efforts to save the business. It would be naive not to prepare in case the decision goes the other way — due to pricing, politics, or another reason beyond your control. If you need to make the *status quo* work and keep the incumbent, here are some ideas for making lemonade from the proverbial lemon:

- **Tell the incumbent they are at risk:** If the incumbent didn't already know they were at risk, it can't hurt to tell them. Some vendors (especially the big ones) don't care, which is probably one reason you were looking at new stuff anyway. Others will get the wake-up call and try to make you happy. That's the time to revisit your platform evaluation and figure out what needs fixing.
- **Get services:** If you have to make do with what you have, at least force the vendor's hand to make your systems work better. Asking a vendor for feature enhancement commitments will likely only compound your disappointment — their failure to execute got you both into this spot in the first place — but there are many options at your disposal. If your issue is not getting proper value from the system, push the incumbent provide professional services to improve the implementation. Perhaps you should send your folks to training. Push for their team to set up a new set of rules and transfer knowledge. We have seen organizations literally start over with the incumbent, which makes sense if your initial implementation is sufficiently screwed up.
- **Scale up (at lower prices):** If scalability is the issue, confront that directly with the incumbent and request additional hardware and/or licenses to address the issue. Of course it might not be enough but every little bit helps, and if moving to a new platform isn't an option at least you may be able to ease the problem. Especially when the incumbent knows you were looking at new gear because of a scaling problem.
- **Add use cases:** Another way to get additional value is to request additional modules thrown into a renewal or expansion deal. You can add the identity module or look at configuration auditing. Or work with the team to add database and/or application monitoring. Again, the more you use the tool, the more value you will get, so figure out what the incumbent will do to make you happy.

Honestly, if you *must* stick with the existing system, you have little flexibility and less leverage. The incumbent doesn't need to know that, though, so use the specter of migration. But at the end of the day it is what it is.

Migration

If you made it this far we know your old platform is akin to an old junker you drive to work every day: noisy, uncomfortable, costly, unreliable, and every time you turn around you're spending more money to fix something. With cars figuring out what you want, shopping, getting financing, and then dealing with sales people is no picnic, but in the end you do it to make your life a bit easier and yourself more comfortable. It is important to remember this because at this stage of SIEM replacement it feels like we have gone through a lot of work just so we can do more to roll out the new platform. Let's step back for a moment to focus on what's important: getting stuff done as simply and easily as possible.

At this stage of SIEM replacement it feels like we have gone through a lot of work just so we can do more to roll out the new platform.

Now that you are moving, how do you get there? The migration process is not easy, and it takes effort to move from the incumbent to the new platform. We have already outlined a disciplined and objective process to determine whether it is *worth* moving to a new security management platform. Now we will outline a process for implementing the new platform and transitioning from the incumbent. *You need to implement, and migrate your existing environment to the new platform, while maintaining service levels, and without exposing your organization to additional risk.* This may involve supporting *two systems* for a short while or using two systems in a hybrid architecture — perhaps indefinitely.

Either way, when a customer puts his or her head on the block to select a new platform, the migration needs to go smoothly. There is no such thing as a 'flash' cutover. We recommend you start deploying the new SIEM long before you get rid of the old. At best you will deprecate portions of the older system after newer replacement capabilities are online, but you will likely want the older system as a fallback until all new functions have been vetted and tuned. We learned the importance of this staging process the hard way. Ignore it at your peril — security management supports several key business functions.

Plan

Our migration plan for moving to the new security management platform covers data collection as well as migrating and reviewing policies, reports, and deployment architectures. We break the migration process into planning and implementation phases. Your plan needs to be very clear and specific about when things get installed, how data gets migrated, when you cut over from old systems to new, and who performs the work. The planning step leverages much of the work done so far to evaluate replacement options — you just need to adapt it for migration.

- **Review:** Go back through the documents you created earlier. First your platform evaluation documents will help you understand what the current system provides and identify key deficiencies to address. These documents become the priority list for migration — the basis for your migration task list. Next leverage what you learned during the PoC. To evaluate your new security management platform provider you conducted a mini deployment. Use what you learned from that exercise — particularly what worked and didn't — as input for subsequent planning, and address the issues you identified.
- **Focus on incremental success:** What do you install first? Do you work top down or bottom up? Will you keep both systems operational throughout the migration, or shut down portions of the old as each function migrates? We typically recommend using your SIEM's deployment model to guide implementation. For example when using a mesh deployment it is often easiest to make sure a single node/location is fully functional before moving on to the next. With ring architectures it is generally best to get the central SIEM platform operational, and then gradually add nodes around it. Hierarchical models are best deployed top-down, with the central server first, followed by regional aggregation nodes in order of criticality, down to the collectors. For platforms that employ big data style architecture, you simply add nodes to scale up. Break the project up to build incremental successes and avoid dead ends. You can learn more about these models by checking out [Understanding and Selecting a SIEM](#)⁶.
- **Allocate resources:** Who does the work? When will they do it? How long will it take to deploy the platform, data collectors, and/or log management support system(s)? This is also the time to engage professional services and enlist the new vendor's assistance. The vendor presumably does these implementations all day long, so they should have expertise estimating timelines. You may also want to engage them to perform some (or all) the work in tandem with your staff, at least for the first few locations, until you get the process down.
- **Define the timeline:** Estimate the time it will take to deploy the servers, install the collectors, and implement your policies. Include time for testing and verification. There are likely to be some guesses but you have some reasonable metrics to plan on from your experience with the PoC and implementing the existing SIEM. You did document the PoC, right? Plan the project commencement date and publish to the team. Solicit feedback and adjust before commencing because you need shared accountability (particularly with Operations) to ensure everyone is invested in success.
- **Preparation:** We recommend you do as much work as possible before migration, including construction of the rules and policies you will rely on to generate alerts and reports. Specify in advance any policies, reports, user accounts, data filters, backup schedules, data encryption, and related services you can. You already have a rule base so leverage it to get going. Of course you will tune things as you go, but why reinvent the wheel or rush if you can avoid it? You will always find something you failed to plan for — often an unexpected problem — that sets your schedule back. But preparation helps spot missing tasks and makes deployment faster.

⁶ <https://securosis.com/research/publication/white-paper-understanding-and-selecting-siem-log-management>

It is helpful for team morale, not to mention the confidence of upper management, to demonstrate the value of the new platform early on. Plan some “quick wins” into the migration process where possible. Delivering what you already have in the incumbent platform may be critical to long-term success, but completely uninspiring to the people deciding your bonus. If there are key facets of the new platform that can be delivered early in the implementation process, it is worth your time to do so.

Implement

The migration need not (and in fact generally *should not*) be an all-at-once exercise — you have the luxury of doing one piece at a time in the order that best fits your requirements.

- **Deploy platform(s):** This varies based on deployment model as discussed above, but typically you install the main security management platforms first. Once the basic system configuration, identity management and access control integration, and basic network configuration are in place, connect to a couple data sources and other aggregation points to make sure the system is operating correctly.
- **Deploy supporting services:** Deploy data collectors and make sure event collection is working correctly. If you use a flat deployment model configure the platform to collect events for the first set of deployment tasks. If you use a Log Management/SIEM hybrid or regional data aggregators, install the additional aggregation points and get them feeding data into the primary SIEM system to confirm proper information flow — at a small scale — before ramping up event traffic. If you are moving to a new platform for real-time analysis, make sure event collection happens properly. Your only concern right now should be getting data into the system in a timely fashion — tune it later.
- **Install policies and reports:** Next deploy the rules that comb through events to find anomalies. Hopefully you created as many as possible during the PoC and planning stages, and perhaps you can leverage your initial implementation. For real-time analysis you need to tune those rules to optimize performance. Remember that each additional rule incurs significant processing cost. It is simple math: correlating multiple data sources against many rules causes the system to do exponentially more work, reducing effective performance and throughput. Look for ways to create rules with fewer comparisons, and balance fine-tuning rules for specific problems against more generic rules that catch many problems. Sometimes you can throw a bigger server at the problem to handle more events, but more efficient policies are always worthwhile.
- **Test and verify:** Are your reports being generated properly? Are the correct alerts generated in a timely fashion? Generate reports, send them to the team for review, and compare what comes out of the new system to reports from the existing platform — which should still be operational. For alerts and forensic analysis it makes sense to rerun your “Red Team” drill from the PoC to make sure you catch anomalies and confirm the accuracy of your results. Verify you get what you need — *now* is the time to find any problems, while you still have a chance to find and fix them, before you start depending on the new platform.

- **Stakeholder sign-off:** Get it in writing — trust us, this will save aggravation in the future when someone from Ops says: “Hey, where is XYZ? I still need it!” Have the compliance, security, and IT ops teams sign off on project completion — they should own it now too. Make sure the group is satisfied and any outstanding issues are documented.
- **Decommission:** *Now* you can retire the older system. You may choose to run the incumbent SIEM for a few months after the new system is fully operational, just in case. But there are not many reasons to keep it around long, and plenty of reasons to get rid of it. Older agents and sensors should be removed, user accounts dedicated to the older platform locked down, and hardware and virtual server real estate reclaimed. Once again, someone will need to be assigned the work with an agreed-on time frame for completion.

Conclusion

Security Management 2.5 is a series of recommendations for deciding whether you need to replace your existing security platform, and if so how. Did you decide it was time for a new SIEM? Let's review the critical bits:

- **Requirements rule:** Take this opportunity to figure out what you *really* need — not what the vendor says you can do, or what users read in a trade rag. Defining your requirements is the linchpin of the entire process so make sure you do it well.
- **Do the work:** When a project is perceived as a failure, the inclination is to just change in hopes the next thing will be better. Ultimately that might be the right answer, but don't embark on such a major project based purely on blind optimism. Evaluate your existing platform objectively and assess the challengers skeptically. Everything looks shiny in a PowerPoint deck, so run a PoC to see what will really work in your environment.
- **Be creative:** In the event you are unable to totally replace your incumbent, you may need to think out of the box a bit to address capability gaps with the existing SIEM. You might want to consider supplementing it, either with a different platform or a managed service. Stay focused on the problems you need to solve (defined when revisiting your requirements) and use your requirements to make a compelling case for the necessity of investment in supplemental technology or services.
- **Be inclusive:** Any security management technology needs to be leveraged across the organization — if only for dashboards and reports — so make it as inclusive as possible. That means getting buy-in from not just the senior team and the money folks, but also from ops and administrators. If you plan to capture data from application and database sources include those teams in the process. You need their help so they should share responsibility for making the project succeed.
- **Get quick wins:** Focus on achieving consistent success. That means starting slowly with areas you know will work well. Get one thing done correctly before moving on to the next. Most likely this whole process stems from issues with the incumbent, so make sure the new tool will work well, which requires finishing what you start.

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 Authors

Adrian Lane, Analyst and CTO

Adrian Lane is a Senior Security Strategist with 25 years of industry experience. He brings over a decade of C-level executive expertise to the Securosis team. Mr. Lane specializes in application, database, and data security. With extensive experience as a member of the vendor community (including positions at Ingres and Oracle), in addition to time as an IT customer in the CIO role, Adrian brings a business-oriented perspective to security implementations. Prior to joining Securosis, Adrian was CTO at database security firm IPLocks, Vice President of Engineering at Touchpoint, and CTO of the secure payment and digital rights management firm Transactor/Brodia. Adrian also blogs for Dark Reading and is a regular contributor to Information Security Magazine. Mr. Lane is a Computer Science graduate of the University of California at Berkeley with post-graduate work in operating systems at Stanford University.

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:

- **The Securosis Nexus:** The Securosis Nexus is an online environment to help you get your job done better and faster. It provides pragmatic research on security topics that tells you exactly what you need to know, backed with industry-leading expert advice to answer your questions. The Nexus was designed to be fast and easy to use, and to get you the information you need as quickly as possible. Access it at [<https://nexus.securosis.com/>](https://nexus.securosis.com/).
- **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/or 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/>](http://securosis.com/).