360 IS

information Security

Preparing for Security Event Management

Methods and tactics for avoiding failure in large SEM implementations

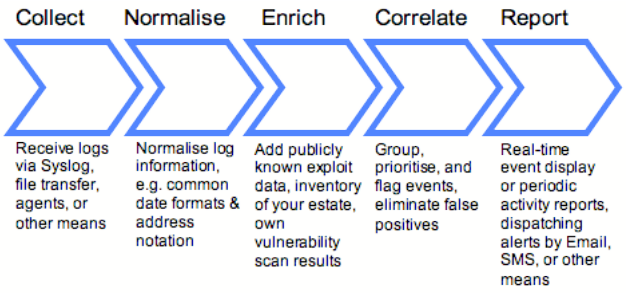
Many will be familiar with the English proverb “more haste, less speed”, or to put it another way, finishing a task quickly is not about rushing. This advice could have been tailor made for complex IT projects. In this paper we learn how to mitigate some of the risks and reduce the costs associated with implementation of Security Event Management systems, arguably among the most complex and highest profile information security projects undertaken today.

Introduction to SEM

What is it?

A Security Event Manager is a piece of software which takes as input logs and alerts from a variety of systems, such as Firewalls, Routers, and Servers, and attempts to inform the engineer of unusual occurrences which warrant further investigation. The SEM benefits from having available to it information coming from many systems at both the network and application level, having an understanding of event severity, and may also have access to vulnerability databases which describe common weaknesses and their exploitation. SEM software may also feature tools to aid the analyst charged with investigating events and producing reports. There has been a vendor-fuelled explosion in acronyms around SEM, and you will see them referred to variously as SEM, SIM, CSEM, CIEM, and ESM systems. All of these perform broadly similar functions with differing scalability, utility, user-friendliness, and price. The diagram illustrates the main activities of a SEM system, as their capabilities grow one can expect to see Remediation being added to this list. Although vendors may use different terminology or allude to proprietary methods, all conform to this basic mode of operation.

Figure 1.0 The SEM process



How does SEM help?

IT infrastructure, particularly security systems, produce vast quantities of logging information of varying quality. Although there is some consensus among groups of vendors for specific applications (e.g. Web Servers software) most logs do not conform to any common format, and frequently do not even record the same basic information about what the system in question is doing. Generally one cannot count on the individual routers, servers, and applications having strong log file management capabilities, nor are they able to confer with one-another on the significance of a group of logged events from disparate systems. This means the hard job of the security analyst is made even more difficult. A SEM system is intended to assist in identifying and investigating anomalous events among this glut of data.

How SEM reduces information overload

- Reduces false positives
- Reduces false negatives
- Exclude normal activity from sight
- Consolidates multiple log lines into single “threads” of activity
- Consolidates logs from different systems into single “events”

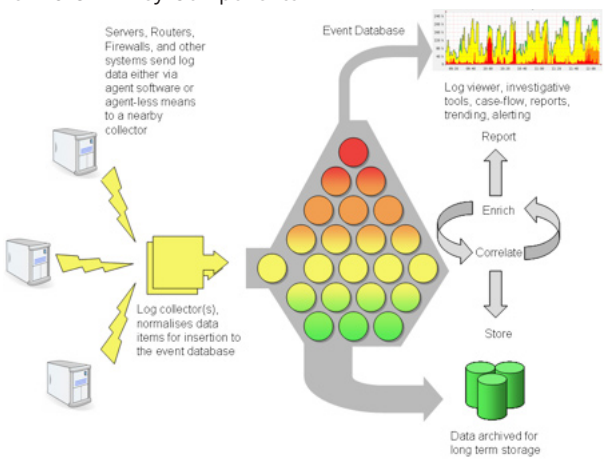
Telephone: **+44 (0)207 871 0454** Facsimile: **+44 (0)870 1340991** E-mail: **sales@360is.com** Website: **www.360is.com**
360 Information Security Ltd. Company Registration Number: 4374942 VAT Registration Number: 776 6209 94

The goal of SEM software is to dramatically improve the signal to noise ratio for the security engineer, and to allow him or her to more easily identify "real" threats from false alarms. In this way SEMs act as a force-multiplier, giving the analyst an ability to do the work of a larger (and possibly more highly skilled) team. Although much is said about the technology involved in the SEM process, ultimately it's all about getting the most out of the human in the loop.

What does SEM look like?

Although there are many SEMs on the market of one sort or another, they all have the same basic components. Each component has a specific task to perform in getting to the final high-grade information product, and may be installed on a discreet server.

Figure 2.0 SEM Key Components



Why Prepare for SEM?

Deployment of a SEM system can be a large, complex affair, requiring integration with several other systems from different vendors. SEM projects represent significant investment in time and money and next to network management systems, they may be the largest undertaking an IT department makes. As with all IT, the larger and more complex the project the greater the risks.

- Implementations can range from a month to up to a year.
- SEMs may require several dedicated servers to be installed.
- Volumes of data and the real-time nature of alerts demand careful consideration of performance and sizing.
- An element of network planning will be required for large, distributed installations. Consider bandwidth demands and modes of failure
- Some systems will require the installation of agents to relay information to SEM collectors, others may be agentless.
- Any ROI from SEM is proportional to the care and attention spent training your analysts in its proper use.

Preparing for this event adequately will deliver benefits not only during SEM installation, but also throughout the life of the system, and will significantly reduce the risks associated with the project. SEM installations cut across organisational and technology boundaries. Within the IT department alone you can expect to involve stake holders in, architecture, operations, help-desk, and security functions. Within business management, you may require the support of compliance, risk management, and of course the sponsoring executive. Because the information needed to properly configure and operate a SEM may reside in so many different departments, it is essential that any SEM project secure buy-in from all stake holders before work begins in earnest. This is a point we shall return-to in the deployment stage of this paper.

Staged Plan

The rest of this document is concerned with the practical steps that an IT organisation can take to achieve the goals listed above. It can be used to form the basis of an internal project plan, a schedule of work for contractors, or a simple checklist of tasks. For all but the simplest SEM installations taking these preparatory steps will affect a net reduction in overall project time. Even the smallest simplest SEM implementation projects should have at least 1 activity in each of these 4 stages. Project managers for larger SEM programs will find it easier to delegate once the job is broken into these stages. A "slow start, quick finish" pace will also improve the quality of the delivered system for its users.

The goals of SEM preparation

- Shorten implementation time
- Reduce amount of professional services required
- Increase signal to noise ratio of information feeding the SEM
- Reduce license and hardware costs
- Extend the lifetime of the SEM
- Increase the SEM's overall value
- Increase utilization & productivity of security staff

Stage 1. Assess

Like the well-prepared barrister, our work begins with a thorough discovery phase. The activity at this point is to gather as much information on your existing information technology and security arrangements as possible within the time available. The aim is to use the information in subsequent phases to maximise the value gained from installing a SEM system. No-doubt your project is already under time pressure, however, remember that time invested at this early stage will pay dividends later.

Activities

- Perform a vulnerability assessment on existing systems and network.
- Catalogue IT assets and the functions they perform, update any configuration management systems.
- Assign a relative or absolute value to the asset or function.
- Identify the current vulnerabilities or potential weaknesses.
- Fix the most serious vulnerabilities for the most valuable assets.
- Review the product of these 5 activities in the light of regulatory and risk management pressures that will lead on to aims.

Aims

- Understand your priorities. What systems to plug into the SEM first, what part of your IT is taking most heat and needs better management most urgently?
- Understand what is critical IT infrastructure and what is not. This is essential later, in order to decide on alert level settings you then configure within the SEM.
- Understand what is logged and what is not, and what detail-level of logging is currently used on your systems.
- Determine what each security product or infrastructure is supposed to be doing, and whether or not it's actually doing it.
- Understand where you need vulnerability remediation before you need event management. SEM software works best when used to monitor well-configured systems, it does not "fix" things that are currently insecure or broken.

Where the suitability of existing systems, configuration, and prior purchase decisions are under scrutiny, you may benefit from an independent, apolitical, eye. The ultimate aim is to establish an acceptable known base line for security. Only then can you move on with the rest of the project.

Takeaway: Risk analysis, prioritisation, then remediation.

Stage 2. Simplify

Attempting to integrate a SEM with unnecessarily complex or contrived infrastructure will generate pain and additional cost at every subsequent stage of the project. The current configuration and placement of security systems may be more complex than necessary, and this is something to be remedied at the earliest opportunity.

Network and IT infrastructure may have changed significantly since your original deployment of Firewalls, IDS, and other security products. Users may have relocated physically or migrated to new methods of accessing their applications and data. Products don't stand still, features and capabilities are added with each release. It may be possible to retire some of your security systems and consolidate networks because their functionality has now been added to other products or the topology no-longer makes operational sense.

Activities

- Review the logical placement of security infrastructure with regard to threats and vulnerabilities catalogued in Stage 1.
- Remove, redeploy, or re-configure existing security products that serve little or no purpose in their current position.
- Review the location of users and the manner in which they access applications and data, do you still operate dial-in remote access when the vast majority of users are now on dedicated VPN over broadband? Take this opportunity to retire legacy access methods, reduce the number of routes into your network.
- Knowing the relative value of systems and networks from Stage 1, consider grouping high value assets together logically in a "green zone" of highest security.

Aims

- Reduce the overall number of security products and systems while maintaining the disciplines of defence in depth and vendor diversity.
- Reduce routes in and out of your networks to a minimum.
- Simplify the job of IDS sensors by grouping systems with the same OS.
- Multiply the effectiveness of the coming SEM installation by logically grouping assets of similar value together.

Opportunities for Increasing Simplicity

Re-Discovering Default Deny

The concept of default deny should be well known to every security engineer and systems administrator. The idea being that since there is a finite and known list of actions we want to allow our users and applications to perform across networks and servers, we will permit just those actions and deny anything else. Default deny makes for short and elegant configuration, fewer events that need investigation, and greater overall security. It necessitates an understanding of what should be happening on your network. Unfortunately it is often implemented only at the Internet gateway, leaving the LAN side as a free-range farm, selectively blocking individual protocols and addresses known to be "bad". Internal Firewalls and router access-lists with default permit policies will subtract value from any SEM implementation since either they must generate vast quantities of events or offer no promise that malicious activity is recorded at all.

- Default deny rewards understanding and incremental tuning.
- Default permit rewards scrambling, long hours, and most of all luck. It reduces the effectiveness of any SEM installation and damages your return on investment.

Not Your Fathers Firewall

As processing power increases, modern security appliances and software are able to do more in a single box than was previously possible. "More" in this context can mean higher bandwidths, additional interfaces, or a greater feature-set. It is possible to take advantage of this to reduce complexity ahead of a SEM installation.

- Network Interfaces are inexpensive and there is now ample CPU power with which to drive them. Consider reducing the overall number of security devices by increasing physical interfaces in modern high-powered appliances.
- Application Proxies were initially popular with security product vendors in the early 90s but later their granularity and rigor was sacrificed by many for speed. With advances in CPU and memory performance, there is now less reason than ever for not using application proxies where they are available in your Firewalls.

Application Proxies:

- May facilitate the retirement of additional devices, e.g. mail relays
- Generally increase the quality of logging information

More Simplicity In Brief

- Further gains in simplicity are to be had through standardisation of cross platform system administration and security tools such as syslog-ng , sudo , and ssh . Thanks to the hard work of the open source community, running different operating systems no-longer means running several different security tools.

- We will leave the broad topic of general server consolidation to others, but multi-CPU, multi-core systems are now available in 1U form factor at very modest cost. Entire server estates can be consolidated into a rack with the aid of virtualisation software. These developments bring obvious benefits to system administrators charged with keeping on top of patching and monitoring. One can easily find current examples of such systems from some well-known vendors .

- Using the discipline of strong compartmentalisation, and by prioritising your deployment of SEM to discreet zones of high-value assets or most exposed systems, it is possible to attain rapid benefits with shorter deployment times than with grand all-encompassing enterprise-wide projects.

Takeaway: Simplifying the network before installing large over-arching management systems, shortens implementation time and provides higher quality input for the SEM to work with while reducing the average number of events per second to contend with.

Stage 3. Tune

Tuning within a SEM context

Although security product categories have blurred (Firewall versus IDS versus IPS) this section is primarily concerned with the major culprit for generating security events, the Network Intrusion Detection/Prevention System. Tuning an IDS can mean different things to different people. For some it means squeezing the maximum raw performance out of hardware by modifying the application, OS, and network configuration. Others take a very practical view of tuning and see it simply as "weeding out false positives".

Tuning strategies, centralised versus decentralised

There is a school of thought, that says don't tune your IDS, leave it running with a full list of signatures and use the centralised IDS management or SEM platform to tune out the noise. This strategy is attractive for a few reasons.

- Little time/effort/skill is required to deploy or hook-up an IDS sensor
- One rule change on the central console filters events network-wide

However there are also some undesirable side effects.

- Event volume may impact network performance in distributed enterprises.
- The requirement to report every event may be too much for your IDS sensors to cope with. If an IDS cannot keep-up with the flow of traffic, information will be lost.
- The cost of your SEM system is broadly proportional to the number of events per second it must handle and potentially store. Expect to pay for the ability to process a "full feed".

Given that we have successfully accomplished Stages 1 and 2, we understand what is happening on the network and have taken the opportunity to simplify things, we advocate some broad tuning of in-place Network IDS sensors in order to reduce the most obvious noise going into the SEM. 1 or 2 simple tuning steps can dramatically reduce the flow of spurious alerts by orders of magnitude.

- UNIX vs Windows

One of the easiest Network IDS tuning activities takes advantage of the fact that you can logically group servers by OS, and so can tell the sensors to selectively ignore Windows attacks directed at UNIX machines and vice versa. This logical grouping does not necessarily mean moving systems and cables. Many modern LAN switches can selectively mirror your traffic based on MAC or IP address to a designated IDS port. Using this combination of intelligent port mirroring and tuned IDS you can opt to show a given sensor "just the UNIX traffic" and so obviate the need for running windows signatures and their false alerts on that sensor/interface.

- Web Servers

Web servers are normally among the most exposed of all systems on a network, because they run large, complex, general-purpose software, and need to be very accessible for impatient users who are unconcerned with "annoyances" like security. These systems are a popular target and may see very high volumes of malicious traffic. If you know which software your organisation has installed, it is possible to screen alerts more effectively. Prime candidates for qualifying in-or-out of your broad signature list include Python, PHP, Perl, ASP, .net, and Content Management software, including free Wiki-type systems

Tuning is never a "solved" problem, whether it is done at the Network IDS or at the SEM. Expect to devote some time each month to adjustments. Some modern IDS couple network scanning with IDS tuning, and facilitate a certain amount of automatic tuning in order to reduce false positives. Such systems typically perform either periodic scans of the network and enumerate operating systems, versions, and applications, or may employ passive fingerprinting to screen alerts before they are raised to the operators attention. Like many active automated response systems, your level of comfort with this technology may vary.

Takeaway: With a few broad rules you can get higher quality information with more signal, and less noise. This means reduced hardware load, less events per second, and greater simplicity.

Stage 4. Deploy

We will leave the intricacies of individual products to the many vendor-authored papers already in circulation. Instead, the focus of this section will be on the generic issues facing all SEM deployments. It is important to realise SEM implementations are no different from any other IT project. Success or failure is dependent mostly on the people involved. Almost all business and technical problems boil down to people problems. We have observed some systematic reasons for this.

Observation	Impact
Peoples status reports are rarely objective	Tasks never complete, deadlines missed
Organisation values compliance, people who don't rock the boat	Early detection of problems is suppressed
Blame culture, people fear losing face, bonus, job	Doomed projects or tasks are not killed

Most failed projects exhibit these signs. One sure-fire indicator of a doomed SEM project is when the project goal is not aligned with business strategy or the information that fuels it simply doesn't exist. We hope that in having followed our advice this far, the latter, if not the former, has already been avoided.

One cannot overstate the value of good project management at this stage, but by listing the common pitfalls in this section, we hope to go some way to mitigating the risk of failure.

Review your expectations

In the interests of ending up with a system that is aligned with business strategy, consider what value the SEM is supposed to deliver. At each decision point in its implementation, keep the businesses expectations in mind.

Some common, simple, business expectations:

- SEM allows you to free up the small, specialist security team from doing day-to-day investigations and device support work.
- SEM facilitates the outsourcing of the intrusion response part of the help-desk, while in-house security engineers remain "SEM administrators".
- SEM allows you to meet compliance requirements for reporting, without large amounts of custom coding and scripting.
- SEM reduces the likelihood that a break-in goes unnoticed and so shortens the clean-up period and reduces overall exposure to risk.
- SEM can provide security staff with situational awareness on unauthorized access, reducing the reaction and response cycle.

Technology deployment considerations

A thorough examination of the relative benefits or weaknesses in different SEM products is beyond the scope of this paper. SEM is a relatively new class of products, and as such continues to evolve rapidly. However there is some generic advice that is worth considering.

- Many organisations find appliance-based systems easier to deploy and support than host-based software. Although it is relatively easy for a vendor to formulate an appliance product (software + hardware + single throat to choke) few ever manage to attain true appliance-level reliability and zero sysadmin time spent on the operating system.
- A fast and reliable event database sits at the heart of all SEM systems, the skills required to tune and maintain it may not reside within your security function.
- A large part of most SEM projects will be spent installing and configuring software agents on your server estate. When evaluating a SEM, get a clear picture of the mix of agent-based and agent-less systems, and how that will impact the work required to deploy.
- A SEM is a distributed system. As such, it is subject to disruption when the links between elements fail or become unreliable. Because of this it is important to understand how the system behaves in the event of partial failure of one or more elements. Critically, are events lost, does recovery require manual intervention, how does the system cope with prolonged outages, what level of redundancy is possible?
- If your IT assets are distributed, can the communication paths between them be encrypted when appropriate? Similarly, when considering low-bandwidth branch-site systems, do agents have the ability to compress event flows before transmission?
- Can the SEM be integrated with, or link-to, your policy management software or repository? If SEM operators are expected flag potential violations of policy that may not constitute intentional unauthorized access, they will need to reference original policy documents and procedures.

People deployment considerations

For all the talk of proprietary software and "hundreds of events per second", for now at least SEM is a tool to be used by people, and not a machine-to-machine system. Many of these people have to divide-up their day between proactive and reactive enforcement of your organisations security policy, only occasionally dipping into the SEM console. Because of this, people-considerations must form a large part of this stage.

Choosing SEM implementation staff

Implementing a SEM system is very much like implementing large enterprise-wide IDS. Sensors are distributed; there are natural aggregation points for data, a central process that screens alerts and archives information. At the end of the chain there is a person who is expected to respond. The ideal engineer to implement a SEM is someone with prior experience of running large IDS projects successfully. Such a person should have a culture of efficiency, seeks to optimise, and values elegance and simplicity since this brings maintainability.

Choosing SEM Operation Staff

The best SEM operators will tend to be those individuals who currently run core network management systems and have demonstrated an inquisitive eye, along with a willingness to investigate using their own initiative. The expert operator will immediately be able to identify where procedures are inadequate or clarity is poor, and will be keen to submit their own procedural improvements to the security management function.

Verifying usage cases

The true value of a SEM system should be felt in its day-to-day use, its ability to allow the security function to "do more with less", and to be able to provide the business with previously unknown information about their exposure to IT security risk. As such, any SEM installation should be verified by use cases.

- What will you do in the event of an alert?
- How will you prioritise workload and staff
- When do SOC staff escalate and to whom?
- When does IT/Security get business managers involved?
- At what point do you shut down a server or network?
- What is the mechanism for updating stakeholders on progress?

Consider scenario-based testing, and the use of penetration testers.

- The insider gone bad
- The Internet worm
- The focused outsider with a mission

Takeaway: People and procedures are vital for a successful deployment.

Conclusions

SEMs are most commonly deployed by large organisations with a multi-vendor security environment consisting of several different firewalls, IDS sensors, and host-based logging systems. Reasons for deployment can vary from a need to meet compliance requirements with less manpower, to increase the work-rate of security teams, to outsourcing your incident response function while retaining visibility and control. In all cases, preparing adequately for such an important IT project can help you avoid failure while maximising the value eventually gained when the SEM goes live.

The secret to a successfully deployed SEM is firstly to establish solid deliverables to the business at the start of the project, and to have your chosen vendor confirm that your goals are indeed attainable with their software. Secondly, understand that in order to properly classify and prioritise alerts, you must educate this platform about your network and how you would like to respond to security threats and information. Templates may be available, but expect to invest time on this task and on the tuning of alerts either directly from IDS or from the SEM itself. Finally, understand that mature security organisations tend to contemplate SEM in the knowledge that there are no silver bullets, only better tools.

In this regard, as a tool for increasing efficiency in your security team, these systems are very welcome addition and a worthwhile investment.

About The Author

Nick Hutton began working as an information security professional in 1995. He spent his early career at Unipalm PIPEX, the UKs first business ISP. Nick has been a guest speaker at the Institute Of Directors and the London School of Economics on matters relating to IT Security and Government Monitoring/Regulation of ISPs. He represented WorldCom at industry bodies including RIPE, MWIF and the GSMA. During his time at high-tech venture capital firm Fidelity Ventures, the company invested in several security-related early stage companies including Sanctum (Acquired by Watchfire), E-Security (acquired by Novell) , and Aventail.

About Three Sixty Information Security Ltd

We are a first class independent provider of Information Security professional services and project management to the public and private sector. We enable our clients to secure their valuable data, meet compliance standards, and maintain customer confidence. Our consultants can help you reduce your exposure to global threats while capitalising on business opportunities, and protecting employees and assets. Our consultants are experts, having worked previously in senior security roles for the world's largest and most successful ISP. With an estimated 70% of the Internet's traffic passing over their network, they deployed and managed thousands of systems securely for blue-chip Times Top 100 and Fortune 500 customers. We are CISSP and BS7799 Lead Auditor certified, and well referenced via previous engagements with top 5 Investment Banks, Telcos, Security vendors and ISVs.