Security Event and Log Management Service:

Comprehensive, Cost-effective Approach to Enhance Network Security and Security Data Management
Executive Summary

The economics of network security have changed. The high cost and complexity inherent in the use of network perimeter defenses has collided with the need to document regulatory compliance and the need to lower costs for redundant network infrastructure. The result is a new recognition – that today businesses need to maintain continuity while analyzing security events and logs from a true enterprise-wide perspective in order to accurately document what happened, how it was resolved and how security policy and implementation improve over time. Security event management and log management technologies are a key part of this goal. However, it takes a managed security event and log management solution – with measurable cost and performance advantages – to fully realize the promise of an enterprise-level security event and log management system.

Security Event and Log Management (Re-)Defined

Security event management tools and services provide an enterprise-wide security monitoring and administration solution that collects data on events, analyzes the data and provides a suitable response to threats on enterprise assets. Security event management is positioned as a security management tool that can be used by enterprise-class network management centers or managed security service providers that are protecting physical and/or logical assets. Security event and log management encompasses the same functionality as security event management, but can collect data not only on security events, but can also collect generic text-based logs generated from various devices such as firewalls, routers and application servers.

Security event and log management technologies were designed to give administrators the ability to analyze and understand every security event and log that occurs within the perimeter of a large enterprise network. Unlike the log analysis tools built into individual appliances or applications, security event and log management works across multiple devices (firewalls, intrusion detection systems, intrusion prevention systems, application servers, etc.) from multiple vendors.
Security event and log management, therefore, delivers a holistic, end-to-end overview of network security performance unavailable via any other means. Given the large amount of data that must be analyzed as part of a security event and log management solution, the key to an effective security event and log management implementation is the rapid collection, collation and correlation of event and log data so that:

- Critical events are easily and automatically separated from normal traffic
- Clear, concise reports are available in near real-time to help administrators understand exactly what happened, why it happened, how it was repaired (or not), and how to prevent similar events in the future
- Security practices can be easily documented to demonstrate and prove regulatory compliance

Most security event and log management products, however, are available only as complex software offerings, and very few customers have the in-house capability to rapidly adapt a security event and log management solution to changes in IT infrastructure. The result? Security event and log management solutions that only cover part of the broader security architecture frequently lag behind changing network topologies and do not provide analysis for events and logs until long after an incident had been isolated or resolved. In addition, older security event and log management software solutions often struggle with moving large numbers of events and log files without consuming huge amounts of network bandwidth. These issues are the reasons why, despite the promise, market acceptance of security event and log management remains somewhat limited.

A service-based security event and log management offering might overcome these challenges. Customers who choose to receive security event and log management as a Web-based or managed service would gain the full advantages of an in-house solution, but without the expense and complexity of building a security event and log management infrastructure and without the staffing overhead of 24x7x365 monitoring and skill training. In addition to basic security event and log management functionality, this service-based offering also would also include the ability to automatically sort relevant information, compress that data and prioritize log transmission so that large, but not urgent, files do not negatively impact network performance.
In short, security event and log management as a service has the ability to deliver a truly comprehensive approach that is difficult, if not impossible, to achieve through in-house solutions. Organizations that have chosen not to implement security event and log management in the past due to the large amount of capital expenditure should consider using managed services to improve the efficiency and performance of security operations and to simplify the security documentation process for regulatory compliance. The challenge is finding a managed security services provider who can truly deliver a full-featured, cost-effective security event and log management solution.

The Need for Security Event and Log Management
Enterprise networks are a heterogeneous mishmash of network devices, operating systems, databases and appliances. Security infrastructure within the enterprise is no different, with software, appliances and services from multiple vendors building over time into a complex web of similar functions with widely divergent log and reporting structures. There are no standards for data storage, collection and distribution. Some devices – especially firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS) – are notorious for the massive amounts of data that they generate.

An ideal security event and log management service would streamline event and log collection to bring these various data sources into a single data store. Information from events and generic text-based logs is automatically aggregated at a central store so that the full impact of security incidents can be seen from the enterprise level, rather than from the perspective of multiple devices. This consolidated view gives organizations critical insight into how security policy works when applied to real-world situations – and how improvements in performance should be documented over time.
With one centralized data store for analysis and an efficient, forensically sound approach to collection, documentation and reporting, a security event and log management service solution can reduce unnecessary duplication of infrastructure and staff. This simple approach to understanding how security infrastructure performs leads directly to:

• "Increased reliability of security operations"
• "Faster analysis and response when the accurate distribution of critical security information is at its most critical"

In sum, the multiplicity of security devices deployed both at the network perimeter and within internal network segments makes it imperative that enterprise organizations develop true, end-to-end insight into ongoing security operations. The cost and complexity of managing these devices as separate groups of technologies is enormous. Managed security event and log management services provide a very cost-effective alternative.

**Managed Security Event and Log Management Services - The Smarter Decision**

At first, it might seem odd to outsource event or log management. After all, it is a bit counter-intuitive to collect data from one organization, move it to another for analysis, and then return it to the source for action. The economics of managed security event and log management, however, are persuasive.

In-house event or log management requires a substantial investment in data collection, correlation, analysis and reporting infrastructure. These costs are in addition to hiring or retaining the technical and professional expertise necessary to design, implement and manage a security event and log management system that operates transparently underneath normal network and security operations and that operates on a continuous basis, day and night.

A managed security event and log management solution is very cost-effective. The service provider builds the infrastructure, and customers, in effect, lease a limited portion of the overall capacity. The provider hires, trains and retains staff, so the customer has both continuity and quality of service. Patches and upgrades take place without burdening the customer's IT or security staff. Maintenance takes place 24x7x365, but the customer does not have to maintain full, around-the-clock staffing.
Security event and log management are different from most IT investments in that they cut across the full breadth of enterprise IT infrastructure. Therefore, it takes a special skillset to implement a security event and log management solution quickly, and without disrupting normal non-IT operations. Security event and log management requires a working knowledge of ALL technologies in use within an organization. Few organizations have this full range of expertise in-house, and it is expensive to hire or retain this type of staff on a 24x7 basis, which slows deployment, acceptance and performance. Managed security event and log management provides both the technology and the professional services necessary for rapid implementation and ongoing management, without the overhead of expensive in-house experts.

Scalability is another key advantage for managed security event and log management services. Managed Security Service Providers (MSSPs) support hundreds of thousands of users and devices, with the proven capabilities to aggregate hundreds of millions logs per day. As networks evolve, adding new capacity, integrating a merger or acquisition or other rapid growth activity becomes a relatively simple process – much easier than having to overhaul the infrastructure of an overstrained in-house security event and log management application. In addition, the data selection, prioritization, compression and reporting processes are already in place. Greater capacity is simply a matter of expanding the scope of the service.


IBM Security Event and Log Management Service is an ASP-based solution that automatically aggregates, correlates, prioritizes and archives security events for cost-effective, 24x7x365 event and log management activities. This service simplifies enterprise-wide analysis of events and logs, collecting and storing essential data for up to seven years.
Like all IBM ISS managed services, the Security Event and Log Management Service operates via an easy-to-use Web-based portal that gives customers rapid access to past and current security events – and equally simple but surprisingly powerful access to network-wide security forensics and analysis. This offering is highly optimized for the managed services environment, with data prioritization and compression features that handle large instances of event and log data without impacting normal network operations.

IBM Security Event and Log Management Service delivers detailed reports in real-time, for in-depth operational analysis that streamlines the process of documenting regulatory compliance. Compliance checks help demonstrate processes and procedures in place to protect critical data. Logs are stored for up to seven years, with complete access to archived data, including ad hoc and customized queries and reports.

The Security Event and Log Management Service offering is part of the IBM ISS protection on demand services platform, enabled by the IBM Virtual-Security Operations Center (Virtual-SOC). The Virtual-SOC gives organizations the ability to see and manage all of their security operations – managed and unmanaged – from IBM ISS or from other vendors, all within the Virtual-SOC Portal, a single Web-based console. In effect, the Virtual-SOC delivers the power of the IBM ISS global security operations centers to each client’s Virtual-SOC Portal, with full access to:

- IBM ISS renowned X-Force® security intelligence
- 24x7x365 monitoring and management
- Comprehensive IBM ISS consulting services
- Trouble ticketing, tracking, alerting, escalation and response
- Reporting, archiving and retrieval
- Live collaboration with IBM ISS certified security experts
This high level of security operations, services integration and client/provider transparency is exceptionally cost-efficient. In fact, IBM ISS managed services customers can realize savings of up to 55 percent on information security management costs. The Virtual-SOC environment also saves time and money by converting multiple security management consoles into a single, unified management environment that streamlines communications between IT, security and IBM ISS staff.

A Better Security Event and Log Management Solution

IBM ISS Security Event and Log Management Service represents a substantial improvement over other vendors’ security event and log management software applications and managed services. The difference begins with IBM ISS itself. With more than 12 years of experience as a global leader and innovator in Internet security and 11 years providing Managed Security Services, IBM ISS has a breadth and depth of scale and experience that few organizations can match. In fact, IBM ISS operates six security operations centers available 24x7, across five continents. This international experience is ideal for any organization seeking a multinational services solution – or any smaller organization needing local knowledge and native language support.

The Security Event and Log Management Service offering supports a wide range of network and security products, from an equally wide range of vendors.
There is no need to uproot existing and productive infrastructure simply to
receive the benefits of the Security Event and Log Management Service. The
Security Event and Log Management service supports software and appliance
products from the following vendors, plus other third-party devices:

- IBM ISS
- Juniper Networks (NetScreen)
- Check Point
- 3Com (Tipping Point)
- Cisco Systems
- McAfee
- And more

IBM ISS industry-leading service level agreements (SLAs) guarantee reliable
service and rapid resolution of client concerns. Data storage uses forensically
sound archival practices, and automatic redundancy of datasets ensures that
events and logs are always protected and recoverable, even after catastrophic
failure. In addition, the log management service will accept data from any
operating system or application that records data in a generic text-based format.

IBM ISS also recognizes that security management is not an either/or, in-house
or outsourced decision. Many organizations prefer to maintain direct control
over significant portions of their security infrastructure. In response, the
Security Event and Log Management Service offering works equally well
for devices managed by IBM ISS, other managed security services, devices
operated in-house, and mixed environments in which in-house staff and IBM
ISS Managed Security Services personnel share responsibility for overall
network security. Protection on demand makes this flexibility possible, letting
customers choose the security technologies they need when, where and how
they need them.
Consider the following two tables that summarize the features and reporting capabilities in the Security Event and Log Management Service. Then compare these capabilities with any other security event and log management offering – whether software, appliance or managed service. This comparison demonstrates that the IBM ISS offering delivers more capabilities, greater cost-efficiencies and easier ongoing management than other security event and log management solutions on the market.

<table>
<thead>
<tr>
<th>Services Features</th>
<th>Security Event and Log Management Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Platforms:</td>
<td>Leading Products From IBM Internet Security Systems, Checkpoint, Cisco, Juniper (Netscreen), McAfee, 3Com (TippingPoint) and Others</td>
</tr>
<tr>
<td>Max. Events Per Second:</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Duration Events Available Online:</td>
<td>One Year</td>
</tr>
<tr>
<td>Duration Events Archived Offline:</td>
<td>Up to Seven Years</td>
</tr>
<tr>
<td>Event Export:</td>
<td>Raw and CSV Format</td>
</tr>
<tr>
<td>Forensically Sound Storage:</td>
<td>Yes*</td>
</tr>
<tr>
<td>Automated Analysis of Event Data:</td>
<td>Yes*</td>
</tr>
<tr>
<td>Real-Time Notifications of Anomalies:</td>
<td>Yes</td>
</tr>
<tr>
<td>Incident Tracking:</td>
<td>Yes</td>
</tr>
<tr>
<td>Simple and Advanced Querying:</td>
<td>Yes</td>
</tr>
<tr>
<td>Detailed Reporting:</td>
<td>Yes, 20+ Templates</td>
</tr>
<tr>
<td>Data Delivery:</td>
<td>Optional Add-On, Via Encrypted DVD</td>
</tr>
<tr>
<td>Integrated Security Intelligence:</td>
<td>Yes</td>
</tr>
<tr>
<td>Trouble Ticket Integration:</td>
<td>Optional Add-On</td>
</tr>
<tr>
<td>Multiple Report Audiences:</td>
<td>Yes*</td>
</tr>
<tr>
<td>Integration With Other MSS:</td>
<td>Yes</td>
</tr>
<tr>
<td>Assists With Regulatory Compliance:</td>
<td>Yes</td>
</tr>
<tr>
<td>Service Level Agreements:</td>
<td>Yes</td>
</tr>
<tr>
<td>SOC Event Monitoring</td>
<td>Yes*</td>
</tr>
</tbody>
</table>

* Automated Event Analysis and Alerting applies to Select IDS/IPS platforms only.
# Competitive Matrix

<table>
<thead>
<tr>
<th>Feature</th>
<th>SELM Products</th>
<th>Other SELM Services</th>
<th>IBM Internet Security Systems SELM Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>SELM technology license costs</td>
<td>$250,000 +</td>
<td>$250,000 +</td>
<td>$0</td>
</tr>
<tr>
<td>SELM license maintenance costs</td>
<td>$50,000 +</td>
<td>$50,000 +</td>
<td>$0</td>
</tr>
<tr>
<td>Technology configuration, deployment costs</td>
<td>$15,000 +</td>
<td>$15,000 +</td>
<td>$0</td>
</tr>
<tr>
<td>Cost of ownership</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Time to deploy</td>
<td>Months</td>
<td>Months</td>
<td>Days</td>
</tr>
<tr>
<td>24x7 monitoring, management</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Regulatory Policies</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrated trouble ticketing, tracking, alerting, escalation and response</td>
<td>Limited</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Security event and log analysis and reporting</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security event and log archival</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Off-site Disaster Recovery</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
IBM SOC Event Monitoring Service

For organizations that do manage the bulk of their own security and event log coordination and management, but from time to time need or want off-hours or scheduled assistance, IBM ISS SOC event monitoring is an additional feature that can be added as part of our Security Event and Log Management Service.

SOC event monitoring acts as a natural extension of an organization’s own SOC, providing automated, real-time analysis of security events using algorithms created and maintained by IBM ISS. Subsequent eyes-on scrutiny of associated alerts helps the IBM SOC notify the customer of potential security risks.

Should a problem arise, the IBM SOC monitoring staff will take immediate action, opening trouble tickets and alerting a customer contact, all while working to ensure that data are not lost or stolen and systems are not compromised.

With SOC monitoring by IBM ISS, customers can:

• **Optimize staffing requirements by outsourcing off-peak or hard-to-fill holiday hours**
• **Improve the overall security posture by leveraging IBM ISS expertise in network security**
• **Benefit from service solutions that address specific security regulations, including:**
  GLBA, HIPPA, ISO 17799:2005, PCI and Sox/COBIT

With the SOC event monitoring, organizations of all sizes can leverage IBM expertise for the flexibility they need to keep their networks and systems operating at peak performance, even when staffing limitations threaten to hamper in-house operations.
Conclusion

Given the changing climate for network security - and with ongoing demands for improved documentation of regulatory compliance – the time has come for a comprehensive, cost-effective, scalable security event and log management solution. The answer is IBM Security Event and Log Management Service. This powerful offering delivers the following advantages that no other software, appliance or services offering can match:

• The power, knowledge and experience of IBM ISS
• Protection on demand services platform that allows organizations to more closely align security with core business processes
• Virtual-SOC technology that unifies security management for all managed services within a single, easy-to-use Web portal
• Comprehensive, enterprise-wide overviews of network security performance that reveal patterns of risk and attack that individual devices cannot identify
• Fast, flexible security event and log management capabilities that support a wide range of security products and vendors
• Detailed, ad hoc and automated reporting to help streamline the process of documenting regulatory compliance
• SOC monitoring on an as-needed basis providing event and alert analysis and correlation

As a Managed Security Service offering, the Security Event and Log Management Service from IBM ISS offers exceptional performance at very low cost, without compromising on breadth of features or usability. It is finally possible to access an enterprise-wide overview of current and past security performance with the Security Event and Log Management Service from the leaders in enterprise security, IBM ISS.
Protection on Demand

Protection on demand is a services-based approach that delivers protection to organizations of all sizes allowing them to proactively respond to Internet threats while integrating security with key business processes. This innovative managed security services approach blends market leading services, technologies, and security intelligence into a single solution that is delivered when, where and how you need it. The result is a cost-effective solution that enables you to optimize resources, enhance profitability, improve flexibility and responsiveness, and address regulatory requirements. The Security and Log Management Service is just one of a broad range of services available through the IBM ISS protection on demand services platform.

Contact IBM Internet Security Systems to Learn More

For more information about the Security Event and Log Management Service from IBM ISS, visit ibm.com/services/us/iss or call 1 800 776-2362.

About IBM Internet Security Systems

IBM Internet Security Systems (ISS) is the trusted expert to global enterprises and world governments, providing products and services that protect against Internet threats. An established world leader in security since 1994, IBM ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise. IBM ISS products and services are based on the proactive security intelligence conducted by the IBM Internet Security Systems X-Force® research and development team – a world authority in vulnerability and threat research. For more information, visit ibm.com/services/us/iss or call 1 800 776-2362.