Security information and event management solutions
Buyer's guide: purchasing criteria

Tivoli® software

Select the right security information and event management solution to automate security and compliance operations.

June 2008

Each day, organizations' IT systems can generate thousands of security events and alerts from a very broad range of sources. Most of these are nonthreatening, routine events. A small — but critical — percentage signal potential security breaches from internal and external sources.

Separating the risky from the routine is daunting enough. But organizations should also ensure that the security information and events that are constantly being generated are properly monitored, recorded and reported for regulatory compliance. Failure can bring swift, heavy consequences, including lost revenue and damaged reputations and IT assets.

One way organizations successfully address these challenges is through security information and event management (SIEM) solutions. Through the ability to centralize security-relevant events and analyze the consolidated data, the right SIEM solution can help you:

- **Increase visibility to quickly identify and react to threats according to their potential impact.**
- **Manage security and compliance operations effectively and efficiently.**
- **Automate repetitive, time- and expertise-intensive activities.**
- **Provide high-level oversight for external and insider threats, incident management and IT security controls.**

Realizing the full vision of SIEM starts with a solution that enables you to collect, record and store an extraordinary volume and diversity of data. But it delivers value beyond log management, translating raw event data into meaningful information that can be acted on and communicated clearly to auditors and customers. It enables you to detect security threats faster and with less effort — and even prioritize them based on their business relevance. And when audit time rolls around, it enables you to know and prove exactly who did what, when, where, where from, where to and on what.

Getting started with SIEM

This buyer's guide outlines capabilities that comprise an effective SIEM solution, including:

1. **Centralized log management.**
2. **Security event management**
3. **Security information management.**
4. **Reporting.**
5. **Event source support.**

The guide discusses the benefits of each capability and provides checklists to help you evaluate whether or not a particular vendor's solutions can address each of these areas. You'll also find checklists to help you evaluate improving productivity and time to value, as well as tips to help you select a provider that can support the full breadth of your security requirements.

1. Centralized log management

One of the most critical components of SIEM is the ability to reliably and verifiably collect original log data. The typical large enterprise generates gigabytes of log data every day from critical applications, databases and platforms, all of which must be captured and retained for extended time periods. Few organizations possess the necessary time and manpower to manually collect this information — nor would it be strategic to do so when these resources could and should be allocated to higher-value activities.

Centralized, automated log management can significantly reduce the time and effort needed to efficiently collect, organize, archive, investigate and retrieve logs for forensic and historical analysis. A superior SIEM solution allows you to reliably collect log data from dispersed sources across the enterprise in a continuous, sustainable manner. Just as important, it provides fast, easy-to-use search capabilities that allow you to retrieve the data without having to resort to cumbersome, homegrown tools or highly technical query languages. So whether you need evidentiary proof or information for historical analysis, the right SIEM solution can ensure you'll have the answers you need quickly.

To find a superior solution, look for one that:	IBM	Other Vendor
Provides a reliable and verifiable log management process.	✓	
Includes a log management dashboard to view the overall status of the log management process.	✓	
Provides administrators with a log collect history report that enables them to view the collect process, determine if it is running well and perform a level of diagnosis using the report.	✓	
Enables auditors and security officers to effectively monitor and audit the actual collection of log data to ensure that no data is lost.	✓	
Provides auditors with a log continuity report (in both graphic and table format) to enable them to see which devices and applications are being monitored, determine if a continuous set of collected logs exist for those devices and indicate where issues need to be followed up.	✓	
Includes a log investigation tool with a Google-like search facility to search the collected raw log data for specific events or data.	✓	
Includes a log retrieval tool that enables the user to retrieve specific log files from the log archive.	✓	
Provides proactive alerting on collect failures so that any potential loss of audit data can be minimized or mitigated.	✓	
Organizes the logs collected using an indexing schema for easier identification and storage.	✓	
Collects and stores raw, original log data from a wide list of supported devices, operating systems, applications, databases and more. (Refer to **Section 5, Event source support** for specific device requirements.)	✓	
Includes generic support for log files, even if the device, application or database isn't specifically supported.	✓	
Can compress all of the raw log data and store it using your existing archiving solution.	✓	
Encrypts log data during transmission.	✓	
Easily integrates with your existing archiving solution.	✓	
Eliminates the need for a database administrator to support a special relational database created for reporting from log data.	✓	
Automates processes to help reduce the cost of ownership and staffing needs.	✓	
Facilitates deployment with out-of-the-box support for a wide range of devices and uses agentless collection methods.	✓	

2. Security event management

From widespread denial-of-service attacks to phishing scams and malware, there's no shortage of potential security threats facing organizations today. These attacks can be quick, and can demand real-time reaction and defense, which can require an enormous investment of time and money. Security teams must constantly monitor and analyze reams of security event data from a number of disparate systems throughout the enterprise to detect potential cyber threats, general misuse or network policy violations.

An efficient way to manage security threats is by implementing a platform that automatically aggregates information collected from across the infrastructure as threats happen, including host logs, security events, asset data and vulnerability data. Ideally, the information should be prioritized through multiple analysis and correlation techniques that target key threats and policy violations. In addition, security managers should have a single event-oriented console that makes it easy to view correlated security events at a glance, as well as drill down and investigate business-relevant events, threats and misuse until they are remediated.

And once you've detected a potential threat, you'll want to make sure that you have the ability to evaluate its potential impact within a business context. Generally, the more granular the filtering capabilities, the better able you are to prioritize security events in alignment with your business goals and policies. That way, you have the visibility to see not only what's important from a security threat or policy violation, but what's important to your business.

To find a superior solution, look for one that:	IBM	Other Vendor
Provides incident investigation with the ability to visualize and easily drill down to determine what really happened.	✓	
Imports all necessary data from other integrated tools to help quickly troubleshoot security incidents.	✓	
Provides a security knowledge base framework to link and import reference industry and company best practices and experiences in identifying and resolving a security problem.	✓	
Helps you quickly and easily determine if an interesting event or set of events represents a true threat to the environment.	✓	
Provides intuitive tools to manipulate incoming data to pinpoint troubled resources in real time with various ways to view and interpret data at a glance: geographically, graphically or tabular.	✓	
Includes a statistical correlation engine to detect new, unknown threats and anomalies with immediate out-of-the-box value that can be improved through tuning.	✓	
Provides a correlation engine that reflects organization policies and business-relevant priorities and delivers the flexibility to use any information in the incoming events, security groups, asset data or vulnerability information to build policy-specific rules.	✓	
Includes a robust, flexible rules engine for correlation of any combination of events or asset groups, along with the ability to monitor customer-specific threats, policies and IT controls.	✓	
Offers predefined event class system (taxonomy) that maps thousands of unique events into useful categories for correlation, monitoring and reporting.	✓	
Includes flexible event filtering system to optimize system performance by only looking at events of interest and providing automatic and customizable categorization.	✓	
Provides predefined watchlists (asset groups) for both threat and policy monitoring functions, and allows assets to belong to multiple groups.	✓	
Offers security domain capabilities to flexibly restrict access to specific events and confidential information to different security event management users.	✓	
Provides a software platform for security operation center (SOC) and service providers that features an investigation tool framework, security domains to separate individual customer/department data and support for multiple, overlapping IP addresses.	✓	

To find a superior solution, look for one that:	IBM	Other Vendor
Displays the top threatened or threatening hosts in addition to a list of events that have occurred in the environment.	✓	
Includes flexible event displays that can show event list views, tabular event views with real-time drag-and-drop investigation and analysis capabilities, graphical views and geographic mapping views that can be customized with filtering and customer preferences as default views.	✓	
Offers simple deployment through agentless architecture with centralized, automatic event source configuration.	✓	
Provides business-relevant incident recognition with asset grouping and threat weighting.	✓	
Offers operational integration with IBM Tivoli® solutions such as IBM Netcool® offerings to provide end-to-end business service dashboard functionality spanning IT operations.	✓	
Allows the operator to easily determine (within two clicks or less) if a host is compromised or infected with a worm.	✓	
Provides an integrated incident ticketing/case management system to manage security incidents and cases, including hyperlinks to original events of interest.	✓	
Maintains the security of the monitoring tool with administration privileges segregated by roles and groups, and with the addition of self-auditing and tracking of all security activities.	✓	
Provides default and customizable event classes to automatically categorize incoming events according to industry standards or company policies.	✓	
Keeps track of the security incident and case management process through a security ticketing system, which has access to all necessary information to resolve a problem before involving the IT help desk.	✓	
Automatically alerts, notifies or takes action on predefined security triggers to quickly react to important events.	✓	
Allows forwarding of certain events into a wider NOC monitoring environment for higher-level visibility of important security events, to facilitate integration of the whole IT organization.	✓	
Supports a wide variety of hosts, clients, network security devices, network nodes and servers that generate real-time security event logs.	✓	

3. Security information management

While external security threats typically receive the majority of attention, internal security incidents can pose an equal — if not greater — threat. Privileged users are the main source of insider threat. These users often have unrestricted access to critical intellectual property and proprietary confidential information that resides on mainframe systems, applications and databases — access that is largely unmonitored. Insider threats can cause a great deal of harm to your enterprise and irreparable loss of information, whether intentional or accidental.

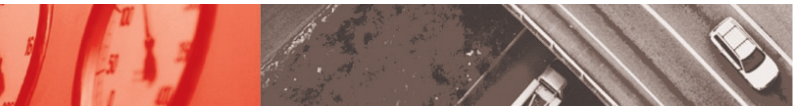
What's needed is continual oversight with maximum visibility of user activity and ready access to information that enables you to monitor who does what, when, where, where from, where to and on what systems. An effective SIEM solution not only collects and preserves raw log data for evidentiary purposes but also translates and normalizes it into meaningful information that enables you to monitor user access and policy compliance. Then it can display the information through an enterprise audit dashboard and dynamic reports that allow you to view logged activity in comparison with user profiles, or drill down to detailed, easily understood reports. And through the comprehensive dashboard, organizations can instantly view their compliance status, allowing them to pinpoint areas of concern and potential violations that require immediate investigation and remediation. So if someone is doing something out of the bounds of policy, you'll quickly know — and in a form you can understand.

Furthermore, you'll have a quick way to demonstrate to auditors that your organization:

- **Logs and reviews systems administrator and systems operator activities on a regular basis.**
- **Analyzes and investigates security incidents and suspicious activity, plus takes remedial actions.**
- **Logs access to sensitive data, including root/administrator and database administrator (DBA) access.**
- **Continually maintains and reviews application, database, operating system and device logs.**

To find a superior solution, look for one that:	IBM	Other Vendor
Includes events from all your major IT infrastructure components in one report, allowing a complete and overall picture to be formed.	✓	
Identifies anyone exercising technical authority without authorization.	✓	
Identifies system changes made outside of the approval process or change control process.	✓	
Identifies accidental destruction of high-value data.	✓	
Identifies malicious or deliberate acts of sabotage.	✓	
Includes a strong normalization process so all events look the same and are transformed to the same format so they can be easily understood by nonsubject-matter experts.	✓	
Allows you to construct a best practice or an acceptable-use policy in an included policy editor so that all activity will be evaluated against this policy, thereby highlighting the out-of-policy activity that needs immediate investigation.	✓	

To find a superior solution, look for one that:	IBM	Other Vendor
Supports compliance- and regulation-specific module definitions that include: – A set of classifications for each of the W dimensions (who, did what, when, where, where from, where to and on what) so that policy rules can be written at a higher level than individual events (for example, referring to the group of users who administer the domains as "Domain Admins" rather than having to list every administrator individually). – A set of audit policy rules that describe acceptable behavior. – Attention rules that define activity that you want to be notified of, even if it's not a policy exception.	✓	
Provides compliance reporting modules specific to your compliance needs, covering major regulations and best practices including International Organization for Standardization (ISO 27001), Sarbanes-Oxley (SOX), PCI, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Basel II and others.	✓	
Includes privileged user monitoring and auditing to monitor, report and investigate the behavior and actions of privileged users on databases, applications, servers and mainframes to ensure that acceptable-use policies are followed and that effective controls are in place.	✓	
Supports exception severity calculations based on the priority of the assets involved in an exception, allowing more critical systems to create higher severity events in reports.	✓	
Supports the three components of what one host did to another host: 1) Host One 2) The Action 3) Host Two	✓	
Provides detailed "Host One" information, including the host, the user login name and the user's given name.	✓	
Provides "Host One" user name correlation to take login names from multiple systems and correlate them back to a user name.	✓	
Provides a broad list of "Actions" that identify the specific action taken by a host or user, including read, write, changed, opened and closed.	✓	
Provides in-depth "Host Two" information, including what object (file, directory, database, application or record) was accessed on the other host.	✓	



4. Reporting

The ability to quickly produce easily understood, detailed reports is a vital concern for many organizations. The right SIEM solution provides superior reporting features that make it easy to analyze thousands of security events to detect potential threats and policy violations, as well as address the compliance burden. These features should include standard and customizable report templates, and an advanced report definition wizard that enables you to create customized reports from scratch. In addition, the wizard should allow you to create best practices, industry-standard audits and compliance-oriented reports to help you get started quickly. These reports should help you manage operational security issues as well as provide support for internal and external auditors.

You'll also want to keep in mind the importance of automated report distribution capabilities that provide fast integration into verification processes or other business workflows, as well as the ability to export reports to other formats or send them back to business owners for further verification.

To find a superior solution, look for one that:	IBM	Other Vendor
Enables you to easily sort and browse 20,000 events, and analyze them from different angles.	✓	
Provides reports in plain language that can be understood by auditors or other nontechnical personnel.	✓	
Includes the user's real name as known by the directory or security system to make the report more readable.	✓	
Has compliance modules for major regulations including SOX, GLBA, HIPAA, Basel II, ISO 17799, ISO 27001, PCI DSS, FISMA and others.	✓	
Includes more than 50 parameterized best-practice audit reports (equivalent to many hundreds or even thousands of individual reports) out of the box.	✓	
Uses a patent-pending strong normalization model.	✓	
Includes a flexible custom report writer that is optimized to the normalization model, allowing you to create your own compliance and audit reports without needing to understand or write SQL.	✓	

To find a superior solution, look for one that:	IBM	Other Vendor
Includes a report distribution system to distribute compliance and audit reports to business owners and stakeholders for review, approval or comment.	✓	
Provides compliance-specific classification templates.	✓	
Provides a compliance-specific policy template that represents the controls within a regulation.	✓	
Provides compliance-specific reports that allow you to monitor compliance posture against specific controls.	✓	
Provides compliance reports that are designed, created and based on standards (versus renaming operational reports).	✓	
Provides a compliance dashboard that shows the current compliance posture in the vocabulary of the regulations or policies in place for easy understanding.	✓	
Provides trending information at the dashboard level to help indicate the trend for compliance posture and ensure goals are being achieved.	✓	
Provides drill-down from the high-level compliance dashboard through to the underlying detail events for further investigation.	✓	
Provides reporting at the raw log level using a simple query mechanism for forensic-type investigations.	✓	
Includes a full-featured reporting engine with scheduled reporting.	✓	
Automates the distribution of reports to business owners for their inspection and approval as part of the overall compliance and business process.	✓	
Includes a custom report designer that requires no special skills (such as knowledge of SQL) to create reports quickly.	✓	
Facilitates communication of threat levels and security activities through out-of-the-box standard and customizable report templates, driven from an automated report scheduler.	✓	
Provides a wide variety of report output formats, including HTML, PDF and XML exporting of all graphs and charts.	✓	
Includes default templates for regulation-specific compliance reports.	✓	
Provides SOC dashboard capabilities that allow security analysts and SOC administrators to quickly manipulate a large number of incoming real-time events to extract consolidated statistics on specific event types or resources.	✓	

5. Event source support

Monitoring thousands of network and security devices, hosts, applications and other sources of events throughout your enterprise can represent a potentially enormous task for your IT staff and can take a substantial amount of manual effort. That's why it's critical to have a single view of security events from diverse devices across the enterprise infrastructure, so you can know exactly who is doing what and when. It's also important that the SIEM solution you choose should be able to support multiple devices — both out of the box and through a toolkit or guide that allows you to add support for unique devices.

To find a superior solution, look for one that:	IBM	Other Vendor
Supports more than 250 unique event sources out of the box, each at different version levels and running on different platforms.	✓	
Supports each device through its specific log or set of logs (ASCII or databases), through the appropriate protocol, like Syslog, SNMP, XML, SDEE, OPSEC or other proprietary interface.	✓	
Includes a toolkit to enable you to easily add support for additional, unique devices.	✓	
Has the capability to automatically recognize an existing data stream and configure the collection according to the device type.	✓	
Provides support for end points primarily through agent-less support, and only uses agent support on special cases, thus minimizing the deployment and event source support burden.	✓	
Provides vendor services to add support for unique customer devices.	✓	
Provides support for an expanding list of specific event sources and devices, including the following:	✓	

Event Sources and Monitored Devices

Authentication and Access Control

- BMC Identity Manager (on Oracle)
- CA eTrust Access
- CA eTrust Secure Proxy Server
- CA eTrust SiteMinder
- Cisco Secure ACS
- IBM Tivoli Access Manager
- IBM Tivoli Access Manager for OS
- IBM Tivoli Directory Server
- IBM Tivoli Federated Identity Manager
- IBM Tivoli Identity Manager
- Infoblox LDAP One
- Juniper Funk Steel-Belted Radius
- Keon Certificate Server and Certificate Authority
- Microsoft® Windows® Active Directory®
- OpenLDAP
- Oracle Identity Management
- RSA ACE/Server
- RSA SecurID RADIUS
- Sun Java™ System Directory Server Enterprise Edition (LDAP)
- Sun Netscape Directory Server
- Sun Solaris LDAP

Antivirus for Desktops

- Kaspersky Anti-Virus
- McAfee VirusScan
- Symantec Norton AntiVirus
- Trend Micro InterScan VirusWall

Antivirus Gateway

- McAfee VirusScan Gateway
- Secure Computing IronMail
- Symantec Norton AntiVirus Gateway
- Trend Micro InterScan VirusWall Gateway

Antivirus Servers

- McAfee ePolicy Orchestrator (ePO)
- Symantec AntiVirus Corporate Edition for Windows
- Trend Micro ScanMail for IBM Domino® on Windows
- Trend Micro ScanMail for MS Exchange
- Trend Micro ServerProtect 5 for NT

Event Sources and Monitored Devices

Applications

- Adobe JRun Application Server
- Apache Web Server
- IBM WebSphere®
- Java System Portal Server
- Microsoft Internet Information Server (IIS)
- Microsoft Windows DHCP
- Misys Opics
- Oracle BEA Clarify TUXEDO
- Oracle BEA TUXEDO
- Oracle BEA WebLogic
- Oracle E-Business Suite
- Oracle PeopleSoft
- SAP NetWeaver Application Server
- SAP R/3
- Sun iPlanet Web Server

Application Security

- Nortel Intelligent Traffic Management (ITM)
- Sentryware Hive

Mail Server/Groupware

- IBM Lotus® Domino (Notes)
- Microsoft Exchange Server

Database

- IBM DB2®
- IBM DB2 Universal Database™
- Microsoft SQL Server®
- Oracle DBMS database server
- Oracle DBMS FGA database server
- Sybase ASE

Content Filtering

- Barracuda Web Filter
- Blue Coat Proxy
- Kaspersky Anti-Spam
- Network Appliance NetCache w/Webwasher
- Secure Computing IronMail
- St. Bernard Software IPrism Firewall
- Trend Micro ScanMail
- Vericept Monitor
- WebSense Enterprise

Event Sources and Monitored Devices

Application Firewalls

- Deny All rWeb
- Juniper DX
- SecureLogix VoIP Firewall
- Teros APS

Desktop Firewall/IDS/IPS

- Cisco Security Agent (CSA)
- IBM Proventia® Desktop
- McAfee Personal Firewall
- Sana Primary Response
- Symantec (Sygate) Secure Enterprise

Network Firewalls, Multifunction Appliances

- Check Point FireWall-1
- Cisco Firewall Services Module for Cisco Catalyst (FWSM)
- Cisco PIX
- CyberGuard Firewall
- Fortinet FortiGate
- GNAT Box Firewall
- IPTables
- Juniper Netscreen Firewall
- Lucent Brick Managed Firewall
- Microsoft ISA Server
- Nortel Switched Firewall (Alteon ASF, standalone and accelerated)
- Novell BorderManager
- Secure Computing Sidewinder
- Secure Computing Webwasher
- SonicWALL Pro
- Stonesoft StoneGate
- Sun SunScreen
- Symantec 5400
- Symantec (Raptor) Enterprise Firewall

Discovery Tools

- Lumeta IPsonar
- Nmap
- Sourcefire RNA

Event Sources and Monitored Devices

Host IDS/IPS

- Cisco Security Agent (CSA)
- Enterasys Dragon IDS-Squire
- IBM Netcool/SSM
- IBM Proventia Server
- IBM RealSecure® OS Sensor
- IBM RealSecure Server Sensor
- InterSect Alliance SNARE for Windows
- McAfee Entercept
- NFR HIDS
- PowerTech (OS/400) PowerLock Interact
- Sana Primary Response
- Symantec Intruder Alert (ITA)
- Tripwire
- Type80 SMA_RT

Event Sources and Monitored Devices

Network IDS/IPS, Network Anomaly

- Acme Packet SD
- AirDefense
- AirMagnet
- Arbor Networks Peakflow X
- Cisco ASA
- Cisco IOS IDS
- Cisco IOS IPS
- Cisco IPS
- Cisco ISR
- Cisco Secure IDS
- Enterasys Dragon
- Enterasys Dragon Sensor
- Enterasys Expedition
- ForeScout ActiveScout
- IBM Proventia ADS
- IBM Proventia G
- IBM Proventia M
- IBM RealSecure Network Sensor
- Intrusion SecureNetPro
- ipANGEL
- Juniper NetScreen IDP
- LaBrea TarPit
- Lancope StealthWatch
- Lucid Security ipANGEL
- Mazu Profiler
- McAfee Intrushield
- Mirage CounterPoint
- NarusInsight
- NFR IDS
- Nortel Threat Protection System (TPS)
- Q1 Labs QRadar
- Securify SecureVantage Monitor
- Snort
- Snort IDS
- Sourcefire Network Sensor
- Sourcefire Snort
- Symantec Network Security
- TippingPoint UnityOne IPS
- TippingPoint UnityOne NDS
- TopLayer 5500-1000
- TopLayer Attack Mitigator

Event Sources and Monitored Devices

Log Aggregator

- Kiwi Syslog
- LogLogic Syslog
- MonitorWare Syslog
- Syslog-NG

Management Console

- Check Point Provider-1
- Check Point SmartCenter
- CiscoWorks
- Enterasys Dragon Enterprise Management Server
- HP OpenView (HPOV)
- IBM Proventia Management SiteProtector™
- IBM Proventia SiteProtector with MS SQL Server back-end DB
- IBM RealSecure Workgroup Manager
- IBM SiteProtector Security Fusion Module
- IBM Tivoli Enterprise Console®
- IBM Tivoli Netcool/OMNIbus™
- Juniper NetScreen IDP Management Console
- Juniper NetScreen NSM
- NetIQ AppManager
- NetIQ Security Manager
- Nortel Defense Center
- SolarWinds
- Sourcefire Defense Center
- Symantec System Center

OS Desktop

- Mac OS X
- Microsoft Windows

OS Server

- Hewlett-Packard (Tandem) NonStop OS
- HP HP-UX
- HP NonStop Safeguard
- HP OpenVMS
- HP Tru64
- IBM AIX®

Event Sources and Monitored Devices

OS Server

- IBM OS/400® - i5/OS®
- IBM Tivoli Netcool Linux® SSM
- IBM Tivoli Netcool Solaris SSM
- IBM Tivoli Netcool Windows SSM
- Nokia IPSO
- Novell Audit
- Novell NetWare
- Novell Nsure Audit
- Novell SuSE Linux
- Red Hat Linux
- Sun Solaris (32-bit & 64-bit)

OS Service

- CRON
- FTPD
- HTTPD
- IPMon
- Logger
- Login
- Microsoft ACS
- SENDMAIL
- SSHD
- X11

OS Syslogs

- Linux 2.2
- Microsoft SNMP Trap Sender
- Microsoft Windows
- OpenBSD
- Stratus VOS
- VMware ESX

Mainframe Security

- Bsafe Security Module VSE Mainframe
- CA eTrust Access Control
- CA eTrust ACF2® (IBM z/OS®)
- CA eTrust Top Secret® (IBM VSE/ESA™)
- CA eTrust Top Secret (IBM z/OS)
- IBM Tivoli zSecure
- IBM Tivoli zSecure Alert
- IBM Tivoli zSecure Audit
- IBM z/OS HIDS
- IBM z/OS RACF®
- Type80 (z/OS) SM_ART

Event Sources and Monitored Devices

Routers/Switches

- Alcatel Switch
- Cisco Catalyst Switches
- Cisco IOS Switches
- Cisco RCMD
- Cisco Routers
- Cisco TACACS / TACACS+
- Citrix NetScaler Load Balancer
- Enterasys Expedition Router
- Extreme BlackDiamond Router
- F5 Big-IP 3DNS
- Foundry Switch
- Hewlett-Packard ProCurve Switch
- Juniper IVE
- Juniper JUNOS Router
- Netopia 3000
- Nortel Ethernet Routing Switch (BayStack)
- Nortel Ethernet Routing Switch (Passport)

Network Infrastructure

- Citrix NetScaler Load Balancer
- Ingrian NAE
- ISC BIND
- ISC DHCP
- Tripp Lite UPS

VPN

- Check Point VPN-1
- Cisco IOS VPN
- Cisco VPN 3000
- Cisco VPN Concentrator 3000
- Juniper SSL VPN
- Juniper VPN
- Nortel VPN Gateway
- Nortel VPN Router

Event Sources and Monitored Devices

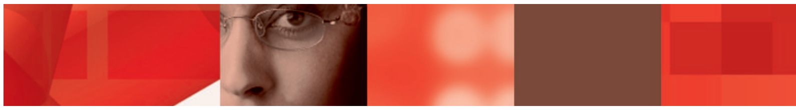
Vulnerability Assessment

- eEye Retina
- eEye REM
- IBM ISS Internet Scanner
- IBM Proventia Enterprise Scanner
- Lumension Security PatchLink Stat
- nCircle IP360
- Nessus
- Tenable Lightning Console for Nessus

Improving productivity and accelerating time to value

As you're evaluating different SIEM solutions, it's important to select one that offers rapid time to value. A cost-effective solution includes a number of key features designed to help improve productivity, integration and flexibility.

To find a superior solution, look for one that:	IBM	Other Vendor
Can be deployed using a phased approach.	✓	
Offers automatic configuration capabilities for real-time event sources.	✓	
Provides immediate coverage for policy exceptions through robust policy-based correlation and default or customizable event classification.	✓	
Demonstrates immediate value with extensive out-of-the-box reports.	✓	
Includes a unique statistical correlation engine that can automatically identify threats with minimal (less than four hours) setup and tuning effort.	✓	
Effectively and efficiently detects zero-day attacks (new threats that have not been seen before).	✓	
Provides scalability of over 10,000 correlated events per second (per single rules engine, inclusive of statistical and rules correlation).	✓	
Automates manual processes, from log collection and analysis through incident management and compliance reporting.	✓	
Is mature, robust and proven in the marketplace as evidenced with numerous worldwide customer installations.	✓	
Is backed by its own experienced worldwide services teams, as well as a strong business partner community available to ensure that your project does not suffer through vendor staff that are learning while implementing your solution.	✓	
Has education and training courses available to enable your staff to become productive more quickly.	✓	
Supports a flexible deployment model with an agentless-centric architecture for noninvasive deployment, or agents where required.	✓	
Provides clear and straightforward vendor pricing and licensing.	✓	



Selecting the right security provider

The provider you choose should be able to support the full breadth of your security requirements. Ideally, you'll also want a provider that can support you throughout the process of implementing your solution. Before you select a provider, make sure to ask these questions:

Does your vendor's security vision align with yours?

Find a vendor that takes security as seriously as you do and understands how the absence of a solid security infrastructure can impact your organization.

Is your vendor focused on true enterprise security needs?

With a vendor who is focused too narrowly on a point solution that addresses only a particular environment, you can run into the "islands of security" problem. Choose a vendor who can address the big picture, including:

- Identity and access management.
- Threat protection.
- Managed services.
- Mainframe security.
- Application security.
- Information and data security.
- Service management.

Is your vendor's SIEM solution integrated with identity and access management as well as network and IT management solutions?

Look for a vendor who can extend the value of your SIEM solution with strong integration to these other key areas.

Does your vendor support your business goals through their technology?

Look for vendors whose solutions align with your business objectives. Do their solutions promote efficiencies, reduce business service deployment time, reduce costs and speed time to market?

What type of global presence does your vendor have?

If your organization has international offices, you should look for a vendor with a global presence and proven international business experience.
Make sure the vendor can support your offices abroad with their own local resources.

Is the solution supported by a mature support organization with the expertise and bandwidth that can be relied on when you need them?

Find a vendor that has a proven support organization to help you maximize the value of your software investment.

Are the vendor's solutions consistently rated highly by the analyst community?

Look for solutions that are recognized through independent analysis and examination across multiple dimensions by leading analysts.

How sure are you of your vendor's stability and staying power in today's tough economy?

A big issue in today's economy is vendor stability and viability. You should consider a vendor who has a long history in the industry, a solid, forward-looking strategy and the resources to overcome adverse economic times.

Can your vendor deliver products that are strategically designed and technically superior?

When comparing various security solutions, look for technical superiority — well-designed functionality, an intelligent architectural design and broad support for industry standards.

Why IBM?

Address your security information and event management needs with IBM

When you evaluate SIEM solutions to meet your goals, you'll find that IBM offers not only best-of-breed solutions, but also exceptional breadth and integration across its security solutions. IBM offers a broad portfolio of SIEM solutions built to provide visibility into your organization's security posture, help control the cost of demonstrating compliance and help reduce the complexity of managing a heterogeneous IT infrastructure. These solutions seamlessly integrate with each other, with other Tivoli solutions such as IBM Tivoli Identity Manager and IBM Tivoli Access Manager, and other IT processes to help you achieve an end-to-end closed loop view of your security and compliance measures. The portfolio of offerings includes the following:

- **IBM Tivoli Security Information and Event Manager delivers a foundation from which to address your SIEM requirements. It centralizes log collection and event correlation across the enterprise, and leverages an advanced compliance management dashboard and reports to link security events and user behavior to corporate policies. Tivoli Security Information and Event Manager is a soft bundle of two products that work closely together: IBM Tivoli Security Operations Manager and IBM Tivoli Compliance Insight Manager.**
- **Tivoli Compliance Insight Manager tracks privileged and other user activities on sensitive or confidential IT assets. It collects, analyzes and interprets native audit log data from a wide range of IT resources in your enterprise, including operating systems, databases and applications. Easily understandable, customizable reports and a compliance management dashboard are designed to address compliance requirements and facilitate rapid responses to exceptional behavior.**
- **Tivoli Security Operations Manager offers real-time security threat management. Its automated event correlation and incident management capabilities facilitate preemptive and rapid-response resolution of security-related problems to help maximize network availability. Integration with IBM Tivoli Enterprise Console and IBM Tivoli Netcool/OMNIbus enables Tivoli Security Operations Manager to provide critical insight into IT and operations problem resolution to help improve resource availability and resiliency.**
- **IBM Tivoli zSecure Audit integrates with Tivoli Compliance Insight Manager to feed mainframe System Management Facility (SMF) records to an enterprise audit and compliance dashboard. Similarly, for real-time threat and operation management, IBM Tivoli zSecure Alert sends real-time alerts to your central security or network management console.**

This broad portfolio of SIEM offerings can help provide the infrastructure necessary to support today's requirements. As a result, you can more efficiently:

- **Lower your exposure to security breaches.**
- **Control the costs of collecting, analyzing and reporting on compliance-related events.**
- **Manage the complexity of heterogeneous technologies and infrastructures.**
- **Recognize, investigate and respond to security incidents faster.**
- **Free IT staff to focus on higher-value activities.**

For more information

To learn more about how Tivoli security information and event management solutions can help your organization facilitate compliance, protect intellectual property and privacy, and optimize security operations, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli/solutions/security

About IBM Tivoli service management software

Tivoli software offers a service management platform for organizations to deliver quality service by providing visibility, control and automation — visibility to see and understand the workings of their business; control to effectively manage their business, minimize risk and protect their brand; and automation to optimize their business, reduce the cost of operations and deliver new services more rapidly. Unlike IT-centric service management, Tivoli software delivers a common foundation for managing, integrating and aligning both business and technology requirements. Tivoli software is designed to quickly address an organization's most pressing service management needs and help proactively respond to changing business demands. The Tivoli portfolio is backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli clients and Business Partners can also leverage each other's best practices by participating in independently run IBM Tivoli User Groups around the world — visit www.tivoli-ug.org

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
June 2008
All Rights Reserved

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.