eXpert-BSM™ – Intrusion Detection System for Solaris

PROTECTING CRITICAL SERVERS IS THE HEART OF DATA SECURITY

Organizations with sensitive information require fail-safe protection of critical systems against data theft, fraud, and abuse. Heightening this need is the escalating number of security breaches causing financial loss and associated damage within organizations.

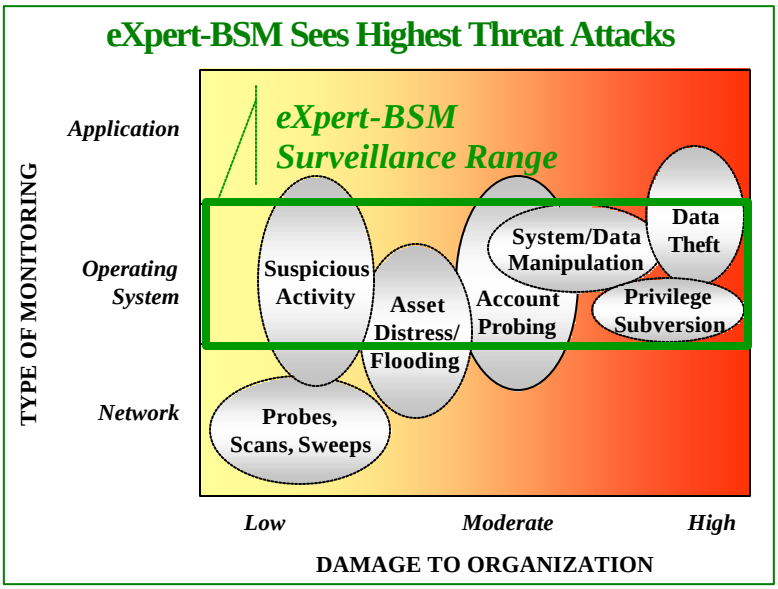
Technical approaches relying on perimeter monitoring around the network, while popular, are not a panacea for data security. In fact, they often fail to see events that security administrators regard as "must nots" for any system user.

The Power of Process Auditing

The richest, yet most overlooked source of data from which to monitor system activity is the OS kernel audit trail. Unlike syslog files, generated at an application's discretion and stored in plain text, the OS audit log is virtually tamperproof and no process request handled by the OS can escape auditing. This vantage point enables thorough, accurate security monitoring, and facilitates catching any user's attempt at insider abuse or external hacking.

EMERALD™ eXpert-BSM™ – Solaris Host Monitoring Like No Other

SRI International, a leading provider of information assurance research to the U.S. government, and a 20-year pioneer in computer and network security innovation, has tapped into the power of the C2-level* auditing capability of Sun Microsystems' Solaris operating environment to encapsulate the most comprehensive knowledge base for detecting insider misuse and security policy violations in Basic Security Module (BSM) audit trails. Called EMERALD eXpert-BSM, SRI's standalone, lightweight software monitor is unparalleled in its ability to protect your organization's most critical Solaris servers and data assets.



THE EMERALD EDGE™

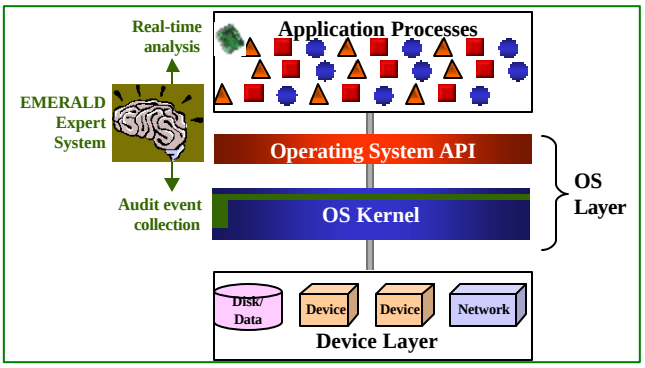
eXpert-BSM is a Solaris system administrator's most powerful tool to detect user attempted "must not" activity, such as privilege subversion, illegal data destruction, random data browsing or theft, or installation of malicious applications or backdoors. eXpert-BSM is straightforward to deploy and designed to provide immediate benefit, based on its unique features:

- **Unparalleled depth of analysis** – eXpert-BSM'S core is an advanced forward-reasoning engine designed for high-performance, real-time monitoring. Its knowledge base represents the most sophisticated suite of generalized misuse detection models available today, eclipsing the coverage of any other Solaris BSM monitor.
- **High accuracy** – the only real-time tool for monitoring C2 audit trail data from the kernel, eXpert-BSM sees deeper into system processes to achieve near-zero false positives.
- **Lightweight** – with a memory footprint similar to Emacs and only 2-5% processor utilization, eXpert-BSM runs on any critical host without degrading availability.
- **Flexible messaging** – eXpert-BSM alert messages can be configured to be pushed or pulled to administrator consoles.
- **Centralized monitor management** – eXpert-BSM supports multimonitor alert handling either by integration into in-house management systems or through use of EMERALD's console and database.

* In the 1980s, the NCSC (National Computer Security Center) of the NSA published its Orange Book Report, defining a set of Common Criteria for system security features. "C2" was one of four levels defined for computer system auditing and is viewed as the minimum acceptable level for commercially used operating systems today.

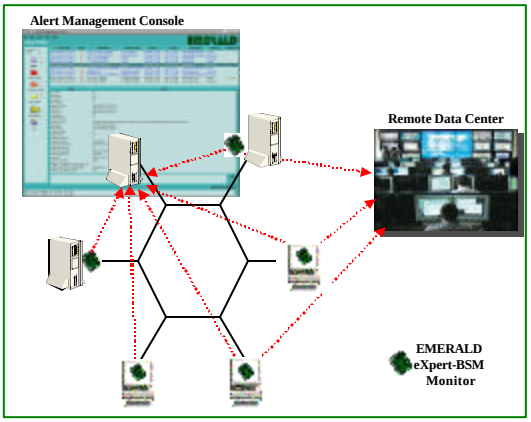
HOW eXpert-BSM WORKS

eXpert-BSM employs a kernel-loadable module that reads the BSM audit records generated each time an application process submits a request to the Solaris kernel. Each audit record is transformed into EMERALD's message format, and messages are forwarded to the event- handling interface of eXpert-BSM's expert system. eXpert-BSM's inference engine then processes the messages it receives against its knowledge base to recognize activity corresponding to one of its rules indicative of system misuse or abuse. Messages describing the alert, along with recommendation directives, are transmitted to an administrator's console.



ADVANCED ALERT REPORTING

eXpert-BSM's alert management features allow organizations to cost-effectively manage monitor alerts from multiple locations. Each eXpert-BSM monitor can automatically forward alerts along with periodic health and status messages to as many as 255 remote alert management consoles.



By using two additional EMERALD components, eAMI and eDBMS, administrators can manage eXpert-BSM monitors deployed on large networks of critical Solaris hosts from a single desktop. eAMI is an alert visualization application that allows multiple administrators to simultaneously monitor the alert database. eAMI features include "smart folders" for faster management of alerts, audio signals, sensor health and status messaging, fast database query formulation, and multiuser alert annotation facilities. eDBMS allows administrators to capture and store misuse alerts into an Oracle or Postgres database. Both eAMI and eDBMS are written in Java, allowing eXpert-BSM's sophisticated alert management services to run on either Unix or Windows consoles.

TECHNICAL SPECIFICATIONS

eXpert-BSM (Monitor)

Processor Type	SPARC™
Operating System	Solaris™ 2.6, 7, 8
System RAM	64MB
Process RAM	12MB
Application Storage	20MB Disk Space
Maximum Processors per Server	4
Maximum Monitors per Console/Database	255
Operating Modes	Realtime or Batch

eAMI/eDBMS (Alert Report Management)

Requires Java™ Runtime Environment	1.2.2
Database Compatibility	Oracle 8, Postgres 7.1
Operating System	Solaris™ 2.6, 7, 8; Linux 2.2
	Microsoft Windows™ 98/NT/2000, FreeBSD 4.2
Maximum Consoles per eXpert-BSM monitor	255

ABOUT EMERALD

Expert-BSM, eAMI, and eDBMS are components of the EMERALD software tool suite for tracking malicious activity through and across large networks. EMERALD introduces a highly distributed, building-block approach to network surveillance, attack isolation, and automated response. It combines models from research in distributed high-volume event correlation methodologies with more than a decade of intrusion detection research and engineering experience. The approach is novel in its use of highly distributed, independently tunable, surveillance and response monitors that are deployable at various layers within a network computing environment (OS, application, network service, TCP/IP). These monitors contribute to a streamlined event-analysis system that combines signature analysis with statistical profiling to provide localized real-time protection of the most widely used network services on the Internet.

For additional information, call (650) 859-4771 or see www.emerald-ids.com.

ABOUT SRI International

Silicon Valley-based SRI International (www.sri.com) is one of the world's leading independent research and technology development organizations. Founded in 1946 as Stanford Research Institute, SRI has been meeting the strategic needs of global markets for 55 years. We serve clients in information, communications, and engineering technologies; pharmaceuticals and biotechnology; chemistry and physics; and the public policy areas of education, health, and economic development. As part of its strategy to bring its technologies to the marketplace, SRI licenses its technologies, forms strategic partnerships, and creates spin-off companies.

Copyright © SRI International, 2001. All rights reserved.

SRI International®, the SRI logo, EMERALD™, EMERALD Edge™, and eXpert-BSM™ are trademarks of SRI International. All other registered trademarks, trademarks, trade names, or service marks are the property of their respective owners. SRI reserves the right to change specifications without notice.