



**Toronto, Canada –
January 19th to 21st 2010**

**PRESENTED BY:
50 MISSION SECURITY CONSORTIUM**

VANQUISHING THE LOG MANAGEMENT ENIGMA – COLLECTION, REPORTING & ANALYSIS

Log management is a complex and daunting task, driven by key business risks: the need for good IT governance, legal and regulatory compliance, and critical metrics for information security management and incident response. These risks are further exacerbated by today's business environment featuring extensive interconnectivity coupled with more intense scrutiny.

Further, the lack of effective log management leaves many organizations vulnerable when systems and networks are attacked or compromised, due to a lack of appropriate and timely information. Add to this the need to handle logging from multiple layers of operating systems, databases, applications and network devices and log management truly becomes an enigma.

Fortunately the enigma can be vanquished with the right logging processes, techniques and tools. This seminar shows you how!

This three-day workshop will provide the attendee with the detailed techniques and tools to use for collecting and managing log data within their organization. It includes a step-by-step process that addresses planning, designing, configuring, analyzing and archiving this important information. Our approach ensures that attendees leave with established skills in log management as well as knowledge of available tools.

Topics covered include:

- Key log management concepts
- Designing a log management structure that works
- Log configuration, reporting, testing, and validation
- Achieving effective management and administration

Date: January 19th to 21st 2010

Location: St. Andrew's Club
150 King Street West
Toronto, Ontario

Fees: \$1,195 (plus GST)
ISACA, IIA & FSP Members

\$1,295 (plus GST)
All others

Fees include all course materials, morning and afternoon refreshments.

Ways to Register:

On-line: www.50msc.com

E-mail: register@50msc.com

Phone: (416) 907-4816

Fax: (416) 777-6768

Payment Options:

Cheque, MasterCard, Visa



Register early! Space is limited.

In our current economic times, getting a budget for training is difficult for many organizations. 50MSC has responded by lowering our course fees by more than 20% from previous seminars.

SEMINAR OUTLINE



Part I – Background

- *Review of business drivers*
- *Understanding the needs and challenges*
- *Overview of the logging process*

Part II – Log Planning

- *Roles and responsibilities*
- *Logging standards*
- *Detailed requirements*

Part III – Designing a Log Management Infrastructure

- *Considering the issues – centralized or not, real time or batch etc*
- *High level design of sources, collection, analysis mechanisms*
- *Overview of solutions (push vs. pull, agent vs. agent-less, SIEM)*

Part IV – Logging Operational Procedures and Mechanisms

- *Configuring sources (Windows, Linux, DBMS, etc.)*
- *Configuring collectors and reporting*
- *Testing and validation*

Part V – Log Follow-up

- *Driving incident response*
- *Driving management reporting and metrics*
- *Ensuring compliance and auditing the process*

Part VI – Log Archiving and Retention

- *Review of requirements*
- *Techniques*
- *Log destruction*

Part VII – Other Issues for Consideration

Session Benefits

- *Ensure regulatory compliance*
- *Learn what metrics you should use*
- *Understand and solve collection issues*
- *Deliver valuable reporting for security management*
- *Learn tools like Snare Server*

Detailed Case Studies and Exercises using a Demonstration Environment.