



## INTRODUCTION

This one day workshop provides a hands-on experience for those interested in examining common compliance and security information event management (SIEM) challenges facing organizations today. Participants will learn how the IBM® Tivoli® “Best of Breed” Tivoli Security Information and Event Manager (TSIEM) solution is best suited to solve compliance, log management, security, and event management challenges.

## OBJECTIVE

Receive hands on experience with TSIEM - Tivoli Compliance Insight Manager

## AUDIENCE

This Proof of Technology is specifically targeted for Enterprise / Security Architects, Systems Administrators, and Systems Analysts Compliance and Security Event and Information Management solutions for their organization. No prerequisite knowledge of any IBM Tivoli Security products is required. However, it is recommended that participants have an understanding of their organization’s business needs and current IT technologies.

## SCHEDULE

For your convenience, registration and continental breakfast will begin at 8:30 AM. The session will start at 9:00 AM and end at approximately 4:30 PM.

## AGENDA

**9:00AM – 9:10AM:** Welcome

**9:10AM – 10:30AM:** TCIM technical overview, architecture, demonstration and discussion

**10:30AM – 10:45:** Break

**10:45 AM - 12:00:** Hands on exercises

**12Noon – 12:45PM:** Lunch

**12:45PM – 4:00PM:** Hands on exercises

- Exercise 1 – Windows® event sources
- Exercise 2 – Rogue trader case investigation
- Exercise 3 – z/OS® RACF® and DB2® event source
- Exercise 4 – z/OS top secret event source
- Exercise 5 – UNIX® syslog investigation
- Exercise 6 – iSeries™ – OS/400® investigation
- Exercise 7 – IBM Tivoli Compliance Insight Manager management console
- Exercise 9 - Creating a new Windows event source
- Exercise 10 - Creating a new custom event source
- Exercise 11 - Tivoli Security Operations Manager event source

**4:00PM – 4:15PM:** Wrap up