# THE SECURITY STANDARD™

## Securing the Enterprise from a Dangerous Cyberworld

**September 19-20, 2011** • Marriott Brooklyn Bridge, New York City

Produced by

CSO

# Security Event and Information Management

By

David N. Kroening

NY State Insurance Fund

# Case Studies on Why SEIM is Important

- Xpress Scripts
- UN RAT
- WikiLeaks

# Examples of Security Events

- System Logon/LogOff
- System shut down/Restart
- Map drive resources
- Burn a CD.

# What are “Logs” and Where Did They Come From

- Came from the Marine Industry
- Line or cord off the side of the ship
- Knot every 50 feet.
- Timed for 30 seconds
- Consistant place of record for other ship actvities.
  - Weather events.
  - Watchstanding.

# What Makes Good Logs

- Consistent Time Source
- Appropriate logging detail settings.
- Enough Space
- Archival strategy

# It All Begins With Policies

- Management approved.
- Communicated to managers
- Communicated to System Admin.

- Suggested Elements
  - All systems must log
  - System Admins must ensure consistant logging
  - Logs must be reviewed regularly

# Who Else Is Interested In This Stuff?

- System Admin – troubleshooting systems.
- Internal Audit – Records of Activity.
- Admin/Personnel – User Activity.
- Internal Controls – Evidence of Activity.

# Government Is Also Interested…

- NY State Office of Cyber Security
- PCI – Infamous Req 10
  - 10.1 – Logging is enabled and active
  - 10.4 – Time Synchronization
  - 10.5 – Audit trail security
  - 10.6 – Log Review –
  - 10.7 – Log Retention
- FISMA – Extensive requirements

# Suggested Goals

- All systems create logs of normal activity.
- More logs if handling sensitive information, user accreditation or money movement.
- SANS Top 5 Reports
- Hold As Long As Possible.

# Log Review Time

- Check for consistancy
- Have admins identify activity in the logs.
- Look for automated solutions.

# Things to Keep In Mind When Picking a Solution

- Budget
- Type of environment (What are you logging)
- Appliance or machine?
- Windows or Unix?
- Resilience Posture.

# Questions?

Thank You!

David N. Kroening
dkny@noah.com