Title
Introduction to responding to an endpoint incident, Malware Discovery, what to configure, and look for (2-Days)

Description (At least a paragraph describing the course that will be used in marketing materials.)
Responding to an incident, malware discovery and basic analysis is an essential skill for today's Information Security and IT professionals. This course focuses on how to discover if a system has malware, how to build a malware analysis lab and perform basic malware analysis quickly. The goal and objective is to respond quickly, obtain actionable information, and improve your Information Security program. Tools and techniques used and steps to analyze a system to determine if a system is clean or truly infected will be covered. The concept of Malware Management, Malware Discovery and Malware Analysis will be discussed with exercises linking the three concepts together.

This course is intended for any Information Security or IT professional. The focus will be on Windows systems; but will touch on some tools for Apple and Linux systems as well. All attendees will get a copy of ***LOG-MD Professional*** as part of the class. Bring a laptop you can infect!

Outline
Day 1

- Introductions, Goals & Objectives and Terms & Concepts
- Configuring/preparing a system for investigation
- Malware Management & Labs
- Lunch – Provided by ????
- Malware Discovery & Labs
- Types of Analysis and Malware Analysis flows
- Malware Analysis Data Labs
- Questions and Discussion

Day 2

- Complete Building a Malware Analysis Lab
- Malware Analysis Introduction
- Malware Analysis Tools
- Lunch – Provided by ????
- Automated Analysis & Lab
- Basic Malware Analysis & Lab
- Logging for Malware
- Questions and Discussion

Target Audience (Who should take the course)
This course is intended for any Information Security or IT professional, newbs to seasoned pro's, just know how to use the windows command line.

Facility Requirements
Overhead projector, power for all the desks, and a 24x36 easel pad with markers or whiteboard.

Student Requirements (what should they bring with them)

Students will need a laptop with Windows. Instructions will be emailed on what to load prior to the class