SOC-Class Executive Summary

The class provides the following:

- Guidance on business orientation, use case development, hunting techniques
- Reference model for all functions of a SOC: monitoring, response, intelligence, metrics
- Guidance on developing internal capability and strategic outsourcing
- Detailed discussion of technology, process, and analytical staff relations and optimization
- Sequence of actions for building a SOC, or cross reference an established SOC's maturity

This course provides a comprehensive picture of a Cyber Security Operations Center (CSOC or SOC). Discussion on the technology needed to run a SOC are handled in a vendor agnostic way. In addition, technology is addressed in a way that attempts to address both minimal budgets as well as budgets with global scope. Staff roles needed are enumerated. Informing and training staff through internal training and information sharing is addressed. The interaction between functional areas and data exchanged is detailed. Processes to coordinate the technology, the SOC staff, and the business are enumerated.

After attending this class, the participant will have a roadmap (and Gantt chart) for what needs to be done in the organization seeking to implement security operations. Ideally, attendees will be SOC managers, team leads in security specializations or lead technical staff, security architects. CIO, CISO or CSO (Chief Security Officer) is the highest level in the organization appropriate to attend.

The inclusion of all functional areas of security operations is intended to develop a standardized program for an organization and express all necessary capabilities. Admittedly ambitious, the intention of the class is to provide a unified picture of coordination among teams with different skillsets to help the business prevent loss due to poor security practices. I have encountered detrimental compartmentalization in most organizations. There is a tendency for a specialist to look only at her piece of the problem, without understanding the larger scope of information security within an organization. Organizations are likely to perceive a security operations center as a tool, and not the unification of people, processes, and technologies.

This class is not technical in nature, but someone without knowledge of IT common practices and Information Security fundamentals (such as the Confidentiality, Integrity, and Availability triad) will be lost very quickly. This is not a class to send SOC analysts, but is great for the technical lead and manager.

Register: https://www.soc-class.com

Topic List

- Class Orientation
  - A Story About Telling Stories
  - First Principles and Terminology

- Business Alignment
  - Steering Committee – Phase 1: Design
  - Requirements
  - Impact
  - Charter

- SOC Design
  - Functional Components
  - Presumed Organizational Support Functions
  - Functional Arrangements
  - Operational and Architectural Considerations
  - SOC Organizational Position
  - Multi SOC Models
  - SOC and IT Relations
  - Size and Maturity
  - Size: What Does It Look Like?
  - Outsourcing Advice

- Overall Program of Operations
  - Intro
  - Command Center
  - Network Security Monitoring
  - Threat Intelligence
  - Incident Response
  - Forensics
  - Self-Assessment

- Business Alignment (2)
  - Defensive Topology
  - Steering Committee: Phase 2: Build

- SOC Design
  - Functional Area Work Products
  - Technology Selection
  - Physical SOC Build
  - Technology Selection
  - Cultural and Organizational Influence on SOC Requirements and Performance
  - Orchestration and Automation

- Analysis
  - Analytical Methodology for the SOC
  - Applied ACH
  - Available Frameworks for Analysis
  - Analytical Methodology: Wrap Up

- Staff
  - Roles
  - Hiring
  - Onboarding
  - Training
  - Meetings
  - Retention

- Operations
  - Tempo
  - Pre-Forensics
  - Threat Hunting
  - Use Case Development

- Metrics
  - Introduction
  - Appropriate Audience
  - Reported
  - Steering Committee: Phase 3: Operations
  - Service Level Objectives
  - SOC Internal Health and Performance

- Maturity
  - Introduction
  - SOC-CMM Walkthrough

- Processes
  - Process list
  - Sequence Walk Through

- Case Study
  - Phin Phisher
  - Insiders
  - Equifax