G. Bina
Secure Your Cyber-Space & IT

Building a Successful Security Operation Center (SOC)

A 3 day learning program which Include demonstrations of the Israeli security operations management state of the art methodologies

Developed by Dr. Col. (res.) Gabi Siboni

Building a Successful Security Operation Center (SOC)

A 3 Day Seminar

Introduction

Designing, building, and managing an internal security operations center can dramatically improve an organization's ability to rapidly recognize and respond to malicious information security events. A SOC can also assist in ensuring organizations leverage the full value of the often expensive investment in security technology and meet a myriad of regulatory compliance requirements.

About the Course Owner and Developer

This course is developed by Dr. Col. (res.) Gabi Siboni, Director of The Cyber Security Program at The Institute for National Security Studies, Tel Aviv University and Serves as chief methodologist of the IDF's Research Center for Force Utilization and Buildup – Experimentation Laboratory.

Dr. Siboni is a domain expert in national security, military strategy and operations, military technology, cyber security and warfare, and force buildup and a thought leader in business operations risk management.

Who should attend?

Information security managers, System information project managers, systems implementers and CIOs who are interested in the field of cyber-security operations and looking to expand and develop their cyber-security capabilities.

Cyber warfare operations, strategic planning, operation and force buildup planning, risk management, command and control systems, etc.

Course Curriculum

This training is designed to present the industry best practices for building and maturing a SOC. It focus on of the SOC typical mission parameters, the business case, people considerations, processes and procedures, as well as learning how to normalize, aggregate, and correlate the security events across technologies.

This training highlight the Israeli security operations management state of the art know-how.

Topic	Contents
Introduction and defining A Security Operations Center	establish the mission, responsibility, and scope of the SOC
Understand the Environment	Determine the technical domain to be monitored, the “Use Cases,” and the type of data that is received by the SOC
Determine the Processes	identify and clearly document key templates, procedures, and processes required to support the SOC
Identify the Customer	Determine the classes of customers and their interaction with the SOC
Monitoring and Intrusion Detection (IDS)	passive and reactive intrusions alarms, detection rate, site policy, site policy awareness
Handling and Responding to Incidents	Incident response methodology, security severity, event categorization and incident prioritization and escalation
SOC management	SIEM systems, SOC staffing, SOC SLAs, SOC KPIs and dashboards
Establishing Cyber Intelligence Capabilities	Direction, Collection, Analysis, Dissemination
Data Leakage	Data leakage threats, Type of data leakage, mitigation and Data Leakage Prevention (DLP) tools.
Intro to digital investigations and Forensics Analysis	Forensic process, digital evidence, investigative tools

* * Learning materials will be provided to participants by a magnetic means