CONCEPTS COVERED

Measuring Defensibility, Durability, and Reducing Liability

Understanding High-Velocity & Violent Attacks

Establish the Golden Hour

Threat Centric Incident Response Policies & Procedures

Rapid Response Methodology

Protocol Driven Response

WHO SHOULD ATTEND

CIO, CISO, COMPLIANCE, INCIDENT RESPONSE TEAM MEMBERS

TRAINING OVERVIEW

The training covers theory and strategy for your hospital's incident response.

Includes hands-on exercises and workshops to customize protocols and drills for your hospital.

You will test your assumptions through tabletop simulations.

TACTICAL CYBERSECURITY INCIDENT RESPONSE TRAINING

3 Sessions: Dec 14, 15, 16 2021
1:00 p.m - 5:00 p.m. ET

REGISTER NOW

$2,500 per person

For NRHA Members: Set a 30-minute Meeting with us and get a code to attend for Free.

www.sensato.co
KEY TAKEAWAYS

Dynamic Incident Response Plan – based on dynamic protocols designed to be flexible and change over time.

Advanced Protocols – based on the approach used by Level I trauma centers. You'll be able to deal with casual to extremely advanced cybersecurity attacks.

Intelligence-Driven Response Plan - We will focus on the use of logical intelligence to manage and drive the incident response.

Comprehensive Incident Response Platform – if an attack occurred minutes after the training, you would be ready to respond.

Tools & Tactics – a set of real-world protocols, immediate action drills, and more.

INSTRUCTOR: JOHN GOMEZ, CEO, SENSATO

john.gomez@sensato.co

John is the founder and CEO of Sensato. In addition to Sensato's portfolio of cybersecurity solutions, Sensato is an Information Sharing & Analysis Organization (ISAO) and coordinates with the FDA, CISA and other government agencies to share cybersecurity information.

John has been involved in cybersecurity and high technology for more than three decades. John has lectured on cybersecurity, physical security, and advanced technology topics worldwide. Before founding Sensato, John has held executive roles at Allscripts, WebMD and Microsoft.