سرفصل دوره آموزشICS515

- **ICS515.1: Threat Intelligence**

  - Case Study: Havex
  - Introduction to ICS Active Defense and Incident Response
  - Intelligence Life Cycle and Threat Intelligence
  - ICS Information Attack Surface
  - External ICS Threat Intelligence
  - Internal ICS Threat Intelligence
  - Sharing and Consuming ICS Threat Intelligence

- **ICS515.2: Asset Identification and Network Security Monitoring**
  Case Study: BlackEnergy2
-
  - ICS Asset and Network Visibility
  - Identifying and Reducing the Threat Landscape
  - ICS Network Security Monitoring – Collection
  - ICS Network Security Monitoring - Detection
  - ICS Network Security Monitoring – Analysis

- **ICS515.3: Incident Response**
  Case Study: Stuxnet

  - Incident Response and Digital Forensics Overview
  - Preparing an ICS Incident Response Team
  - Evidence Acquisition
  - Sources of Forensic Data in ICS Networks
  - Time-Critical Analysis
  - Maintaining and Restoring Operations

- **ICS515.4: Threat and Environment Manipulation**
  Case Study: German Steelworks

  - ICS Threat and Environment Manipulation Goals and Considerations
  - Establishing a Safe Working Environment

  - Analyzing Acquired Evidence
  - Memory Forensics
  - Malware Analysis Methodologies
  - Case Study: BlackEnergy2 Automated Analysis
  - Indicators of Compromise
  - Environment Manipulation

- **ICS515.5: Active Defense and Incident Response Challenge**
  Scenario One

  - Identify the assets and map the ICS networks
  - Perform ICS network security monitoring to identify the abnormalities
  - Execute ICS incident response procedures into the SANS Cyber City data files
  - Analyze the malicious capability and determine if the threat is an insider threat or a targeted external threat
  - Scenario Two
  - Identify the software and information present on the DCS
  - Leverage ICS active defense concepts to identify the real-world malware
  - Determine the impact on operations and remediation needs