CATEGORIZATION OF CYBER TRAINING ENVIRONMENTS FOR INDUSTRIAL CONTROL SYSTEMS

Evan Plumley, Mason Rice, Stephen Dunlap and John Pecarina

Abstract First responders and professionals in hazardous occupations undergo intense training and evaluation to enable them to efficiently and effectively mitigate risk and damage. For example, helicopter pilots train with multiple simulations that increase in complexity before they fly real aircraft. However, in the industrial control systems domain, where incident response professionals help detect, respond and recover from cyber incidents, there is no official categorization of training environments, let alone training regimens. To address this gap, this chapter provides a categorization of industrial control training environments based on realism. Four levels of environments are proposed and mapped to Bloom’s Taxonomy. The categorization enables organizations to determine the cyber training environments that best align with their training needs and budgets.

Keywords: Industrial control systems, incident response, training environments

1. Introduction

In the evening of April 17, 2013, an act of arson at a fertilizer plant in West, Texas resulted in an explosion that killed fifteen people, including ten first responders who were fighting the fire [10, 19]. The first responders were not trained to handle a chemical fire and did not fully comprehend the explosive hazards posed by the materials in the plant. The U.S. Emergency Planning and Community Right to Know Act requires all companies to report hazardous chemicals stored in their facilities. However, there are no legal requirements for local first responders to be trained adequately based on the hazard reports.

To avoid disasters like the Texas explosion, it is imperative that incident responders receive training in environments that teach them the required incident response knowledge and skills as well as help assess the extent of the acquired
knowledge and skills. Processes in an industrial environment are managed using industrial control systems that have limited or weak cyber security protections and can pose physical threats to personnel and equipment. The first responders tasked to respond to incidents in industrial control environments must be properly trained and prepared to deal with the complexity and diversity of cyber incidents.

This chapter proposes a framework for identifying and mapping industrial control system cyber incident response knowledge and skills to training environment components. This chapter also proposes a categorization of training environments based on practicality and realism. The categorization assists organizations in determining the cyber training environments that best align with their training needs and budgets.

2. Incident Response Training Environments

The lack of industrial control system defenses is a cause for concern in the community. Contributing factors include cost, system diversity, long lifecycles and organizations that are reluctant to make changes to their operational systems [28]. Generally, the personnel employed at industrial control facilities do not have the skills to properly collect, analyze and examine the command and control traffic in their networks and they find it difficult to differentiate cyber attacks from non-cyber-induced malfunctions [9]. While most organizations are unable to provide high levels of training to their cyber response teams, they can support effective – albeit lower levels of – training that balance organizational goals and budgets. This section discusses the current state of industrial control system training and training environments at U.S. Government, industry and academic entities.

2.1 U.S. Government

The U.S. Department of Homeland Security Department is the U.S. Government entity that provides the vast majority of training programs in the area of industrial control systems. The training efforts primarily focus on the effects of attacks and the development of mitigation strategies as opposed to emergency incident response.

Training courses offered by the Industrial Control System Cyber Emergency Response Team (ICS-CERT) leverage a partial industrial control system to demonstrate exploits and their impacts; the courses culminate in a red and blue team exercise where participants attack and defend an industrial control system [14]. While the training environment is by no means a full-scale system, it incorporates realistic hardware and displays real physical effects. Participants in the advanced course are expected to have prior knowledge of information technology as well as industrial control systems. The advanced course encourages discussion between information technology and industrial control system professionals, which enhances the development of contextual knowledge in both communities. In a real incident response setting, profesion-