Cybersecurity at MIT Sloan

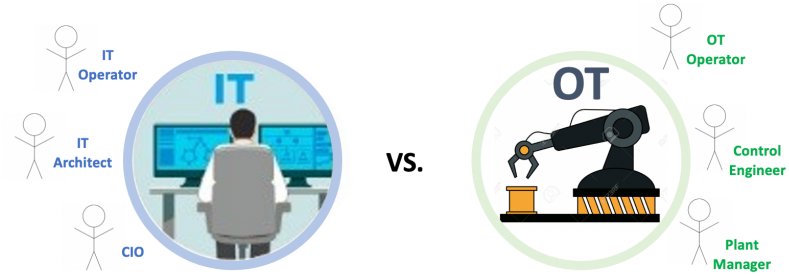
Cybersecurity at MIT Sloan
Developing a Cyber Range for Simulating Attack Scenarios

Cybersecurity at MIT Sloan brings thought leaders from industry, academia, and government together with MIT faculty, researchers, and students to address strategy, management, governance, and organization of cybersecurity of critical infrastructure using an interdisciplinary approach.

The Cyber Range Simulation

The Cyber Range is a safe, isolated approach to security training and learning how to secure OT environments without impacting business or operations. This research project examines both the IT and the OT side of the cyber range and looks at them in a holistic way. Securing industrial networks without disrupting operations or risking non-compliance is possible using the Cyber Range. CAMS modeled a physical process that considers both environments to predict a systems' behavior with changeable parameters of a model. Users can design and play out a simulation to better understand what happens during an attack, why it happens, and how to secure their real OT systems based on this information.

The goal is to provide a training platform for joint IT/OT Cybersecurity operations to predict, detect, and respond to cyber-attacks.



Business Priority	Data Confidentiality, Integrity	Availability (Equipment Downtime)
Attack Surface	Computers, Servers, Printers, Network Switches	Industrial devices, PLC, HMI, Field Devices
Consequences	Loss of Data	Physical Damage

How the Simulation Works

The simulation works by having parameters and settings that are modified to specific use cases. The user selects the industrial setting and the exercise type for a storyboard of a training exercise that applies to their company. The simulation then allows for two people to be on either ends of an attack. Both the attacker and the operator can simultaneously control the simulation in real time. The attacker first makes his way to the original network where he starts interfering with the OT environment. This helps to understand hackers' actions. The system responds in real time to the changes in exhaust temperatures and other control features.

IMPACT: The advantage of having a cyber range platform is the ability to model a specific type of IT and OT network and have system interconnection. It is a safe, isolated approach to training and learning without impacting business operations. The ICS Cyber Range enables enhanced cyber awareness for OT and IT operators and brings OT and IT together to improve cyber resilience.

Cybersecurity at MIT Sloan welcomes funding from sponsors for general support of the consortium research, and from organizations interested in specific research topics. All members and sponsors receive invitations to consortium events and activities, and access to consortium research, websites, and newsletter. For more information visit cams.mit.edu or contact:

Dr. Stuart Madnick • Professor and Director • smadnick@mit.edu
Dr. Michael Siegel • Director • msiegel@mit.edu
Dr. Keri Pearlson • Executive Director • kerip@mit.edu