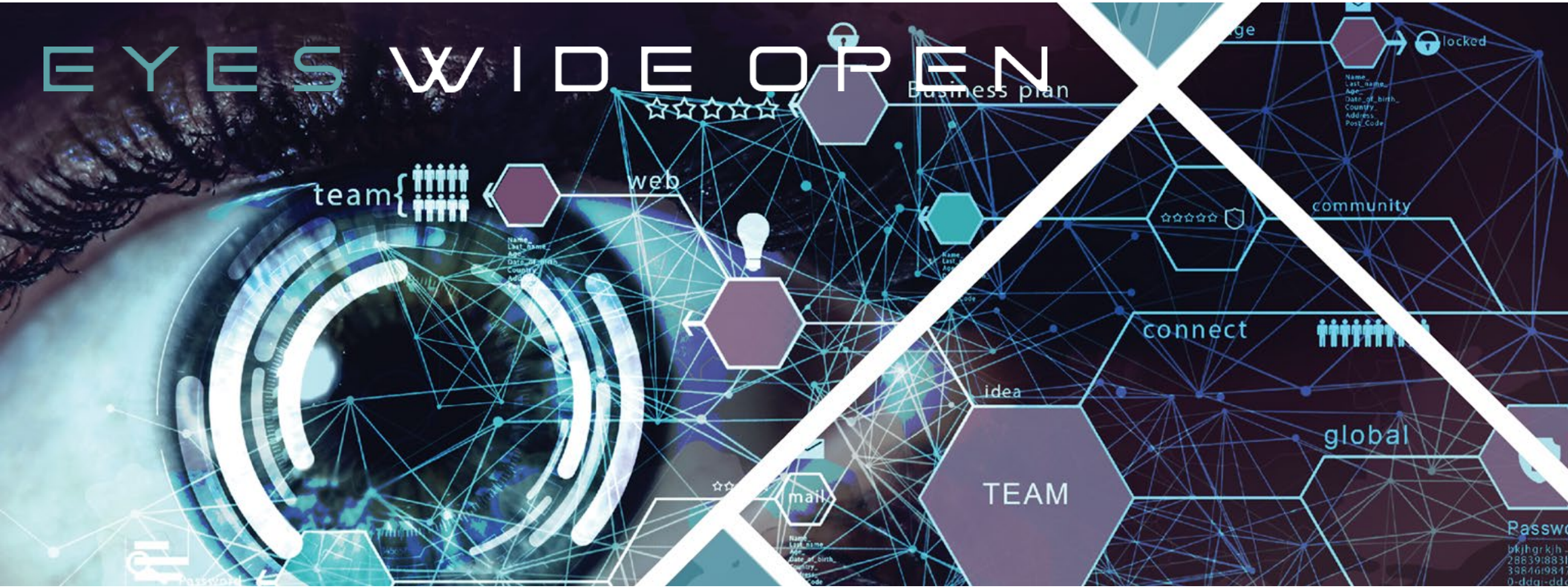
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

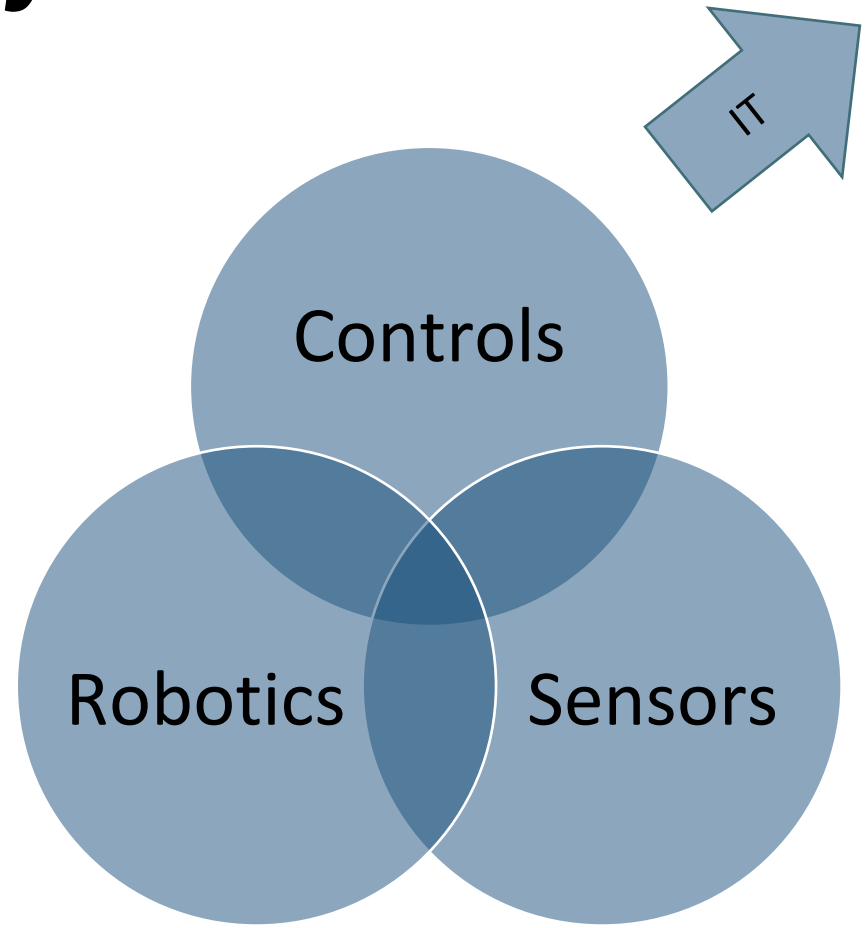
TITLE SPONSOR

Island



Operational Technology at Dunwoody College

E.J. Daigle
Dean – Advanced Manufacturing, Robotics & Computers



A History of Manufacturing & Automation

Machining	108 years
Welding	107 years
Electronics	75 years
Robotics	35 years
IT/Computers	30+ years

A History of Partnerships

Machine Tool

12 Haas CNC machines all networked to industrial ethernet

Wire & Sinker CNC EDMs

Welding & Metal Fabrication

18 Lincoln 300C MIG

18 Miller Dynasty 280 TIG

All Lincoln machines are connected to industrial ethernet.

FANUC Robotics Lab

10 FANUC LR Mate robots

12 EPSON SCARA robots

2 UR Collaborative robots

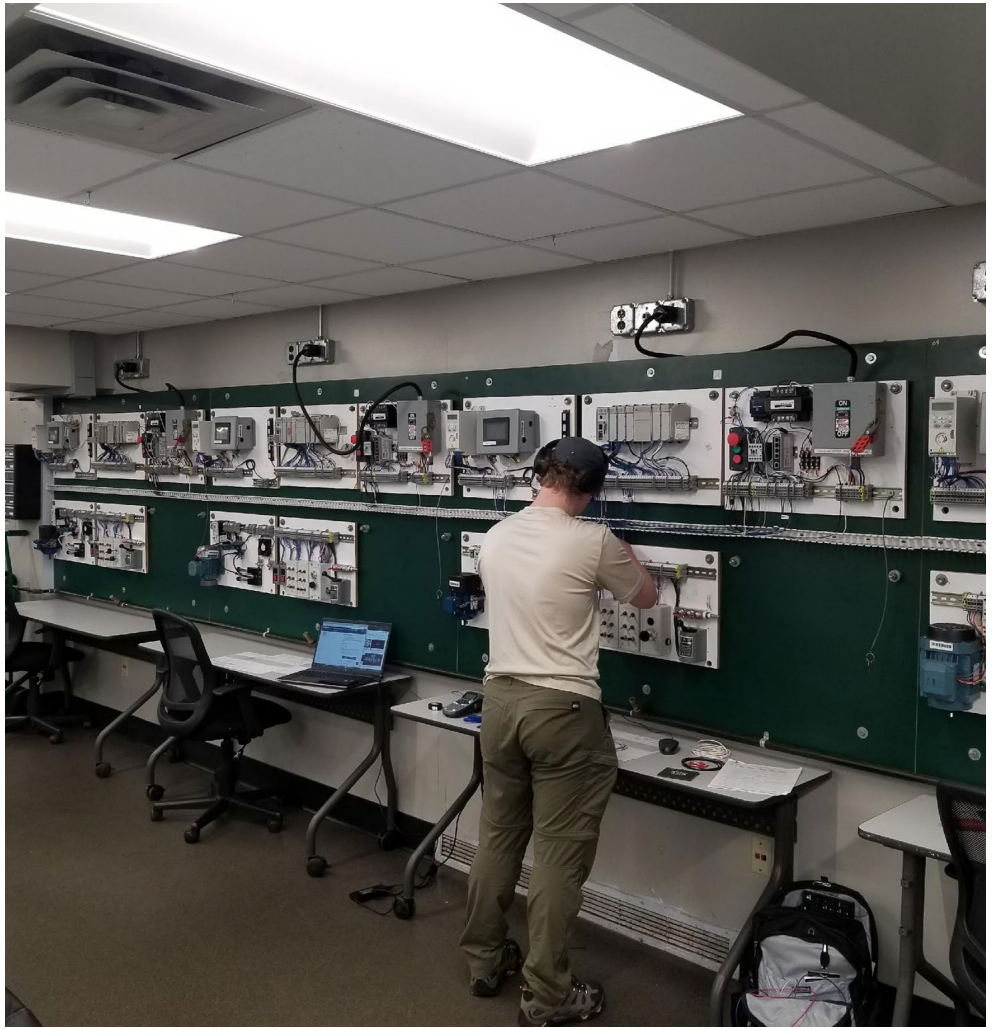
Programmable Logic Controllers

12 AB MicroLogix PLCs

12 AB CompactLogix PLCs

12 Siemens S7-1200 PLCs

Large Industrial network with PLC tags shared across the labs



Controls Engineering Lab

24 stations of PLC, HMI, VFD, SERVO, SCADA, and VISION controls

162 total networked devices all talking to each other in this lab

Emerson Process Controls

Two 60-gallon tanks

Two centrifugal pumps

12 Rosemount instruments – PLC produced tags shared with 24 lab PLCs

https://youtu.be/oe4SmsVHYmY

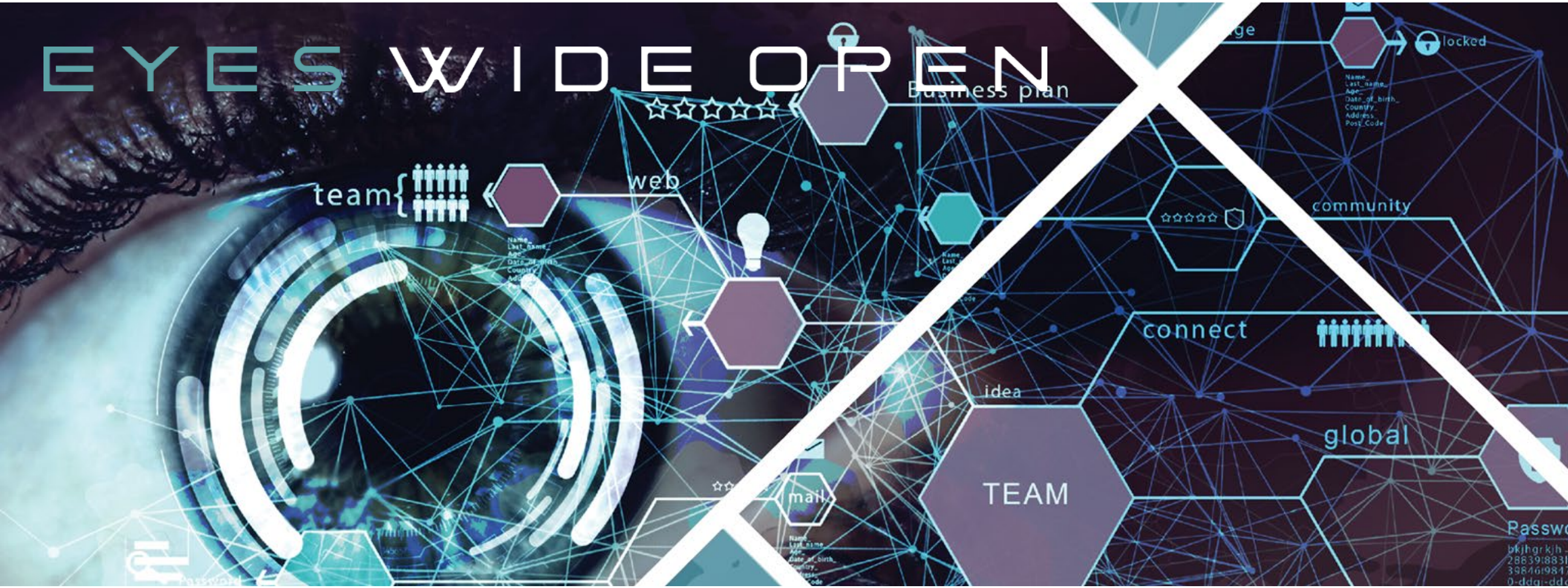
12TH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

TITLE SPONSOR

Island



Industrial Cybersecurity

IT and OT blended

Industrial cybersecurity

Industrial cybersecurity references the software, hardware, practices, personnel, and services deployed to protect operational technology(OT) infrastructure, people, and data.

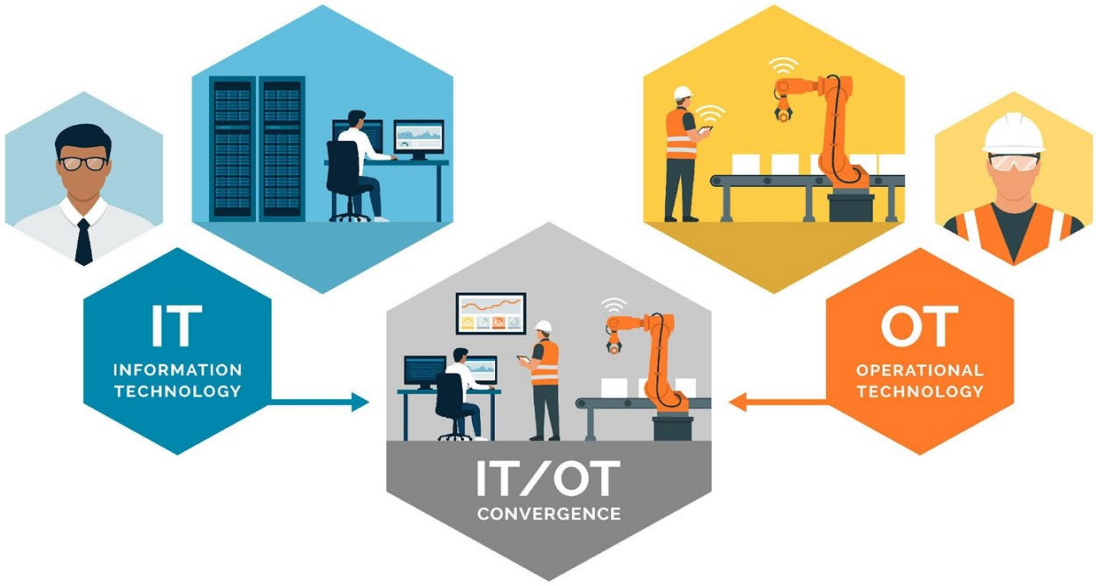
The Business Case for Industrial Cybersecurity

The broad adoption of big data analytics, has prompted organizations to further integrate traditional IT systems and traditional OT infrastructure.

Connecting industrial systems to an IT network allows a more detailed view of individual equipment and creates a comprehensive view of the entire industrial ecosystem, simplifying management and operation.

This enables constant monitoring of the performance and condition of equipment and systems, which improves uptime.

These benefits are compelling and explain the explosion of interest in IT/OT integration.



IT CIA vs OT CAIC Model of Priorities

The standard for IT cybersecurity, The (CIA) triad.	The standard for OT cybersecurity, CAIC
• **C**onfidentiality, Keeping digital assets safely under lock and key	• **C**ontrol, control of all physical assets to ensure their safe operation at all times is the primary objective
• **I**ntegrity, ensure that data is not corrupted in any way	• **A**vailability, critical infrastructure typically needs to be available 24/7/365
• **A**vailability, data needs to be available internally to appropriate employees and partners, and potentially customers	• **I**ntegrity, it ensures safety and availability
	• **C**onfidentiality, Confidentiality of OT data is far less of a concern than it is for IT data

State Of Enterprise IoT Security: A Spotlight On Manufacturing

- 73% of organizations surveyed estimate that at least half of all devices in their enterprise are unmanaged or IoT devices
- 74% are “very-to-extremely concerned” about the risks posed by unmanaged and IoT devices
- 66% have experienced an IoT-related security incident
- 96% plan to increase their budget dedicated to unmanaged and IoT device security
- 48% are planning to deploy an agentless security platform over the next 24 months are planning to increase spending on security for IoT and unmanaged devices over the next 24 months

The Mythical OT Air Gap

The classic method for OT security was air gaping systems, OT was not connected to the IT network and therefore protected from the outside world.

“Complete isolation has become all but impossible today, however, and to mitigate new risks to OT, organizations will need to deploy a combination of traditional IT cybersecurity products and services with tailored, OT-specific cybersecurity solutions.”

“Maintaining control of all physical assets to ensure their safe operation at all times is the primary objective of OT cybersecurity and overrides all other concerns.”

Taking Responsibility for OT Cybersecurity

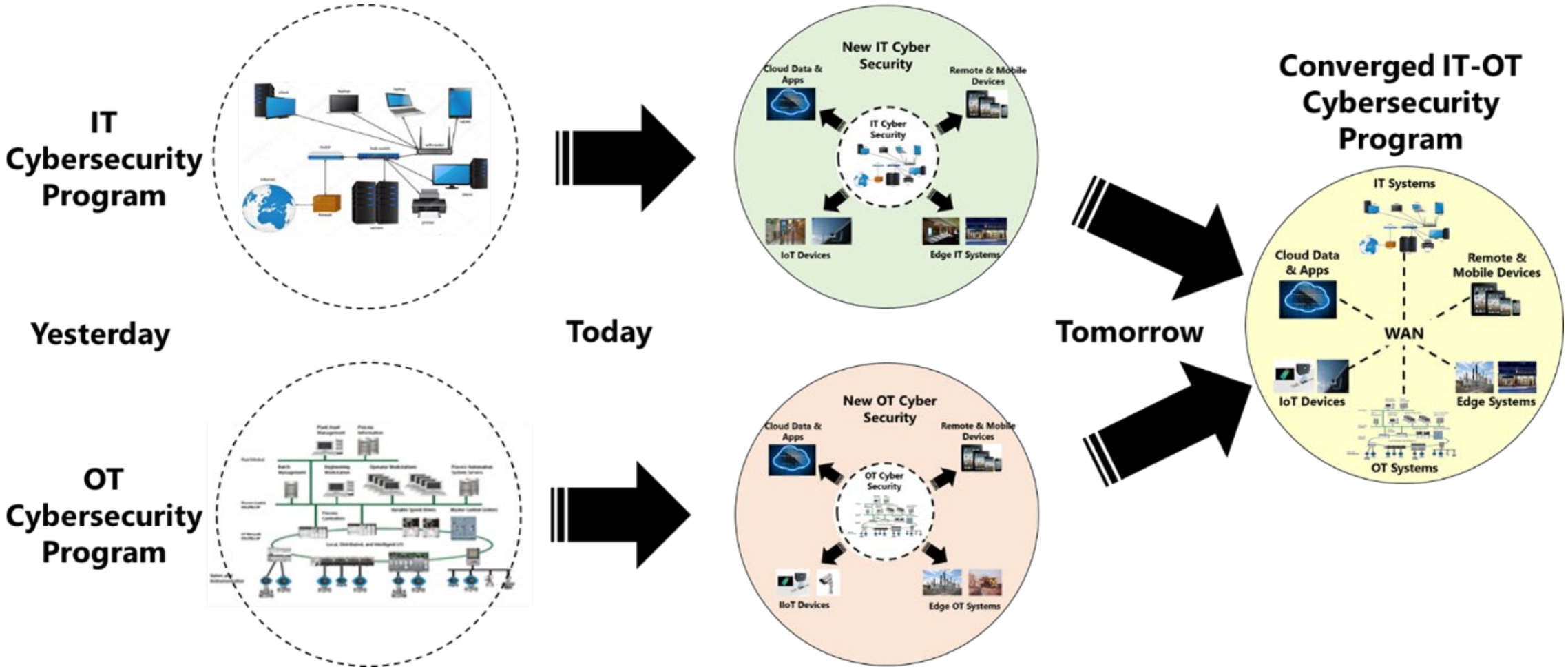
A recent McKinsey report noted:

"Many heavy industrials we surveyed could not identify a party responsible for OT cybersecurity.

The chief information-security officer (CISO) may set policy and develop security standards but often has no responsibility for implementing OT cybersecurity in the operations, or for auditing adherence to it.

At the same time, many operational units have no clear cybersecurity counterpart responsible for deploying, operating, and maintaining OT cybersecurity controls at the plant level. Therefore, they often neglect OT cybersecurity."

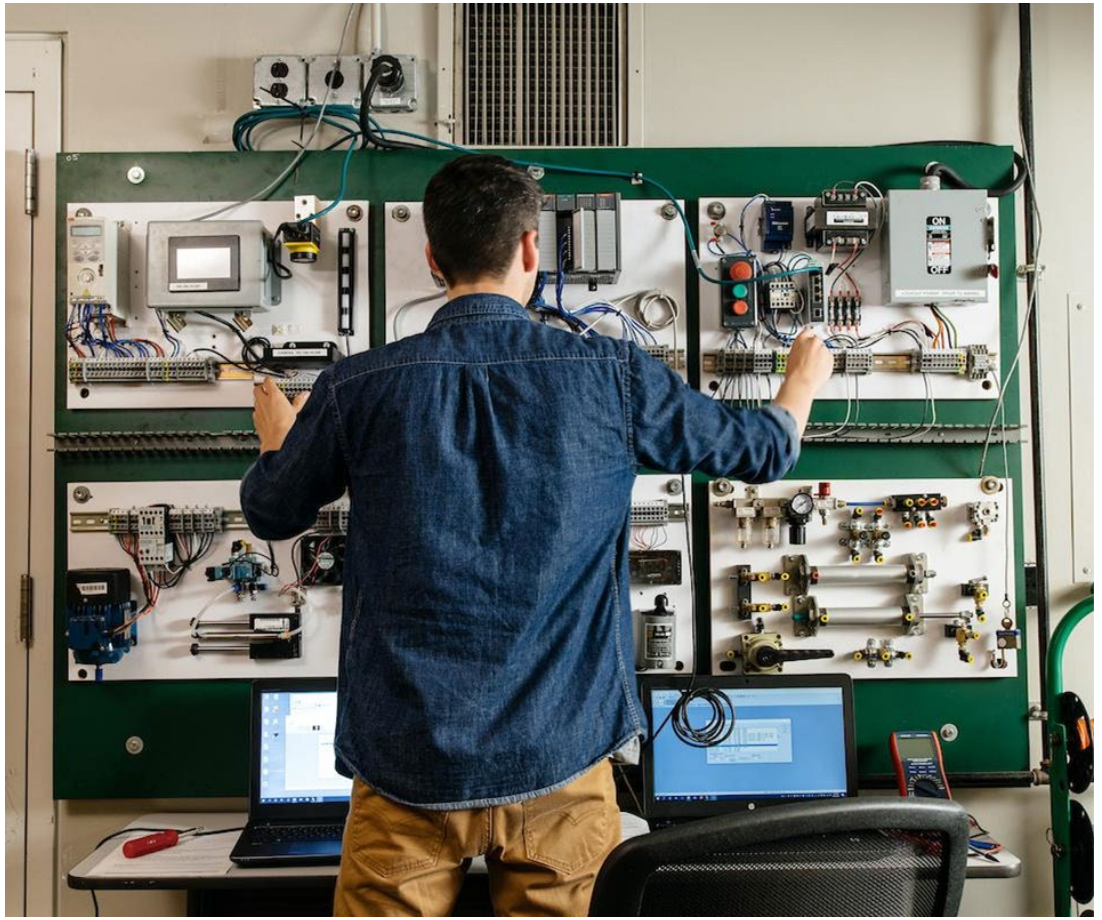
The opportunity



Dunwoody part of the solution

Leveraging Dunwoody College of Technology's experience in OT and IT

We are creating an **I**ndustrial **C**enter for **C**ybersecurity and **C**loud Technology ready to develop the workforce for the challenges presented by the fourth industrial revolution.



IC³

Industrial Center for Cybersecurity and Cloud Technologies

Our partners in building the curriculum

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

ISA International Society of Automation

IEC International Electrotechnical Commission

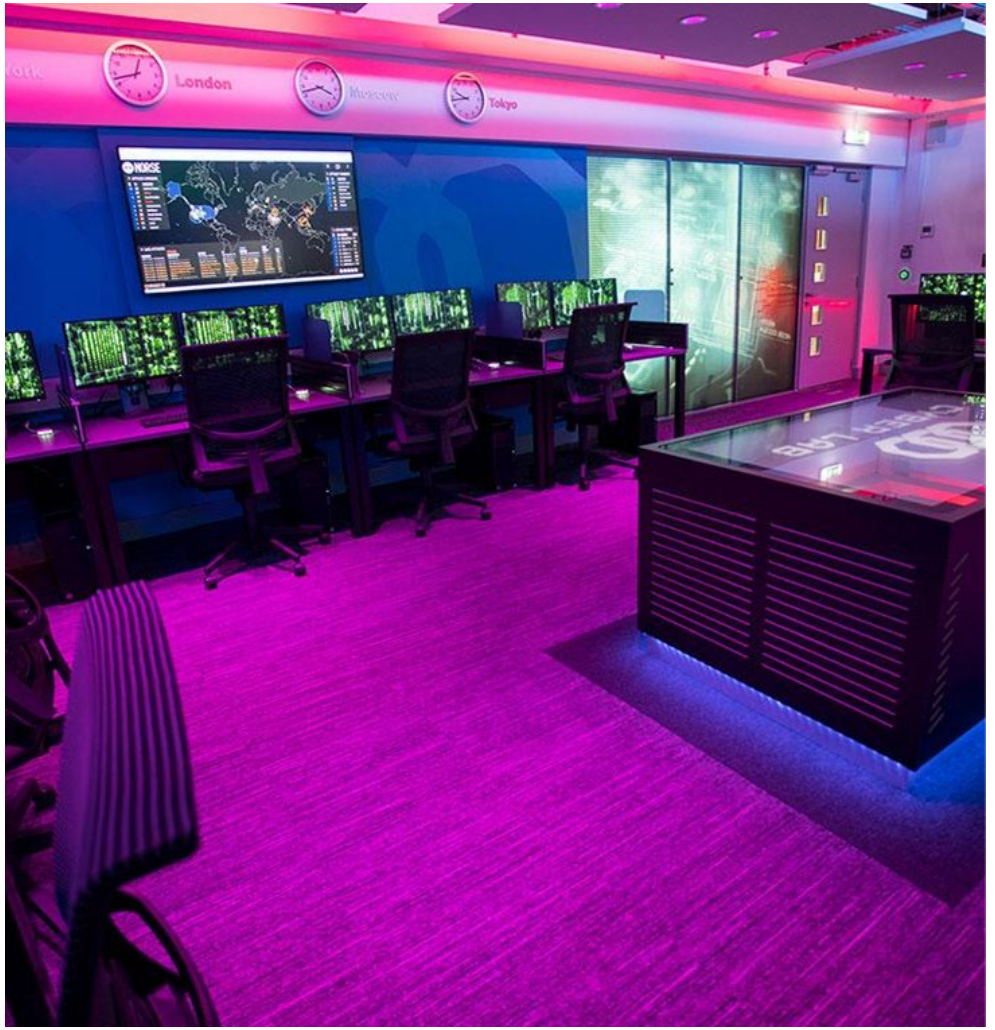
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

U.S. DEPARTMENT OF HOMELAND SECURITY

Coming soon: Industrial Cyber range fronted by a Security Operations Center (SOC)

Industrial Cyber range

- Used in the classroom for running simulated attacks allowing students to get hands on experience in cyber defense of OT , IT and mixed environments.
- Will be available for our business community partners to hold training days and events.

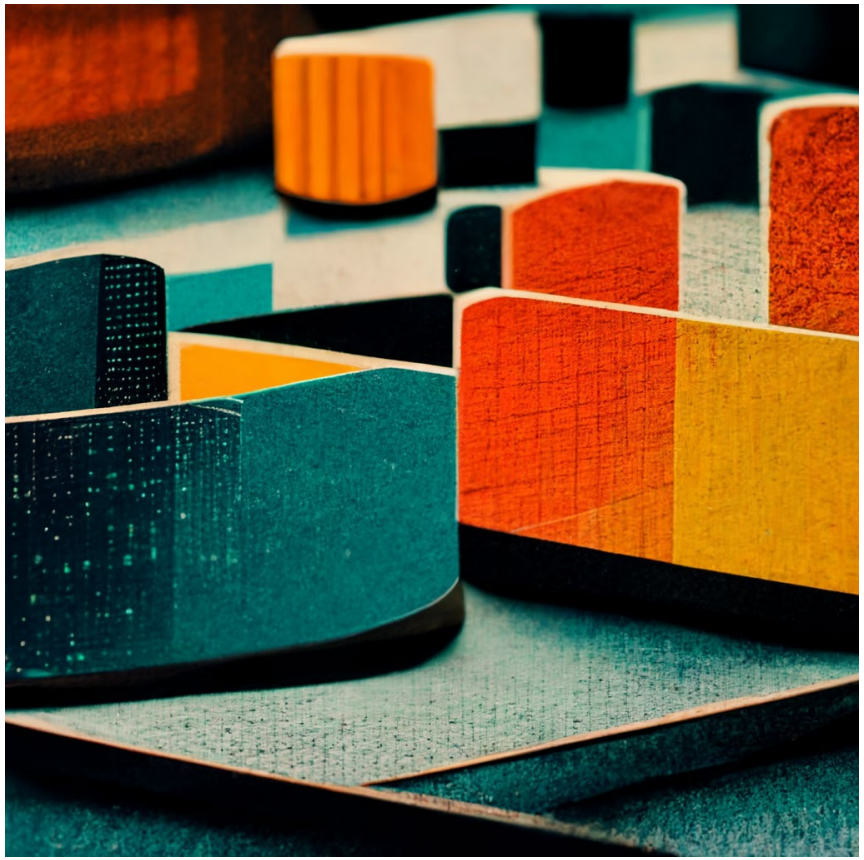


Our challenge

As a private nonprofit,

Keeping tuition affordable for our students.

Where you can help



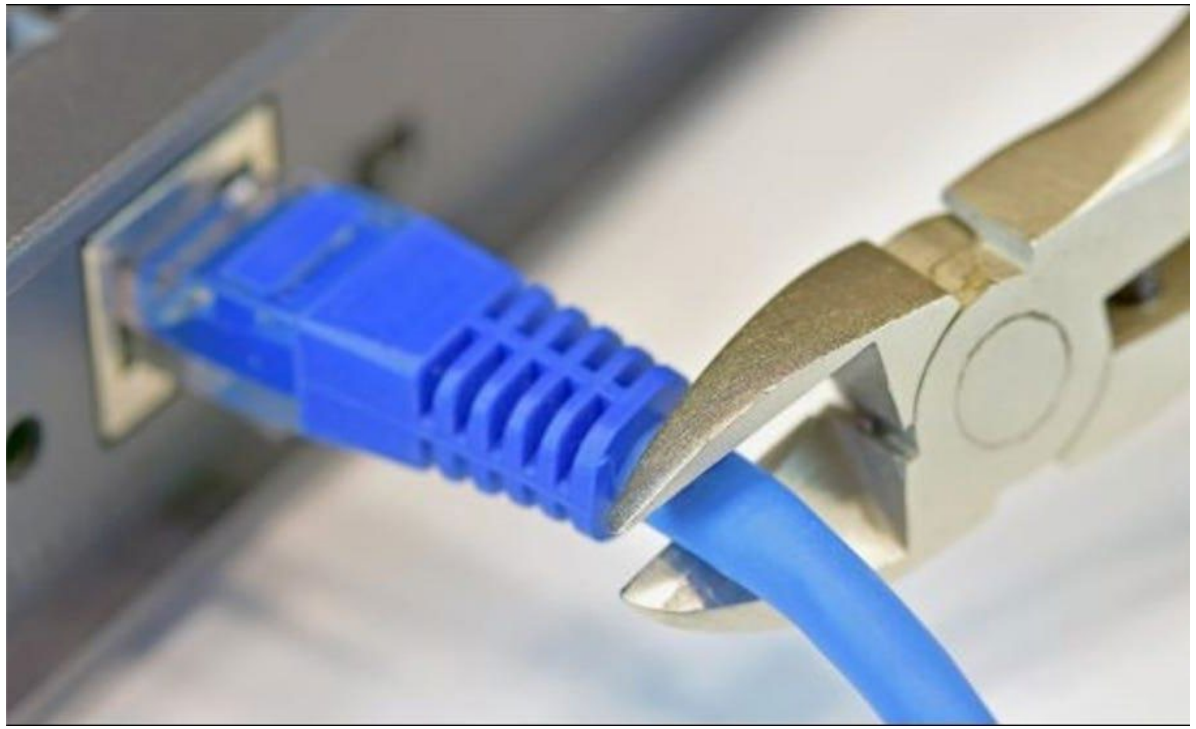
We need creative solutions for funding faculty with the skills and training needed.

To teach the next generation of cyber professionals the skills needed to protect IT and OT operations into the future.

Questions ?

Julie McFadden
Director of Computer Technology

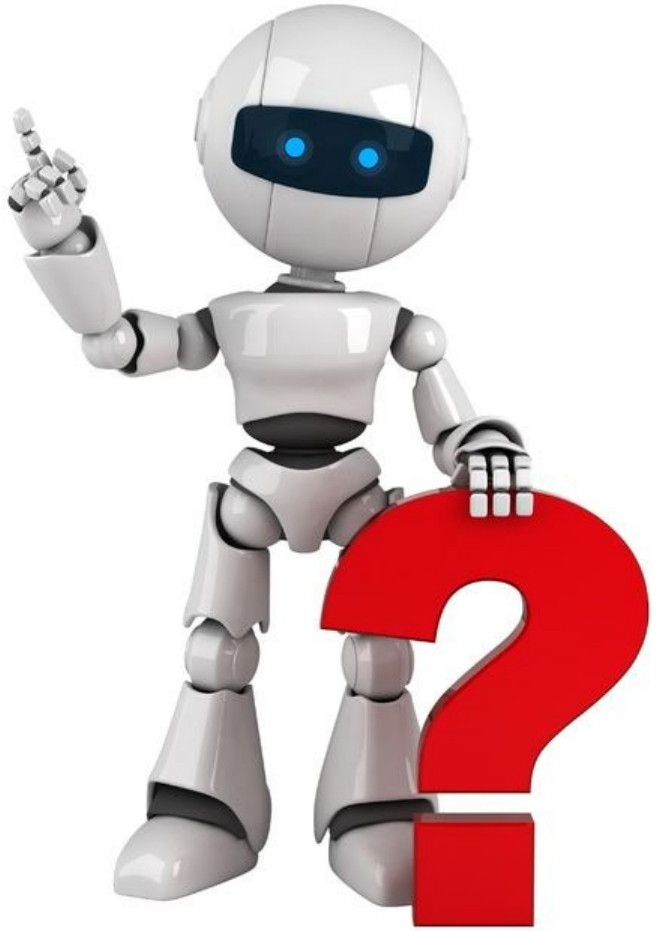
DUNWOODY
COLLEGE OF TECHNOLOGY



Dunwoody OT Cybersecurity

- Hundreds of networked devices.
- Dozens of switches
- Really good at OT!
- Limited Cybersecurity

Questions ?



E.J. Daigle

edaigle@dunwoody.edu

612-381-8172

DUNWOODY
COLLEGE OF TECHNOLOGY