The SANS Institute has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. ICS410: ICS/SCADA Security Essentials provides a set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats. It also helps participants with preparation for the Global Industrial Cyber Security Professional (GICSP) certification exam. This unique vendor-neutral, practitioner-focused industrial control system certification is a collaborative effort between GIAC and representatives from a global industry consortium involving organizations that design, deploy, operate and/or maintain industrial automation and control system infrastructure.

GICSP will assess a base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments. This certification will be leveraged across industries to ensure a minimum set of knowledge and capabilities that IT, engineering, and security professionals should know if they are in a role that could impact the cybersecurity of an ICS environment. Visit www.giac.org for complete certification information.

Prerequisites: A basic understanding of technology, networks, and security; specific understanding of networking and system administration, TCP/IP, networking design/architecture, vulnerability assessment, and risk methodologies.

** Exam voucher not included.

ICS410: ICS/SCADA Security Essentials
February 22 – 26, 2016  |  M – F  |  8:30 am – 4:30 pm  |  3.5 CEUs  |  $4615**

This course will provide you with:
- An understanding of industrial control system components, purposes, deployments, significant drivers, and constraints
- Hands-on lab learning experiences to control system attack surfaces, methods, and tools
- Control system approaches to system and network defense architectures and techniques
- Incident-response skills in a control system environment
- Governance models and resources for industrial cybersecurity professionals

Who should attend:
Individuals who influence the attack surface and are responsible for or support efforts to maintain a secure, safe and reliable Industrial Control System environment. The roles performed by personnel specific to this field can be divided into four domains: IT (includes OT support), IT security (includes OT security), engineering, and corporate, industry, and professional standards.

Course will be held at Wilson Hall 207 located on the UAH campus.

REGISTRATION DEADLINE: FEBRUARY 15, 2016 – REGISTER TODAY!

For more information, visit www.PCS.uah.edu/SANS-ICS410 or call Lane Fabby at 256.824.4430.
Global Industrial Cyber Security Professional (GICSP)

The GICSP exam has 115 questions and a time limit of three hours. Once achieved, the GICSP certification is valid for four years. The GICSP certification focuses on the knowledge of securing critical infrastructure assets. The GICSP bridges together IT, engineering and cybersecurity to achieve security for industrial control systems from design through retirement. This unique vendor-neutral, practitioner-focused industrial control system certification is a collaborative effort between GIAC and representatives from a global industry consortium involving organizations that design, deploy, operate and/or maintain industrial automation and control system infrastructure. GICSP will assess a base level of knowledge and understanding across a diverse set of professionals who engineer or support control systems and share responsibility for the security of these environments. This certification will be leveraged across industries to ensure a minimum set of knowledge and capabilities that IT, engineering, and security professionals should know if they are in a role that could impact the cybersecurity of an ICS environment.

GICSP Certification Objectives:
- ICS architecture
- ICS security assessments
- Industrial control systems
- ICS modules and elements hardening
- Cybersecurity essentials for ICS
- Configuration/change management
- ICS security governance and risk management

For a complete list of GICSP certification objectives, visit www.giac.org

Register on or before February 15th to reserve your seat!

COURSE DAY TOPICS

Day 1: ICS Overview
- History and overview of ICS
- Field and network components
- Communications
- ICS application overview
- Industry models
- ICS drivers and constraints
- Physical security and safety systems

Day 2: ICS Attack Surface
- Overview of attacks
- Attacks on HMIs, control servers, network communications, remote devices

Day 3: Defending ICS Servers and Workstations
- ICS Server/Workstation technologies
- Microsoft Windows based systems
- Unix and Linux based systems

Day 4: Defending ICS Networks and Devices
- Network fundamentals
- IP Concepts and behaviors
- Firewalls and perimeters
- Wireless
- Cryptography for ICS
- Controller and field-device security

Day 5: ICS Governance and Resources
- Information assurance foundations
- Computer security policies
- Contingency and continuity planning
- Risk assessment and auditing
- Password management
- ICS Incident Handling
- Resources

5 Easy Ways to Register

1. ONLINE
   www.PCS.uah.edu

2. PHONE
   256.824.6010 or 800.448.4031
   8:15 am – 5 pm (CST), Monday – Friday

3. FAX
   registration form to 256.824.6760

4. IN PERSON
   UAH, Wilson Hall, Room 103

CONTINUING EDUCATION UNITS
UAH Professional and Continuing Studies (PCS) courses meet requirements for providing Continuing Education Units (CEU).
- One CEU = 10 contact hours of instruction
- One PDH, CLP, CPE, or CMU = one contact hour of instruction
- One CEU = 10 PDH, CLP, or CPE

Successful course completion requires participants to attend 80% of scheduled class meetings (and complete associated exams or projects, if applicable). Participants receive a certificate indicating the number of CEUs earned.

For a complete list of policies, visit www.PCS.uah.edu.

REGISTRATION DEADLINE: FEBRUARY 15, 2016
Register on or before 5:00 pm on Monday, February 15, 2016 to reserve your seat in this course. No exceptions. Phone Lane Fabby at 256.824.4430 for more information.