abhisam

Industrial Cybersecurity Certification Course

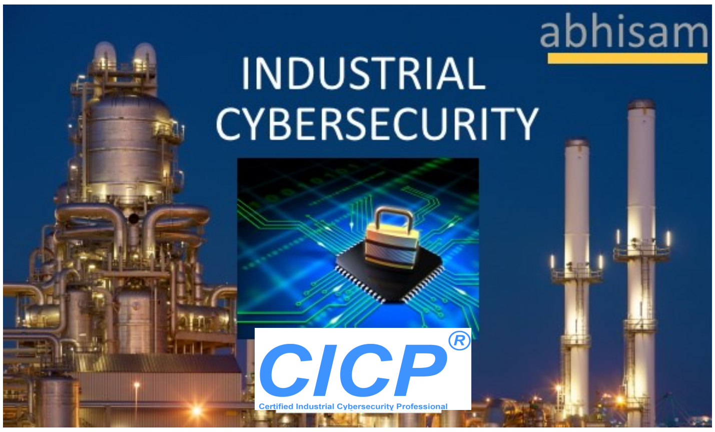
CICP®

Certified Industrial Cybersecurity Professional

The CICP® mark is owned by Abhisam and is a Registered Trademark in multiple countries including the United States.

sales@abhisam.com

Introduction



Industrial Cybersecurity is all about protecting Industrial Automation, Control Systems, Safety Systems (IACS for short) and other OT (Operational Technology) systems against cyber threats.

This Industrial Cybersecurity Course from Abhisam helps engineers, managers and technical professionals in learning how to protect these systems from cyber attacks.

On successfully completing this course, passing the associated exam and successfully submitting the assignments, learners qualify as a **CICP® - Certified Industrial Cybersecurity Professional.**

Why take this course

Every year, there are a large number of attacks on Industrial Control, Automation and Safety Instrumented systems, as well as on other OT systems and the number keeps growing. Many of these systems are legacy systems that were designed many years ago, when today's cyber threats were not present. The consequences of attacks on unsecured Industrial systems and other critical infrastructure related systems, can be very severe. This may result in not just loss of confidential information, but also physical damage to assets, process upsets that may lead to fire, explosion, possible loss of containment and /or injury to humans.

Why take this course from Abhisam

Abhisam is a global leader in technical e-learning and certification for engineers, technical professionals and managers all over the world. Since 2003, Abhisam courses have been taken by thousands of professionals, working for marquee corporations (including Fortune 500 companies) and government authorities, as well as by individuals, consultants and universities/colleges.

In the year 2018, Abhisam introduced this Industrial Cybersecurity course, a complete e-learning course, designed by experts in Industrial Cybersecurity, so that it becomes very easy to learn everything that you need to know about this important subject. The course has animated simulations, videos, interactive exercises and other material that make learning the subject, fun and easy! Since then, the course has been updated several times and is frequently updated so that it remains current.

Compared to courses from other providers, Abhisam courses have better content, but cost much less and can be deployed to even thousands of learners, simultaneously, via the Abhisam Learning Management System, or via your organization's own SCORM or xAPI compliant LMS.

Key Benefits of taking the Abhisam Industrial Cybersecurity Course

- Covers everything that you need to know about ICS security and OT security
- No need to take multiple courses– just this one course covers almost everything related to ICS security.
- Situational videos that make understanding easy.
- Easy to understand text, animations, simulations and graphics.
- Self Assessment Tests that helps you prepare for the final exam.
- Real Life Case Studies and examples.
- Covers all parts & aspects of the IEC 62443 standard.
- Earn the CICP® certification at no additional cost. This is much more cost effective than other certifications.
- Participate in a simulated Case Study –The Industrial Cybersecurity Thriller (Coming Soon)

Enterprise Customer Review

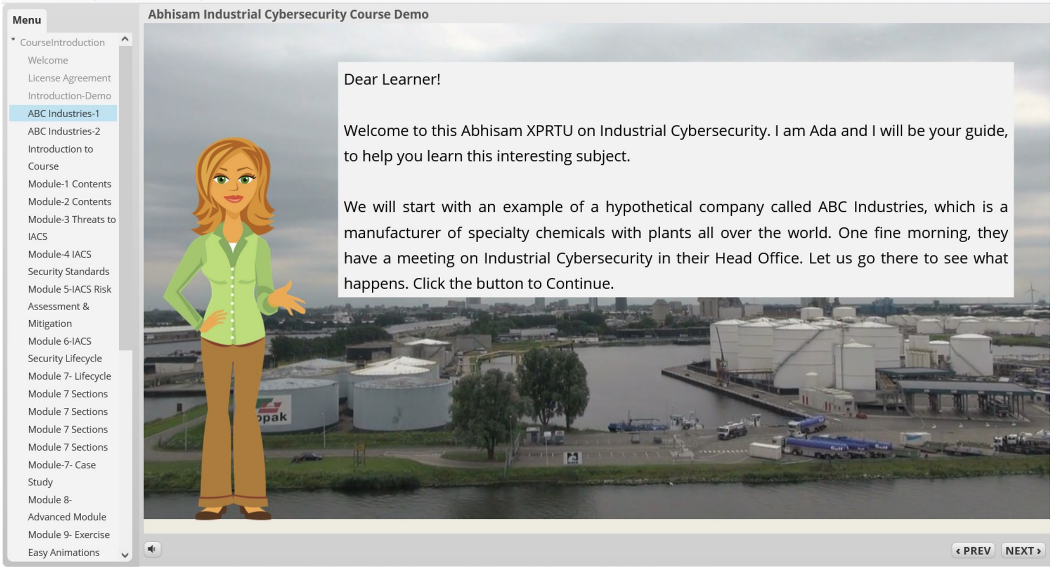
"I am working in one of the world's leading EPC company , engaged in the Cement and Mining industry. We purchased the Abhisam ICS CYBER SECURITY TRAINING & CERTIFICATION e-learning courses. I found this course to be very informative and easy to understand. I and my colleagues in Denmark completed the course successfully and got the certificates and badges. I personally recommend this course to whoever is interested to learn about Industrial Control System Cybersecurity.

I wish success to the Abhisam team for their great work."

D. Anbudurai, FLSmidth

DEMO

To view a demo of the course, please click the picture below. You must be online for this to work. Please allow Autoplay in your browser if it does not load. Note the Standard version of the course is not available for new customers.



Abhisam Industrial Cybersecurity Course Demo

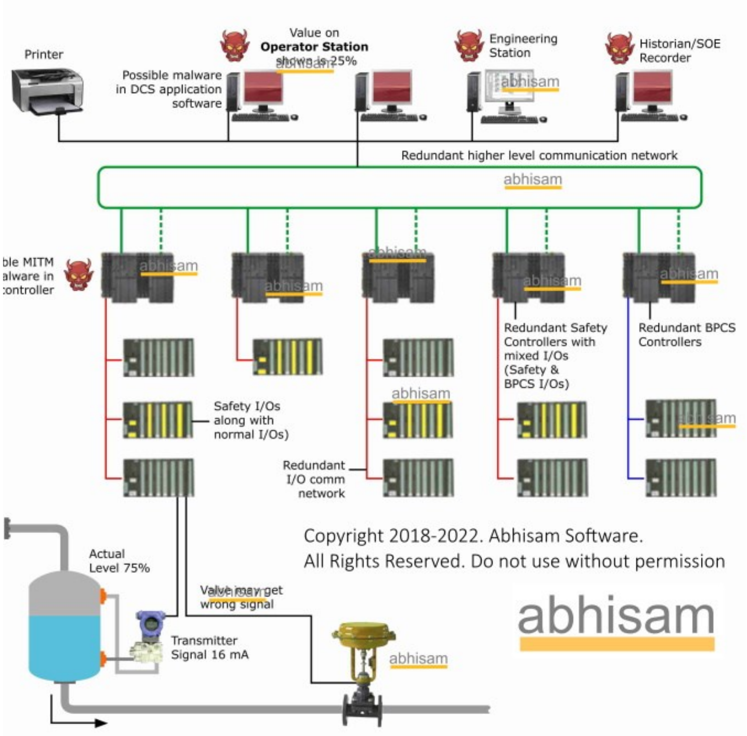
Dear Learner!

Welcome to this Abhisam XPRTU on Industrial Cybersecurity. I am Ada and I will be your guide, to help you learn this interesting subject.

We will start with an example of a hypothetical company called ABC Industries, which is a manufacturer of specialty chemicals with plants all over the world. One fine morning, they have a meeting on Industrial Cybersecurity in their Head Office. Let us go there to see what happens. Click the button to Continue.

Complete Case Study

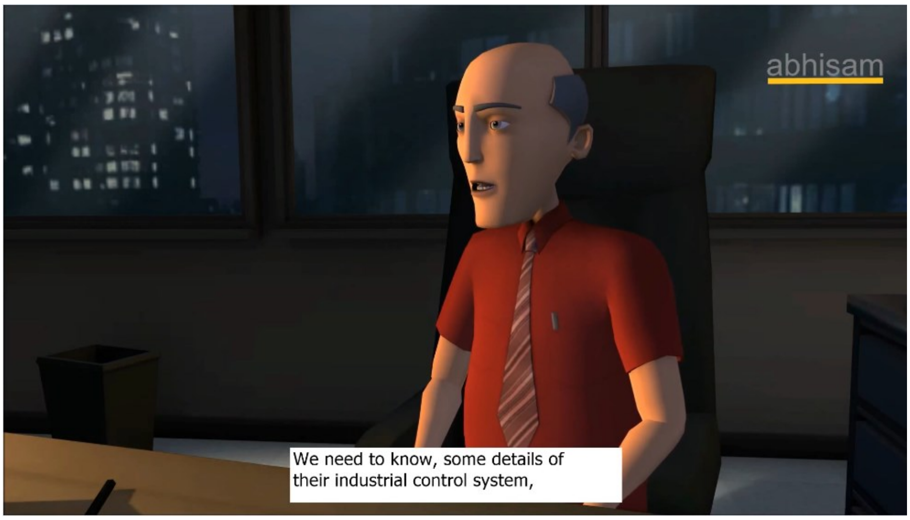
Get a complete Case Study of an attack on a critically important manufacturing facility that resulted in extensive damage to assets.



Representational Image

Abhisam Cybersecurity Thriller (Coming soon)

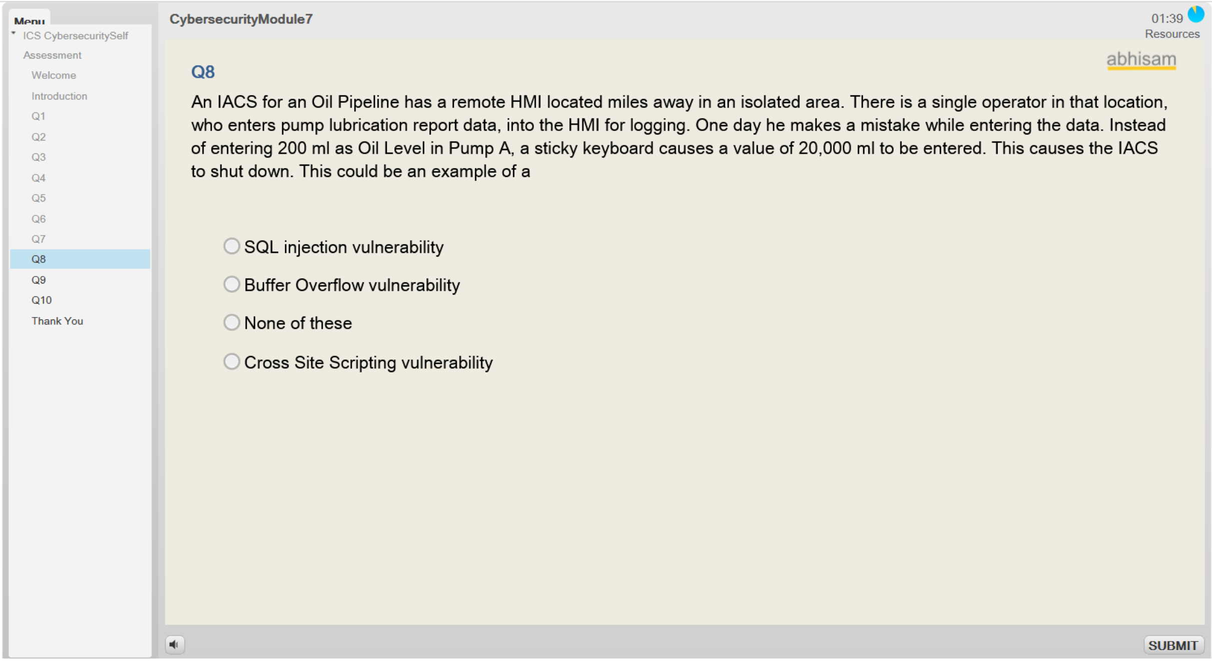
Participate in this simulated real life thriller that deals with attack/defense, of an Industrial Control System at a manufacturing plant. This is a tabletop Red Team/Blue Team exercise that you will enjoy.
You can choose to participate in the Red Team (Attackers) or the Blue Team (Defenders).



We need to know, some details of
their industrial control system,

Self Assessment Test

Know your own understanding of the subject, via the included Self Assessment Test. This also prepares you for the actual Certification Exam. Below is a screenshot of one of the questions from the Self Assessment Test.



Q8

An IACS for an Oil Pipeline has a remote HMI located miles away in an isolated area. There is a single operator in that location, who enters pump lubrication report data, into the HMI for logging. One day he makes a mistake while entering the data. Instead of entering 200 ml as Oil Level in Pump A, a sticky keyboard causes a value of 20,000 ml to be entered. This causes the IACS to shut down. This could be an example of a

○ SQL injection vulnerability

○ Buffer Overflow vulnerability

○ None of these

○ Cross Site Scripting vulnerability

Advanced Modules

Also get several advanced modules that include the MITRE ATT&CK® for ICS matrix model, Honeypots, Shodan alternatives and more. The “Understanding IEC 62443-2-4” module is also included in the Professional version of the course.

COURSE CONTENTS

MODULE 1 - Overview of Industrial Automation & Control Systems (DCS / PLC / SCADA /SIS)

- Introduction to Industrial Automation & Control Systems (IACS)
- IACS Application Areas
- Cyber physical systems
- Evolution of IACS
- Pneumatic Controllers
- Single Loop Controller architecture
- Control Rooms
- Control Room & Field
- Analog Electronic Signals
- Traditional Controls
- Point to Point Architecture
- Direct Digital Control (DDC) to Distributed Control Systems (DCS)
- DCS as a group of controllers
- DCS Connection to field devices
- Fieldbuses
- MODBUS
- Programmable Logic Controllers (PLC)
- PLC HMI
- SCADA
- PLC-SCADA
- Safety Instrumented Systems
- SIS Cybersecurity
- Typical IACS Architecture
- Automation Hierarchy

MODULE 2- Basic Concepts of Cybersecurity

- Cybersecurity Basics
- Cybersecurity Policy
- Authorized Access
- Unauthorized Access
- Brute Force Attacks
- Secure Communication
- Authentication
- Non Repudiation
- Encryption
- Public and Private Keys
- Locking and Unlocking
- Public Key Cryptography-
- Digital Signature
- Defense in Depth
- Privileges
- Role of Malware
- Understanding malware delivery
- Attack Surface
- Threats & Vulnerabilities
- Viruses
- Worms
- Trojans
- Types of Trojans
- Ransomware
- Scareware
- Spyware
- Command & Control
- Firewalls
- Firewall Basic Working
- Classes of Firewalls
- Deep Packet Inspection Firewalls
- Intrusion Detection Systems (IDS)
- Denial of Service
- Distributed Denial of Service (DDoS)
- Telephonic Denial of Service (TDoS)
- Penetration Testing
- Backdoors
- Backdoor Examples
- Demilitarized Zone
- Privilege Escalation Vulnerability
- Network Hardening

Note: The Contents are subject to change without notice as the Course gets updated from time to time in order that it remains aligned with current developments.

MODULE 3 - Threats to IACS

- Introduction
- Threats to IACS
- IACS Threat Severity
- Vulnerability Causes
- Increased Connectivity
- Insecure by design
- Use of COTS
- Shodan
- Skill Levels needed
- Lack of awareness
- Predisposing Conditions
- Four Steps to an Attack
- Vectors
- Phishing
- Spear Phishing
- Social Engineering
- Fake Profiles
- Insecure Connections & Firewalls
- Malicious Websites
- Waterholing
- Fake Updates and Pirated Software
- USB Drives
- Devices and Software with Vulnerabilities
- Buffer Overflow
- SQL Injection
- Advanced Persistent Threats (APT)
- Port Scanning
- Cross Site Scripting
- Packet Sniffing
- Zero Day Exploits
- Exploit Markets
- ICS Attack Categories
- ICS Targeted attacks
- Attack Sequence of Events
- Man in the middle attack
- MITM in ICS
- Denial of Service
- Replay attack
- Spoofing
- Blended Attacks

MODULE 4 - ICS Cybersecurity Standards

Section 1 – Overview

- Overview of standards in ICS security
- ISA 99
- Purdue Model & Architecture
- ISA/ IEC 62443 Overview
- IEC 62443 Organization-1
- IEC 62443 Organization-Updated
- IEC 62443 published parts
- System Under Consideration (SuC)
- IEC 62443-1-1 Overview
- Concept of Zones & Conduits
- Defining Zones & Conduits
- Security Levels (SL)
- Example- IACS Zones & Conduits
- Security Levels & Types
- What do SLs mean?
- IEC 62443-1-5
- Security Profiles

Section 2 – Foundational Requirements of IEC 62443

- Introduction
- Foundational Requirements-1
- Foundational Requirements-2
- FR-IAC
- FR-UC
- FR-SI
- FR-DC
- FR-TRE
- FR-RA

Section 3 – Zone Partitioning Example

- Introduction
- Example Intro- Chlorine Facility
- Determining SLs
- Target SLs
- Achieving the SL

- Final architecture
- Next Steps

Section 4 – IEC 62443-2

- Introduction
- IEC 62443-2-1
- IEC 62443-2-3
- IEC 62443-2-4
- Vendors & System Integrators
- Relationships
- Example– Simple
- Example– Complex

Section 5 – IEC 62443-3

- Introduction
- IEC 62443-3-1
- IEC 62443-3-2
- The IEC 62443-3-2 Process
- IEC 62443-3-2 Process details
- IEC 62443-3-3 Overview
- IEC 62443-3-3 Details
- Security Levels
- Mapping SLs to FRs
- Mapping FRs and REs to SLs
- Self Assessment

Section 6 – IEC 62443-4

- Introduction
- IEC 62443-4-1 and IEC 62443-4-2
- IEC 62443-4-1
- Secure Product Development Lifecycle
- IEC 62443-4-1 and 2-Applicability
- Capability Maturity Model
- SDLC Practices (1-8)
- IEC 62443-4-2
- Technical Security Requirements
- Foundational Requirements revisited
- Component Requirements (CRs)
- CRs and REs
- Mapping CRs and REs to SLs
- Common Component Security Constraints
- CSSC-1 Support of Essential Functions

Section 6 – IEC 62443-4 (Contd)

- CSSC-2 Compensating Countermeasures
- CSSC-3 Principle of Least Privilege
- CSSC-4 Design and support as per SDLC
- Self Assessment

Section 7 – Other Standards & Schemes

- Introduction
- ISA Secure Scheme
- ISO 31000
- ISO 27000
- IEC 61508 Functional Safety
- IEC 61508 Security Clauses
- IEC 61511 Process industries Standard
- IEC 61511– Security Clauses
- Cybersecurity - Safety Instrumented Systems

MODULE 5 – IACS Risk Assessment

- Introduction
- Risk Assessment Case Study
- Risk Assessment & Mitigation, Incident Response
- Non Safety Consequences
- Risk Assessment Process
- Security Vulnerability Analysis
- ICS Security Evaluation
- Initial Risk Assessment
- Threat Assessment
- ICS Vulnerabiility Assessment
- Consequence Analysis
- Example Calculations
- Tolerable Risk
- Modification-Small Site
- Modification-Medium Site
- Modification-Large Site
- Modification-Remote Site
- Seven Steps to be carried out
- Secondary Risk Assessment
- Periodic Assessment
- Cyberattack Mitigation

MODULE 6– IACS Cybersecurity Lifecycle

Section 1 to Section 10

This module has TEN sections that cover the following topics in detail:

1. People, Policies, Procedures and Standards
2. Hazard and Risk Assessment
3. Asset Inventory
4. Training & Competency
5. Secure Architecture, Devices, Configuration, Software
6. Intrusion Detection & Prevention
7. Event Logging and Analysis
8. Incident Response
9. Backup & Restore
10. Patch Management & Testing

MODULE 7 – IACS Cybersecurity Case Study

In this module, study in detail the STUXNET cyber attack

MODULE 8 – Demo of an attack on a PLC

In this module, watch how an industrial PLC is attacked in a few minutes. The attacker can grab control and remotely change any Inputs/Outputs as well as Stop/Start the PLC.

MODULE 9 – Advanced Module 1

- The Cyber Kill Chain Model
- MITRE ATT&CK for ICS Framework
- Honeypots for IACS
- Advanced SHODAN techniques and other methods using other tools

MODULE 10 – Self Assessment Test

The Self-Assessment test gives you an idea of how well you have understood the subject. You can also take this as a Mock Exam before you take the CICP exam.

MODULE 11 – Advanced Module 2

Advanced Module-2 is only in the Professional and Enterprise versions. It includes the following parts.

- Understanding and Complying with IEC 62443-2-4 (also available as a separate course)
- Supply Chain Cybersecurity for IACS & SBOMs

MODULE 12 – Abhisam Cybersecurity Thriller (Coming Soon)

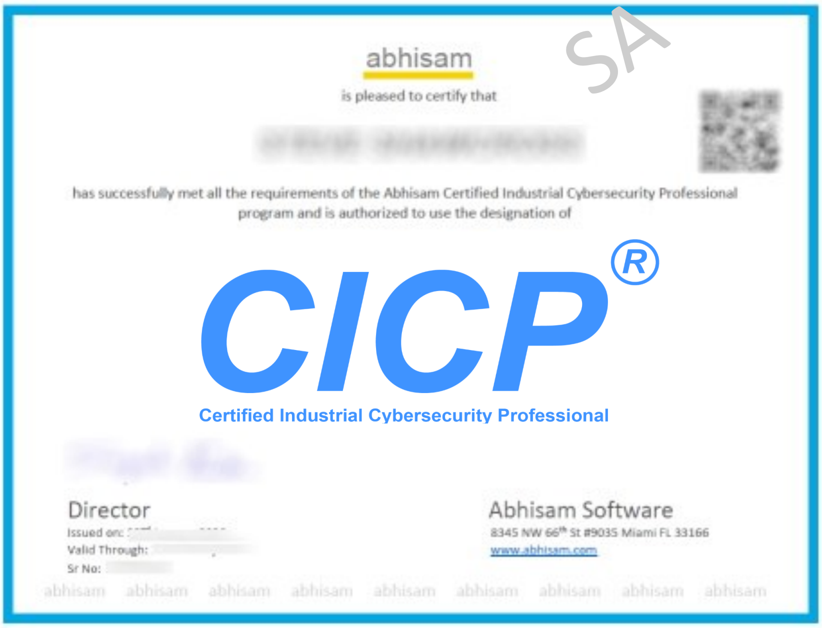
Participate in this tabletop Red Team/Blue Team exercise to have a deeper understanding of Industrial Cybersecurity.

CICP® EXAM

After completing the modules, you are eligible to take the CICP® Exam. This is an online exam that you can take anytime after course completion (but within 1 year of enrolment).

The exam will have questions drawn from a large database of questions, based on what you learned in the course.

On passing, you earn the title of CICP® – Certified Industrial Cybersecurity Professional.



abhisam

is pleased to certify that

[redacted]

has successfully met all the requirements of the Abhisam Certified Industrial Cybersecurity Professional program and is authorized to use the designation of

CICP®

Certified Industrial Cybersecurity Professional

Director

Issued on: [redacted]

Valid Through: [redacted]

Sr No: [redacted]

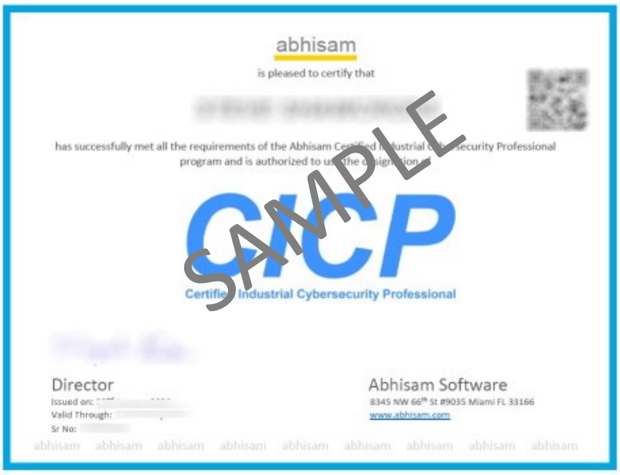
Abhisam Software

8345 NW 66th St #9035 Miami FL 33166

www.abhisam.com

Get Certified. Earn Electronic Badges too! Display and Share them online.

After you complete the course and pass the exam, you earn a title of **CICP – Certified Industrial Cybersecurity Professional** with a certificate and an electronic badge, issued via Badgr, that you can add to your LinkedIn profile or other places online. This enables you to show your credentials to bosses, clients or potential customers.



abhisam

is pleased to certify that

[redacted]

has successfully met all the requirements of the Abhisam Certified Industrial Cybersecurity Professional program and is authorized to use the designation of

CICP

Certified Industrial Cybersecurity Professional

SAMPLE

[redacted]

Director

Issued on: [redacted]

Valid Through: [redacted]

Sr No: [redacted]

Abhisam Software

8345 NW 66th St #9035 Miami FL 33166

www.abhisam.com

abhisam abhisam abhisam abhisam abhisam abhisam abhisam abhisam abhisam

mozilla OpenBadges Linked in

Your badge and certification information will then appear under the Certifications section of your LinkedIn profile. The title of the achievement, will link to a verification page where additional information is available, including a longer description, evidence, the badge image and criteria for the accomplishment, details about the issuer, and validation of the achievement's authenticity. Thus your skill is easily verifiable by any third parties including clients, customers, employers and peers.

This is a great way to enhance your public profile regarding your skills and is available for all learners. You can also add your Badge to the LinkedIn feed, where you can announce your achievement to your LinkedIn connections.

Display your achievement badge to Facebook

Similarly you can post to Facebook and other social media platforms easily via Badgr.

Conformance to global standards- Mozilla Open Badge framework

Furthermore, Abhisam badges conform to the Mozilla Open Badge framework and can be easily added to your Mozilla back pack.

Note: The Badgr, Linkedin, Facebook and Mozilla OpenBadges logos belong to the respective organizations

VERSIONS

The Industrial Cybersecurity e-learning course is available in versions as outlined below.

Standard Version

The Standard version has all the modules, including the Advanced Module-1 and comes with 1 year online access to the course, accessible from any smart device. Currently this is available only as a part of GOLD Membership. *This version is now being discontinued and only the Professional version will be available in future.*

Professional Version

The Professional version has everything in the Standard version plus access to the course for 3 years, and also includes the Advanced Module-2 that includes the "Understanding IEC 62443-2-4" module and the Supply Chain Cybersecurity module.

Enterprise Version

This version is for organizations with multiple numbers of learners (10 or more). It Includes everything in the Professional version and an optional Dashboard for Managers. It can also be licensed as a SCORM/xAPI version (optional at extra price) for use in your own Enterprise LMS. When you order 10 or more licenses you can opt for the Enterprise version.

Benefits	Standard*	Professional	Enterprise
All Modules except Advanced Module-2	✓	✓	✓
Understanding IEC 62443-2-4 module	✗	✓	✓
Other modules in Advanced Module –2 (Supply Chain Cybersecurity)	✗	✓	✓
Red Team/Blue Team Tabletop Exercise (Coming Soon)	✗	✓	✓
CICP Exam & Certification	✓	✓	✓
Access Devices	**PC, Mac, Tablet or Smartphone via any browser that supports HTML5**	**PC, Mac, Tablet or Smartphone via any browser that supports HTML5**	**PC, Mac, Tablet or Smartphone via any browser that supports HTML5**
Access Period	**One Year**	**Three Years**	**Three Years**
Ideal for	*** Not available to new customers**	**Individuals**	**Organizations**

Industrial Cybersecurity Certification Course

How to order

This course & certification can be ordered in a variety of ways, by online payment via credit or debit card, via wire transfer payments, physical checks, Paypal or several other options.

Our online orders are processed via FastSpring, who are our authorized resellers and act as the merchant of record.

Local taxes are extra and will be applicable depending on the ordering location.

Contact us for more information

sales@abhisam.com

US

Abhisam Software
8345 NW 66th St #9035
Miami FL 33166-2626
USA
Phone: +1 (305) 407 2679
Email: sales@abhisam.com

INDIA

Abhisam Software Pvt Ltd
Pokhran Road #2
Thane
India
Phone: +91 7208060349

www.abhisam.com

The course structure, illustrations, examples, animations, videos and all content is owned exclusively by Abhisam and is only licensed to learners and/or the buyer as a course. No Intellectual property is being sold or transferred to buyer/learner. The examples, case studies and recommendations in the course are given for educational and training purposes only. You are responsible for proper use of the course material when applying to your own situations. No safety, financial or legal advice is being given by Abhisam. The Abhisam name, logo and the CICP marks are owned by Abhisam and cannot be used without express permission.