wurldtech
A GE Company

Online Industrial Security Training Program Datasheet

BUSINESS CHALLENGE

Effective cyber security for operational environments requires common understanding of best practices, awareness of emerging threats and attention to existing vulnerabilities.

SOLUTION

Wurldtech's Online Industrial Security Training Program offers flexible, web-based learning that improves awareness, establishes common understanding and helps to harden the attack surface.

BENEFITS

- Enables fundamental cyber security awareness for both IT and OT professionals
- Flexible, web-based training to accommodate busy schedules
- Improves cross-function collaboration with common understanding

Online Industrial Security Training Program

Unique needs require different approaches

Cyber threats to operational environments are on the rise, but the unique nature of those environments requires different approaches to secure them. Many organizations are finding that existing IT security controls are inadequate to address OT security, but lack the understanding necessary to adapt their efforts to protect critical infrastructure. To catch up to the rapidly expanding threat landscape, companies recognize a need for new skills, and are seeking better awareness and OT-specific training for both operators of assets and IT security professionals.

Wurldtech offers a full schedule of self-paced, online courses that provide necessary knowledge, without requiring time away from the operation. The courses are designed with both operators and IT security professionals in mind, with a focus on actionable learning, not just theory.

Challenge

Cyber risk is growing for industrial operations. New threat actors, inherent vulnerabilities and lagging technical controls present significant challenges for the protection of critical assets. Many organizations recognize that effective cyber defense requires collaboration between IT security and asset operators, but a lack of common awareness leads to communication challenges and frustration on both sides.

Addressing the skills gap requires training, but taking time away from vital functions is often not possible. Industrial companies are seeking flexible solutions that provide the necessary understanding but do not disrupt operations.

Solution

Wurldtech's Industrial Security Training Program is a set of web-based courses that offer flexible, as-needed training that accommodates busy schedules. This comprehensive training curriculum is divided into three training series:

- **Industrial Security Introductory Training**
- **Industrial Security Intermediate Training**
- **Industrial Security Advanced Training**

These courses incorporate the expertise and experience of our recognized OT industry experts to improve security understanding. The course content is focused on providing actionable insight, not just theory. Students will gain knowledge about OT environments, cyber risk and best practices for protection.

The courses are self-paced, allowing maximum flexibility for completion, and include embedded knowledge tests to ensure understanding.

Course Descriptions

Industrial Security Introductory Training Series

This series provides an introduction to the concepts of cyber security and their application in the Industrial Controls domain.

FEATURES	
Course 1: Introduction to Cyber Security	The course lays the foundation for the rest of the series. It describes the basic functions and goals of cyber security services and mechanisms.
Course 2: Overview of the Computer Network	The course provides an overview of how data flows through a basic computer network and how network components and protocols ensure the safe and secure communication of data through a network.
Course 3: Cyber Security and the Industrial Network	In this part of the series, participants will be introduced to the unique aspects of industrial computer networks and gain an initial perspective of the challenges in cyber security that surround these complex environments.
Course 4: Introduction to Network Models and Protocols	Participants will be review how network models work using the TCP/IP model and protocols as an example. Throughout the course participants will identify how protocols support cyber security goals.
Course 5: Common Network Protocols and Security	This review of common protocols used in industrial control networks will help the cyber security professional identify potential gaps and security concerns in a network. It will also identify insecure protocols commonly present in a network.

Industrial Security Intermediate Series

FEATURES	
Course 6: Cryptography Basics	The course describes typical network scenarios and network security services and mechanisms. Course participants will review the process of creation and implementation of cryptography and explore known cryptography weak points.
Course 7: Attacking and Protecting the Network	The course begins with an overview common attacks on cryptography. Then it moves on to cover commonly used secure protocols and the cryptography strategies these protocols use to protect network communications.
Course 8: Wireless Networks and the (IACS)	As wireless networks increase in popularity, thanks to increased reliability and decrease in cost, this course will make participants aware of common wireless sensor networks and their corresponding security features.
Course 9: The Wireless LAN and WAN	Continuing the overview of wireless networks, this course expands to include information about the Local Area Network and the Wide Area Network, their strengths and their vulnerabilities.
Course 10: State of the Industry in Cyber Security	This review covers current efforts by government and industry leaders in the field of cyber security as well as important developments and standards in specific regions and industries.
Course 11: ICS Standards	The course offers a closer look at specific industry standards created for the ICS domain. The participants will gain knowledge on the strengths and weaknesses of industry standards and become aware of additional attack vectors used by threat sources to circumvent today's security efforts.

Industrial Security Advanced Series

FEATURES

Course 12: Uncovering Cyber Security Vulnerabilities	Participants will see an overview of strategies used by expert cyber security professionals to investigate, identify, and classify vulnerabilities in an industrial network.
Course 13: The Cyber Security Risk Assessment	The course shows participants how to conduct a risk evaluation and address the results of their findings using risk actions appropriate to the situation. Participants will also have the opportunity to see the impact realized ICS threats have in real-life scenarios.
Course 14: ICS Vulnerabilities	This course provides an overview of known vulnerabilities in network architectures as well as host systems, embedded systems and network systems.
Course 15: Managing and Tracking Vulnerabilities	This course provides an overview of effective strategies to manage and track vulnerabilities.
Course 16: Security Controls Overview	Participants will be introduced to security controls and review some examples of common security controls used to increase overall security posture and reduce risk. The course will help cyber security professionals lay a foundation for ICS security.
Course 17: Intermediate and Advanced Security Controls	The course presents a series of intermediate and advanced resources for cyber security professionals. While the controls reviewed here are not meant to be an all-encompassing solution for ICS security, they provide a thorough representation of the most common intermediate and advanced control strategies available today.

We also offer in-person training sessions for more hands-on instruction, and can even custom design training programs specific to your needs and program requirements.

NEXT STEPS

For more information or to schedule training, please contact Wurldtech sales:
Toll free: 1 877 369 6674
Email: sales@wurldtech.com
or visit **wurldtech.com**