ICS Risks Are Unique.

Are your employees trained to deal with them?

Empower a secure workforce with SANS Security Awareness.

With security threats to critical infrastructure and industrial control systems (ICS) on the rise, nearly half of ICS networks have faced some kind of cyberattack. It comes as no surprise that seven in 10 companies operating in these environments have concerns about when and how the next attack will take place. With a ICS cybersecurity expertise in short supply, the onus on front-line employee behavior is increasing.

At SANS Security Awareness, we know that ICS working environments are very different from their corporate counterparts – which means so, too, are their security risks. That's why we've designed a unique computer-based training solution to help employees who support, interact with, or operate within ICS environments effectively recognize and respond to cybersecurity threats, reducing the risks of data loss, system breakdowns and physical damage.

One-of-a-Kind Training Built Exclusively for ICS

Backed by SANS, the largest and most trusted source for information security training in the world, SANS Security Awareness ICS Training provides relevant, fully SCORM-compliant learning modules that don't just meet ICS compliance requirements – they develop cyber-resilient workforces by effectively managing human risk.

SANS Security Awareness ICS Training delivers:

Unmatched Expertise

All training is developed by ICS cybersecurity experts who are actively working in the industry. With a day-to-day pulse on ICS-specific cybersecurity threats, our professionals ensure training is fresh, relevant and addresses the latest challenges.

Strategic Learning Approach

Teaching people about ICS attacks, defenses and best practices is not enough – they must know how to bring it all into play. That's why we apply and constantly assess adult learning science principles when designing our learning modules, ensuring curricula is pertinent, engaging, and effective.

Best-in-Breed Content

For training to be impactful, it must be relevant and engaging without overwhelming your learners. Our training illustrates real-world ICS working situations and is presented in compact modules to reduce learner fatigue. All content is developed in-house, maintaining the consistent, high-quality production value associated with SANS.

Create a More Secure ICS Environment with SANS Security Awareness.

From plant managers to operations engineers to vice presidents of operations, each individual in the ICS hierarchy has an important role in protecting the infrastructure of major industries. Yet many of these individuals receive training better suited for the corporate environment or, worse yet, no security training at all.

SANS Security Awareness ICS Training keeps the unique needs of ICS industries in mind, equipping anyone who works within ICS environments with the information and tools necessary to protect and defend all types of control systems, including Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS) and other small systems, such as Programmable Logic Controllers (PLCs).

SANS Security Awareness ICS Training Modules

Our 12 computer-based ICS learning modules are fully SCORM compliant and can be deployed on an existing learning management system, or on the SANS-hosted learning platform powered by SAP Litmos. Each module builds upon the last to provide a progressive and engaging learning path.

1. **ICS Introduction:** A brief history of ICS, regulation and why ICS-focused security behavior training is critical.
2. **ICS Overview:** A breakdown of ICS components, industries and support personnel roles and responsibilities.
3. **ICS Drivers and Constraints:** A deep dive into the principal cybersecurity drivers and constraints that impact how a control system needs to be engineered, managed and supported.
4. **ICS Overview of Attacks:** A review of ICS Threat Actors and examples of ICS-based attacks and trends.
5. **ICS Attack Surfaces:** An analysis of specific attack approaches that target various layers of the ICS system.
6. **ICS Server Security:** An examination of concepts specific to defending ICS environments at the server layer.
7. **ICS Network Security:** An overview of concepts specific to defending ICS environments at the network layer.
8. **ICS System Maintenance:** An audit of ICS system maintenance tasks like patching, backups, change management, monitoring and logging.
9. **ICS Information Assurance:** An in-depth synopsis of ICS-focused information assurance program concepts, like risk management, account management, data classification and defense.
10. **ICS Incidence Handling:** A review of critical ICS incident response topics for all individuals that interact with ICS environments.
11. **ICS Attack Scenario:** A detailed walkthrough of a cyberattack against a fictional organization from the unique perspective of the attacker.
12. **ICS Ukraine Attack:** A real-world case study illustrating how to limit the effect of multiple individual attacks that are linked within a targeted environment.

Cybersecurity risk is a people problem.
Empower your people to be its solution.

www.sans.org/security-awareness-training

SANS SECURITY AWARENESS