

ICS Risks Are Unique

Are your employees trained to deal with them?



Security Awareness is Foundational to ICS Defense

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 ICS cybersecurity expertise in short supply, the onus on front-line employee behavior is increasing.

Role-Based Training Built Exclusively for ICS

At SANS, we know that ICS working environments are very different from their corporate, IT counterparts – which means so, too, are their security risks. That's why we've designed a unique, role-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.

SANS ICS Cybersecurity Awareness Training delivers:

- **Unmatched Expertise**

This all-new training content is authored and hosted by Tim Conway and Dean Parsons, who are both SANS instructors and experts in the field of ICS cybersecurity. Bringing real-world insights into ICS-specific cyber threats, the two have created unique training material that is both current and highly relevant.

- **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.

- **Targeted, role-focused learning**

Organized into easily digestible minutes-long modules that showcase authentic, real-world ICS scenarios, this role-based training series is designed to offer valuable lessons for all employees, not just ICS engineers. Ensuring that your entire organization gains a understanding of critical ICS cybersecurity issues as they relate to each employee's responsibilities.

Create a More Secure ICS Environment with SANS Workforce Security & Risk Training

From plant managers to operations engineers to vice presidents of operations, everyone 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 ICS Role-Based Training Modules

Modules in this course have been targeted towards **Administrative End User (E)**, **ICS Practitioner (P)**, and **Senior Leadership (L)** roles as follows:

- ICS Personal Introduction: Tim Conway (E,P,L)
- ICS Personal Introduction: Dean Parsons (E,P,L)
- ICS Introduction (E, P, L)
- ICS Overview (E, P, L)
- ICS Tabletops for Leadership (L, P)
- ICS Malware, Cyber to Physical Attacks (P)
- The Five ICS Cybersecurity Critical Controls (P, L)
- Cloud Services for ICS & OT (P)
- ICS Penetration Testing Considerations (P)
- ICS and AI (E, P, L)
- ICS Drivers and Constraints (P)
- ICS Overview of Attacks (P)
- ICS Attack Surfaces (P)
- ICS Server Security (P)
- ICS Network Security (P)
- ICS System Maintenance (P)
- ICS Information Assurance (P, L)
- ICS Incident Response (P, L)
- ICS Attack Scenario (E, P)
- ICS Ukraine Attack (E, P)
- ICS Phishing (E, P)
- ICS Ransomware (P)
- ICS Awareness and Reporting (E, P)
- ICS Removable Media (E, P)
- ICS Cyber Engineering Oldsmar CIE (E, P, L)
- ICS Transient Cyber Assets (P)
- ICS Operating through a Ransomware Attack (P, L)
- ICS Perimeter Attack (P)
- ICS Supply Chain Summary (P, L)
- ICS Conclusion (E, P, L)

Translated subtitles and text slides are available for all modules in:

1. Arabic
2. Chinese Simplified
3. Dutch
4. English (Australia)
5. English (UK)
6. English (US)
7. French
8. French (Canada)
9. German
10. Italian
11. Japanese
12. Korean
13. Polish
14. Portuguese (Brazil)
15. Spanish (Latin America)
16. Swedish



**Workforce Security
& Risk Training**

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

www.sans.org/workforce