Business challenge

Production systems continue to be increasingly interconnected, further exposing industrial control systems and SCADA systems to network-based cyber incidents.

Solution

Wurldtech's Site Security Assessment helps system operators understand the security posture of their processes, architecture, and technology. The assessment identifies security weaknesses, prioritizes areas of improvement, and aligns security practices to industry standards.

Benefits

- **Optimizes production and system reliability** by identifying, prioritizing, and mitigating risks that impact critical production systems
- **Improves overall security** by identifying weaknesses and mitigation strategies that address individual weaknesses in systems, assets, or data flows
- **Enables compliance efforts** by helping to align with relevant industry standards, regulations, and best practices
- **Provides comprehensive reports** and documentation to assist with regulatory compliance efforts and audits for IEC62443, ISA99, and more

Site Security Assessment

Cyber attacks on critical infrastructure are on the increase, and are a growing concern for system operators. In December 2014, it was revealed that a steel mill in Germany was the victim of a cyber attack, which gave the attackers access to the plant's production network; a blast furnace was prevented from being properly shut down, causing 'massive' damage. Earlier in the year, the U.S. Department of Homeland Security announced it would investigate the possibility that the Havex Trojan had targeted industrial control systems, compromising over 1,000 energy companies across Europe and North America. Attacks such as these severely impact service uptime, data integrity, compliance, and public safety.

It is imperative that companies that rely on computer networks for industrial control system (ICS) operations assess their current security posture, understand potential security risks, and develop effective risk mitigation strategies.

Challenge

ICS networks are increasingly targeted for cyber attack, and system operators are experiencing cyber incidents at an ever-expanding rate. Operators need to understand their current security status and develop a plan to improve their security posture. They also require documentation and assistance to comply with industry regulations such as IEC 62443, ISA99, and other industry standards.

Solution

Wurldtech's Site Security Assessment is a comprehensive evaluation of an operating facility (such as oil refineries, electricity generation facilities, and others) that helps system operators reduce the risk of a network-based cyber attack. It helps them understand the security posture of their processes, architecture, and technology. The assessment also provides findings to equip operators with the ability to identify security weaknesses, prioritize areas of improvement, and align security practices to industry standards.

The Site Security Assessment follows a proven, repeatable methodology specially developed to protect industrial control systems. Several security analysts come onsite to complete the full facility review. This comprehensive assessment enables operators to mitigate immediate risks, while developing an effective long-term strategy to improve their overall security posture.

Features

Each assessment includes:

- **Information gathering:** Request relevant, customer documentation relating to people, architecture, and technology
- **Documentation review:** Analyze documents detailing network configuration, topology, policies, and other relevant aspects unique to each customer
- **Interviews and inspection:** Meet on-site with subject matter experts (SMEs) to gain additional technical and contextual understanding not apparent from documentation reviews alone
- **Technical testing:** Assess and evaluate the cyber security posture of assets on-site based upon Wurldtech and customer agreed rules of engagement
- **Offline data analysis:** Utilize Wurldtech's best practices methodology* to assess customer risks
- **Risk assessment:** Identify sources of vulnerability, determine security posture, identify, prioritize potential risks, and provide roadmap for remediation
- **Findings report:** Share assessment findings, including recommended mitigations based on prioritized risk

**Wurldtech's best practices methodology is based on many industry standards. Some of these standards include: ISA-99/IEC 62443, NIST 800-53, DHS-CSPL, ISO27001:2005*

BENEFITS	
Provides in-depth visibility	Discovers current security posture via a comprehensive report and workbook that maps out the potential risks for each system analyzed
Delivers actionable results	Supports immediate security risk remediation as well as long-term financial planning and resource justification with analysis based on the leading experience in the field
Enhances security	Applies industry best practices methodology to identify key risks and the necessary strategies to improve security posture

DELIVERABLES	
Actionable report	Includes: • Executive summary • Assessment methodology overview • Risk criteria and threat model • Risk assessment • Assessment observations (people, architecture, and technology) • Prioritized recommendations and mitigations • Security roadmap
Asset review workbook	Includes: • Security posture assessment, including all the collected raw data • Detailed analysis of potential cyber security risks for systems, including: system policies, account and password controls, installed security and software, patch versions, configuration settings, network information, and more
Results presentation	Includes: • Overview of the process and the results for management • High-level summary of the full report, including identified weaknesses and recommended mitigations

Wurldtech customers include five of the top six super-major energy companies, and nine of the top 10 automation vendors

The Wurldtech advantage

The assessments are based on international best practices, standards, and Wulrdtech's proprietary methodology. The comprehensive reports include actionable insight covering gaps in security procedures and standards compliance, as well as remediation recommendations to immediately improve security.

Wurldtech's industrial security experts have deep experience in critical infrastructure, including detailed analysis of the most extensive set of devices and systems from all major manufacturers. This includes practical, hands-on experience conducting hundreds of onsite customer security assessments. The security analysts are also key contributors and authors of international standards, including IEC 62443, and hold HUET/BOSIET, RigPass, and TWIC certifications. Wurldtech analysts can conduct assessments anytime, anywhere, including production plants, remote sites, and even oil rigs at sea.

Summary

Wurldtech's Site Security Assessment helps system operators of industrial control systems understand their system security weaknesses, identify and prioritize areas of improvement, and align security polices to industry best practices. Wurldtech site assessments are delivered by experienced industry experts who have completed 200+ assessments to enhance our customers'

security postures and align with industrial security best practices.

COMPARISON OVERVIEW

Service components	Site Security Assessment	Site Security Health Check
Customer Goal	Comprehensive view of security posture	Rapidly gain high-level insight into current operational security posture
Assessment Methodology	Wurldtech Proprietary*	Wurldtech Proprietary*
Security Gap Analysis	In-Depth	Targeted
Architectural Review	✓	(Scaled)
DELIVERABLES		
Findings Report	✓	(Scaled)
Close-out Presentation	✓	
Detailed Asset Review Workbook	✓	
PROCESS		
Information Gathering	✓	✓
Documentation Review	✓	(Scaled)
Interviews & Onsite Inspection	Senior analyst, 2-days on-site	Analyst, 1 day on-site
Technical Testing	✓	
Offline Data Analysis	✓	
Risk Assessment	✓	(Scaled)
Risk Mitigation Recommendations	Prescriptive, detailed strategies	High-level general direction

** International standards-based*

About Wurldtech

Contact

Americas: 1-877-369-6674
sales@wurldtech.com
www.wurldtech.com