KENEXIS·INDUSTRIAL CYBER SECURITY
INDUSTRIAL CONTROL SYSTEM SECURITY, PERFORMANCE, & RELIABILITY SERVICES

The process itself is at stake. Instead of trying to protect data like your personal banking information, industrial control systems manage the operation of machines, processes, and protections them if something malfunctions. Kenexis focuses on the process so we are able to make cyber security a manageable engineering problem.

For instance, if you are running a process like a chemical reactor and it can become unstable in certain scenarios, then we focus on insuring that those scenarios can never be created even if a hacker has complete control and knowledge of the process and control system.

Our OT cybersecurity team is comprised of seasoned industrial control system and IT technology experts with many years of experience. We have a deep bench of control system experts in process control, discrete manufacturing, building automation, and IoT technologies.

Vulnerability Assessments

A vulnerability assessment evaluates the ICS network for security weaknesses primarily. We are looking for known and not so known problems that we all tend to miss sometimes. This type of testing is delicate on industrial control or OT type networks because the devices like a PLC were built to control a process and not run antivirus software and support a bunch of inquiries from cybersecurity tools. Consequently, it takes a very capable team to deeply analyze an industrial network.

Running a common scan with a tool like Nessus, can stop the process or even destroy machines.

Additionally, knowing where to gather traffic in an industrial control network can be challenging. For instance, in an IT network most traffic is from your desktop to a server or the Internet. Not so in an industrial network. You can have machines talking to machines anywhere in the network based on coordinating motion and product flow. Additionally, communications can look significantly different in an OT environment where UDP protocols are commonly used for timing and control.

We also assume that we should analyze for performance and reliability during a vulnerability assessment. We look for poorly performing devices while analyzing your network architecture, critical assets or processes, network technologies, data flows, process flow diagrams, and previous assessments including risks assessments like HAZOP. A vulnerability assessment will identify vulnerabilities and rank them, remove false positives, and develop prioritized recommendations for remediation. Our final report includes asset inventory, vulnerabilities discovered, severity ratings, recommendations, overview of tools and methods utilized and findings. Once the project is complete, we either destroy or return of all raw data. While a vulnerability assessment is passive, a penetration test is performed with specific written permission to pursue vulnerabilities further into the system to discover the extent of possible exposure or risk.

Risk Assessment, Design, and Migration

Our services include risk assessment of the process, system, or network with design and migration planning for OT networks based on OT vulnerability assessments and critical process analysis using Security Process Hazards Analysis (HAZOP) Review methods.

Whether the vulnerability assessment or Security PHA(HAZOP) Review reveal weaknesses in your design, we will work with you to develop the best design and migration plan to resolve the weaknesses. This might include anything from process safety devices like analog mimics or relief valves, in addition to industrial network design and migration planning.

Our OT Cybersecurity services follow NIST Cybersecurity Framework for appropriate standards in specific areas like the ISA / IEC-62443 standard for the industrial control system environment as well as NERC CIP, NIST SP800, and ISO/IEC 27001 most often. We also follow appropriate standards for the local areas where a standard has been established. Consequently, our network design services focus on providing secure and reliable industrial networks including designs to implement SIEM and other cybersecurity monitoring like Nozomi Networks SCADAGuardian that will serve your business well with better visibility, secure remote connectivity, and less unexplained downtime.

Policy, Procedures, and Training

We will also work with your organization to evaluate and develop a cybersecurity policy, procedures, and training that are appropriate for industrial control systems. We will work with your team to insure agreement across your organization, rollout, and adoption. The established policy, procedures, and training will drive security focused behaviors without compromising performance and connectivity. It will also establish a method for budgeting decisions, and accountability.

Our services start with robust & secure industrial network design and migration planning. Design services are based on solid industrial control system network design with secure communication and reliability as defined in ISA/IEC 62443 and other standards as required by your industry or region of the world. Our design services focus on providing secure and reliable industrial networks including designs to implement SIEM and other cybersecurity monitoring like Nozomi Networks SCADAGuardian that will serve your business well with better visibility, secure remote connectivity, and less unexplained downtime.

Historical Perspective

Industrial Control System protocols are modified Ethernet protocols. Many of those Ethernet protocols were created originally as serial communications before the wide spread use of Ethernet networking. They support proprietary inter-process communications and were originally built to provide reliable and deterministic communications long before routable protocols and Ethernet security was a consideration.

Today, many devices like MTUs, RTUs, PLCs, building automation, access control systems, Internet of Things (IoT), and other controllers including devices like variable speed drives and instrumentation have routable protocols. The devices and the protocols were created long before cybersecurity concerns of today and the devices do not have the capability to protect themselves. In fact, many even lack means of authentication or integrity checking and are vulnerable to potential attack or just mistakes.

Consequently, it is up to all of us to protect industrial purpose made controllers from attack using solid, proven engineering and security techniques.

Industrial Experience

- Oil & Gas, Petrochemical, Chemical, Pharmaceutical
- Power Generation including Nuclear, Gas, Coal, and Hydro
- Manufacturing including Automotive, Metal, Food & Beverage
- Transit including Rail, Shipping, and Terminals
- Government & Municipalities including Military, Research, Water & Wastewater

About Kenexis

Kenexis is an independent engineering consulting firm headquartered in Columbus, Ohio, with offices in Houston, Singapore, and Dubai. Kenexis was established in 2004 and is a privately held. Kenexis clients span the globe in many industries. For more information, go to www.Kenexis.com.