Nexus Controls
a Baker Hughes business

Nexus OTArmor† Professional and Consultancy Services

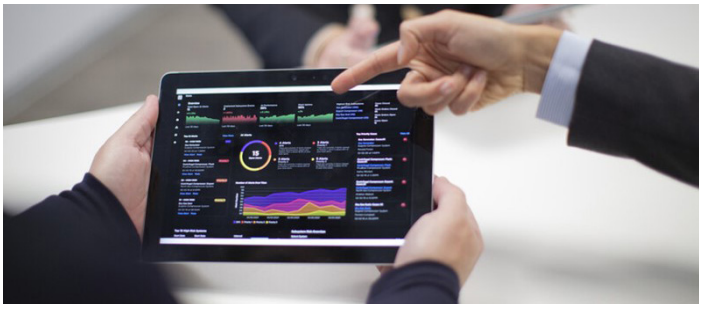
Overview

Organizations greatly benefit by starting with a bench-marking exercise to understand the current state of security readiness. **Nexus Controls offers a control system agnostic cybersecurity risk assessment service** to support compliance with industry standards such as **ISA99/IEC 62443, NEI 08-09, NIST SP800-161, NIS-D** and **NERC-CIP** and will help elevate your cybersecurity awareness and identify potential vulnerabilities. After the assessment is conducted, the final report provided **enables the creation of an actionable road map of prioritized mitigations to improve your security posture.**

Cybersecurity Assessments

Nexus **OTArmor** offers a large variety of security assessment services. Designed so the CEO, CISO, Plant Manager or Compliance Manager can prioritize steps for mitigation and even to help obtain future budgets within a multi-year cybersecurity program.

- Useful for obtaining budget and prioritizing cybersecurity road map
- Understanding current state of security readiness
- Your results versus industry expectations
- Identify weakness early to prevent exploitation
- Delivers prioritized, actionable mitigation steps tailored to your environment



Types of Assessments Offered:

- Vulnerability and risk assessment
- Asset inventory assessment
- Compliance framework assessment (IEC62443, NERC, NEI, ISO27001, NIST, NIS-D)
- CIS top 18 controls
- Highly complex risk assessments or penetration tests
- Product security assessment (IIOT, controller, etc.)
- Hunting as a Service (HaaS)
- Network architecture assessment
- Threat assessment
- Assessment against customer specific framework

Features of a Nexus OTArmor Cybersecurity Assessments

Below is a list of some of the important items that are reviewed during the assessment:

- **Control system application:** Control system or PLC configuration review, network security configuration, control system integration methodologies, and technical support agreement status
- **HMI server hardware configuration:** Hardware warranty status, health, environmental conditions, and physical security
- **HMI operating system configuration:** Access control, account and password review, anti-virus configuration, patch management, logging, backup and recovery, server performance and resource snapshot, installed applications, TCP/IP network integration and architecture, performance, availability, and health monitoring

- **Control system protection:** Password strength, control system integration methodology, TCP/IP network integration architecture, environmental conditions, and physical security
- **TCP/IP network infrastructure review:** Review firewall, router, and switch configuration, firmware updates, and management process, access control and authorization, system performance and availability management, physical security, and environmental conditions
- **Process review:** Change management, IT incident management, patch management, system access authorization, and implementation, lost/forgotten password, key management, and governance documentation

Other Professional and Consultancy Services

Some of the other professional and consultancy services Nexus Controls offers are listed below:

Professional/ Consultancy Service	Description
Cybersecurity Profiling	Current state analysis of organization's cybersecurity maturity level, followed by reporting based on responses from a detailed questionnaire
Industrial Wireless Network Services	Assessment on existing networks, pinholes, unmanaged plant Wi-Fi, weak performance areas, outdated equipment and unauthorized access to plant Wi-Fi
Cybersecurity/Compliance audits	Report on current compliance level to a specific standard or regulation and gap analysis
Incident Response Planning	Definition of roles, processes, communication and constraints. Context based classification of incidents to provide meaningful alerts, root cause analysis, post incidence support, reporting
Incident Response: Onsite services	Resident Engineer services
Forensics & Analysis services	Digital Forensics readiness and engagement
Tabletop exercises (TTX)	Interactive simulation of business's response to a cybersecurity incident
Virtual CISO	Creation, improvement and maintenance of Cybersecurity Management System (QMS)
Prioritized Security Roadmap	Developing a multi-year roadmap based on types of assets and risk prioritization
Advanced security consulting	(Ex. architecture review)
Policy & procedure development	Building the governance model and procedures (network security governance)
Industrial Cybersecurity Training	Training on OT cybersecurity awareness, product installation, maintenance and technical support
Threat Intelligence	Insights on OT application/network vulnerabilities from experts, in-house vulnerability database and external vulnerability announcements
Installation Services	Installation and technical support (onsite and remote) of sensors, appliances and security management console

Note: Some services may not be available in all countries (or locations). Please check with your local Nexus Controls representative on availability of service in your area (or location).

Compliance Standards

Below are some of the common cybersecurity compliance standards that Nexus Controls provides professional and consultancy services for.

IEC 62443 – A published international standard, defining cybersecurity capabilities that Industrial Automation and Control System (IACS) service providers may implement and offer. The standard can help asset owners consistently procure and manage control systems security expertise. IEC 62443-2-4 was developed by IEC technical committee 65, in collaboration with the International Instrumentation Users Association (previously WIB) and ISA 99 committee members. Nexus Controls hardens customer systems using a combination of technical and procedural measures (including patch management) that have been certified to meet IEC 62443-2-4 security standards. These standards specify a comprehensive set of security requirements for the installation and maintenance of IACS.

NEI 08-09 – US nuclear power companies are federally mandated to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks. As part of having a cybersecurity plan, operators are required to address known ICS security vulnerabilities and have solutions in place for operating system, application, and third-party software updates, Host Intrusion Detection (HID), and non-repudiation, among others.

NERC CIP – Many US electric utilities are now federally mandated to comply with NERC CIP requirements that dictate industrial security and remediation technology, including required compliance. To be considered in adapting operations to these regulations is the difficulty of patching industrial controls and the frequent attacks on the equipment. In addition, customers need to address known ICS security vulnerabilities without disrupting operations. Because of these factors, electric utilities require a solution that is easy to implement and provides visibility into the industrial network and compliance.

NIST SP800-161 – NIST is the National Institute of Standards and Technology at the US Department of Commerce. The NIST Cybersecurity Framework helps organizations to better understand, manage, and reduce their cybersecurity risk and protect their networks and data. The NIST framework is based on the following 5 core elements:

BHCS39310 (08/2022)

Baker Hughes

nexuscontrols.com