FINITE STATE

Achieving IEC 62443 Compliance with the Finite State Next Generation Platform

A Detailed Look at Meeting IEC 62443-4-1 and 4-2 Requirements

Introduction

In the world of industrial automation, maintaining compliance with cybersecurity standards is critical to ensuring the safety and reliability of operational technology systems. The IEC 62443 series of standards provide a comprehensive framework for securing industrial automation and control systems (IACS), with specific requirements outlined in IEC 62443-4-1 and 4-2.

The Finite State Next Generation Platform is designed to help industrial automation vendors meet these stringent requirements by offering a comprehensive solution to software supply chain security and enabling transparency throughout the development process. In this data sheet, we will discuss how the Finite State Next Generation Platform addresses the specific requirements of IEC 62443-4-1 and 4-2, including the critical requirement of vulnerability testing for compiled software.

IEC 62443-4-1: Secure Product Development Lifecycle Requirements

The Finite State Next Generation Platform is equipped to address multiple aspects of the IEC 62443-4-1 requirements, including:

Requirement 9.4 SVV-3: Vulnerability Testing: The Finite State Next Generation Platform's binary software composition analysis (SCA) and binary SAST capabilities enable vendors to perform vulnerability testing on all compiled software, including binary executable files and embedded firmware. This analysis detects known vulnerabilities in product software components, linking to vulnerable libraries, security rule violations, and compiler settings that can lead to vulnerabilities, as required by the standard.

SBOM Management: The platform's comprehensive support for SBOM management helps vendors meet requirements for defining and designing secure products throughout the entire product lifecycle.

Component Selection and Evaluation: IEC 62443-4-1 outlines the need to evaluate and select third-party components based on their security properties. SBOMs help organizations identify the origin, version, and security status of components, making it easier to select secure and well-maintained components for use in their products.

AppSec Tools Integration: The platform's ability to integrate with over 120 AppSec tools enables vendors to adhere to secure coding practices as required by the standard and gain unified visibility into those practices across their portfolio.

Incident Response Workflows: The Finite State Next Generation Platform's incident response workflows facilitate efficient maintenance procedures and help vendors meet the requirements for handling security incidents in a timely and effective manner.

IEC 62443-4-2: Technical Security Requirements for IACS Components

The Finite State Next Generation Platform also addresses various requirements in IEC 62443-4-2:

SAST: The platform's static application security testing (SAST) capabilities enable the static analysis of compiled binaries, ensuring compliance with the standard's requirements for identifying and mitigating vulnerabilities.

Binary SCA: The platform's binary software composition analysis (binary SCA) capabilities help vendors meet the standard's requirements for analyzing third-party components and identifying any potential vulnerabilities.

0-day Vulnerability Detection: The Finite State Next Generation Platform can detect 0-day vulnerabilities resulting from coding errors in 1st and 3rd-party software, operating system misconfigurations, and insecure services, ensuring that vendors can proactively identify and address potential security issues.

Patch Management: IEC 62443-4-2 recommends timely patching of security vulnerabilities in software components. SBOMs enable organizations to track the patch status of components, ensuring that they stay current with security updates and comply with the standard.

Reporting & Documentation: The platform's robust reporting and documentation capabilities enable vendors to demonstrate compliance with the IEC 62443-4-2 standard and provide the necessary evidence to support their claims.

Conclusion

The Finite State Next Generation Platform offers a comprehensive solution to help industrial automation vendors meet the challenging requirements of IEC 62443-4-1 and 4-2.

By using SBOMs as part of their development processes, organizations can enhance their ability to comply with IEC 62443-4-1 and IEC 62443-4-2, ensuring that their industrial automation and control systems are secure and resilient. SBOMs can serve as evidence that an organization is following secure development practices outlined in IEC 62443-4-1 and addressing the technical security requirements of IEC 62443-4-2. Also, during an audit or assessment, SBOMs can demonstrate that organizations have a comprehensive understanding of their software components and their security posture.

By providing capabilities for vulnerability testing, SBOM management, AppSec tool integration, and incident response workflows, the Finite State Next Generation Platform enables vendors to address the specific requirements of the standard and ensure the security of their industrial automation and control systems.

With the ability to work with compiled software binaries and provide transparency throughout the development process, the Finite State Next Generation Platform is a valuable tool for vendors looking to maintain compliance with IEC 62443 and enhance the security of their products.

© 2023 Finite State, Inc.