RUNSAFE SECURITY

RunSafe Identify generates Software Bill of Materials (SBOMs) for embedded systems, identifies vulnerabilities present in software, and quantifies available risk reductions for the identified vulnerabilities. By offering insights into software components, vulnerabilities, and effective mitigation strategies, RunSafe empowers organizations to enhance the resilience of their software against evolving cyber threats.

THE PROBLEM

Organizations are largely unaware of the software in their supply chain and lack visibility into the vulnerabilities coming in through that supply chain. This is especially true in C/C++ applications, where there has not been an efficient way to generate accurate SBOMs. Binary-based solutions miss components or guess components that are not actually present. Source-based solutions do not have all the information to statically determine library versions used when the software is built.

OUR SOLUTION

RunSafe Identify is a comprehensive solution designed to enhance the security of embedded systems. It focuses on three critical areas: build-time SBOM (Software Bill of Materials) generation, vulnerability identification and quantification, and identification of available remediations.

BENEFITS

- **Enhanced Security Posture:** By generating SBOMs, identifying vulnerabilities, and quantifying ways to reduce the attack surface, RunSafe provides a robust security framework for embedded systems.
- **Regulatory Compliance:** RunSafe simplifies the compliance process by ensuring adherence to industry standards and regulatory requirements.
- **Operational Efficiency:** RunSafe automates the identification and management of security risks, allowing organizations to focus on innovation and development without compromising security.

RUNSAFE SECURITY

SBOM GENERATION

RunSafe Identify generates detailed Software Bills of Materials (SBOMs) for embedded systems at software build time. An SBOM is a formal record containing the details and supply chain relationships of various components used in building software. This transparency is crucial for identifying and managing potential risks associated with third-party components, ensuring compliance with regulatory standards, and maintaining a secure software supply chain.

IDENTIFYING AND QUANTIFYING VULNERABILITIES

RunSafe's solution includes advanced tools for assessing vulnerabilities within embedded systems. By identifying weaknesses in libraries, components, and packages, RunSafe enables organizations to understand their security posture better. This proactive approach helps prevent potential exploits by addressing vulnerabilities before they can be targeted by attackers.

QUANTIFYING RISK REDUCTION

RunSafe focuses on minimizing the attack surface of embedded systems. This involves reducing the number of potential entry points for attackers. RunSafe Identify quantifies your risk reductions, enabling organizations to prioritize their security efforts and measure the effectiveness of their security strategies. This process not only enhances overall security but also helps in demonstrating compliance and governance to stakeholders.

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security proactively protects embedded software for both commercial and defense deployments across critical infrastructure with comprehensive risk identification, protection, and monitoring, ensuring robust, continuous security without affecting performance. Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace, defense, energy, industrial, and national security verticals. Learn more at: **RunSafeSecurity.com.**