Reduce Exploit Risk in Industrial Control Software

Identify vulnerable components and strengthen protection in embedded applications.

RUNSAFE SECURITY

Documentation Category	Requirements / Example Content	RunSafe	RunSafe Capability/Notes
Secure Development Lifecycle Governance Establish governance for secure product development	Define secure development lifecycle policies and procedures		Subject to RunSafe customers' practices
	Define security roles and responsibilities within development teams		Subject to RunSafe customers' practices
	Define cybersecurity requirements for industrial software products		Subject to RunSafe customers' practices
Threat Modeling and Secure Design Identify potential attack paths and incorporate mitigations during design	Conduct threat modeling for industrial software components	✓	Risk Reduction Analysis identifies memory corruption vulnerabilities and exploitability, informing potential threats and attack feasibility
	Identify potential exploit paths within software architecture	✓	RunSafe automates SBOM generation at build time with a full dependency tree, analyzing software to verify that no known vulnerabities are included in components.
	Design security controls to mitigate identified threats	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon). RunSafe Protect makes vulnerability non-exploitable if a patch is not readily available.
Software Component Visibility and Vulnerability Assessment Maintain visibility into software components and vulnerability exposure	Maintain inventory of software components and dependencies	✓	RunSafe generates an SBOM at build time that includes a full dependency tree of all software components, including third-party libraries.
	Generate and maintain SBOMs for industrial applications	✓	RunSafe automates SBOM generation at build time.
	Identify software components affected by newly discovered vulnerabilities	✓	Risk Reduction Analysis Tool shows residual risk to determine urgency to remediate (patch now or soon).
Component Security Capabilities Ensure industrial software components include security protections	Protect compiled applications from memory exploitation	✓	RunSafe Protect makes vulnerabilities non-exploitable by randomizing memory layouts of executables at runtime to prevent memory exploitation.
	Protect application execution integrity	✓	RunSafe Protect hardens binaries, randomizing the location of software functions in memory each time the application runs
	Implement runtime protections for industrial software components	✓	RunSafe Protect relocates software functions in memory each time an application runs, providing runtime protection against memory-based exploits
Vulnerability Response and Patch Management Manage vulnerability remediation and software updates	Establish vulnerability disclosure and response processes		Subject to RunSafe customers' practices
	Assess risk associated with discovered vulnerabilities	✓	Risk Reduction Analysis tool analyzes exposure to CVEs and potential zero days; and determines if a vuln is exploitable
	Develop patches and provide secure software updates	✓	RunSafe Protect makes vulnerabilities non-exploitable until patches are released. Patch development are subject to RunSafe customers' practices.