niagara
marketplace

Security Self-Assessment Q & A

Self-assessment is to provide potential customers with some peace of mind about the safety of software they purchase. Tridium does not perform any verification of answers to this questionnaire, and the issuance of a self-assessment security badge is based solely on the answers to these questions. Customers who would like additional assurances about the safety of a listing are encouraged to take additional steps to ensure safety.

Q. Do you document and perform quality and cybersecurity reviews and testing, including vulnerability scanning covering static, dynamic, and secure code testing using best practices prior to release?

A. Yes, we are ISO27001 certified and perform testing and reviews to that standard.

Q. Do you warrant that products have been developed in accordance with principles of secure software development best practices such as OWASP, CSA & IEC62443 including security design review, secure coding practices, risk-based testing?

A. Yes

Q. Do you perform audits or other reviews of your software to warrant that security controls are being implemented and operating effectively? If not, please explain.

A. Yes, all source code is open for read access to all internal development teams to review and comment prior to any release.

Q. Do you have a publicly documented process for managing security vulnerabilities in your application(s)? What is your process for managing and communicating security vulnerabilities in your application?

A. Any security vulnerabilities would be tracked in Gitlab against the codebase of the application, and all builds containing the issue marked as not for release until it is fixed. All existing installs of the software would also be tracked via licensing and informed of the issue, and a free security update offered.

Q. If compliant on previous question, do you warrant that all vulnerabilities rated critical and high have been remediated before making your product available on the Niagara Marketplace?

A. Yes

niagara
marketplace

Q. Do you warrant you have removed unnecessary features, components, back doors, files, protocols, and ports from your software or product your are offering through the Niagara Marketplace? That is, does it weaken the Niagara Framework?

A. Yes, we take steps to thoroughly test for any workarounds or backdoors in our software. All software is strictly version controlled so any unnecessary components are not included.

Q. Do you have a formal change control and release management processes to manage code changes?

A. Yes, we use Gitlab for version controlled and code push sign off. All builds are explicitly marked as internal or development builds until approved for release.

Q. Do you perform Input Data Validation checks on your product to verify that the inputs (e.g., character set, length, numerical range, and acceptable values) match specified definitions for format and content to prevent injection attacks?

A. Yes, all software is thoroughly reviewed and tested before being marked as release.