Red-Blue Security Services

Bringing formidable offensive and defensive security capability to the most critical embedded system development efforts

QVLx Labs strives to become a leader in the critical embedded systems safety and security domains through the delivery of disruptive research, services, products, and training.

One such value-add is our security product, Salvum®. This analysis and hardening suite grants users much of the capability of our security services team in a pre-packaged and carefully curated toolkit.

However, programs with the most stringent security requirements may need additional rigor that a canned software solution cannot provide. Examples of this are detailed radio frequency analysis, complex software control flow analysis, and performing of sophisticated local (physical) attacks.

That is why QVLx offers its Red-Blue Security Services: two dedicated teams that bring offensive and defensive security expertise to you directly.

Red Team

- **Reverse Engineering**: Source code and hardware are reversed to measure the degree of obfuscation of the system.
- **Static Binary Analysis**: Binaries are analyzed to discover exploitable vulnerabilities in images and study software control flow.
- **Runtime Analysis**: Running executables are observed closely under emulated or HIL conditions to find attack points.
- **Perform Attacks**: CVE-known or novel attacks are performed remotely or locally on the system. Includes DoS attacks.
- **RF, Network, Bus Interface Analysis**: RF signals, network, and other packets are analyzed to discover vulnerabilities.

Blue Team

- **Digital Asset Hardening**: Protection is added to the kernel, firmware, applications, and other assets for general resilience. This includes software anti-tamper techniques.
- **Attack Surface Reduction**: Unused code is removed and image sizes reduced. Code is improved in areas that make it vulnerable.
- **Feature Configuration**: Mandatory access controls are set and other security features are enabled, not including chain-of-trust.
- **Detection and Mitigation Implementation:** Deploy tripwires and countermeasures to protect against specific attacks.
- **Other Services Employed**: If needed, other security services can be employed such as secure boot and system key management.

For inquiries, contact us at security@qvlx.ai