QVLx Salvum® Security Engine

Atelier for the refinement of embedded systems.

QVLx Salvum® is a novel framework for embedded systems penetration testing and software development that is guided by NIST SP 800-115 recommended practices. Originally developed as an internal training platform, Salvum has grown into a comprehensive nexus of security capabilities and productivity enhancement tools. The engine comprises of a hardened core that provides modules with a secure shell and API functionality, nearly a hundred foundational applets, and hundreds of offensive and defensive security apps. It can be seen as the world's first app store centered exclusively around embedded systems security and potentially other cybersecurity domains. In addition, Salvum has been carefully designed to be able to run on a wide variety of host systems. By incorporating collaborative contributions from various open-source communities with in-house development, QVLx Salvum captures decades of security expertise in a validated, commercial-grade product and at a fraction of the cost of comparable competitor offerings.

Salvum Key Features

- ☑ Secure core providing unified access to module ecosystem and customizable policy layer.
- ☑ Validated and modular apps/applets that can be imported or excluded on demand.
- ☑ Smooth integration with Lynx Luminosity, Wind River Workbench, QNX Momentics, and other Eclipse-based development environments.
- ☑ Support for Linux, Windows, and MacOS host operating systems on x64-based hardware.
- ☑ Auxiliary reporting engine for interpolation of raw data into actionable analytics.
- ☑ SDK and clean API for development of custom modules and platform extension.
- ☑ SlmCompile build utility for easy compilation of C or C++ binaries.
- ☑ Built-in disassembler for Intel, Arm, PowerPC, MIPS, Sparc, AVR, and RISCV Instruction Sets.
- ☑ Audited, production-ready cryptographic algorithms and curated wordlists provided.
- ☑ Vendor-specific modules implemented for VxWorks, QNX, LynxOS, Segger JLink, and more.

Current Module Classifications

- Host hardware querying utilities (Applets)
- Data manipulation utilities (Applets)
- Secure POSIX utilities (Applets)
- Compression/Archiving/Compilation (Applets)
- Text editors (Applets)
- CPRNG/PRNG/RNG (Blue Apps)
- Entropy analysis (Blue Apps)
- Password tools (Blue Apps)
- Obfuscators (Blue Apps)
- Dynamic code Analyzers (Blue Apps)
- Advisory detectors (Blue Apps)
- Dependency checkers (Blue Apps)
- Input sanitizers (Blue Apps)
- Model checkers (Blue Apps)
- Security linters (Blue Apps)
- Cryptography suite (Blue Apps)
- Cyclic redundancy checkers (Blue Apps)
- Error correction coding (Blue Apps)
- Hashers (Blue Apps)
- Kernel Hardeners (Blue Apps)
- Netloaders (Blue Apps)
- Vendor-specific defensive tools (Blue Apps)
- Binary maniplation tools (Red Apps)
- Decryption utilities (Red Apps)
- Steganography tools (Red Apps)
- Parsers (Red Apps)
- Network sniffers (Red Apps)
- DoS Detection (Blue Apps)
- Intrusion Detection (Blue Apps)
- Steganography detection (Blue Apps)
- System auditors (Blue Apps)
- System rootkit detectors (Blue Apps)
- Vulnerability databases (Blue Apps)
- Runtime binary analysis (Red Apps)
- Static binary analysis (Red Apps)
- Cracking tools (Red Apps)
- Decompilers (Red Apps)
- Denial of Service (Red Apps)
- Detection evasion (Red Apps)
- Disassemblers (Red Apps)
- Exploit Injection (Red Apps)
- Forensics (Red Apps)
- Fuzzers (Red Apps)
- Man-in-the-Middle (Red Apps)
- Unpacking utilities (Red Apps)
- UART/JTAG tools (Red Apps)
- Spoofers (Red Apps)
- Vendor-specific offensive tools (Red Apps)

Purchasing Options

Researcher Package	Developer Package
Prebuilt engine with full app access	Salvum SDK and full app access
Extended Applications	**Reporting Engine**
Grants access to extended apps	Access to reporting backend

Call: (256)-607-4044 Email: security@qvlx.com

© 2021 QVLX LLC. All Rights Reserved.