PALM Associates, Inc.

Software product development for communications.

Version 0.9

System Security Audit and IT Hardening.

A practical service for developers in the medical, connected car and embedded markets.

The objectives of this service are to provide engineers with a useful action list to increase the security of their design or implementation of security sensitive software.

Many systems today are ‘life critical’ and require diligence in the security design and operations. Medical systems, self-driving automobiles, auto pilots for aircraft are just a few examples. For new startups the security implementation and server hardening activities often take back seat to product deployment. These services are intended to help developers of such systems to improve their security architecture implementation and harden their web servers against modern attacks.

PALM’s staff has developed secure systems for the intelligence community, Fortune 10 companies and multiple medical/health informatics systems. These systems were developed using NIST, HIPAA and government security guidelines. Some were developed from scratch using these guidelines, others required audit and analysis of already deployed products. Hardening exercises were necessary to counter bot attacks of servers, to bring the servers into compliance with HIPAA and NIST, and in other cases to correct programming practices.

PALM’s staff will conduct the following tasks and deliver a plan of action to the program manager.

1. Conduct security audit to identify areas of vulnerability.
2. Review vulnerabilities as defined by OWASP. Best software and encryption practices, cert information, etc. changes at a rapid rate, usually with a six month window. For this reason, software implementation practices are reviewed and suggested changes incorporated into the PALM system report.
3. Develop a plan of actions to fix vulnerabilities, implement screening and sanitization of input, upgrade security features and functions, remove careless programming such as passwords in the clear, update programming to best practices level.
4. Review logs and detect offshore hackers, or bot attacks.
5. Identify changes needed in UI to plug vulnerabilities.
6. Review the HHS risk assessment and update policies to comply with HIPAA and NIST guidance.
7. For services deployed on Amazon Web services (AWS), review server architecture, deployment strategy and suggest updates, improvements and alternative services to achieve cost savings, improve robustness and survivability.
8. For HIPAA compliance a HIPAA sensitivity training class is offered as well as support for preparation of HIPAA policies and conducting the HHS Risk Assessment.

Once in the market the product is now vulnerable to breach. Many of these operations and updates may not have been completed due to the time pressure of product development and deployment.