

## Capabilities Statement

### Summary

---

proVM Auditor was developed to **eliminate** the need to copy and paste, script and parse vulnerability scan data. After performing a vulnerability scan of your environment using multiple scanning engines, a typical information security professional must then manually compile and aggregate this data to present meaningful views to management and to begin remediation efforts. proVM **automates** this process and turns days and weeks of work into merely **minutes**. Through various case studies, we've seen as much as a 64% reduction in resource requirements annually. Spend less time, and headache, aggregating data, and more time securing your infrastructure!

### Why the need?

---

- Assessing infrastructures annually (as required by DoD) creates a lot of scan data
- Presenting an enterprise view of the security posture can be problematic and time consuming
- Many methods are not repeatable
- There is a high likelihood of error and incomplete data/reports

### Currently Accepted Scanning Engines

---

proVM Auditor is capable of accepting the native (raw) output of the following scanning engines and aggregating this data into one consolidated format.

- DISA's Production Gold Disk
- DISA's Security Readiness Review Scripts (SRR)
- eEye Retina
- Lumension PatchLink (Harris STAT)
- AppSec Inc AppDetective
- Nessus
- NMAP
- .....We also can take a look at adding any tool that you currently use that is not listed

### Features

---

- Presents data utilizing Microsoft Excel into 3 main views:
  - Summary Tab – total vulnerability counts by tool and device
  - Unique List – vulnerability data listed per finding
  - Details – detailed vulnerability findings per device
- No manipulation of data – data in/data out
- Filtering data – able to filter out unwanted data so it doesn't affect totals
- Report on NF/NR/NA for SRRs
- Mapping to 8500.2 controls – if scanning engine contains mappings, proVM will identify it
- Pre-populate findings – if known findings are present they can be pre-populated
- OS fingerprinting override – Override fingerprinting attempts with known OS for each device
- Gold Disk registry keys – can generate individual registry key fixes for Gold Disk
- Identifies scanning tool version whenever possible

## Benefits

---

- 🚀 Expedites the Certification and Accreditation, FISMA and IAVM processes
- 🚀 Provides a standard view of vulnerability data to management
- 🚀 Transforms manual, time-intensive process into quick and efficient progress
- 🚀 Exceptionally simple to use
- 🚀 Designed as an Auditor's Tool
- 🚀 Small footprint / portable – only need a Java Runtime environment to use
- 🚀 Able to build in specific views or tools upon request

## Specifications

---

- 🚀 Java Runtime Environment Version 6 Update 17 or better on Microsoft Windows
- 🚀 2GB RAM
- 🚀 1.8GHz processor or better
- 🚀 250MB of free disk space

## Contact

---

Senior Business Development Engineer

Warren Bailey

Email: [wbailey@prolific-solutions.net](mailto:wbailey@prolific-solutions.net)

Office: 804.601.2721

Cell: 804.221.1090