Vulnerability Assessment Service

Management Brief

Introduction:

Vulnerability Assessment (VA) is the process of determining the security status of the IT infrastructure. The objective of VA is to present a comprehensive yet easy to understand picture of compliance with organizational security policies (or recognized best practices).

Vulnerability Management is a complete set of processes including: defining the desired state for device configuration and resource access; assessment activities (discovery, scanning and reporting); remediation and/or mitigation activities, and continuous monitoring (e.g. new threat assessment).

Rationale: Vulnerability assessment and management are not a panacea for all of IT’s challenges! However, implementing these processes can help make IT environments more secure and improve an organization’s compliance ‘posture’. By mitigating threats, VA and VM are closely tied to enterprise risk management, enabling IT management to demonstrate risk mitigation activity.

VA service is a tool to assist system administrators, as well as a vehicle for discovering devices, new services (changes), and exposures (common exploits, vulnerabilities and threats) that administrators and management need to be aware of.

The CIO has committed to strengthening the University’s overall security practices, and has partnered with Audit Services to demonstrate auditable progress to the University’s Board of Governors’ Audit Committee.

Background:

The desire for implementing vulnerability management within CCS is not new. The CCS Security Infrastructure Team (SIT) and the IT Security Manager made a preliminary effort at establishing vulnerability management with a 2004 project to identify and select an assessment tool. This led to the acquisition of a VA product from Visionael (based on the Nessus remote security scanner).

While the early experience with Visionael was positive, the vendor arbitrarily terminated support in November, 2005 and it was necessary to repeat the product evaluation and selection process.
SIT convened a new working group charged with evaluation and product selection in early 2006, and by August a recommendation to acquire the Foundstone Enterprise VA appliance was submitted. (See Appendix for final Product Assessment Review.)

Foundstone was very well known and respected for the *Hacking Exposed* series of books. The company had been acquired by McAfee in 2004 which addressed vendor credibility concerns.

A major attraction of the Foundstone system is its reporting capabilities, ranging from high-level management “dashboards”, detailed scanning results of vulnerabilities (including CVE identification), unique “Foundscore” rating, ability to prioritize assets, and most importantly reporting vulnerability status over time.

While the recommendation to acquire Foundstone moved through funding and acquisition, work commenced on the policy and standard practices associated with implementing the new tool. In late 2006, SIT completed policy and standards documents (CCS-SIT-03) and these were approved by the CCS A-D’s in January, 2007. (Stored on: G:\shared\CCS-Management\SIT\Policies\FinalPolicies)

The Foundstone appliance was purchased and installed early this year. There have been some difficulties and frustrations configuring the Foundstone appliance and learning its capabilities. In retrospect, acquiring formal training and consulting assistance would have been helpful and expedited progress (see Next Steps below).

The current status of utilization is informal and not yet adhering to the SIT-03 policy. Doug Blain has been working with three CCS areas as “early adopters” (University Systems, Departmental Services, Campus Services). Some scanning history is being retained, however assets have not been classified/prioritized, nor has remediation activity been formalized.

**PLANNING CONTEXT:**

**Introducing the IT PMO!**

The primary mandate of this new function is supporting the new IT Decision Framework by:

- Documenting the impact and value of IT decisions
- Communicating IT decisions, tracking progress, and assessing impact
- Improving the decision making process
- Track the “big picture” regarding the existing IT environment and current projects that extend or augment that capacity
IT Portfolio Management Office

Oct. 10, 2007

PMO & “Systems Assurance”:

Bringing IT Security into the PMO, enables a holistic approach incorporating risk management, security, and compliance efforts. The focus of risk management activity during the past year has been on business continuity and the institutional dependency on IT.

The ERM Steering Committee identified seven “core” systems/services and their Business Owners:

- University network and telephony system: Mike Ridley
- Oracle Financials: John Miles
- Colleague Student System: Brian Pettigrew
- Cyborg H.R. system: Martha Harley
- OLIS: Virginia Gray
- Desire2Learn: Virginia Gray
- Audit Services

The 2007-08 Audit Plan includes collaboration between Audit Services and the Office of the CIO and will include a joint report addressed to the Audit Committee of the University Board of Governors.

Objective/scope: “An Annual Report on core systems as maintained by the Office of the CIO.” The “core” IT systems and services (per the ERM Steering Committee) will be reported on for 2007-08.

Requirement: Procedures and reporting must be auditable! N.B. Reporting must be continuous (not one-off) and contain metrics.

Reporting to be provided for 07-08 includes:
- information related to breaches or attempted breaches of the core IT systems
- significant changes to procedures and/or protection used by IT maintain and strengthen IT security
- status of use or planned use of external consultants to test IT security of core systems

Based upon the Vulnerability Management initiative underway, Audit Services will utilize the GTAG (Global Technology Audit Guide) #6: Managing and Auditing IT Vulnerabilities (published by the Institute of Internal Auditors) to assess the “organizational maturity” of the IT organization. A PDF of the Guide is available on request.

Bottom Line!

The CIO (and the Director, IT PMO) have committed to producing auditable vulnerability assessment reporting before December/07 for the three enterprise business production application environments (Colleague, Cyborg, Oracle Financials).
Next Steps:

Working collaboratively, we need to move the VA service to a limited-production status shortly after the scheduled upgrade and training taking place this month (see proposed phases below).

The PMO has contracted with the: Herjavec Group (formerly Metacomm/Metasecure) to upgrade the Foundstone appliance to the most current release (version 6.0), provide training on new functions and features, and integrate the system with McAfee’s ePolicy Orchestrator (EPO).

We have a tentative agreement with Leon Loo to provide operational-level (system administration) support based on a defined Service Level Agreement (to be developed). In addition, we will be discussing a potential value-added relationship with Herjavec as per SIT-03 (Policy Statement 3) that could include off-loading some administrative and reporting effort from in-house staff.

Utilization of the McAfee Foundstone Enterprise application will enable a VA service to be provided by the IT Portfolio Management Office (IT PMO). The service will support the CCS Vulnerability Management Policy (CCS-SIT-03), with the intention to expand the service University-wide (i.e. to other IT service providers) in 2008.

Vulnerability management, including defining device configuration standards and remediation of discovered vulnerabilities is the responsibility of IT management. The PMO role (Manager IT Security) will be limited to monitoring that discoveries and scans are performed in accordance with agreed policy and standards, maintaining an auditable log database for trend reporting, and approving policy exceptions as required.

The growing Managed Desktop service, leveraging the functionality of EPO to ensure adequate “end-point” security, will significantly increase the number of Foundstone device licenses required, however the additional licenses only cost a nominal amount, and we are already negotiating increasing our current 250 device license to 500.

The realignment of responsibilities within CCS into technology layers will require increased liaison effort by Doug Blain and additional Foundstone ‘end-users’.

Remediation processes:

Foundstone has its own ticketing system for tracking remediation activity, and can (potentially) export tickets to Footprints. However, our recommendation for the initial implementation period (remainder of this fiscal year) is that we keep the process simple but formalized and utilize e-mail to track communication between the Foundstone administrator and “users” (i.e. designated personnel with technical support responsibility and applicable managers/team leaders).
We propose expanding the VA service scope in discrete phases, initially prioritizing auditable compliance with the SIT-03 policy for the major business applications.

Proposed Phases:

One:

**October 19 - December, 2007**

CCS-administered “core” business systems (Colleague, Cyborg, Oracle Financials).

Two:

**January - April, 2008**

All remaining CCS-administered services

Three:

**May, 2008**

All remaining services (in stages) connected to the University network.

To discuss with CCS-MT:
Concern about resource efforts to analyze and respond to scan reports.
Appendix

N.B. Excerpted from Vulnerability Product Assessment Review
(Final Report) Doug Blain, April, 2006

McAfee - Foundstone

Web site http://www.foundstone.com/

Description Scanner appliance

Platform appliance

Supported Target Systems Multiple Unix, Linux and Windows.

Databases yes

Discovery yes

Reporting yes

Ticketing yes

Patch Management yes

Cost Scanner and management software $35000 US

Product Description (Vendor)

Benefits:

- **They scale to meet your needs**
  These appliances are flexible and customizable, so you can tailor your vulnerability management strategy to meet your unique business, technical, and compliance requirement

- **You get flexible deployment options**
  Options include the FS1000 appliance for accurate and scalable vulnerability management and the FS850—our remotely managed scan engine—ideal for service providers and remote deployments

- **Our hardware passes the test**
  Our appliances have been designed and tested with security in mind; we make sure they meet the most stringent security standards

- **Improve risk management**
  These appliances power Foundstone Enterprise, our world-class vulnerability management solution, which helps you prioritize threats and vulnerabilities to mitigate risks more efficiently
Features:

- **Appliances are a smart investment**
  Foundstone appliances are a low-cost solution for reliable, high-performance vulnerability management that requires minimal IT involvement

- **No maintenance**
  You get continual protection without manual intervention; our update service automatically delivers product updates for hands-off appliance management

- **Easy-to-install remote scan engine**
  The FS850 remotely managed scan engine appliance installs in less than one minute; you don’t have to be an IT wizard to perform the simple three-step installation process; the remote scan engine is ideal for large distributed networks

- **With one appliance, you get it all**
  The FS1000 combines a scan engine, database, and manager in a powerful and scalable vulnerability management appliance

- **Get high-performance scanning**
  Our FoundScan technology is at the heart of the FS1000 and FS850 appliances; these appliances typically scan a class C network in less than 20 minutes, a class B network in 6 hours, and a class A network in less than 48 hours

- **You can set your scan schedule**
  Define your scan schedule—daily, weekly, monthly, continuously, or one time only; once you’ve done that, the scan engine takes over and automatically scans your network

- **Our appliances scan in parallel**
  These appliances are based on a unique parallel scan architecture that performs multiple assessments from one engine simultaneously without a decrease in performance; multiple operators can use the same engine without waiting in line

Vulnerabilities in your infrastructure can put your business at risk. And, your IT staff isn’t equipped to prioritize and manage the critical tasks associated with vulnerability management. McAfee Foundstone appliances, which are at the core of our enterprise solution, take the pressure off IT by automating vital processes.

You don’t need any technical expertise to get started. Simply follow the wizard-driven setup, and your appliance is ready to go. Plus, your Foundstone systems are automatically and continually protected from the latest threats without manual intervention, thanks to the McAfee Foundstone Update Service. This service automatically downloads and installs operating system updates and patches. We install only the patches you need, and we test all patches before they are installed. The service also automatically delivers all product updates that address the latest vulnerabilities and threats.

Foundstone appliances are the most powerful on the market—a single FS850 can scan approximately 25,000 IP addresses. With the unique combination of our hardware and software, you get the most scalable scan engine available today. Our scan engine technology lets you protect more IP addresses with fewer appliances.
Foundstone appliances are flexible too. They can be easily adapted to your business processes. For example, you can define your scan schedule—daily, weekly, monthly, continuously, or ad hoc. For each scan, you can also specify the window of time when a scan should be done. (For example, between midnight and 5:00 A.M. daily). If a scan is not completed within its defined scan window, the scan is automatically paused, and then resumed during the next available scan window.

Foundstone appliances are based on our unique parallel scan architecture, so you get more efficient protection against attacks. Multiple scans can be performed from the same engine simultaneously without affecting overall performance. Most vulnerability assessment products operate in a serial fashion, where a single scan begins only after a prior scan has finished. With our appliances, multiple operators can use the same scan engine without waiting in line for the system to become available. Plus, you can respond to an urgent threat such as a worm without interrupting a routine scan.

Foundstone appliances are self-contained devices, so there are no minimum software or hardware system requirements.

**Gartner - G00125094 - 2003**

McAfee provides vulnerability assessment software and appliances that run on the Windows platform. McAfee is included in this segment because of its recent acquisition of Foundstone, a major provider of network-oriented vulnerability assessment technology. Foundstone Enterprise has comprehensive reporting and enterprise management capabilities, two of the feature sets that organizations often mention as the deciding factor when selecting the vendor. Foundstone Enterprise has imbedded workflow and the ability to export trouble tickets to systems such as BMC Software/Remedy.

We expect McAfee to continue to provide network-based vulnerability assessment and to eventually integrate it with its ePolicy Orchestrator and network- and host-based blocking technologies. ePolicy Orchestrator is a centralized management tool that will also increase the value add and management and reporting capabilities of Foundstone products. McAfee will have to prove that it can execute against the integration of Foundstone products.

**PC Magazine – 2003**

If you're in charge of a large, complex network that is geographically dispersed, have to handle hosts on multiple subnets, and have $34,200 handy to dedicate to the task, consider the Foundstone FS1000 Appliance, a turnkey network vulnerability hardware solution.
The FS1000's scanning engine is impressive, but the most valuable aspects of the unit are its reporting and threat correlation capabilities. After running a vulnerability assessment, the device generates data that is presented in multiple ways, ranging from very-high-level overviews to extremely detailed reports.

Foundstone's FoundScore rating is another way of making results data more digestible. FoundScore is especially helpful if you want to track the security of your network over time. Every scan generates a score based on an algorithm that starts with 100 points (for a network with no severe vulnerabilities) and then deducts points for detected weaknesses, based on their severity. Some of the higher-level views available are Risk by Platform, showing the distribution of serious vulnerabilities based on operating system, and Risk by Vulnerability, which reports the distribution of host risks.

Using the threat correlation module, we were able to match vulnerabilities to hosts based on several criteria: OS, ports, available services, and banner information retrieved from the system. You can also assign a "criticality" score from 0 (none) to 5 (extensive), to the overall risk score of any given host, bringing it to the top of your list if a matched high-risk vulnerability is identified. This enables you to identify and prioritize your most crucial hosts. We think similar features should be found in all vulnerability scanners.

The FS1000 is built on a 1U rack-mount server with dual Intel Xeon processors, running Microsoft Small Business Server 2001. The device also runs Foundstone Enterprise, which has three components. An SQL back-end database is used to store all data, including scan configurations, results, and reports. The scan engine is the heart of the device and provides configuration options in a Win32-based application. And finally, Foundstone's easy-to-use Web-based portal provides access to all aspects of the application, including scan configuration, asset management, reporting, and threat evaluation; it can also function as a central access interface if you are using multiple third-party scan engines that report to a centralized database. The Web portal module even includes code sifting, a technique employed to identify potentially sensitive content, such as e-mail addresses or names in your HTML source.

Though we almost choked when we saw the FS1000's price, we remain extremely impressed. It provides all the important data analysis features as well as a mature and easy-to-use interface. The FS1000's tested configuration ($34,200 direct) includes the appliance ($6,700), Foundstone Enterprise software ($25,000, which covers 500 active devices), and the Threat Correlation and Remediation components ($2,500). (877-913-6863, www.foundstone.com)