# VULNERABILITY MANAGEMENT

## A White Paper


**Presented by:**

**MindPoint Group, LLC**

**8078 Edinburgh Drive**
**Springfield, VA 22153**

**■ (o) 703.636.2033 ■ (f) 866.761.7457**
**■ www.mindpointgroup.com ■ blog.mindpointgroup.com**

**■ SBA 8(a) Certified Small Disadvantage Business ■ Woman-Owned Small Business (WOSB)**
**■ Economically Disadvantaged Woman-Owned Small Business (EDWOSB) ■ Minority-Owned Small Business**

## BACKGROUND

Vulnerability management is a process that can be implemented to make IT system environments more secure and to improve an organization's regulatory compliance posture. To be effective Enterprises need to have a robust program for identifying and eliminating vulnerabilities throughout their IT infrastructure. The expected result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities.

Proactively managing vulnerabilities of any system will reduce or eliminate the potential for exploitation and involves considerably less time and effort than responding after exploitation has occurred. A comprehensive vulnerability management program must be comprised of both tools and process to be effective. Solutions that are tools focused alone are insufficient when used without the appropriate implementation processes. Regardless of the customization done to develop a process that fits a particular organization, a standard vulnerability management process will probably include the following basic tasks:

- **Preparation:** Determine assets to be included, classify groups of asset values, and define scan policies.
- **Scan:** Perform scans according to a schedule which reduces impact to operations and supports timely identification of emerging vulnerabilities.
- **Prioritize:** Determine which issues are the most serious based on external threat information, internal security posture, and asset classification.
- **Report:** Report to personnel responsible for testing and implementing fixes, and track progress over time using a pre-determined set of metrics.
- **Remediation:** Eliminate the root causes, or implement mitigations using complementary security tools.
- **Maintenance:** Maintain and continually monitor the environment to identify new vulnerabilities.

In terms of tools, there are a variety of different options which fully or partially satisfy an organization's vulnerability management needs. Passive scanning or discovery tools, like the following are helpful in identifying active unknown hosts on the network but can completely miss quieter hosts, and often will incorrectly identify hosts:

- SourceFire's Real-time Network Awareness (RNA)
- Tenable Passive Vulnerability Scanner (PVS)

Patch management tools, like the following are helpful in identifying vulnerabilities in known, cataloged systems that have been patched by the vendor:

- BigFix
- Microsoft System Center Configuration Manager (SCCM)
- Windows Server Update Services (WSUS)

However, patch management products fail to identify vulnerabilities that exist outside the vendor ecosystem; misconfiguration issues such as default credentials; system settings that fall outside organizational compliance targets; and they simply cannot track unknown or unmanaged systems that exist on the network. Active scanning tools fill the gaps left by these other tools. They provide an organization with the ability to accurately and actively identify vulnerabilities,

unknown hosts, and compliance issues on their network. This whitepaper will describe a brief case study of our experience implementing such a tool.

## OUR EXPERIENCE

MindPoint Group has extensive experience providing vulnerability management. We recently were contracted to design and build a security monitoring infrastructure and support vulnerability scanning tasks. A framework was established to improve visibility, security, and compliance. Although our client's organization already had Tenable Security Center (SC) and Nessus deployed, we identified early that this tool set was not adequately provisioned to support an effective monthly vulnerability management process.

While results were being generated and sent to administrators for remediation, proper verification of remediation activities was not being completed. Additionally, the results were being delivered to the administrators in a raw format that made it difficult for the teams to identify and correct vulnerabilities quickly based on risk and criticality. Resource allocation for the hardware and software, and the licensing supporting the vulnerability scanning tools was not planned accordingly during the initial implementation.

First, we were able to redesign and deploy the tools to adequately provisioned hardware, upgrade the system and application software to support UI and feature improvements, and increase allocated licensing. We also redesigned scan policies to support more accurate and complete coverage, and provide more relevant results for scanned devices while eliminating false positives. Although we went back to the preparation stage these two changes did not require a great deal of time and effort, but they made the biggest impact on supporting monthly vulnerability scanning efforts.

Second, the result reporting process was identified as being deficient. End-users of the results (system administrators) were not gaining value from the previous result format, patching was suffering, non-patch related weaknesses were identified but lost in the noise of patch results, and remediation efforts were not being verified or tracked.

Our team developed a vulnerability management process document for the organization, and identified and implemented a better reporting format. The Tenable SC reporting system was utilized in the process to provide results in a more effective format that was useful to the end-users of the information being presented. A vulnerability tracking system was developed and used to track reported vulnerabilities, remediation plans, remediation actions, and verification of remediation actions. The system was also designed to be able to provide tracking metrics to the security program manager and the CIO. By focusing on improving the **reporting** of vulnerabilities, significant improvements to the organization's security posture through **remediation** were realized.

Through the implementation of the above changes to the vulnerability management program and vulnerability scanning tools we were able to help the organization identify patch levels of systems that were falling severely behind, misconfiguration issues (i.e. default credentials, poorly configured email systems, etc), rogue or unauthorized network devices, and retired or stale devices and network segments still live on the network. Additionally, network-wide scan times were brought down from days to hours and network utilization during scans was greatly

reduced. These improvements to the **scanning** task are immediate and noticeable to users and management. Also, scan result quality was increased while the quantity of spurious results was reduced.

## TAKEAWAYS

Vulnerability management is about much more than the use of tools. Base on our experience, this is not just conjecture. It is a fundamental fact. Ignoring it will lead to deployment of a great tool that simply does not satisfy the needs of the organization. In order to get vulnerability management right, you need to consider who consumes the information produced, what they are supposed to do with it, and what the overall process should look like.

Vulnerability management is a core process aimed at continually mitigating risks as they emerge in your environment. For such a crucial function you might assume that a solution will cost you an arm and a leg, but it shouldn't. The cost for our services described in the case study here were actually reasonable. Although the client organization spanned multiple geographically disparate sites, we were able to engineer a solution that incurred minimal license costs. Our engineer was also able to avoid doing any reworking of the solution by first evaluating the client needs so that the tool would support their needs once it was deployed.

Any vulnerability management solution which includes only tools is likely not going to work well for you. Essentially, our delivered solution consisted of the following components:

- A Tenable SC installation for managing scans, reporting, and end-user access to these vulnerability management essentials.
- A Tenable Nessus scanner for actually running the scans.
- A Standard Operating Procedure (SOP) detailing the vulnerability management process.
- Reporting templates designed to suit the client's needs.
- Scan templates designed around the client network environment and scanning needs.

## ABOUT MINDPOINT GROUP

MindPoint Group, LLC (MPG) is a Small Business Administration (SBA) certified 8(a), Woman-Owned (WOSB), Economically Disadvantaged Woman-Owned (EDWOSB), and Minority-Owned Small Disadvantaged Business (SDB) with its headquarters in Springfield, VA. MPG's Information Security and Privacy (ISP) services provide program management support, security assessment & authorization (S&A formerly C&A), independent verification and validation (IV&V), continuous monitoring, cyber security, security controls and vulnerability assessments, penetration testing, and security operations center support. MPG understands that information security has a broad scope, and an effective information security program must integrate with a number of other organizational processes in order to function effectively. MPG has experience developing and implementing a wide range of security policies, procedures, and technologies in a variety of environments with the goal of ensuring the c*onfidentiality, integrity, and availability* (CIA) of our clients' sensitive assets and information systems.

MPG specializes in implementing IT Security Program Management through our IS&P methodology of establishing a collaborative working environment across all disciplines through innovation, technical excellence and a dedication to repeatable processes. MPG goes beyond FISMA compliance by helping our clients align Federal regulations with their operational mission. Through this methodology, MPG has successfully supported various clients integrate security across a wide range of security domains and environments.

For more information on our solutions, please visit our web site at www.mindpointgroup.com, or check out our blog at blog.mindpointgroup.com.