

Foundstone Professional Services – Vulnerability Management Health Check

According to Gartner, “Enterprises that implement a vulnerability management process will experience 90 percent fewer successful attacks.”

Overview

When was the last time you evaluated your vulnerability management program? Is your scanner detecting all the latest vulnerabilities? Are some of your systems being overlooked during the remediation process? Is your remediation process efficient, responsive, and up to date?

Benefits

Foundstone® consultants can help you assess your current vulnerability management program. Our Vulnerability Management Health Check analyzes the gaps in your vulnerability management program and identifies the areas where you may not have the right balance of people, process, and technology.

Methodology

Successful vulnerability management balances the demands of security against the demands of individual business units. It includes these eleven steps:

1. Current policy review relative to generally recognized standards and compliance guidelines
2. Asset inventory:
 - a. By type
 - b. By owner
 - c. Specifications
3. Data classification to create an asset criticality profile, which defines how important each asset is to your organization.
4. Vulnerability assessment
 - a. What and when
 - b. Vulnerability classification
5. Threat correlation
 - a. Worms, exploits, wide-scale attacks, new vulnerabilities
 - b. Correlation of high-profile threats with the most important assets
6. Determination of risk level based on the intersection of assets, vulnerabilities, and threats so that you can put your focus and attention on truly critical risks
7. Remediation
 - a. Factoring the cost to remediate versus the cost to ignore
 - b. Zeroing in on must-have remediations
8. Metrics
 - a. Accurate metrics for more informed and more effective management
 - b. Evaluation of your current state of security measurement against current baselines and against ideal conditions (e.g., Six Sigma)
9. Training
10. Communication
11. Definition of organizational roles and responsibilities

Foundstone assesses your current vulnerability management program in the eleven best practice areas and makes recommendations on next steps. These recommendations are made based on interviews with key personnel and a review of policies and procedures.

Scope

The typical scope of this engagement ranges anywhere from three days to one week, depending on the size of your organization and project scope.

Deliverables

Our deliverables include:

1. Vulnerability Management Gap Analysis Document
2. Next-step recommendations
3. Half-day Vulnerability Management Health Check presentation and results review workshop

All Foundstone projects are managed using Foundstone's proven **Security Engagement Process (SEP)** for project management. A pivotal aspect of this process is continual communication with your organization to ensure the success of your Foundstone consulting engagements.

Related Foundstone Services

Foundstone offers many related services and training classes.

- Policies and Process Health Check
- Policies and Process Development
- Foundstone Training
- Comprehensive Security Health Check
- Comprehensive Network and Infrastructure Security Assessment

Contact

For additional information about this or other Foundstone service offerings, please contact your local sales representative:

- Phone: 1.877.91.FOUND
- Email: Consulting@foundstone.com
- Web: www.foundstone.com

About Foundstone Professional Services

Foundstone® Professional Services, a division of McAfee, Inc., offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, Foundstone identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company's professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military.