DIGITAL DEFENSE INCORPORATED

TAG cyber

## Vulnerability Management Maturity Model

# VM3 Companion Guide

A Digital Defense, Inc. Guide

# Digital Defense
# Vulnerability Management Maturity Model (VM3)
# *Companion Guide*

### Purpose

This short guide is intended as a companion document for enterprise security teams who are making use of the Digital Defense Vulnerability Management Maturity Model (VM3) to improve their day-to-day control of known and unknown exploitable weaknesses.

### Background

In 2016, Digital Defense engaged in a study which detailed the organizational challenges and factors influencing levels of maturity with respect to vulnerability management (VM). This study resulted in a Whitepaper designed to help organizations gauge their VM maturity level, as well as guide them in their VM improvement and evolution. This short guide is a primer aimed at jump-starting the evaluation of an organization's VM maturity level. The guide summarizes the Digital Defense VM3, including brief description of the maturity levels and key challenges organizations face. The guide also includes a set of recommendations per maturity level that organizations may follow to evolve to the next VM maturity level.

### VM3 Overview

Vulnerability management (VM) is an ongoing process which all organizations must perform to some degree. VM includes multiple activities aimed at managing an organization's IT security risk. The VM process includes six high level steps which control and continuously improve the process. Each of the six steps includes many possible sub-activities. Figure 1 illustrates this underlying VM process, inclusive of activities and surrounding business environment. Some of the actions may be automated; however, regardless of how much is automated, there must be oversight by humans who are responsible for this process on behalf of the organization.

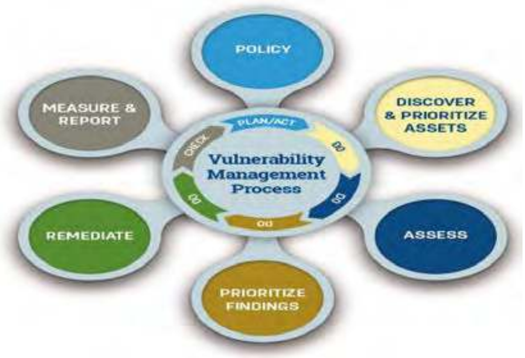

**Figure 1**. Underlying VM3 Process

The VM maturity level of an organization depends on the degree to which it embraces the more specific sub-activities, and emphasizes business oversight and management commitment. Additionally, the maturity level will also depend on the level of financial investment allocated to this process. A detailed coverage of the various challenges organizations face is covered in the Whitepaper.

**Vulnerability Management Preliminaries**

The VM3 model dictates attention to six specific areas of vulnerability management, with focus on assuring excellence in all aspects of the attendant tasks. These six areas – *policy, assets, assessment, prioritization, remediation,* and *measurement* – are briefly outlined below:

*Policy*

Organizations need to develop and maintain a strong business policy regarding VM. Business unit leads, for example, should recognize the importance of VM and should provide whatever resources are required to the security team to accomplish the VM objectives. Having a weak or non-existent VM policy will result in lower maturity scores in the VM3.

*Assets*

Accurate inventories of IT assets are prerequisite to proper VM attention. Sufficient budget, technology, and processes must be in place to create and maintain correct views. Obviously, if the enterprise desires a clear view of vulnerabilities in assets, then knowing what assets are in place is the first step. Poor asset management will result in lower maturity scores in VM3.

*Assessment*

Ongoing VM assessment is a clear indicator of a mature VM process. The ability to rely on a programmed process where VM is performed on internal and relevant external assets is a clear prerequisite to high maturity scores in VM3. Increasingly, assessments can be automated, which is good news for VM teams.

*Prioritization*

Having a reasonable means for prioritizing vulnerabilities allows an enterprise to develop a mature understanding of their true posture. Organizations typically must use more than the traditional vulnerability severity rating in prioritizing findings. Using limited prioritization dimensions typically results in higher risk and consequently lower VM maturity.

*Remediation*

A common challenge faced by organizations is finding the IT asset owner for the assets which have findings that have been deemed as requiring remediation. Many organizations struggle in finding the correct IT asset owner leading to delays and inefficiencies in remediation which in turn influences their VM maturity level. The VM3 study has found that smaller organizations typically experience less challenge in this area as compared to larger ones. A second common challenge faced by organizations in this area is related to IT organizational structure.

*Measuring*

Measurement of the VM process is key to keeping it on track and ensuring continuous improvement. Organizations with insufficient measurements and metrics for the VM process typically operate at lower maturity levels as compared to those with solid process measurements.

## VM3 Maturity Levels

The VM3 Model highlights six maturity levels ranging from the lowest level 0, where the function is acknowledged but not valued up to the highest level 5, where the function is embedded into the ecosystem and automated for continuous attention. Figure 2 depicts the six VM3 levels.

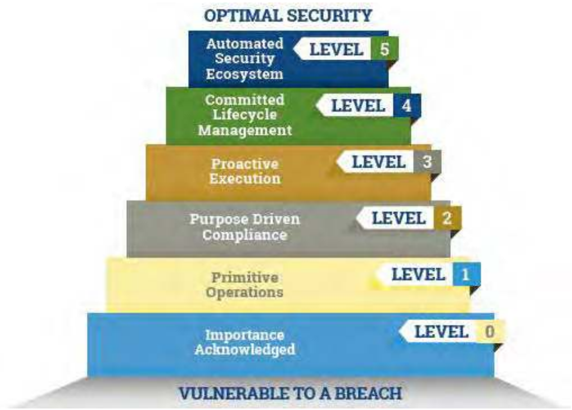

**Figure 2**. VM3 Maturity Levels

*Level 0 – Importance Acknowledged*

This maturity level is characterized by a lack of risk policy or threshold, as well as limited commitment to the process from upper level management.

*Level 1 – Primitive Operations*

At this maturity level, VM policies are present, but no measurements are in place, and the organization might struggle in achieving compliance to regulations.

*Level 2 – Purpose Driven Compliance*

At this maturity level, the organization lacks strong commitment from executives, but it performs regular internal and external scanning. Remediation of findings is present but there are no SLAs in place. Assessment Reporting is present but only for minimal compliance.

*Level 3 - Proactive Execution*

At this maturity level, there is some commitment from executives regarding VM. Security awareness is present, but may not permeate the organization. The security team prioritizes vulnerabilities, and deeper scanning is. The organization correlates assessments across time, either with VM technology or by loading findings into an external system which performs the correlation.

*Level 4 – Committed Lifecycle Management*

At this level, there is strong VM process commitment from top level executives. Security awareness permeates the organization. Sensitive data locations and critical asset availability are known and used to prioritize findings. IT asset owners are largely known, facilitating the assignment of findings. Remediation SLAs are in place, as are measurements and reporting.

*Level 5 – Automated Security Ecosystem*

At this maturity level, all previous functions and capabilities are in place, but the organization also employs a wide range of assessment methods covering all IT assets. The organization prioritizes findings across at least three dimensions, one of which is threat intelligence. VM is integrated with many other of the organization's security technologies, enabling more seamless automation of the entire process.

## Gauging your VM Maturity Level

Digital Defense has developed a simplified self-assessment questionnaire to help organizations gauge their VM3 maturity level, and includes recommendations to help organizations move to a higher maturity level. The self-assessment questionnaire includes a short series of questions which are automatically scored and which provide results in the form of an organization's estimated VM maturity level.

## Organizational Action Plan for VM3 Improvement

Once an enterprise has worked through the Digital Defense VM3 assessment process and determined its level of maturity, the VM team is advised to gather and discuss results and insights gained from this simple process. In some cases, the improvement process is straightforward, such as if some policy or process is missing from the overall VM ecosystem. Security awareness is another example case where improvements will tend to heighten VM maturity. In other cases, however, fixes might be more complex, such as if the IT organizational structure does not lend well to optimal VM processes. Clearly, reorganization of group roles and responsibilities to improve communications for VM will exceed the authority of VM teams, so these situations will require escalation.