FORTRA™

GUIDE (VULNERABILITY MANAGEMENT)

Climbing Vulnerability Management Mountain

A Journey to Minimize Risk in Your Environment

Building out your vulnerability management program is a lot like climbing a mountain. There's a great deal of planning and work involved, but once you get to the top, it was well worth the journey. Climbing the vulnerability management mountain will be a lot of work, so we've outlined the Vulnerability Management Maturity Model to help guide your journey.

This effort will improve the security of your environment and will be repeatable when new groups, organizations, or acquisitions are brought in.

The Vulnerability Management Maturity Model

The Vulnerability Management Maturity Model is your guide to building a strong vulnerability management program. Pictured above, this metaphorical mountain outlines the five goals—we'll call them maturity levels (ML)—that you'll need to hit to summit the vulnerability management mountain. Each level has items that you'll need to focus on in order to move on to the next level. As you assess your current state, you may already be more advanced in some areas than others. However, it's important to note that you won't be able to advance to the next maturity level until you've met all the items on that level. It's crucial to build your program sequentially.

This paper will guide you through the process of climbing the vulnerability management mountain.

Planning Your Journey

Just as you wouldn't begin to climb a mountain without any preparation, you'll need to prepare for climbing the vulnerability management mountain. You need a plan—or a map—for the climb. Keep in mind that this plan will not be static; you will likely have to readjust and reassess as roadblocks inevitably come up.

One of the first things you'll need to assess is what equipment you will use. There are a lot of options, both commercial and open source tools, that can help you on your journey. Depending on what is the best fit for your organization, you may choose to use a VM suite that will combine most of the tasks for you in a single product, or you may opt for an option where you can pick and choose tools for specific tasks. There are positives and negatives for each of these methods, so choose what is best for your organization.

KEY TERMS

- **Vulnerability** – A vulnerability is a weakness or flaw that can be found in a system's design, operation, or implementation that could violate the system's security policy if exploited.
- **Asset** – An asset can be anything from physical hardware to virtual devices. Examples of assets are servers, desktops, network gear, containers, serverless code, and even IoT devices.
- **Vulnerability assessment** – This process will assess that state of your assets at a single point in time, aiming to identify any vulnerabilities in the network or environment. This assessment can be done by an assessment tool or a manual pentest.
- **Remediation** – The process of fixing, stopping, or working around a vulnerability. Remediation can be done by applying a patch, changing a configuration, or even blocking exploit attempts with a network device.
- **Vulnerable** – Assets with a vulnerability are vulnerable only until the vulnerability has been fixed or patched, meaning a vulnerable asset is not necessarily exploitable.

You should not embark on this journey alone. You should work with penetration testing teams and trusted security advisors. The pen testing team, whether they are internal or external, will assess the network and applications by combining various methods that are not as easy to deploy in a single VM application. Your advisors will likely be from the commercial company that you have purchased tools from or industry contacts solving the same issues as you.

You will also need to consider how you would like to break your network up for assessment. This is necessary because unless you have a very small network, doing one full network assessment will return so much data that will be very difficult to sift through.

Some common ways of dividing your networks are:

- Functional group (HR, Engineering, Finance, Sales, etc.)
- Owners (which System Administrators own the systems)
- Geographic location

Finally, you'll need to take inventory of your gear—or assets. This may sound easy, but this can end up being a fairly difficult challenge, as you need to consider cloud assets, virtual assets, and if your organization allows employees to use personal devices, such as home computers or smartphones. Your best option for accomplishing this task to use a tool that will complete an in-depth scan of your network.

When doing this, you will need to get at least the following pieces of information about each of your assets:

- IP address
- Type
- Operating system/firmware
- Applications

First Steps: Maturity Level 0

You've made your preparations, drawn up your plan, and built your asset inventory. It's now time to embark on your journey climbing the vulnerability management mountain. This first step of getting to Maturity Level 0 may be the hardest—you're starting from scratch and will be doing a lot of manual work. However, similar to a hiker getting used to the terrain and eventually getting into a rhythm, you will, too.

Take a look at your asset inventory. What do you focus on first? Unfortunately, it's unrealistic to assess everything at once. If you're using a vulnerability assessment tool or pen testing team, you will likely get far more information than you'll be able to take action on.

Here are some considerations that will help you prioritize:

- How valuable is this asset to the company?
- How easy will it be to remediate?
- Who owns these assets?
- What are the change control windows?
- Can the asset be restored from a backup if compromised?
- Is the asset under a maintenance contract so that I can get patches?
- Are there any mitigations in place (IPS, network/host configurations, etc.)?

There is no one best place to start. It's different for every organization, depending on their business and security goals.

For example, if the next change control window for servers in the demilitarized zone is three months away, this is likely not the best place to start because there is such a big gap of time in between the assessment and when you'll be able to make changes. On the other hand, if these are the most valuable servers for your company, then it may be useful to do an assessment so you'll have insight into their status.

Once you have the results from your vulnerability management's vulnerability scan or results of your pen test, you need to prioritize these results. The results may already be sorted, but you may have to do more sorting from here. Depending on how this assessment was done, the results may be sorted in different ways. It may be sorted merely into critical, high, medium, and low, using the Common Vulnerability Scoring System (CVSS), or a different, more granular scale. In this case, having a vulnerability management tool that will give you more granular results is better. If vulnerabilities are divided into bigger buckets, you may get 50 vulnerabilities labeled as critical, but it can be hard to figure out which of those is most critical.

Now that you have this data, a good place to start analyzing is by looking at the vulnerabilities on the most important asset. Sort these vulnerabilities by ease of exploit and risk. The vulnerabilities that are easiest to exploit and give the most access to the system pose the highest risk.

This risk matrix on the following page indicates how easy a vulnerability is to exploit and the level of risk of that vulnerability being exploited. In this example, the first vulnerabilities you'd want to explore are the 42 vulnerabilities in the top right corner of the matrix.

Once you have all this information, look into the remediation information for these vulnerabilities and act accordingly, either by applying patches or by making configuration changes on the host or network.

And with that, you've reached Maturity Level 0 of the Vulnerability Management Mountain.

Maturity Level 1

When you are ready, you can start your climb up to Maturity Level 1. By this point, you are familiar with what's on your network, how many vulnerabilities you tend to have, and about how much time and money it costs to patch them. Since manual tests are costly, you'll want to invest in a tool that will do an assessment at the push of a button.

Along with this, you'll want to break your environment into logical chunks that will make it easier to assess and mitigate vulnerabilities. There are many different ways you

can separate these, depending on what works best for your network.

Here are some examples:

- Internal and external (if your network is <1000 machines)
- Geography
- Types of operating systems
- System administrators

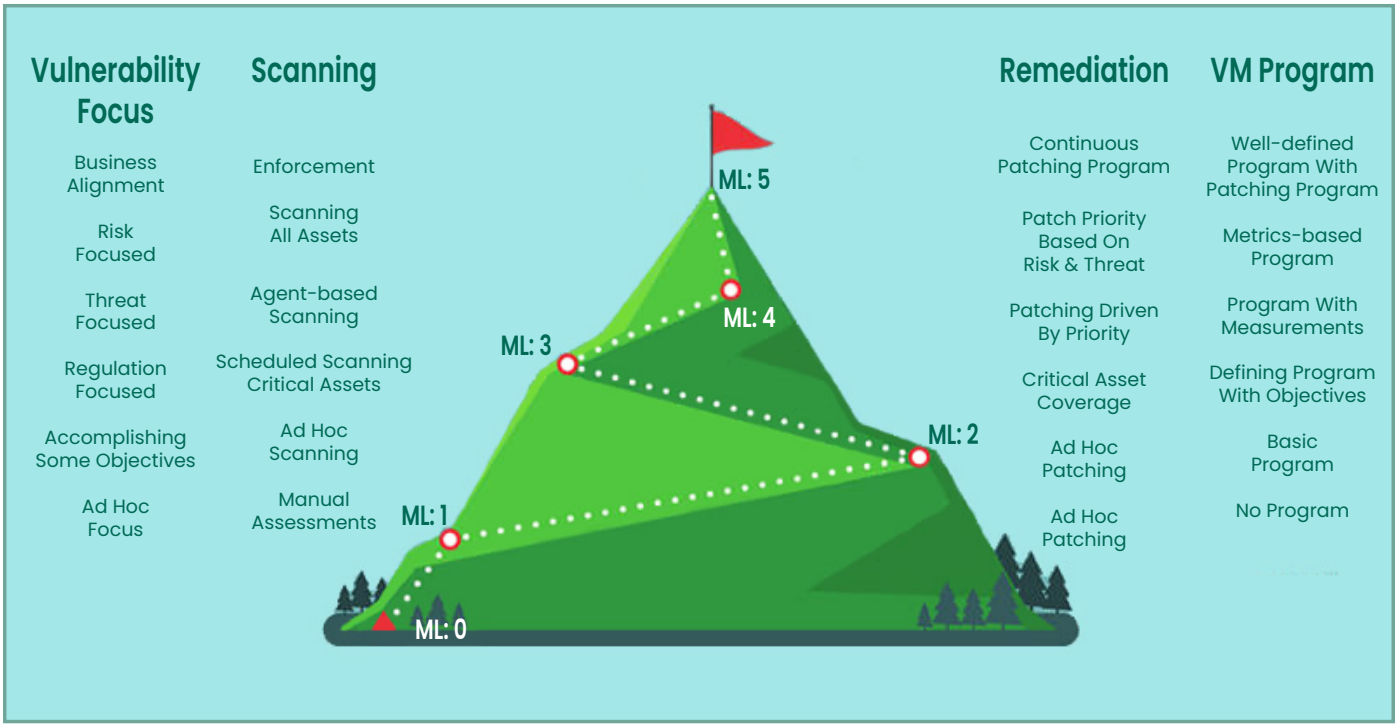
An important consideration for this stage is figuring out when and how often to scan. For many organizations, not launching a scan during business hours is a good option; this means that if a system goes down, it won't disrupt work during the day. At this stage, you should consider scanning weekly, monthly, or quarterly. If you scan more than your team can take on, you won't have enough time to respond to results and will be overwhelmed with more data than you know what to do with. Once you have your cadence down, take a look at large asset vendors that you leverage in your network, such as Microsoft, Oracle, and Cisco. They have a cadence for when they release patches, so you may want to sync up with these releases.

While you're remediating vulnerabilities in an ad hoc manner right now, you may want to start implementing some processes and goals around this work. For example, fix every issue with a CVSS score above nine before the next scan. There may be some trial and error to this, but know that you can always adjust your goals and you'll soon get into a rhythm.

Maturity Level 2

As you embark on your climb towards Maturity Level 2, it's time to start building your vulnerability management program. You'll need to outline goals and objectives, define stakeholders from multiple departments such as IT, legal, security teams, and critical service and system owners, and get executive buy-in. Endorsement from senior management is especially important because you will need a budget and personnel in order to run this program. It is difficult for the program to survive if it is not properly supported.

In this stage, you will fully move away from ad hoc assessments and establish scheduled ones instead. The cadence for these assessments should be at least weekly for critical assets and monthly for non-critical assets. You also need to be ready to run assessments at any time if any critical vulnerabilities are identified, but setting a cadence will keep you organized. Additionally, you'll want to have goals for making sure at least critical assets are remediated in a timely manner.



The path up "Vulnerability Mountain" requires meeting multiple checkpoints for each Maturity Level (ML).

Maturity Level 3

Reaching Maturity Level 3 is a big accomplishment—you've already built a great program that many organizations don't reach. However, there's still more to go to reach the peak of the vulnerability management mountain.

Your next focus will be on expanding the breadth of your assessment in your organization. You'll want to expand incrementally, increasing your coverage monthly. You've already prioritized your assets, so use this information to guide you on where to expand next.

As you continue to increase coverage, it's important to know the three different categories of scanning:

1. **External assessments or remote checks:** These assess the vulnerability of a system without logging into the system. This style of scanning will send packets to the target and determine vulnerability status based on the reply from the target.
2. **Internal assessments or local checks:** These use credentials to log into the asset and determine a vulnerable state by checking items like file versions, configurations, rpm versions, registry keys, etc. These require elevated system access on each asset to perform correctly.
3. **Agent-based checks:** These perform like the local checks, but instead of logging in to an asset, the agent runs assessments locally on a cadence. The agent runs with elevated privileges, so there is no need to manage passwords. This is good for transient assets that may not be on the network at the time of a scheduled scan.

At this stage, you'll also want to start gathering data points so you'll be able to start tracking some program metrics.

What you choose to measure is up to you, but here are some examples to consider:

- What percentage of your organization is covered?
- How many truly critical vulnerabilities are in your environment?
- What is the mean time to resolution (MTTR)?
- How much time did it take to discover a vulnerability since it was introduced?

Maturity Level 4

Now that you've collected data points, your next step is to turn them into metrics that are tracked at least monthly, and build processes that will help you find the root cause that might be having a negative influence on these statistics.

Let's revisit the example metrics we outlined in Maturity Level 3, and set expectations for what these should look like:

Coverage should always be very high. If not, why? Are systems not being assessed for some reason? Are new systems coming online without proper assessments?

Truly critical vulnerabilities can be defined when considering the overall risk score. Factors to consider when putting together the risk score include the vulnerability score, the importance of the asset the vulnerability is on, how easy it is to exploit, etc.

MTTR will fluctuate because some fixes are harder to fix than others, or there may be times where it's impractical from a business perspective to make the fix.

The time it takes to detect a vulnerability should be close to zero if new systems, CI/CD pipelines, and upgrades are being monitored.

This stage will involve some trial and error as you work to find the right risk profiles and metrics for you. It may take a few iterations until you find what works best for your organization.

Maturity Level 5

Congratulations, you've reached the final stretch of the climb. The key to this final level is business alignment. If everyone is not agreed on the goals and metrics, things won't run smoothly.

Here are some examples of areas to align on:

- What risk level is acceptable on vulnerable assets? Does it differ depending on the asset?
- What is the SLA for remediating a vulnerability? Does it differ depending on the network or use of the asset?
- What is the process for fixing a critical vulnerability that can impact the business?
- What is the process for allowing and assessing new assets on the network that have vulnerabilities?

You should focus on figuring out root causes of issues you may find and figure out constructive changes that you can implement to improve your processes. Having business alignment will help this effort be more productive.

Continuous patching should also be implemented at this level. Using data from your vulnerability management tool, a worklist should be generated of which assets need to be patched. This shouldn't be an exhaustive list of all of the organization's vulnerabilities—it should be a short list of the most important vulnerabilities that need to be addressed. You do not want the list to be too long that it is

overwhelming and not actionable. Perhaps make a "Top 10" round-up that goes out to system owners each week.

Not every organization will make it to the top of the vulnerability management mountain. Some choose to not aim for the top due to a lack of skills, manpower, or desire and accept a higher risk of having a less robust program. Many organizations experience setbacks along the way. While the goal may be to reach the top of the mountain, they may choose to hang out at one level for a while. Some choose to outsource this effort and instead invest in a trusted security advisor. However you go about building your vulnerability management program, remember that the harder the climb is, the better the view.

Fortra's VM platform is a broad and inclusive suite of solutions designed to fulfill your organization's vulnerability assessment and management needs. Our VM platform includes solutions for on-premises, cloud, and hybrid deployments from IT to OT. Learn more about Fortra Vulnerability Management by visiting www.fortra.com.

QUESTIONS YOUR VULNERABILITY MANAGEMENT PROJECT PLAN SHOULD ADDRESS

- What are the roles and responsibilities?
- Who runs the tool(s) used to find vulnerabilities?
- Who is responsible for the remediation of any vulnerabilities that are found?
- How often will assets be evaluated?
- How and when are the results being communicated?
- What are the standard remediation timelines?
- How are exceptions handled?
- How is success measured?
- What metrics will be tracked to make sure the program is working?
- When are the metrics being reviewed?
- Who is the owner of each metric?
- Does the business need to adhere to any special regulations that will impact the program (PCI, SOX, HIPAA, etc.)?

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

(tw-gd-0424-r1-hm)