FORTRA™

WHITE PAPER (TRIPWIRE)

Building a Mature Vulnerability Management Program

An enterprise vulnerability management program is able to reach its full potential when it is built on well established foundational goals that address the information needs of all stakeholders, its output is tied back to the goals of the enterprise, and there is a reduction in the overall risk of the organization. Vulnerability management technology can detect risk, but it requires a foundation of people and process to ensure that the program is successful.

There are four stages in building a mature vulnerability management program:

1. The process that determines the criticality of the asset, the owners of the assets, the frequency of scanning, and the timelines for remediation
2. The discovery and inventory of assets on the network
3. The discovery of vulnerabilities on the discovered assets
4. The reporting and remediation of discovered vulnerabilities

The first stage focuses on building a process that is measurable and repeatable. Stages two through four focus on executing the process, with an emphasis on continuous improvement.

Stage 1: The Vulnerability Scanning Process

The first step in this stage is to identify the criticality of the assets in the organization. To build an effective risk management program, one must first determine what assets the organization needs to protect. This applies to computing systems, storage devices, networks, data types, as well as third party systems on the organization's network. Assets should be classified and ranked based on their true and inherent risk to the organization. Many facets need to be considered in developing an asset's inherent risk rating such as physical or logical connection to higher classified assets, user access, and system availability. For example, an asset in the DMZ with logical access to an account database is going to have a higher criticality than an asset in a lab. An asset in production is going to have a higher criticality than an asset in a test environment. An internet-routable web server will have a higher criticality than an internal file server. However, just because an asset is a lower criticality, remediation on that asset should not be ignored. The remediation effort should always be based in relation to overall risk.

The second step is to identify the system owner(s) for each system. System owners are ultimately responsible for the asset, its associated risk, and the liability if that asset becomes compromised. This step is critical in the success of the vulnerability management program as it drives the accountability and remediation efforts within the organization—if there's no one to take ownership of the risk, there won't be anyone to drive remediation of that risk.

The third step is to establish the frequency of scanning. The Center for Internet Security in their CIS Controls recommends that an organization should "run automated vulnerability scanning tools against all systems on the network on a monthly or more frequent basis." Advanced vulnerability scanners even release vulnerability signature updates on a weekly bases to keep customers as up-to-date as possible.. Scanning this frequently allows the owners of the assets to track the progress of remediation efforts, identify new risks, and reprioritize the remediation of vulnerabilities based on any new intelligence gathered. When a vulnerability is first released it may have a lower vulnerability score because there is no known exploit. Once a vulnerability has been around for some time, an automated exploit kit may become available which would increase the risk of that vulnerability. A system that was once thought to not be vulnerable may become so due to new software installed or a patch roll back. There are many factors that could contribute to the changing of an asset's risk posture. Frequent scanning ensures that the owner of the asset is kept up to date with the latest information. As an outer limit, vulnerability scanning should occur at least monthly.

The fourth step in building this process is to establish and document timelines and thresholds for remediation. Vulnerabilities that are able to be exploited in an automated fashion that yield privileged control to an attacker should be remediated immediately. Vulnerabilities that yield privileged control that are more difficult to exploit or are currently only exploitable in theory should be remediated within 30 days. Vulnerabilities lower than this can be remediated within 90 days. In the event of a system owner being unable to remediate a vulnerability within the approved time frame, a remediation exception process should be available. As a part of this process, there should be a documented understanding and acceptance of the risk by the system owner along with an acceptable action plan to remediate the vulnerability by a certain date. Vulnerability exceptions should always have an expiry date.

Stage 2: Asset Discovery and Inventory

This and the following stage primarily occur using the organization's technology of choice for vulnerability scanning. In this case the discussion will focus around Fortra's vulnerability management solutions.

Asset discovery and inventory accounts for Critical Security Controls (CSC) one and two. These are the foundation for any security program—information security or otherwise—as defenders can't protect what they don't know about. CSC 1 is to have an inventory of all authorized and unauthorized devices on the network; CSC 2 is to have an inventory of authorized and unauthorized software installed on the assets on the organization's network.

These two controls go hand in hand as attackers are always trying to identify systems that are easily exploitable so they can get into an organization's network. Once they're in, they can leverage the control they've gained to attack other systems and further infiltrate the network. Ensuring that the information security team is aware of what's on the network allows them to better protect those systems and provide guidance to the owners of those systems to reduce the risk those assets pose.

There have been many cases where users deploy systems without informing the information security team. These could range from test servers to wireless routers plugged under an employee's desk. Without the appropriate asset discovery and network access control, these types of devices can provide an easy gateway for an attacker into the internal network.

Fortra's vulnerability management solutions conduct asset discovery within defined ranges, as well as discover which applications are running on those assets prior to conducting a vulnerability scan.

Stage 3: Vulnerability Detection

Once all the assets on the network are identified, the next step is to identify the vulnerability risk posture of each asset. Vulnerabilities can be identified through unauthenticated and authenticated methods. Typically, an attacker would view a system with an unauthenticated view. Therefore, scanning without credentials would provide a similar view to a primitive attacker. This method is good for identifying some extremely high-risk vulnerabilities that an attacker could detect remotely and exploit to gain deeper access to the system. There is, however, a higher likelihood for false positives as it is very difficult to validate the presence of a vulnerability without exploiting it.

A much more comprehensive and recommended method for vulnerability scanning is to scan with credentials. This allows for increased accuracy in the determination of the organization's vulnerability risk. Vulnerability signatures specific to the operating system and installed applications that were detected in the discovery and inventory stage are run to identify which vulnerabilities are present. Vulnerabilities in locally installed applications can only be detected with authenticated scans. An authenticated Fortra vulnerability scan also identifies vulnerabilities that an attacker would see from an external unauthenticated vulnerability scan.

Many vulnerability scanners simply detect the patch levels or application versions to provide a vulnerability posture reading. Fortra's vulnerability management solutions provide a much more detailed analysis as the vulnerability signatures are able to determine factors such as the removal of vulnerable libraries, registry keys, and whether or not a reboot of the system took place for the remediation to apply.

Stage 4: Reporting and Remediation

Once the vulnerability scan is complete, a score is attached to each vulnerability using an exponential algorithm based on three factors:

- The skill required to exploit the vulnerability
- The privilege gained upon successful exploitation
- The age of the vulnerability

The easier the vulnerability is to exploit and the higher the privilege gained, the higher the Fortra risk score will be. In addition, as the vulnerability age increases the vulnerability score also increases.

The first metric that should be taken is an overall baseline average risk score for the organization. Successful Fortra vulnerability management customers start by targeting a risk reduction of 10% to 25% year over year. As the program matures, a target risk score can be set for the organization to achieve. In the initial years, an average risk score per asset of below 5000 is a good target. Most mature organizations strive to have even lower averages, and focus on addressing any single vulnerability with a score higher than 1000.

The next metric that should be taken is the average risk score by owner. The ownership of assets was identified in the first stage, therefore, each owner should be able to see the baseline risk score for their assets. Similar to the target for the overall organization, each owner should target reducing their average risk score by 10% to 25% year over year until they're below the accepted threshold for the organization. System owners should be able to view their scores in comparison with other system owners to create a sense of competition among their peers. Those who have the lowest scores should be rewarded for their efforts.

In order to drive remediation, system owners need empirical vulnerability data to outline which vulnerabilities should be remediated along with instructions of how to conduct the remediation. Reports should outline the most vulnerable hosts, the highest scoring vulnerabilities, and/or reports targeting specific highly vulnerable applications. This will allow the system owners to prioritize their efforts with a focus on the vulnerabilities that will reduce the most amount of risk to the organization.

As new vulnerability scans are run, the metrics from the new vulnerability scans can be compared to the previous scans to show trending analysis of the risk, as well as remediation progress.

Some metrics that can be used to track remediation are:

- What is the average vulnerability score of each asset by owner, and overall?
- How long does it take, on average, to remediate infrastructure based vulnerabilities by owner, and overall?
- How long does it take, on average, to remediate application based vulnerabilities by owner, and overall?
- What is the percentage of assets that haven't recently been scanned for vulnerabilities?
- How many remotely exploitable vulnerabilities yielding privileged access are exposed on systems?

It's not uncommon for an organization in the initial stages of building the program to have a very high average vulnerability score with lengthy remediation cycles. The key is to show progress month by month, quarter by quarter, and year by year. The vulnerability risk scores and time to remediation should decrease as teams become more familiar with the process and become more educated on the risks that the attackers pose.

Conclusion

Vulnerability and risk management is an ongoing process. The most successful programs continuously adapt and are aligned with the risk reduction goals of the cybersecurity program within the organization. The process should be reviewed on a regular basis and staff should be kept up to date with the latest threats and trends in information security. Ensuring that continuous development is in place for the people, process and technology will ensure the success of the enterprise vulnerability and risk management program.

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.