CORE SECURITY

Best Practices for Threat & Vulnerability Management

Don’t Let Vulnerabilities “Monopolize” Your Organization

March 2016

Table of Contents

Are You in the Lead?

Avoid making the same wrong moves that allow attackers to win. Vulnerability exposure, elimination, and control require management.

Are your critical assets really that secure?

While the need to manage and analyze risk has existed for some time, a "new era" of cybercrime may be causing you to question your current vulnerability management practices.

Are traditional vulnerability management solutions enough?

To find out, start with the basics.

A vulnerability can be defined as a defect or bug that allows an external entity to directly or indirectly influence the availability, reliability, confidentiality or integrity of a system, application, or data.

New vulnerabilities appear daily because of software flaws, faulty configuration of applications, and human error. When discovered, these can be exploited, resulting in erratic program behavior, illicit network entry, privacy violations, and interrupted business operations.

Why risk it?

Remember:

Risk knows no boundaries.

How much risk is acceptable to your organization?

It doesn't matter if you're a small business, a large corporation, or a government entity–every organization with an Internet connection is at risk.

New vulnerabilities are discovered each day and the speed at which these new threats are created makes securing your critical assets even trickier. The solution is to quickly immunize your infrastructure from these threats by eliminating their foundation: vulnerabilities.

> *"44% of breaches are due to known vulnerabilities that are two to four years old."*
>
> *—HP Cyber Risk Report*

A Winning Vulnerability Management Program

Stop! Too much data:

Remember: Too much vulnerability data is a problem when building any sort of risk assessment. In many organizations there are no effective processes in place to consolidate and prioritize results.

A Holistic Defense:

Most attacks today incorporate multiple steps, crossing different vectors (Network, Web, Mobile, Wireless, Endpoint). An isolated view of any of these steps could appear harmless – causing a potentially drastic oversight.

Here are a few best-practices to keep in mind when maturing your own vulnerability management program.

Winning vulnerability management programs have evolved to include additional solutions and workflow beyond scanning, adding to a larger picture required to truly understand how an adversary could, and will, attack.

Most organizations use traditional scanning to uncover vulnerabilities, but this approach is often a flop – too much data is a problem. IT security teams are drowning in data, producing the infamous "300-page report" with a mind-numbing table of vulnerabilities and no business context, risk prioritization, or actionable quick fixes.

Once the data is prioritized, automating the analysis of the vulnerabilities will allow remediation efforts to focus on critical risks and not waste time and resources chasing low-risk assets.

Create a short list of action items that can be completed quickly to reduce and eliminate the risk of exploitation.

There are two approaches:

1. **Asset Categorization and Prioritization:** An approach that helps determine whether the vulnerability is threatening an important system and what will happen if it is exploited.
2. **Attack Path Analysis:** An approach that demonstrates how attackers can chain vulnerabilities across vectors to move through your environment.

An effective vulnerability management program is nearly impossible to do manually. Organizations need to simplify each element of their programs to win.

Don't let vulnerabilities win. How do you determine which are critical and which aren't?

Vulnerability Management's Seven Primary Objectives

These are the seven simplified objectives of any successful vulnerability management program.

1. Discover and categorize your assets

In order to manage vulnerabilities, you must understand what assets you have in your network and then test to find any vulnerabilities that exist. This is done by creating and continuously maintaining a database of all IP devices attached to your network. Scanning is most often done by focusing on a particular IP or range of addresses, therefore, organizing your database by IPs is more effective.

2. Identify assets based on business risk

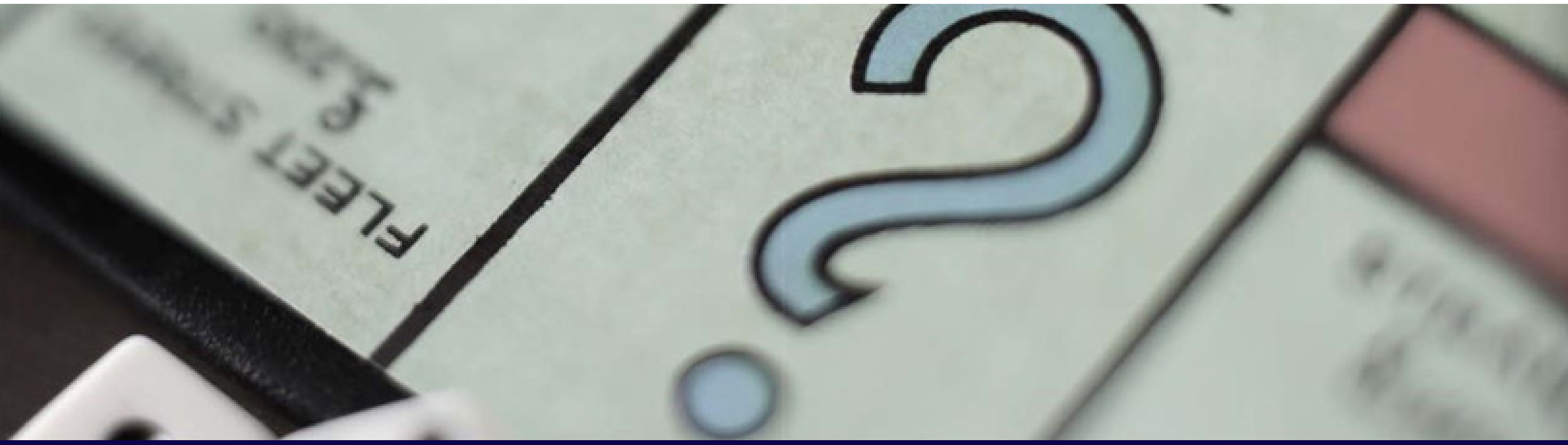
Now that you have a big-picture view of your assets, where they reside, and how they are categorized, it's time to prioritize. It is important to isolate critical assets that have a direct impact on business risk — such as a database that contains social security numbers or credit card information.

3. Scan for vulnerabilities

Scanning is the foundational process for finding and fixing network vulnerabilities. Traditional vulnerability scanners are isolated from each other, each collecting their own set of vulnerabilities, resulting in a data overload. Scan results should be consolidated and normalized into a unified repository.

Remember:

Too much vulnerability data is a problem when building any sort of risk assessment. In many organizations there are no effective processes in place to consolidate and prioritize results.



4. Prioritize vulnerabilities

Traditional vulnerability management solutions often produce thousands of “high severity” vulnerabilities for the operations staff to remediate. This scan data overload leads to confusing priorities and complicates remediation efforts. Prioritization based on previously defined critical assets, exploit types, and business risk, among other things, can help reduce this overload.

5. Generate attack paths to high-risk assets

Attack paths reflect the ability to understand not only where the critical assets are, but also what the topography around those assets looks like considering vulnerabilities, exploits, network configurations, and potential attacker patterns. This will help define exposure points that should be locked down along with any other areas of the network that could lead an adversary to your critical data.

6. Remediate. Patch. Monitor.

As these areas have been defined, they should be shared with other constituents. Strong reporting at all levels within the organization is required for risk reporting, trending, compliance efforts, remediation efforts, and overall business risk. The data discovered by scanning, consolidating, prioritizing, and modeling attack paths should be translated into tangible remediation tasks for IT Operations through service desk tools or patch management.

7. Validate

Validation is extremely important and often overlooked. Since remediation responsibilities usually fall on a different team than information security, remediation validation is an important step for closing the loop. These validation efforts should output to a report, comparing new results with original results, to ensure the vulnerabilities have been addressed.

“Scanning isn’t your get out of jail free card.”

What's Next?

- Gather your team and plan your program
- Create processes to collect, analyze, and act on threat data
- Measure risk to critical assets
- Start prioritizing threats