A GUIDE BY
FORTMESA

RESEARCH CATEGORY
USING VULNERABILITY INSIGHTS TO REDUCE CYBER RISK

VULNERABILITY MANAGEMENT 101

The all-in-one guide on how to stop attacks before they start using vulnerability management

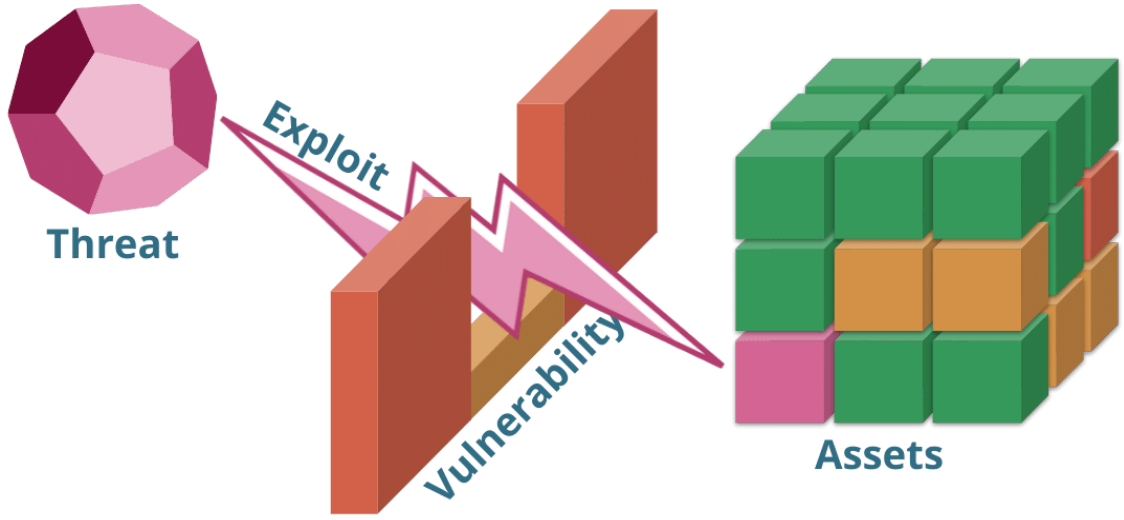


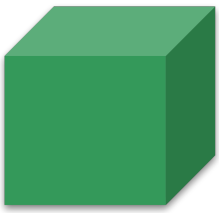
Table Of Contents

Introduction

Before you can understand the nature of vulnerability management it is first necessary to understand some related cyber risk concepts. Let's start with a quick overview of concepts.

Definitions

Assets



An "Asset" is anything that is valuable, this is the thing you're trying to protect.

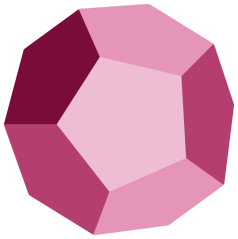
In cyber we usually mean Data, Software or an IT component such as a physical device. An asset might also be an entire IT system (or collection of systems) such as "Payroll", it might also be part of an outsourced business function like "Stripe" (or another payment processor).

Vulnerability

A vulnerability is a weakness in your asset or asset protection, this is the opening allows an attacker in.

When evaluating cyber risk we look at different types of vulnerabilities. Some are inherent in the way a system is designed or operated. Others exist due to weakness in how an overall system is designed or configured. The most pernicious are software vulnerabilities because they exist everywhere and are newly discovered every day. A well designed system can be secure on a Friday and an open door by Monday when a vulnerability is found in a critical asset.

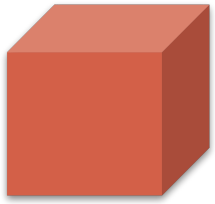
Threat



A threat is any circumstance or actor that could have a negative impact on an asset, if not stopped in some way.

Most people are aware that threat actors exist in the form of cybercriminals or even nation states that through persistent effort or sophisticated methods can subvert cyber systems to make money or cause other mischief. A threat actor however can include other situations such as accidental data loss, fire damage, or all too frequently a disgruntled or unwitting insider.

Loss



A loss is a negative impact or consequence of damage or compromise of an asset.

Typically expressed in dollars, a loss measures the damage or cost of impact. Human time, reputational damage, and lost productivity can be particularly difficult to quantify and thus losses are just as often ignored or accepted as cost of doing business (this is the most expensive way to manage).

Exploit

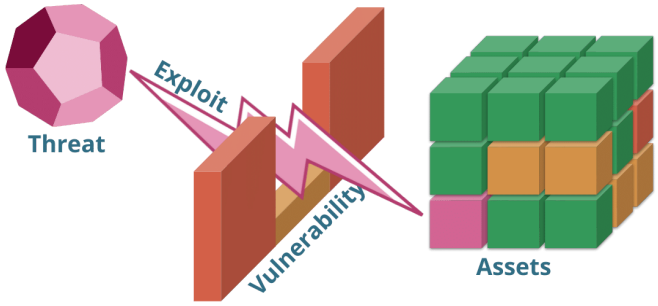
An exploit is the act that leads to compromise and/or loss of an asset.

An exploit is the action a threat actor or agent uses to take advantage of a vulnerability. Though technically this is a verb, it is also common to refer to specific pre-packaged code as “an exploit” (noun).

Why Vulnerability Management?

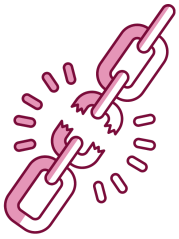
The Attack Chain

Let's put all the above concepts together into a form that makes practical sense.



A Threat actor uses an Exploit to leverage a Vulnerability and create a Loss in an Asset.

Cyber professionals have a whole universe of highly specialized technical definitions and concepts just to describe attack chains for security analysis. The MITRE ATT&CK Framework is the predominant leader in this space and is intended as an up-to-date observation-based knowledge base of adversary tactics and techniques.



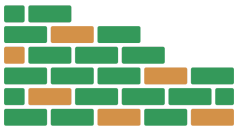
Breaking Attack Chains

A loss can be prevented by breaking the attack chain and therefore stopping a threat from acting.

The Defender Advantage

Since the attacker needs a series of circumstances or actions in a chain to create a loss, breaking the chain in any location can stop the attack.

The Attacker Advantage



To the advantage of the attacker, a defender needs to succeed in protecting every angle to stop an attack, and an attacker only needs to succeed once. There are many routes that can be used to create an attack chain.

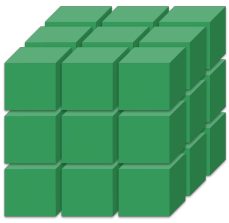
Effective Defense

An effective defense requires identifying the assets that need to be defended (asset management), then discovering and eliminating weaknesses that can compromise those assets (vulnerability management).

Since essential cyber hygiene gained from asset and vulnerability management are the most cost effective measures (most bank for the buck), security architects and compliance standards all rate these functions as high priority essential functions.

How Vulnerability Mgt. Works

Asset Management



Quick Side Note About Assets

Asset management is its own topic and highly effective security requires more consideration here.

In simple terms just understand that you can't defend what you don't know about. You need to make a list of what you're trying to defend before you can measure risk or take defensive action.

For those of you considering implementing vulnerability management, you're in luck. Many vulnerability management tools are paired with basic asset management features, and this is good enough for many organizations.

Discovering Vulnerabilities

Both attackers and defenders discover vulnerabilities using automated tooling.

How Attackers Do It

Attackers utilize discovery tools with the intent of leveraging exploits they have access to via vulnerable software.

Open-source scan tools such as NMAP do a good job of looking for vulnerable versions of known software. More sophisticated scan and attack automation tools like the open-source tool Metasploit are also common. A whole constellation of freely available attack tooling exists on the open web, while crimeware vendors operate illicit commercial subscription software ventures on the darkweb.

If you've ever watched a firewall log for a day you'll have seen a constant bombardment of this type of scan traffic.

How Defenders Find Vulnerabilities

Defending from a continuous bombardment of attack against external internet surfaces, malicious webpages or ads, or phishing attacks requires scanning for vulnerabilities everywhere as frequently as possible.

In previous times an enumerative vulnerability scan sometimes called an "external penetration test" or "public IP scan"

was best practice. These tests were commonly combined with the annual risk assessment cycle.

Since new vulnerabilities are discovered every day, best practice is now daily or weekly scanning. This means it is necessary to deploy sensors that continuously monitor assets for vulnerabilities (and not wait around for the auditors to show up).

This gives the defender a chance to patch a newly discovered vulnerability within a remediation SLA (such as 14 days) or faster when required.

About Vuln Scanners

Vulnerability scanners are built in a two-part architecture that should be familiar to anyone who has installed antivirus applications, a scanner and a scan database. Most vulnerability scanning solutions combine these two technologies into a single product (but this is not always the case).

Unlike antivirus scanners, US NIST has standardized both the scanning technology and data feeds in a way that makes these products easier to compare. All modern vulnerability scanners leverage the same Security Content Automation Protocol (SCAP) specifications designed and tested by NIST.

Vulnerability Checks (SCAP Feed or OVAL Data)

The cybersecurity industry collectively researches and trades in standard tests for software vulnerabilities. While all feeds that include a specific test should test equally, not all feeds have all tests.

Some SCAP data is freely available via the US NVD, but unlike CVEs (human readable reports of a vulnerability discovery) SCAP data has a high commercial value and as such vulnerability scan products have varying levels of access to these tests.

The best feeds are aggregated from as many sources as possible through license and information sharing agreements that would be impossible for individual organizations to acquire themselves. The quality of the feed should be a determining factor in what vulnerability scanner you select.

Scan Engine or Agent (SCAP Validators or OVAL Scanners)

While there are open source and freeware SCAP Validators, they should be referenced for research or academic use only. Real world environments have diverse environments and uniquely commercial

functionality is required to cover the operating systems, device types, and software platforms encountered in the wild.

Network Scans (Unauthenticated Scans)

Network scanners are run from sensors that are configured with unlimited access to the target network. These tools scan the entire network address space looking for target systems, then enumerate exposed services on each system to find vulnerabilities that are visible from the outside.

A network scan is important because it can find unknown devices, and can scan devices that do not support more advanced scan types. While it's recommended that everyone deploy network scanners, it's important to note the scan should be from the inside to find vulnerabilities across the network (not just at it's edge).

Agent Scans (Authenticated Scans)

While an authenticated scan can be implemented in agentless fashion, regardless of method it's important that data is collected from inside a device (not just it's network surface). This can be done by distributing remote admin credentials to your network scanner, or more safely and commonly using locally installed scanning agents.

An authenticated scan, because it has local access, can find all software on the system and check it for vulnerabilities. This is necessary because some vulnerabilities are not network scannable (such as an old version of Chrome that can be hijacked via a malicious ad), or a network service or website that can't be distinguished as vulnerable or not-vulnerable from the outside.

Other Scans

When it comes to finding vulnerabilities it is not always possible to design standardized tests. Organizations with self-engineered or otherwise bespoke software systems may need to have their source code inspected on a regular basis. Organizations should consider whether they need to implement a static (SAST) or dynamic (DAST) source code analysis tool.

Using Vulnerability Knowledge

You've Got A Vulnerability Inventory

Okay so you've managed to deploy vulnerability sensors and you are now collecting a vulnerability inventory.... Now what?

If you're like most organizations and you're new to this game you'll find many hundreds or just as frequently many thousands of vulnerabilities across your devices and network.

The first few weeks or months after implementing a vulnerability management system will be a triage effort of eliminating the most risk with the littlest amount of effort.

You'll probably find that your list dwindles quickly as you address:

- Turning on automatic updates (because it's never as automatic as you thought it was)
- Removing old software (because cruft tends to collect, and the easiest way to address it is to exorcise it)
- The absolute most glaring critical issues that require manual intervention

It's a Big List - How To Begin

After a first pass of cutting the list down in size using those methods you're still going to be overwhelmed with vulnerabilities that require manual action and this is where you want to start looking at how to prioritize a remediation project.

Asset Criticality

The first thing you should always look at is your highly critical systems (if you have any). If you're already doing a good job of asset management you already know what systems are critical. If you have not yet just ask yourself, is there a system that would be world ending if it was compromised? More than one?

Do you have any critical assets? Carefully clean these up first.

Unfortunately even if you only care about your critical assets, you can't stop there. Your other systems ultimately will interact with critical systems, and thus you need to make sure to keep the whole house in hygienic condition.

CVSS Scoring

The Common Vulnerability Scoring System (CVSS) was standardized by a Special Interest Group of the Forum of Incident Response and Security Teams. Adopted universally by products and security organizations worldwide CVSS provides a way to objectively classify "just how bad is it".

While CVSS scores provide more information for specialized security analysts, the base score (or "CVSS Score") is a simple number from 0 (informational only) to 10 (the barn door is wide open). CVSS Scoring is the most widely used method to prioritize vulnerability management

CVSS Base Scores can be simplified even further:

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

EPSS Scoring

You could just fix every vulnerability the day it is discovered of course, but most organizations find this goal not economically viable.

Also developed by a FIRST SIG (just like CVSS), EPSS leverages machine analysis of what's currently known about every CVE, then factors in real world threat data found by security organizations all over the planet to generate a predictive model of how likely a particular vulnerability is to be exploited, and how that likelihood relates to all other CVEs.

It's been estimated that by combining EPSS and CVSS scoring in remediation efforts, remediation efforts might be cut by as much as 78%.

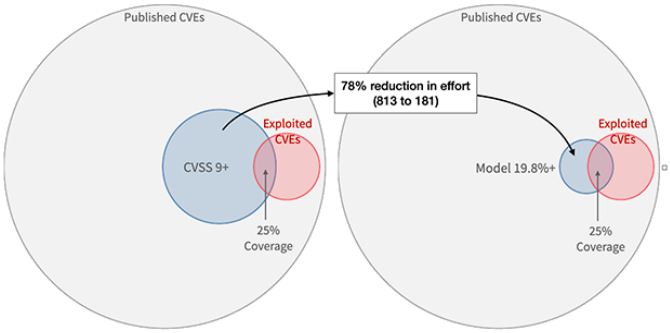


Figure courtesy of the EPSS SIG

Learn more about EPSS and why it's joining CVSS in a triage scoring club of 2.

Sometimes, the scanner is wrong

It's rare, but sometimes after a deep dive on an issue a technologist will discover the vulnerability does not in fact apply.

This should never be confused with "we don't think it's very risky" and should be reserved specifically for actual errors in detection logic.

In these cases the technologist and/or security officer or engineer should document the exception and exclude it from the scan results.

It's OKAY to "Wont-fix" ... but

Accepting Risk must be formalized

Running any organization is a giant risk management exercise. A zero risk business would have no revenue.

It's perfectly okay to decide you've identified a problem and you're not going to fix it because it would be too costly or damage the business in some way. Making this decision is called "Risk Acceptance" and is happily endorsed by auditors everywhere.

It's important however not to confuse "Risk Acceptance" with a related but totally unacceptable concept called "Risk Ignorance".

Formalizing a Default Risk Accept

Organizations may with approval of the Chief Information Security Officer (CISO or ISO) identify a level of risk they accept by default, such as vulnerabilities with a CVSS of less than 5.

Accepting Individual Vulnerability Risks

To adequately accept that exceeds the organization's default SLA:

- A system owner (or business owner) responsible for the business value or who would be most affected by a loss should formally take responsibility for the "wont fix". The system owner must confirm they are taking responsibility and they have been adequately informed on the potential impact.
- A technical or security professional should work with the system or business owner and make sure they indeed have been coached.
- When both parties agree this is risk acceptance, and it should be documented.

Other Stakeholders

It's important to note the system or business owner is not the only system stakeholder, and risk rolls uphill.

A business process owner (such as Payroll Manager) is responsible for the entire payroll systems, and would automatically assume the risk accepted by a timesheet clerk. If the payroll manager disagrees with assuming this risk they must negotiate with their clerk to get the issue resolved. The Payroll Manager probably reports to the CFO or HR Director, and as department heads one of them also assumes this risk and the responsibility be held accountable for the risk accepted by their employees.

All risk eventually rolls up to the chief executive (such as CEO), and cannot be delegated. The CEO is after all ultimately responsible for the business.

While it's true there will be systems that are designated as IT owned, if all your risk is sitting in the IT department your organization is not demonstrating acceptable enterprise risk management practices. IT is probably only the custodian for most systems, and the risks and benefits should accrue to individual business lines.

Vulnerability Management For The Win

Success in vulnerability management is most commonly measured by how well your organization complies with the target SLA (and how aggressive the SLA is).

After you've completed initial triage and introduced your teams to the vulnerability

management workflow it is possible to set a Vulnerability Management SLA (Service Level Agreement).

Here's an example:

Management SLA	CVSS Default Risk Accept
Vulnerabilities are remediated or accepted within 14 days	Accept vulnerabilities with a CVSS score of less than 5.

This SLA may be modified over time. Consider a good starting place might be an initial SLA of 30 days with a default accept of vulnerabilities below 9. As your organization continues to mature and invest in it's vulnerability management practice the SLA can be gradually lowered to decrease risk over time.

Next Steps

What is Enough Security?

It's never possible to eliminate 100% of risk, so businesses must accept some risk of failure or loss.

It is reasonable to accept residual risk when you've covered all the commercially reasonable best practices in your industry for a company of your size.

Risk Assessment is Mandatory

One practice you can't reasonably skip is some sort of risk assessment. It's mandatory because you cannot reasonably say you have enough security if you have not studied what risks you face and evaluated whether your practices provide sufficient risk reduction.

Adopting A Cyber Compliance Framework

There are many security standards worth considering and choosing one deserves it's own article. It's important to note however choosing a compliance framework is also in the mandatory category because:

- A standard framework ensures your security dollars are distributed in an effective way. It does no good to build a 20 foot castle wall then leave the side door open. All good security standards address this by helping you target a level of investment first, and then instructing you how best to deploy your resources.
- Formalizing your security on a standard compliance framework also lets you communicate credibility to stakeholders inside and outside your organization. By letting others know what framework you are following you are signalling the approximate maturity of your security without disclosing details that an attacker could leverage.

Cyber Hygiene Eliminates The Most Risk

If you've done a good job of implementing cyber hygiene you've already eliminated most of your risk, and laid the necessary foundations of more advanced defensive measures.

Advanced Security

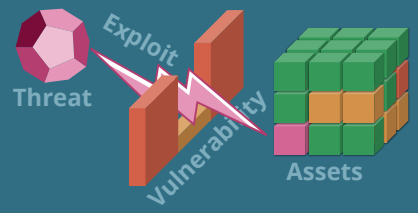
For organizations with the appetite to use sophisticated and expensive methods to stop even more risk, it's time to consider other compensating controls such as real-time anomaly detection, ongoing forensic analysis, and retained incident response specialists.

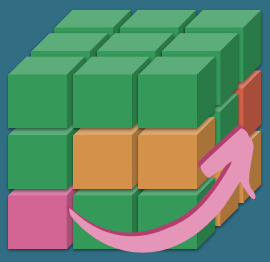
All of these methods require the groundwork achieved by implementing cyber hygiene, so if you are not yet performing effective vulnerability management make sure to go back and do that first.

What is Vulnerability Management?

The Attack Chain

A threat actor exploits a vulnerability to attack an asset.





Attackers chain multiple vulnerabilities and exploits to reach a target.

After gaining a foothold, an attacker can move across systems.

Your security surface has vulnerabilities

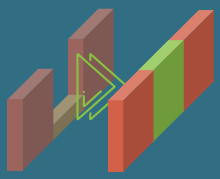
Vulnerabilities exist in:

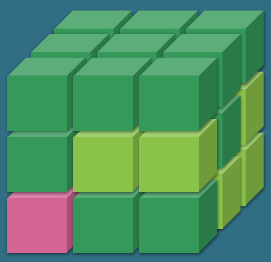
- Perimeter systems
- Anything that reads email
- Any device used to browse the web
- Any system that downloads software
- Any company you exchange data with

Breaking The Attack Chain

When you fix a vulnerability, it can no longer be exploited.

Effective vulnerability management stops attacks by breaking the attack chain.





Find them
Scan systems and networks

Don't stop at the surface
It's critical to scan inside systems with authenticated agents

Make a list
Inventory and triage

Low risk vulns can often be accepted, others are remediated with a fix or compensating control.

Fix It

A technical custodian can remediate the vulnerability with a patch or config change.

Accept The Risk

If nothing is done, this is the default.

A functional business leader accepts responsibility for risk.

A smart business leader should make informed decisions.

Deploy A Control

With engineering time or security product spend, compensating controls can harden systems to eliminate risk.

Glossary

Vulnerability
A weakness in an asset or protection

Threat
A threat is any actor that can cause losses

Exploit
Action or code used by a threat to create loss

Asset
This is the thing with value you're trying to protect

Loss
Negative impacts that damage asset value