FORTRA

Taking Back Control:

A Proactive Approach to Advance Your Security Maturity

Taking Back Control: A Proactive Approach to Advance Your Security Maturity

After countless headlines, government alerts, and warnings from experts, the message could not be any clearer: threats to cybersecurity are on the rise. There are more cyber criminals than ever, and they're growing bolder. For example, it is estimated that a ransomware attack occurs every 11 seconds, and a record payout of $50 million was made in the summer of 2021. With news like this, it's easy to get discouraged. Should we simply resign ourselves to focusing on how to recover from an inevitable attack?

While it's important to be prepared for all circumstances with reactive solutions and processes, adding a proactive approach to your cybersecurity strategy can help anticipate attacks, enabling you to stay flexible and adapt to address new attack vectors and an ever-changing threat landscape. Infrastructure protection focuses on staying one step ahead of attackers with actionable insights that help to identify and prioritize risk, providing a pathway to remediation and bolstered security. In this guide, we'll go over different facets of a proactive strategy, highlighting the unique strengths of vulnerability management, penetration testing, and Red Teaming, as well as how they work together to help organizations close gaps in their security before an attacker even attempts a breach.

A Sample Model for Maturing Your Security

Implementing a vulnerability management program cannot and should not be done overnight. While it's easy to get overwhelmed by everything that vulnerability management programs can entail, the maturity process can be broken into steps so you can sustainably maintain growth. First, it's important to take a step back to figure out where you are in the process before deciding how to gradually move forward.

Advancing your vulnerability management program may be a journey, but it's one well worth taking. The more your program matures, the better your organization can avoid costly attacks and breaches that may harm your business and reputation. Though it may look slightly different to everyone, the following Threat and Vulnerability Maturity Model can help give an idea of what a roadmap may look like, with each level progressively leading to an understanding of how you may be attacked and exploited, as well as effective methods of countering adversaries.

Level 0: Non-Existent

No vulnerability scanning, manual vulnerability assessments, sporadic patching, few processes in place, no metrics

Many companies still find themselves with no real strategy for tackling vulnerabilities. This can happen for any number of reasons— some companies have focused primarily on reactive defenses like antivirus, while smaller companies may not have resources for anything but manual patching. No matter the size of your organization, ad hoc vulnerability management is not sufficient or structured. The way to advance out of a non-existent program is straightforward. Organizations will need to begin regular vulnerability scans, either with a tool, service, or both. Scans should cover web and network vectors, as well as checks for device misconfigurations.

Level 1: Scanning

Sporadic vulnerability scans, essential patching, basic processes, simple metrics

With the addition of vulnerability scanning, organizations will have a lot of new information on their hands. They'll be able to see how vulnerable their IT environment is and get a sense of what types of risk they may be facing. However, this information only has value if you do something with it. To progress to the next level, you'll need to begin shaping a strategy for next steps after scans are complete, such as remediation plans and follow up scans. Additionally, a key part of an effective security strategy is looking at industry best practices and compliance. Nearly every industry today has regulatory requirements and security mandates that organizations in that sector must comply with.

Level 2: Assessment & Compliance

Using regulatory framework as a baseline, scheduled vulnerability scans, patching lifecycle, more complex processes, little measurability

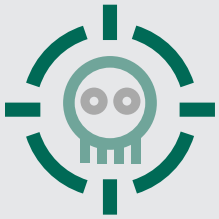
Organizations at this level have gone from a largely makeshift approach to a structured security strategy that uses regulations or industry best standards as a guide to fully build out a vulnerability management framework. For example, the Payment Card Industry Data Security Standard (PCI DSS), which applies to any organization that stores, processes, or transmits cardholder data, sets a timeline for patching and requires scans to be run on a quarterly basis, as well as when significant changes occur in the network.

Once at this level, organizations should also consider running basic penetration tests, which can help prove adherence to regulations and validate any remediation measures, such as patch implementation. Moving onto level three further fleshes out the program, providing more context to enhance vulnerability risk prioritization.

Level 3: Analysis & Prioritization

Risk-focused, prioritized data analytics, data-driven patching, measurable processes, emerging metrics and trends

While compliance standards are an excellent baseline for security, meeting requirements does not mean you've reached the pinnacle of vulnerability management – often it's the bare minimum. Instead, it enables you to dive deeper into the specifics with further penetration testing, which can add more business context by verifying threat potential, ranking the danger of vulnerabilities based on exploitability within your environment. Moving to the next level involves more insight and strategy, viewing vulnerabilities not just in a single unit or context, but considering the entire attack path that may be used in pivoting across multiple threat vectors.



Level 4: Attack Management

Attacker and threat focused, multiple threat vectors scanned, patching based on risk to critical assets, threat driven metrics and trends

Once at this level, vulnerabilities are seen in the framework of an entire ecosystem of management, from discovery to exploitation to remediation to validation. Attack management uses scan and penetration testing data to identify how a threat actor could move through the system, using different vulnerabilities to gain access to business-critical assets. Prioritization is based specifically on risk to these assets. Additionally, Red Teams may be utilized to simulate a realistic attack scenario, emulating adversaries to test an organization's defensive procedures.

Level 5: Business-Risk Management

Threat and risk aligned with business goals, all threat vectors scanned and prioritized, continuous patching, unified processes

Ultimately, this is the level that all organizations should strive for: a fully developed management program that takes the entire environment into account, analyzing data from vulnerability scans, pen tests, and Red Team engagements; examining metrics to identify trends; using enhanced processes; and implementing remediation techniques. However, it's important not to grow idle. In order to stay at level five, you must continue to validate your program, revisiting processes and tools in order to stay up-to-date with the latest tactics and techniques.

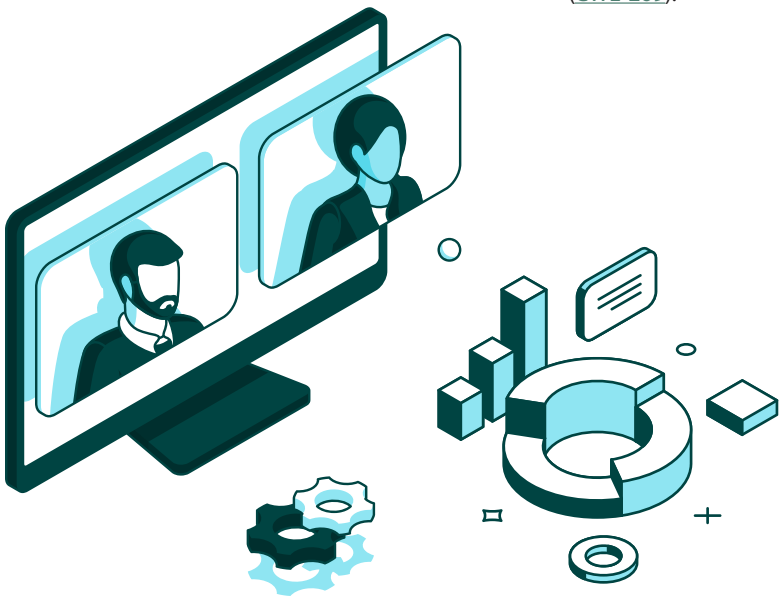
Vulnerability Management

A security vulnerability is a weakness, flaw, or misconfiguration that can be exploited by an attacker to gain initial access to, move laterally within, or escalate privileges in an IT environment. Security vulnerabilities are an endemic part of technology that every organization must constantly do battle with. According to the National Vulnerability Database (NVD), over 19,000 vulnerabilities were discovered in 2020, and over 20,000 were found in 2021. The goal of cybersecurity is no longer an eradication of vulnerabilities, but rather effective management to minimize the attack surface as much as possible. Vulnerability management, which focuses on uncovering these security weaknesses, isn't simply a part of a proactive approach to infrastructure protection, it is critical for the creation of a sturdy foundation for any cybersecurity program.

Classifying Vulnerabilities

Vulnerabilities, which affect hardware and software, can be the result of anything from a flaw in an application to improper configurations to risky end-user behavior. They vary widely in terms of severity— some have very little chance of impacting the system, whereas others may enable an attacker to gain remote access. The Common Weakness Enumeration (CWE) is a community developed, comprehensive list of the hundreds of types of weaknesses, which is unfortunately continuing to grow. Some of the most dangerous software weaknesses can be seen in the sidebar.

In addition to keeping track of different types of vulnerabilities, security professionals also keep track of every unique instance of these weaknesses as they appear in the wild. The Common Vulnerabilities and Exposures (CVE) system is a reference list providing an ID number and a description of specific, known vulnerabilities. For example, CVE-2021-41379 is a privilege elevation vulnerability in Windows Installer. The CVE system has become the standard method for documenting specific vulnerabilities, used by the National Vulnerability Database (NVD) and other databases around the globe. Each known vulnerability can be classified with a CWE ID. For example, CVE-2021-41379 is considered an instance of improper privilege management (CWE-269).



Common Software Vulnerabilities

CWE-787	Out-of-bounds Write
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-125	Out-of-bounds Read
CWE-20	Improper Input Validation
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-416	416 Use After Free
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-434	Unrestricted Upload of File with Dangerous Type

Vulnerability Management Tools

Having effective vulnerability management tools is critical to keeping track of the current security status of an organization. The most common type of solution is a vulnerability scanner, an automated tool that scans network or web applications in order to identify vulnerabilities. While every scanner is different, an effective solution will help to evaluate these vulnerabilities using external intelligence, generating a report which prioritizes them based upon risk and a standardized or proprietary scoring system. Vulnerability scanning is now considered so vital to cybersecurity that it is required for many different compliance regulations, including PCI DSS, HIPAA, and SOX.

Vulnerability management solutions, like Frontline VM, are particularly useful because they can be fully automated and easy to use. Organizations can frequently run scans to get an up-to-date picture of the security of their environment, which can change daily, particularly when software or hardware is being added or updated. Scanners aren't the only vulnerability management tools. Other, more specialized tools can also help to identify security weaknesses. For example, application developers commonly use Dynamic Application Security Testing (DAST) tools, like beSTORM, to perform black box fuzzing, which can uncover bugs through random data injection. They may also use Static Application Security Test (SAST) tools, like beSOURCE, to examine their application's implementation (the source code). This analysis includes a full source code audit (also referred to as a code review).

Penetration Testing

Penetration tests use the same techniques as an attacker to uncover and safely exploit vulnerabilities to determine whether a threat actor could use a security weakness to successfully breach an environment, as well as if they could pivot from this breach to gain access to other parts of the system through privilege escalation or other means. In other words, pen tests measure the feasibility of systems or end-user compromise and evaluate any related consequences such incidents may have on the involved resources or operations.

Once a penetration test has been completed, a report is created that details the level of risk vulnerabilities pose based on how effectively testers were able to exploit them. These reports help to demonstrate the efficacy of defensive mechanisms, as well as end-user adherence to security policies. Additionally, this gives organizations a path forward for remediation.

The Distinction Between Penetration Testing and Vulnerability Management Solutions

Though they are often mistaken as synonymous processes, penetration tests and vulnerability scans have several marked differences. However, they are closely linked and equally essential, as penetration testing builds on the work of vulnerability management, taking the next steps to evaluate the security of an IT environment and further prioritize risk. There are three primary differences between the two security processes:

1. As stated earlier, vulnerability management focuses on scanning for known security weaknesses and prioritizing them based on external threat intelligence. Penetration testing focuses on the exploitation of these weaknesses to see if and how easily an attacker may be able to breach an environment.

2. Vulnerability management tends to be a bit higher level, scanning large portions or the entirety of a security environment. Penetration tests typically limit their scope, homing in on one or two key areas to dive deeper into threat potential.

3. Vulnerability assessments are often run more frequently than penetration tests. If their VM solution is user friendly, organizations can even run them daily to ensure vulnerabilities are not introduced, especially during periods of infrastructure transition, such as systems migrations. Penetration tests typically need a bit more planning done before execution and are consequently run less often.

Penetration Testing Teams

Penetration testing teams can either be in-house or external, third-party services. Oftentimes, larger organizations invest in having a full in-house team to bolster their vulnerability management program with more consistent initiatives, particularly for maintaining compliance. In-house teams can also help to quickly follow through on any remediation measures.

However, expert penetration testers can be a scarce resource, so creating a full in-house team may be quite challenging. In fact, according to the 2021 Cybersecurity Workforce Survey, 60% of study participants reported that the cybersecurity workforce gap is placing their organizations at risk. As a result, it's also common to have smaller security teams that handle basic, routine tests, while third-party services are called upon for more complex tests.

Even those with full in-house teams may call on third-party services for various reasons. For example, it may be difficult for internal IT or security teams to see every problem because, as in everyday life, being habituated to the situation or environment can make it difficult to see the forest for the trees. Pen testing services offer an external point of view, providing a fresh perspective and objectively identifying security issues that may have been overlooked. Additionally, since third-party services are executing penetration tests and other security assessments full time, they can stay up to date on the latest attacks, in addition to providing unique combinations of tactics and techniques.

Penetration Testing Tools

Just as threat actors use tools to swiftly compromise an environment, pen testers utilize a number of tools, like Core Impact, to streamline the process of exploiting vulnerabilities. For example, there are tools that help create sophisticated spear phish for campaigns testing employees' ability to identify such attacks. Other specialized pen testing tools include port scanners, password crackers, SQL injection tools, and Wi-Fi auditors. Other tools may offer multiple features to centralize the testing process.

Some tools can even automate routine tasks so that pen testers can concentrate on more dynamic issues. Such penetration testing tools can be used by security team members who may not have an extensive pen testing background, using them for tests that are easy to run, but essential to perform regularly, like validating vulnerability scans.

Red Teaming

Red Teaming is an offensive exercise which tests an organization's defenses by fully simulating a cyber-attack scenario. The concept of Red Teaming has its roots in military planning, as leaders realized there were circumstances that were not considered in the original planning, but which could jeopardize its success. Confronting the intended approach with unpredictable events is now a recognized method of critical testing. Red Teams translated perfectly to the cybersecurity realm and are used to challenge the strength of cybersecurity programs, particularly their defensive assumptions. These are assumptions the security team has built about how a threat might get in and how they would detect and defend against such an attack.

The Distinction Between Penetration Testing and Red Teaming

While penetration testing does mimic an attacker in the sense that they are trying to gain a foothold or escalate their privileges within an IT environment, the focus is primarily on whether such actions are possible within a specific scope, going more in-depth in fewer areas. Since an actual attacker would not limit their movements to one specific aspect of an infrastructure, a penetration test is limited in how well it represents a threat actor in the wild.

Red Teaming emulates a real-world scenario with a broader scope but clear objectives. These teams take on the offensive role of an attacker who will have to evade detection and beat security controls, including the organization's own security team. While the goal of a penetration test is exploitation, the goal of a Red Team exercise is testing an organization's ability to successfully detect and respond to attacks.

Red Team Scenarios

Just as there are many different types of breaches, there are many different types of scenarios that Red Teams may run. Not all of them begin from the same starting point, and different strategies may be used even when an objective stays the same. However, most engagements fall into one of the following categories:

- **External Breach:** The Red Team takes the role of an attacker who has no access into the organization and must find an initial entry point. One of the most common ways to gain access—both in the real world and during an engagement—is through the use of a phishing campaign, as employees are the most common and reliable attack vector.

- **Assumed Breach:** The Red Team takes on the role of an attacker who is either an internal threat (like a disgruntled employee), or simply an attacker who has already gained access. These engagements tend to focus more on whether the security in place can limit damage after a successful breach, testing their ability to detect and defend against an actor who is pivoting within the system.

- **Embedded Actor:** Some of the most nefarious attacks may be ongoing or take place weeks, months, or even years after an initial breach. Red Teams can take on the role of an Advanced Persistent Threat (APT)—highly skilled attackers who manage to evade detection, entrenching themselves within the environment so they have ample time to complete one or more attack cycles.

Red Teaming Tools

Of course, the biggest asset in Red Teaming is the team itself. The skills a team has and how they work together can directly impact the success of an engagement. These teams can be quite small, even consisting of as few as two people, or can scaled to over twenty members. Ideally, Red Team members should possess different specialties, as a diverse set of skills and backgrounds will help provide coverage for the many scenarios they may be required to run. Additionally, how a Red Team runs engagements also determines its effectiveness. They must have a process that measures and tests the overall security program, determining how capably they can detect and respond to unknown threats.

The impact and effectiveness of Red Teams can be amplified with threat emulation software and attack kits that provide structure to execute a threat plan and the tactics and techniques of an adversary in a network. For example, tools like Cobalt Strike provide a flexible postexploitation framework that can emulate embedded adversaries.

Unified Infrastructure Protection

While individually all of these types of solutions are valuable, they are even more effective when used in tandem. Together, they cover every layer of complexity to create a mature security program and ensure an organization can overcome cybersecurity challenges.

Vulnerability management provides a contextual view of threats so vulnerabilities that are of no real risk can be immediately dismissed so no time is wasted on investigating an innocuous weakness. From there, penetration tests descend into the particulars of the risks that may have been prioritized by vulnerability scanners, figuring out how serious the potential danger is and what remediation is needed. Finally, Red Teams move from theoretical attacks to realistic scenarios, testing the defenses and strengths of security operations. Additionally, many of these solutions integrate with one another, helping to centralize security. As cybersecurity portfolios continue to expand, it is essential to bring as many of them together as possible so security teams don't miss anything due to console fatigue.

A Layered Approach to Cybersecurity

The days of impenetrable cybersecurity are long past us—if they were ever even here to begin with. Instead, the motto "Prevent First, Detect Always" is a better approach towards setting and achieving the goals of security operations. For a security operations team to be successful, they must not only reduce the attack surface through preventative controls but be able to detect and respond to threat activity before serious impact is felt. A proactive approach can serve as the first line of defense in your overall security strategy, providing significant obstacles that make breaking in so labor intensive that the vast majority of attackers, who always look for the easiest wins, won't even attempt it. Ultimately, a well-rounded program of prevention, detection, and response separates organizations that are pushed around by threats from those organizations that push back against threats.

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.

fta-cs-gd-1022-r1-79d