FORTRA

GUIDE (INFRASTRUCTURE PROTECTION)

Guide to Creating a Proactive Cybersecurity Strategy

First responders run drills to make sure they're ready when disaster strikes. They understand the importance of being tested under pressure before an event occurs to ensure their readiness. Security teams should also bear in mind the importance of this readiness, and that proactive assessments and testing are critical to ensuring your organization's preparedness for a cyber attack.

89.7% of organizations in the United States experienced at least one cyberattack within 12 months, according to TechReport.

Attacks are a fact of life now and your organization will experience them. The important question is, will you stop the attack or will the attackers be successful?

The benefit of having a well-developed proactive security strategy is incalculable, and an extraordinary advantage if leveraged correctly. Proactive security is a way to battle-harden your cybersecurity defenses, check for and bolster high-risk weaknesses, stress-test your software development lifecycle, and put your team through their paces so they'll be ready at the onset of an attack.

Creating a full-fledged proactive cybersecurity program used to be the purview of well-resourced companies and the specialists they could afford. But now, thanks to modern security solutions, a robust proactive security stack is available, in all its parts, to organizations of any size, type, and skill level.

Let us show you how.

Proactive Security

Proactive security is the practice of exposing your network, team, software, and security controls to the same types of reconnaissance and attacks they would face if targeted by a real-world adversary. A proactive security approach can be summed up as taking preemptive measures to prevent a breach from happening by preparing your environment to successfully withstand an attack.

This can be broken down into two categories:

- **Offensive security,** or applying these principles to your network, architecture and environment.
- **Application security,** or applying these principles to your software solutions.

Proactive security teams add value to an organization by discovering and prioritizing weaknesses and security gaps before they can be discovered and exploited by threat actors. By mitigating the highest risks first, they help companies make the best, most judicious use of their security dollars instead of wasting them patching, bolstering, and remediating low-level problems that don't represent the most significant risk to the company.

Offensive Security

An offensive security approach entails such activities as:

- **Vulnerability management** | The ongoing process of finding, assessing, classifying, prioritizing, reporting on, and remediating risks and flaws in your network, architecture, environment, and software that could put your organization at risk.
- **Penetration testing** | Also known as ethical hacking, penetration testing validates your system's vulnerabilities (typically, as found in your vulnerability scan) to determine whether they pose a real threat to your organization. The goal of pen testing is to identify the exploitable weaknesses in your environment that can be paths to data breach or compromise.
- **Red teaming** | While penetration tests exploit known vulnerabilities, red team engagements subject your entire enterprise (environment, network, architecture, systems, solutions, devices and people) to a simulated full-fledged cyberattack, using any and every available means necessary to do so (social engineering, APTs, physical access, and more).
- **Overall attack surface management** | Staying ahead of threats is an ongoing process and must be cyclical if it is to be effective. Attack surface management means repeating the above steps to scan the environment for new threats on a regular basis – because new devices, software, and applications are constantly being introduced – so as your environment changes, your knowledge of your attack surface and ability to secure it will keep pace.

These offensive security components can work alone or in tandem, but to truly stay on top of new attack vectors, a defense-in-depth approach using all proactive technologies is needed.

Application security

Application security applies the same overarching proactive security principles of discovery, prioritization, and mitigation to the software development lifecycle (SDLC). The CIS Controls cover numerous ways in which organizations can secure the code, data, and various moving parts within their software products, including:

- Secure coding practices
- Developer training
- Vulnerability management
- Securing third-party code

And application security testing procedures, such as SAST and DAST. While these will be covered more in-depth later in the Guide, SAST tests the source code of an application for vulnerabilities while DAST tests without access to source code, attacking the application like a malicious actor would. DAST can include Black Box fuzzing to find implementation bugs. It tests the software at the end of its development cycle, right before it ships.

Critical Steps Towards Proactive Security

While a mature proactive security strategy is certainly a critical asset for teams wanting to be secure in their cybersecurity initiatives, it doesn't happen overnight. However, with the right game plan, it can be a reality sooner than many organizations may think.

The following steps provide a roadmap for getting your proactive security program off the ground.

1. **Assess your assets** | Inventory all your assets to define the scope of your assessment. These are the assets you want to protect.
2. **Perform risk assessment** | Perform risk assessment of your security posture. This is where your offensive security stack comes in. You need a vulnerability management solution to identify known vulnerabilities, prioritize them by actual risk (vs. busy work) and manage their remediation. Penetration testing software or services will help you evaluate the exploitability of your weaknesses, and then enable your team to retest to gauge the efficacy of remediation efforts. Additionally, red team engagements test your security operations detection and response capabilities and provide your blue team with invaluable feedback. Nothing will prove you are ready to foil an attack like putting your security strategy to the test; solutions, strategies, playbooks, teams, and all.
3. **Organize your security infrastructure around your results** | Build out your security mechanisms around your discovered weaknesses, bolstering them and adding layers of protection where your environment is vulnerable. This is where risk context becomes very important.

> Your team can burn valuable time and resources remediating unimportant vulnerabilities if you don't use risk context to prioritize them.

Ensure you are looking beyond CVE ratings when prioritizing your vulnerabilities lists—consider exploitability and positioning within your unique infrastructure to ensure you fix the high-risk weaknesses first. Perform patching and configuration corrections and seek outside expertise from proactive security experts if necessary to find optimal configurations, monitoring applications, and detection and response solutions to strengthen your security infrastructure in a manner that directly addresses your unique challenges.

4. **Establish efficiencies** | This can go hand-in-hand with the previous step, but it deserves its own moment of attention. Putting up the right security measures is key, but if you want to establish security processes that can scale as your business grows, employ user-friendly solutions that offer automation where possible. One rule of thumb is to automate everything that does not require human judgment to accomplish, and as artificial intelligence (AI) improves, even that list is getting shorter. With time-saving tools like Robotic Process Automation (RPA) Extended Detection and Response (XDR), mundane tasks like threat hunting (and even remediation) can be offloaded to custom playbooks, leaving your team with more time on their hands to push the proactive security needle even further.
5. **Train all employees to report suspicious activity** | Your employees can be one of your best assets when it comes to catching cybercrime. A proactive security strategy extends beyond the SOC and reaches all components of the organization if it is to be successful. Security awareness training (SAT) programs are effective at helping employees recognize inlets of danger (phishing, BEC scams, social engineering) in which threat actors can enter to exploit vulnerabilities. Non-security leaning workers may not be able to patch and remediate threats on their own, but they can certainly help keep Black Hats at bay while security teams bolster the back end.
6. **Keep going** | One proactive security cycle – vulnerability scan, penetration test, red team engagement - is only effective until its expiration date, and that could be as soon as a new IoT device is introduced. Every bit of code, every new device, and even every new employee opens up avenues for error and undetected threats. Put your proactive security strategy on a recurring schedule so you can consistently pass audits, maintain compliance with industry standards, justify security spend, and keep your business, investments, data, and customers safe.

The Benefits of Adopting a Proactive Security Strategy

Beating adversaries to the punch – as in, discovering weak spots in your enterprise before they do – is its own reward. However, an enumeration of the additional benefits of adopting a proactive security strategy is below. Keep in mind, apart from a list of several distinct advantages, one overarching appeal is the fact that acting, not reacting, will produce better, more well-thought-out results in any cybersecurity environment. Stephanie Hagopian, VP of Security at CDW, highlighted this thought in an interview with, noting that, "Adopting a proactive cybersecurity strategy allows the time and space for organizations to make data-driven decisions about risk prioritization and resource allocation to mitigate negative outcomes."

That being said, additional proactive security upsides include:

- Being able to prove the effectiveness of your cybersecurity solutions to top executives, auditors, investors, partners, and the public.
- Deterring breaches and avoiding costly downtime.
- Ensuring compliance and sidestepping regulatory fines.
- Making your company cyber resilient at a time when AI-based threats are ramping up.
- Keeping the "wheels on the bus" and being able to sustain normal operations for longer, instead of being in "crisis mode" as systems, software, and solutions were not vetted the first time.

By using proactive security as a calculated strategic move, companies can slough off the tedious cat-and-mouse cycle and evolve to a higher level of organization and security, freeing up time to move forward in other areas, stay agile, note broader security trends, and innovate in crucial and competitive ways.

3 Components of a Proactive Security Strategy

Proactive Security tests an enterprise environment for technical and configuration vulnerabilities, quantifying their risk and providing companies with the transparency they need to prioritize threats and allocate resources. It also uncovers gaps in compliance so that organizations can take the necessary steps to fill them. Below are three crucial components to any proactive security strategy:

1. Vulnerability Management (VM)

What is Vulnerability Management?

Vulnerability management solutions identify, evaluate, prioritize, track, and report on the weaknesses that can undermine your organization. Once a vulnerability scan has been completed, teams will not only know which CVSS scores to watch out for, but which ones present the most present and immediate risk – and which ones can wait.

This must be done early and often. Scanning for vulnerabilities is not a static task, as each new service, device, application, and API introduces new opportunities for trouble. Vulnerability management is an ongoing process and an important level-set for proceeding to further offensive security techniques.

Application Security: A Crucial Component of VM

As previously mentioned, application security is an integral part of VM, as it targets the software development lifecycle and leans on proactive shift-left principles. Its two main components are:

- **Static Application Security Testing (SAST):** SAST hunts for weaknesses early in the software development process, identifying and eliminating them before the product is built, packaged, deployed, and in a position to endanger other players in its software supply chain.
- **Dynamic Application Security Testing (DAST):** DAST covers the front-end of application security testing, once the application is running. Testers are given no foreknowledge of the app's internal designs, programming, or systems, and must probe and attack it blind, like an attacker (or a pen tester). The purpose behind DAST is to test the application in the real world and see how it responds to this "black box" testing. Its behaviors under pressure will indicate whether it might have unresolved vulnerabilities that require further examination.

What to Look for in a VM Solution

When looking for the right VM solution for your organization, it's important to keep in mind that enterprise-grade vulnerability management can:

- Scan local systems and the entire network.
- Correlate data from and on dynamic assets.
- Save time by being easy to deploy, learn, and maintain.
- Segment reports by location, team, department, and more.
- Integrate seamlessly with other tools in your stack.

2. Penetration Testing

As captured in our 2024 Penetration Testing Report, a full 72% of respondents said that penetration testing has prevented a breach in their organization. And it's no surprise; penetration testing lets you exploit latent vulnerabilities before the threat actors do, allowing you to simulate a breach of your own network instead of letting Black Hats do it for you.

Penetration testing, or pen testing, uses the vulnerabilities discovered in the VM stage as a jumping-off point to see if they can be exploited – and how far. Per our 2023 Penetration Testing Report, 69% perform pen tests to assess risk and prioritize remediation, many using it as a precautionary practice against ransomware (72%), phishing (70%), and misconfigurations (58%). It can also be used after remediation is completed to gauge the effectiveness of the fixes.

Where to Find Pen Testing Resources

Pen testers are worth their weight to an organization, but at a time when most companies are struggling to fill cyber talent gaps, they might not be part of the in-house team at every organization. That's fine. Penetration testing, as a service or a technology, can be outsourced.

Fortra's Core Impact leverages guided automation and certified exploits so teams of any skill level can test their environment using the same techniques as today's threat actors. You can also use our penetration testing services (Core Security SCS) if resources are running short.

Another option is to upskill current employees to give them the pen testing skills you need them to have. More and more organizations are turning to upskilling and reskilling to plug cybersecurity skills gaps and offer their employees more job security, flexibility, and growth opportunities.

Key components for successful pen testing

In a successful penetration test, the following elements will be present:

- **Network security tests** | Uncover network vulnerabilities as well as weaknesses on your routers, switches, and network hosts.
- **Web application tests** | Test web applications for coding errors, broken authentication, and injection vulnerabilities.
- **Social engineering tests** | Put your employees and defenses to the test by launching phishing simulations and vetting the effectiveness of your detection tools in action.
- **Automation** | Automated pen testing tools systematically compromise potential places of exposure.

3. Red Teaming

Red team engagements take things a step further than pen testing, subjecting the whole cyber defense strategy to adversarial-level scrutiny. Red teaming can include anything from phishing to social engineering executives to leveraging the most advanced techniques used by threat actors today. And the test is for the security team as much as it is for the security defenses

> In a crisis, what you can *do* under pressure is worth ten times more than what you *know* in theory.

Fortra offers advanced tools that enable red teamers to perform advanced engagements.

- Cobalt Strike – enables teams to emulate a stealthy, advanced adversary that's been embedded in the network long-term and supports the use of different malware and social engineering ploys likely to be encountered. Its flexible Command and Control (C2) framework gives in-house staff the ability to modify, work around, or use built-in behaviors. View a Cobalt Strike demo here.
- Outflank Security Tooling (OST). Dive more in-depth with evasive attack simulation. This a broad set of tools designed to help red teamers create attacker scenarios that put defensive measures, detection tools, and response skills to the test. These offensive security tools also simplify red teaming engagements, allowing users to easily perform complex tasks safely.

Attack Surface Management

Ultimately, proactive security is the art of attack surface management. As new elements get sewn into your environment and find themselves settling on your network, the attack surface grows, whether you want it to or not. Repeating the above three steps as part of an attack surface management routine – vulnerability management, penetration testing, and red teaming – will help you spot new threats as they appear on the scene, make the team aware of them, determine whether or not they are truly a threat, and improve your organization's resiliency to attacks.

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.