ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

PROACTIVE CYBERSECURITY GUIDE

How to Assess and Mitigate Your Cyber Risks

A GUIDE TO PROACTIVE CYBERSECURITY

Under unrelenting pressure, many cybersecurity teams function entirely in a reactionary mode. They struggle to hire and retain qualified staff, and while thinly stretched teams do their best to protect the organization, they remain at a distinct disadvantage. Reactive security often leaves organizations exposed to attackers who always seem one or two steps ahead.

A reactive approach to security means that an organization only responds when needed.

Of course, it's not up to the security team to decide when that moment will come. Instead, it must respond when forced to do so by circumstances outside its control.

That's why employing a reactive approach restricts the time available to identify weaknesses or shore up defenses. And in an era when cybersecurity professionals are both overworked and in high demand, burnout and employee departures remain ever-present threats.

Alternatively, when organizations adopt a proactive approach, they afford themselves the time to detect and remediate vulnerabilities before attackers can exploit them.

Since the security team receives the backing and support to improve the organization's defenses proactively, the potential for a successful attack to cause lasting damage drops significantly. And for many cybersecurity professionals, the ability to make significant and sustainable improvements to the organization's defenses generates a sense of pride and accomplishment.

As a result, a proactive approach typically reduces stress and raises morale.

WHAT CONSTITUTES A **PROACTIVE APPROACH TO CYBERSECURITY?**

There are many terms and practices associated with proactive security. Many organizations use these terms interchangeably, even though they are not synonymous. Of critical importance, security departments must agree on what constitutes a vulnerability, a threat, and a risk.

VULNERABILITY

According to the National Institute of Standards and Technology (NIST), the most commonly used definition for "vulnerability" is a weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source.[1]

ASSETS

According to NIST, "assets" can be people, property, and information. People may include employees and customers along with other invited persons such as contractors or guests. Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include information, data, trademark, copyright, patent, reputation, and proprietary information. Tangible assets include physical items such as hardware, software, firmware, computing platforms, network devices, or other technology components.[2]

THREAT

NIST defines a "threat" as any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.[3]

RISK

Finally, according to NIST, "risk" is a measure of the extent to which an entity is threatened by a potential circumstance or event, which is typically a function of both the adverse impacts that would arise if the circumstance or event occurs and the likelihood of such an occurrence.[4]

To bring those concepts together, consider the engineering concerns when building and maintaining a bridge.

Weaknesses in the infrastructure are vulnerabilities; a car driving across the bridge is a threat to the bridge's vulnerabilities. Risk is the potential damage the car inflicts when it crosses the bridge and puts pressure on the infrastructure's weaknesses.

To extend that concept further, the risk of loss goes up as the threat, or in this case the volume of cars, increases. Conversely, the risk of loss drops as the volume of cars crossing the bridge decreases.

There are other key terms, too, for which everyone involved in the process must agree upon and use the same definitions:

The Common Vulnerability Scoring System (CVSS)

The framework for communicating the characteristics and severity of software vulnerabilities. It includes three types: base, temporal, and environmental. The CVSS provides a standardized approach to vulnerability severity scores.

Rating	CVSS Score[v3]
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Vulnerability assessment

The process of identifying, classifying, and prioritizing vulnerabilities in business systems. Assessments can focus on internal, external, or host-based vulnerabilities. A vulnerability assessment has a specific start and end date.

Vulnerability management

Solutions identify, track, and prioritize internal and external cybersecurity vulnerabilities, optimizing cyberattack prevention activities such as patches, upgrades, and configuration fixes. It relies upon the Common Vulnerability Scoring System (CVSS).

Risk-based vulnerability management (RBVM)

Also known as threat and vulnerability management or enterprise risk management, is a process that reduces vulnerabilities across your attack surface by prioritizing remediation based on the risks they pose to your organization.

RBVM goes beyond just discovering vulnerabilities. It helps you understand vulnerability risks with threat context and insight into potential business impact.

Also, it correlates asset criticality, vulnerability severity, and threat actor activity.

A PHASED AND STRUCTURED APPROACH TO PROACTIVE SECURITY

PREWORK

It's a common misconception that cybersecurity is all about technology. Technology is obviously a massive part of cybersecurity, but it alone is not enough to protect you from modern cyber threats. Effective and robust cybersecurity requires three pillars: people, processes, and technology.

Let's start with the technology component.

During this phase, ascertain how tools talk to each other. This should include a discovery effort to uncover assets in the IT infrastructure. Reviewing the configuration management database is also part of this step, as this can help locate hardware and software and determine how those assets interact. After this step, your organization should possess a firm grasp of its digital footprint.

There are two key aspects to the people component of the three pillars of robust cybersecurity. First, everyone in the company needs to be aware of their role in preventing and reducing cyber risk; for example, they must know how to handle sensitive data and understand how to spot phishing emails. After all, cybersecurity a business issue, and everyone has a role to play.

An effective security awareness program helps reduce the risk of cyber threats that directly target and exploit people.

Secondly, there are specialized technical security staff that need to fully understand their roles and responsibilities. These staff members must always be up to date with the latest skills and qualifications to ensure that appropriate controls and technologies are implemented against the cyber threats. Now is also the time to engage stakeholders and ensure they understand the phased approach to the vulnerability management lifecycle and their role in the process. This includes security and risk management, security operations, IT operations, and executive management. These stakeholders will perform various roles, such as defining the approach to vulnerability management, performing the vulnerability assessment process, remediating gaps, and monitoring the vulnerability management process and its effectiveness.

Processes are key to establishing an effective cybersecurity strategy.

To ensure that vulnerable items are processed correctly, you need to create policies and procedures. They must include firmly defined service level agreements (SLAs) that empower security and IT professionals. In fact, the SLAs will serve as guideposts in subsequent phases. It may make sense from an efficiency standpoint to engage stakeholders or their representatives from across the enterprise to gather the SLAs and make sure that processes have been implemented properly.

ASSESSMENT

Completing the assessment phase allows your organization to define the attack surface. Accomplishing this step requires complete visibility of your assets. However, it's challenging to identify your entire list of assets if you don't already have visibility into your environment. Network mapping and gathering a comprehensive asset inventory by endpoint can help accomplish this. Developing a detailed understanding of information technology (IT) versus operational technology (OT) is vital since this will guide your efforts to remediate vulnerabilities.

For example, not every single vulnerability can be patched. Suppose the assessment discovers a vulnerability in an OT asset. In that case, the mitigation and remediation efforts will differ from an IT asset in a noncritical area.

Once you identify assets across the enterprise, you can then scan for vulnerabilities.

This forms the basis for the next phase, managing vulnerabilities, which will be the crux of a proactive effort.

VULNERABILITY MANAGEMENT

During this phase, your organization will prioritize vulnerabilities according to a defined methodology. Using the CVSS allows you to score and rank vulnerabilities from 0 to 10—the higher the score, the more severe the vulnerability. A CVSS score does not reflect an organization's unique IT environment. Instead, it provides general guidance to serve as a starting point to prioritize vulnerabilities.

However CVSS scores alone are insufficient to properly evaluate today's threats, and the enterprise must take contextual information such as threat, asset criticality, and controls into account to prevent future data breaches and successful cyber attacks based on software flaws.

Additionally, organizations must go one step further into prioritization. A CVSS 10 vulnerability with no exploit publicly available can certainly be fixed after a vulnerability with the same CVSS value that is known to be actively exploited by common malware. Alternatively, advanced vulnerability management involves correlating a CVSS score with third-party threat intelligence, asset criticality, and the existence of internal controls to arrive at a deeper, more nuanced understanding of the vulnerability and its implications.

Understanding your risk requires implementing the following formula:

Risk = Likelihood of targeted attack (vulnerability and threat) x Impact (asset criticality and classification) – Controls (firewalls, password protection)

Having completed this formula, your organization can determine, in concert with your SLAs, whether the residual risk (the amount of risk that remains after the application of controls) meets your tolerance.

It's important to note that since threat intelligence is crucial to developing an advanced approach to vulnerability prioritization and management, third-party intelligence should come from reliable sources that take the time to validate the information they provide. Interpreting such intelligence and turning it into actionable intelligence may also require expert assistance from suitably qualified cybersecurity professionals.

HARDENING

With a prioritized list of vulnerabilities, the next phase involves hardening your defenses. There are different ways to treat vulnerabilities, including:

REMEDIATION:

Fully fixing or patching a vulnerability so it can't be exploited. This is the ideal treatment option that organizations strive to achieve.

MITIGATION:

Reducing the likelihood and/or impact of a vulnerability being exploited. This is sometimes necessary when a proper fix or patch isn't yet available for an identified vulnerability. This option should ideally be used to buy time for an organization to eventually remediate a vulnerability.

RISK ACCEPTANCE:

Taking no action to fix or otherwise reduce the likelihood and/or impact of a vulnerability being exploited. This is typically justified when a vulnerability is deemed a low risk, and the cost of fixing the vulnerability is greater than the cost incurred by an organization if the vulnerability were to be exploited.

In its simplest form, remediation involves the deployment of a patch to address one or more vulnerabilities. Mitigation can include deploying additional controls, such as more robust password management tools or techniques.

Your organization can also choose to accept a risk. It is not highly recommended because "accepting a risk" creates an exception. Organizations should be careful on making exceptions and there should always be an expiration date for the accepted risk; otherwise, you can suffer with the consequences because it leaves a door open for the hacker to enter your environment.

For example, if you operate a legacy system that the developer no longer patches, and it is not feasible to replace it, you might decide to accept the risk.

Organizations should have a section in their policy and procedures on their remediation exceptions.

Ideally, the decision to accept a risk should follow a defined methodology—it should be documented, communicated, and agreed upon by senior executives with the authority to accept the risk associated with a vulnerability. This is also the phase to acknowledge the presence of false positives, meaning vulnerabilities that appeared valid and required addressing, but upon further investigation did not constitute a vulnerability. This finding helps improve subsequent assessments, providing feedback to security analysts to refine the list of vulnerabilities discovered in the future.

When it comes to hardening your security posture, Arctic wolf suggests that you establish two streams of patching schedules.

The first is for emergency patching procedures where you should patch vulnerabilities within 24-48 hours of the release date. The second schedule is for routine patching, which should occur within 7- 90+ days of release, depending on the risk profile.

VALIDATION

In the closing phase, the assessment team should rescan the environment to make sure the team's efforts discovered and led to the remediation, mitigation, or acceptance of the vulnerabilities within the organization's digital footprint.

A closed ticket by a system administrator cannot be considered a validation.

Validation may include rescanning, configuration management tool validation, targeted penetration testing, or by applying a breach attack simulation (BAS) tool to verify the attack scenarios.

Metrics can play an important role as part of this effort, such as the time to remediate a vulnerability according to its risk priority and the organization's SLAs related to resolution. The assessment team can also provide a matrix for organizations to monitor with their security partners, which can provide structure and accountability, and help maintain the momentum related to the proactive security effort.

A COMPELLING CASE FOR ACTION

A structured, focused approach will enable you to switch from a reactive to a proactive approach to cybersecurity and reduce the stress on your organization and those tasked with protecting it.

In fact, according to Gartner, organizations that rely on risk-based vulnerability management experience 80% fewer breaches.

While proactive security does not eradicate the need for services in response to a data breach or an attack, it lessens the need for additional support, because fewer vulnerabilities exist to remediate.

Vulnerabilities Will Be Exploited

Vulnerabilities which require no user interaction to exploit are growing in number, representing 68% of all CVEs recorded in 2020.

– US National Institute of Standards and Technology and its National Vulnerability Database

Businesses Struggle to Deploy Patches

The time it takes to deploy patches for vulnerable systems has increased by an extra 40 days since March 2020.

– Arctic Wolf 2020 Security Operations Report

FINDING SECURITY PARTNERS **TO HELP**

If your organization lacks the people, expertise, or access to reliable threat intelligence to manage a proactive approach to cybersecurity, a partner can help.

If you plan to outsource vulnerability management, the partner you select should possess the people, processes, and technology to support this project, as well as your ongoing security needs as you improve and fortify your security posture. For example, the solution provider should offer an expert security team with the ability to function as an extension of your existing team.

Many organizations also contend with ineffective communications, process gaps, and insufficient remediation resources.

Engaging a third party can allow for a fresh approach, including infusion of the latest tools and techniques gathered from multiple industry verticals.

THERE IS NO **QUICK FIX**

An effective, sustainable, proactive security program does not simply involve a one-time effort.

There's a lifecycle for organizations to follow and revisit as the IT and OT environments change and the threat landscape evolves. Moreover, a managed risk approach removes much of the fear, uncertainty, and doubt that can plague security departments. It allows organizations to assess and strengthen their approach to vulnerability management. After all, you cannot manage risk and protect your organization if you do not know where and in what form it exists.

Managed Risk

Learn more about Arctic Wolf® Managed Risk, which enables you to discover, assess, and harden your environment against digital risks by contextualizing your attack surface coverage across your networks, endpoints, and cloud environments.

Sources

[1] https://csrc.nist.gov/glossary/term/vulnerability

[2] https://csrc.nist.gov/glossary/term/asset

[3] https://csrc.nist.gov/glossary/term/threat

[4] https://csrc.nist.gov/glossary/term/risk

ARCTIC WOLF

SOC2 TYPE II CERTIFIED

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

CONTACT US

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com

END CYBER RISK

ABOUT ARCTIC WOLF

Arctic Wolf® is a global leader in security operations, delivering the first cloud-native security operations platform designed to end cyber risk. Powered by threat telemetry spanning endpoint, network, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes trillions of security events a week across the globe, enabling critical outcomes for most security use cases. The Arctic Wolf® Platform delivers automated threat detection and response at scale and empowers organizations of any size to stand up world-class security operations with the push of a button.

For more information about Arctic Wolf, visit arcticwolf.com.

REQUEST A DEMO