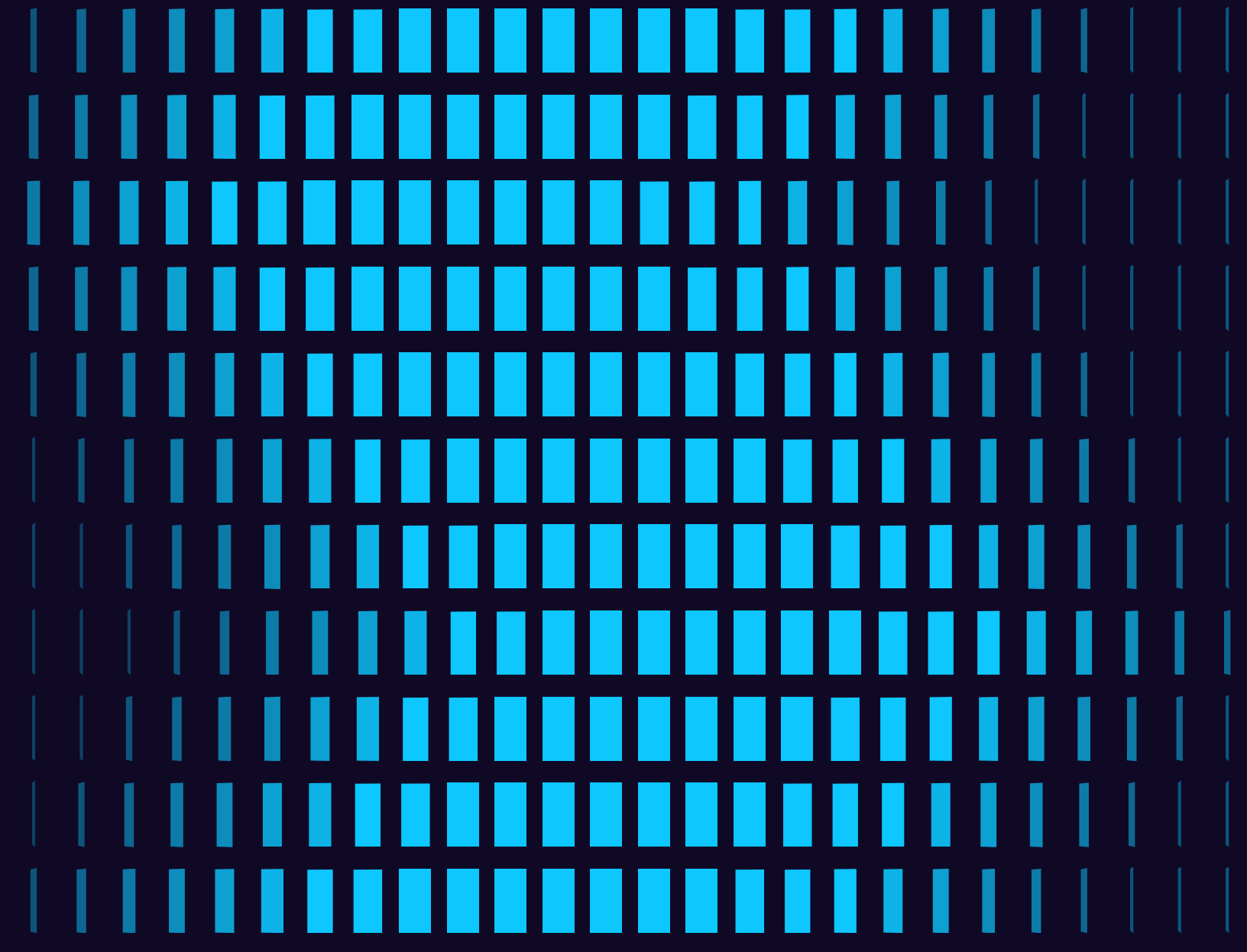
HADRIAN

Vulnerability management maturity model from legacy to optimal

The Hadrian's guide to upgrading your vulnerability management program



The current state of vulnerability management

Vulnerability management is a challenging yet critical undertaking for CISOs in an era of rapidly escalating cybersecurity threats. The increasing frequency and complexity of cyber-attacks, coupled with financial constraints and talent shortages, exacerbate the burden.

Notably, a staggering **70%** of organizations have suffered attacks exploiting unknown or poorly controlled external assets, marking a **30%** surge of external assets than companies expected. This comes at a steep price, with weekly remediation and vulnerability detection efforts costing an average of **$20,000** per organization.

It's no wonder that CISOs are looking for sure ways to get the most out of security postures. They need their cybersecurity tactics to work smarter. They can't afford to chase down false positives and low critical risks. In addition, they want their enterprise to be free to invest in technology without the fear of adding unmonitored attack points. But all this is nearly impossible without a mature vulnerability management program.

The increasing intricacy of managing external attack surfaces calls for a revised approach. Assets are not only linked by a connection within the infrastructure but by the way an attacker moves between them. Bad actors take a top-down approach to infiltrating a system. Unfortunately, most cybersecurity programs don't operate that way, and the scope of the attack surface exceeds the typical focus of the program. Often immature models defend inside the moat, patch old legacy systems, and hover over protecting the least likely points of entry for hackers.

Supporting these observations, Verizon's 15th Annual Data Breach Investigations Report [1] highlights a **25%** increase in ransomware attacks in 2022, with **82%** of breaches involving a human factor. Gartner[2] predicts that human error will cause over **50%** of significant cyber incidents by 2025, with cyber and social engineering attacks targeting humans on the rise. This human aspect, amplified by the increasing reliance on remote work and shadow IT, underscores the necessity for CISOs to maintain a firm grip on their expanding attack surface.

[1] Verizon, Data Breach Investigations Report 2008-2022

[2] Gartner, "Gartner Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025," Gartner Newsroom

What makes a vulnerability program mature?

Most vulnerability programs merely check the box on security by using routine scans to launch reactive initiatives. These enterprises might have tools in place, but they lack a broad program. For substantial improvement in cybersecurity posture, **vulnerability management must be prioritized at all levels of the organization** - from the C-suite to the frontline. It needs to be part of the business plan and have the budget to back it. If not, a half-hearted form of protection will be just that—a very flimsy defense against attacks that will just keep coming, bringing devastating consequences to an enterprise's bottom line.

A mature vulnerability management program is efficient when it comes to compliance, using fewer resources. It is agile and exacting. A mature model can not only pinpoint a threat, but it can act swiftly to remediate it and understand the steps needed to prevent a full breach. This is important because bad actors are increasingly using patience to lurk on the edges of a system, infiltrating their way in slowly and planning the final attack.

Mature programs assess, prioritize, and remediate vulnerabilities. This is much more than a scanning and patching process. According to Deloitte,[3] a mature vulnerability management program is secure because:

- It's broad enough to include frontline defenses along with policies, procedures, and controls.
- It's also a more vigilant warning system because it identifies potential threats before they hit.
- It is resilient because, though it can respond quickly to an incident, it doesn't tax the security team, and the cybersecurity program stays on a steady course.

[3] Deloitte, "Take the lead on cyber risk,"

Assessing the maturity of a vulnerability management program

Vulnerability management programs can be conceptualized along two key dimensions: scope and capability.

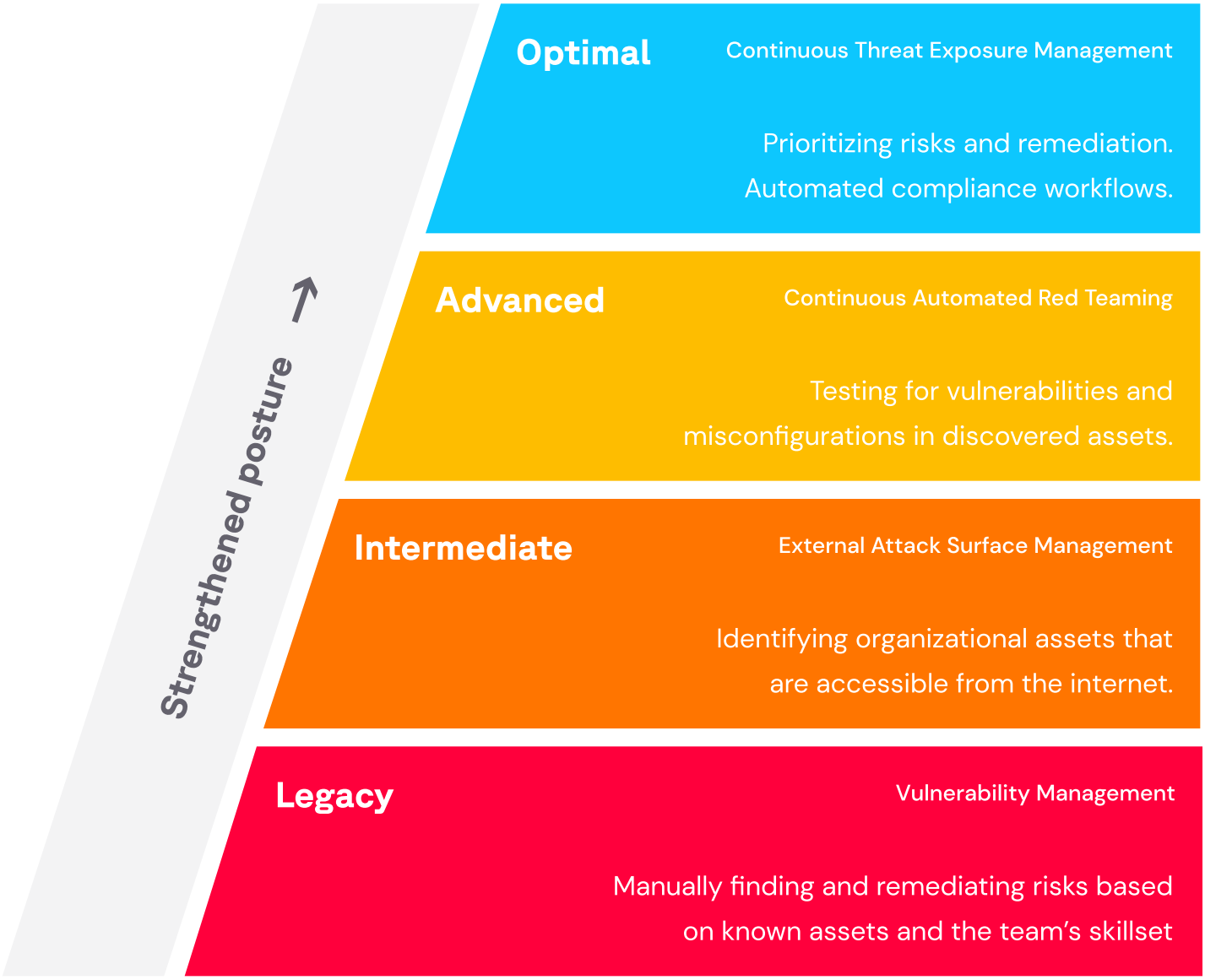
Scope refers to the range of assets monitored by the program. In less mature programs, the scope is often limited to a small defined list of critical assets. However, considering that attacks can move laterally, protecting every asset is crucial to prevent ingress from any vector. Therefore, to mature, organizations should expand their scope to cover every system that could potentially be accessed by a threat actor.

Capability involves the stages of vulnerability management, namely discovery, contextualization, risk identification, prioritization, and remediation. Less mature programs tend to rely heavily on manual processes at every stage, utilizing point solutions, manually maintained databases, and human-powered research. This significantly reduces efficiency. In contrast, mature programs automate and streamline these processes, thereby enhancing the capacity to identify, prioritize, and remediate more risks.

Moving from a low-maturity state to an optimal one is not a simple task. The maturity model operates on the principle of incremental progression, encouraging organizations to take small, manageable steps. By following the roadmap outlined by a maturity model, organizations can gradually build up their capabilities, improve efficiency, and enhance their overall cybersecurity posture.

A Roadmap to Maturity: From Legacy to Optimal

Every enterprise today will find itself somewhere along the continuum of vulnerability management models, but only those with a mature model have the best chance of protecting their enterprise. Let's take a look at the range of vulnerability models, what they entail, their effectiveness, and some advice for improvement. Where does your organization stand when it comes to vulnerability management?



Legacy - Vulnerability Management

This lowest level of vulnerability management is outdated, with ad-hoc, and manual asset scanning that only allows for remediating risks based on known assets and a case-by-case basis. This strategy inherently lacks breadth, concentrating predominantly on a minimal array of core systems. Further, it may be deficient in visibility to even identify, let alone evaluate, cloud applications, third-party systems, or Internet of Things (IoT) devices.

Older systems often lack the latest security patches and updates, making them more vulnerable. The process of identifying vulnerabilities and patching remains time-consuming, as well as labor-intensive—and it is not an easily scalable process. The legacy infrastructures organizations have at this level most likely need updating, but that will be a slow process.

Many organizations or companies embrace a hybrid approach with some legacy core infrastructure and more modern systems that are customer-facing. It is essential that the customer-facing systems are secure in order to protect the core, which is likely to have exploitable vulnerabilities.

Start using scheduled scanning and continuous monitoring, in addition to creating and reporting metrics. Broaden your focus to cover all internet-facing assets by incorporating an Attack Surface Management (ASM) solution. This will effectively help you identify and manage risks across your digital environment.

Intermediate - External Attack Surface Management

Organizations at this level of cybersecurity are still at an immature level. They identify organizational assets that are accessible from the internet using scheduled scanning and some integrated automation. Some may have applied enterprise service management (ESM) solutions. These might work for six months before a CISO realizes it's just another source of information that is overloading an already overwhelmed security team.

In addition, these organizations frequently struggle to differentiate between actual threats and false positives in the sea of potential risks. The process of manually validating and triaging risks is time-consuming, which significantly undermines the effectiveness of their security programs.

Move to the stage that gives actionable results. Do this with risk-based insight and focus on only patching critical risks. Move ahead by introducing red teaming to emulate a potential adversary's attack capabilities against the enterprise's security posture. Best practices should include continuously reassessing posture instead of relying on one-off or annual reports.

Advanced - Continuous Automated Red Teaming

At this level, an organization is becoming more mature. The security team is testing for vulnerabilities and misconfigurations in discovered assets and in the expanded attack surface, including cloud computing, IoT devices, and mobile applications.

The organization is beginning to visualize how assets link together to help it understand the multi-stage attacks a malicious hacker might perform. Attackers that take advantage of misconfigurations in one asset often don't stop there and will go on to launch attacks from the new access point.

Level 3 security programs use red teaming to improve enterprise cybersecurity by demonstrating the impacts of successfully staged attacks. Most organizations only carry out red team exercises annually or on an ad hoc basis. Given the current pace of digital transformation, this is vastly inadequate because too much can happen during that time.

At this stage, organizations struggle to identify their priorities and determine which risks require immediate resolution. They lack the critical understanding of which vectors are most likely to be exploited and the potential business impact of such attacks. Consequently, without a clear perspective of risk prioritization and the repercussions of potential breaches, these organizations struggle to implement an efficient and effective vulnerability management program.

Adopt compliance frameworks, understand the business context of the risks, and introduce purple teams. Purple teams pit red team attackers against blue team defenders to discover and learn from what works in various scenarios. Utilizing AI can streamline offensive security by automating the different attacks from a malicious actor.

Optimal - Continuous Threat Exposure Management

The optimal and most mature level of vulnerability management uses Continuous Threat Exposure Management (CTEM). This solution monitors for threats in real-time and identifies assets that are accessible from the internet, not just known assets. It prioritizes risks and patching based on the business context, not just isolated conditions. It also identifies the weak points that threat actors are looking for and automates the entire lifecycle of exposure management to reduce risks and improve efficiency.

To prevent multi-stage attacks, Level 4 models always assess each risk against how assets are linked. An organization with a mature vulnerability model remediates these risks and retests them automatically, to verify that they are resolved.

CISOs at this level understand the necessity of frequent purple teaming as a way to gain valuable insight into how to up the game on the constantly changing threat landscape. Their purple teams are collaborative and work toward the successful training of a company's whole security team to meet threats early.

Gartner's "Top Trends in Cybersecurity 2023"[4] advises a proactive and strategic approach to cybersecurity. Organizations that don't use this strategy will be at a significant disadvantage in detecting and responding to threats.

[4] Gartner, "Top Trends in Cybersecurity 2023," Richard Addiscott, et. al.

The next step: Where do you go from here?

Ultimately, organizations should aim to mature toward CTEM. Hadrian helps organizations at every stage of the roadmap. Our solution provides attack surface management, autonomous red teaming, and risk prioritization to automate the external exposure management lifecycle, from initial asset discovery to risk remediation:

Automated Discovery

Hadrian uses cutting-edge technology to automatically discover and catalog all external facing assets, both known and unknown, to provide a comprehensive view of your attack surface.

Continuous Monitoring

It doesn't just stop at discovery. Hadrian continues to monitor your attack surface, identifying changes and new vulnerabilities as they arise.

Risk Prioritization

By using a contextual understanding of threats, Hadrian moves beyond simple CVSS scores to prioritize vulnerabilities in the same way a hacker might, focusing on the most likely points of attack.

Integrated Remediation

The system integrates with existing security infrastructure for effective and timely response to identified vulnerabilities, making the remediation process smooth and efficient.

Scalability

As your organization grows and evolves, so too does your attack surface. Hadrian's technology is designed to scale with your needs, ensuring your cybersecurity measures grow with you.

The next step: Where do you go from here?

Utilize the table below to assess the current maturity level of your vulnerability management program and identify the roadmap objectives that should be implemented.

	Legacy	Intermediate	Advanced	Optimal
Process	Case-by-case basis	Compliance-driven, infrequent process	Schedule and prioritized patching	Prioritized and continuous patching
Operational workflow	Manual	Some automated integration	Fully automated	Fully automated, unified with business goals
Scope	Known assets	Internet-facing assets	Vulnerabilities and misconfigurations in discovered assets	Business and wider risks
Metric	Basic or no metrics	Busy metrics	Emerging metrics and trends	Threat-driven metrics
Roadmap objective	Monitor the entire attack surface	Add continuous risk finding	Improve prioritization and remediation	None- achieved CTEM

About us

Hadrian is a leading provider of External Attack Surface Management (EASM), Continuous Automated Red Teaming (CART), and Continuous Threat Exposure Management (CTEM) solutions. Our platform catalogs known and unknown assets wherever they are, investigates vulnerabilities by executing exploits like a threat actor, and prioritizes risks for fast remediation based on your unique environment.

> Hadrian went a step beyond other ASM tools by guaranteeing that the insights they provided aligned with our current concerns and needs. We were able to remediate risks quickly and effectively without wasting resources
>
> CISO, London Business School

Trusted by market leaders

BIOLANDES
CTC GLOBAL
beyond.
KCK
KINGSWAY CAPITAL
ABN·AMRO
LEROY MERLIN
London Business School