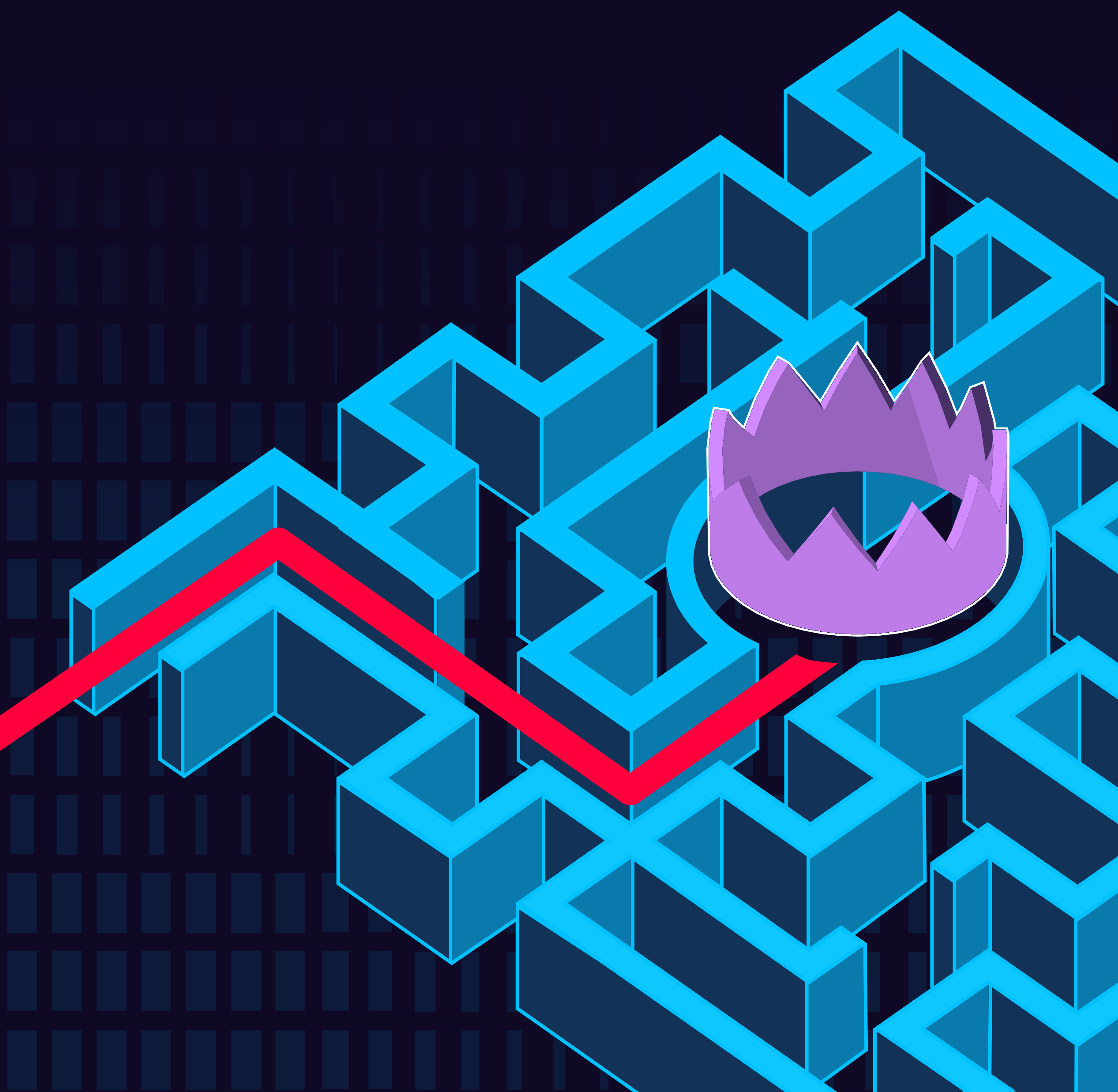
HADRIAN

# Why Continuous Automated Red Teaming Makes Sense

Traditional penetration testing and red teaming can’t keep up with today’s threat landscape



# Today's CISOs wrestle with a rapidly evolving and ever-expanding attack surface. And this is going to continue.

Cybersecurity teams struggle to defend their enterprises in the face of the Internet of Things, more remote workers, shadow IT, cloud migration, third-party vendors and edge computing, and more. Defining the perimeter is nearly impossible. In fact, it's as if the perimeter doesn't exist.

> "The next few decades promise to be a time in which technologies progress ever-more quickly from science to engineering to impact—at scale, and around the world," [1]
>
> McKinsey & Company

Cybersecurity teams struggle to defend their enterprises in the face of the Internet of Things, more remote workers, shadow IT, cloud migration, third-party vendors and edge computing, and more. Defining the perimeter is nearly impossible. In fact, it's as if the perimeter doesn't exist.

Meanwhile, cyberattacks are increasing at a rapid pace.2 Ransomware groups are relying more heavily on vulnerability exploitation than ever before, a new report says. They are paying hackers to find vulnerabilities, then they are abusing these vulnerabilities on a large scale.3

With so many unseen assets and unknown threats, it's no wonder that security teams can't keep up. The environment is changing constantly, due to both internal and external factors, not just because of the expanded attack surface. It's becoming clear that the only way to protect security is with a holistic approach.

> "Security leaders improve the security of their digital ecosystem when they implement controls that take a holistic view of their increasingly fragmented attack surfaces and brittle identity infrastructure," [4]
>
> Gartner

[1] McKinsey & Company, Technology Trends Outlook 2022, August 2022
[2] McKinsey & Company, What is Cybersecurity?, April 2023 (Accessed 7/27/23)
[3] CSO, "Ransomware victim numbers surge as attackers target zero-day vulnerabilities," Foundry (Accessed 8/18/23)
[4] Gartner, Top Trends in Cybersecurity 2023

# What today's pen testers and red teams are up against

For decades, CISOs have used penetration testing and red teaming to test their security preparedness. But today, a large majority of these tests don't come close to simulating the reality of modern threats. This is partly because the tests require gathering intelligence to understand the threats and the potential risks they may have. Some organizations might shun this process as too time-consuming, but they shouldn't. It is essential if you want to accurately replicate real-world attacks.

Today's CISOs and their teams are up against a vast array of threats. Attacks can come because of:

- sensitive data in unknown locations
- websites with paths to the corporate network
- unknown SaaS applications
- applications with 0 users
- misconfigured SSL certificates

In addition, other more complex and menacing factors are making cybersecurity difficult, including:

- Threat actors scaling their efforts. Malicious actors are no longer crafting tailor-made exploits for specific businesses. They are going after common technologies that span across millions of companies. Once they develop an exploit for a given technology, they can unleash it on a broad scale. They are getting faster and more efficient at scouring the internet for access to your system.
- Ransomware hackers buying access. Ransomware attackers are no longer doing everything themselves. Instead, they buy access from Initial Access Brokers (IABs), who are specialized at it. This gives ransomware criminals more time to do what they do best. These threat actors then take their time, working deep into your system, until the time is right to attack.

## Not enough red teaming

Many cybersecurity teams carry out red teaming annually. This won't work given the current pace of digital transformation. Too much can happen during that time. A flaw or loophole in your system could develop or you could inadvertently open a port in a firewall. A threat actor could discover a vulnerability in your system and exploit it. Annual red teaming leaves your enterprise open to attack.

There are many other reasons that security teams don't conduct enough red teaming. Some say they are pressed for time. Others feel they don't have the internal expertise to conduct red teaming, and some find it too expensive.

Whatever the reasons for neglecting this important cybersecurity strategy, the stakes are too high to ignore the benefits that red teaming has to offer.

Time is of the essence. Hackers are getting smarter and faster.

"Attackers using advanced tools such as AI, automation, and machine learning will cut the end-to-end life cycle of an attack from weeks—to days—or even hours," **McKinsey** says. [5]

## The pros and cons of traditional red teaming

By simulating real-world attackers, red teaming allows organizations to identify vulnerabilities and strengthen their defenses before one of these attacks occurs. Because red team exercises are carried out with no warning, they force a company to respond as if the attack is real.

The results of a red teaming exercise shed light on vulnerabilities and risk areas within an organization's security posture. The exercise provides a valuable opportunity for debate among the security team on how to improve defenses.

However, even if red teaming is put to good use, it's still antiquated. It is largely manual, hard to scale and prohibitively expensive for frequent use. For some organizations, it is too expensive to do at all. Today's growing threat landscape calls for a more proactive strategy.

> Experts advise moving past traditional red teaming. "It's time to upgrade and expand security operations," [6]
>
> **Enterprise Strategy Group™**

**Gartner** says, "CISOs must scale security operations to address the threat landscape and growing attack surface, while adopting modern security and data management technologies to help them tackle growing data and alert volumes." [7]

[5] McKinsey & Company, What is Cybersecurity?, April 2023 (accessed July 27, 2023)
[6] Enterprise Strategy Group Research, Inc., The rise of cloud-based security analytics and operations technologies, 20197
[7] Gartner, Chief Information Security Officer Persona Priorities, 2023

# What is Continuous Automated Red Teaming (CART) and how does it work?

Continuous Automated Red Teaming (CART) is, obviously, continuous. This is vastly better than an annual test. It is also focused on a goal. That goal is to hack your company — giving it a much broader scope than penetration testing.

Unlike traditional red teaming, CART never quits in its mission. And it uses artificial intelligence (AI) and machine learning to grow even smarter at hacking you. Just like a real hacker.

CART attacks any vulnerability it can find, making it much more like a real world attack. It exposes a company's security weaknesses the same way a hacker would — with no warning and no predictability.

## Benefits of CART:

- **Operates across large networks and systems with little human intervention:** This makes it well-suited for organizations that want to conduct frequent and extensive testing.
- **Is less likely to err than humans:** Because CART is automated, it reduces human error and the likelihood that a weakness is overlooked.
- **Is consistently updated to test for the latest threats:** This differs from traditional penetration testing, which is often planned in advance and may become outdated quickly due to the rapidly changing threat landscape.
- **Eases your security team's workload:** The automation of CART frees up time for your team to do more challenging tasks.
- **Focuses on an organization's entire network:** This includes systems and applications. It provides a targeted assessment of an organization's security posture by assessing weaknesses and is ideal for security control validation and benchmarking security performance.
  Bridges the gap between annual penetration tests and red/blue team testing: Its goal is to remediate vulnerabilities with increased speed.
- **Considers how assets link together and 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.

# External Attack Surface Management (EASM) and CART

The whole CART process starts with External Attack Surface Management (EASM) -- because hackers look at your system from the outside in.

In this first stage in the CART workflow, EASM maps an organization's digital attack surface from the perspective of a threat actor.

## It looks for:

- Exposed credentials
- Vulnerable databases
- Unprotected cloud assets and buckets
- Open ports
- Misconfigurations

EASM discovers assets and finds risks, and when combined with CART, fortifies a security posture. The two work together, and each serve their distinct and crucial functions.

Primarily focused on identifying and managing an organization's internet-facing digital assets, EASM provides a comprehensive view of an organization's external attack surface and is useful for asset discovery, risk management, and compliance. It works best when used with CART.

Once CART finds a vulnerability, it launches a simulated attack in a multi-stage operation from its attack engine. Its mission is to find the attack paths and blind spots that provide that vulnerability that threat actors hope to exploit.

# Why you need CART

**By using CART, you can shorten the time it takes to remediate a risk, while hardening your perimeter.**

You can fortify your security posture in a timely manner, with a real-time, broad view of your risks.

If done effectively, a CART program should:

- Test your system for weaknesses regularly
- Monitor your system to uncover threats
- Communicate the risk level of threats
- Collect data on how your system is behaving
- Resolve any vulnerabilities it discovers
- Validate the remediation

## CART creates a roadmap for future security strategies

Data collected from the CART platform can be used to benchmark security posture. CISOs can take this information to the board, with a comparison to the industry. And they can use it to measure the performance of their security vendors. It can also be used to present the case for a bigger security budget.

"The role of CISO continues to evolve from a technology-focused position to a business-enabling one," **Gartner** says.

- 70% of organizations are mapping cybersecurity investment to business outcomes to inform budget priorities
- Nearly 50% of the organizations are linking security metrics to business performance[8]

CISOs need to back their new role up with data and be prepared to "talk the talk" with the business team. No longer is the security team out of the loop, speaking their own tech language.

Companies are standing up and taking notice of the cybersecurity risks before them. The losses from a cybersecurity event could be critical. And likewise, good security can build a company's reputation. The CISO is now at the center of it all. And soon, cybersecurity will be part of the board.

> "By 2026, 70% of boards will include one member with cybersecurity experience,"
>
> Gartner®

[8] Gartner, Chief Information Security Officer Persona Priorities, 2023

# Hadrian’s CART matures your vulnerability management program

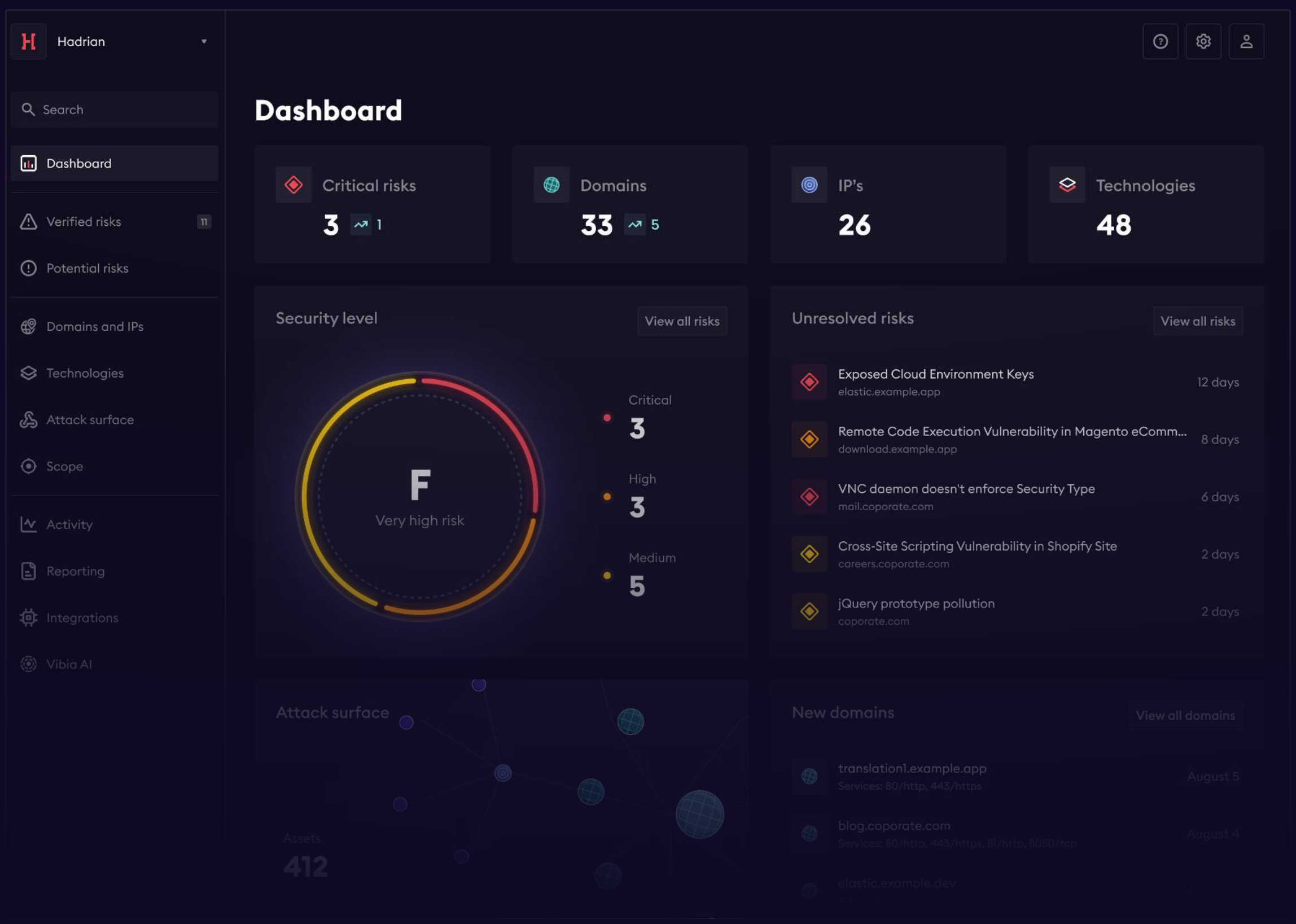
Hadrian was founded by white hat hackers, and we have automated the work that we've been doing manually for thousands of customers for many years.

At the heart of our platform is Orchestrator, which conducts 24x7x365 analysis like a real-world adversary, by dynamically chaining 200+ “hacker” modules together.

We use the power of AI to predict attack paths out of trillions of possibilities. Then, we use cross asset testing and modules to mimic hacker creativity. We do this because hackers can't rely on inside knowledge, so they link multiple assets together to find vulnerabilities. Hadrian knows that triggering an event on one asset should result in testing other assets.

Primarily focused on identifying and managing an organization's internet-facing digital assets, EASM provides a comprehensive view of an organization's external attack surface and is useful for asset discovery, risk management, and compliance. It works best when used with CART.

Once CART finds a vulnerability, it launches a simulated attack in a multi-stage operation from its attack engine. Its mission is to find the attack paths and blind spots that provide that vulnerability that threat actors hope to exploit.



# With Hadrian's CART platform, you can:

**Monitor your attack surface with continuous asset discovery**

We help you gain complete visibility of external-facing assets and reduce the risk of a breach caused by an exposed asset. By continuously discovering and taking inventory of your internet-facing assets, we provide you with comprehensive visibility.

**Eliminate the risks that matter most with risk-based vulnerability management**

We find and eliminate your most impactful vulnerabilities. With our comprehensive, real-time vulnerability management solution, we prioritize exploitable risks for effective remediation, helping to maintain a robust security posture.

**Simulate real-world cyberattacks with automated penetration testing**

Hadrian enhances cybersecurity with automated penetration testing, emulating hackers for comprehensive security validation using its event-based AI.

**Defend against supply chain attacks with 3rd party risk monitoring**

We continuously assess 3rd party applications for risks that could result in a breach of your critical data.

**Stay compliant with compliance reporting automation**

Hadrian automates reporting, providing consistent and accurate insights. The on-demand reports can be easily exported and shared with stakeholders.

**Gain visibility of all your assets with external IoT & OT visibility**

We protect any exposed IoT and OT assets by identifying, mapping, and contextualizing your IoT and OT devices, discovering potential attack vectors and strengthening your security posture.

**Detect exposures in cloud systems with comprehensive cloud monitoring**

Hadrian continuously scans, detects, and remediates misconfigurations and other threats to multi-cloud infrastructure to prevent breaches.

**Protect investments from cyberattacks during mergers and acquisition asset protection**

We ensure secure and successful mergers and acquisitions by protecting valuable digital assets during M&A activity. Hadrian protects your investments by eliminating application security risks.

**Prevent confidential data exposure with sensitive file discovery**

Hadrian secures confidential data with advanced algorithms. We meticulously find your internet-exposed sensitive files, mitigating risks while ensuring regulatory compliance.

**Strengthen and protect DNS infrastructure with DNS monitoring**

We secure your digital landscape by delivering a comprehensive DNS protection solution that stops phishing and brand abuse. Hadrian proactively secures subdomains from hijacking attempts and ensures that your business operations are uninterrupted.

## In summary

Red teaming allows you to see how your organization will respond to a genuine cyberattack. But to do an effective job at red teaming, you need to study threat intelligence and emulate the latest in cyberattacks. This is time consuming and uses valuable resources.

Red teaming is adversarial and can root out undiscovered weaknesses. But a red team exercise conducted annually or even bi-annually will do little to protect against hackers coming at you 24/7. You need continuous automated red teaming informed by the latest information on cyberattack trends. You need to think like a hacker or hire ethical hackers to back you up.

Hadrian's CART is part of a mature vulnerability management program that is agile and exacting. It can pinpoint a threat and act swiftly to remediate it. Because we are white hat hackers, we can help. We know the steps needed to prevent a full breach, and we know how to research the trends.

Our CART is programmed to assess, prioritize and remediate vulnerabilities. This is much more than a scanning and patching process.

You can't afford to let your vulnerability management lag in the legacy era. It needs to evolve and be continuous.

HADRIAN

**Hackers are upping their game — shouldn't you?**

Find out more about Hadrian's 24/7 cybersecurity platform that uses a proactive, automated, and adaptive approach to identify and address security vulnerabilities.

Get a demo  Learn more