HADRIAN

Guardians of the Cyber Realm

CISOs and the New Age of Threats

Today’s CISOs are expected to do more with less

Threats have increased, but talent is short

CISOs have an overwhelming job. They are responsible for fighting immediate threats and for staying proactive against potential threats – all in an environment that gets more complex and dangerous by the day.

> A lot of organizations I talk to are overwhelmed with traditional vulnerability management.
>
> **Richard Stiennon - Chief research analyst @ IT-Harvest**

At a minimum, CISOs are expected to:

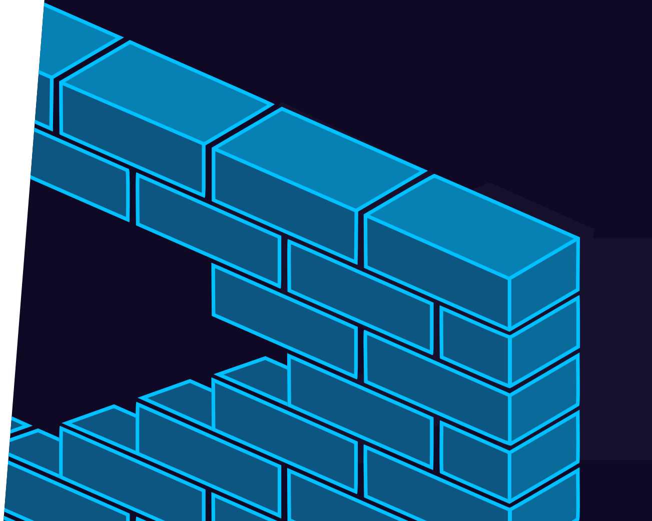
- ·Know their organization’s cybersecurity strength.
- Discover where their security may be weak and what to prioritize.
- Implement continuous improvement plans.

This is not an easy feat when it is becoming more difficult to assemble a good cybersecurity team. According to Gartner, churn is posing a significant threat for security teams. [2]

66%

of security teams say it is difficult to protect complex and dynamically changing attack surfaces [3]

By **2025**, lack of talent or human failure will be responsible for over half of significant cyber incidents [4]



The attack surface has grown

How do you protect what you don't know is there?

Up until recently, a CISO could rely on PDCA methods for cybersecurity, but now things are more complex. The attack surface has grown significantly. Threats are increasing, and so is alert fatigue. Third-party vendors and new applications on the edge are leaving too many unprotected gaps for cybercriminals to access your system.

> The time from CVE publication to mass scanning the internet with a POC by malicious actors is not days anymore. It's not hours anymore. We're talking about minutes.
>
> **Rogier Fischer - Co-founder and CEO @ Hadrian**

The speed of cybersecurity has picked up. Planning, doing, checking and acting is too slow to be used alone. Initial access brokers, a new part of the criminal underworld, specialize in gaining access to your system. They sell that access to other bad actors, intent on ransomware and more.

With all this added vulnerability, the stakes are higher. You need more help identifying where to spend your resources. You can't afford to chase breaches after the fact, you need to prevent them in the first place.

Just **51%** of global enterprises are **able to fully define the extent of their attack surface**

Only **9%** of organizations believe they actively **monitor 100% of their attack surface** [5]

CISOs need to be business leaders like never before

C-suite and board buy-in on cybersecurity is critical

It used to be that the cybersecurity world was separate from the business world in an enterprise, but those days are gone. To succeed as a CISO, you must be able to show your organization's cybersecurity value to your c-suite and board. That's probably why cyber risk quantification is fast becoming a top priority among CISOs. Benchmarking your cyber data against the industry is also helpful in painting a picture of where you stand. When it comes time to report to the board, you'll need to speak to them in their language--business-speak.

Cybersecurity has a direct impact on an organization's bottom line. And no one knows that better than the CISO. That's why you need to be out front in presenting the business value of cybersecurity. Only you can give your executive team the full picture.

The majority of CISOs are now realizing that they must lead, teach and persuade executive colleagues who hold the purse strings--because today's cyberwar calls for more and better security measures, solutions and awareness. Breaches are costly.

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

70%

of organizations are mapping cybersecurity investment to business outcomes to **inform budget priorities** [7]

Nearly 50% of the organizations are **linking security metrics to business performance** [8]

Not all threats are created equal

Why prioritization is key

A CISO is responsible for 24-hour protection against threats, but there isn't enough time in a day to respond to every alert. That's why it is so critical to know what threats are most pressing.

> If you are not able to understand your scope and really understand where you should be testing for vulnerabilities, you are missing out on key insights.
>
> **Rogier Fischer - Co-founder and CEO @ Hadrian**

Doing things the old way is no longer working. Choosing which alerts to remediate based on their age leaves room for breaches. And using CVSS scores isn't the best way to prioritize reactions, because the likelihood of risk needs to be determined within the context of your organization.

An effective patch management solution is essential for prioritizing what to patch. It helps reduce breaches and boosts productivity by reducing downtime. But that's not enough. CISOs need to look at misconfigurations and consider their impact on the entire organization.

Nearly a **quarter** of alerts are ignored [12]

Nearly **50%** of all security alerts are false positives [10]

Security teams spend more than **25 minutes** investigating one alert [11]

Cybersecurity is not about being reactive anymore

It's about being proactive

Threat actors don't sleep, and that's why your organization needs to be protected 24x7x365. With Hadrian, continuous monitoring of your attack surface is automated. Our Orchestrator AI, at the heart of our platform:

- Searches for vulnerabilities and misconfigurations.
- Identifies potential attack paths.
- Ranks risks by impact and likelihood of exploitation.
- Accurately prioritizes remediation efforts.
- Reduces response time.

> Modern Security doesn't just mean traditional security with cloud native solutions tacked on. It requires an entirely different approach that emphasizes dynamic, granular, and nuanced control rather than legacy checklists. [13]
>
> **Cloud Native Computing Foundation**

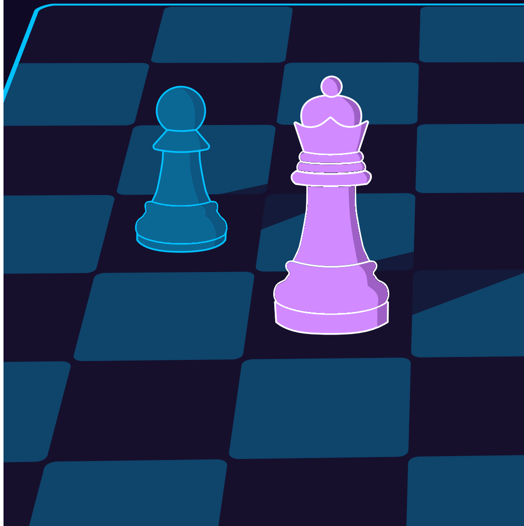
Reacting to threats is a slow process, at best. Proactively monitoring on a continuous basis raises the bar on your security posture. And this is much needed. Because the entire game has changed.

Orchestrator AI is designed by hackers to beat hackers, at their own game. It's like a real world adversary, and it does it by dynamically chaining 200-plus "hacker" modules together.

Attack surface discovery takes more than **40 hours** at 72% of organizations [14]

Only **51% of global enterprises** are able to fully define the extent of their attack surface [15]

80% of public exploits are published before the CVEs are published [16]



Continuous Threat Exposure Management makes a CISO's job easier

Without help, you are basically flying blind

Most enterprises today fall somewhere along the continuum of vulnerability management models. Some identify organizational assets that are accessible from the internet using scheduled scanning and some integrated automation. Others are fully automated and are beginning to visualize how assets link together. None of this is bad. But it could be better.

Hadrian's Continuous Threat Exposure Management (CTEM) is offensive security testing. It helps you identify and effectively harden your attack surface. CTEM provides real-time insights into:

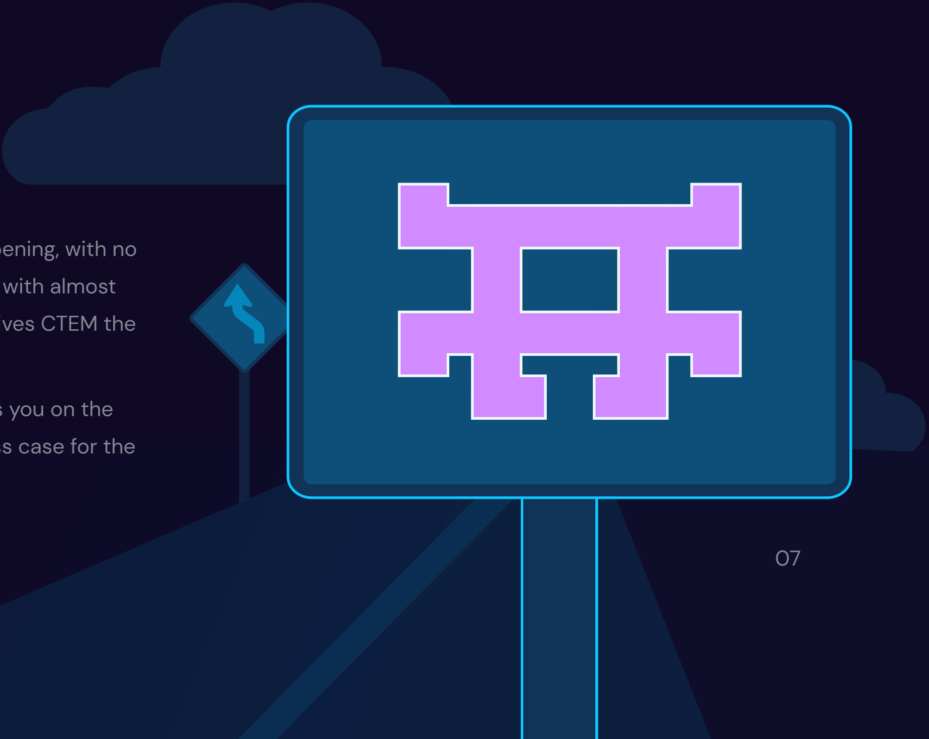
- Where your organization is weakest.
- What a threat actor is most likely to attack.

CTEM also:

- Helps you track progress as you remediate threats.
- Conserves your security team resources.
- Helps you bring the cyber battle to the point of attack, on the edge.

Security validation, like that provided by CTEM, is about knowing what is happening, with no false positives, and no alert fatigue. It's about being able to validate your data with almost 100% certainty, because a data-driven patch management strategy is what gives CTEM the power to contextualize and prioritize your vulnerabilities.

This kind of threat intelligence takes the guesswork out of remediation. It puts you on the offense, one step ahead of cybercriminals. And it helps build a strong business case for the allocation of more resources for your team.



HADRIAN

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.

Get a demo

Learn more

[1] EM360 podcast, "Hadrian: Continuous Threat Exposure Management as a Way to Benchmark CISO Success," May 6, 2023

[2] Gartner, Predicts 2023: Cybersecurity Industry Focuses on the Human Deal, 2023

[3] Ponemon, The Cybersecurity Illusion: The Emperor Has No Clothes, 2019

[4] CyCognito and ESG Report Shows Attack Surface Management is Critical But Few Organizations Do It Well (accessed 6/21/23)

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

[6, 7, 8] Gartner, Persona Priorities, 2023

[9] EM360 podcast, "Hadrian: Continuous Threat Exposure Management as a Way to Benchmark CISO Success," May 6, 2023

[10] Fastly, Inc., Enterprise Strategy Group, Reaching the Tipping Point of Web Application and API Security, 2021

[11] IDC, In Cybersecurity Every Alert Matters, 2021

[12] IDC, 2021

[13] Cloud Native Computing Foundation, Cloud Native Security Microsurvey, 2021

[14] Randori and Enterprise Strategy Group, Trends in Security Hygiene and Posture Management, 2023

[15] Trend Micro, Mapping the Digital Attack Surface, 2023

[16] Palo Alto Networks, Ransomware Extortion Report, 2023

Trusted by market leaders

BIOLANDES

CTC GLOBAL

beyond.

KCK

KINGSWAY CAPITAL

bank prov.

LEROY MERLIN

London Business School