HADRIAN

WeatherTech protects its proprietary technology with Hadrian's continuous monitoring

Manufacturing | Illinois, USA

Challenge

- # WeatherTech utilizes third-party platforms as part of its technology environment. Attacks on any of these providers can expose WeatherTech to critical cyber risks.
- # WeatherTech's proprietary technology and processes allow WeatherTech to stay competitive. IP theft can be detrimental to the business.
- # External risk assessments are frequently requested by partners, but they are time- and resource-intensive.
- # As a long-established company, WeatherTech has developed a complex network of IoT and OT, which is becoming increasingly difficult to manage.

Solution

- # Hadrian's innovative asset discovery engine scans the entire internet for WeatherTech's digital assets and maps them on a clustered Asset Graph.
- # Autonomous AI-driven fingerprinting allows Hadrian to gather details on Technologies (3rd party vendors) and DNS records associated with WeatherTech's domains.
- # Hadrian's proprietary reconnaissance technology collects insights into the context of these assets, creating a prioritized list of risks.
- # Executive Summary Export enables WeatherTech to produce an external risk report to its partners in one click.
- # Hadrian's eventing mechanism monitors for new changes in the environment 24x7x365 to identify potential risks the moment they occur.

WeatherTech®

About WeatherTech

WeatherTech designs, manufactures and supplies world-class auto-, home- and pet- plastic accessories in the US. The security team at WeatherTech was looking for an external monitoring solution to safeguard its patented technology from IP theft.

1989

Foundation

84+

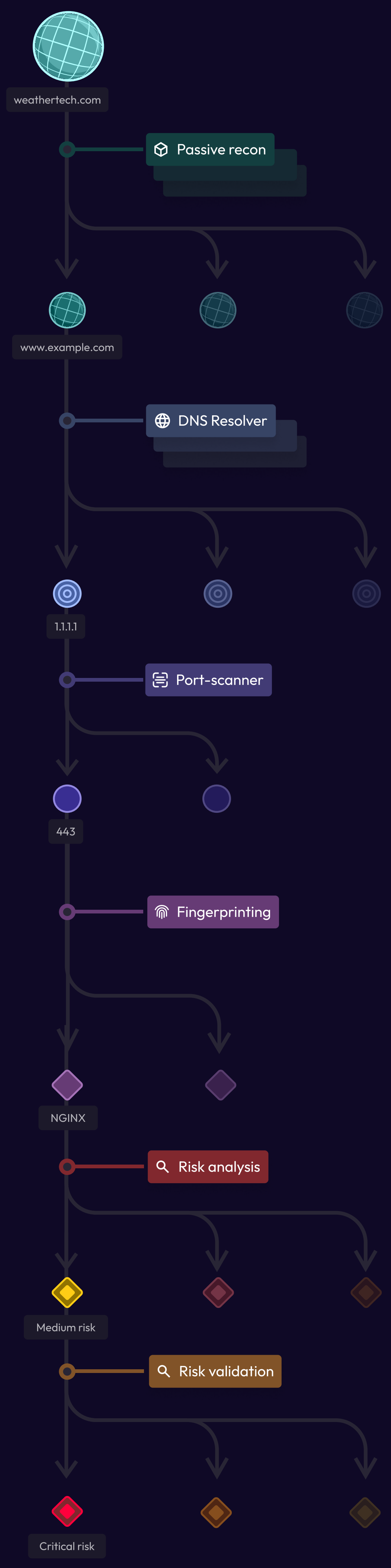
Countries distributing to

USA

Manufacturing

Outcome

Going deeper to safeguard IP



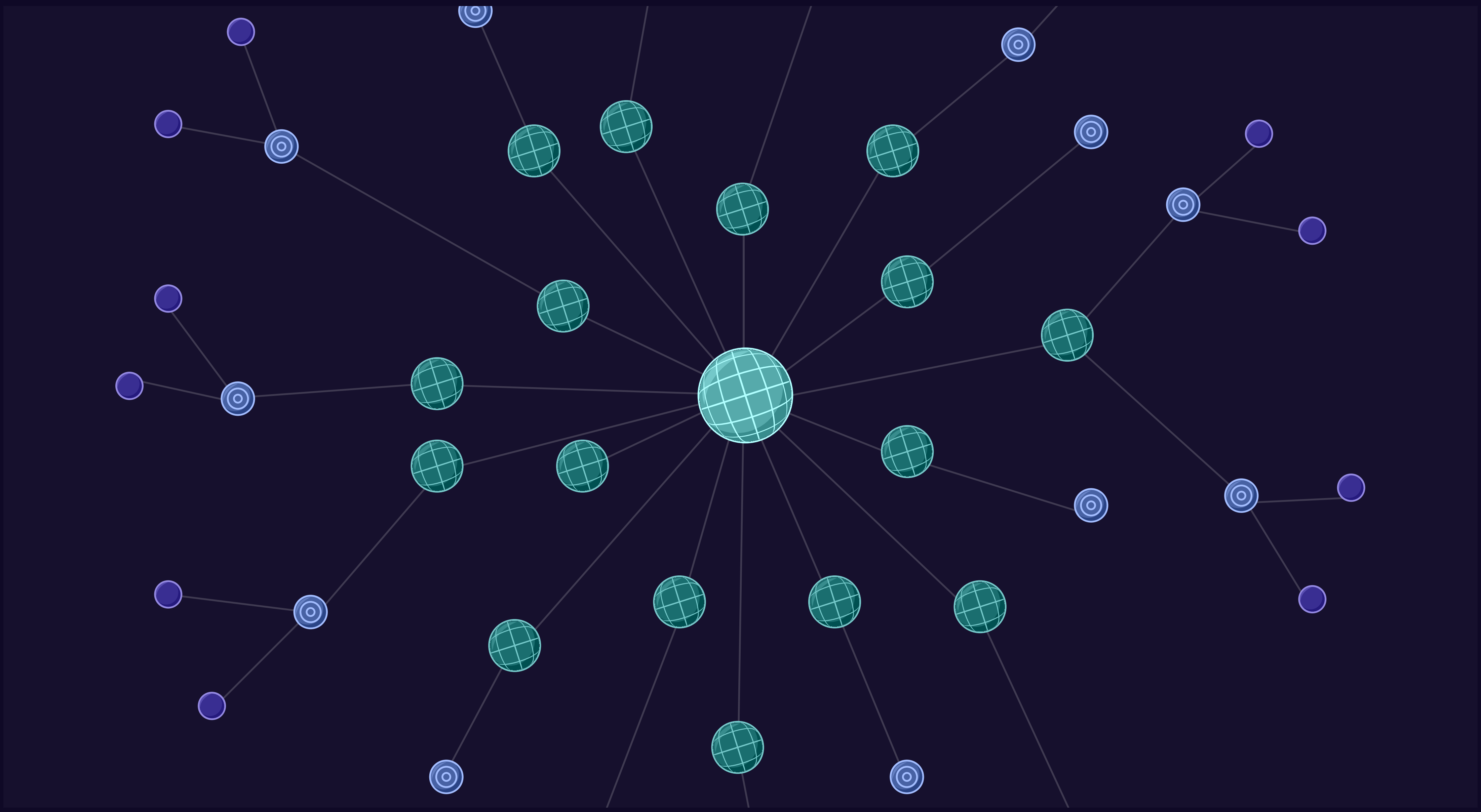
WeatherTech invents, engineers, and manufactures its products all in-house. Its proprietary technology and processes allow it to stay competitive in the market. However, some IP is located on 3rd party platforms creating additional risk exposure. In May 2023, after a new vulnerability was disclosed, WeatherTech's security team observed a string of automated attacks on their main domain provider. This led them to look for a solution that could provide best-in-class continuous exposure monitoring of their 3rd party vendors.

Hadrian's innovative outside-in security platform was the ideal solution for their needs. After WeatherTech was added to the Hadrian platform, immediately Hadrian's investigative Orchestrator AI scanned the entire internet to identify and analyze assets that belonged to WeatherTech. Using proprietary fingerprinting and reconnaissance technologies, Hadrian was able to go a level deeper and gather data around the context of each asset (Technologies, versions, configurations, 3rd party providers).

Then Hadrian's AI security engine began to deploy hacking modules on its findings, identifying real and relevant risks for WeatherTech. Each risk was assigned a level of criticality based on its unique context. The end results were visualized in a clustered Asset Graph, so that WeatherTech's security team could understand how each risk propagated the company network.

Hadrian went beyond other solutions by verifying each risk. This meant WeatherTech did not have to waste time on chasing false positives and could focus on remediation, which resulted in better patching cadence.

> Hadrian's innovative technology and experienced team wowed us from the first meeting. The platform discovered risks that other solutions did not find, and the lack of false positives was another big 'plus'. At which point, it was a no-brainer for us to add the solution to our security stack.
>
> Jason V, CISO, WeatherTech



Continuous security, without operational disruption

Whilst undergoing digital transformation and connecting new Operational Technology to the network, WeatherTech's external attack surface continues to evolve. Their ever-changing attack surface, coupled with the increase in automated attacks, created a business case for a proactive solution. WeatherTech was concerned if they could achieve continuous proactive security without disrupting their business operations.

Hadrian's platform was designed to provide 24x7x365 monitoring without any disruption to the client's systems. Hadrian has two types of scanning - active and passive. Passive scanning is virtually 'silent' and cannot impact the infrastructure. The active scanning is only deployed when necessary, thereby spreading the 'load' on the network. If a new asset is discovered or the configuration of an existing one changes, an active scan may be triggered. Thanks to this innovation in scanning, Hadrian is able to provide probing and monitoring with no disruption to operational continuity.

> Hadrian was able to analyze our attack surface in such depths and find those risks other tools didn't pick up on. It's amazing to work with a tool with so little noise. If it came from Hadrian - we know it's real.
>
> Jason V, CISO, WeatherTech

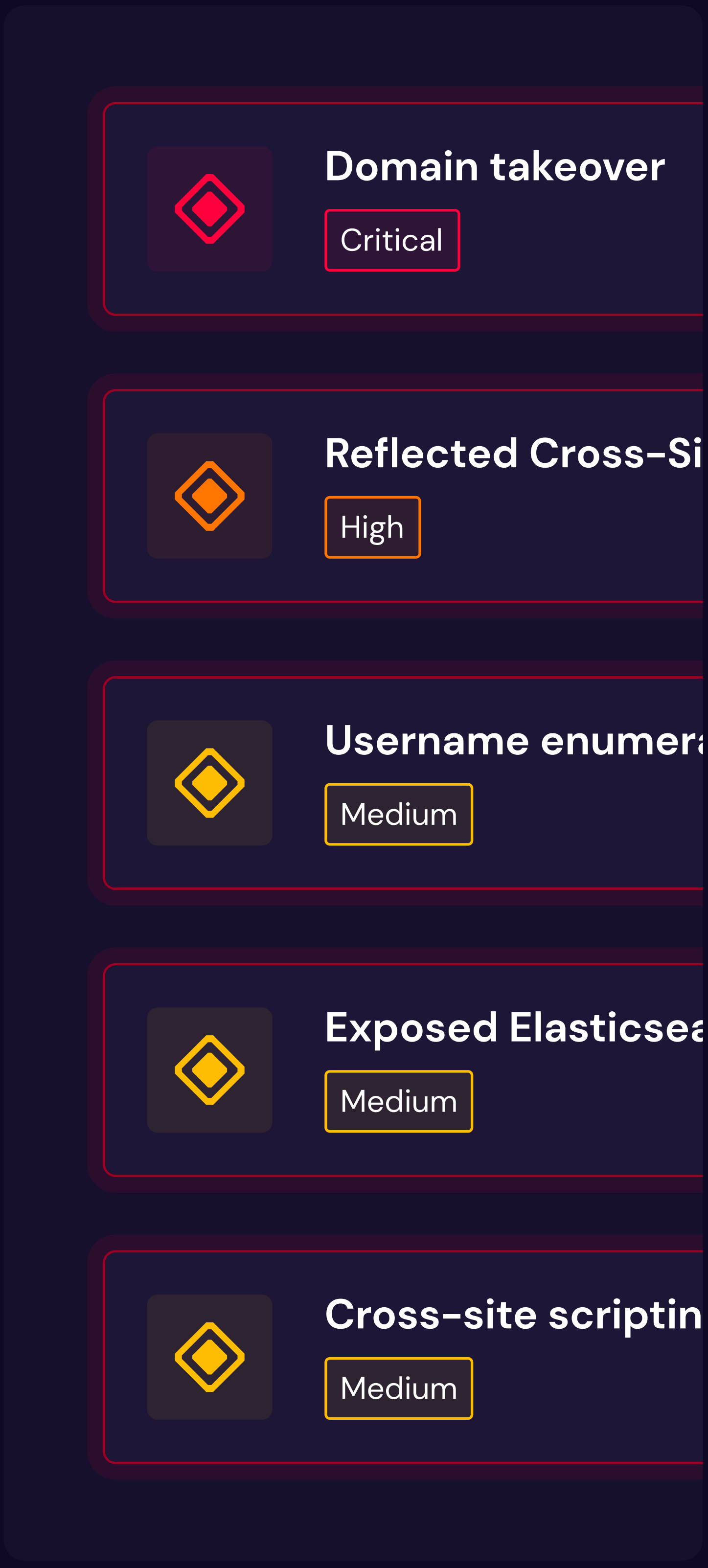
Gaining the trust of partners with risk transparency

With distribution links in over 80 countries, WeatherTech relies on global partners to enable its operations and growth. As a consequence, the company is regularly required to prove compliance and undergo due diligence. Compliance reporting was previously resource-intensive for WeatherTech's security team, as it had to be done manually and by contracting external services.

Hadrian's platform provided Weathertech with a one-stop-shop for their external risk management. The platform's user-centric features catered to teams like WeatherTech, helping them streamline remediation, compliance and risk communication.

Besides the aforementioned risk verification that saves security teams days of time, Hadrian uses stakeholder-specific risk-scoring. This alternative methodology assesses risks more accurately by considering how actively risks are exploited, the technical impact they could have, whether the exploit could be automated, and the impact on the business operations. As a result, companies gain a more accurate metric of their external risk exposure that they can communicate.

Furthermore, Hadrian's Executive Summary Report feature allows the information to be exported and shared with other stakeholders in one click.



Domain takeover
Critical

Reflected Cross-Si
High

Username enumera
Medium

Exposed Elasticsea
Medium

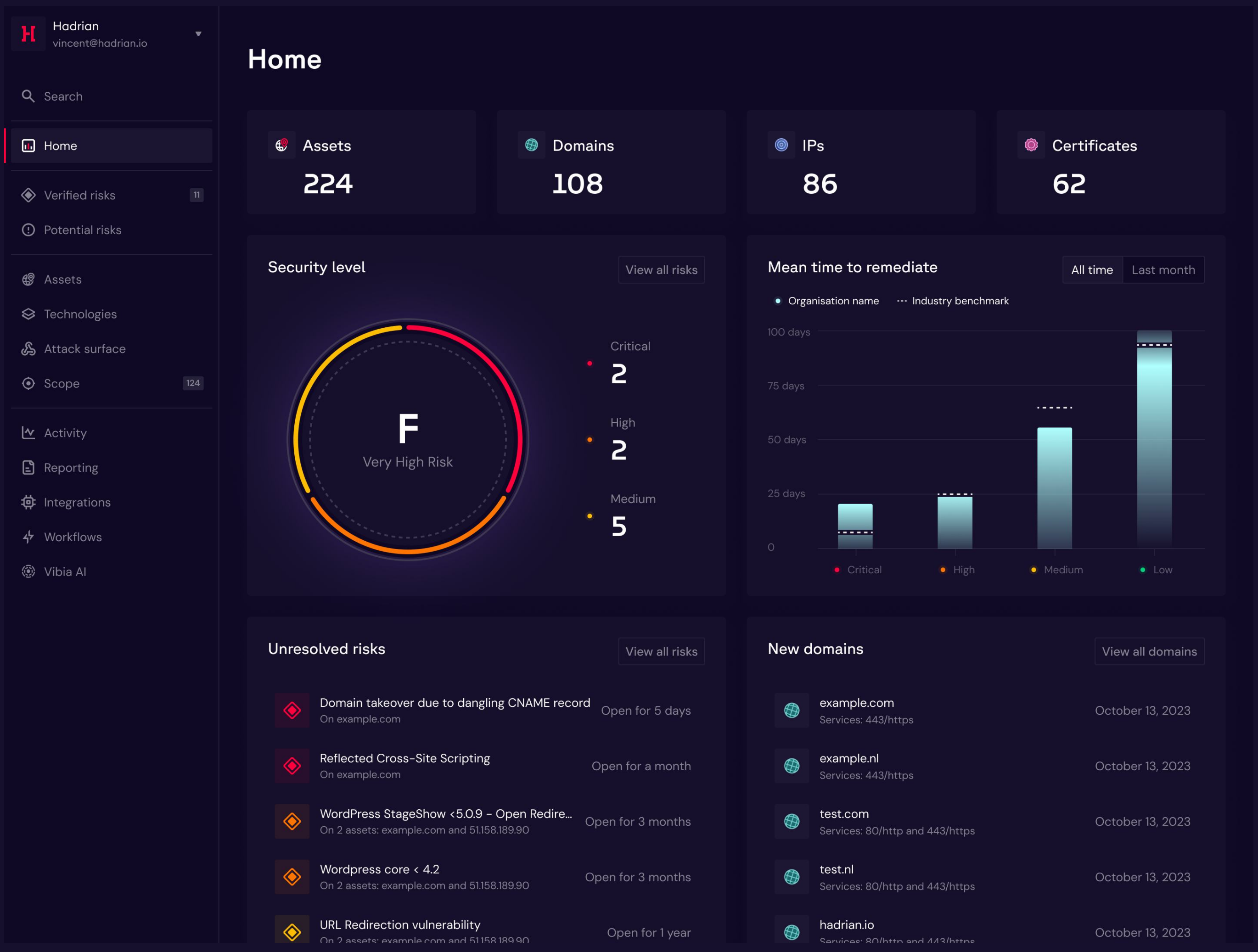
Cross-site scriptin
Medium

Get hands-on with the platform with a quick 15 minute demo

We only need your domain for our system to get started autonomously scanning your attack surface.

Book a demo

Learn more



Home

Assets 224

Domains 108

IPs 86

Certificates 62

Security level

F
Very High Risk

Critical 2

High 2

Medium 5

Mean time to remediate

Unresolved risks

Domain takeover due to dangling CNAME record
On example.com
Open for 5 days

Reflected Cross-Site Scripting
On example.com
Open for a month

WordPress StageShow <5.0.9 - Open Redire...
On 2 assets: example.com and 51.158.189.90
Open for 3 months

Wordpress core < 4.2
On 2 assets: example.com and 51.158.189.90
Open for 3 months

URL Redirection vulnerability
On 2 assets: example.com and 51.158.189.90
Open for 1 year

New domains

example.com
Services: 443/https
October 13, 2023

example.nl
Services: 443/https
October 13, 2023

test.com
Services: 80/http and 443/https
October 13, 2023

test.nl
Services: 80/http and 443/https
October 13, 2023

hadrian.io
Services: 80/http and 443/https
October 13, 2023