HADRIAN

Case Study

Working with Leroy Merlin's security team to prioritize risks in alignment with their needs

Retail | Milan, Italy

Challenge

- # Implementation of websites, mobile apps, and digital payment methods to support e-commerce lead to expanding attack surfaces
- # Customers making purchases online expose themselves to compromised financial accounts, PII and payment card information
- # Attacks lead to loss of revenue and credibility for impacted retailers

Solution

- # Hadrian's attack surface management tools used open source data collectors and passive data sources to identify assets previously unknown to Leroy Merlin
- # Cross-asset testing analyzed assets across multiple cloud sharing providers and domains and provided information on how they linked together
- # Fingerprinting technology contextualized assets by considering the language of the application, version and common vulnerabilities
- # Insights collected were used to develop unique attack paths tailored to Leroy Merlin's attack surface
- # Hadrian collaborated with Leroy Merlin's security team to prioritize risks in alignment with their needs

About Leroy Merlin Italy

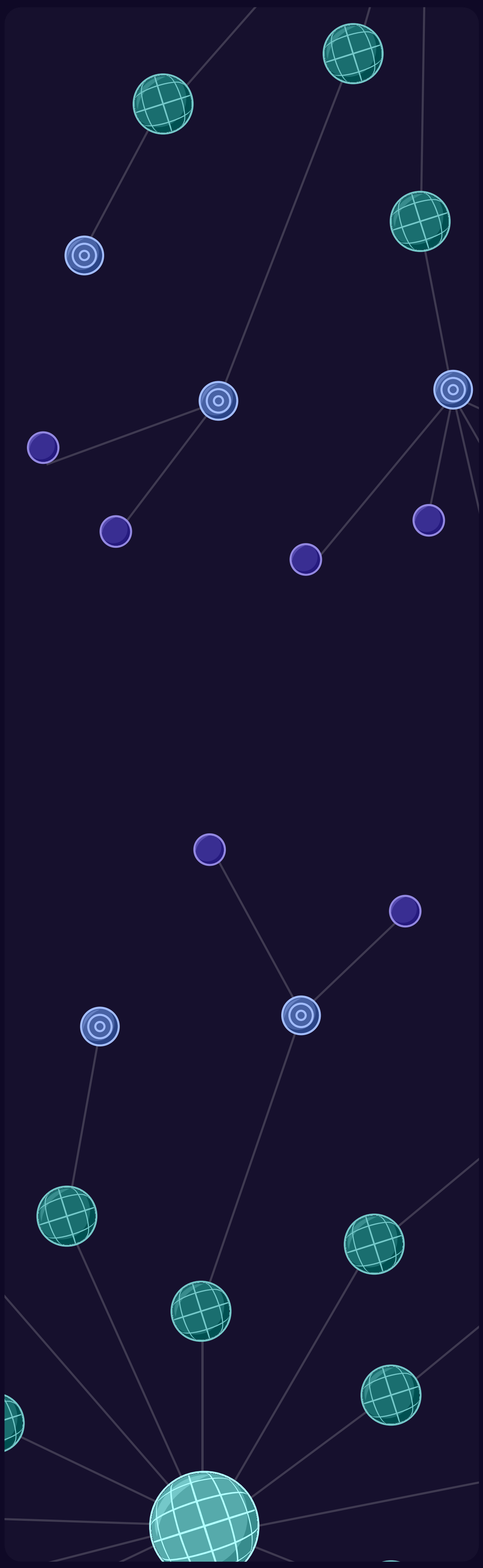
Leroy Merlin Italy is subsidiary of Adeo and is based out of Milan, Italy. A home improvement and gardening retailer, Leroy Merlin serves countries in Europe, South American and Africa.

Leroy Merlin has 9000+ employees, and €7.5B in annual revenue. In 2020 Leroy Merlin accelerated its digital and cloud transformation, developing online shopping tools and an app.

9000+
Employees

€ 7.5B
Annual revenue

Outcome



Discovering Forgotten Assets

Hadrian deployed asset discovery tools with the express purpose of identifying unknown assets. In the case of Leroy Merlin, Hadrian used prior knowledge of e-commerce security to deploy tools which targeted areas most likely to contain forgotten assets.

For example, application developers in the e-commerce industry often accidentally leave administration pages available allowing attackers to access sensitive administration functions. Hadrian used this insight and deployed a hacking module designed to identify forgotten administration directories/pages.

Hadrian was able to identify a vulnerable endpoint with an unmonitored administration page.

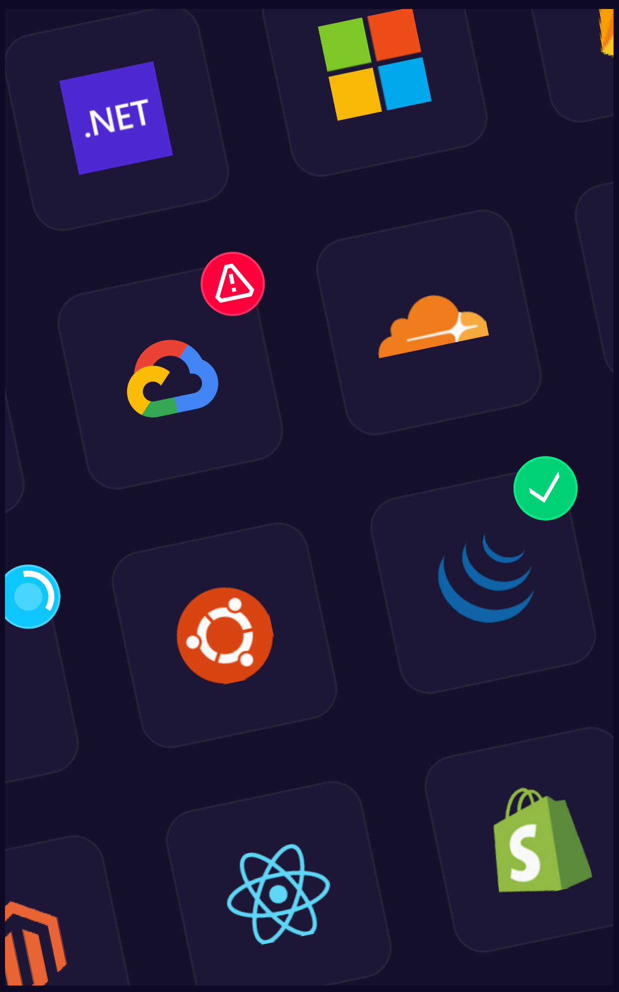
100+

False positives removed

3

Critical risks found

> Hadrian's platform identifies vulnerabilities in a deeper way than other fully automated tools. The insights provided by Hadrian helped us to improved our systems hardening. Excellent insights.
>
> CISO - Leroy Merlin



Developing Targeted Testing to Identify Potential Data Breach

When a forgotten or unmonitored asset was identified Hadrian drew on open source information and its own logic to determine relevant attack paths. Targeted testing allowed Hadrian to validate Leroy Merlin's security without overburdening IT infrastructure.

In the case of the unmonitored administration page Hadrian was able to determine the most effective test by considering the context of the application, specifically its language and framework. Hadrian ran a test which often revealed risks on assets with similar frameworks.

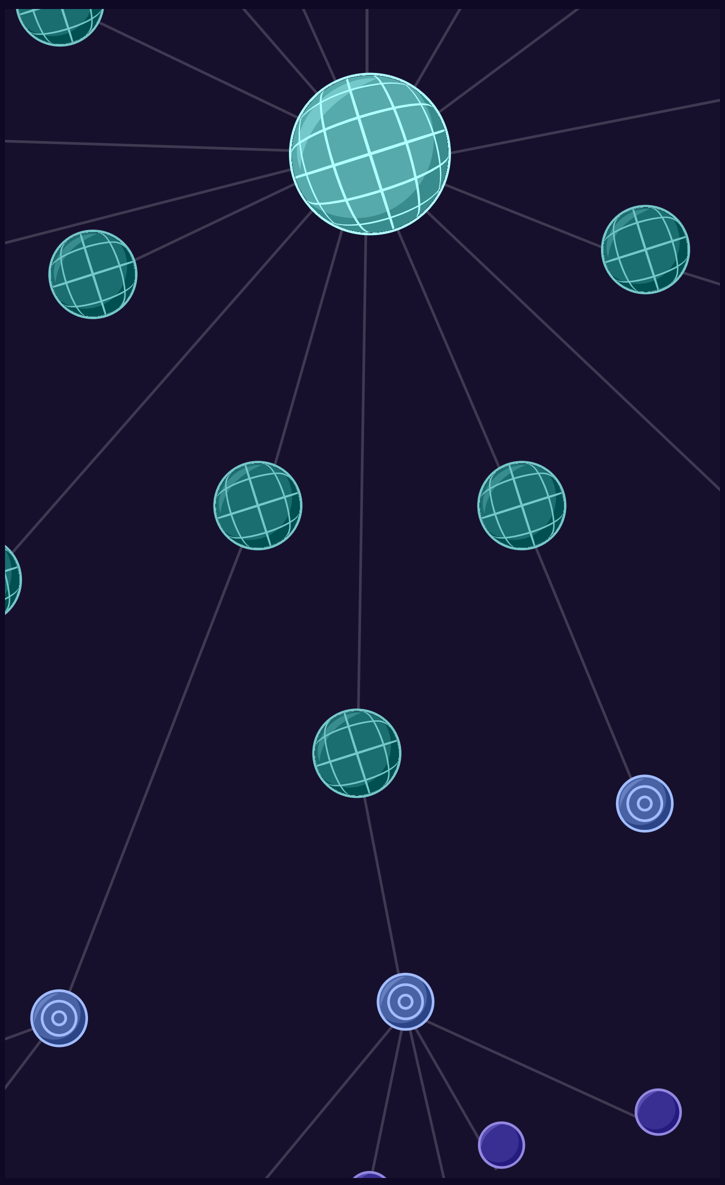
The test revealed credentials for database passwords and Google Cloud, as well as cookies containing sensitive user information.

Eventing Technology Generates Complex Attack Paths

Hadrian was built using event-driven technology. Event-driven testing means long, complicated attacks are broken down into smaller components and can be combined in different sequences allowing for flexibility. In addition, insights collected through past tests trigger new modules resulting in testing methodology that is highly adaptable. The smaller components allow Hadrian to adapt as new insights are revealed.

For example, when Hadrian discovered the cookies in the administration page it triggered a hacking tool. The hacking tool used the cookies to gain access to accounts containing sensitive company and customer information.

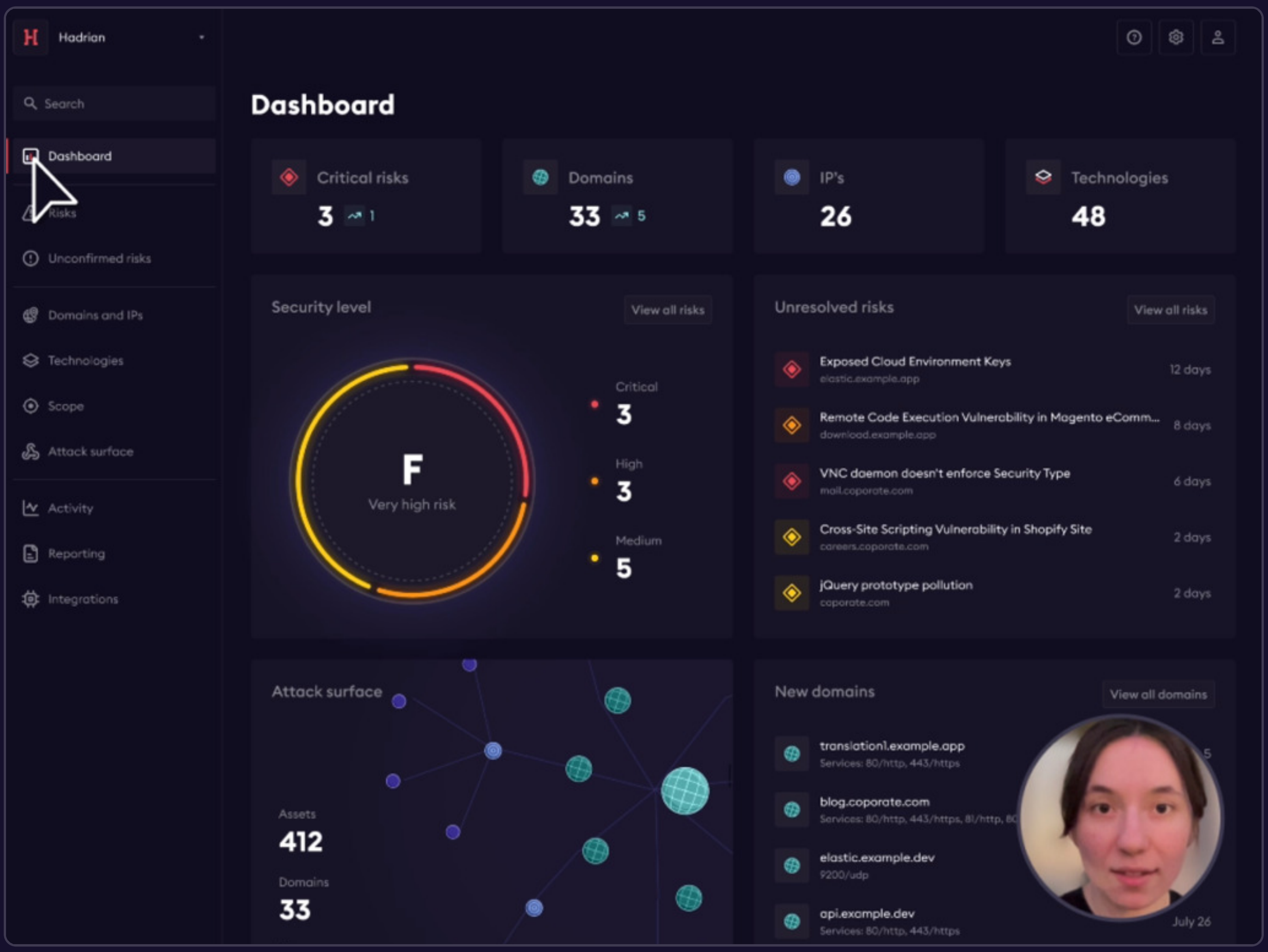
Hadrian will continue to collect insights and deploy tests in response to changes in Leroy Merlin’s attack surface.



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



Dashboard

Critical risks 3 1

Domains 33 5

IP’s 26

Technologies 48

Security level

View all risks

F

Very high risk

Critical 3

High 3

Medium 5

Unresolved risks

View all risks

Exposed Cloud Environment Keys elastic.example.app	12 days
Remote Code Execution Vulnerability in Magento eComm... download.example.app	8 days
VNC daemon doesn't enforce Security Type mail.coporate.com	6 days
Cross-Site Scripting Vulnerability in Shopify Site careers.coporate.com	2 days
jQuery prototype pollution coporate.com	2 days

Attack surface

Assets 412

Domains 33

New domains

View all domains

translation1.example.app Services: 80/http, 443/https	5
blog.coporate.com Services: 80/http, 443/https, 81/http, 80	
elastic.example.dev 9200/udp	
api.example.dev Services: 80/http, 443/https	July 26