HADRIAN

DAMEN

CASE STUDY

Damen Shipyards Group

About Damen Shipyards Group

Damen Shipyards Group owns and operates over 50 shipyards, repair facilities, and related businesses across 120 countries. The company specializes in ship design, construction, maintenance, and repair services across a wide range of watercraft of all sizes.

REVENUE	COUNTRIES	EMPLOYEES
€3.1B	120	12,500

Challenges

01 **Digital transformation**

Damen aims to be the world's most connected shipyard, with its digital experience platform at the core. However, as the number of digital touchpoints grows, so does the attack surface, increasing the workload of their security team.

02 **Overloaded teams**

Damen's utilized Security Scorecard to benchmark security posture, but the volume of alerts was high and contained a high portion of false positives, overwhelming security teams.

03 **Global presence**

Damen Shipyards Group consists of over 30 operating companies, reflecting its presence in more than 100 countries and its growth through acquisitions. Having fragmented security processes and teams can make coordinating remediation difficult.

Solution

✓ **Automating Attack Surface Management**

Damen has fully automated the process of mapping the attack surface. Hadrian scans the internet to build an inventory of Damen's external-facing infrastructure, utilizing ML-algorithms to identify forgotten assets and shadow IT.

✓ **Proactive remediation with validated results**

Damen dramatically reduced the amount of time spent triaging false positives, focusing on a small number of validated issues. Hadrian provides reproduction steps for all exploits, enabling the team to quickly confirm the results and become more proactive.

✓ **Faster remediation with global collaboration**

Damen's centralized security team can monitor the entire attack surface with Hadrian and easily collaborate with the local entity's security team, the IT department, and 3rd parties to quickly remediate any security vulnerability in their attack surface.

Outcome

Mapping an Ever-Changing Attack Surface

Damen Shipyards Group has been implementing a digital experience platform (DXP) to enhance customer engagement, streamline operations, and drive digital transformation. Alongside its technology roadmap, Damen has evolved its security posture, implementing Zero Trust and Security by Design principles, along with other key improvements in recent years.

As Damen's digitization program progressed, more digital customer touch points were exposed to the internet, dramatically increasing the size and rate of change of the attack surface. When a forgotten marketing webpage was exploited and utilized for SEO poisoning, the security leadership at Damen recognized that the visibility of their organization was limited and that there were blind spots.

With Hadrian, Damen has been able to completely map their attack surface and have a detailed inventory of assets including the certificates, technologies and services associated with each one. Hadrian utilizes machine learning (ML) algorithms to identify forgotten assets and shadow IT, building a unique digital fingerprint of assets, and scanning for assets that match it. The inventory is updated in real time, allowing Damen to proactively remove assets that should not be exposed.

Increasing Risk Detection Accuracy

Damen's security operations team is continuously monitoring and remediating issues in order to maintain a strong security posture. They were utilizing Security Scorecard to analyze their posture and understand how their organization compared against others in their industry.

While the Security Scorecard assessment was valuable to the board and senior stakeholders, the security team found the results very noisy. There were hundreds of issues and many of them were false positives, it took many hours of time to validate, prioritize, and triage each one.

Damen introduced Hadrian to automate the removal of false positives that their team had to manage. The "Verified Risks" feature shows only vulnerabilities that have been tested and confirmed to be exploitable. Included with each Verified Risk are detailed reproduction steps, uniquely generated for that asset, allowing security teams to validate them quickly.

Coordinating Remediation Across Teams

a significant portion still operates independently. With multiple teams involved, identifying the responsible remediation team, providing the necessary information, and confirming resolution was a challenge.

Hadrian provides the central security team with a single pane of glass to monitor the entire attack surface of Damen. The platform also enables Damen to assign role-based access, giving different teams visibility of different areas of the attack surface.

When an issue arises, Damen uses the Secure Share collaboration feature to provide the resolving team with all necessary risk details and remediation steps. This has enabled Damen to respond more effectively and measurably strengthen its security posture.

> "Other tools we evaluated generated a lot of alerts that had no value to us and created a huge backlog for our team to investigate. Hadrian enables us to pinpoint the real security issues that we should be working on."
>
> Hans Quivooij
> CISO at Damen Shipyards Group