PPG protects its attack surface with continuous monitoring of external threats

About the company

PPG is a U.S.-based multinational company in the paints and coatings industry. Through its Comex brand and other subsidiaries, the company operates an extensive network of physical stores, digital platforms, and authorized dealers. PPG remains strongly committed to innovation and brand protection.

The Problem

Before Axur, PPG needed a solution capable of controlling the exposure of sensitive data, such as code repositories, credentials, and new domains. In addition, the company needed a tool to identify fake profiles on social media, distinguish legitimate dealers from scammers, and monitor brand misuse across marketplaces and digital platforms.

Even when using other monitoring tools, the coverage was limited, and the response speed was insufficient for the scale of risks.

The Solution

Axur provided full visibility into PPG's digital attack surface. The platform began continuously monitoring code repositories, exposed credentials, unauthorized domains, social media profiles, and marketplaces.

With the ability to request takedowns and investigations directly from the platform, PPG's security team gained agility to respond to critical incidents, untangle complex cases, and act proactively before they could cause a greater impact on the business.

Use Cases that Made a Difference

Code Exposure on GitHub

PPG discovered that external developers hired for specific projects had published proprietary company code in public GitHub repositories. In addition, malware developments and spam campaigns using company domains were identified. Without Axur, this exposure would have gone unnoticed, putting intellectual property and operational security at risk.

Compromised Credentials

Continuous monitoring detected credentials stolen by infostealers that granted access to systems without multi-factor authentication. The team identified domains and portals created by developers without the security team's knowledge. These credentials were valid and provided unrestricted access, representing a critical entry point for attackers.

Brand Misuse

The platform identified an individual posting inappropriate photos on social media while using Comex products and logos. The ability to monitor profiles on platforms such as Facebook, Instagram, and others allowed the team to quickly identify the individual, request content removal, and protect the brand's reputation before the damage escalated.

Impact in Numbers

+ 1.447 takedowns requested in 6 months

1.300 fake profiles identified

450 piracy or illegal sale cases detected

Incident Investigation Involving Hacktivism

Digital displays installed in Comex stores, managed by an external partner, were compromised by hacktivists who modified advertising content to display messages related to the conflict in Gaza. PPG leveraged Axur's incident investigation data to trace the origin of the attack, understand the full context of the threat, and take preventive measures to mitigate risks and avoid recurrences.

Data Exposure in a Proof of Concept (POC)

During the evaluation of a solution offered by a vendor, generic credentials were used to conduct a proof of concept (POC). After deciding not to acquire the tool, the vendor failed to remove the test interface. Axur detected that the POC was still active, with exposed credentials and real PPG data, including information belonging to a company director. The incident was handled immediately, preventing the leak of sensitive corporate information.

Beyond Traditional Coverage

Axur stands out by covering areas that other solutions fail to reach. While traditional tools focus solely on monitoring the dark web and domains, Axur's platform supervises digital marketplaces, social networks, and code repositories, attack surfaces increasingly exploited by cybercriminals.

The ability to request takedowns directly from the platform made operations much faster. In a highly competitive market, Axur stands out for its advanced technology, which provides broad coverage and intelligent automation, accelerating decision-making and significantly reducing exposure time to risk.

> *"Ease and speed are the key points. Axur sees things that other tools don't. There's no other solution in the market that offers what Axur offers. Whenever we have an issue or a question, Axur resolves everything quickly. Plus, the cost-benefit ratio is very competitive."*
>
> **Ernesto Origel,**
> **IT Security at PPG**

PPG strengthened its digital security posture with a solution that provides complete visibility, rapid response, and coverage in areas that other tools often overlook. With Axur, the company protects not only its systems and data but also its reputation and the trust of millions of customers.

Protect Your Brand and Operations Against Digital Threats

Discover Axur's solutions and expand the monitoring of your external attack surface.

BOOK A DEMO

Gartner Peer Insights 4.9 ★★★★★

Learn more about our solutions at: **axur.com**

///AXUR