cybersixgill

CYBERSIXGILL ENABLES ONE OF EUROPE'S LARGEST PUBLIC PENSION OFFICES TO CAPTURE EMERGING CYBERSECURITY THREATS

Customer Overview

Managing one of the largest public pension systems in Western Europe, the customer oversees 16 regional pension funds, thousands of employees, and millions of insured persons and pensioners domestically and abroad. In addition, the company is tasked with processing and paying pensions, conducting employer and insurance tax audits, providing participation benefits such as medical rehabilitation, and distilling information and advice through various touchpoints, including online, telephone, and in-person consultation locations.

Business Challenge

Serving millions of residents domestically and abroad with pension services and support, the company oversees regional pension funds with multiple offices across Germany. While the company had a series of checks and balances to ensure compliance and consumer protection, it lacked visibility when it came to dark web threat intelligence to protect its business-critical assets. Additionally, it did not have access to crucial information, resulting in a reactive cybersecurity posture.

Before implementing Cybersixgill, the company used numerous cybersecurity processes like SIEM, vulnerability management, and threat intelligence for several years. Additionally, they did periodic penetration tests on their web applications but did not know if there were activities on the dark web about their organization. This was a significant blindspot for them.

The company needed a solution that could capture real-time intelligence as it happened and before attacks were deployed.

16
regional pension funds

thousands
of employees

millions
of insured persons and pensioners

Solution

Through free and paid feeds, the company first learned about Cybersixgill through its extended detection and response (XDR) provider, Anomali. Then, the company tested, paid fees for 30 days, and contacted Cybersixgill. Through this, they learned about Cybersixgill's portal.

Cybersixgill provided the company with a product demonstration, during which Cybersixgill found that the company's information was being sold on the dark web. For instance, the company received compromised credentials notifications in some web applications. As a result, the company contacted those responsible about the risks in their web applications to mitigate them.

Cybersixgill worked with the company's security team to implement an effective threat intelligence program. Soon after a seamless integration, the company realized continuous improvements in its cybersecurity processes. Today, the company's security team utilizes the investigative portal daily and receives real-time alerts notifying them of compromised credentials and web applications. In addition, Cybersixgill's automated Dark Feed has significantly reduced manual processes, improving the company's security posture and operational efficiencies.

About Us

Cybersixgill continuously collects and exposes the earliest possible indications of risk produced by threat actors moments after they surface on the clear, deep, and dark web. This data is processed, correlated, and enriched with machine learning techniques to create profiles and patterns of threat actors and their peer networks, delivering critical insight into each threat's nature, source, and context.

Our extensive body of threat intelligence can be consumed through scalable, searchable solutions and seamlessly integrated into our partner's existing security stacks, arming teams with critical insights to proactively block threats before they materialize into attacks. For more information, visit cybersixgill.com.

> "Our relationship with Cybersixgill comes down to partnership and trust; it's about protecting the organization. Cybersixgill provides information we can't get from any other source. With Cybersixgill's insights, we can preemptively stop an attack and understand a threat actor's method of operation. It's one of the best solutions I have seen in my security career."