CybelAngel

CUSTOMER CASE STUDY

Sanofi Secures Attack Surface With The Help Of CybelAngel

How the global leader in healthcare prevents hundreds of data leaks from turning into major breaches across complex supply chains

> With CybelAngel, we establish a new border of detection outside of our architecture, encompassing the world of our partners and suppliers, where we can’t, by design, take control of their security.

Jean-Yves Poichotte

Global Head of IS Security, Sanofi

ABOUT SANOFI

Sanofi is a global leader in healthcare across seven major therapeutic areas from cardiovascular to vaccines.

The company was founded in 1973 and now employs over 100,000 people across more than 100 countries.

It relies on 73 manufacturing sites operating in 32 different locations.

Though the covid crisis has shed a dire light on the structural vulnerabilities and daunting attractiveness of global pharmaceutical supply chains for hackers, cyber-attacks against players like Sanofi aren't news. Both state-affiliate and criminal organizations have well understood how targeting healthcare organizations can be an efficient way to weaken nations, and make some money while doing it. "Some people just want to see the world burn."

CHALLENGES

In a recent interview, Jean-Yves Poichotte, Global Head of IS Security, Sanofi, described "facing cyber-criminal activities against ourselves as day-to-day cyber-activity." As an organization providing healthcare solutions in more than 170 countries, Sanofi has maintained a state-of-the-art approach to cybersecurity, through the work of its IS Security team.

"Protecting Sanofi is great, explains Jean-Yves Poichotte, but it is not enough because we are not alone." Indeed, almost half of Sanofi's operations are in fact delegated to third parties.

"Each time we open our organization, explained Jean-Yves Poichotte, it is a new opportunity for the hackers to penetrate our infrastructure, and to steal some information. The others are my weak point. So **our posture is to say that if we can't protect, we have to detect** and to react fast in order to prevent the damages. And this is when CybelAngel comes into play."

> our posture is to say that if we can't protect, we have to detect.

SOLUTION

"Sanofi has been working with CybelAngel for five years. **Our intent is to push CybelAngel's digital risk protection solution widely on our market, in order to establish a new border of detection outside of our architecture, encompassing the world of our partners and suppliers, where we can't, by any type of action, take control of their security.** To compensate as much as possible the risk related to our vendors is to detect any data leakage. This is what we achieve with CybelAngel."

Thanks to CybelAngel's contextualized Incident Reports, Sanofi's IS Security team is able to mitigate risk on the spot. "Timing is everything. I know that with CybelAngel, we are sure to receive alerts upon detection. If the Incident is critical, CybelAngel's team will do everything to reach someone within my team to make sure the issue is dealt with. The information compiled in the Incident Reports allows us to contact the third party immediately to start the remediation."

"Without this intelligence preparation and context analysis, we would have to investigate which organization is leaking, what contact we have to reach out, resulting in unnecessary loss of time."

More than often, negligence is the primary cause of data leakage: **"People just don't realize that they are not applying the best security practices."** As a mature organization, Sanofi chose to help faulty providers and guide them to secure the data. "When we engage the other entities, we train and educate them using real use cases. We also include them within our single incident response process to improve efficiency and responsiveness over time."

> Timing is everything. I know that with CybelAngel, we are sure to receive alerts upon detection.

CybelAngel's data leak detection solution has become a part of an ongoing vendor risk assessment program. **Each vendor has their own maturity map**, which is communicated to procurement to provide guidance when the time comes to contract or renew with a specific partner. The IS Security team is able to strongly encourage the business to select a preferred list of secure vendors.

RESULTS

- **120+ third-party-related breaches** are prevented each year
- **Increased visibility** over blindspots into vendors' IT infrastructure
- **Incident response down** to hours instead of days thanks to zero-false positives, real-time alerting, detailed and actionable incident reports
- **Robust, ongoing vendor risk assessment program**

Watch the full interview