Orange
Cyberdefense

Customer stories

SOC provides cyber insurance to P&V Group

- Better insights into the risks
- Reduced workload for internal IT team
- Tickets of much higher quality
- Peace of mind through proven expertise

Security challenge in highly digitalized insurance sector

P&V Group is a cooperative insurance group that has been active on the Belgian market for more than 100 years. The insurance solutions are distributed through a network of agents and brokers who work for different brands: Vivium, Actel, Arces and P&V Assurances Verzekeringen. In total, the group has about 1,700 employees. The group's ambition is to provide insurance products that are tailored to the various needs of private and independent customers as well as companies and institutions.

Digitalization today offers the insurance sector opportunities to meet those needs with new services and new user experiences. Think of sending photos with an app to complete a claim file or opening portals where the customer can follow up his own file. But the industry does not escape the challenges. For example, insurance companies hold a great deal of confidential customer information – up to and including their medical history – which makes them an interesting target for cyber criminals. "We work with sensible data and are part of the financial sector: this makes us a popular target for phishing attacks, CEO fraud or ransomware attacks", says **Krist Cappelle, Information Security Program Manager for P&V Group**. Security is therefore very important, but the various agents also have to handle the data in the safest possible way.

In addition, for P&V Group the cloud story brings new security challenges related to authentication and rights management. IT security is also becoming increasingly important in audits. "We receive multiple checks and audits a year from various institutions: the FSMA, the National Bank, and our own audit department."

Solution via SOC

Digitalization, the cloud story, the strict rules regarding authentication and checks, … all of these bring with them a lot of security logs. Finding a way to better manage and handle these many logs was the direct reason for P&V Group to look for a solution. The existing solutions mainly

> "Cybersecurity is like fire insurance. Every year your pay for it and you may think it is a waste of money, until you need it. Then you are happy to have insurance."
> **Krist Capelle | Information Security Program Manager at P&V Group**

created a lot of security logs, but there were not enough people to monitor them all at the right times. "That's why we were looking for a partner that could help us with this through a Security Operations Center or SOC", says Krist Cappelle.

P&V Group defined several criteria. First, it had to be a complete solution that could encompass Windows, Linux and mainframe. A second requirement was that the information had to be usable for the system engineers who needed to find solutions for error notifications and security anomalies reported by the logs. But the SOC's information also had to be transparent to the management to develop a strategic vision and support the necessary IT initiatives. "Through clear reports, the management must be able to see how mature the P&V Group is in terms of IT security, the number of attack attempts, without getting into too much technical detail."

P&V then put an RFP in the market in 2020, and at the end of the process Orange Cyberdefense emerged as the most interesting party. The cost price and the extensive knowledge of the various technologies certainly played in Orange Cyberdefense's favor. Krist Cappelle: "The most important point where Orange Cyberdefense really made a difference, was that they proposed second-generation SOC. Not purely automated, but also containing a pool of security specialists who immediately propose a solution."

Collaboration and benefits

The SOC has been active since 2021 and sits externally with Orange Cyberdefense. The key systems are internally linked with Orange Cyberdefense's SOC. A data lake with a lot of unstructured data, all load balancer logs, firewalls, … Those are monitored by experts of Orange Cyberdefense. "In practice, Orange Cyberdefense examines all security logs in detail and filters them. They then only send us the things we need to check. If a known user logs in, they do not report this (unless the location is suspicious), but if for example an unknown user tries to log in 17 times in 10 minutes, they do sound the alarm", says Krist Cappelle.

The collaboration goes well with meetings at various levels and adapted to different terms and goals. Krist Cappelle: "They know who to address for what and are very dynamic in their approach. For example, during the project there were regular moments when the planning and agenda had to be adjusted because of, among other things, a fundamental change of direction in our data center. Orange Cyberdefense has responded very flexibly. The advantage of Orange Cyberdefense is the fact that they already have in-depth knowledge of the insurance industry. Because they are part of a larger whole, they have much more knowledge internally and you get an answer to every question."

On a technological level, the added value of Orange Cyberdefense and the SOC lies mainly in **having a better overview of all the risks.** Incoming tickets are of a better quality – where there used to be a lot of 'trash', now what comes in is important – so there is **less workload**. **It takes the burden off** the system engineers who can now focus on other issues related to business development. "Because of the scale of the group, they can guarantee that somewhere in the world they have the knowledge for every problem. This way we can turn to them for all our installed technologies. Being able to fall back on the knowhow and expertise of Orange
Cyberdefense also gives us peace of mind", says Krist Cappelle.

Result

As a result, the system engineers know that the security logs they now receive must be looked at immediately. “In addition to a better overview of the activities in and around our IT environment, we also have a more secure environment thanks to the proactivity and initial analysis by the SOC. Moreover, this saves time as false positives are filtered out.”

Security is a topic that is being discussed at the highest level in the organization. There is a lot of budget, which also demands concrete results. For the management, the added value was only clear after the first reports. “As an insurance group we get attacks all the time, but so far no one has managed to penetrate. The SOC reports make that ‘visible’. Because in our sector (IT security), your work is only done when you are ‘invisible’. Thanks to the SOC we can now prove this and report. We can indicate whether we are still up to speed with developments and are still protected against attacks such as those appearing in the media. Above all, the SOC provides assurance that we are mitigating the risks and preventing IT disasters. Because the SOC helps you to prevent this, you stay out of the media and your reputation as a solid partner is upheld. This is certainly crucial in the insurance world. Also towards customers”, says Krist Cappelle about the business benefits.

In that respect, cybersecurity is like fire insurance. Every year you pay for it, and you may think it is a waste of money. Until your house burns down. Then you are happy to have insurance.

The Future

Two years ago, P&V Group’s IT team drew up a security roadmap towards 2024. This helped to convince the management that security is necessary and always requires investments. “The next step in the plan is to raise security awareness among employees and brokers”, concludes Krist.

About Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe’s go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.