Business challenge

As a multinational banking and insurance business, KBC Group needed to oversee and coordinate its cybersecurity response and meet strict regulatory reporting requirements for cyber incidents.

Transformation

When KBC implemented the IBM® Resilient® Security Orchestration, Automation and Response (SOAR) Platform, it gained a central hub for cybersecurity incident response. The company now visualizes threats in its entities and launches local and group-level responses required by numerous regulations.

Results

Provides a single-pane-of-glass view

into cyber incidents across multiple entities in different countries

Allows flexibility to add localized actions

while maintaining an overall standardized framework for incident response

Manages compliance with legal notification requirements

for numerous European-level regulations

KBC Group

How to create a cyber-resilient multinational banking and insurance group

KBC, headquartered in Brussels, Belgium, was formed in 1998 from the merger of two Belgian banks and a Belgian insurance company. The bank-insurance group serves 11 million customers throughout Europe in its core markets of Belgium, the Czech Republic, Slovakia, Hungary, Bulgaria and Ireland. It also has a limited presence in the US and Asia, primarily to serve clients from its core markets. KBC's 42,000 employees strive to offer the group's customers a unique and personalized banking and insurance experience through more than 1,400 branches and various electronic channels.

> *"The Resilient platform automatically triggers crisis management tasks and notifications wherever they are relevant within the banking group."*
>
> —Kris Caron, Head of Crisis and Incident Management, CERT, KBC Group

Share this

The challenge of multilevel cybersecurity

KBC operates across Europe through fully-owned banks and insurance companies with a high level of local autonomy in its core markets of Belgium, the Czech Republic, Slovakia, Hungary, Bulgaria and Ireland. Although financial services regulations are largely driven at the country level, these KBC entities also fall under the purview of the European Union (EU) and European Central Bank (ECB). Several new or updated regulations, such as the General Data Protection Regulation (GDPR) and Payment Services Directive 2 (PSD2), in addition to the ECB's cyber-resilience oversight expectations, placed stricter requirements on the group and its subsidiaries for reporting and responding to cyber incidents and data breaches.

In 2016, KBC formed its Cyber-Expertise and Response Team (CERT) in its Brussels, Belgium, headquarters. The team was tasked with orchestrating the response to cyberthreats throughout the group's multiple entities throughout Europe. The CERT needed to centrally oversee its incident response process, but it did not want to create a large, centralized department for doing so. The group's various European and international entities had well-established, and largely autonomous, security and incident response teams. Rather than duplicate efforts, the KBC CERT would supplement them and ultimately improve on the group's overall cybersecurity effort through heightened awareness and response coordination at the group level.

> ***"We needed speed. We have a lot of reporting regulations, and one is the ECB requirement to report cyber incidents within two hours."***
>
> —Kris Caron, Head of Crisis and Incident Management, CERT, KBC Group

KBC sought a mechanism by which the CERT could record and visualize threats in the group's various entities and launch local and group reporting and responses required by the various regulations.

Kris Caron, Head of Crisis and Incident Management at the CERT, describes the team's relationship with the country-level security offices: "If an incident spans more than one country or if we are requested to take control by local or HQ management, we take over, but otherwise we are in supporting mode. So, we needed to have an overview, a single pane of glass on all incidents."

KBC sought a technology solution to help implement incident response playbooks for different incident types to enable consistent execution across the group. These playbooks provide a step-by-step process, parts of which may be automated, for responding to specific incidents. For example, when malware is detected in a bank's PCs, the playbook will outline the steps for escalation, containment and remediation.

"We needed something which would allow the CERT to coordinate the response and that would integrate with existing technical tools, and automate some responses," says Caron. "On top of that, we needed speed. We have a lot of different reporting regulations, and one is the ECB requirement to report cyber incidents within two hours."

Cybersecurity orchestration and visualization

KBC conducted a request for proposal (RFP) process, which included demonstrations of a number of security reporting platforms, and selected the Resilient SOAR Platform. The Resilient solution offers a powerful foundation for response planning, management and mitigation for a wide range of incident types at multiple levels of the KBC organization.

"A major reason that we chose Resilient was that the people we spoke with really understood cybersecurity and were willing to work with us to adapt it for our specific needs," says Caron. "One key factor was when we went to Boston and met the people there, to shake hands and get to know the organization. This personal contact was the cornerstone for the partnership we currently have to further develop the Resilient footprint."

The Resilient team contributed to integrating the platform with the client's existing security and IT infrastructure. KBC used the standard, preloaded playbooks for common incident types, such as malware, denial of service and phishing, to transform their KBC playbooks into Resilient. Resilient consultants worked with KBC to add specific legal reporting triggers into its playbooks. These included requirements for GDPR, ECB, PSD2 and the EU Network and Information Security (NIS) Directive on critical infrastructure. In addition, the team implemented more cybersecurity threat playbooks, including CEO Fraud and others specific to KBC.

The work with Resilient began in October 2017 with the first go-live occurring in February 2018 with the CERT and Brussels organization. From February to May 2018, Resilient and the CERT worked with other entities to train personnel and integrate the Resilient playbooks into the security infrastructure. During that time, KBC added any local content requested by the country-level organizations.

Caron describes how KBC can use the flexible SOAR platform to augment the group playbooks with local content: "While we left some autonomy to the local entities, we wanted a common taxonomy and basic set of tasks in these playbooks. They can have their own tasks for local processes or regulations, but we needed to stick to a common framework in order to be able to cooperate with multiple teams on the same incident. Therefore, we also switched to English as the common language for registrations."

Centralized view, local and virtual response

The Resilient SOAR Platform now provides the KBC CERT with a single view into cyber incidents across multiple entities in different countries. "I think we benefit the most from bridging all the silos," says Caron. "With a single-pane-of-glass view, we get better insight into whatever is happening in the other countries and can coordinate our response with those teams."

Designed for flexibility and extensibility, the platform allows KBC to add localized responses to playbooks while maintaining an overall standardized framework for incident response. It makes security alerts instantly actionable, provides valuable intelligence and incident context and enables an adaptive response to complex cyberthreats.

Caron states: "The Resilient platform introduced the 'break-the-glass' principle to raise alarms. It automatically triggers crisis management tasks and notifications wherever they are relevant within the banking group."

KBC can now better manage compliance with the GDPR, ECB, PSD2 and NIS legal notification requirements. The Resilient SOAR Platform helps reduce incident response time by taking much of the analytical burden from KBC's cyber analysts. Automating many processes helps the cyber teams prioritize and respond to the most critical incidents quickly, as required by the new legislation.

To test the system, the CERT introduced a cyberthreat drill during a group-wide financial crisis exercise run by the bank's executive committee. The CERT entered the case into the Resilient solution and requested a response. "It was out of the box, something new, and cyber-related, and we got a good, fast response with much less effort than in the past," says Caron. "We were able to concentrate on the crisis mitigation, able to quickly request extra intermediate actions to the group, instead of losing time by calling our international teams."

KBC registers all cybersecurity incidents in the Resilient platform, ranging from small, localized events to larger, group-wide incidents. The group has added an additional 60 users to the platform and continues to expand use to help manage incidents of fraud, e-fraud, vulnerability management issues and more. "We want our offices that are specialized in crisis and incident management to offer the service to other teams now that we have the Resilient SOAR Platform," explains Caron. "We're connected from New York to Hong Kong and across Europe, and business continuity and crisis management are the next domains to tackle."

Solution component

- IBM® Resilient® Security Orchestration, Automation and Response Platform

Take the next step

To learn more about the IBM solution featured in this story, please contact your IBM representative or IBM Business Partner.

> ***"With a single-pane-of-glass view, we get better insight into whatever is happening in the other countries and can coordinate our response with those teams."***
>
> —Kris Caron, Head of Crisis and Incident Management, CERT, KBC Group