Chronicle SIEM

BBVA

BBVA: Collaborating with Chronicle SIEM to predict and prevent cyberattacks using custom AI tools

Ensures optimal security and reliability of BBVA's services

Cybercrime is big business. The World Economic Forum ranks it as the most significant man-made threat to global economies today. Recent research suggests that cybercrime's impact could cost an estimated $10.5 trillion annually by 2025. Financial institutions are particularly attractive targets, accounting for 26% of all attacks world-wide between 2016 and 2020. And, the cost to affected businesses can't be measured in monetary loss alone, with significant reputational damage at stake for those unable to bolster their defenses.

BBVA is tackling this issue head on as part of a wider digital transformation that has seen the business streamline its operations over recent years. It has steadily moved away from a traditional banking model to bring its growing digital capabilities to the forefront. As an institution with more than 160 years' experience, BBVA knows the value of adaptability in meeting the challenges of an ever-changing world. In adjusting to the needs of the 21st century, BBVA has three priorities: reducing operational costs, increasing functionality, and ensuring the security and reliability of its services. "Back in 2001, our President gave a speech outlining the digital journey that was to come," says Juan Calatrava, IT Strategy, Deployment & Regulations Head at BBVA. "What we're seeing today is the result of that vision from almost 20 years ago."

When the time came for the company to build its new 'Security Operations Center (SOC) of the Future' platform, BBVA decided to partner with Chronicle SIEM. The Google Cloud security analytics platform enables them to create an artificial intelligence-based system that detects and prevents possible cybersecurity threats. "Security is paramount for BBVA, but you always have to do things differently from the past," says Jorge Blanco Alcover, Global Head of Security Solutions, BBVA. "Working with Chronicle SIEM offers us the chance to share responsibility for risk management, and to leverage the expertise and infrastructure of Google Cloud to protect our customers."

Chronicle SIEM

BBVA

> Security is paramount for BBVA, but you always have to do things differently from the past. Working with Chronicle SIEM offers us the chance to share responsibility for risk management, and to leverage the expertise and infrastructure of Google Cloud to protect our customers."

—Jorge Blanco Alcover, Global Head of Security Solutions, BBVA

Detecting and responding to threats more intelligently

BBVA's 'SOC of the Future' project began life in 2018, but it soon became clear the project could benefit from outside assistance. "We wanted to add a layer of intelligence to the process," explains Blanco Alcover, "so that we could classify threats and respond more quickly. Due to the scale of the challenge, we soon realized that we needed a partner. There's a joke among some of my colleagues that there's no such thing as the cloud, there's just another person's data center. That means you're sharing all of the regulatory responsibilities, certificates and standards. We needed a partner and knew we had to pick wisely."

BBVA began exploring various options for partnering on the project, but none of the alternatives had the right tools for the job. Everyone involved kept coming back to Google, whose example had been formative in BBVA's original conception of its digital transformation journey. Blanco Alcover adds: "We became aware of Chronicle SIEM and the work that it was doing, and we seemed to share the same goals and philosophy. But Chronicle SIEM had the added computing and engineering power of Google behind it. We ran a pilot with Chronicle SIEM last year to test the technology, as well as the fit with our philosophy and architecture, and it was a perfect match."

Another key Chronicle SIEM feature that drew the BBVA team to the platform is its ability to highly automate the response to potential threats. "Our strategy is to rely on Chronicle SIEM as our main security engine," says Blanco Alcover, "because it's integrated so seamlessly into our own orchestration platform. We love the maturity of Chronicle SIEM's technology but, even more, we love the philosophy behind it, particularly the extreme automation of our responses, which are now faster and smarter than ever."

Chronicle SIEM

BBVA

> Our strategy is to rely on Chronicle SIEM as our main security engine, because it's integrated so seamlessly into our own orchestration platform. We love the maturity of Chronicle SIEM's technology but, even more, we love the philosophy behind it.
>
> *—Jorge Blanco Alcover, Global Head of Security Solutions, BBVA*

Collaborating closely to ensure future success

While the technology Chronicle SIEM provided was clearly a good match for BBVA's needs and values, Santiago Alarcón, Global Head of Google Cloud, BBVA, says the changes resulting from the collaboration with Chronicle SIEM, and BBVA's digital transformation more widely, have had a significant beneficial impact on the company's culture too. "Many people tell us that they want to do something similar, and they think that it's just a question of hiring the right people to install the right software. But transformation isn't that simple, you have to transform the mindsets of everyone within the organization. "The cultural change has been as important as the technological change and the results won people over. Before Chronicle SIEM, we were working with about 60TB /month, and we expect to finish 2021 ingesting and treating 200 TB/month. Plus, we inject three times more data with Chronicle SIEM and we can access in seconds information that previously took minutes or even hours."

Calatrava agrees, and acknowledges that this process has not been without its challenges. "The journey to reach this position has been an educational one," he says, "but you need to be willing to learn along the way and accept the fact that mistakes will be made, before you're ready to roll out to the public. That's not easy for a bank. Now everyone understands exactly what it is that we're doing, we have the confidence of the organization and the ability to move forward, grow-ing this collaborative approach to offer even more functionality, while ensuring the security of our customers."

Chronicle SIEM

BBVA

> It's been a very rich and rewarding relationship. We deal directly with the engineering team, rather than salespeople, and we're constantly having very deep discussions on our technology road-map. And that has benefits for both parties.

—Jorge Blanco Alcover, Global Head of Security Solutions, BBVA

The future of BBVA and Chronicle SIEM, when it comes to security, seems to be a story of ever-closer collaboration. A significant reason for the growth of this relationship has been Chronicle SIEM's willingness to adapt its approach, based on BBVA's needs. "We're really just one team now," says Jorge. "We have the faith and the confidence that Chronicle SIEM will continue to advance its technology, and our product, in order to meet our changing expectations. It's been a very rich and rewarding relationship. We deal directly with the engineering team and we're constantly having very deep discussions on our technology roadmap. And that has benefits for both parties. We gain their expertise and knowledge, and they get feedback from a large company that, by its nature, has to be at the forefront of cybersecurity."