ROI CASE STUDY
PROGRAM: SECURITY AND INFRASTRUCTURE
DOCUMENT NUMBER: U179 JANUARY 2021

NUCLEUS RESEARCH

ROI: 393%

Payback: 4.8 Months

# CHECKMARX

# EUROPEAN FINANCIAL SERVICES INSTITUTION

ANALYST
Nick Grizzell

## THE BOTTOM LINE

Squad, an independent IT services company providing cybersecurity and DevOps consulting at one of the largest European financial services companies, deployed Checkmarx Static Application Security Testing (CxSAST) and Checkmarx Codebashing (CxCodebashing). With Checkmarx, the banking group realized a wide range of benefits from increased scalability, improved employee productivity, streamlined security management, accelerated project development, and reduced coding vulnerabilities. In the end, the company realized a 393 percent ROI and will recover its initial investment in less than five months after implementation.

## THE COMPANY

The company is one of the largest European financial services institutions providing banking, financial, and real estate financing for 40 million customers throughout Europe. The company has a strong commitment to complying with all legal and regulatory mandates with teams dedicated to minimizing financial fraud. The banking group is dedicated to compliance with the principles and rules provided by French law and in accordance with the standards defined by the FATF, the United Nations, and EU institutions. Furthermore, at the beginning of 2017, the company began heavily investing in digital transformation with the intention of raising the digital Net Promoter Score (NPS). With digital transformation efforts comes exposure to security risks, and with a strong commitment to meeting regulatory and legal standards, the company hired a consulting group to implement Checkmarx solutions and reduce security risks.

The company hired Squad, an independent IT services company providing cybersecurity and DevSecOps consulting to customers throughout France. The company assists clients in the management of their cybersecurity infrastructure by preventing threats and securing sensitive assets.

## THE CHALLENGE

Before deploying Checkmarx, the banking group did not have a solution to address vulnerabilities in custom code and relied on manual processes to detect errors. The challenges centered around the legal and industry standards for security and compliance. As the second-largest banking group in France, compliance with strict regulations surrounding application security, data protection, and fraud detection was necessary to continue operating within the country and throughout Europe. The banking group considered approaching these challenges manually with internal solutions but instead decided to utilize Squad developers to assist in implementing the Checkmarx solutions.

If the banking group decided to move forward with internal solutions, manual processes would open the door to increased security risks, a longer development lifecycle, and a resistance to scalability. Internal IT teams would need to conduct continuous code reviews to ensure the overall stability of the source code provided by developers. Developers would also need to continuously review integrations, ServiceOps, and data analyses. After conducting these reviews, IT teams would then need to communicate any necessary improvements and highlight security concerns within the coding structure. The entire process could extend the delivery date of projects and reduce the IT teams' overall productivity as they focus on fact-checking instead of innovation and building new solutions.

Cost : Benefit Ratio | 1 : 4.3

## THE STRATEGY

After determining that it needed a new application security testing system to help with process efficiencies, monitoring capabilities, and application security, the banking group immediately looked towards Checkmarx. Briefly, the company considered Fortify, but the solution deployed legacy capabilities and did not fully meet their needs. The code for Fortify is also all SaaS, and due to the company's requirements, it could not send source code externally over the cloud. The banking group needed to have source code analysis on-premises, and Checkmarx easily met that requirement.

When facilitating the Checkmarx deployment, Squad chose to take an "automatic" approach to challenging manual processes allowing users to focus on more value-driven work instead of analyzing the source code for vulnerabilities. Squad deployed two Checkmarx solutions, which are CxSAST and CxCodebashing, at the financial institution. Around 200 users, who are mainly tech leaders, developers, and data engineers, utilize the CxSAST platform to simplify the process of reviewing projects. The CxCodebashing platform is used by 1000 developers to help them bring security right into the development process, allowing them to understand security needs and incorporate ideas as soon as possible. The implementation was handled by a team of three employees: two Security Analysts and one System Administrator. The implementation project took two months to complete, with all three stakeholders only devoting 15 percent of their time each week to implement Checkmarx. On an ongoing basis, the same three employees support the system and focus their time to help maintain the two Checkmarx solutions. Furthermore, within the license costs, Checkmarx provided services for fine-tuning the system, and no additional training or third-party programs were required for the developers.

## KEY BENEFIT AREAS

Key benefit areas seen as a result of the CxSAST and CxCodebashing deployment include increased growth and scalability, improved employee productivity, streamlined security management, accelerated project development, and reduced coding vulnerabilities.

- **Increased employee productivity.** If the banking group had decided to move forward with their internal solution, they would have needed a team of 50 employees to oversee all the developers and projects created. With Checkmarx, the company decreased the necessary employee requirements by 80 percent to just ten employees who could easily oversee projects and integrations. Furthermore, the banking group realized significant benefits surrounding CxCodebashing. They could train their users and their developers to create more secure code and to better understand security vulnerabilities, weaknesses, and how to discover these issues. Furthermore, CxCodebashing could help users understand how an application or portion of code might be exploited and how to prevent this from happening. Across 1000 developers, CxCodebashing helped save two hours per developer per week from not wondering if a code was vulnerable and taking the necessary steps to remedy the issue. The time savings translated to savings of 104,000 hours annually and 1.7 million Euros annually through increased employee productivity.

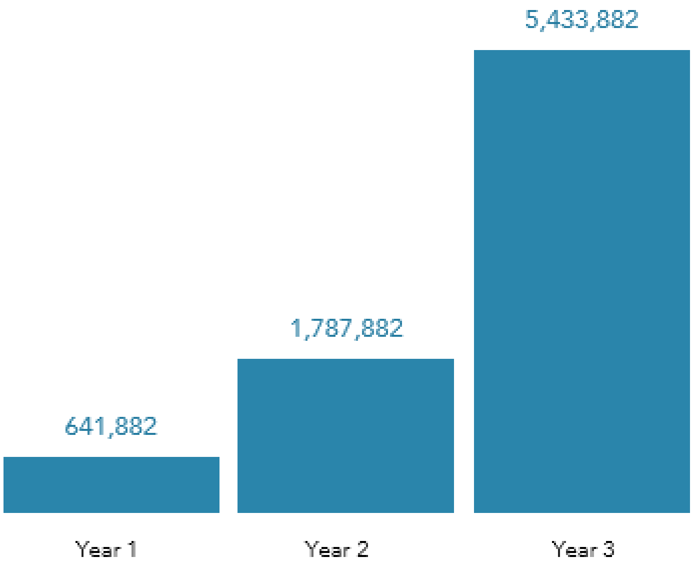
- Cost savings from reduced vulnerabilities. Squad highlighted the immense weight lifted by deploying the Checkmarx solutions at the financial institution. CxSAST and CxCodebashing supported IT teams when working towards adhering to regulations and creating integrations among software solutions. In addition to possibly losing clients, security vulnerabilities would bring sanctions and fines for the banking group, which could further compound the financial detriment. Without Checkmarx, the company would be out of regulation and subject to significant sanctions from the government, the European Commission, and regulatory banking systems. On a single platform, Checkmarx allowed the company to address all security concerns by increasing visibility, reducing vulnerability, and providing actionable insights. Checkmarx helped the company avoid an estimated 2 million Euros in fines from the banking regulatory services and GDPR by protecting systems and applications.
- Scalability. For many organizations, growth is a positive factor but can increase costs surrounding employees, infrastructures, and maintenance. As the company expands to new landscapes, users will adopt more applications and data management tools, leading to increased workflow processes. Additionally, coding integration projects are often large tasks for even a skilled and robust team of developers. Working between applications that may or may not use the same coding or structure can create issues within the integration. Troubleshooting compatibility issues can turn into an entire project consuming more time and resources. Without an application security management platform like Checkmarx providing security insights, developers can spend days, if not weeks monitoring new code and applications to check for security vulnerabilities. The process is time-consuming and can lead to multiple errors that further compound the development lifecycle. With Checkmarx, the financial institution increased productivity, leading to increased customer satisfaction and growth in the number of new clients. As the company needed to scale up, demand increased, and Checkmarx helped them address these concerns by providing developers with the necessary tools to succeed even in a rapidly growing environment. At first, the banking group, with the help of Squad, was working on 300 different projects on an ongoing basis, and after deploying Checkmarx, that number is approaching thousands of projects while onboarding 5-

10 new projects every day. This is all achieved with the same number of developers before deploying Checkmarx, which displays the solution's overall scalability.

## KEY COST AREAS

The most significant cost area of the CxSAST and CxCodebashing deployment was the product license charge itself, which soon provided a full ROI and further cost savings. Other costs over the three-year period included the minimal initial deployment cost and the cost of the three employees who support the solution on an ongoing basis. Training sessions were not required as Squad highlighted that Checkmarx solutions are straightforward to learn for developers.

### CUMULATIVE NET BENEFIT



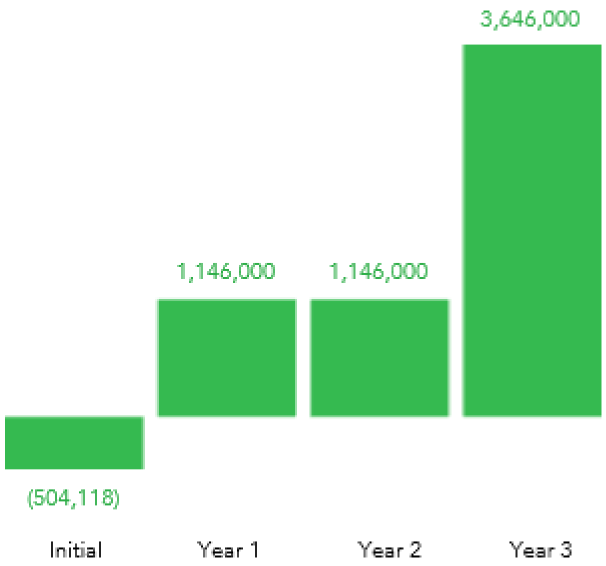
## LESSONS LEARNED

The implementation of CxSAST and CxCodebashing highlights the necessity of exploring alternative solutions over internal projects, even when facing a new system's switching costs and implementation costs. The banking group did not deploy a solution before Checkmarx and instead relied on internal teams to maintain integrations and deployments while monitoring security across application codes. The internal solutions ultimately proved to be inefficient and led to further challenges surrounding visibility, security, and scalability throughout the organization.

With CxSAST and CxCodebashing, developers could automate security processes and gain better awareness surrounding vulnerabilities. CxSAST enabled developers and technology leaders to identify security vulnerabilities with tools to scan source code early in the SDLC and provide actionable insights. CxCodebashing helped the company train developers to increase their understanding of how vulnerabilities are created and how to avoid creating risks when writing code. The solution also enabled developers to think and act securely, leading to less time spent checking if written code had security concerns. By enabling developers to write more robust code, CxCodebashing saved the company's developers two hours per week. Across the 1000 developers using the platform, this saved the company 1.7 million Euros due to increased efficiency. Furthering cost savings, Checkmarx helped the company meet the regulatory requirements with ease and avoid significant fines and sanctions. Without Checkmarx, the company would have more difficulty preventing security issues and vulnerabilities, leaving them exposed to security breaches and exposing end users. The company would be fined millions of Euros for not implementing the correct security functionalities as well as losing many clients in the process. Checkmarx helped eliminate almost all security concerns and save an estimated 2 million Euros in avoided fines from GDPR. Additionally, Checkmarx helped the company retire legacy third-party tools and libraries incorporated within the code. Retiring the technology helped reduce the applications' overall vulnerability and gave the developers a more modern environment to work in to improve productivity and increase visibility over security concerns.

Checkmarx gives developers a greater view of security and application architectures. With the confidence to move forward with projects, developers can push managers to implement security features without being asked to create new projects. The increase in productivity and communication leads to hundreds of hours gained by avoiding going back and forth, creating projects between upper-level management and developers. Instead, the time can be reinvested into value-driven processes such as taking on new clients and projects to increase revenue within the company. This deployment demonstrates how an organization can effectively implement and manage application and software security solutions without a complex implementation. Three employees oversaw the entire deployment during a two-month period, with the employees devoting less than 15 percent of their time per week to the implementation. With the ease of deployment of solutions like CxSAST and CxCodebashing, companies in a similar situation to that of the large European financial services company can see this use case as an example of why alternatives must be explored. There is always more room to create more efficient processes, reduce costs, and increase employee productivity and visibility. Companies like this large financial institution can deploy Checkmarx solutions to drive insights to improve the company's security infrastructure and operational efficiency. By leveraging CxSAST and CxCodebashing, the banking group could avoid security vulnerabilities and augment their developers' overall capabilities.

## NET CASH FLOWS



# CALCULATING THE ROI

Nucleus Research analyzed the costs of software, hardware, personnel, professional services, and user training over a three-year period to quantify the financial institution's total investment in CxSAST and CxCodebashing technology.

Indirect benefits quantified include the time savings for increased growth and scalability, improved employee productivity, streamlined security management, accelerated project development, and reduced coding vulnerabilities. The indirect benefit is multiplied by a correction factor to account for the inefficient transfer of time between time saved and additional time spent working.

Benefits not quantified include improved customer satisfaction, increased operational visibility, and improved management practices.

# FINANCIAL ANALYSIS

**Annual ROI: 393%**
**Payback period: 0.4 years**

| BENEFITS | Pre-start | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|
| Direct | 0 | 0 | 0 | 2,000,000 |
| Indirect | 0 | 1,700,000 | 1,700,000 | 1,700,000 |
| **Total per period** | **0** | **1,700,000** | **1,700,000** | **3,700,000** |

| COSTS - CAPITALIZED ASSETS | Pre-start | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|
| Software | 0 | 0 | 0 | 0 |
| Hardware | 0 | 0 | 0 | 0 |
| Project consulting and personnel | 0 | 0 | 0 | 0 |
| **Total per period** | **0** | **0** | **0** | **0** |

| COSTS - DEPRECIATION | Pre-start | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|
| Software | 0 | 0 | 0 | 0 |
| Hardware | 0 | 0 | 0 | 0 |
| Project consulting and personnel | 0 | 0 | 0 | 0 |
| **Total per period** | **0** | **0** | **0** | **0** |

| COSTS - EXPENSED | Pre-start | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|
| Software | 500,000 | 500,000 | 500,000 | 0 |
| Hardware | 0 | 0 | 0 | 0 |
| Consulting | 0 | 0 | 0 | 0 |
| Personnel | 4,118 | 54,000 | 54,000 | 54,000 |
| Training | 0 | 0 | 0 | 0 |
| Other | 0 | 0 | 0 | 0 |
| **Total per period** | **504,118** | **554,000** | **554,000** | **54,000** |

| FINANCIAL ANALYSIS | Results | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|
| All government taxes | 45% | | | |
| Cost of capital | 7.0% | | | |
| Net cash flow before taxes | (504,118) | 1,146,000 | 1,146,000 | 3,646,000 |
| Net cash flow after taxes | (277,265) | 630,300 | 630,300 | 2,005,300 |
| **Annual ROI - direct and indirect benefits** | | | | **393%** |
| Annual ROI - direct benefits only | | | | 55% |
| Net Present Value (NPV) | | | | 2,499,251 |
| **Payback period** | | | | **0.4 years** |
| Average Annual Cost of Ownership | | | | 555,373 |
| 3-Year IRR | | | | 251% |

All calculations are based on Nucleus Research's independent analysis of the expected costs and benefits associated with the solution.