CASE STUDY
THE FINANCIAL CASE FOR DEVSECOPS

How banks can save 40% on their pentesting budget and increase security
Software Unlimited is a software developer that focuses on the financial and consulting market. They realized the need to implement an agile security strategy after switching to agile development processes. The head of agile security strategy needed to find a way to embed security in the development process, handle more and smaller changes, and automate security tasks. Besides, he needed a quick win to show results to his managers.

By implementing Crashtest Security to automatically scan every release of software, Software Unlimited not only achieved these goals, but also had additional benefits that made the agile security initiative a success. Software Unlimited saved more than 40% on their pentesting budget, while increasing security test coverage. What is more, developers were delighted by the quick feedback and provided remediation support when vulnerabilities were found - before they were deployed to production. Due to Crashtest Security, Software Unlimited is now set up for scaling releases up even further - without compromising security.

**CUSTOMER PROFILE**

While Crashtest Security is not allowed to give details about the customer (we call them Software Unlimited in this case study), we can give you some pointers about the scale:

- Industry: Financial
- Revenue: 9 digit figure in EUR
- Employees: 4 digit figure
- Developers: 4 digit figure
- Web Applications and APIs: Roughly 100
Software Unlimited had implemented an agile development strategy and CI/CD processes within the last years. With the increase of releases and deployments to production, Software Unlimited realized the need to switch their approach to security. The “traditional” approach to security in which every major release was tested manually before going to live environments would not work in the agile work environment. The bank wanted to implement agility in their security department.

The newly appointed “Head of agile security strategy” was given a clear goal by the boardroom: Keep Software Unlimited’s position as a digital champion and ensure the highest grade of security measurements for their customers. The “how” was also set: “Modernize all security measures within the company related to their core products (web applications and APIs).” The head of agile security strategy broke this high-level goal down into more actionable steps. (see box)

**BUSINESS NEEDS**

**DAST AS A PERFECT FIT FOR AGILE SECURITY STRATEGY**

One part of the agile security strategy was to implement a DAST tool, the Crashtest Security Suite. The reasons for choosing Crashtest Security will be explained further below. The Crashtest Security Suite achieves the above-mentioned initiative-wide goals as following:

**HANDLE MORE, INCREMENTAL CHANGES**

Crashtest Security scans can be started without human interaction for every release. This means every release can be tested for the most common vulnerabilities.

**KEY CUSTOMER GOALS FOR AGILE SECURITY STRATEGY:**

+ **Handle more, incremental changes**
  Instead of handling few, large releases, the security department should be set up to handle many small, incremental changes.

+ **Automate everything**
  This meant to automate as many tasks as possible - to spend time and attention on deeper security topics that require manual attention.

+ **Embed security in the development process**
  A “Shift Left” of security measures to support developers already during the development of new features with advice on security vulnerabilities.

**WHAT IS „CI/CD“?**

CI stands for Continuous Integration and means to integrate small software changes as often as possible. CD stands for Continuous Deployment and means that software changes are automatically tested and published to the live environment.

**WHAT IS “SHIFT LEFT”?**

“Shift Left” is a practice intended to find and prevent defects earlier in the software delivery process.

**WHAT IS “DAST”?**

DAST stands for Dynamic Application Security Testing and means a security test from the outside (or black-box) in the running state (dynamic).
## Automate Everything

With the basic vulnerabilities already covered through Crashtest Security, the QA team and pentesters were able to focus on security issues that require human attention.

## Embed Security in the Development Process

With tests being run for every deployment to a staging environment, code with security vulnerabilities was never deployed to production. Instead, developers got instant feedback on any vulnerabilities in the form of a created ticket in their ticketing system - remediation advice included.

## Why DAST Was Chosen as a Quick Win

Below are proven advantages of implementing the Crashtest Security Suite. These were the reasons for Software Unlimited to choose a DAST tool to be one of the first initiatives:

### More Than 40% Savings on Pentesting Budget

After embedding security testing in every release, Software Unlimited knew that basic vulnerabilities will never be released to live environments. Therefore, the intervals between manual penetration tests could be increased. The money that was saved early on in the agile security strategy implementation secured the initiative a quick win with the board. The saved budget could then be reinvested in other agile security measures. For comparison, take a look at the box that shows the testing intervals between manual pentests before and after the implementation of Crashtest Security.

### How Software Unlimited Saved More Than 40% of Their Pentesting Budget

<table>
<thead>
<tr>
<th>Yearly Pentesting Cost</th>
<th>Without Crashtest Security</th>
<th>Total Cost</th>
<th>With Crashtest Security</th>
<th>Total Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>350,000 €</td>
<td></td>
<td>200,000 €</td>
</tr>
<tr>
<td>A</td>
<td></td>
<td>100,000 €</td>
<td></td>
<td>50,000 €</td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>100,000 €</td>
<td></td>
<td>100,000 €</td>
</tr>
<tr>
<td>C</td>
<td></td>
<td>150,000 €</td>
<td></td>
<td>50,000 €</td>
</tr>
</tbody>
</table>
The implementation of the Crashtest Security Suite was also met with enthusiasm by the 800 developers of Software Unlimited. In the past, developers had to spend time to set up a system for a manual pentest, wait two weeks for the results, and were left with no advice on how to fix issues. With Crashtest Security, the tests are built into the automated toolchain, so no manual effort is needed to run the tests. The results from the tests are arriving in real-time, in their ticketing system, and even include helpful tutorials and code snippets for faster remediation. Last, but not least, the personal comment from one developer said it all:

»With manual pentests, I have to remember how I implemented this feature and the code from 5 months ago. It takes me some days to work on the code and check for dependencies. With Crashtest Security, the code was just released. I instantly know what I did, where to find it, and there are no dependencies yet.«

Another reason for choosing Crashtest Security as the first initiative of the agile security strategy was the fast implementation. After showing impressive scan results for test applications, as well as the easy integration in the CI/CD pipeline, the technical implementation process went through in a matter of weeks.

TIME SAVINGS FOR DEVELOPERS

The implementation of the Crashtest Security Suite was also met with enthusiasm by the 800 developers of Software Unlimited. In the past, developers had to spend time to set up a system for a manual pentest, wait two weeks for the results, and were left with no advice on how to fix issues. With Crashtest Security, the tests are built into the automated toolchain, so no manual effort is needed to run the tests. The results from the tests are arriving in real-time, in their ticketing system, and even include helpful tutorials and code snippets for faster remediation. Last, but not least, the personal comment from one developer said it all:

»With manual pentests, I have to remember how I implemented this feature and the code from 5 months ago. It takes me some days to work on the code and check for dependencies. With Crashtest Security, the code was just released. I instantly know what I did, where to find it, and there are no dependencies yet.«

Another reason for choosing Crashtest Security as the first initiative of the agile security strategy was the fast implementation. After showing impressive scan results for test applications, as well as the easy integration in the CI/CD pipeline, the technical implementation process went through in a matter of weeks.

TIME SAVINGS FOR DEVELOPERS WITH CRASHTEST SECURITY

<table>
<thead>
<tr>
<th>Developers</th>
<th>Time Saved</th>
<th>Money Saved per Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>100 Hours</td>
<td>- 40,000 €</td>
</tr>
<tr>
<td>100</td>
<td>100 Hours</td>
<td>- 400,000 €</td>
</tr>
<tr>
<td>500</td>
<td>100 Hours</td>
<td>- 2,000,000 €</td>
</tr>
<tr>
<td>800</td>
<td>100 Hours</td>
<td>- 3,200,000 €</td>
</tr>
</tbody>
</table>

Developers can use their time for development

* Assuming an average salary of €60,000 p.a., with a 40 hours work week.
Besides delivering a software that has all the above mentioned features and benefits, Software Unlimited chose Crashtest Security due to the following reasons:

+ Find a single solution that guarantees a specific security level across many applications and scales with release frequency.

+ The focus on saving time for developers during remediation with the self-developed and cared for wiki system.

+ Software Unlimited preferred to have a company that develops and hosts in Germany, which allowed for fast alignment, developing a personal connection, and helped with communication.

+ Software Unlimited knew that they would need a partner that allows for a quick and custom integration.

+ The speed of adopting specific feature request, such as using specific authentication flows on the development system (e.g. Smartcards).

Below is an exemplary chart of the security level of Software Unlimited before and after implementing Crashtest Security.
SUMMARY

In the end, Software Unlimited was very happy with the implementation of Crashtest Security:

“We showed a quick win for the agile security strategy to all stakeholders. The board was happy with the fast start while freeing up money for further initiatives. Our developers were happy with less burdens from manual testing and the added, faster feedback and support. Our CISO was happy to see the security level increased and never releasing untested code again.”

ABOUT CRASHTEST SECURITY

Crashtest Security is a Munich-based IT security company.

As an innovator of cyber security solutions for web applications, it develops automated solutions for vulnerability analysis.

Based on artificial intelligence, vulnerabilities are detected, protection against hacker attacks is increased and transparency for companies, users and developers is created.

Visit our website for more: