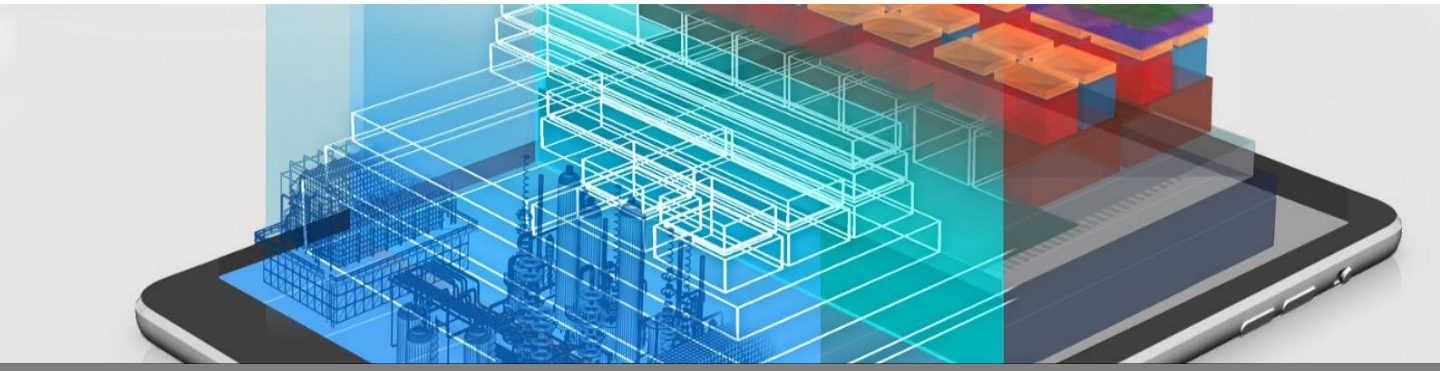
CASE STUDY



Security Features as a Quality-Assurance Task in SCRUM and DevSecOps Processes

This case study describes the introduction of a security expert into the development of an eFood shop (overall project size more than 40 man-years). The early integration enabled a security-by-design approach. The customer acknowledged our lean-security model. It allows the smooth integration into the established workflows and avoids wasting efforts. Also, it proved successful in the timely go-live due to the penetration test without objection.

Initial Situation

The customer is a full-range trader in the retail sector. Having great experience in the chain-store business, the project constituted the step into the online food market, usually called eFood. The offering included nearly the whole product range of the food sector including fresh and chilled goods.

The customer outsourced the whole shop development to a subsidiary company. This company employed and engaged people with all necessary expertise to develop and run the above-mentioned web shop: business analysts and operations experts moved from the parent company, business consultants, software architects and developers as well as quality assurance testers and security experts came from mgm.

Goals & Requirements

We found ample free space to model, including issue tracking, documentation, policies, processes, environments, and systems. The hosting environments – four stages from DEV over QA and INT to PROD – were set up by the customer over time. The team started as a small task force to set up an issue tracking system and a wiki for documentation. The architects configured and deployed the given SAP Hybris eCommerce app (today: SAP Customer Experience) on the DEV (development) stage. The business consultants phrased the first tickets towards the intended minimum viable product (MVP).

Why mgm security partners?

The described case study depicts an instance of our overall achievement: With our lean-security-by-design approach, we contribute to the goal to go live on time with all intended security features at calculable cost.

Contact

Dr. Bastian Braun

089/358680-424
Bastian.Braun@mgm-sp.com

mgm security partners gmbh
Frankfurter Ring 105a
80807 München

Tel +49 89 / 358 680-880
office@mgm-sp.com
www.mgm-sp.com

The main challenge for us as security consultants in such a situation is the integration into a highly dynamic development process with conflicting interests and ever-changing priorities. This means in particular:

- We need to assess the value of security with respect to other application features to identify the crucial security tasks.
- We need to integrate into established but dynamic processes without "disturbing" the development progress.

Approach

In this case, we were particularly fortunate because the whole team was keen on security and delivering a secure product. We first completed a basic security training to enable the ops part of the team to configure and deploy our artifacts securely. The reason was to make the business consultants aware of abuse cases on the logic layer of an application and to train the developers to write secure code.

With the awareness and basic know-how, the whole team agreed on a common set of security policies covering the protection of data and the integration of security activities into the development workflow. Such integration includes two main approaches:

- First, some features of an application require special security properties that may be missed if not defined explicitly. For instance, credentials must be stored cryptographically secure, APIs must be protected against automatic abuse attempts, and multi-step workflows must (under enforcement) be followed in the intended order.
- Second, the intended security properties must be verified. This verification may happen manually or automatically, on the code or on the running application.

In any case, the security expert in the DevSecOps team is responsible to define and verify the security properties after the agreement with the customer. However, no security expert can succeed without the support of the team. The expert relies on the awareness of the team, be it hints and questions concerning different implementation options, risks in data processing, e.g. in the back-end, or common code walkthroughs. Also, some verification tasks can be assumed by QA testers after a quick briefing to save the usually lean security resources. The whole project team understood the achievement of the security properties as a team commitment which built the basis for the final success.

Lessons learned

We can conclude that:

- our lean-security approach is applicable to small and large teams
- any security expert can only succeed with the support of the team
- technical and awareness trainings support the acceptance and understanding of security
- a security expert does not replace a penetration test as an independent final review
- security consulting contributes to:
    - go live on time
    - calculate the cost of security
    - compromise on usability, security, and cost

mgm security partners gmbh
Frankfurter Ring 105a
80807 München

Tel +49 89 / 358 680-880
office@mgm-sp.com
www.mgm-sp.com