devon

CASE STUDY

“Implementing Security into DevOps”

By Marudhamaran Gunasekaran (Senior DevSecOps Consultant @DevOn)

Implementing Security into DevOps

Because of organizational and compliance regulations like GDPR are becoming an indispensable part of software and IT operations, security is becoming more important as well. Therefore, the customer wanted help with implementing Security into their software development.

Customer profile

The customer is one of the largest energy suppliers in Europe with strong footsteps in sustainable and secure energy supplies for over two million customers. Their total revenue is over 4.0 billion euros and manages a well-maintained network of windmills, solar energy projects and biomass plants.

Customer situation

The customer had a varied portfolio of energy supplies and a huge IT landscape with a mixture of on premise legacy systems and cloud systems. Some of the systems include, online lead generation portals, order management systems, contract management systems, invoicing systems, billing systems, self-service customer portal and much more. When an order was placed for an energy supply request (anywhere from a consumer, small/medium business or an enterprise) there was a slew of operations and workflows that were triggered to complete and fulfill an order. The increasing reliance on IT systems, and the ever-increasing complexity of the intertwined architecture made the organizations security efforts more difficult.

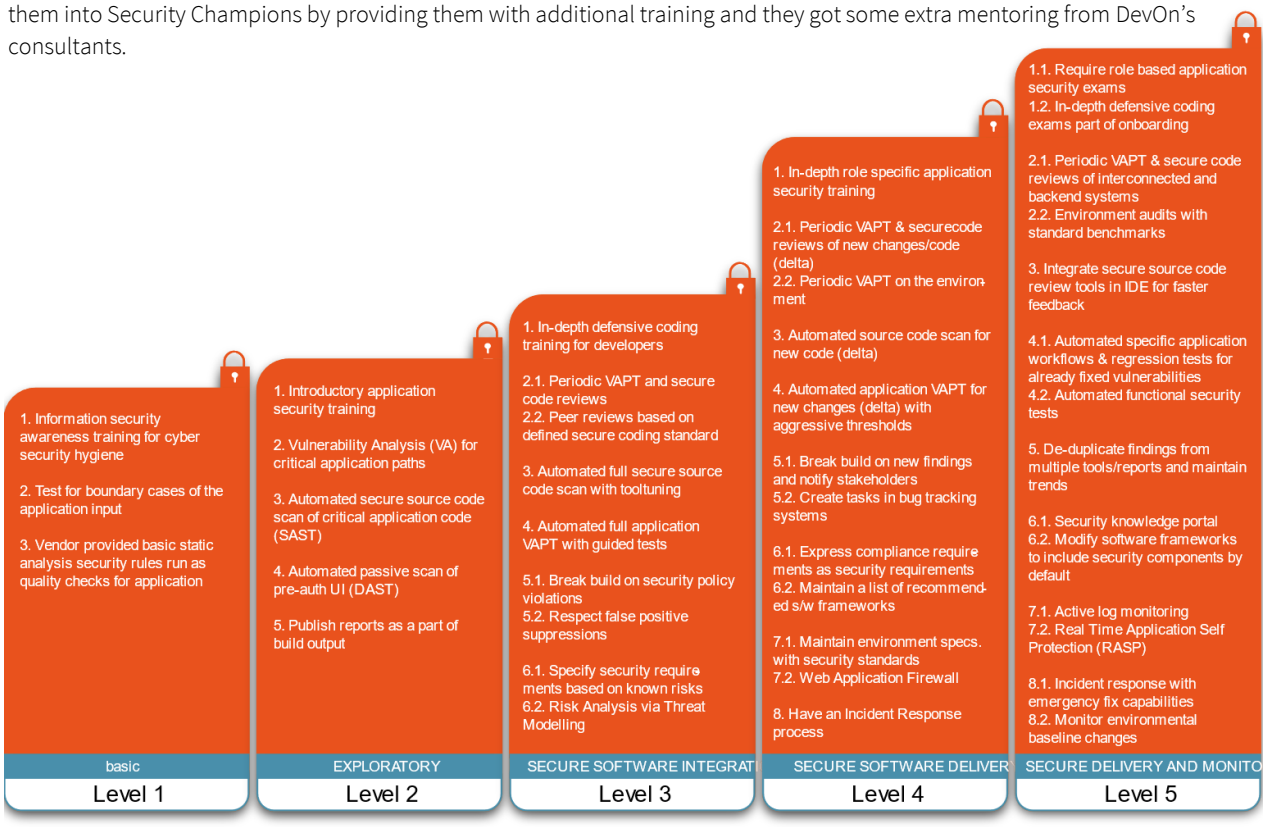
Approach

Considering the urgency of the situation and understanding the customer's pain points about complex integrations in software architecture, DevOn proposed a Software Risk Rank based approach.

Firstly, we did an assessment on the current state of security in the software development process and checked their current maturity according to our Continuous Software Security Maturity Model. We also performed interviews with many developers, stakeholders and security officers.

Based on the results of the assessment and the interviews, we prioritized the teams we would help first and created a DevSecOps program for them. This program consisted of several training courses (including a "Hack-yourself-first" training), coaching and consulting.

During the DevSecOps program we also initiated a track for people who were really interested in security. Here, we turned them into Security Champions by providing them with additional training and they got some extra mentoring from DevOn's consultants.



DevOn
Brasserplein 1
061121254454

Results

The DevSecOps transformation resulted in several major improvements. Due to the Hack-yourself-first training, the developers would find a lot more vulnerabilities, that they normally would not find. This created a higher sense of ownership amongst the software developers. So, they would not only locate more bugs, but they would also fix these themselves. Moreover, the security bugs were identified earlier in the coding stages itself. Because of this, the customer was able to reduce the number of bugs with over 55%.

Secondly, because the security was built in the development process, there was no delay at all in any of the releases. Which resulted in a faster feedback loop from the stakeholders and customers.

The introduction of the Security Champions played a big part in creating accountability within the development teams. They were responsible for creating a secure DevOps culture and organized several hackathons to improve the awareness of Security in the company.

End state

Developers and Operations personnel were able to make secure decisions before a piece of code is written or deployed.

Security checklists became one of the important artifacts in deciding whether a feature is production ready or not.

Commonly found vulnerability identification was automated to be repeatable teats with custom policies so vulnerabilities are identified right during the build process

Business value delivered

There were no outages in production due to the increased security of releases and hence making the infrastructure available at all times.

The customer was able to deploy and deliver secure software with increased security confidence that was an outcome of security education, and automated security scanning systems.

Security became one of the main areas of focus during software development itself hence increasing the awareness and effort required to deliver secure features through early and fast deployments leading to no delayed releases and faster time to market.

Key take-aways

Accountability is key in every DevSecOps initiative. Though everyone is responsible for security, the accountability to ensure that everyone is responsible lies within the organization's stakeholders and management. Also, no software engineer is cut out for security. It highly depends on their intrinsic motivations to develop good quality code. That's why, finding the right security flag bearers as security champions, could lead to software written with secure intensions.

Staying unbiased towards development team and management is crucial. Developers are essential in building secure code. But management and product owners also need to provide developers with that additional time that is required to develop secure software. Support the developers in providing the required tools and techniques to write secure code, at the same time educate the management to understand software security challenges.

Phasing security initiatives help to test a security program pilot. This often helps other software development teams in the organization get excited about security.

Automated vulnerability detection and reporting is key Remember to make sensible use of security tools to provide just enough security coverage and vulnerability results. Otherwise it may lead to prolonged scans, and report fatigue.

Reoccurring Security events Conducting quarterly security hackathons for introducing security policies, security checks, etc. engages developers and the operation's personnel with higher levels of security awareness.

Curious where you stand?

This quick security assessment gives you a summary of your organization's progress in terms of security including:
Incident Response

- Software Security
- DevSecOps
- Information Security Awareness and Education
- GDPR
- And much more.

It only takes a few minutes to complete and a report will be sent over to by email.

To the free assessment

DevOn
Brasserplein 1
061121254454