The Importance of DevSecOps

BOOLEANS

true digital security

Colofon

Author: Erdi Aktan
Version: 12/22

Introduction

As organizations need to focus on their core business, they are also faced with new business expectations in this digital age:

- Employees need flexible solutions to work from home (hybrid is the new standard)
- Online customers want seamless access to their applications on all their devices with optimum user experience
- Regulators demand consumer consent when using their data, higher security and guaranteed consumer privacy levels
- Business requirements for cost-efficient and scalable cloud solutions
- These challenges are about identities, access rights and being able to scale them securely. These domains are the core expertise of Booleans.

At Booleans, our main goal is to unburden you by offering creative high-quality solutions for various digital security challenges in your organization, so you can focus on your core business. Our services consist of two main building blocks:

- DevSecOps
- Digital Identity

In this brochure you can find more information about our DevSecOps services and our way of working. Are you also interested in receiving more information about Digital Identity? Please send an email to marketing@booleans.com.

The Importance of DevSecOps

> *Security is a more important quality aspect than ever and needs to become a natural part of developing software in a fast and agile way throughout the entire IT lifecycle.*

Does this sound familiar to you?

You are creating your software by considering today's standards and requirements and it may require a bunch of new functions to be competitive in the market or satisfy the customers' needs. In addition, it is required that this software needs to be implemented as soon as possible. Shipping software fast and frequently has become the new norm to respond to today's needs. To give an example, well-known streaming companies deploy thousands of lines of code into production every day.

Today's most mature methodology developed to keep up with this speed is 'DevOps'. 'DevSecOps' is explicitly embedding Security activities in the DevOps way of working.

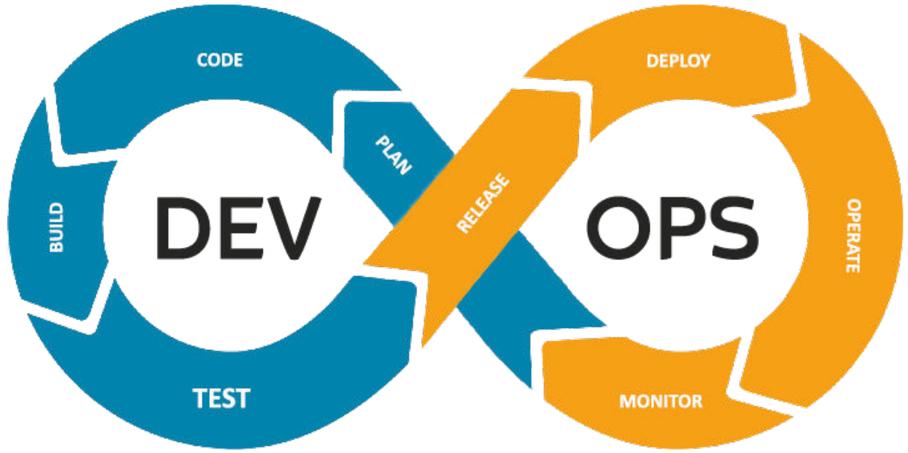
Our company employs people who not only have a strong background in security, development and operations, but are also able to help DevOps teams hands-on to increase their security posture.

Why do you need DevSecOps?

DevSecOps is about integrating security at every phase of the DevOps cycle, from initial design and coding to testing, deployment and running. This allows devops and developer squads to identify and remediate security vulnerabilities much earlier in the DevOps cycle, creating better quality code and fewer hassles in later stages.

Web application attacks, for example, are one of the most used patterns (%38) in breaches according to Verizon's data breach report. Although it is not limited to web applications, Log4Shell is just one of them. This vulnerability is exploited in many different forms by threat actors. For example, it was exploited to spread ransomware which resulted in a loss of reputation for big enterprises and harmed them economically.

Proper DevSecOps implementation helps enterprises to reduce security risks by allowing quick prevention, detection and remediation of vulnerabilities. Where there is software there is a flaw. Acting on it quickly may prevent significant negative impact on your business like losing reputation, competitiveness in the market and economic as well as regulational consequences.



1. DevOps Cycle

The advantages of DevSecOps at a glance:

- Secure by design and the ability to measure
- Lowering the costs and increasing the product delivery rate
- Having quick recovery mechanisms in the case of security incident
- Providing transparency right from the beginning of development
- Maintain and ensure compliance.

Our DevSecOps Services

We can support you in various DevSecOps aspects. The way these services are embedded into your organization depends quite a bit on what you do, which technology you use, and what your current way of working is. We are there to help do just that, by adapting these services to the situation at hand.

Threat Modeling

Threat Modeling is a discipline that stimulates thinking about risks for a system early in the development process, to allow DevOps teams to mitigate these security risks as soon as possible. There are various Threat Modeling methodologies one can use. It may be a hassle to pick the right one for your specific environment. At Booleans, we are not restricted to one specific approach to threat modeling. By leveraging our experience we can combine the best features of different approaches together, tweak them according to your needs and help you to embed this approach into your designing phase.

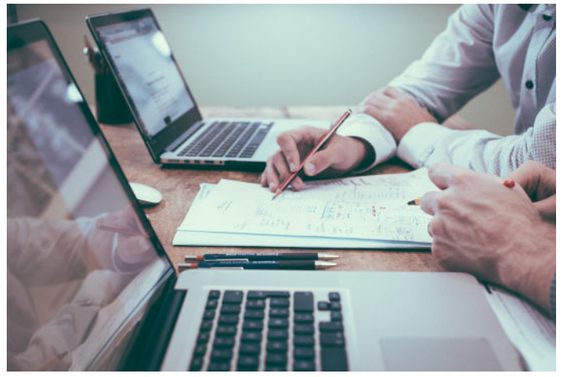
Security Maturity Level Assessment

Security Maturity Models are used to measure the security posture of an organization or a DevOps team. They allow your organization or team to get insight into where they stand when it comes to security best practices, and provide a structured way to grow. Determining the targeted level and knowing which security level you are at is a great starting point to increase the company's security posture. The Security Maturity level can be measured on various metrics, for example; the awareness of security in the team and tooling efficiency. At Booleans, we use our DevSecOps Maturity Model Assessment methodology referenced by reliable authorities and updated according to the current conditions in our services.

2. Security Maturity Levels

Security Training

Security training is often needed to create more security awareness and improve knowledge among all the teams responsible to create and manage the software. The 'Secure by Default' principle is only possible by broadening the participating team's vision by embedding security approaches into their daily habits. The training sessions should always be as relevant as possible to the organization's culture, core business and its unique environment. At Booleans, we provide tailor-made security training sessions which are interactive, well structured and knowledge transfer oriented instead of non-effective, trainer-oriented training sessions.



Automated Security Testing

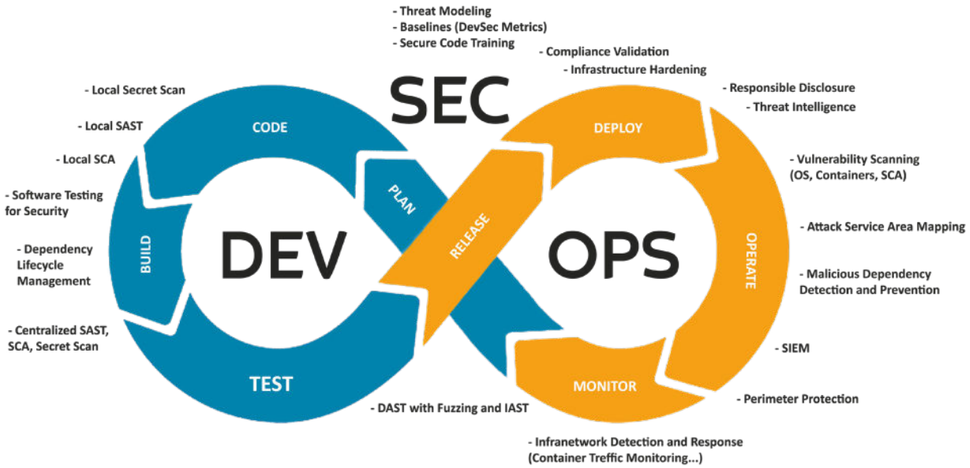
Automated security testing is a way of testing the security aspect of software projected to be deployed and its underlying infrastructure while it gets built and deployed. Examining source code, application dependencies and the application runtime behavior are key factors to achieve proper security testing. Automating, fine-tuning and orchestrating the siloed tools that are used in security testing is essential to derive filtered, meaningful test results which can help you to act quickly and efficiently in order to create secure software. At Booleans, our technology independent security experts will help you build your own security automation-orchestration environment which fits your unique needs.

Vulnerability Analysis

Vulnerability Analysis is the art of diving deep into a security vulnerability, understanding its impact, prioritizing or eliminating it, and finding proper ways to resolve or mitigate the vulnerability. Unfortunately, there is no magic box that performs security tests, covers all the attack surface area of the application automatically, and presents a false positive eliminated, vulnerability prioritized report. Besides tools, experienced security experts are often needed to examine the findings and provide structured, risk-oriented action tasks. At Booleans, we assist you with our experience and knowledge to achieve having a mature, risk-oriented and prioritized vulnerability management lifecycle.

Our Way of Working

As Booleans, we have created a template DevSecOps playbook which we update regularly. This playbook provides us with a structured methodology to look at all the necessary security activities that have to be performed on all the DevOps phases in order to achieve the most robust AppSec posture. This methodology also guides us on where to start or move on while embedding security into DevOps.



3. Booleans' DevOps Cycle PlayBook

> *We refrain from using the traditional security approaches which can not keep up with today's dynamics.*

What Differentiates Booleans?

Helping your DevOps team to build and operate software securely requires specialized knowledge and skills. Today, unfortunately, the ratio of security experts to others in big enterprises is not enough. The below chart can give an idea about the real time proportion.

The amount of Security Experts in an IT squad responsible for delivering a software product is often too low compared to others and we advise at least 10-15 experts in this example. However, due to scarcity it is very hard to find these experts. We can help you by offering enthusiastic security experts who are experienced especially in DevSecOps. Our security experts, who also have a lot of experience in varied fields of security domains, are focused on harmonizing their security knowledge with modern software development and deployment technologies by continuously practicing and learning. We refrain from using the traditional security approaches which can not keep up with today's dynamics.

Booleans can help you to improve your organization's security posture by providing sustainable and quality DevSecOps services.

4. Real Time Proportion DevOps Team

Some advantages of working with us:

- At Booleans, you only work with technical specialists with at least 5 years of relevant experience, who are also very communicative
- We give software-independent advice
- We are adaptable, which means that our services can grow with our customers by providing the latest software and digital security solutions
- We have zero-knowledge protocols in place, so no leaking of any secret information during implementation
- We focus on the best quality solution possible for our customers
- We are a ‘no bullshit’ organization. This means we will be transparent and honest in everything we do.

B

BOOLEANS.COM