BASE4 SECURITY

We help building a
more secure digital ecosystem!

Application Security

DATA SHEET

General aspects of the area.

Base4 Security accompanies companies towards the automation of security controls within the SDLC of their projects where we help them integrate security into DevOps through continuous collaboration between development, operations and security teams. Incorporating security into the software development life cycle.

It is a method that is part of agile software development and is an evolution towards a shared responsibility for security. It involves taking software security into account from the beginning, as well as automating processes so as not to slow down the DevOps workflow within the application development pipeline according to its maturity level.

Objective

Our goal is to achieve faster and safer software deliveries, without turning security into a bottleneck. In other words, DevSecOps tries to guarantee a fast and secure delivery by solving common problems between development and security. To this end, it relies on tools such as Veracode.

Visibility

We perform GAP Analysis based on the OWASP SAAM framework as an effective and measurable way for your organization to analyze and improve its software security posture.

Benefit

- Gain visibility into the current security maturity stage of your development pipeline within SDLC.
- Obtain an accurate plan for growth and investment in application security covering criticality levels.
- Coverage of the latest global vulnerabilities constantly uploaded to your cloud without the need to install patches.

Control points

We perform One Shot services as security checkpoints in your application such as Agile Ethical Hacking, Static Code Scanning, Third Party Library Analysis and Dynamic Analysis.

Benefit

- Limited and fast services to measure the degree of risk of your application both externally and from the source code.
- Find the most important vulnerabilities and separate them by level of criticality to be able to fix them quickly and obtain a better time-to-market.
- Follow-up on remediation until the application reaches 100% stability before going into production.
- Implementation of centralized policies gives greater focus and orientation to the analysis, as well as control from Information Security without influencing the development process.
- Analyze the entire compiled project at code level in addition to having integrations with the most relevant IDEs in the market, continuous integration tools and project management.

- Show a degree of severity found under the applied policy constraint is more severe in the sense of indicating the vulnerabilities and issues found.

Personal

We perform OutSourcing of 5x8 DevSecOps profiles to be in charge of providing a continuous improvement of security in the development pipeline, as well as visibility of the improvements to the business.

Benefit

- To have a person within the DevOps world with experience and capacity in cybersecurity.
- Avoid staff turnover in similar positions.
- Improved application security checkpoints.
- Greater integration with cybersecurity area.
- Training to the development team.
- Support in the implementation of technologies and integrations.
- Creation and automation of analysis.
- Presentation of vulnerabilities and recommendation of best practices.
- Creation of metrics and indicators.

Technology

We commercialize technology to provide automated cross security in all types of applications with independent control from the development area under cybersecurity policies.

Benefit

- Improve time-to-market.
- Reduces development time costs
- Process automation
- Optimize security and development processes.
- Teaching good safety practices to the different teams.
- Evaluate risks and define contingency plans.
- Identify threats and vulnerabilities before going into production.

Why apply DevSecOps?

Integrating security throughout the development process and not just at the end allows DevOps and security professionals to get the most out of agile methodologies, removing obstacles to secure code.

These are the main benefits of adopting DevSecOps:

- Develop secure software from design.
- Identify vulnerabilities in the code and attacks before.
- Apply security in a faster and more agile way.
- Respond to changes and requirements quickly.
- Improve collaboration and communication between teams.
- Generate greater security awareness among all members.
- Focus on generating the greatest business value.

DevSecOps Best Practices

These would be good practices when implementing DevSecOps:

- Optimize security and development processes.
- Teaching good safety practices to the different teams.
- Manage and improve access controls.
- Automate repetitive processes.
- Evaluate risks and define contingency plans.
- Use safety tools.
- Proactively identify threats and vulnerabilities.
- Conduct security audits on a regular basis.

Gartner Recommendations

Integrating security into DevOps requires a change in mindset, processes and technologies. Thus, Gartner makes a series of recommendations for successfully practicing DevSecOps:

- Adapt tools and processes to developers and not the other way around.
- Do not try to eliminate all vulnerabilities during development.
- Focus on identifying and eliminating known open source vulnerabilities first.
- Adapt static and dynamic test analysis (SAST /SCA/ DAST) to the new reality.
- Train developers in security, without expecting them to become experts.
- Adopt a Security Champion model (security specialist who mentors the rest of the teams) and implement a simple requirements gathering tool.
- Ensure and apply the same operational discipline to automation scripts and security infrastructure.

Implement robust version control on all code and components.

- Implement the management of secrets.
- Adopt an immutable infrastructure mentality.
- Rethink how service delivery incidents, including security, are handled.
- Use dynamic access provisioning for developers in DevSecOps.

Audit OWASP DEVOPS

Audit risks in the development process, architecture and communications, to understand the cybersecurity maturity of the pipeline.

The process is carried out through meetings in order to see the GAP between the best practices in the market and what the client is doing under a detailed work plan. Subsequently, the execution involves the review of one or more applications, interviews with developers, review of tool inventories, pipelines, best practices, results of previous pentesting, among many others.

You will receive a report detailing the controls, statistics, and recommendations of implementations and best practices in the use of tools, documents, validation checklist, online wiki with recommendations of development practices in the organization, subsequent advice, among others.

The service is oriented to obtain a better ROI, increasing the security of the applications from its own development, automating it, gaining time-to-market against its competition and avoiding risks in production that may have a negative impact on the economy and image of the client.

Threat modeling

Protect your applications from the very beginning to avoid future risks. The objective is that the security of such an application is implemented from its inception, modeling future threats.

The implementation of threat modeling occurs in early stages of software design. It is oriented to ensure that the development area is clear about the possible threats that the application may have from the conception and business idea to its execution in development cells, as well as the validated architecture from a cybersecurity point of view.

Through meetings with the validated interlocutors, a document will be designed with the topology of the application and the best practice recommendations to be taken into account at the time of starting its development, both for development and infrastructure areas.

The purpose of the service is to contemplate the major risks that the application may have according to its use, connections, architecture, design and language. With this, these risks will be reduced during the development process so that its passage to production is accelerated, in order to gain time-to-market, reduce development times and involve the cybersecurity area from the very beginning.

BASE4 Security also markets Threat Modeling technology to automate the process within companies.

Code scanning

Gain visibility into current vulnerabilities in your source code with this One Shot service, which will help anticipate and assess risks before moving to production.

Using first class cloud tools, BASE4 Security provides the Static and Dynamic Code Scanning service to discover current vulnerabilities in the same.

The service has a short duration and helps to foresee threats and risks prior to the application going into production, being a very productive tool to reduce attacks on the applications.

A report of the vulnerabilities segregated by criticality will be delivered to the clients, as well as a recommendation on their remediation.

BASE4
SECURITY

www.base4sec.com