nuaware
An Exclusive Networks Company

Whitepaper

DevSecOps Maturity Model

Nuaware created a DevSecOps Maturity Model which is now available to you.

Read this whitepaper to get a clear understanding on how to grow your DevSecOps initiatives by assessing your organization against technical as well as business related aspects.

Table of contents

Management Summary

In this whitepaper you will find more information about the DevSecOps Maturity Model as well as practical guidelines to increase your level of maturity.

After reading this Whitepaper you have a thorough understanding on how to best utilise the DevSecOps Maturity Model so you can get most out of it.

DevOps quickly becomes the facto standard to deliver high quality software applications at a rapid pace. Security in DevOps often was an afterthought. Hackers and other bad actors constantly pose a threat to your valuable data. Security has become a topic which requires more attention than ever.

"DevOps quickly becomes the facto standard to deliver high quality software applications at a rapid pace. Security in DevOps often was an afterthought."

Business leaders feel the need to apply security to their DevOps initiatives to ensure their mission critical applications remain secure at all times. Continuous security is one of their main concerns.

The State of DevSecOps

Our DevSecOps Maturity Model helps you to make this a reality.

A lot of companies don't have a clear picture of their current state of DevSecOps. Typical questions we noticed while speaking with enterprises are:

- Where do we stand now in our journey and where to go next?
- How to get there in a meaningful way?

Organizations require a maturity baseline to define where they are now in the journey and how to proceed. Our interactive wizard helps to establish that baseline. Besides that, it also provides a way to advance to the next maturity level as well as tips and tricks to help you throughout your journey. We also added a business justification and relevant links to strengthen your knowledge.

Why DevSecOps matters for your business

Nearly every organization applies the Agile way of working now. Software development teams deliver new features every sprint.

What is DevOps

Development and Operations blend together to form DevOps. Organisations who practice this empower developers to deploy and monitor the software they create themselves. Those companies broke down the silos which existed between software developers and traditional system administrators. Yet something was missing….security.

What is DevSecOps

DevSecOps puts security in the heart of the Software Development Life Cycle (SDLC). Don't assess your applications on security issues after they are deployed, but start taking security into account as soon as possible. This is called the "shift left principle. DevSecOps teams are constantly on the lookout for security issues in every step they take. Continuous security becomes a common habit.

"DevSecOps puts security in the heart of the Software Development Life Cycle (SDLC)."

Business aspects count!

Organisations who focus on security aspects after new application versions have been deployed are late to fix any issues. They face high costs to fix them due to the following reasons:

- It is much more costly to fix an issue in production compared to fixing it in the development phase.
- You don't want to incur valuable downtime if you require a service window to deploy your application (again).
- Don't miss out on business opportunities. Sometimes you need to be ready at the right time.
- Customers might file big fines against you if you leak their personal data and what about reputational damage.

Your DevSecOps Journey

So, our focus is on DevSecOps. Easier said than done. Three questions are important here:

1. **Where does my organization stand as of now?**
2. **What are our goals - where do we want to be**
3. **And how to get there?**

To properly answer these questions, you need to establish a baseline of where you are right now. This baseline should be agreed upon by everyone in the organization. Once that is in place, you need to define where you want to be in the (near) future. Carefully select your goals which are based on the activities that provide the most business value. Be sure your goals are realistic and make a plan on how to get there.

The DevSecOps Maturity Model

Our DevSecOps Maturity Model helps you to start with this journey. It consists of four levels and seven categories which cover nearly every aspect of a typical DevSecOps journey. By answering the questions in the Maturity Model, you establish that baseline.

All questions provide answers which can be seen as “scenarios” in a typical organisation. There is no good or right. Sometimes a different scenario fits best for you. Based on this Model, you can plan ahead to take the next steps to advance to the next level. We can help you analyse your “blind spots” to discuss the best solution for your typical situation.

Our DevSecOps Maturity Model

Intended audience

Our Maturity Model is not just for technical security experts. We aim to help business representatives and other key stakeholders in organizations to understand the above-mentioned questions. This includes but is not limited to the following persons/roles:

- IT Lead
- Dev(Sec)Ops Lead
- CISO or Department Head
- Business Owner
- Lead Developer
- Partner Executive
- Security Leads
- Security Architect

Categories

To support business representatives we added several categories which are important for them. Currently we cover the ones in the table below.

Category	**Description**
Automated security testing	Various questions which focus on the level of automation you practice in terms of security testing.
Daily Software Operations	All about the organizational processes around software development methodologies and how your organization deals with security patches and data (management).
Data protection	This is a broad topic which focuses on relatively new concepts such as API security and signing. Besides this, data classification plays an important role to define how critical an application and it's infrastructure components are.
Organizational aspects	One of the most important business related categories. It's about the overall (high-level) viewpoint of various security related aspects. Especially the management view and how the business departments perceive cloud technology and security.
Risk management	Risk management is all about striking a balance between accepting risks and business opportunity which increases (security and organizational) risks. The questions are written with this perspective in mind.
Software development & testing	A category which heavily focuses on software development activities in relation to the dynamic aspects of disposable infrastructure and how your organization deals with it.
Tools & automation	To be successful in DevSecOps depends heavily on your tools and the level of automation you achieved with them. This category is about how to select and use the tools rather than the tools itself. Business plays an important role here.

Maturity levels

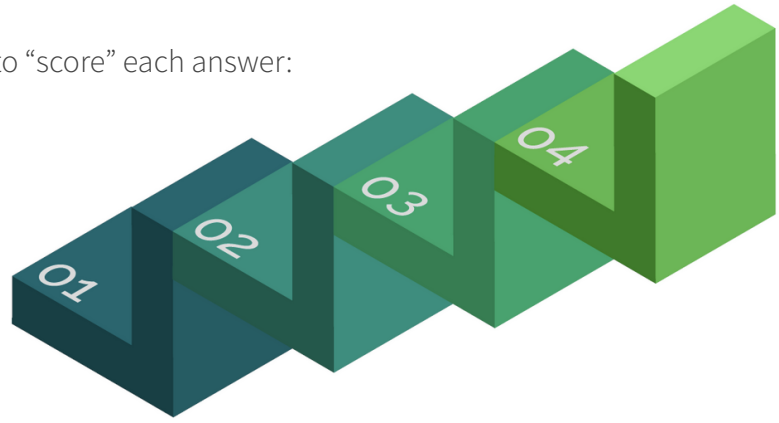
Currently we use the following maturity levels to “score” each answer:

Level 4: Shining stars / experts

Level 3: autonomous teams

Level 2: initial / just started

Level 1: basic awareness / dependent



Level 1

Your organization has heard of the topic (or not). Most of your teams heavily depend on (external) consultants and/or experts to help you take the first steps. DevOps barely exists. Management needs to be informed and convinced about almost every business benefit which is a result of spending time on the topic.

Level 2

Some of your DevOps teams have started small scale initiatives which they try-out in pilot projects. Extra help (from other teams and external experts) is needed to let them progress to the next level.

Level 3

DevOps teams act as autonomous teams in much of what they do. Silos are breaking apart and the business heavily supports these teams. No battles needed to justify why things are needed.

Level 4

Regular speakers at conferences and webinars, they are the rock-stars of your organization. Everyone wants to become one of them. Heavily successful teams. Care for them as much as you can.

Questions and answers

Every question belongs to one category and has four answers. Answers are shown in random order so you need to carefully read them and select the answer which best fits your situation. There is no right or wrong, it’s all about situations and scenarios which typically happen in each (large) organization.

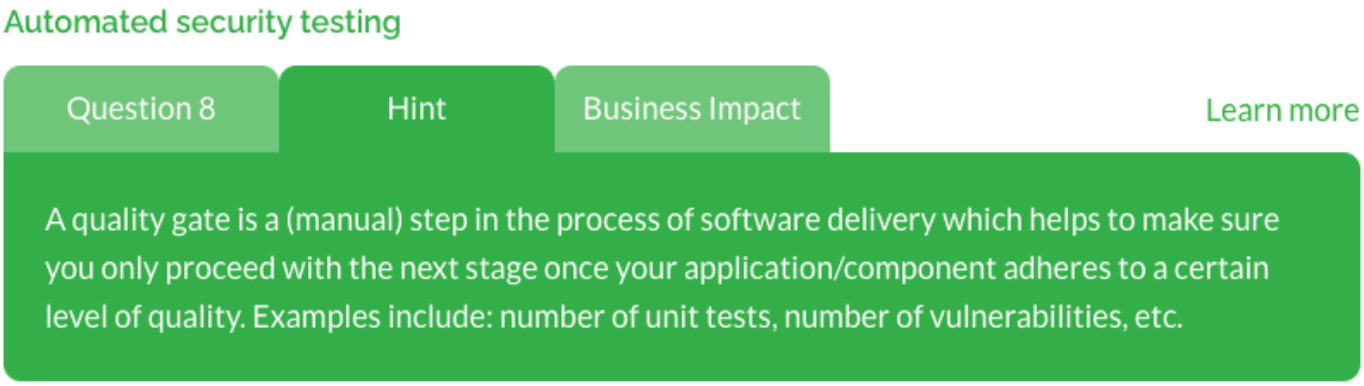
See the following example question to emphasize this:

Question	How do you select a new security tool or (cloud) solution for your organization? Requirements are very important.
Answer level 1	Requirements are not defined carefully. We don’t know the exact processes, most likely procurement has a big vote in it.
Answer level 2	We reach out to the security department and they handle it from what they think we as an organization need. Requirements are scattered and not centrally registered.
Answer level 3	The security department collects requirements and uses them to select a security tool. Big focus on technological aspects.
Answer level 4	Someone at the security department or the business department identifies new types of risks. They work together to gather proper security requirements, which are collected, prioritised and shared before a decision is made.

If your answer does not match with one of the predefined answers, you can select the 'My situation is different' option. As we collect the results, we can then contact you to find out what your situation is different. Based on the context you provide, we can help to find a customized solution or guidance on how to proceed to the level which closely matches your specific situation.

Hints

Since we also aim to provide this solution to business representatives, we provide hints and extra explanations to get them up to speed with the specific topic. For example, we explain what the "least privilege principle" is or why containers differ from Virtual Machines and what that means to security related aspects.



These tips also help you to discuss any details / questions you might have with us or your development teams. Feel free to stop and restart the wizard at any time. Your intermediate results are stored and secured.

Business impact

Security always has an impact on your business. The information in this tab focuses on two aspects which complement each other: risks and risk mitigation benefits.

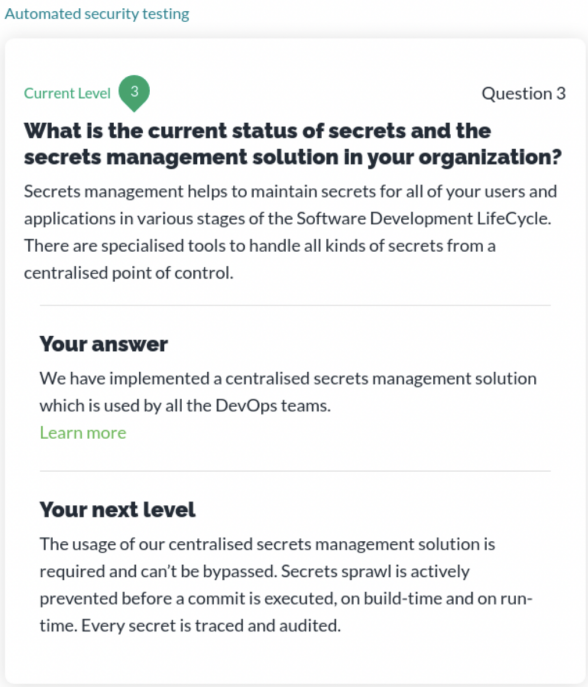
Risks have to do with business risks. What happens when you do not spend time and energy on a specific security related topic. What does that mean to your organizational processes, data security, customer satisfaction, etc. And how important is the specific topic to your business continuity.

Risk mitigation benefits provide an answer to the above. It helps your business representatives justify why time and effort should be spent on a certain topic. This pushes discussion in the right direction and helps you to get (senior) or executive management support for your decisions.

Learn more

Every question has a so-called "learn more" link which brings you to another website / webpage that explains in deeper detail what the topic of the question is about. Sometimes the information is deeply technical but hopefully you will get an idea of what it is all about. You can also use this information to steer discussions with (technical) persons in your organization to help you bring the message to who-ever decides about important subjects.

Keep in mind that the "learn more" link opens in a new tab or window, so be sure to return to the wizard once you've read the contents.



Score report

As soon as you finish all of the questions you will get a so-called “core report”. In this score report you will find the following aspects:

- The total score for all of the questions.
- An explanation about the levels.
- The list of questions and your answer plus the score level of that answer and how to advance to the next level.
- A graph which depicts how well you score for each category.
- The option to contact us and discuss your score.

The following screenshot depicts the answer to one of the questions.

Advance to a higher level

Business value and customer satisfaction can be increased by the following main drivers that proved to be successful in the software industry:

- Customer satisfaction increases since you can ship secure software faster. This helps to build trustful relationships with your customers and they might also be more involved in your software application. With the help of them (by ways of feedback gathering) you can continuously grow your efforts. In the end it helps your entire organization.
- Every phase of the Software Development LifeCycle is packed with security best practices which answer the needs of all the stakeholders. This increases the transparency, trust and confidence of everyone who is involved. All together this results in lower business risks.
- Reduce development and operation costs by enabling fast feedback loops. These feedback loops help to capture software defects (bugs) and this eliminates the number of errors / incidents in production. Fixes happen very fast and your customers won’t feel the pain.
- Being able to respond faster to changes (becoming more Agile) and a reduced time to market. Adding security early on in the Software Development LifeCycle helps to eliminate security-related bottlenecks later on in the process.

Based on the score report, it's advised to make a plan to advance to a higher level for each question in which you can improve. There are multiple ways to do it. We would suggest the following 10 steps:

Step 1 Group your questions/answers per category.

Step 2 View the average score per category.

Step 3 Select the questions/answers (per category) which have the lowest score.

Step 4 Determine the next steps to improve your score.

Step 5 Concentrate on a few topics at a time, don't try them all at once.

Step 6 Start with some pilot teams.

Step 7 Evaluate and let those pilot teams share their success

Step 8 Convince the business representatives or funding partners to proceed with the next questions.

Step 9 Repeat these steps as long as this is needed.

Step 10 Re-evaluate every now and then to verify your growth.

One suggestion to practically implement the plan is to scope the security related aspects through (a series) of threat modelling which focus on the entire organization. Automated tests which you execute based on trial and error should reveal a gradual increase of maturity over time. This also helps to filter out false positives which tend to create an "alert fatigue" that makes your people ignore the issues. Your goal is to get better test results in the future.

In the end you would achieve higher levels of maturity in the different categories and you would reap the benefits.

Nuaware Assessment Workshop

Duration: 2x half-days

The end goal of the guided assessement is to establish a so-called "baseline" of which improvement projects can be started. Together they form the Maturity Assessment Project (MAP).

Step 1 Identify key persons

Identify a SPOC on both ends.The SPOC of the organisation presents a brief overview of the organisation itself (how many teams, number of employees (per role), the main departments and activities, etc) to Nuaware. This forms the basis from which the next steps are carried out.

Based on this information, nuaware helps to identify the main persons which are needed in every following phase of the MAP. End result is a list of key persons that have the authority to do whatever is needed from the perspective of their role. Besides this, they also have the right mandate to propagate changes which are needed as a result of the next steps.

Step 2 Conduct the DevSecOps Maturity Assessment

A consultant from Nuaware explains the main concepts and background of the DevSecOps Maturity Assessment to the key pers ons. Every key person answers the questions in the wizard. At the end, each key person can view the end report and check the links of the topics of the different categories.

STEP 3 Collect results and draw conclusions

In this phase, Nuaware collects the end results from their system. Based on these, they will draw conclusions and lay out the baseline. From here, Nuaware advises on the most important topics to improve.

STEP 4 Share results with key persons

A new meeting/session is held. Nuaware presents the (aggregated) results and the baseline. This is discussed with the key persons. The end conclusion is an agreement on the topics that are indeed most important to improve.

STEP 5 Create an improvement plan

This step is conducted together with the key persons. The plan consists at least of the following topics:

- Which aspects of the organisation to improve?
- How to actually improve it?
- Who is involved and who is (end) responsible?
- Use cases and/or success criteria
- Regular reporting and feedback loops

About this whitepaper

This whitepaper has been created by the DevSecOps consultants from Nuaware together with their partners. We based our contents on several years of the practical experience we gained through our customers and other organizations.

The following persons contributed to the DevSecOps Maturity Model and/or the whitepaper. Based on their expert level knowledge we ensure you get the best for your DevSecOps journey.

nuaware
An Exclusive Networks Company

Thank you.

nuaware.com

info@nuaware.com

+44 (0) 203 488 0530