

avatao

ASAP

Avatao Security Awesomeness Program

Ultimate guide to a thriving cybersecurity culture

Dear Security Fan, welcome to Avatao!

Our journey to develop the security culture in your organization using awesome hands-on training starts here. In this brochure we've collected all the useful information that will help you deploy a successful security program for your developers.

At the end of this guide you will find a survey that will help us gather the right information about your learning preferences. Please fill out the form so we can get back to you with our recommended training program.

Table of content

1. Glossary of terms
2. Prerequisites, a few important steps before you start deploying a security program
 - 2.1. Training types
 - 2.2. Defining objectives
 - 2.3. Defining roles (owners, team leads, security champions)
 - 2.4. Defining Team Structures
 - 2.5. Training scheduling
 - 2.6. Mandatory or voluntary
 - 2.7. Creating a training incentives
 - 2.8. Defining where they can go for help
3. Preparation for a successful rollout
 - 3.1. Programming languages
 - 3.2. Gathering vulnerabilities
 - 3.3. Team setup
 - 3.4. Collecting training materials and assigning to teams
4. Implementation
 - 4.1. Onboarding
 - 4.2. Monitoring the progress of the roll out on a weekly basis
 - 4.3. Populating your Teams
 - 4.4. Training advertisement
 - 4.5. Allowing system messages
5. Monitor, measure and optimize
 - 5.1. Tracking progress
 - 5.2. Checking vulnerability reports and comparing them to the previous period
 - 5.3. Soft results

1. Glossary of terms

Platform: next.avatao.com is the website where you can access the Avatao training platform.

Organization (aka ORG): Every group of learners has a separate customizable area within the platform.

Owner: Every ORG has at least one master user with the highest rights.

Admin: General administrator of the ORG, with slightly less rights than the Owner. Can add and delete members, create teams and add members to them, create custom modules, assign learning materials for users, and follow their progress via statistics and leaderboards.

Member: The learners who have access to the learning materials on the platform. They can complete their assigned learning tasks and are free to browse all the exercises.

Team: Group of Members and Admins who follow the same learning process and get the same assignments.

Team lead: Dedicated Member with Admin rights only for their Team.

Language: Programming languages, which are the most typical tags on the exercises.

Exercise: One single lesson, the smallest unit of the learning materials. There are two types of exercises:

- **Tutorial:** These are the easier of the two types of exercises. You can find step-by-step guidelines on how to finish the exercises on the sidebar.
- **Challenge:** This type of exercise is typically harder, and gives you a chance to practice what you have learned in the tutorials.

Module: A collection of similar exercises. We've prepared plenty for you, but you can always create your own modules.

2. Prerequisites

Defining the Training Type

You probably already decided on the type of training before you bought your Avatao licenses, but it might be worth taking a minute to think about whether or not there's anything else that could be useful for you.

Typical types security programs:

- **Awareness:** Here you aim for basic secure coding awareness for all developers.

- **Continuous learning:** With a constant learning process, developers need to be able to write less vulnerable code, which means the organization spends less time and money on fixing recurring bugs and reviewing code.

- **Compliance:** When you need to prove your developers' security skills meet the requirements of a particular set of compliances, you don't want to overdo the training. Short but relevant annual trainings will provide you with the right certifications.

- **Onboarding:** When you hire new employees, you can set their security mindset when you make a secure coding module part of their onboarding process. This way, they start working with being already security-conscious.

- **Recruitment:** It's hard to evaluate new employees' skills based solely on a CV. With an authoritative test you can make sure you're hiring developers with the right skills.

- **Challenges / CTF:** Want a fun way to challenge your developers? Run a CTF for individuals to identify security experts or for teams to make it a team building event.

Objectives of your Security Program

When you start implementing a security training program in the organization, the first step is to define a clear and measurable goal. We understand that your primary objective is to create an awesome product or service with secure code, and to achieve that, not all of your developers have to become security experts.

Sample objectives:

- **Awareness:** Every developer has to have basic security knowledge and secure coding skills regardless of role, seniority, location, or type (employee/contractor/supplier).

- **Continuous learning:** Reduce the cost associated with fixing bugs by 20%.

- **Compliance:** 80% of the developers have to finish a learning path within 4 weeks.

- **Recruitment:** Every candidate has to pass a test with a score of 80% or higher to proceed to the next round.

- **Challenges / CTF:** Two events per year to identify security experts and bring colleagues together.

Defining Roles

Implementing new training for the company culture is always a challenging task and can't happen without leadership buy-in and support. To ensure successful trainings, you need enthusiastic leaders to round up developers and smooth the way of their learning path.

Key roles:

- **Owner/Admins:** Your keenest security manager who, with Avatao's training, can take the company to a higher level. They are responsible for setting up the environment within the platform and monitoring the process based on the pre-determined objectives.

- **Team leaders:** The first one to call when it comes to the training itself. Responsible for keeping a clear team structure to make sure all the learners are getting the right training material and working on engagement within their own team.

- **Security champions:** Not necessarily your best security expert, but without a doubt the most dedicated learner. They're the first to finish all the assignments and are always there to help other team members.

Defining Team Structures

Before you start setting up your training, you need to think about how you want to categorize learners. Make sure to consider that members of each team will get the same learning assignments.

Typical considerations:

- **Language:** Make teams based on the programming language of the learners.

- **Location:** Categorize your colleagues according to which office they belong to.

- **Product:** Co-workers are teamed up based on the product or service they work on.

- **Job role:** Team together people with a similar job role to receive similar training.

You can also combine these groupings to create sub-teams, ensuring the right content is assigned to every member.

Training Scheduling

Specifying how much time you want your learners to spend with the training will highly affect the results. Too many assignments can easily overwhelm your developers, but keeping their interest up is key for continuous improvement. Based on our experience, 1-3 hours per month is what's needed to see progress. The best way to make sure your colleagues are aware of your expectations is to regularly give them training assignments with an achievable deadline.

Mandatory or Voluntary

It's always tough to decide whether a training should be mandatory or voluntary. Forcing employees to finish a course may not make them too happy, but you can be sure engagement will be high. Voluntary training, on the other hand, is often forgotten, and regardless of the number of reminders, a majority of the employees will never finish the course. If you decide to go with a voluntary training, think about rewarding the active learners to encourage better engagement.

Creating Training Incentives

Plan prizes like tickets to a security conference, mugs, stickers, and other swags to motivate your teams to take part in the training and increase team spirit and mutual learning. This will also be an opportunity for you to identify the developers that are truly motivated when it comes to learning about the security space.

Define where they can go for help

Any particular training can be simple for some developers but challenging for others, and getting stuck on an exercise can be very demotivating. Make sure all your learners are aware of where they can get the right support. You can report technical issues and bugs through the platform, and Avatao professionals are always around to give a helping hand. It's also important to announce who your internal support is: the admins, team leads, and security champions must be the primary support contact for your learners.

3. Preparing for a Successful Rollout

Programming Languages

The most important part of getting great engagement in security training is providing relevant training materials. Defining the programming languages for developers is essential to building a successful training program.

Gathering Vulnerabilities

Based on your bug reports and pentest results, team leaders can adjust the Avatao Learning Plan based on the recurrent and existing vulnerabilities you find in your organization. Make sure you personalize the trainings and focus on your developers' specific skills.

Team Setup

You probably already have an idea about what the best structure for your teams is and most likely also know who the team leaders are. At this point, you can create the team structure based on this guide: <https://avatao.com/media/Avatao-06-Teams-2022.pdf>

Be careful, you can't add members to the teams until they accept the invitation and register to the platform. We're not quite there yet.

Collecting Training Materials and Assigning to Teams

Your teams are ready to go and you have the finalized Learning Plan for each team, so there's not much left to do other than assigning the related exercises for the first learning period to each team.

4. Implementation

Onboarding

We're now at the point where your training platform is prepared and it's time to show off to your colleagues. To get started, you need to invite all your team members to the platform. Once they are in, the system automatically assigns them the onboarding module that will teach them the basics of navigating the Avatao learning platform. To avoid any confusion, please share the step-by-step kick-off guide with all learners through this link.

Pro tip: We recommend importing email addresses from a CSV file, as this way you'll be able to follow who hasn't yet accept the invitation.

If your company is using any of these identity providers (<https://auth0.com/docs/authenticate/identity-providers>), please contact support@avatao.com to complete SSO set up.

Monitoring Progress of the Rollout on a Weekly Basis

It's very important to get everyone on board, so it's worth taking a few minutes every week to monitor who hasn't registered yet and sending them a reminder or asking if they need any assistance.

Populating your Teams

Once your colleagues have all registered to the platform and finished the onboarding module, it's time to organize them into the pre-made Teams. Make sure everyone is placed into the right team based on the previously defined conditions.

Training Advertisements

Our team is prepared to provide you customized online flyers with step-by-step instructions, pro tips, or best practices that you can share with your colleagues. Sending these out regularly within your intranet/ mailing system will help the team keep up-to-date with the training.

Allowing System Messages

The Platform sends automatic reminders about new assignments, upcoming assignment deadlines, and other important information about the training process to members. Please make sure your company's mailing system is not blocking these messages.

5. Monitor, Measure, and Optimize

Tracking Progress

Even though we've created a solid learning program for the whole training period, from time to time it will need some maintenance. You regularly need to make sure all of your team members are on the right track and progressing with their training plan as you expect them to. Following up on whether or not the assignments are done in time and giving new assignments at the beginning of every period is key, but it shouldn't take too much time for you and your team leaders if everything was properly planned out. Though of course there is always room for improvement if it turns out the pace is too fast or too slow for your team.

Checking Vulnerability Reports and Comparing them to the Previous Period

To see the real, measurable results of your training, it is worth checking your vulnerability reports and comparing them to the previous period. The considerable metrics can be:

- number of vulnerabilities disclosed
- time needed to fix vulnerabilities
- number of security issues solved
- reduction of delays in product development

Note that the Avatao team does not have access to this security information beyond the learning platform, but our Customer Success Team is always here to discuss adjustments based on the learnings.

Soft results

In addition to the measurable results mentioned above, you can also build a strong security-minded culture within the company. Check to see if security and dev teams are collaborating more: developers and security need to speak the same language and work together!

Talk with your team and get their feedback about what they learned and how it applies to their daily job. This can be a good way to measure their behavioral changes towards security.

.

avatao

Thank you!

In case of any questions contact us:
customersuccess@avatao.com