KONDUKTO

How to Scale A Security Program?

Case Study

How Trendyol, a decacorn e-commerce company uses Kondukto for **security automation**

A case study about security automation and AppSec effectiveness with Trendyol.

Chapters

The Challenges

- There was not enough **security automation** to catch up with the speed of software development
- **Lack of visibility** made it difficult to assess the effectiveness of AppSec program
- **Lack of orchestration** made it difficult to put the pieces together

KONDUKTO | trendyol.com

How to Scale A Security Program?

Case Study

About Trendyol

Founded in 2010, Trendyol has grown to be the largest **e-commerce company** in Turkey by reaching the decacorn status in 2021. After the investment of Alibaba in 2018, the company also started to serve in many European countries and expanded into new lines of business such as **second-hand clothing** and **on-demand delivery.** Massive operations and rapid growth of the tech team required an efficient and scalable AppSec program to keep up with the speed of company growth accompanied by a proliferation of applications.

The Situation

With development teams growing each day, it was frustrating for security teams to make sure applications were shipped to production without exploitable vulnerabilities. Manual processes were **time-consuming** and with security and development teams working in silos, the **lack of collaboration** hindered security from being an integral part of software development processes.

A plethora of findings discovered by **various automated tools** and **manual activities** were scattered across different interfaces which were **challenging for the security team** to keep up with.

That is when our paths crossed with Trendyol security team and with their vision to support promising start-ups in the security space, we started working together to find creative solutions to their problems.

KONDUKTO | trendyol.com

How to Scale A Security Program?

Case Study

Our Approach

1. In the beginning, to prevent losing time with manual scans, **all scanners of Trendyol were connected with Kondukto** platform to trigger scans in an automated fashion using the scheduler of Kondukto and the CLI to trigger scans within pipelines.

2. To enable a **self-service security approach**, new applications created by development teams were **automatically pushed from the source code management tool** to Kondukto through CLI. This way security teams did not have to deal with creating new applications on security tools each time a new application was created on the source code management tool.

3. Various **open source security tools** that come out of the box with Kondukto were also used in the process before Trendyol made an investment in commercial alternatives. These open source tools were also **customized based on Trendyol's needs to keep** the spotlight on the prioritized vulnerability types.

4. For grouping applications based on their risk profile, **applications were labeled** on Kondukto **based on the threat modeling questionnaire** filled out by development teams. **Different automation rules were created** for different labels as applications with high-risk profiles required more immediate attention than others.

Results

Creating a CI/CD pipeline where each security test is run through Kondukto CLI has quickly made manual scans redundant and security has become an integral part of pipelines for more than 3.000 applications.

Security and development teams are **instantly notified about scan results** on their Slack channels to make sure no critical vulnerability goes unnoticed.

Combining the results of automated tools with vulnerabilities discovered in manual activities such as penetration tests, manual reviews and bug bounty programs, **overall security posture can easily be tracked on a single platform** where development and security teams can speak the same language.

Tickets are created on the Jira boards of developers by security teams through Kondukto UI and remediation metrics can also be measured to decide if everything is on the right track. When a developer closes an issue, Kondukto **automatically runs a validation scan** and **reopens the issue if the vulnerability is rediscovered** by the scanner.

Results

To prevent recurring vulnerabilities in the future, **developers are assigned personalized secure coding courses** on Codebashing through Kondukto UI after analyzing the types of vulnerabilities introduced into the source code by each developer.

Using this risk-based approach to create separate automation rules for different applications, Kondukto, **security teams made sure they quickly raised the flag for vulnerabilities** that posed a real threat **with minimum human effort.**

Using all the orchestration and automation capabilities of Kondukto, Trendyol made strides in **creating a scalable and automated AppSec program that is developer-friendly** at the same time.

Did You Read Our New Case Study White Paper?