No.36
April 2nd, 2020

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UN-SPONSORED**

Orange Funds New CI/CD Security Tool

HardenStance spoke with Orange Polska's security team as well as independent developers to appraise 'Mixeway', an open source security tool the company is funding.

- Orange Polska is funding Mixeway, an open source security orchestrator that automates security testing in CI/CD pipelines. It's already in use in two projects.
- Mixeway has a lot of things in common with other tools and needs improving but the GUI and aspirations to add correlation via machine learning do look interesting.
- In this emerging space, the role of open source and proprietary software is in the early stages of being contested. Open source needs critical mass to succeed at scale.

Development is Automating Faster Than Security

A major challenge for companies undertaking digital transformation is that the rate at which many steps in a CI/CD pipeline are being automated is accelerating faster than automation of the security testing components.

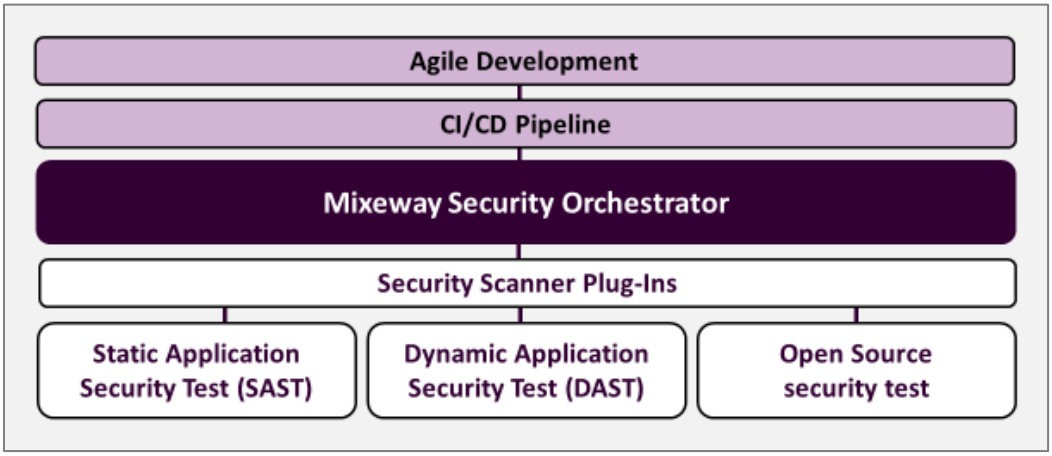
On its own, shifting security to the left only gets you so far. If CI/CD security testing isn't automated as well – if we don't evolve to Security as Code – it becomes the modern-day version of the multi-week or multi-month delay inflicted by security reviews at the end of a waterfall development project.

Most vulnerability scanners used in development today just weren't built to be automated in a CI/CD framework.

The trouble is that many of the vulnerability scanners in use today weren't built to be automated in a CI/CD framework. Integrating, say, dynamic application security scanning with a security vulnerability scanner requires adding a lot of code to the configuration of the pipeline. This increases complexity and makes it harder to maintain.

Another approach, shown in **Figure 1**, introduces a security orchestrator that is abstracted from the development team's code and provides plug-ins to the various security testing tools. On the downside, this adds another element into the tool-chain to be updated, secured and managed. On the upside, it gives developers a single pane of glass from which to manage their suite of security tools from within the CI/CD pipeline

Figure 1: A Security Orchestrator to Secure the CI/CD Pipeline



Source: HardenStance

and run them automatically. It does away with the need for a significant portion of Jenkins integration work. From a development perspective the integration and operational process remains constant, independent of which security tools you use.

Two years ago, working in collaboration with Poland's Ministry of Education and the Warsaw University of Technology, Orange Polska's CISO, Przemyslaw Deba, assigned a member of his information security team, Grzegorz Siewruk, to come up with a solution as part of an Industrial PhD programme. As shown in **Figure 1**, the result of this work is Mixeway, an open source security orchestration platform, written from scratch in Java using the Spring Boot framework.

Mixeway is already being used by some of Orange Polska's developers across two agile projects.

Although they were both an approximate match for Orange Polska's requirements, the idea of using available open source security orchestration tools, such as OWASP DefectDojo and Reapsaw, was rejected. Neither was considered capable of supporting all of the many security testing tools that Orange Polska uses, or the breadth of functionality supported by some of those tools. Both were also considered to be lacking in terms of auto service discovery capabilities. Rather than having to redefine the scope of a test whenever new assets are put in the cloud, Orange Polska wanted IaaS plugins to allow data to be collected about cloud assets by an automated API.

Static Application Security Tests can already be used

Mixeway is already being used by some of Orange Polska's developers across two agile projects. It's already being used to run Static Application Security Tests (SAST). Next up will be network scanners and Dynamic Application Security Tests (DAST). A patch has recently been added to support open source security scanning as well.

Although it wasn't expressly stated on the Mixeway home page at launch, the longer term vision consists of evolving it to become what the Orange Polska team thinks of as a broader, more fully-featured, type of security gateway. The goal here is to apply machine learning algorithms to Mixeway so that vulnerability correlation can be done more effectively across multiple tools. This should then reduce false positives, thereby increasing confidence in automating security in the CI/CD pipeline.

Mixeway was released as open source into the community on GitHub on March 11th. Orange Polska's CISO, Przemyslaw Deba, promoted it to developers on several cyber security and social media sites, inviting them to leverage it and "start securing your pipeline now". Mixeway is potentially applicable to any large organization with a wide variety of security testing requirements, not specifically a telco's.

Growing Open Source Adoption in Cyber Security

As well as speaking with Grzegorz Siewruk and Przemyslaw Deba, HardenStance obtained reviews of Mixeway from four different independent software developers, security professionals and software consultants. Before turning to that, it's worth considering the context of the broader landscape in terms of the open source movement.

To begin with, Mixeway's prospects certainly shouldn't be viewed through the lens of the telecom sector's record of driving its own open source projects. The record isn't very impressive but that's not very relevant. Rather this should be viewed in the context of an open source project within the cyber security discipline, irrespective of the type of organization, industry sector or security use case.

In this context, arriving at greater collaboration and automation through openness across different vendor products in security operations is absolutely key to hardening enterprise security posture. And the growing potential of open source software in cyber security is increasingly important to achieving that.

Open source software has been making its way into the cyber security space for some years but adoption is accelerating now. Recent examples of how, at a high level, Mixeway fits with the open source security zeitgeist include:

- The importance of open source components to the phenomenally popular MITRE ATT&CK Framework in terms of open source reporting and attack simulation options.
- The end of 2019 launch of the now 27 member Open Cybersecurity Alliance (OCA). Driven initially by IBM Security and McAfee, OCA has as part of its core mission statement the goal to "develop and promote sets of open source common code, tooling, patterns and practices for sharing data among cyber security tools."
- IBM Security's portfolio is increasingly dependent on open source. To give just one of many examples, look under the hood of the company's new Cloud Pak for Security for cloud migration and you'll find that one of the components driving it is Stix-Shifter. This is an open source python library allowing software to connect to products that house data repositories using STIX Patterning. The acquisition of RedHat is only accelerating the rate of open source adoption by IBM Security.

Two reviewers consulted by HardenStance point to a valuable innovation in the form of Mixeway's GUI.

Reviewer Feedback Points to GUI Differentiation

Now to the initial reviews of Mixeway that HardenStance's relevant contacts shared. The following is a representative sample of those reviews:

- Two of the reviewers that were consulted point to a valuable innovation in the form of Mixeway's GUI. One, stated that "the visualization of results looks nicer than that found in Jenkins." Another, from an individual in a company that is a leader in using open source software, referred to Mixeway's GUI as "a differentiator".
- Other than with respect to the GUI, reviewers didn't find Mixeway especially ground-breaking. In addition to overlap with DefectDojo and Reapsaw, reviewers pointed HardenStance to some commonality with other some other tools as well.
- The Mixeway website has been improved since the March 11th launch but it still isn't as clear and compelling as it should be. Whether it's as a result of lack of time or disdain for marketing glitz or pizzazz, the error is the same. It's not just other developers that need convincing to invest time in a project. Their boss, and the boss of their boss, need convincing too. A project's mission and long term goals need to be really well articulated on the home page. Heavily time-constrained professionals of all sorts need to be able to quickly understand whether what's on offer is a piece of software they can use tactically or a bigger relationship that's worth investing time and resource in towards a common, long term, goal.
- The Mixeway code itself is improving but it's still some way short of high quality software. For example, there are insufficient supporting comments. Grzegorz Siewruk recognizes this himself. After all, he's an information security professional, not a software developer. The scarcity of people that are strong in both disciplines – and the associated costs of employing such people – is one of the biggest challenges to securing the CI/CD pipeline.
- Organizations should be thinking in terms of shifting security to the left and automating it across multiple pipelines covering not just software but cloud deployments and web applications as well.

What makes the job of assessing the outlook for Mixeway a lot more complex is that it isn't just any old security tool, it's an orchestrator. As in many other contexts – security as well as other domains - Mixeway is intended to fill a gap in the market in open orchestration products which isn't adequately filled today by vendors.

User organizations fear the cost and lock-in potential of vendor-supplied orchestration tools that the likes of Tenable or Qualys are well-suited to supply in this space. Vendors don't always do the best job when it comes to openness. But they're also rightly wary of committing development dollars to truly open orchestration platforms for which there might not be enough demand (at the right price to generate an ROI) and which also risk cannibalizing their own portfolio. The demand and supply side of industry is wrestling over who should bear the cost of this critical integration and abstraction software that's required, what form that cost should take, and what price tag should be attached to it.

Orange Polska's security team is trying to drive the open source model with Mixeway but it faces two big challenges to take it to the next level:

- While it has won over a subset of the company's developers to using Mixeway, the security team still has to persuade many more. As in most companies, it faces an ongoing internal challenge of positioning itself as peer to peer advisors and enablers rather than obstructive gatekeepers. Mixeway can help developers solve a problem but only if they are persuaded that it's in their own - and their company's - interest to take the required role in solving it. This is a challenge of management leadership and interpersonal skills - bigger challenges than the technical ones.
- The second challenge is to engage others outside Orange Polska to use Mixeway and contribute to the further development of the code. As initial reviews suggest, there are some aspects that should trigger third party interest. However, more is needed in both software development and business development savvy.

For now, Mixeway is a contribution to addressing an important problem space. To stand any chance of making a mark, it needs to engage a lot more stakeholders. ■

More Information

- Review Mixeway on GitHub
- Contact Grzegorz Siewruk: Grzegorz.Siewruk@orange.com
- HardenStance: "Cyber Security Innovators: Orange Polska" (February 2019)
- HardenStance: "Security Imperatives for Digital Transformation" (September 2019)
- HardenStance: "A Blueprint for a Cloud Native Telco" (February 2020)
- Contact HardenStance's Principal Analyst: patrick.donegan@hardenstance.com
- Register here for free notifications whenever HardenStance releases new content.
- HardenStance received no payment – direct or "in kind" – for publishing this briefing.

HardenStance Ltd Disclaimer of Warranty and Liability