CASE STUDY

COMPANY DETAILS:
French carpooling marketplace with 90 million members in 22 countries.

BUSINESS NEEDS AND CHALLENGES:

- Reduce risk by detecting suspicious activity and misconfigurations.
- Automate alerts and streamline incident response.
- Secure containers without adding operations management overhead.
- Flexibility to fine-tune security to their needs.

BUSINESS IMPACT OF SYSDIG:
The security team of four has been able to empower the 200 developers to own their applications from development through the container lifespan, including managing the security posture. BlaBlaCar is able to keep its security team and overhead small with an efficient secure DevOps model.

SYSDIG PLATFORM BENEFITS:

- Deep visibility to detect suspicious activity and misconfigurations.
- An easy to deploy and maintain SaaS-first solution.
- The power of open source Falco with an enterprise experience.
- Forensics capabilities.

INFRASTRUCTURE:
Google Cloud Platform (GCP) and Yandex Managed Service for Kubernetes

ORCHESTRATION:
Google Kubernetes Engine (GKE) and Yandex.Cloud

The BlaBlaCar Security Team of 4 Empowers Developers to Manage Security Risk with Sysdig

Overview

BlaBlaCar is the world's leading long-distance carpooling platform, with a global community of 90 million drivers and passengers across 22 countries. The platform connects people looking to travel long distances with drivers heading in the same direction so they can travel together, share the cost, and reduce their impact on the environment.

Challenge

After deciding to add more than 120 nodes to Google Cloud Platform (GCP) and Google Kubernetes Engine (GKE), the BlaBlaCar security team of four people looked for a security solution. Supporting a development team of more than 200, the security team needed a way to empower developers to build and run applications in production, and to ensure security throughout the container lifecycle.

According to Jeremy Courtial, Security Engineer at BlaBlaCar, “We run what many would consider ‘DevOps.’ The developers are responsible for everything, including security. It's not just an ops team that gets the application, then deploys and monitors them in production, but it is the developers that are doing all of the work from the beginning to the end. The ops team is mainly here to set up the infrastructure and give the right tool for the developer to monitor and deploy the applications. The security team is there to empower them.”

When working through the selection of possible tools to use, the security team narrowed their consideration to five solutions to be tested against specific criteria. According to Courtial, “Some of the things we compared included the ability to detect misconfigurations in the Kubernetes workload and suspicious activity. For example, would it detect if someone downloaded a binary, started it, and then it started a connection to something else on the internet? We also had some image scanning benchmarks, like how many vulnerabilities were detected? We wanted to see how they are displayed in the solution, including the level of detail or lack thereof. ”

Why BlaBlaCar chose Sysdig

After comparing the five solutions, BlaBlaCar selected Sysdig. As Courtial explains it, “One of the most important tests for us was the ability to detect both suspicious activity and misconfigurations, and Sysdig did so the best. We also wanted to avoid having a whole platform deployed inside our production, so we preferred a SaaS solution. Lastly, we were also looking for something that we could really fine tune, not only the rules, but also the way we receive these alerts and the ability to export them. Sysdig’s forensics capabilities were really impressive. Price played a role as well.”

Knowing the solution they picked would run on GKE also factored into their decision making. According to Courtial, “Sysdig’s eBPF instrumentation and the work the Falco community and Sysdig has done with Google gave us confidence knowing Sysdig would run on GKE, and we saw that first hand during the evaluation stages. There was one tool in particular that we evaluated that had issues with GKE.”

Evaluating Sysdig and Falco

Sysdig is built on Falco, along with several other open source tools, including open source sysdig, Sysdig Inspect, Prometheus, Anchore Engine, and Cloud Custodian. Falco, a cloud-native runtime security project created by Sysdig and contributed to the CNCF, is considered the de facto Kubernetes threat detection engine. Sysdig and Falco were evaluated separately during the POV process.

Walking through the decision of selecting Sysdig over Falco, Courtial said, “We considered Falco alone, but we went with Sysdig in the end because we are a small team. We have four security people and not everyone is working on the platform. Having

> “Having a technology as complex as Falco packaged together with professional support and a SaaS infrastructure allows us to focus on the integration instead of spending time on setup and maintenance.”
>
> – Jeremy Courtial,
> Security Engineer at BlaBlaCar

a technology as complex as Falco packaged together with professional support and a SaaS infrastructure allows us to focus on the integration instead of spending time on setup and maintenance. We also wanted some container scanning features, which would have meant we needed to find, deploy, and maintain an additional tool. With Sysdig, we get an all-in-one package."

Going into further detail, Courtial said, "Sysdig customers benefit from the community contributing, just as Falco users benefit from Sysdig's contributions to Falco. The fact that Sysdig extends Falco was really enticing to us. With Sysdig, we knew we were getting the best tool integrated with Falco. Finally, and to be totally honest, as Sysdig uses Falco rules, we knew that if Sysdig didn't fit our needs in the end, we could still migrate to Falco without having to start everything from scratch."

Equipping developers with secure DevOps

Sysdig provides deep data insights and problem isolation across the entire cloud-native environment to help monitor and troubleshoot health and performance. This visibility and alerting empowers the hundreds of developers at BlaBlaCar to take control of their security risk.

> "We use Sysdig to identify and alert us to suspicious activity and misconfigurations, and more generally, workloads that may cause security risk."
>
> – Jeremy Courtial,
> Security Engineer at BlaBlaCar

Explaining how Sysdig is used at BlaBlaCar, Courtial said, "We use Sysdig to identify and alert us to suspicious activity and misconfigurations, and more generally, workloads that may cause security risk. How it works for us, we set up Sysdig to monitor specific rules. In the event that one is triggered, the developer gets an alert from Sysdig via PagerDuty that includes documentation for the specific alert, such as how to whitelist the behavior by adding a line to the Falco rule. Developers receive the alerts, take a look at them, and then come to us if they have questions or have any doubts. We want them to be able to investigate themselves."

Expanding on the process, Courtial said, "Our job is to empower the developers. The end goal is for it to be self-service for them. It is less efficient for the security team to do everything ourselves. Rather, we are here to support them and help them if they get stuck, but we don't fix issues or check every alert ourselves. We do check some alerts, but we won't go deeper unless we think it's really suspicious or dangerous. Generally, we expect the developers to maintain the security of their workload in the same way they do with any other metrics, such as performance or reliability."

Easy to deploy, easy to maintain, and a true partner

Being a small group, BlaBlaCar's security team needs an easy-to-maintain solution. According to Courtial, "Being a SaaS solution, Sysdig was very easy to set up and to maintain. We just deployed the agent. Sysdig does all the hard work, so it was really easy for us. The ease of use with the tool has been great, and since day one, the Sysdig support team has been very good. They are very responsive. Several of the features we requested were implemented in the product."

Relationships are important to BlaBlaCar and it's also a reason BlaBlaCar selected Google as its cloud provider. As Courtial explains, "We saw that we could have a good partnership with Google. They would give us support that we didn't think we could get with the other cloud providers we looked at. Sysdig has been similarly just as responsive when we reach out."

Advice for peers getting started with container security

Asked what advice he has for companies moving to containers, Courtial recommended two things, "First, you need to work to get every stakeholder on board from the beginning. We worked with the ops team so they knew what we were expecting. We had discussions from the very beginning. That helped both of our teams to understand the requirements, specificities, needs, and constraints."

> "Being a SaaS solution, Sysdig was very easy to set up and to maintain. We just deployed the agent. Sysdig does all the hard work, so it was really easy for us."
>
> – Jeremy Courtial,
> Security Engineer at BlaBlaCar

Courtial's second piece of advice outlines how to make the developers and operations teams more efficient. "After you have buy in, you need to consider some type of security monitoring and you should make sure the alerts are actionable. We used another security tool first and we didn't do the same work to make the alerts actionable like we have with Sysdig, so when our developers and the operations teams received alerts, they didn't really know what to do with them. The idea is for the developers and operations team to make sure they have all the information they need to understand an alert so they can take action. It's really important to explain what is wrong and why, and what they can do to fix it rather than just saying something is wrong. DevOps has empowered our developers to be more efficient, but it's up to the security team to put the right tools in place."

To learn more about Sysdig, visit www.sysdig.com or to try a free trial visit www.sysdig.com/trial.