LACEWORK

CASE STUDY

Visibility into Amazon ECS provides application context

Poka

Challenges

- Scaling up monitoring with new AWS Elastic Container Services (ECS)
- Overcoming alert fatigue and alert management
- Demonstrating security and compliance to customers

Solutions

- Provides visibility inside AWS ECS
- DNS enriched alerts
- Easy to implement and learn

Results

- Better application context for alerts, faster alert resolution, and reduced alert fatigue
- Replaced several security tools, reducing complexity and improving cost efficiencies
- More time to fix real issues

> "We were receiving logs from the machines, but not the containers. We weren't getting the application context we needed."
>
> MAXIME LEBLANC, INFORMATION SECURITY SPECIALIST (SECOPS) AT POKA

The company and its business

Poka is a connected worker application built specifically for manufacturers. It brings together collaboration, training, and skills management into a single integrated platform to empower factory workers to learn continuously and solve problems autonomously. Designed from the ground-up as a cloud native application, Poka lets companies build their own proprietary knowledge base to use and share globally. The Poka application is built on an Amazon Elastic Container Service (ECS) architecture running in their AWS environment. As the application grows, the company continually adds new containerized instances and features.

The security challenge

As Poka grew, customers wanted to see more evidence that their proprietary operational knowledge would be protected. Also, as Poka added more ECS containerized instances, they struggled to keep up with a growing number of security alerts. Tools they adopted to automate aspects of monitoring and log analysis failed to provide the visibility they needed. "We were missing depth," says Maxime Leblanc, Poka's Information Security Specialist (SecOps). "All those tools are host-based. We were receiving logs from the machines, but not the containers. We weren't getting the application context we needed."

Choosing Lacework

Early on, Poka adopted Threat Stack to help automate alerts, but they spent too much time analyzing alerts to see which ones posed real threats, and they had to continually adjust rules to whitelist certain types of alerts. Then they discovered Lacework, which checked all of the boxes. It provided full visibility into the inner workings of AWS ECS, included a dashboard to demonstrate compliance to customers, and promised to ease alert fatigue through AI-learning.

Implementation

Poka found that implementing Lacework went very fast. "It was very easy and only took one day," says Leblanc. He credits the short learning curve to Lacework's industry-standard user interface.

Simplify monitoring and enrich alerts

With Lacework, Poka has accelerated alert analysis and resolution. Leblanc explains, "We are very impressed with the graphs that show all the DNS enriched network flows that go from the process to the Amazon service. It's easy to pinpoint an issue and go from the alert to the actions you need to take." The dashboards also simplify compliance reports. Having Lacework enabled Poka to drop other tools they were using, including Threat Stack. This saved them money and simplified their security management workflow. "It's much easier to centralize our entire alerting system," says Leblanc. It also reduced alert fatigue and streamlined the alert whitelisting process. Leblanc says, "Lacework learns the rules changes as they come. I can spend my time fixing real issues instead of fixing the whitelisting."

An added benefit is Lacework's ability to track multiple AWS accounts with CloudTrail integration, which helps developers who typically work with several accounts. Leblanc says, "Now each developer has their own job trail that lets them keep an eye on everything."

Find out more at lacework.com