CASE STUDY

Swimlane transforms compliance processes and vulnerability management with actionable insights

SWIMLANE

Challenges

- Assess overall risk posture of enterprise cloud operations
- Automate real-time container image vulnerability assessments
- Improve complex and inefficient compliance audit processes

Solutions

- Met success criteria (e.g., anomaly detection, compliance reporting) with integrated solution
- Detected anomalies and vulnerabilities within 30 minutes of setting up Lacework
- Easily integrated with the Swimlane security automation platform through the Lacework API

Results

- Save ten hours per week on monitoring and improving compliance
- Patch several hundred CVEs on hosts, including critical vulnerabilities like Log4j
- Shift security practice left with Lacework IaC Security

> "The Swimlane low-code automation platform enables fast automated response on its own, but we needed a partner with strong application programming interfaces (APIs) in order to access the granular telemetry we needed."

MICHAEL LYBORG, SENIOR VICE PRESIDENT OF GLOBAL SECURITY AND ENTERPRISE IT, SWIMLANE

“

We estimate that Lacework has saved us ten hours per week on monitoring and proving compliance.”

MICHAEL LYBORG, SENIOR VICE PRESIDENT
OF GLOBAL SECURITY AND ENTERPRISE IT, SWIMLANE

About Swimlane

Swimlane was founded in 2014 to provide a cloud-scale, low-code security automation platform for enterprises and service providers. The platform harnesses the power of the world’s most extensible security automation engine to unlock the potential of automation beyond the security operations center (SOC) and serve as the system-of-record for the entire security organization. Swimlane benefits customers by uniting disparate alerts, products, processes, and teams for faster and more effective security and incident response.

Michael Lyborg, Senior Vice President of Global Security and Enterprise IT, leads a hybrid team of seven specialists to manage Swimlane’s Zero Trust model. Lyborg’s team enables a global workforce by automating and managing Swimlane’s infrastructure, security, technology, business intelligence systems, and operations. By working closely with teams including cloud infrastructure, product, engineering, and delivery, Lyborg supports Swimlane’s internal and external customers.

Swimlane operates predominantly on Amazon Web Services (AWS) and utilizes Amazon Elastic Kubernetes Service (EKS) for their containerized environments. “We’re moving more and more towards cloud-native services,” Lyborg explains. Swimlane also supports Google Kubernetes Engine (GKE), Azure Kubernetes Service (AKS), bare metal, and hybrid cloud environments. “We make sure that our product works well in Google Cloud and Azure since we have customers who run those environments, but we mainly deploy our own production workloads in AWS,” says Lyborg.

Challenges

In their search for a cloud security solution, Swimlane needed a platform that offered the full spectrum of coverage: file and host integrity monitoring; vulnerability, intrusion, and anomaly detection; and compliance reporting. Ultimately, states Lyborg, “We needed to be able to assess our enterprise cloud operation’s overall risk and posture, and use that information to prioritize our work.”

Although the Swimlane team already had security automation, endpoint detection and response (EDR), and managed detection and response (MDR) capabilities, Lyborg adds, “We wanted to get more granular with the actionable insights we use to automate standard incident response and remediation playbooks. The Swimlane low-code automation platform enables fast automated response on its own, but we needed a partner with strong application programming interfaces (APIs) in order to access the granular telemetry we needed.” In particular, explains Lyborg, “Vulnerability management was key for us, because if we can control identities, and if we can control vulnerabilities, then the exposure and risk decrease exponentially.” By strategically deploying agents across their cloud environments, they hoped for visibility into any changes that would occur, including new vulnerabilities. “We didn’t necessarily have a gap because we had a lot of point solutions, but this process was complex,” says Lyborg.

Swimlane’s approach to compliance also needed some simplifying. Previously, they had done compliance through semi-automated scans, mapping, and disparate tooling. “We could automate parts of our compliance process, but we had to do manual mapping to each model to see where we were compliant,” remembers Lyborg. While the team performed these operations for both infrastructure and cloud environments, Lyborg adds, “The cloud is more difficult because it’s a dynamic, ever-changing environment. There were a lot of manual steps and spreadsheets involved just to gather the evidence.” To help maximize efficiency, Swimlane’s lean team sought a partner who could support their automation goals through strong APIs.

Solution

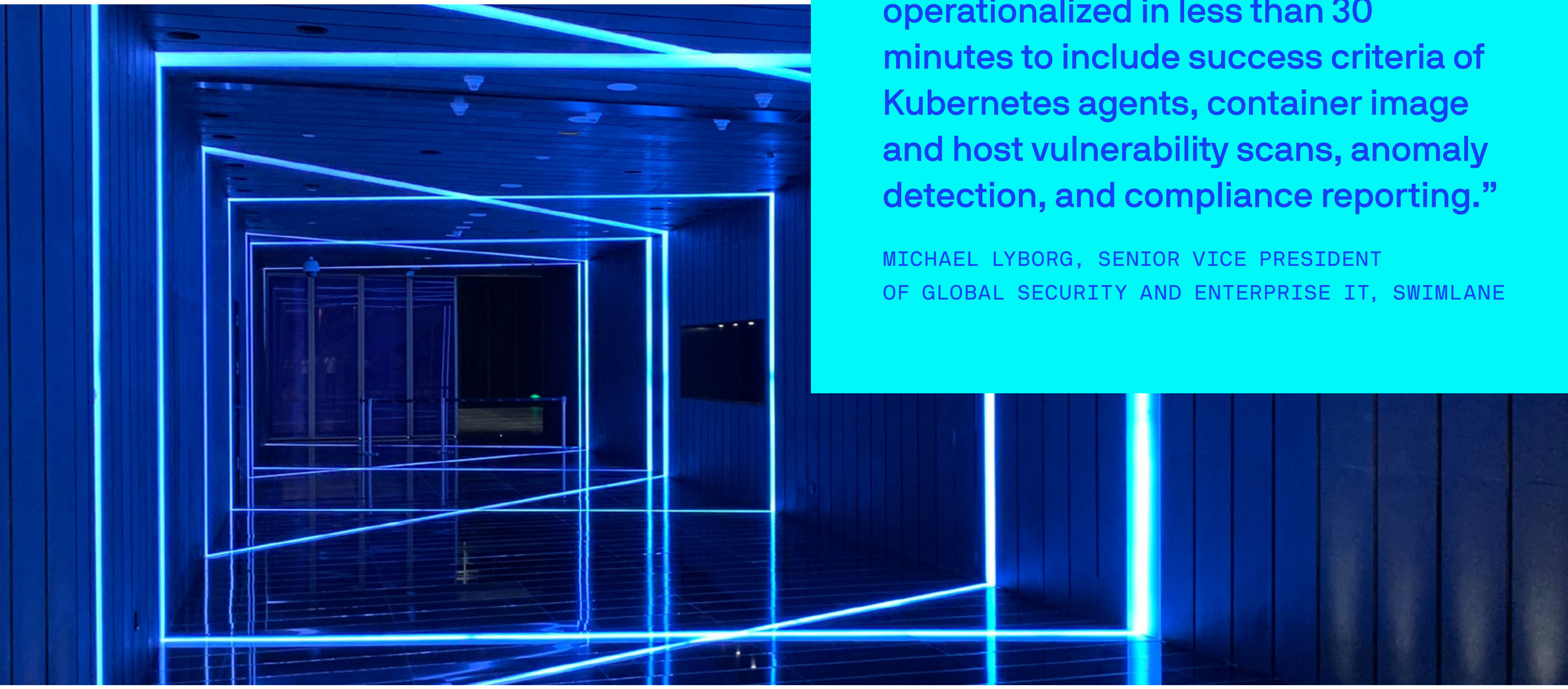
When Swimlane started a proof of concept with Lacework, they were on a tight timeline. “By the time we started engaging with the Lacework team, we were within a 30- to 45-day window of going to production,” Lyborg remembers. “We had to decide whether to ingest telemetry from multiple sources or use the Lacework API to streamline our automation goals.” According to Lyborg, “Our proof of value deployment was operationalized in less than 30 minutes to include success criteria of Kubernetes agents, container image and host vulnerability scans, anomaly detection, and compliance reporting.” By seeing the Lacework Polygraph® Data Platform in action, Lyborg says, “We quickly observed our success criteria being met and checked each off the list. Our deployment showed that a single platform could effectively include Kubernetes agents, container image and host vulnerability scans, anomaly detection, and compliance reporting.”

The deployment also proved that the integration of Lacework and the Swimlane platform would provide actionable insights to Lyborg’s team, allowing for hyperautomation and eliminating the need to hire several people. “Lacework was phenomenal,” says Lyborg. “You’re only as good as what you know and what you see, and Lacework gave us incredible insight in one place.” Swimlane selected Lacework as their partner for posture and vulnerability management, and workload protection.

By ingesting data into the Swimlane platform in a matter of seconds, Lacework enabled Swimlane to understand their overall risk and more easily prove compliance. The OpenAPI spec was especially compelling. Swimlane can extract host and container vulnerability data directly from the Platform with the Lacework API. The data parity between the user interface and API gives Swimlane the freedom to integrate it into their workflows and downstream tools. “We looked at some other vendors that didn’t have APIs, which makes it really difficult to pull the information you need if you’re working with other tools,” Lyborg recalls. “Part of our partner selection included evaluating the ease of integration.”

Compliance was another key reason Swimlane opted to bring on Lacework. Achieving compliance and answering auditors’ questions is one of the most challenging tasks for Lyborg’s team. “It’s generally easy to show auditors the policies and controls, but providing evidence, especially for multiple certifications, is a full-time job,” Lyborg states. “With Lacework, we were able to just log in, export all of our evidence, and immediately see where we’re doing work and where we have gaps.”

> “Our proof of value deployment was operationalized in less than 30 minutes to include success criteria of Kubernetes agents, container image and host vulnerability scans, anomaly detection, and compliance reporting.”
>
> MICHAEL LYBORG, SENIOR VICE PRESIDENT
> OF GLOBAL SECURITY AND ENTERPRISE IT, SWIMLANE



Results

Streamlining compliance

Lacework has helped Swimlane with compliance standards including SOC 2, ISO 27001, and NIST 800-171. With general compliance violation reporting and alerting from Lacework, Swimlane has been able to automate their trend reporting and posture management. "With Lacework, we know we're following best practices," says Lyborg. "For example, Lacework will show us if we are non-compliant, explain why, and then give us a recommended course of action so we can show compliance."

Moreover, Swimlane has drastically improved their automation outcomes. Explains Lyborg, "We take data from Lacework and put it into our platform through the API. Then, we put it into the Swimlane platform (our system of record), map it to all of our existing controls, and get risk calculation scores." While their compliance process was previously time-consuming and challenging, "Now that we can ingest data from Lacework into Swimlane, we can easily correlate and aggregate alerts and events in order to threat hunt across our enterprise cloud technology stack," Lyborg says. "Lacework standardizes the format for pulling the data, which has been one of the biggest areas of time savings." Though they're still building their baseline, Lyborg notes, "We estimate that Lacework has saved us ten hours per week on monitoring and proving compliance."

Consolidating telemetry sources

With an integrated solution, Swimlane has noticed a positive cultural shift. "The infrastructure and site reliability engineering (SRE) teams use Lacework to help with our day-to-day operations and the health of our infrastructure as well," says Lyborg. As the primary Lacework user at Swimlane, Lyborg adds, "Every time you bring in a source of information, there's an immense amount of transformation you have to do. I think the cost, time savings, and personal satisfaction that Lacework provides is huge." And down the road, he hopes that the outcomes he's accomplished using Swimlane and Lacework together will be a draw when it's time to hire new talent. "We've seen a transformative and progressive improvement with our joint solution," states Lyborg.

Improving alert quality

With Lacework, Swimlane has observed a significant increase in the quality of alerts. "There are two factors to consider when it comes to alerts and signals," Lyborg explains. "If you don't tune your signals well, you're going to have tremendous alert fatigue. And if you do tune them and start missing things, then you'll stop trusting the tool. And trust is pretty much everything." Luckily, Lacework has earned Swimlane's trust. "Now, we can actually stack, rank, and prioritize things because we trust Lacework," says Lyborg. "The alerts we get are legitimate and actionable. When we get an alert through Lacework, we have the ability to see who did it, why the signal fired, what all the API calls are, and where it happened." Best of all, adds Lyborg, "The evidence is easy for pretty much anyone to understand."

Recently, one of Swimlane's clients got to see Lacework alerting for themselves during a visit to their headquarters. "We spun up their cloud environments and deployed Lacework, and it went into their infrastructure to make a few changes," remembers Lyborg. "We saw our client get an alert, and he had to authorize and validate that we were taking those actions. Justifying it in front of the customer made them believe in our security practice. Without Lacework, we probably would not have caught those activities unless we were digging into cloud trails all day." By surfacing only the most critical risks and providing context-rich visualizations, Lacework eliminates alert fatigue and allows Swimlane to take quick action.

> "
>
> We have patched several hundred CVEs on hosts, as well as in our container images. Some of them were critical, including Log4j. Having the ability to search for vulnerabilities and see our status was a really big win and saved us a tremendous amount of time. I'm not sure how we would have managed that over all our cloud infrastructure without Lacework."
>
> MICHAEL LYBORG, SENIOR VICE PRESIDENT
> OF GLOBAL SECURITY AND ENTERPRISE IT, SWIMLANE

Shifting left and saving time

To build upon the DevOps culture they already had in place, Swimlane has worked to shift left with the help of Lacework Infrastructure as Code (IaC) Security. "We improved our IaC practice to make sure that we're deploying and monitoring each account and sub-account," Lyborg notes. "At first, we were wary that this would take a lot of effort, but it was pretty much non-existent."

Similarly, Swimlane's vulnerability management was eating up a significant amount of time, especially with the container images. "Integrating the Lacework inline and proxy scanners with Swimlane has greatly increased visibility to all published container images while allowing us to properly prioritize the ticket submissions and manage risks," says Lyborg. This ability has also helped streamline the organization's cross-functional effort. "We can submit only what's fixable to the product and engineering teams, which has been extremely helpful for remediating quickly. It's been important for us to filter vulnerabilities and add exceptions," Lyborg explains.

For common vulnerabilities and exposures (CVEs), Lacework has been indispensable. "We have patched several hundred CVEs on hosts, as well as in our container images," Lyborg says. "Some of them were critical, including Log4j. Having the ability to search for vulnerabilities and see our status was a really big win and saved us a tremendous amount of time. I'm not sure how we would have managed that over all our cloud infrastructure without Lacework." Since then, when Lyborg finds other CVEs, he's been able to address them easily: "I just go to the console and search."

A valuable partnership

Swimlane initially chose to adopt Lacework because of the strong partnership potential that existed between the two companies. "The Lacework team executed one of the most seamless and professional sales engagements that I have experienced," Lyborg notes. "From consultation to close, their commitment to superior service and efficient delivery was patent. Lacework not only demonstrated technical proficiency, but also went to great lengths to personalize their communications with the Swimlane team."

Across the board, the collaboration remains strong. "We're seeing a huge improvement in our mean time to respond and remediate by integrating Lacework with Swimlane," Lyborg observes. As Swimlane continues to grow, scale, and further automate their SOC, they know Lacework will be right alongside them. "The faster remediation and response time wouldn't be possible without combining Swimlane and Lacework," Lyborg concludes. "This is a really valuable partnership for us."

Schedule a demo today

SWIMLANE

Swimlane is the leader in cloud-scale, low-code security automation. Swimlane unifies security operations in-and-beyond the SOC into a single system of record that helps overcome process and data fatigue, chronic staffing shortages, and quantifying business value. The Swimlane Turbine platform combines human and machine data into actionable intelligence for security leaders. Learn more at www.swimlane.com.