Case Study

Alamy

SECURITY > COMPLIANCE AND RISK MANAGEMENT

Developing Proactive Security Measures: Lessons from Lemonade

Insurance company Lemonade built a proactive cybersecurity strategy to ensure that it could do more than simply react to security incidents. Discover how the company did it.

Karen D. Schwartz | Apr 24, 2023

Lemonade is an insurance company that has a customer-focused approach, which is built largely on its own technology. The company handles everything from underwriting, pricing, and selling policies to handling and paying claims. Additionally, it distributes extra profits to charities chosen by customers.

Related: Why Security Logging Is Key to Ransomware Response

The company's goal is to provide customers with a fair, no-hassle experience. That includes qualifying for insurance in under two minutes and getting claims paid within three minutes. To do that, the Israeli-based company, which started in 2016, developed an AI-driven bot that assesses risk, helps customers select the right policies, and underwrites those policies. Under the hood is additional technology that Lemonade developed, including systems to help predict fraud, track extreme weather in specific regions, and calculate customer churn.

But when it came to cybersecurity, Lemonade CISO Jonathan Jaffe knew that it made better sense for the company to tap third-party security providers for tools rather than build its own. Lemonade implemented a variety of tools to protect sensitive data. While those tools work well, they were geared toward responding to cybersecurity incidents rather than proactively preventing attacks.

Staying Ahead of Cybersecurity Threats

Jaffe concluded that Lemonade could improve the proactive end of incident readiness and response. For example, while Lemonade uses a security information and event management (SIEM) service for log searching, investigating a potential incident meant sifting through disconnected logs – a time-consuming process.

Jaffe opted to contract with managed services providers (MSPs), signing Digital Forensics and Incident Response zero-dollar agreements with three different companies. That way, in the case of a breach, Lemonade could simply call one of those companies for help.

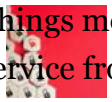
But that still didn't satisfy Jaffe, especially in terms of timely response. The problem, he determined, was that the response would require Lemonade to provide the MSP with credentials and logs, which would delay the response. "Doing that at the time of a breach is probably the worst time you could be doing that, but we didn't see any other way at the time," he said.

That's when lightning struck, in the form of a friendly talk with another CISO. While trading tips, the

0 COMMENTS

"He told me that they had an interesting approach where they ingest your logs ahead of time so they can start working immediately if you have to call on them," Jaffe said. "I'd never heard of a company that did that, but it made a lot of sense to me."

RECOMMENDED READING


Vulnerabilities
MAY 22, 2023


Breaches?
MAY 17, 2023


OpenAI CEO's AI Regulation Recommendations
MAY 16, 2023


Celebrating World Password Day: Best Practices for Secure Accounts
MAY 04, 2023

Things moved quickly from there. By the second half of 2021, Lemonade had signed up for the service from Mitiga, a New York-based cloud incident response vendor. Mitiga not only collects all logs in advance but performs automated, continuous cloud forensics investigations. If Lemonade was attacked, Mitiga could provide valuable information within 30 minutes, Jaffe said.

Ready or Not?

After they signed the agreement, the first thing Mitiga did was conduct a ransomware readiness assessment for Lemonade.

During the assessment, Mitiga and Lemonade did a tabletop exercise that focused on a hypothetical ransomware attack. "During something like that, you always learn that there are things you can be more prepared for, like making sure you have access to the right people or improving your communications plan," Jaffe said.

About
Advertise
Contact Us
Sitemap
Ad Choices
Privacy Policy
Terms of Service
Content Licensing/Reprints
Cookie Policy
Follow us:
Privacy Policy | Cookie Policy | Terms

What To Do After a Ranson

	Tip	Description
1	Do Not Pay the Ransom	Payment can embolden attackers and do
2	Contain the Damage	Shut down any affected systems and ren
3	Consider Your Obligations	Determine your legal requirements (e.g.
4	Perform a Thorough Forensic Analysis	Find out how the attack happened, whic
5	Do Not Attempt to Fix the Damage	Completely reimage affected systems an systems back online
6	Perform an Active Directory Audit	Verify that attackers have not tampered later exploited

The ransomware readiness exercise led Jaffe to create a Slack workspace that was separate from

Lemonade's regular workspace. That way, if there was an account takeover and the attackers gained access to the regular Slack workspace, colleagues can still work together in that separate workspace.

In addition, Mitiga performed active threat hunting, where it examines events occurring with other customers. With that information, Mitiga then looks for activities in Lemonade's environment. That kind of "crowdsourcing" can only be helpful, Jaffe noted.

Mitiga also set up a dashboard that scores how ready Lemonade is for a security incident at any given time. The dashboard can makes recommendations. For example, the dashboard might suggest that if Jaffe sends specific additional logs to Mitiga it would increase Lemonade's readiness score. The dashboard also enables Jaffe to prioritize his security team's actions related to readiness versus other projects.

Proactive Security Measures for Future Growth

With the relationship with Mitiga in place, Lemonade is now focused on replacing its SIEM with a Lemonade-developed security data lake. That work, currently underway, will let Lemonade consolidate all its logs into one location and write its own active threat detection rules.

"It's similar to what we do now with a SIEM, but the structure of the data isn't as rigid as it is with Splunk or the ELK Stack [an Elastic offering that allows users to collect and analyze logs]," Jaffe explained.

Over time, Jaffe expects the security data lake will help address other security issues within the business that aren't even in his domain – things like internal and external fraud.

"When you have a data lake where you can bring in more and more data, you can start to see that there might be correlations between different datasets," he said. "The idea is that we can build better detection by having more data than if we limit it to CrowdStrike and load-balancer logs."

As Lemonade prepares for more company growth – it already has revenues of more than half a billion dollars – Jaffe said more innovation is in the cards.

In addition to hiring its first data scientist later this year, the company has two major projects queued up. The first project is to enhance trust in employee devices. Although Lemonade already has a device program and has moved from multifactor to passwordless authentication, Jaffe says more can be done.

The second project is to enhance API security. "The next wave of attacks outside of supply chain attacks will probably be more and more on API endpoints, especially with the possibility of using

generative AI where people can develop attacks easily," Jaffe said. "I'd like for us to be ahead of the curve there."

About the author

Karen D. Schwartz is a technology and business writer with more than 20 years of experience. She has written on a broad range of technology topics for publications including CIO, InformationWeek, GCN, FCW, FedTech, BizTech, eWeek and Government Executive.