Lennar Corp. Moves From XSOAR to Torq, Freeing SOC Analysts From Tedious, Manual Work

Nationwide homebuilder significantly improves phishing remediation time from hours to minutes

About Lennar Corporation

Lennar Corporation, founded in 1954, is one of the nation's leading builders of quality homes for all generations. Lennar builds affordable, move-up, and active adult homes primarily under the Lennar brand name. Lennar's Financial Services segment provides mortgage financing, title, and closing services primarily for buyers of Lennar's homes and, through LMF Commercial, originates mortgage loans secured primarily by commercial real estate properties throughout the United States. Lennar's Multifamily segment is a nationwide developer of high-quality multifamily rental properties. LENX drives Lennar's technology, innovation, and strategic investments. For more information about Lennar, please visit www.lennar.com.

Key Metrics

- Signed with Torq: 2023
- SOC Team Published Workflows: 5
- SOC Team Active Users: 8
- Time to Resolve Phishing: From Hours to Minutes

The Problem

Lennar's security operations center (SOC) monitors alerts for three different business units within the nationwide homebuilder and is responsible for identifying malicious logins, rooting out malware, and remediating phishing attempts.

The eight-analyst SOC team was spending too much time on phishing remediations, with time to resolve taking hours and requiring significant manual work.

Lennar needed an automation solution that offered the flexibility and functionality to reduce phishing remediation times while also offering extensibility that enabled them to connect to any tool in their security stack.

Their previous solution, XSOAR, could not do any of that.

> "We were in need of an automation tool and we found a real fit with Torq due to its flexibility and functionality to connect to any tool"
>
> Daniel Gross, Senior Operations Analyst at Lennar

The Solution

Gross' team discovered Torq and immediately noticed several key advantages over their previous solution.

Resolving Phishing Incidents Faster

Before Torq hyperautomation, a phishing incident would take hours to resolve. Now it takes just minutes, marking what Gross calls "a significant drop in time to resolve those incidents."

> "The phishing remediations that we've done with Torq have significantly reduced the amount of time put into phishing remediations and allowed us to further refine our other tools and alerts"
>
> Daniel Gross, Senior Operations Analyst at Lennar

Eliminating Manual Work

Lennar also eliminated much of the time-consuming manual work required to resolve phishing incidents.

"Before we had Torq, we would do a lot of manual phishing remediation, which was a big time-taker," Gross says. "We would spend hours and hours.

"We were able to really cut down a lot of manual work," he adds, noting that the team can now apply that time saved to tune other tools. "With the time saved by the Torq workflows, we can measure how much overhead we would need."

The time saved by not having to do manual work gives the Lennar SOC team the freedom to do more threat hunting and research, which are critical to their roles.

Gross adds that Torq's no-code functionality and AI support make the platform "plug and play" incredibly easy to use for all skill levels.

Introducing Simplicity With No-Code, AI

"The no-code solution – the ease of use – allows us to collaborate and also to build ourselves workflows," Gross says. "Whereas the functionality in the other tools wasn't as easy to use."

And adding AI functionality on top of it with a prompt-based step builder makes it even easier.

"With the no-code solution and a feature like the AI wizard, it allows someone who doesn't know a JQ, for example, to easily say in human-readable context, 'I would like to do this,' and it will build you out a script or something you can easily use," he says.

The ease of use of Torq surpasses the Lennar team's expectations, and Gross said it is a major differentiator compared to XSOAR.

"When we do it with the other tool, it's not as easy and fast as with Torq," he says. "We would do a lot of manual Excel work where we have to build a formula and export it to excel. Where in Torq, you just build in a variable or a step where you can define variables, and it allows you to do less exporting and manual work and keep it really in the tool."

The Future

Going forward, Lennar has started implementing Torq into its asset management, which has already introduced significant time savings. Gross said the Lennar SOC team hopes to put more workflows into production very soon.

"We're using Torq now to better understand our asset inventory," Gross says. "We're able to pull from all of our tools and we're able to do within the workflow some comparisons and see from each tool how many assets we really have. It really reduces the amount of time. To do that manually, it takes us a few hours. These workflows cut it down to minutes."

> ## "To do that manually, it takes us a few hours. These workflows cut it down to minutes."
>
> Daniel Gross, Senior Operations Analyst at Lennar

About Torq

Torq is transforming cybersecurity with its pioneering enterprise-grade, AI-driven hyperautomation platform. By connecting the entire security infrastructure stack, Torq makes autonomous security operations a reality. It empowers organizations to instantly and precisely remediate security events, and orchestrate complex security processes at scale. Fortune 500 enterprises, including the world's biggest financial, technology, consumer packaged goods, fashion, hospitality, and sports apparel companies are experiencing extraordinary outcomes with Torq.

Get a Demo