How Torq HyperSOC Eased Alert Fatigue For Check Point

Alert fatigue is real, and it can cause big problems in the SOC. Learn how generative AI improved security outcomes and reduced analysts' frustration for Check Point.

About Check Point

Check Point is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times. The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network, and Check Point Infinity Core Services for collaborative security operations and services.

The Problem: Too Many Alerts and Too Few SOC Analysts

Cybersecurity executive Jonathan Fischbein had a problem to which his peers can likely relate: too many security alerts and too few security operations center analysts.

"We have a tight budget," said Fischbein, CISO, Check Point. "I'd say that, in the SOC, we were lacking between 30% and 40% manpower."

Without enough staff to respond to the constant flood of security alerts coming from the organization's SIEM platform, conditions were ripe for disaster. "If you have an alert that you're not addressing, that alert might become an incident," Fischbein said. "And that is something that, as the CISO, I don't want."

The Solution: Unseat Legacy SOAR With Torq HyperSOC

With the aim of reducing his team's alert fatigue and improving Check Point's security posture, Fischbein began exploring automation platforms. Feedback from fellow CISOs and CIOs led him to bypass legacy security orchestration, automation and response (SOAR) products in favor of a hyperautomation platform from startup Torq.

"We really liked the fact that the UI is graphical and that there are a lot of workflow automation templates," Fischbein said, adding that the platform's design centers SOC analysts' experience to make their jobs easier.

Check Point initiated a proof of concept. Within a few days of the trial's inception, Fischbein said, Torq had deployed more than two dozen AI-driven playbooks, automating responses to some of the organization's most repetitive security alerts.

Importantly, Torq HyperSOC also integrated easily with Check Point's existing infrastructure and security stack, ingesting and analyzing data from a variety of systems and tools. "It fit like a glove," Fischbein said.

He was sold.

> "With Torq HyperSOC, we can react automatically to problems before they become security incidents."
>
> Jonathan Fischbein CISO, Check Point

Torq AI Goes to Work in the SOC

Today, Torq's technology -- now known as HyperSOC -- investigates, triages and remediates many of Check Point's internal security alerts without any human intervention. If an alert meets certain parameters based on organizational security policies, the platform autonomously takes relevant predefined steps, such as initiating an MFA challenge or locking out a suspicious user.

"We can react automatically to problems before they become security incidents," Fischbein said.

When events are potentially critical or complex, HyperSOC flags them for analyst oversight or intervention and offers suggestions for next steps.

According to Torq, organizations can also train the generative AI-driven SOC platform to consider contextual factors in its decision-making -- for example, requiring confirmation from a human operator before locking the CEO's account.

Natural Language Processing Speaks Up

Fischbein compared Torq's HyperSOC to a Swiss Army knife in that it helps address diverse security events of varying severity.

Some of that flexibility is thanks to the technology's large language model capabilities, which enable it to ingest material written in natural language -- ranging from proprietary in-house playbooks to documentation of industry frameworks, such as Mitre ATT&CK -- and cross-reference it during event triage, investigation and response efforts.

In cases requiring human intervention, the platform also uses natural language to summarize its own workflows, present relevant data and offer next-step recommendations. This helps human analysts make more efficient and informed decisions, minimizing the time and effort they spend on tedious and manual investigative tasks during active incidents.

Torq HyperSOC Makes a Major Difference

According to Fischbein, Torq's AI-driven HyperSOC has successfully increased efficiency and reduced alert fatigue among Check Point's security analysts.

> "It's a cat-and-mouse game," Fischbein said.
> "And, with Torq, we can catch the mouse more easily."
>
> Jonathan Fischbein CISO, Check Point

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