Query.ai

Case Study

Hogan Lovells Combats Cybersecurity Investigation Burnout and Boosts High-Confidence Outcomes

Overview

Hogan Lovells is a global top 10 legal services provider that serves clients in more than 45 countries. With more than 7,000 employees and a large security operations infrastructure to manage, Hogan Lovells chose Query. AI to streamline what was an exhausting cybersecurity investigations process that required logging into 20 different tools.

Situation

Joe Oney, security operations manager for Hogan Lovells, has a strong commitment to continually advancing the firm's cybersecurity processes. Looking at his team's investigation efforts, he identified several opportunities for improvement. With the firm's broad and varied security infrastructure, a single incident response required individual analysis across a minimum of five tools. It could take up to an hour to reach an answer to an inquiry such as "what other system has been to this domain?" across multiple technologies.

"Our team had to use 20 different syntaxes to look at 20 different systems, which meant 20 possible mistakes. Even with a highly skilled team, there's still a chance of a typo, which then muddies the investigation analysis. We wanted to reduce the clicks and manual analysis required to increase the accuracy for our incident response," said Oney.

Hogan Lovells

At a glance

Industry

Global law firm

Environment

45+ offices across the globe

Challenges

- Time consuming investigations, requiring individual analysis across 20 tools.
- Complex search using each tools' syntax, which opened up opportunities for typos.
- Low confidence in the accuracy of investigation outcomes.

Solution

Query.AI security investigations platform

Results

- Eliminated time consuming management of SOAR solution.
- Accelerated alert triage and investigations with a platform that is querying desired systems with a single question.
- Eliminated search "clicks" across individual tools and reduced opportunities for errors.
- Increased accuracy and confidence in investigation outcomes.

To improve the incident response process, Hogan Lovells initially adopted SOAR technology. “SOAR promised automation and enrichment, but we never found success. The process of managing the API integrations alone was a time sink. Building each enrichment playbook required a pre-cognitive understanding of what data an analyst would need. Investigations are dynamic and that just wasn’t realistic,” Oney stated. “Adding to that, each playbook required a dedicated software engineering effort.

Solution

In pursuit of a streamlined approach for security investigations, Hogan Lovells engaged Critical Start, a Query.AI partner. Critical Start recommended the Query.AI platform as a lightweight solution that didn’t require ripping and replacing any existing technologies, centralizing the firm’s data, or assigning a dedicated engineer for management.

According to Jay McKinzie, director of sales for Critical Start, “In meeting with Hogan Lovells and aligning on their security operations goals, we saw the high value Query.AI would deliver by enabling the team to gain speed and efficiency in their security investigations.”

Providing a control plane that overlays all of an organization’s data silos, Query.AI accesses and analyzes data in real-time from across systems, directly where it lives. This eliminates the need to centralize data to gain centralized access and removes the time-consuming process of investigating from one security tool to the next. As a result, companies are empowered to manage security investigations efficiently and swiftly.

“Query.AI was really attractive for us as a solution because it didn’t require the effort to centralize or orchestrate our data like a SIEM or SOAR. The platform is laser-focused on helping our security team reduce the clicks required to answer investigation questions quickly and accurately, out of the box. It also automates historically manual and time-consuming security analyst processes,” said Oney.

Results

Successful integrations

To put the Query.AI platform through the paces, Oney started out with three of the firm’s toughest integrations: Expel, Microsoft Defender ATP, and Guardicore. Hogan Lovells engages with Expel for tier-1 analyst support services, so this integration was important to ensure smooth security processes across team members.

“Integrations that we hadn’t gotten to work with our former SOAR solution after six months of overhead and development effort, Query.AI was able to knock out in a month, which was a clear win for us. It validated that Query.AI could support and keep up with our APIs to meet our continuously evolving enterprise security requirements,” said Oney.

> “The Query.AI platform eliminates the multiple searches across individual tools and lets us quickly gain the context to determine which alerts are high-fidelity by letting us easily assess what each system says about it. Our team now has greater accuracy with less clicks and time required to reach an outcome. By eliminating the search pivots across tools, we now have confidence in our incident response decisions and have improved our security posture.”
>
> **Joe Oney**
> Security Operations Manager
> Hogan Lovells

Oney continued, "With the Query.AI platform managing integrations, I know that the APIs are going to work if we're ever in a time pressure situation to conduct incident response. My team is now empowered to do the required scoping as quickly as possible, and the platform provides a good idea of the data and what's happening."

Fast, efficient investigations

One of the biggest competencies that the security team has gained with the Query.AI platform is single place to search for handling triage and investigations across the security tools. Now, with a single question, the team gets a collective answer for all of the relevant systems, which reduces analyst burnout chasing low-fidelity alerts.

"The Query.AI platform eliminates the multiple searches across individual tools and lets us quickly gain the context to determine which alerts are high-fidelity by letting us easily assess what each system says about it. Our team now has greater accuracy with less clicks and time required to reach an outcome," said Oney. "By eliminating the search pivots across tools, we now have confidence in our incident response decisions and have improved our security posture."

Looking ahead

Streamlining email incident response

Planning ahead, Oney has big plans as the team progresses on their journey with Query.AI. For example, streamlining email investigations is at the top of the list.

The firm's email routing scheme is complex with multiple email security systems and a ticketing system that receives notices from different regional offices. Handling incident response for a phishing email can require searching across multiple email systems to see each triggered policy across the tools to determine if the email should be treated as malicious or not. Once the email systems are integrated with the Query.AI platform, a query on a suspicious email will provide the team with the detection details from all of the email tools in a single view, making it fast and easy to assess an email's risk level.

Getting started with Query.AI is fast and easy

1

Set Up a Meeting

Meet with us so we can get to know you and understand where you want to go.

2

Configure in Minutes

Connect our unified browser interface to your security systems via APIs.

3

See Results

Accelerate cybersecurity investigations and efficiently respond to threats.

GET STARTED

https://info.query.ai/contact-us