Computer Services

Business challenge

After experiencing downtime with its existing SIEM tool, SecurityHQ needed a more reliable security platform.

Transformation

After sustained growth, IBM Business Partner SecurityHQ needed to update the security information and event management (SIEM) platform that backed its managed detection response services. Relying on IBM Security™ software delivered under an IBM Embedded Solution Agreement (ESA), the firm can now readily scale its monitoring to match user demand.

Results

30% – 40% cheaper

than the previous SIEM platform

Reduces downtime

improving overall system availability and reliability

Supports >40 independent networks

through a single contract

SecurityHQ

Coordinated insight yields a coordinated response

IBM Business Partner SecurityHQ (external link) prides itself on its global reputation as an advanced managed security service provider, delivering engineering-led solutions that combine security experts with cutting-edge technology and processes. Originally founded in 2003 as Si Consult Ltd., the business is headquartered in London, UK with additional offices in the Middle East, Americas, India and Australia.

> "Once you model the cost of the ESA, it's actually very well priced. Over the first three years, I've saved 30% – 40% on my cost of SIEM."
>
> —Feras Tappuni, Founder and Chief Executive Officer, IBM Business Partner SecurityHQ

Share this

Risk is on the rise

Data has become the currency of the modern age, and keeping it safe is only growing more challenging. Hospitals held hostage by ransomware, banks robbed of personal customer data, small business sites hacked and loaded with malware—there seems to be an ever-shrinking window between each new headline recounting the latest cyberattack.

These assaults are only growing more frequent and more bold.

"I don't think people realize what we've been seeing in the last year," notes Feras Tappuni, Founder and Chief Executive Officer at IBM Business Partner SecurityHQ, a managed security services provider. "The number of attacks—of incidents—that we've observed from our offices around the world is up. The alarm count has gone through the roof."

And alongside this spike in cyberattacks, SecurityHQ had witnessed a similar spike in its overall business, adding new customers and expanding the scope of existing contracts to help offset these increased threats. But this rapid, sustained growth was beginning to cause inefficiencies with some of the key management tools that the company used to support customers.

"We were having significant problems with the SIEM software we were using," recalls Tappuni. "It just couldn't handle the capacity we were seeing. When you're running a 24x7 security operation with service level agreements of 15 minutes, the idea of having any downtime is scary enough. But when you have hours of downtime in a single week, you're having major issues. You cannot ignore that."

> ***"[W]ith the ESA, we had something that was tailored for us. That gave us the right commercial model to rapidly scale up our business."***
>
> —Feras Tappuni, Founder and Chief Executive Officer, IBM Business Partner SecurityHQ

Trying to determine what measures SecurityHQ should take going forward, Tappuni pursued an unconventional approach. He talked to his competitors.

"We're all engineers," explains Tappuni, "so they were more than willing to discuss and troubleshoot the mechanics of the problem. I spoke to the head of infrastructure of a service provider out of the US who had gone through the same issues that we had. He used some of the exact phrases to describe their past issues as I had been using to describe our problem."

Tappuni continues the story: "I asked him what they had done, and he told me that they moved to IBM. The migration had taken some work, but when it was finished, he was able to sleep at night. That's what I wanted too—I wanted to be able to sleep at night."

One contract, one console

To better avoid potential service interruptions, SecurityHQ standardized its managed detection and response operations on IBM® QRadar® SIEM software. Now, when customers send in security logs for processing, SecurityHQ analysts—from within the IBM tool—can review any related events, report on what happened and recommend next steps. And the business can extend this insight to users of its SecurityHQ Response App, which delivers mobile access to the partner's security platform and offers the ability to respond quickly to an incident, even when not in the office.

"QRadar is the cornerstone of our solution," notes Tappuni. "When a user logs in, they're now seeing all the tickets, all the reports generated regarding the infrastructure. All of them correlated correctly. All of them given an alarm sequence and the name of the analyst that worked on it." And with this insight, analysts can then properly prioritize and manage responses.

> ***"The support I'm getting from IBM is on a whole other level. It's been a fantastic relationship."***
>
> —Feras Tappuni, Founder and Chief Executive Officer, IBM Business Partner SecurityHQ

Alongside the QRadar technology, SecurityHQ also uses IBM Security Orchestration, Automation and Response (SOAR), previously IBM Security Resilient®, software. The tool automates alarm management and response efforts. As Tappuni explains, "Because of our growth, we're trying to focus in on the quality alarms that we really need to investigate and section off the noise."

And to simplify the integration and delivery of the IBM Security software within its management platform, SecurityHQ signed an IBM Embedded Solution Agreement (ESA).

"Our previous SIEM contract model was very limiting," Tappuni adds. "If we overused it, there were additional costs. It was very difficult to narrow down what our spend should be. I'd dedicate hours trying to calculate how much we would need for the upcoming year, and I would always be off by 20% – 30%."

He continues: "The challenge is we don't have one client and one network. We're monitoring 40 to 60 networks, and they're constantly changing. But with the ESA, we had something that was tailored for us. That gave us the right commercial model to rapidly scale up our business."

Lower cost, greater reliability

With the new IBM software in place, SecurityHQ quickly resolved the availability challenges that the business had been facing. The flexible, scalable IBM QRadar platform can readily accommodate the company's shifting workloads and support the high volume of messages and reports that SecurityHQ works with for its day-to-day tasks.

In addition, the IBM solution helped to rein in related spending. "Once you model the cost of the ESA, it's actually very well priced," notes Tappuni. "Over the first three years, I've saved 30% – 40% on my cost of SIEM. And because of the contract structure, it will continue to go down going forward."

Further, the IBM Security brand helps to draw market interest and promote further sales. "Our clients like to know what the products we use are," notes Tappuni, "and when you tell them that you're an IBM partner, that gives you a huge edge. There are few providers out there where you have such a depth of security products."

He continues, adding: "The support I'm getting from IBM is on a whole other level. It's been a fantastic relationship. They actually talked us out of spending more money—they said you don't need to buy more yet, just wait and get it when you need it. It's rare that you find a partner so focused on making sure you succeed."

Solution components

- IBM® QRadar® SIEM
- IBM Security Orchestration, Automation and Response

Take the next step

To learn more about the IBM solutions featured in this story, please contact your IBM representative or IBM Business Partner.

To explore how to use IBM technology to build a solution for your clients, please visit: IBM Build Partner Program

To explore if an IBM Embedded Solution Agreement is right for your organization, please visit: ESA

To learn more about its security monitoring solutions and what SecurityHQ can do for you, please visit: SecurityHQ