CASE STUDY

Encompass Health

Innovative SOC Strategy Helps Tackle the Cybersecurity Skills Shortage

// BEYOND SIEM

JASK

CASE STUDY

Innovative SOC Strategy Helps Tackle the Cybersecurity Skills Shortage

> *"Organizations rely on cybersecurity professionals to defend against skilled cyber adversaries that are employing increasingly sophisticated attacks. Unfortunately, many report that despite an increased investment in cybersecurity defenses and oversight, they are still fighting the fight with suboptimal resources."*
>
> **JON OLTSIK**
> Senior Principal Analyst

About Encompass Health

Encompass Health is a leading provider of facility-based and home-based patient care with a network of inpatient rehabilitation hospitals, home health agencies and hospice agencies. Based in Birmingham, Alabama, it has a national footprint that spans 128 hospitals and 268 home health and hospice locations across 36 states and Puerto Rico.

The Challenge

With multiple locations, a continually rising number of devices that require connectivity, and the ongoing need for operating efficiency, the Encompass Health Chief Security Officer (CSO) is continually challenged by the current cybersecurity skills shortage -- not only when it comes to finding, but also retaining the talent they need to defend the organization from modern cyber attacks. Encompass Health is not alone. In fact, a recent report published by Enterprise Strategy Group (ESG) and the Information Systems Security Association International (ISSA)1 highlighted that 45% of surveyed organizations reported having a problematic shortage of cybersecurity skills.

"Organizations rely on cybersecurity professionals to defend against skilled cyber adversaries that are employing increasingly sophisticated attacks," said Jon Oltsik, Senior Principal Analyst and ESG Fellow. "Unfortunately, many report that despite an increased investment in cybersecurity defenses and oversight, they are still fighting the fight with suboptimal resources."

While this is a known global challenge, Encompass Health Chief Security Officer Mitch Thomas explained that his organization faces a challenge that is unique to companies operating in regions with a smaller talent pool.

"In Birmingham, it's even more difficult to find people with the skills needed to read the cyber tea leaves, so our focus then must turn to training and retention. Once we have fully trained our analysts, they become highly sought after, and it can become difficult to retain talent from both a resource and cost perspective."

MITCH THOMAS
Encompass Health Chief Security Officer

The ongoing training requirements and skills shortage makes maintaining a 24x7 security operations center (SOC) a constant struggle. Currently, Encompass Health operates a hybrid SOC in which a small, internal team is dedicated to analyzing events and identifying threats, while a managed security service provider (MSSP) focuses on critical assets. The tier 1 and tier 2 analysts are tasked with collecting logs and performing traditional SIEM analysis, relying on two managers to support them with tier 3 support.

For Thomas, with such a small team, it's difficult to stay focused on 24x7 response from a tactical perspective. "Threats don't take vacations and they don't stay within business hours," he added. "So, we have to function around the clock at our highest efficiency at all times."

All of this is quite costly. On top of cybersecurity staff salaries and MSSP outsourcing costs, keeping the security stack up to date with all available point products is a huge challenge. It can be difficult to maintain executive support for such costly operations that don't offer any revenue growth to the company.

A Military Mind for Strategy and Tactics

To help address these challenges, Encompass Health implemented the JASK Autonomous Security Operations Center (ASOC) platform. Thomas was impressed by the technology's innovative artificial intelligence (AI) and machine learning capabilities that automate many SOC functions, helping to take over the highly repetitive and time-consuming tasks often handled by tier 1 security analysts. In its traditional SOC structure, the team collects system logs and network traffic, then sends it to a traditional SIEM where analysts respond to thousands of alerts received throughout the course of a regular day.

"As a former officer of the U.S. Cyber Command unit, I'm a traditional military guy. I apply an old military fighter pilot tactical approach to processing threats called the OODA Loop, which focuses on the continuous loop of observation, orientation, decision and action. In our SOC, we work to close that loop on each incident. The better we are at moving through the loop, the quicker our response. It's a tactical methodology that truly works but is a challenge to sustain."

The automation delivered through the JASK ASOC platform helps sustain this process in a way that a human can't.

Closing the OODA Loop

The JASK ASOC platform optimizes the Encompass Health team's SOC efforts through automated assessment of the majority of daily incidents, freeing up analysts to focus on higher-priority threats.

The technology also offers full attack profiles that provide the necessary context for analysts to move through the OODA Loop decision process more quickly, allowing them to respond within seconds as opposed to minutes or hours.

As a result of automating certain SOC functions, tier 1 analysts can be used for more critical tasks. Thomas says, "I'm able to pay the members on my security team a slightly higher salary, making it easier to keep existing team members and attract new talent in a very competitive area. They can now manage things from a higher level and help us analyze our data and provide predictive analysis as opposed to the traditional defense response."

Previously, the Encompass Health SOC team didn't have the time or resources to establish a good threat hunting process in their environment. They were too busy chasing the "blinking lights" of incidents and events.

"JASK's automation process and machine learning capabilities have helped us implement a threat hunting process that often doesn't even need a human involved. Based on profiles that have been established by industry leaders on the JASK team -- guys who really understand how to analyze a threat -- threat hunting is applied in our environment through AI, then our small team can jump in more quickly with a much more intelligent response."

"JASK's automation process and machine learning capabilities have helped us implement a threat hunting process that often doesn't even need a human involved. Based on profiles that have been established by industry leaders on the JASK team -- guys who really understand how to analyze a threat -- threat hunting is applied in our environment through AI, then our small team can jump in more quickly with a much more intelligent response."

MITCH THOMAS
Encompass Health Chief Security Officer