



Industry: Healthcare

Enabled Health Information Management Consulting Service Provider from The USA through our SIEM, SOC and VAPT services

► Background

Coming from the healthcare sector, our client rendered comprehensive health information management consulting services to hospitals, health systems, physician groups, and clinics. They specialized in rendering compliance audits, backlog coding, and interim management both remotely and on-site from their headquarters in California. They assisted their clients in staying compliant with the regulatory environment for healthcare information management that was constantly subjected to change. Because they have been operating since 1994, they had developed a reputation with their customers nationally which they couldn't risk tarnishing as a result of any cyber attack.

► Objectives

- ✓ Identify the security risks in the current posture and establish a framework for security.
- ✓ Protection of all the health related personal data of customers.
- ✓ Implement measures to achieve all GRC goals.
- ✓ Setup a dedicated team for cybersecurity.
- ✓ Prepare for cyber incidents like data breaches.
- ✓ Implement the security controls to meet all the compliance goals.

► Challenges

Since they rendered information management consulting services, it was critical for them to have a cybersecurity posture that takes care of the most emerging cyber threats. Protection of sensitive information from theft, manipulation, and loss was their top priority. However, they did not possess the skills or expertise to tackle their challenges. The following are the challenges they faced:

- There was no team to identify their IT infrastructure's vulnerabilities and security flaws.
- They did not have any solution fully managed by experts that served both of their goals - compliance, and cybersecurity.
- No 24x7 team or solution that rendered round-the-clock security.
- There was no visibility despite having security solutions such as firewall, endpoint security etc.
- They had to manage multiple vendors for handling multiple aspects of security.
- Their information was vulnerable to cyber criminals who were looking to exploit it via ransomware attacks.
- No reports that could be used to make decisions.
- There was no existent incident response plan.

► Solutions

Our client was looking for a dedicated security team that rendered round-the-clock security, solving all of the above challenges and eliminating their reliance on multiple vendors for security. SharkStriker helped them solve their challenges by rendering holistic solutions and services that single-handedly catered to each challenge. The following are the solutions we offered them:



- Before we started our execution, we discussed and understood the client's security requirements.
- Once we framed the scope, we engaged in rigorous VAPT testing of their IT infrastructure to identify and remediate security vulnerabilities.
- Post VAPT, we implemented security measures to remediate vulnerabilities.
- We tailored our SIEM specifically to our client's challenges.
- Our SIEM rendered round-the-clock security monitoring. Through its integrated SOAR, it responded to threats automatically with the help of AI and ML.

- It rendered centralized visibility of all the ongoing security events through easy-to-use live dashboards.
- It provided a comprehensive understanding of the TTP (Tactics Techniques and Procedures) deployed by cybercriminals.
- The SOC team deployed some of the top-notch analysis techniques in place and assisted in triaging threats that improved the precision of our client's response to threats.
- It generated actionable compliance-friendly reports that could be used to make valuable decisions and achieve compliance requirements.

► Outcome

SharkStriker's holistic services and SIEM helped the client in achieving the following outcomes:

- They met all the security requirements through a single company.
- As a result of expert-driven VAPT, SOC, and SIEM, their cybersecurity posture improved significantly
- Our client now has 360-degree visibility of all of their security events
- They were able to achieve compliance easily with reports generated by SIEM
- A dedicated cybersecurity team that focused on all specific security needs
- Round-the-clock security through the SOC team and continuous monitoring with SIEM
- All of their sensitive healthcare-related and company specific information assets were safeguarded, without any loss of fidelity
- They were better prepared for the event of a breach through comprehensive incident response planning
- Their productivity improved as a result of enhanced security from cyber attacks
- There was a noticeable improvement in their reputation with all the customers and investors due to increased cybersecurity posture

Achieve cybersecurity
and compliance goals
with 360 degree
visibility with our SIEM-
as-a-service

GET STARTED





SharkStriker



1990 N California Blvd Suite 20,
Walnut Creek, CA 94596, USA



+1 925 5321900



sales@sharkstriker.com



www.sharkstriker.com



[/company/sharkstriker](https://www.linkedin.com/company/sharkstriker)



[/thesharkstriker](https://www.facebook.com/thesharkstriker)



[/TheSharkStriker](https://twitter.com/TheSharkStriker)



[/thesharkstriker](https://www.youtube.com/thesharkstriker)