

Assisted a leading brokerage firm achieve its GRC goals with SIEM

Outcomes Delivered

- ✓ 40+ compliance gaps identified and addressed
- ✓ Reduced events by 60% through customized workbooks
- ✓ Time to value reduced from 44 days to 3 hrs.
- ✓ 30-40 alerts tagged per day from automated investigations

SharkStriker Solutions

Managed SIEM & SOC Services

USE CASES

1. 24x7 SIEM management and monitoring
2. Adherence to security guidelines by NIST

Challenge

To balance between business operations and compliance while ensuring complete visibility of security operations.

As a growing brokerage firm, our client had to ensure that it adhered to the recommended information security processes, procedures, policies, controls, and log management guidelines recommended by NIST and those specific to SIEM. It had Elastic Security SIEM in place to address the security needs of the organization.

However, the organization was witnessing a high daily volume of alerts without having color or context on alerts. With the growing customer base across the states, they were seeking to reduce the time to value. Due to a lack of visibility and struggle with making quick and precise context-based decisions, security operations consumed a huge chunk of business time. They were looking for an organization that helped them identify the compliance gaps specific to SIEM and gain context on alerts, decentralized governance, and control over cybersecurity across multiple members. They were looking for a vendor that could help them address their governance, risk, and compliance goals.

- ☑ Achieve governance, risk, and compliance goals.
- ☑ Gain more context on alerts and meaningful insights.

Brokerage and M&A services

Our client is an award-winning firm from Denver, Colorado that offers brokerage and mergers & acquisition services. It has helped businesses with gaining maximum value from selling their business through their expertise in brokerage, corporate accounting, middle-market investment banking and small business ownership.

Its team is comprised of former business owners, investment bankers and public accountants with M&A advisors that are almost in every major metro area in the US.

All their clients have a valuation of 3M to 100M. They have rendered expertise to businesses from more than twenty industries including manufacturing, technology, services, property management, consumer products, healthcare, and other industries.

Solution

SharkStriker assisted in addressing all the cybersecurity and compliance gaps through seamless management and monitoring of their SIEM solution, helping the firm make most of their SIEM solution. SharkStriker's 24x7 SOC team managed and monitored their SIEM solution, with the industry best practices and NIST-recommended guidelines, helping the firm with boost of reputation and trust through round the clock security of their most precious information assets.

"Doing business with the giants also means ensuring that all the client specific confidential data secured as per the NIST and other information security standards. Through SharkStriker, we were able to effectively achieve our compliance goals with our SIEM solution. They have helped us to bring and enabled us to focus on our improving our client experience without having to worry about breaches or non-compliance"

- Founder, CEO

80% Reduction in alert noise

5000 Hrs saved on service delivery.

Results

Decentralized control over cybersecurity with round the clock support.

Through SharkStriker's human-led tech-driven security platform STRIEGO, the organization gained seamless visibility into security operations with meaningful insights on posture. It helped experts across different levels with decentralized control and visibility of the security posture and has allowed the security team to focus on what is critical.

Periodical security posture assessments helped them understand their security posture across timelines. With a dedicated SOC, the organization can reach out to the experts for any troubleshooting or technical support.

"It was always a challenge figuring out cybersecurity with limited visibility, lack of insights, and limited control. There was a persistent challenge of ease of control, visibility, and inequity across multiple levels when it comes to cybersecurity. SharkStriker helped solve all that with STRIEGO, backed by their 24x7 experts. It helped us work with ease with the much-needed visibility of our security operations."

- Founder, CEO

Adherence to compliance requirements.

As a brokerage and M&A services provider that had clients worth millions, safeguarding the trust of its stakeholders and clients while being compliant was one of the top priorities. The firm sought to secure all sensitive information of clients with NIST-recommended information security best practices. However, with a limited team, it was challenging to achieve that goal. SharkStriker offered the round-the-clock dedicated expertise in cybersecurity and compliance that helped the firm identify and address the gaps and implement the SIEM best practices recommended in the NIST guidelines.

SharkStriker has helped us identify and address the compliance gaps in the current posture. The team has managed and monitored our SIEM with best practices that helped us derive ROI from it through effective design and provisioning, use case management, and risk and compliance management. Through the automated compliance features offered by their security platform STRIEGO we were able to ensure compliance in a regulatory environment that is constantly subject to change.

- Founder, CEO

Results

Enhanced focus on client value delivery.

The firm was unable to gain the required visibility on the threats or gather evidence in the form of telemetry across the posture despite having a SIEM solution onboard. It was facing the challenge of being overwhelmed by alerts that mostly comprised of false positives.

SharkStriker helped solve this by offering experts that managed and monitor their SIEM as per the NIST recommended guidelines. With effective log management, customization of playbooks and automated compliance features like periodical CIS-based posture assessment, the firm could focus on improving their service value without having to worry about cyber threats and non-compliance.

Thanks to SharkStriker, we can focus on improving service value while enjoying a reduced time to deliver because of 24x7 security against known and unknown threats. We have witnessed a significant decrease in mean time spent on investigating security alerts from SIEM with more context on alerts with specific information such as history, frequency and severity, helping us improve precision.

- Founder, CEO

50% reduction in time spent to investigate.

90% decrease in the overall time spent to respond to security alerts.

**DISCOVER
OTHER CASES BY US
FROM A SPECIFIC
INDUSTRY**

[CLICK HERE TO READ](#)

