

# Assisted a bookkeeping & tax Services firm in turbocharging its SIEM

## Outcomes Delivered

---

- ✓ Reduced false positives by 90%
- ✓ Cut down time to detect by half - 30 minutes
- ✓ Compliance gaps addressed - 100+
- ✓ Sensitive assets secured – 40+

## SharkStriker Solutions

---

Managed SIEM & SOC Services

## USE CASES

---

24x7 SIEM management and monitoring  
Compliance achievement

---

## Challenge

Tackling cybersecurity with the growing threat of non-compliance was the biggest challenge.

Our client had a SIEM in place, however, the organization faced challenges from multiple fronts.

Their SIEM was getting more and more expensive to maintain overflowing with alerts that comprised a high number of false positives. It was unable to keep up with the growing assets. Due to a limited team comprising, mostly IT experts with general expertise in cybersecurity, the organization was finding it challenging to identify gaps in SIEM and address the challenge of missing critical alerts.

They couldn't find what was amiss in the SIEM that prevented it from offering them the visibility of their complete cybersecurity posture. The organization wanted a company that could help them secure their most precious assets while adhering to the SIEM-specific guidelines recommended by regional and global standards like ISO27001 and FISMA.

- ☑ Focusing on critical alerts.
- ☑ High risk of non-compliance due to a limited team to configure SIEM as per compliance recommendations.
- ☑ The increased cost of maintaining SIEM.
- ☑ Limited visibility of the posture despite having SIEM in place.

---

## Financial services

Our client was an accountancy, bookkeeping, and tax services firm that works with business owners and individuals in Orange County, especially small business owners, assisting them in addressing their accounting and tax-specific challenges. Their services include – small business accounting financial and business consulting, QUICKBOOKS setup support and training incorporation and new business advisory, and assisting high net worth individuals with wealth management, budgets, and tax services.

Over the years of working with businesses, they have created a reputation by delivering quality services in accounting, booking, tax planning, and reduction of tax liability. They have helped businesses charter their profit journey and save costs on non-compliance to tax regulations through accounting and bookkeeping solutions. By assisting them with tax return preparation and proactive tax planning, they have built a preferred local brand. Their clientele comes from industries like construction, manufacturing, healthcare, and real estate.

---

## Solution

The firm began researching plausible security vendors to help them address this two-faced challenge of cybersecurity and compliance. However, they found it challenging to find a vendor focusing on cybersecurity and compliance. It is where they found SharkStriker, which offered them expertise in both cybersecurity and compliance. With SharkStriker, they prepared a detailed set of requirements with a detailed scope.

" Non-compliance is one of the biggest fears that few people talk about. Since we save businesses from non-compliance to tax regulations, we wanted to ensure that we are compliant. We found a lot of cybersecurity vendors that offered expertise that was limited to just cybersecurity. It is where we found SharkStriker, they offered us the much-needed expertise to configure, manage, and monitor our SIEM as per the recommended guidelines."

**- Founder, CEO**

---

Time to Value

**300 hrs. → 20 hrs.**

Time to discover

**1hr → 1 min**

---

## Results

### Ease of cybersecurity and compliance management

The platform comes with SOAR (Security Orchestration and Automated Response) that automatically detects and responds to suspicious activities before they become serious threats. STRIEGO's robust features include - CIS based benchmark assessments, vulnerability management and smart reports. Through these features, organizations were able to gain complete visibility of vulnerabilities with important information on them, such as severity and frequency of exploitation. It empowered the security team to engage in precise and quick patching with clear prioritization of vulnerabilities. With periodical reports and security advisories, the firm was able to prepare its posture against evolving threats proactively.

"Earlier, it was a struggle approaching cybersecurity, given how complex it was to manage multiple aspects of security while not being able to get a granular view into cybersecurity operations. Despite having an industry-leading SIEM, we struggled to take quick and precise actions on posture and compliance-recommended actions. Thankfully with SharkStriker's STRIEGO platform, we were able to address the complexity with centralized control and dedicated compliance-friendly features that addressed cyber security seamlessly. The dedicated expertise offered by their team helped us address the gaps in compliance-specific SIEM "

- Founder, CEO

---

Time to manage event reduced by

**50mins to 5mins**

**90%** reduction in alert noise

---

Saved time for important functions like proactive threat detection and customer value enhancement.

SharkStriker's STRIEGO addressed the challenge of alert fatigue through high-precision AI ML-based detection and expert-backed SIEM monitoring. It allowed experts to focus on critical alerts that demanded more attention before they escalated to something serious. It helped them reduce their time to detect and time to respond. With a dedicated team of experts managing and monitoring SIEM, the organization can focus on customer value enhancement.

"It can be a challenge thinking about innovation or working on improving the quality of services when your security team is constantly overwhelmed with alerts. SharkStriker helped us address this challenge by offering a platform that automatically catered to suspicious activities, reducing false positives significantly and allowing our security teams to focus on more important cybersecurity matters while we focus on improving service quality and innovating our services."

**- Founder, CEO**

---

**70%** reduction in time spent to investigate

**90%** reduction in fatigue due to events generated from customized playbooks

---

Extended visibility with posture-specific insights to make quick and meaningful decisions.

STRIEGO gave the firm access to multiple dashboards, offering context and color specific to their security posture. These dashboards gave a bird's eye view of the status of the posture, with insights to make meaningful decisions. Experts could generate customized reports that fulfilled multiple compliance requirements. Through customized workbooks and alert & log management, SharkStriker's experts assisted the organization in deriving ROI outcomes from its SIEM solution.

"We were looking for a vendor that could help us derive value from SIEM while fulfilling the guidelines recommended in various compliance standards applicable to our organization. SharkStriker helped us achieve that through effective log management as per recommended guidelines, customization of workbooks for efficient detection and alerting, and a significant reduction in time spent on investigations through effective first-level triage "

**- Founder, CEO**

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

**CLICK HERE TO READ**

