SharkStriker

CASE STUDY

Industry: IT Services

SharkStriker assists IT service provider from the UAE in improving the overall cybersecurity posture with SIEM as a service and SOC as a service

Background

As an IT service provider from the UAE, our client wanted to channel productive outcomes across their software development cycle and improve its customer experience through integration of cloud environment with the IT infrastructure. However, it was full of security vulnerabilities that needed to be identified and addressed by experts. There was a serious need of round the clock security of all the digital assets with a solution that automatically monitored and responded to threats. This is when SharkStriker came into the picture.

Objectives

- Set up a baseline cybersecurity framework accommodating business growth and the ever-changing threat landscape.
- Deploy a security solution that works as a standalone solution for all cybersecurity needs.
- Gain centralized visibility of all the security operations in the organization.
- Bridge awareness gaps in cybersecurity and establish a culture for cybersecurity.
- Identify all the existing vulnerabilities in the IT infrastructure and take necessary measures to remediate them.
- Establish a dedicated team for addressing all the matters of cybersecurity and compliance.

Chanllenges

Our client belonged to the IT industry and needed to secure their services through round-the-clock protection of all customers' data processed through the services offered. However, due to the skill shortage in cybersecurity, they faced challenges in achieving their objectives. The threat of a data breach was looming, and they had to ensure they took measures immediately. The following are the challenges they faced:

- Absence of a team to assess the posture against the industry's best practices
- There has been no review of the existing configurations and controls for response effectiveness against the most immediate cyber threats.
- No assessment of the existing IT infrastructure for existing security risks and vulnerabilities
- Information security measures for protecting the most valuable customers' information were absent.
- No security solution rendered round-the-clock protection of all critical components of their IT infrastructure, including their valuable digital assets.
- They did not have insights into their security posture to make meaningful decisions.
- No expertise on board to assist them with threat triage.
- Incident response planning was absent.

Solutions

Our client was looking for a single-stop solution that catered to all their challenges and helped them improve their cybersecurity posture. It is where they found us. Through our holistic services and human-led AI and ML solutions, we were looking to solve all their industry-specific and company-specific challenges. Since they wanted a security solution that could provide them with real-time security of their IT infrastructure around the clock and that was fully managed by cybersecurity experts, we offered them our SIEM solution backed by our SOC team. The following are the ways in which we assisted them in solving their challenges:

- Our SOC team conducted a fundamental assessment of their cybersecurity posture.
- We implemented all of the security measures based on the identification of vulnerabilities.
- As per their scope, we tailored our SIEM and deployed it to their IT infrastructure.
- SIEM provided them with real-time protection of the entire IT infrastructure.
- It rendered them continuous monitoring with AI and ML-based automated response to threats.
- The SOC team filled the cybersecurity skills gap in their organization, working as an extension of their cybersecurity team.
- Experts-guided triage allowed them to respond with precision.

- Incident responders at SharkStriker assisted them in drawing a comprehensive incident response plan.
- We identified the gaps where they lagged and created a set of procedures and policies, and implemented the controls for increased protection, detection, and response.
- With dashboards, they were able to generate reports and gain access to insights specific to their cybersecurity posture.
- They got the much-needed threat intelligence they needed, updated from time to time on the various TTPs.

Outcome

Our client finally had a cybersecurity posture that was built taking into account the most dangerous threats ofAs a result of availing our SIEM and SOC as a service, the company achieved the following outcomes for their business:

- Established a baseline framework for cybersecurity addressing some of the most immediate threats and vulnerabilities
- Round the clock security through a dedicated team of cybersecurity experts
- They got expert guidance on threat triage that allowed them to respond to threats more precisely
- Overall improvement of cybersecurity posture
- Implemented a measure to protect assets and control damage in the case of cyber incidents
- They were able to make better decisions through actionable repots generated with dashboards
- Assistance with compliance through implementation of all the hygiene security measures recommended in the compliances applicable.
- Through SIEM, they were able to get a centralized visibility of their entire security process across their IT infrastructure

SharkStriker

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

+1 925 5321900

sales@sharkstriker.com

www.sharkstriker.com

/company/sharkstriker

/thesharkstriker

/TheSharkStriker

/thesharkstriker