SharkStriker

DATASHEET

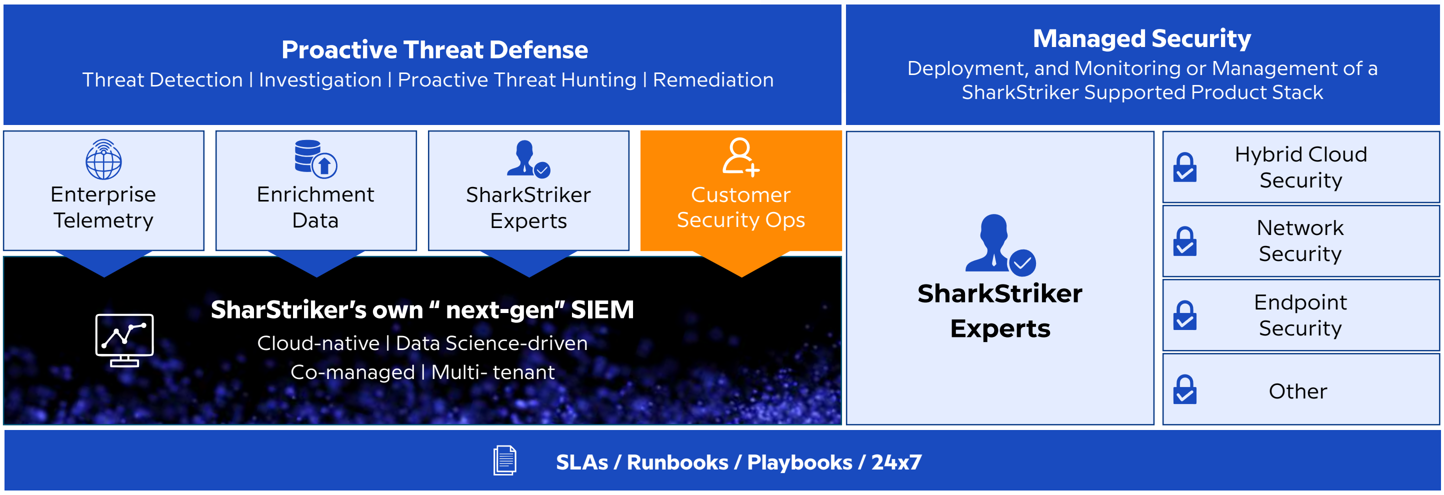
SOC as a Service

SOC as a Service Defined

- As the world continues to go digital, the threat landscape is constantly changing. The evolving landscape makes every business equally vulnerable to cyberattacks, whether big or small. Hence, detecting and responding to risks in real time has become vital.
- SharkStriker's SOC-as-a-Service perfectly blends the resources, skills, and tools to offer a robust 24/7 SOC that works as an extension to your local team. When you choose SharkStriker as your SOC partner, you get a host of additional benefits covering the core pillars of a SOC: people, processes, and products.
- Our SOC teams comprise threat researchers, threat hunters, security analysts, administrators, SIEM specialists, forensic experts, etc., to provide all-encompassing cybersecurity through our Security Operation Centers. They leverage our machine-accelerated MDR platform and best-in-class tools to ensure optimal security.

What do you get?

- Provides unified multi-cloud visibility for AWS, Azure, and Google Cloud
- Continuous monitoring for cloud misconfigurations
- Protects cloud workloads from Exploits, Ransomware, and Adversaries
- Reduces alert fatigue with machine accelerated incident response
- Assesses the vulnerabilities and baseline
- Delivers Cloud Monitoring, Posture Management (CSPM), and Workload Protection (CWPP) under one service



Proactive Threat Defense

Threat Detection | Investigation | Proactive Threat Hunting | Remediation

Managed Security

Deployment, and Monitoring or Management of a SharkStriker Supported Product Stack

Enterprise Telemetry

Enrichment Data

SharkStriker Experts

Customer Security Ops

SharStriker's own " next-gen" SIEM

Cloud-native | Data Science-driven

Co-managed | Multi- tenant

SharkStriker Experts

Hybrid Cloud Security

Network Security

Endpoint Security

Other

SLAs / Runbooks / Playbooks / 24x7

SharkStriker's SOC-as-a-Service Key Features

24/7 Monitoring

- Our cybersecurity experts work round-the-clock for continuous monitoring, detection, and response. Moreover, our machine-accelerated platform helps detect and respond to threats in real time. It also enables our experts to go proactive on threat hunting and deliver immediate incident management.

Open Architecture MDR Platform

- Our MDR platform is a unique open-architecture technology stack that can easily integrate with any existing security tools for quick results. We have built it with an adversarial mind set. The MDR platform leverages machine intelligence, and our experts blend it with human intelligence to provide hands-on keyboard-based protection.

Next-Gen SIEM

- Our next-gen SIEM allows the SOC teams to bring triage data from all the security tools to a single platform for a granular view. The centralized visibility helps our experts to perform ongoing and in-depth log management and analysis. Built with security orchestration, threat detection engine, behavior analytics, and compliance capabilities, the SIEM platform brings together all the essential modern-day SOC requisites to a single platform to convert raw triage data into actionable insights for developing correlation rules.

Top-Notch Threat Intelligence

- We have our threat database of historical and real-time data comprising known IOCs, bad domains, IP addresses, triage data, etc. Our cybersecurity experts leverage all this data throughout the threat hunting process for a thorough inspection and quick detection. We also use it for data enrichment to bring context to telemetry data and act accordingly for incident response.

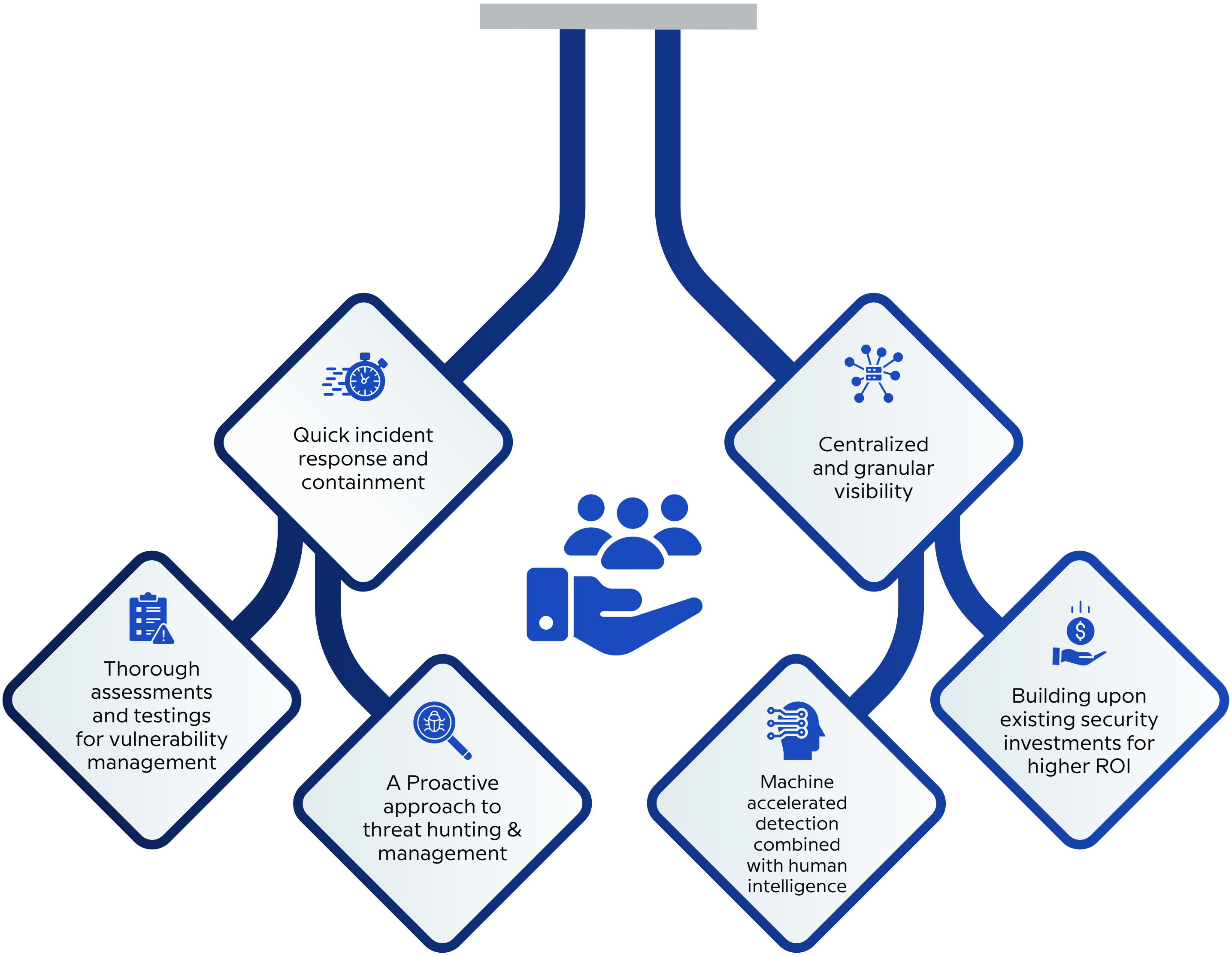
The Right Expertise

- Security tools alone cannot protect your organization. You also need the expertise to leverage them. SharkStriker's SOC team members are certified experts with profound industry knowledge. Moreover, our best-in-class research labs help them stay updated with the latest techniques used by threat adversaries. The blend of the right expertise and robust platforms, mapped against the MITRE ATT&CK framework, ensures that all the risks are detected and mitigated before they become dangerous for your organization.

Additional Managed Services Stack

- SharkStriker is a one-stop comprehensive cybersecurity provider. Our managed security services cover the entire threat life cycle according to security best practices to remediate cybersecurity risks. Hence, we can take complete control of your security requirements, including cloud, endpoint, network, and firewall security, so that you can focus on increasing your business.

Benefits of Using SharkStriker SOC-as-a-Service



Quick incident response and containment

Centralized and granular visibility

Thorough assessments and testings for vulnerability management

A Proactive approach to threat hunting & management

Machine accelerated detection combined with human intelligence

Building upon existing security investments for higher ROI

About SharkStriker

SharkStriker is a trailblazing cybersecurity services vendor with a mission to simplify cybersecurity for its partners across industries through its technologically driven human-led open architecture platform STRIEGO. It seeks to cater to some of the industry's most immediate challenges such as siloed cybersecurity, increasing cost of cybersecurity solutions, changing regulatory environment, and increasing reliance on multiple vendors for multiple aspects of cybersecurity and compliance.

With STRIEGO, SharkStriker is able to assist its network of partners and customers through effective augmentation of cybersecurity posture as per use cases, extending visibility, compliance management, and round-the-clock support for incident response.

Through a team of threat-striking experts, they have made their presence across MEA, North America, Europe, and Asia.

Globally recognized, Globally trusted.

Phone: +1 925 5321900
Email: sales@sharkstriker.com
Website: www.sharkstriker.com

SharkStriker