SharkStriker

DATASHEET

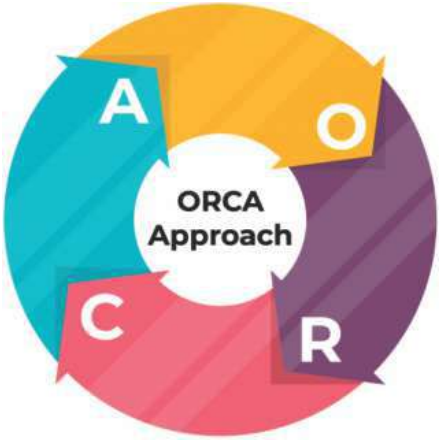
Human-Led MDR That Blends Machine and Human Intelligence

Managed Detection and Response Service Defined

SharkStriker's Managed Detection and Response (MDR) service platform is based on our ORCA (Observe,Response, Compliance, Awareness) philosophy. The ORCA philosophy is taken from the real-life world.Sharks only fear the killer whale or ORCA. SharkStriker's unique platform acts as the ORCA to strike all the sharks in the cybersecurity ocean. Through our ORCA philosophy, our elite team of cybersecurity experts provides hands-on keyboard-based incident response and human-led threat hunting.

It is a machine-accelerated platform that uses modern-day technologies like Machine Learning and Artificial Intelligence for real-time threat hunting without taking away the human factor. Our cybersecurity experts use the platform to deliver hands-on keyboard-based threat hunting and incident responses. We don't limit the number of Incident Responses (IR) in our MDR service. Hence, the customers don't have to worry about retainers or hourly-based IR charges. Our MDR platform is based on open architecture, meaning it can easily integrate with any existing cybersecurity solution, eliminating the need for any additional investments.

Our MDR service covers the entire business ecosystem through our ORCA philosophy, whether hosted on the cloud or on-premise, by securing the endpoints, network, cloud environment, etc. The open-architecture MDR easily integrates with any existing security solution to quickly align the detection and protection to the MITRE Att&ck Model and optimize response. Our MDR also uses AI/ML for machine-accelerated threat hunting, threat intelligence, contextual analysis, behavior analytics, and automated detection and responses. AI and ML ensure that our customers are not overwhelmed by false positives to save resources and time. It also helps in providing actionable insights so that even manual detection and response action can be done swiftly.



O **OBSERVE**
Collect, Store, Detect, Analyze and Visualize the Cyber Security Attack

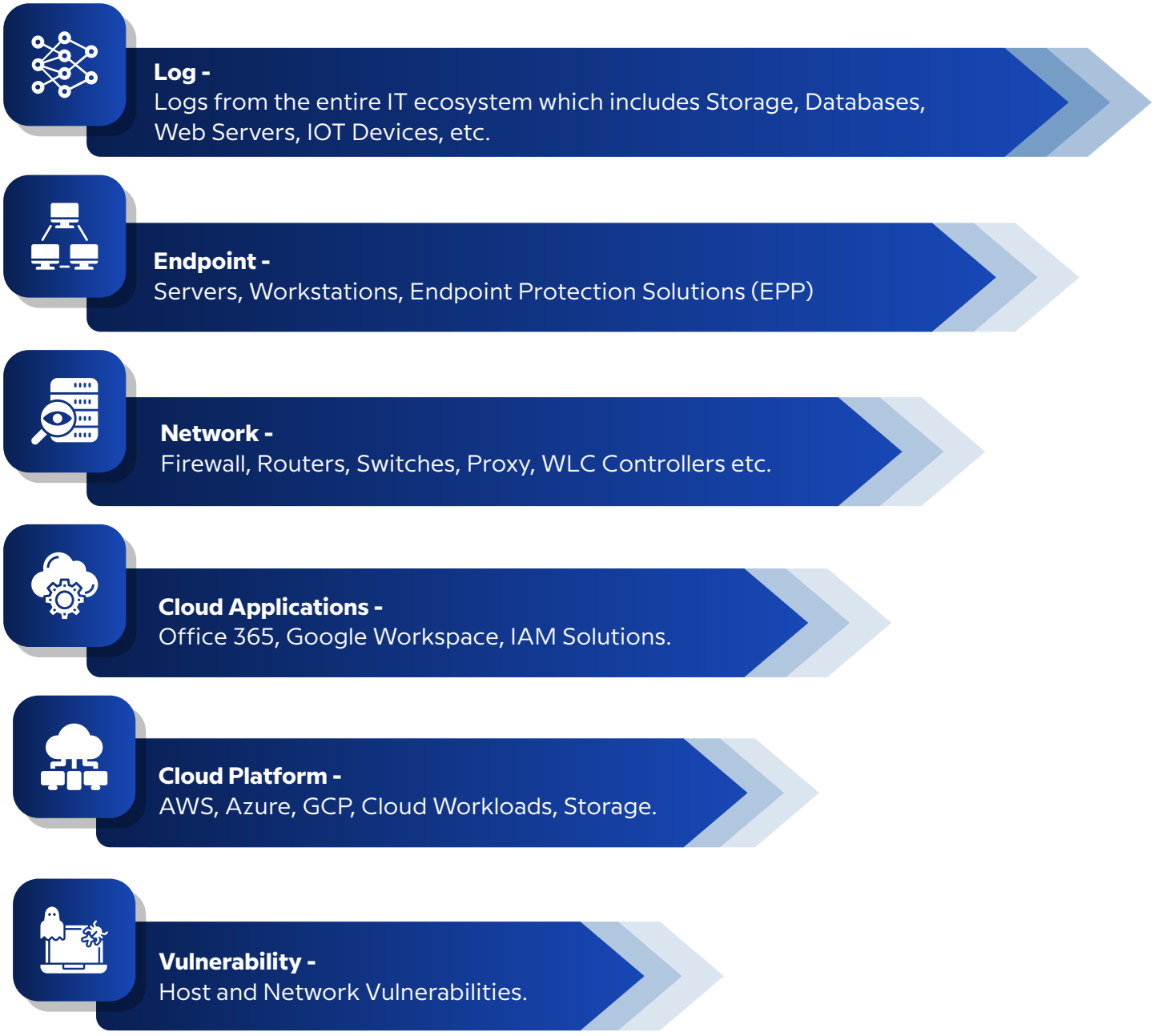
R **RESPONSE**
Incident Investigation and Machine-Accelerated Automated Responses

C **COMPLIANCE**
Security controls to stay compliant with PCL-DSS, GDPR, HIPPA, NIST

A **AWARENESS**
Build Cyber Security Culture by raising the Awareness in the organization

Multi-Vector Threat Detection and Visibility

At SharkStriker, we believe that risks can take shelter anywhere across the attack surface. Hence, a multi-signal, 360° is essential to protect your organization. Through our MDR platform, we ingest data from various sources, including network, endpoint, cloud, switches, logs, events, etc., to strengthen our detection and response capabilities. As an open-architecture machine-accelerated platform, our MDR collects data from multiple sources, providing a centralized visibility through a single platform. Our SIEM administrators correlate Indicators of Compromise and detection data across the infrastructure, and our 24/7 SOC Analysts alongside our expert Threat Hunters analyze, investigate, and implement response actions against the sophisticated threats that have bypassed your security.



Whether you host your applications and business environment on the cloud or on-premises, we have the right tools and expertise to get the visibility to see the security gaps that other MDR providers might miss.

Machine Accelerated Human Lead Threat Hunting

Intel Driven Threat Hunting:
Disparate third-party data sets are converted into actionable threat intelligence to identify malicious actors lurking on your network.

Adversary Driven Hunting:
Our Cyber Security experts spend a considerable amount oftime understanding adversary tactics, techniques and procedures by analyzing indicators of compromise, to give you the benefit of 'smart defense' driven by adversarial intelligence.

Retrospect Hunt:
The use of latest threat detection technologies enables retrospective threat hunting that helps search for threats by going through rich meta data and retrospective analysis.

Analytics Driven Hunting:
Tailored data science algorithms, ML and statistical data is merged and analyzed to identify potential risks that cannot be detected through conventional security products.

Live Hunt:
Superior telemetry integrated with high-fidelity threat intelligence hunts for threats across endpoints that have evaded security protocols.

24/7 Threat Hunting:
Our global SOCs enable our cybersecurity experts to work round-the-clock for continuous threat hunting.

Incident Response

Skills and Expertise
SharkStriker Incident Response Services teamcomprises experienced professionals with profoundskills and knowledge in Incident Response and forensic research.

Root Cause Analysis
Our Incident Response experts will conduct anin-depth analysis of the threats targing your organiztion. SharkStriker provides insights andanalysis for multple threats, including malware, IPS,DDoS, botnets, firewall, data loss, etc.

Comprehensive Containment and Remediation
If we detect any compromised host, our IncidentResponse experts will use our threat labs to performdigital forensics. Accordingly, we will start with the containment process and real time remediation, including isolating, killing processes, suspending threat activities, etc.

Detailed Documentation

We will hand over a detailed report on all our findings and the steps taken for future references. We also mention the best practices for improving processes, response time, and overall security to prevent recurrences.

Unlimited Incident

We don't limit the number of Incident Responses (IR)in our MDR service. Hence, the customers don't have to worry about retainers or hourly-based IR charges.

Tailored Solution Plan

SharkStriker's Incident Response Services experts work as an extension to your in-house team for seamless communication and transparency to create custom response and containment plans.

SharkStriker Advantages

01

24/7 Cybersecurity Experts

Cyber adversaries don't have any working hours. Our cybersecurity experts work 24/7 so that cybercriminals cannot take the advantage of non-working hours to penetrate your system.

02

Leverage Existing Investment

Built with an open architecture, SharkStriker's MDR platform can integrate with your existing security solutions to enable you to leverage existing technologies and eliminate reinvestments.

03

Hands-on Keyboard Responses

Our machine-accelerated MDR platform is used by our cybersecurity experts to deliver human-led, keyboard-based threat responses.

04

Unlimited Log Retention

SharkStriker MDR platform has built-in SIEM capabilities that allow retaining unlimited logs to help you abide by primary compliances and you don't have to worry about retention-based pricing.

05

Vulnerability Management

Our cybersecurity experts conduct thorough vulnerability assessments and penetration testings to identify potential loopholes and mitigate them.

06

Baseline Security Assessment

We match your security posture against the CIS baseline security to detect deviations. Our cybersecurity experts also provides our customers with a detailed report and help them align with the benchmark security.

SharkStriker MDR Features

Feature	MDR Core	MDR Pro	MDR Complete
Compatible With 3d Party Security Products (EDR/AV/EPP/Firewall)	Yes	Yes	Yes
24/7 Expert-led Threat Monitoring and Response	Yes	Yes	Yes
24/7 SOC Access	Yes	Yes	Yes
Weekly & Monthly Assessment Reports	Yes	Yes	Yes
Monthly Security Posture Review	Yes	Yes	Yes
Inbuilt Endpoint Detection and Response (EDR)		Yes	Yes
Proactive Threat hunting		Yes	Yes
Incident Response	Actionable Guidance	Containment	Full Cycle IR
CIS Based Baseline Security Assessment		Yes	Yes
Vulnerability Management		Limited	Yes
Security Awareness		Yes	Yes
Network Detection & Response (NDR)			Yes
Deception Technology			Yes

About SharkStriker

SharkStriker is a global security services vendor with SOCs and offices across the globe.We are your cybersecurity team. We are the gatekeepers of your network. We ensure that you get maximum value from your cybersecurity framework.

Our purpose-built cybersecurity-centric, AI/ML-powered platform with a well-honed adversarial orientation delivers all-encompassing protection to the organization through - proactive protection, automated detection, machine learning-based response, threat intelligence, incident management, compliance management, and security awareness.

Our cybersecurity team uses their expertise to hunt for threats leveled at your organizational network and remediate these effectively and quickly. Our focus is simple – address threats before they become a problem.

Our Certifications and Awards

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