SharkStriker

# Human-Led MDR That Blends Machine and Human Intelligence

Data Sheet

## 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 Responese

**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

# Human-Led MDR That Blends Machine and Human Intelligence

## 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.

- Network - Firewall, Routers, Switches, Proxy, WLC Controllers etc.
- **Endpoint -** Servers, Workstations, Endpoint Protection Solutions (EPP) Solutions.
- Log - Logs from the entire IT ecosystem which includes Storage, Databases, Web Servers, IOT Devices, etc.
- Cloud Platform- AWS, Azure, GCP, Cloud Workloads, Storage.
- Cloud Applications- Office 365, Google Workspace, IAM Solutions.
- Vulnerability- Host and Network Vulnerabilities.

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.

# Human-Led MDR That Blends Machine and Human Intelligence

## 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 of time 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.

# Human-Led MDR That Blends Machine and Human Intelligence

## Incident Response

### Skills and Expertise

SharkStriker Incident Response Services team comprises experienced professionals with profound skills and knowledge in Incident Response and forensic research.

### Root Cause Analysis

Our Incident Response experts will conduct an in-depth analysis of the threats targeting your organization. SharkStriker provides insights and analysis for multiple threats, including malware, IPS, DDoS, botnets, firewall, data loss, etc.

### Comprehensive Containment and Remediation

If we detect any compromised host, our Incident Response experts will use our threat labs to perform digital 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.

# Human-Led MDR That Blends Machine and Human Intelligence

## SharkStriker Advantages

### 24/7 Cybersecurity Experts

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

### 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.

### Hands-on Keyboard Responses

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

### 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.

### Vulnerability Management

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

### 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.

# Human-Led MDR That Blends Machine and Human Intelligence

## SharkStriker MDR Features

| Service | MDR | MDR Pro | MDR Elite | MDR Ultimate |
|---|---|---|---|---|
| | | | | |
| **End Point Detection and Response (EDR)** | | | | |
| | | | | |
| **Protection** | | | | |
| Ransomware Protection | √ | √ | √ | √ |
| Phishing Prevention | √ | √ | √ | √ |
| Signatureless Malware Prevention | √ | √ | √ | √ |
| Exploit Prevention | √ | √ | √ | √ |
| Adversary Prevention | √ | √ | √ | √ |
| Fileless or Zero-Footprint or In-Memory Attack Prevention | √ | √ | √ | √ |
| Credential Theft Protection | √ | √ | √ | √ |
| Memory Injection Prevention | √ | √ | √ | √ |
| Comprehensive MITRE ATT&CK® protection | √ | √ | √ | √ |
| Security event collection and storage | √ | √ | √ | √ |
| Protection for Windows, Linux, and MacOS | √ | √ | √ | √ |
| Attack Root Cause Anslysis (RCA), enriched with context from MITRE ATT&CK | √ | √ | √ | √ |
| | | | | |
| **Threat Hunting** | √ | √ | √ | √ |
| AI-powered natural-language query chat-bot | √ | √ | √ | √ |
| Realtime Threat Detection & Monitoring | √ | √ | √ | √ |
| Search for IoCs and hunt using Event Query Language (EQL) | √ | √ | √ | √ |
| Audit system information, applications, file systems, and host firewall | √ | √ | √ | √ |
| Audit loaded drivers and removable media | √ | √ | √ | √ |
| Audit running processes, network events, registry hives, and discover persistence | √ | √ | √ | √ |
| Automated memory analysis | √ | √ | √ | √ |
| Outlier analysis | √ | √ | √ | √ |
| | | | | |
| **Incident Investigation and Response** | | | | |
| Automated Response | √ | √ | √ | √ |
| Isolate Hosts | √ | √ | √ | √ |
| Kill Process | √ | √ | √ | √ |
| Suspend Threat Execution | √ | √ | √ | √ |
| Automated File Quarantine | √ | √ | √ | √ |
| Delete, upload, execute files | √ | √ | √ | √ |
| | | | | |
| **SIEM** | | | | |
| Fully managed and hosted SIEM | √ | √ | √ | √ |
| Raw Log retention for compliance (Retention period 1 year) | √ | √ | √ | √ |
| SIEM correlation rules including AI/ML based (Default and Custom) | √ | √ | √ | √ |
| Alert notifications | √ | √ | √ | √ |
| Live Dashboards Access (Threat / Compliance) | √ | √ | √ | √ |
| Support of multiple log sources | | √ | √ | √ |
| User Behavior Analytics (UBA) | √ | √ | √ | √ |
| Cloud infrastructure Monitoring like AWS, Azure, Google Cloud | | | √ | √ |

# Human-Led MDR That Blends Machine and Human Intelligence

| Service | MDR | MDR Pro | MDR Elite | MDR Ultimate |
|---|---|---|---|---|
| | | | | |
| **SOC Service** | | | | |
| 24x7 SOC team | √ | √ | √ | √ |
| Automated Incident Response (Active Response) such as blocking IP, FQDN, Endpoint Isolation etc | √ | √ | √ | √ |
| Threat Intelligence (Threat Feeds) | √ | √ | √ | √ |
| Threat Hunting | √ | √ | √ | √ |
| Incident Response & Mitigation Service | √ | √ | √ | √ |
| Monthly Assessment Report | √ | √ | √ | √ |
| | | | | |
| **Compliance Management** | | | | |
| File Integrity Monitor (FIM) | √ | √ | √ | √ |
| Host vulnerability detection | √ | √ | √ | √ |
| Log and events data collection | √ | √ | √ | √ |
| Configuration assessment and policy monitoring | √ | √ | √ | √ |
| Security Controls for Regulartory Compliance like PCI, GDPR, NIST | √ | √ | √ | √ |
| Regulatory Compliance Report | √ | √ | √ | √ |
| | | | | |
| **Vulnerability Management (VAPT)** | | | | |
| Host Vulnerability Assessment (VA) (Quaterly) | √ | √ | √ | √ |
| Network Vulnerability Assessment (VA) (Quaterly) | | √ | √ | √ |
| Cloud Vulnerability Assessment (VA) (Quaterly) | | | √ | √ |
| Network Penetration Testing (PT) (Yearly) | | | | √ |
| | | | | |
| **Security Awareness Training (Quarterly)** | | | | |
| Phishing Simulation | | √ | √ | √ |
| Phishing Awareness Training | | √ | √ | √ |
| | | | | |
| **Cloud Infrastructure Monitoring** | | | | |
| Security Audit for Cloud Platform (AWS, Azure, Google) | | | √ | √ |
| AI-Powered Security Analytics and Monitoring | | | √ | √ |
| Smarter DevSecOps | | | √ | √ |
| Alert Correlation and Smart Alerts | | | √ | √ |
| Automated Incident Response | | | √ | √ |
| Network Topology Visualization | | | √ | √ |
| Anomaly Detection and Analytics | | | √ | √ |
| Real-Time Inventory Management | | | √ | √ |
| Automatic Asset Discovery | | | √ | √ |
| Continuous Assessments | | | √ | √ |
| Monitoring of Office 365 or G Suite | | | √ | √ |
| | | | | |
| **Network Traffic Analysis (NTA)** | | | √ | √ |

# Human-Led MDR That Blends Machine and Human Intelligence

| Service | MDR | MDR Pro | MDR Elite | MDR Ultimate |
|---|---|---|---|---|
| | | | | |
| **Network Security** | | | | |
| Firewall Configuration Audit & Assurance | | √ | √ | √ |
| Firewall Traffic Monitoring | | √ | √ | √ |
| Firewall Event Collection and Correlation | | √ | √ | √ |
| Device Configuration Backup | | √ | √ | √ |
| | | | | |
| **Deception Technology** | | | | |
| Active Directory Server Deception | | | | √ |
| Web Server Deception | | | | √ |
| Database Server Deception | | | | √ |
| Windows Client Deception | | | | √ |
| Email Server Deception | | | | √ |
| FTP Server Deception | | | | √ |
| | | | | |
| **Password Manager for IT Team** | | | √ | √ |
| One Administrator Per Company | | | √ | √ |
| Centralized password vault | | | √ | √ |
| Password sharing and management | | | √ | √ |
| Password policies | | | √ | √ |
| Audit and instant notifications | | | √ | √ |
| User / User group management | | | √ | √ |
| Mobile access (Android, iOS, Windows) | | | √ | √ |
| Browser extensions (Chrome, Firefox, IE) | | | √ | √ |
| Export passwords for offline access | | | √ | √ |
| Backup and recovery provisions | | | √ | √ |
| | | | | |
| **Darkweb Monitoring** | | | | |
| Domain Monitoring1 | | | | √ |
| Stolen Credentials | | | | √ |
| Leaked Source Code | | | | √ |
| | | | | |
| **Code Repositories Scanning** | | | | |
| Scanning of public code repositories | | | | √ |
| Accidentally leaked source code / credentials | | | | √ |
| Secret scanning (Token Scanning) | | | | √ |

# Human-Led MDR That Blends Machine and Human Intelligence

## About SharkStriker

SharkStriker is a USA-based Managed Security Service Provider (MSSP). Our MDR platform is a white-labeled, open-architecture solution that empowers our partners and customers to strengthen their fight against cybersecurity. The platform can easily integrate all your existing security tools so that you don't have to worry about extra or re-investments. Our machine-accelerated MDR enables our cybersecurity experts to get a granular view across your business ecosystem and leverage the data to offer hands-on, keyboard threat hunting and response.

### Compliant

SOC 2 TYPE 2 · ISO 27001 · GDPR

### Mapped

MITRE ATT&CK™

### Awarded

CYBER SECURITY EXCELLENCE AWARDS — Fastest Growing Cybersecurity Company — ★ WINNER ★ 2022

CYBER SECURITY EXCELLENCE AWARDS — Managed Detection and Response — ★ WINNER ★ 2022

**Reach Us to Learn More**

**Email:** sales@sharkstriker.com