SharkStriker

Incident Response Service

Data Sheet

Benefits of SharkStriker's Incident Response Services

Unique Platform

SharkStriker's cloud-based cybersecurity platform is machine-accelerated,enabling identifying attacks in real-time for quick containment and recovery.

Skills and Expertise

SharkStriker's Incident Response Service team has a profound and diversified incident response and forensics experience and skills.

Tailored Solution Plan

SharkStriker's IR team works with your in-house team to create a tailored cybersecurity plan to prevent future incidents based on analytics and learnings.

Granular View

All the solutions used to deliver our Incident Response (IR) Cybersecurity services are open architecture solutions. They can easily integrate with any existing security tools for granular view and better results.

The SharkStriker's Incident Response (IR) team and services can offer rapid control, clarity, organization, and response to a sophisticated and chaotic cyber situation. As the current cyber security threat landscape is changing exponentially, most companies, regardless of size, are likely to face a cyber incident. Responding to such an incident quickly and managing it effectively is the only way to mitigate the disastrous consequences of a cyberattack that can lead to the loss of hundreds and millions.

The SharkStriker's IR team works as an extension of your in-house security team to manage such critical incidents. They help with root cause analysis to determine the cause of the attack, analyze it, resolve and respond to immediate issues, and implement a solution capable of preventing such recurrences. Our IR team leverages our cloud-hosted, machine-accelerated MDR platform while taking a human-led, keyboard-based approach to blend machine and human intelligence perfectly. The MDR platform allows monitoring and responding to attacks and malicious events in real-time to eradicate any threats from your environment. SharkStriker's unique MDR platform, methodology, expertise, and approach cover the entire incident response lifecycle, from detection and analysis to containment and recovery to reporting and implementing appropriate solutions. The IR team also notes the key pointers and lessons that can serve as insights to prevent any future incidents. They aim to minimize downtime and other impacts to bring your company back on track quickly.

Incident Response Service

SharkStriker Incident Response Services Approach

SharkStriker takes a standard but tailored approach to cover all the aspects of incident response.

Step 1: Requirements Gathering

We believe in getting our Incident Response Services started without wasting time,but only after a thorough requirement gathering. It is essential to ensure that all the services are performed based on the requirements to achieve goals. This step helps agree on the services' scope and time and helps gather all the information required from stakeholders, the in-house security team, and the IT team. Some of the activities occurring during this step include:

- Introductory conference call
- Interviews with stakeholders and others for information gathering
- Setting scope of the services
- Assigning engagement resources
- Identifying authorized accounts and client contacts

Step 2: Deploy Tools and Integrate With Existing Solutions

Continuous monitoring and centralized visibility across the environment are crucial for efficient incident response. SharkStriker's security tools and platforms are built with an open architecture that perfectly meets this requirement. Open architecture means that our tools can easily integrate with existing security tools for quick deployment.

In the second step of our Incident Response Services, we integrate all the assets and security solutions with our cybersecurity platform for a granular, single pane of glass view. Integrating all the solutions enhances data flow and traige to help with root cause analysis further incident response activities.

Incident Response Service

Step 3: Evaluation and Analysis

SharkStriker will gather all the information specific to threats for detection and analysis. Our IR team also offers a complete analysis of specific malware targeting your organization. Based on the malware sample, our threat researchers and threat hunting experts will craft a detailed report containing the properties, detailed description, and basic remediation plan for the malware. Our IR analysis also helps to:

- Identify compromised hosts and accounts
- Identify IOC
- Document timeline through recurring events
- Identify forensic artifacts
- Identify exfiltrated data and methods
- In-depth malware analysis
- Identify initial access to the environment

Step 4: Containment

If any compromised host is detected, our cybersecurity experts use the Threat Lab to perform Digital Forensics to understand what's going on exactly and take the necessary containment actions to mitigate further movement. The IR team will also provide a detailed report regarding the analysis and the appropriate actions taken against issues to the customer. This will be done with an aim to:

- Isolate hosts
- Kill processes
- Suspend threat execution
- Quarantine compromised files

Step 5: Short-Term and Long-Term Remediation

Besides containment, the SharkStriker Incident Response Services team will also take all the necessary remediation steps. The remediation actions will be based on the learnings from the threat analysis. Our incident responders will use a hands-on, keyboard-based approach and triage with customers to respond to detected threats. The IR team will terminate the affected process, implement essential security solutions, remove any compromised files, etc. Also, the team will provide other remediation suggestions for long-term prevention to avoid recurrences. Lastly, SharkStriker's end-to-end report for the entire analysis and response process will be handed over for reference purposes.

Incident Response Service

About SharkStriker

SharkStriker is a USA-based comprehensive cybersecurity provider with SOCs and offices worldwide. Our Incident Response Services team can offer quick and efficient containment and response with a wide array of tools, expertise, and services in the arsenal. Our cybersecurity experts utilize our AI/ML-powered MDR platform based on our ORCA philosophy and built with an adversarial mindset to cover all the aspects of cybersecurity. We deliver all-encompassing protection to the organization, including proactive protection, automated detection, machine learning-based response, threat intelligence, incident management, compliance management, and security awareness for enhanced ROI on cybersecurity investments.

To learn more, visit: https://sharkstriker.com/

Or shoot an email at: sales@sharkstriker.com