



## SIEM as a Service

### | SIEM - Your all-pervasive eyes & hands of cyber security + Compliance

Gain enhanced visibility and achieve compliance

#### | The Benefits



Renders  
360-degree  
visibility



Helps you  
achieve regional  
and international  
compliance



Easily  
integrates  
with all  
your existing  
security  
investments



Empowers  
your IT  
teams with  
super-  
accurate  
insights



Fully managed  
and monitored  
by SOC experts

### | The challenges

Staying afloat in the digital sea is a challenge, especially with the ever-evolving threats and increasing competition. Managing the high volume of alerts without any visibility of cybersecurity posture, IT infrastructure can render an easy checkmate in any cyber threat game. It stands even true for small and medium business owners who lack the skill set or have a limited team with no expertise in cyber security. The following are the challenges faced by most of the small and medium businesses when it comes to cybersecurity:

- ✓ Lack of centralized visibility
- ✓ No centralized solution for multiple cyber security challenges
- ✓ Absence of compliance-friendly reporting
- ✓ No team or lack of skilled experts

- ✓ No 24x7 monitoring
- ✓ Alert fatiguing caused as a result of high quantity of alerts
- ✓ Lack of categorization of security alerts
- ✓ Zero guidance on cybersecurity measures to be implemented
- ✓ No incident response planning
- ✓ Lack of data protection and file monitoring

## | Enter SIEM - a single platform for 360-degree visibility & compliance

SIEM (Security Information and Event Management) solves these challenges. It engages in continuous monitoring through seamless monitoring. It comes with SOAR ( Security Orchestration and Automated Response) that automatically caters to alerts assisting security personnel to focus on what is more important.

Driven by Artificial Intelligence and Machine Learning, SIEM can automatically analyze the bad from the good, and the anomalous from the usual. It goes beyond alert monitoring and enables security experts by providing context-based analysis on alerts improving the effectiveness and accuracy of manual triage.

It is fully managed by experts who add a human touch assisting it to work at its full potential. It helps you achieve all your compliance goals seamlessly through continuous collection of logs and events and generation of reports that can be easily used for compliance.

With SIEM you can carve new avenues of growth for your business being stress free from the worry of disruptions from cyber attacks through expert driven incident response planning.

## | Unique values delivered

### | Easily works with what you already have

- + SIEM easily integrates with your IT infrastructure so you don't have to worry much about change.

### | Enables enterprises for productivity

- + By blending human expertise with cutting edge technology, it enables your business to focus on productivity, uninterrupted from cyber threats.

### | Round-the-clock Incident Response support

- + We offer full-cycle incident response with unlimited coverage.

### | Protects your valuable digital data assets through continuous monitoring

- + It engages in continuous monitoring of all your digital assets across your IT infrastructure securing your

**| Empowers your security team with a dedicated SOC team**

- + A dedicated team of cybersecurity analysts, incident responders and compliance consultants who render expertise driven guidance.

**| Renders centralized 360-degree visibility**

- + SIEM offers a centralized visibility of the cybersecurity posture of your IT infrastructure.

**| An automated response driven by AI/ML**

- + Say goodbye to alert fatigue with SIEM's super accurate automated response that is driven by AI/ML.

**| It allows you to focus on critical**

- + The SOAR integration assists the security team to focus on the critical alerts that need more attention and immediate action.

**| Continuous Configuration Assessment**

- + CIS benchmark-based baseline configuration assessment to improve overall security posture.

**| Renders context-based insights for effective triage**

- + SIEM engages in deep analysis of alerts and offers context based insights for our security team to accurately triage threats.

**| Smooth compliance through reports**

- + It periodically retains logs and events and generates reports that are compliance friendly for smooth achievement of compliance goals.

**| Continuous monitoring and analysis**

- + SIEM acts as a vanguard of your IT infrastructure's security rendering continuous monitoring, collection of logs and analysis.

**| Streamlined work flows for super accurate threat hunting, response, and remediation**

- + It provides security analysts with a streamlined workflow for more effective threat hunting, response and remediation.

**| Vulnerability Management**

- + Continuous vulnerability assessment of monitored hosts for operating systems and application-specific vulnerabilities.

**| AI powered UEBA**

- + User and entity behavior analytics powered by Artificial Intelligence to identify most dangerous actors.

Wait..... there is more!

We render a range of additional benefits so you can gain more value through our SIEM-as-a-service.

For instance, SIEM is fully managed by our SOC experts implementing some of the best cyber security practices to assist you in improving the ROI across your existing security investments.

## **| Additionally, we provide the following benefits:**



Free Installation +  
Deployment  
services from  
our experts



Tailored  
configuration  
specific to your  
enterprise



Tailored pricing -  
We offer predictable  
asset-based pricing  
opposed to log/volume/EPs  
that can be expensive,  
giving you the freedom  
to pay-as-you-grow

# **Deploy AI-ML powered human led SIEM for max achievement in compliance and cybersecurity**

Connect with our cybersecurity experts who will assist you in choosing the plan that best suits your budget and all of your requirements.

## | 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



©2024 ©SharkStriker Inc. All rights reserved.

