

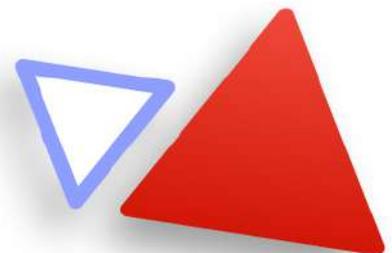
vSOCBox™

PRODUCT GUIDE

# AI/ML based SIEM (UEBA+XDR+SOAR)

Flexible Integration To Augment  
Your **Security Stack**

Let's Explore





## vSOCBox's **Cloud SIEM**

Discover and Prioritize Real Threats in real-time

vSOCBox SIEM is a cloud-native security operations center (SOC) solution that automatically analyzes and correlates threat alert data to help SOC analysts more efficiently discover and resolve meaningful threats.



## vSOCBox's Cloud SIEM **Capabilities**



User and Entity Behavior Analytics (UEBA)



Compliance Reporting



Security Orchestration, Automation, & Response (SOAR)



Advanced Correlation-based detection



ML and AI based Alarm Analytics



Alarms Prioritization & Triage



Advance Threat Intelligence



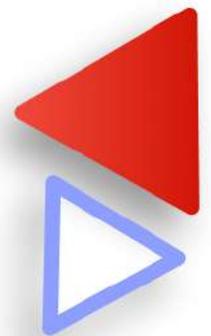
Asset Risk Scoring



Vulnerability Assessment

- Limitless log Collection & Storage
- Detect any Complex Security Threat 3m 47s
- Enhanced Visibility of all cyber infra layers
- Fast & Effective Data Protection
- Advanced Insights

vSOCBox is an Integrated Security Platform (SIEM + UEBA + CASB + IDM) provider that enables continuous monitoring & detection of Threats, Vulnerabilities, Risk of IT Network, and Applications and by users in a single pane based on SOAR.





## vSOCBox's Cloud SIEM enables SOC team with

vSOCBox's Next-Gen SIEM is capable of offering an effective and efficient means to monitor your network round the clock.



## vSOCBox's Cloud SIEM with XDR

vSOCBox's SIEM with XDR, an integrated functionality delivers improved visibility with contextualization of advanced threats to assist with triage, investigation, and rapid remediation efforts.

### SIEM

### XDR

<p>Multi domain coverage</p> <ul style="list-style-type: none"> <li>• Threat detection, investigation, and response (TDIR).</li> <li>• Compliance.</li> <li>• Centralized storage.</li> </ul>	<p><b>Domain Coverage</b></p>	<p>Single domain coverage:</p> <ul style="list-style-type: none"> <li>• TDIR</li> </ul>
<p>Designed for customization and "just in case" situations</p>	<p><b>Design Approach</b></p>	<p>Designed to be focused on efficient TDIR</p>
<p>Typically assumes that the data needs to be centralized in the SIEM.</p>	<p><b>Data Location</b></p>	<p>Typically assumes that data could be stored anywhere and/or doesn't need to be stored for the long term</p>
<p>Can be on-premise, cloud-delivered or both</p>	<p><b>Delivery Model</b></p>	<p>Cloud-delivered</p>
<p>Typically focuses on correlation based analytics</p>	<p><b>Storage Requirement</b></p>	<p>Typically offers machine learning based advanced analytics</p>
<p>Typically replaces or displaces legacy SIEMS, CLMS and/or data lakes.</p>	<p><b>GTM Motions</b></p>	<p>Typically augments legacy SIEMS, CLMS and/or data lakes.</p>

# vSOCBox's Cloud-Native SIEM **Benefits**

Empowering organizations with vSOCBox **NXT-GEN SIEM** with **XDR & UEBA** benefits with Flexible Integration to Augment your Security Stack

- Monitor logs efficiently and report suspicious events
- Collect, normalize and analyze logs and ingest threat intelligence feeds directly.
- With customizable reports, present data in different ways to spot trends, patterns, anomalies etc.
- Adhere to various compliance legislations like GDPR, CCPA, HIPAA, PCI-DSS etc.

## About vSOCBox

vSOCBox is an Enterprise Cyber Security SOC Platform Solution Company powered by AI & ML. It Serves to Detect, Analyze, & Automate response to all Cyber Threats & Advance attacks over network, cloud, user, data, & applications.



### Understanding Threats

Monitor logs efficiently and report suspicious events from humongous amount of data generated and collected from various business processes



### Present Data

With customizable reports, present data in different ways to spot trends, patterns, anomalies etc. and increase visibility and transparency within the network.



### Correlate Data

Collect, normalize and analyze logs and ingest threat intelligence feeds directly to understand real indicator of compromise (IOC) to further safeguard the network.



### Compliance Guideline

Adhere to various compliance legislations like GDPR, CCPA, HIPAA, PCI-DSS etc. through custom SIEM reporting and safeguard data as well as organizations.