

VSOCBOX OPERATIONS

Your Log Data is Talking. Are You Listening?

As modern IT environments continue to grow in size and complexity, visibility into IT issues is becoming more difficult as applications, systems, and devices across the network produce larger amounts of log data. Manual approaches to log collection, normalization, and analysis scale poorly, so organizations need a better way to collect and analyze large volumes of log data without creating a heavy burden on IT and DevOps professionals.

Enterprise-class Log Management and Analysis for Improved Visibility

Delivered to you in either a self-managed or cloud-native experience, vSOCBox Operations is a comprehensive log management and analysis solution that helps you centralize, search, and analyze event log data so resource-constrained IT and DevOps professionals can identify performance issues faster, reduce downtime, and streamline operations.

VSOCBOX OPERATIONS AT A GLANCE

Event Log Collection and Analysis for Improved Visibility

Your infrastructure, devices, and applications are generating volumes of log data that can give you insight into the health of your environment. All log data, including syslog, Windows, or VMware® events, are crucial components of the complete picture of your environment,

vSOCBox™

VSOCBOX LTS SECURE OPERATIONS BENEFITS

- Consolidate log data from across your into a centralized repository for analysis
- Scour volumes of data in seconds with lightning-fast search capabilities
- Focus IT performance efforts on what matters by filtering out alert noise
- Increase productivity with automation you can trust for repetitive tasks



and can help with troubleshooting. vSOCBox Operations can collect, normalize, and analyze log data so you can find the root cause of performance issues and bottlenecks faster.

Powerful Search and Filter Capabilities for Easier Troubleshooting

Log data comes at you fast, and locating the right piece of information can be like trying to find the needle in a haystack. vSOCBox Operations is designed to parse terabytes of data in seconds, allowing you to quickly find data in real-time and easily apply color coding to your log data to aid with filtering and identifying performance issues.

Bring Your Log Data to Life with Visualization Capabilities

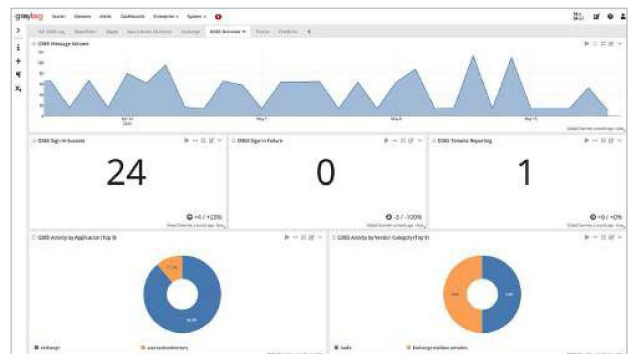
Easily visualize your log data via an interactive stream to identify potential issues as they occur in real time with vSOCBox Operations.

Identify Priority Events in a Sea of Alerts

Getting to the data you need quickly doesn't have to be difficult. vSOCBox Operations make it easy to filter out the noise so you can focus on the events that really matter, reducing alert fatigue and eliminating the need to go outside the platform for additional analysis.

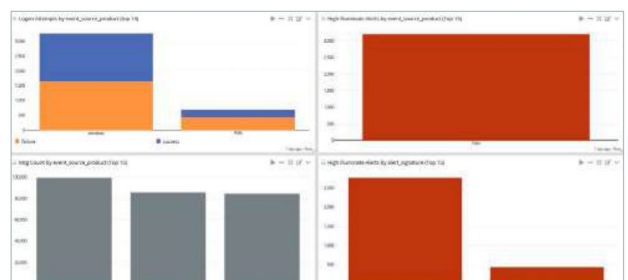
Spring Into Action Quickly with Customizable Alerts & Notifications

Your users shouldn't discover problems before you do. The vSOCBox Operations intelligent alert engine allows you to customize alerts and delivery options, including email and Slack® notifications, and the ability to trigger an external script so you can start fixing issues before they impact your customers.



Out-of-the-box Content Provides Value Quickly

vSOCBox Operations comes equipped with out-of-the-box content to help you streamline IT operations. Start fast with out-of-the-box content like pre-configured search templates, dashboards, correlated alerts, and more and get to the root cause of IT issues faster.



ASK OUR EXPERTS AND SEE VSOCBOX OPERATIONS IN ACTION

Don't just take our word for it. At vSOCBox , we believe you should have a chance to get all your questions answered before you buy. That's why we offer scheduled product demos that demonstrate full product functionality and dedicated time for Q&A. Simply [schedule your vSOCBox Operations demo today](#) & see how easy it is to seamlessly collect, normalize, and analyze your log data to identify performance issues.

VSOCBOX OPERATION FEATURES

ALERTS AND NOTIFICATIONS

Customize alerts and receive them via email, text, Slack®, and more.

ARCHIVING

Archive event logs for analysis and identify trends over time.

CORRELATION ENGINE

Automatically piece together information from different log data to identify potential issues.

FORWARDER

Easily send data to LTS Secure Cloud or to an on-premise LTS Secure Server installation.

ILLUMINATE

Start fast with prebuilt parsers and dashboards leveraging the LTS Secure Schema.

INTEGRATE USING REST API

Easily share data with other business-critical systems for full transparency and collaboration.

INTERACTIVE DASHBOARDS

Combine widgets to build customized data displays and automate the delivery of reports to your inbox.

LOG VIEW

Visualize data in real-time as events occur, ensure continued availability, streamline investigations.

SCHEDULED REPORTS

Leverage LTS Secure's dashboard functionality to easily build and configure scheduled reports.

SEARCH TEMPLATES

Save and share parameterized searches and dashboards.

SEARCH WORKFLOW

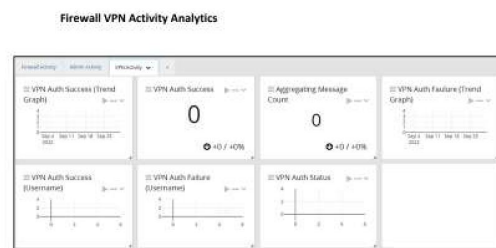
Build and combine multiple searches for any type of analysis into one action.

TEAMS MANAGEMENT

Control entity access and capabilities. Includes LDAP/Active Directory integration.

ABOUT VSOCBOX

vSOCBox is a leader in log management and Security Information Event Management (SIEM), making the world and its data more efficient and secure. Built by practitioners with the practitioner in mind, vSOCBox unlocks answers from data for thousands of IT and security professionals who solve security, compliance, operational, and DevOps issues every day. vSOCBox platform built for speed and scale in capturing, storing, and enabling real-time analysis of terabytes of machine data. vSOCBox eliminates the noise and delivers an exceptional user experience by making data analysis, threat hunting, detection, and incident investigation fast and efficient using a more cost-effective and flexible architecture.



www.vsocbox.com

enquiry@vsocbox.com

201, Tower S4, Phase II, Cybercity,
Magarpatta Township, Hadapsar,
Pune, Maharashtra 411013

2024 vSOCBox, Inc. All rights reserved.