SIEM OPERATIONS EDITION

CRITICAL INSIGHT FOR ENTERPRISE OPERATIONS CENTERS

Trustwave SIEM Operations Edition is the security event management solution for automating enterprise operations centers.

PROACTIVE THREAT MANAGEMENT: YOUR BEST DEFENSE IN THE BYOD AGE

The rapid development and proliferation of mobile operating systems and apps has exponentially introduced new vulnerabilities and legitimate threats into the enterprise ecosystem. BYOD exacerbates this proliferation because organizations no longer have complete control the mobile platform (unlike the case of a mobile company-issued laptop) and cannot guarantee systems have up-to-date configurations.

Trustwave SIEM OE helps ease BYOD support efforts by:

- Detecting highly sophisticated behavioral anomalies and Advanced and Persistent Threats with SIEM's advanced correlation capabilities.
- Automating remediation proactively with SIEM OE configuring and controlling BYOD enforcement technologies including NAC and SWG.
- Reducing risk through lowering of detection and reaction times to BYOD, mobile, and other threat vectors
- Finding the "needle in the haystack" using automated analysis and visualization of real-time events faster than any human inspection.
- Helping you better understand security and compliance threats and risks to your organization through insight into what's happening on your network with business and technical reporting.

SIEM OE offers unique actionable alerts to provide highly refined security intelligence unavailable with other event management tools.

- **Fast, collaborative research:** One-click alert assessments and contextual detail combined with simple drilldown to the parsed and raw events provides a complete picture for any alert under investigation. Alert annotation and guidance promotes understanding among security operator, analysts and other members of the IT team.
- **Elimination of false positives:** SIEM OE draws attention to alerts determined to have an impact on compliance with internal policies or regulatory standards. A configurable nine-factor risk score automatically prioritizes alerts based on the complete picture of history of source and target, vulnerability and asset type, and places greater weight on alerts that have the potential to negatively impact a business.
- **Fast, efficient investigation:** There are never enough eyes to monitor millions of logs or events for critical issues. SIEM OE does the monitoring, encoding and automating the steps an expert takes to investigate an alert.

SIEM, MOBILE SECURITY AND BYOD

SIEM OE is the nerve center of Trustwave's Mobile Security solution. Trustwave secures your BYOD deployment w/ integrated technologies that protect networks, users and data.

Learn more at:

www.trustwave.com/mobilesecurity

INTRODUCING TRUSTWAVE SIEM OPERATIONS EDITION

Trustwave SIEM Operations Edition (OE) is event management software for the enterprise – scalable, flexible and easily integrated with the enterprise infrastructure. SIEM OE automatically transforms logs into security events and prioritizes high risk events, providing actionable alerts to help businesses stay secure and compliant.

Trustwave SIEM OE is a comprehensive enterprise security management solution that simplifies the supervision of security and compliance issues and adapts to any size and any type of security landscape. With unprecedented ability to scale, SIEM OE consolidates and analyzes data from any number of security devices, networks, operating systems, databases and applications without customization. Simple to deploy on one server or distributed on multiple servers across the country or around the world, SIEM OE supports real-time alerting and incident management and reporting.

SIEM OPERATIONS EDITION AND BYOD

In the age of Mobile Computing and BYOD, SIEM Operations Edition helps organizations that need to improve the efficiency and effectiveness of their security operations.

Trustwave SIEM OE is a comprehensive enterprise security management solution that simplifies the supervision of security and compliance issues and adapts to any size and any type of security landscape including BYOD. With unprecedented ability to scale, SIEM OE consolidates and analyzes data from any number of security devices including personal mobile devices, networks, operating systems, databases and applications. SIEM OE supports real-time alerting and incident management and reporting.

SUSTAINING COMPLIANCE: YOUR BEST INVESTMENT

Trustwave provides daily automated value for organizations concerned with regulatory compliance or monitoring the effectiveness of internal controls:

- SIEM OE automatically correlates disparate events to accelerate understanding, calculates a composite risk score and then notifies the team through actionable alerts via e-mail, service management (ticket) integration, or the built-in monitoring console. By accessing the alert details, analysts have on-demand access to recent history about the alert and the network asset, as well as users involved in the base events. When every minute counts, automated assessment equals rapid response.
- SIEM OE employs a consistent set of controls from best practice frameworks like ISO, NIST and CoBit and then monitors control performance. This real-time element increases effectiveness, reduces cost and quickly reflects changes in standards or policy.
- Trustwave provides hundreds of packaged, auditworthy reports. These reports, combined with the report customization wizard, offer the needed analysis without having to know a query language. Automation frees up valuable headcount for more urgent and critical tasks.

WHY CHOOSE TRUSTWAVE

Trustwave solutions and products are designed to meet business needs today and into the future. Trustwave products adapt to enterprise security management processes — our product collects logs from anything located anywhere — including custom applications. More companies and agencies are choosing Trustwave:

- Trustwave features a single source of security information, the Security Data Warehouse (SDW). The SDW is composed of compressed file stores and an optimized relational database that requires no database administrator and provides efficient, affordable storage of logs and events to support searches and automated analysis.
- SIEM OE works with the Trustwave SIEM appliances. This means appliances can be located in remote and even unmanned locations, where they will work alone or with SIEM OE to provide logging and event management for remote offices or separate logical business units. Together, they provide organizations consolidated control of information security.
- All Trustwave products are easily configured to adapt to enterprise business requirements. SIEM OE features active integration and response, which provides quick click access from SIEM OE to any security management product to accelerate and automate response to security incidents. Additionally, SIEM OE sends alerts as trouble tickets to the customer's service management platform and displays the alerts on the enterprise console. SIEM OE makes the most of every dollar spent on securing the enterprise.

LEARN MORE AT TRUSTWAVE.COM

Trustwave®
Smart security on demand

For more information: https://www.trustwave.com