SIEM ENTERPRISE

CRITICAL INSIGHT FOR PROACTIVE RESPONSE AND RISK MANAGEMENT

Trustwave Security Information and Event Management (SIEM) Enterprise provides superior quality and advanced expertise to help you meet compliance requirements, improve your security posture and protect your critical data.

Organizations require the ability to meet today's compliance and security challenges with the flexibility to address tomorrow's evolving needs. Trustwave SIEM Enterprise helps organizations meet their mandates with powerful features to monitor and detect threats and manage risk and compliance controls. SIEM Enterprise provides the critical insight and information needed for organizations to proactively respond and manage risk in easy to understand ways.

NOT OVERLY COMPLICATED—NOT OVERLY SIMPLIFIED

SIEM Enterprise enables organizations to quickly address their compliance requirements and take a proactive approach to their security risk management strategy. Purpose-built with a focus on simplified management, SIEM Enterprise's intuitive, browser-based user interface makes it easy to centrally configure, update and operationally maintain across your environment. SIEM Enterprise is your go-to solution for organizations who want to detect threats and manage risk and compliance requirements—all with little overhead.

ENABLE COMPLIANCE

SIEM Enterprise lets you effectively meet your audit needs with consistent controls based on best practice frameworks and regulatory and industry requirements. And, it's powerful features—including, real-time control monitoring, compliance reporting, automated compliance alerting, notification and scheduling capabilities—ensure your organization stays ahead of the threat curve.

- COBIT
- FISMA (NIST 800-53)
- GLBA

SIEM ENTERPRISE KEY FEATURES AND BENEFITS

Analytics and Intelligence

- Advanced Correlation and Threat Management
- Industry leading correlation engine offers flexibility and configurability to meet your ever-evolving needs
- Correlation capabilities include rule, vulnerability, statistical, historical, heuristic, threat, asset, behavior and risk-based support

Big Data

- Incorporates advancements that address bigger data and analytics challenges
- Features highly scalable, distributed architecture capable of collecting, normalizing, correlating and reporting on more data than ever before

Threat Intelligence

- Integrated advanced warning intelligence provided by our Threat Correlation Service to help you clearly identify emerging threats
- Enables proactive measures to protect your organizational assets and data from theft

Advanced Search and Forensics

- In-depth data at your fingertips with full Boolean logic filtering
- Easily save, share and re-use searches, filters, lists and reports through an easy to use wizard-like interface

Visibility and Reporting

- Over 600 compliance focused reports with more than 2,600 overall reports available across both holistic security and compliance
- Configurable dashboards, correlations and filters to let you quickly gain value and reducing risk
- Reports can be scheduled or run ad-hoc against alerts, events and trend data

OPERATIONS

User Experience

- Familiar browser-based UI design with workflow support for analyst threat monitoring and incident response tasks
- A Finder function greatly enhances the ability to quickly identify events and activity of interest

Operational Maintenance

- Easy to install Data Modules enable standard and customized log acquisition from almost any audit source complemented by automated updates and centralized management

Blended Architecture Support

- Complements existing investments in Trustwave Log Management Appliances to help simplify large and complex deployments

High Availability

- Supports high availability with intuitive browser-based configuration

THREAT CORRELATION SERVICES

Information sharing is a critical component of any defense. Intelligence communities and law enforcement have been collaborating for decades to improve their effectiveness. This enables operations, such as Interpol, to warn organizations around the globe of dangerous criminals and to tighten the law enforcement net. Trustwave Threat Correlation Services (TTCS) employ these same principles by sharing learned information about criminals and known threats with our customers. This information enables organizations to identify possible threats and to monitor with higher scrutiny—before they have a chance to cause damage.

The threat intelligence feeds from TTCS are securely synchronized from the cloud with SIEM Enterprise. SIEM Enterprise applies this knowledge within the advanced correlation engine—automating detection and notification to evolving threats, which might otherwise fly under the radar.

THREAT INTELLIGENCE

Trustwave aggregates information from numerous sources and applies automated confidence algorithms to produce intelligence and reputation data. Our sources of information include:

CROWD SOURCE

- Information on correlated threats from TTCS Crowd Source customers
- May include compromised hosts and malware domain information derived from automated SpiderLabs research and behavioral analysis

OPEN SOURCE

- A large library of openly available information lists, which is consolidated, classified and automatically analyzed to derive intelligence and reputation information with confidence

Sources include:

- Botnet Domains
- Botnet URL's
- Malware Domains
- Malware URL's
- Email Phishing
- Phishing Domains
- Phishing URL's

ENTERPRISE SOURCE

- Powerful correlations available to our SIEM Enterprise and SIEM OE customers
- Correlations derived from best practices and specific configuration settings to meet our customer's local policies and requirements
- Environmental metadata specific to each customer's environment and assets

SERVICE SETUP

Our experts help get you up and running smoothly while maximizing your return on investment. Analyzing your security requirements and working closely with your team, our experts will help with the solution set up and testing as well as provide knowledge transfer on our Trustwave Threat Correlation Service.

Trustwave®

Smart security on demand

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