Trustwave®

Security Information and Event Management

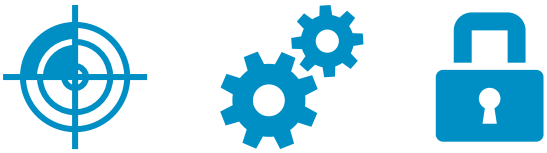
TRUSTWAVE SIEM ENTERPRISE

Trustwave Security Information and Event Management (SIEM) Enterprise unterstützt Sie bei der Erfüllung von Compliance-Anforderungen, der Verbesserung der Sicherheitslage und dem Schutz Ihrer geschäftskritischen Daten. Hervorragende Qualität und fortschrittlichstes Know-how zeichnen das System aus.

Organisationen müssen den heutigen Security- und Compliance-Herausforderungen mit hoher Flexibilität begegnen, um auch für die Anforderungen von morgen gerüstet zu sein. Mit seinen leistungsfähigen Funktionen ist Trustwave SIEM Enterprise ein wertvolles Werkzeug, um Gefahren zu erkennen, einzudämmen und um Risikomanagement- und Compliance-Vorgaben gerecht zu werden. SIEM Enterprise verschafft Ihnen einen besseren Einblick in das Netzwerkgeschehen und automatisiert die Analyse von Informationen, die erforderlich sind, um auf Risiken proaktiv zu reagieren und diese zu managen.

Ausgefeilt, aber unkompliziert

Mit SIEM Enterprise erhalten Sie die Möglichkeit, Compliance-Anforderungen schnell gerecht zu werden. Sie setzen Ihre Risikomanagement-Strategie proaktiv um. Die intuitive, Browser-basierte Benutzerschnittstelle wurde entwickelt, um Aufgaben wie die zentrale Konfiguration, die Aktualisierung und die operationelle Wartung Ihrer Netzwerkumgebung zu erleichtern. SIEM Enterprise ist die Lösung, wenn Sie Gefahren schnell erkennen und Risiken sowie Compliance-Anforderungen managen wollen – und das mit wenig Aufwand.



SIEM Enterprise Dashboard: kritische Daten einfach verfügbar

Ermöglicht Compliance

SIEM Enterprise erlaubt Ihnen die effektive Erfüllung Ihrer Audit-Ziele mithilfe konsistenter Controls, die sich auf Best-Practice-Frameworks, Industrienormen und gesetzliche Vorgaben stützen. Die leistungsfähigen Funktionen – darunter Echtzeit-Überwachung, Reporting, automatische Warnungen bei Compliance-Verletzungen sowie Status-Benachrichtigungen und Planungshilfen – stellen sicher, dass Ihr Unternehmen den Bedrohungen immer einen Schritt voraus ist.

- COBIT
- FISMA (NIST 800-53)
- GLBA
- GPG 13
- HIPAA
- Internal GRC
- ISO 27002
- NERC CIP
- PCI DSS

Key Features und Vorteile von SIEM Enterprise

Analyse und Aufklärung

Fortschrittliche Korrelation und Threat Management

- Die branchenführende Korrelations-Engine ist so flexibel und individuell konfigurierbar, dass sie auch Ihren zukünftigen Bedarf abdeckt.
- Die Korrelationsfunktionen erfassen Regeln, Schwachstellen, statistische Daten, Verlaufsinformationen, Heuristiken, Bedrohungen und Assets. Sie arbeiten verhaltens- und risikogestützt.

Big Data

- SIEM Enterprise ist bereits auf Herausforderungen ausgelegt, die durch Big Data und die Notwendigkeit der Analyse großer Datenbestände entstehen.
- SIEM Enterprise bietet eine hoch skalierbare, verteilte Architektur, die mehr Daten als je zuvor sammeln, normalisieren, korrelieren und in Berichte umsetzen kann.

Bedrohungserkennung und -analysen

- Unser Threat Correlation Service identifiziert aufkommende Bedrohungen und warnt Sie klar und deutlich.
- Ermöglicht proaktive Maßnahmen, um die Assets und Daten Ihrer Organisation vor Diebstahl zu schützen.

Erweiterte Recherche und Forensik

- Gründliche Datenanalyse zu Ihrer sofortigen Verfügung, mit boolescher Filterlogik.
- Assistenten vereinfachen das Speichern, die Weitergabe und die Weiterverwendung von Suchergebnissen, Filtern, Listen und Berichten.

Transparenz und Reporting

- Über 600 Berichtsvorlagen mit dem Fokus „Compliance“ und über 2.600 Berichtsvorlagen insgesamt zu den Themen ganzheitliche Sicherheit und Compliance
- Konfigurierbare Dashboards, Korrelationen und Filter, aus denen Sie schnell Nutzen ziehen und mit denen Sie Ihr Risiko verringern können
- Berichte können vorab geplant oder ad-hoc auf der Basis von Warnungen, Ereignissen und/oder Trenddaten erstellt werden

Betrieb

Benutzeroberfläche

- Die vertraute, Browser-basierte Benutzeroberfläche unterstützt optimal den Workflow beim Threat Monitoring und bei Incident-Response-Fällen
- Eine spezielle Suchfunktion verbessert deutlich die Identifikation von Events und Aktivitäten, die Aufmerksamkeit verdienen

Anpassung und Wartung

- Einfach zu installierende Datenmodule ermöglichen es, auf der Basis von standardisierten und individuellen Protokollen Log-Daten aus praktisch jeder Audit-Quelle zu verarbeiten. Automatische Updates und zentrales Management ergänzen das System.

Unterstützung für gemischte Architekturen

- Ergänzt bestehende Trustwave Log Management Appliances, um komplexen Einsatzszenarien gerecht zu werden und Investitionen zu schützen.

Hochverfügbarkeit

- Unterstützt Hochverfügbarkeit durch intuitive, Browserbasierte Konfiguration.

Das Trustwave SIEM-Produktportfolio

Das Trustwave SIEM-Portfolio bietet eine große Palette an Ansätzen und hohe Flexibilität bei der Erfüllung Ihrer jeweiligen Bedürfnisse – von Log Management und Gefahrenerkennung bis hin zu Alarmfunktionen, Gegenwehr und Abhilfe. Die Trustwave SIEM-Produkte umfassen:

SIEM Log Management Appliances

Vereinfachtes Log Management und Compliance in einer bequem zu verwaltenden Appliance, die mit anderen Trustwave SIEM-Produkten kombiniert werden kann, um Ihren individuellen Bedarf an SIEM und SIM zu erfüllen. Zu den SIEM-Appliance-Optionen zählen:

- Log Management Enterprise
- Log Management Operations
- Log Collector

SIEM Enterprise

Einfache Nutzung und Wartung, überragende Korrelations-, Alarmierungs- und Berichtsfunktionen in einer mächtigen softwarebasierten Lösung. SIEM Enterprise ist die erste Wahl für Organisationen mit hohen Anforderungen.

SIEM Operations Edition (OE)

SIEM OE ist eine fortschrittliche, vollständig individualisierbare Software-Lösung, die sich optimal für Organisationen mit ausgereiften Sicherheits- und Compliance-Programmen und erfahrenem Personal eignet. SIEM OE ist zudem bestens geeignet für Organisationen, die eine individualisierbare, bidirektionale Integration in ihre bestehenden Unternehmensanwendungen benötigen.

Managed SIEM

Die weltweit verteilten, rund um die Uhr besetzten Trustwave Security Operation Centers überwachen Ihre Audit-Geräte und benachrichtigen Sie bei Gefahren und Compliance-Risiken. Verschiedene Service-Level stehen passend zu Ihren Anforderungen zur Verfügung; sie können SIEM-Log-Management und Monitoring sowie personelle Unterstützung zur Verwaltung weiterer SIEM-Lösungen umfassen.

Trustwave SIEM-Portfolio

<table>
<tr><td colspan="3">Log Management Appliances</td><td>SIEM Enterprise Software</td><td>SIEM Operations Edition Software</td></tr>
<tr><td>Log Collector</td><td>Log Management Operations</td><td>Log Management Enterprise</td><td colspan="2">Trustwave Threat Correlation Service</td></tr>
</table>

Das Trustwave SIEM-Portfolio erfüllt alle Ihre Anforderungen, von Log Management und Gefahrenerkennung bis hin zu Alarmierung, Abwehr und Abhilfe.

Threat Correlation Services

Informationsaustausch ist eine kritische, zentrale Komponente bei allen Abwehrmaßnahmen. Geheimdienste und Vollzugsbehörden arbeiten seit Jahrzehnten zusammen, um ihre Effektivität zu steigern. Dies ermöglicht es beispielsweise Organisationen wie Interpol, andere Organisationen weltweit vor gefährlichen Kriminellen zu warnen und das Netz der Strafverfolgung enger zu ziehen. Die Trustwave Threat Correlation Services (TTCS) verfolgen das gleiche Prinzip, indem sie gewonnene Informationen über Kriminelle und bekannte Gefahren an Trustwave-Kunden weitergeben. Mithilfe dieser Informationen können die Organisationen mögliche Bedrohungen identifizieren und ihre Überwachungsmaßnahmen exakter darauf abstimmen – bevor Schaden entstehen kann.

Die Threat Intelligence Feeds des TTCS werden per Cloud sicher mit SIEM Enterprise synchronisiert. SIEM Enterprise wendet die Erkenntnisse in seiner fortschrittlichen Correlation Engine an – mit automatischer Erkennung und Benachrichtigungen zu aufkommenden Gefahren, die ansonsten möglicherweise unentdeckt blieben.

Threat Intelligence

Trustwave führt Informationen aus verschiedenen Quellen zusammen und wendet Konfidenz-Algorithmen an, um aus den Informationen bessere Erkenntnisse und Einschätzungen zu gewinnen. Zu unseren Informationsquellen zählen:

Open Source

- Eine große Bibliothek mit frei verfügbaren Informationen – konsolidiert, klassifiziert und automatisch analysiert, um daraus zuverlässige Erkenntnisse und Reputations-Einschätzungen zu gewinnen

Zu den Quellen zählen:

- Botnet-Domains
- Botnet-URLs
- Malware-Domains
- Malware-URLs
- E-Mail-Phishing
- Phishing-Domains
- Phishing-URLs

Crowd Source

- Informationen über korrelierte Gefahren der TTCS Crowd-Source-Kunden
- Eventuell zusätzliche Informationen über kompromittierte Hosts und Malware-Domains, die aus automatisierten SpiderLabs-Recherchen und Verhaltensanalysen stammen

Enterprise Source

- Leistungsfähige Korrelationen, die unseren SIEM-Enterprise- und SIEM-OE-Kunden zur Verfügung stehen
- Aus Best Practices und spezifischen Konfigurations-einstellungen gewonnene Korrelationen, um den lokalen Anforderungen und Richtlinien unserer Kunden gerecht zu werden
- Umgebungs-Metadaten, spezifisch für die Umgebung und die Assets jedes Kunden

Setup-Dienst

Unsere Experten verhelfen Ihnen zu einem reibungslosen Start, um Ihren Return on Investment zu maximieren. Trustwave-Spezialisten analysieren Ihre Sicherheitsanforderungen und arbeiten eng mit Ihrem Team zusammen, um das Setup der Lösung und die Testläufe zu vereinfachen. Sie lassen Ihnen außerdem wertvolles Wissen über unseren Trustwave Threat Correlation Service zukommen.

WEITERE INFORMATIONEN FINDEN SIE UNTER TRUSTWAVE.COM

Trustwave ist ein führender Anbieter von Sicherheitslösungen für Compliance, Web-, Anwendungs-, Netzwerk- und Datensicherheit, die als Cloud, Managed Security Services, Software und Appliance zur Verfügung stehen. Organisationen, die sich mit dem heutigen, fordernden Sicherheitsumfeld auseinander setzen müssen, erhalten von Trustwave einen einmaligen Ansatz mit umfassenden Lösungen, die das TrustKeeper®-Portal und andere proprietäre Sicherheitslösungen umfassen. Trustwave hat bereits hunderte Organisationen, von Fortune-500-Unternehmen und großen Finanzinstitutionen bis hin zu kleinen und mittleren Einzelhändlern, unterstützt, ihre Compliance zu managen und die Netzwerkinfrastruktur, Kommunikation und geschäftskritische Datenbestände zu schützen. Trustwave hat seinen Hauptsitz in Chicago und weltweite Filialen.

Trustwave®

Weitere Informationen finden Sie unter www.trustwave.com

MIDS_PCI3.1_1015