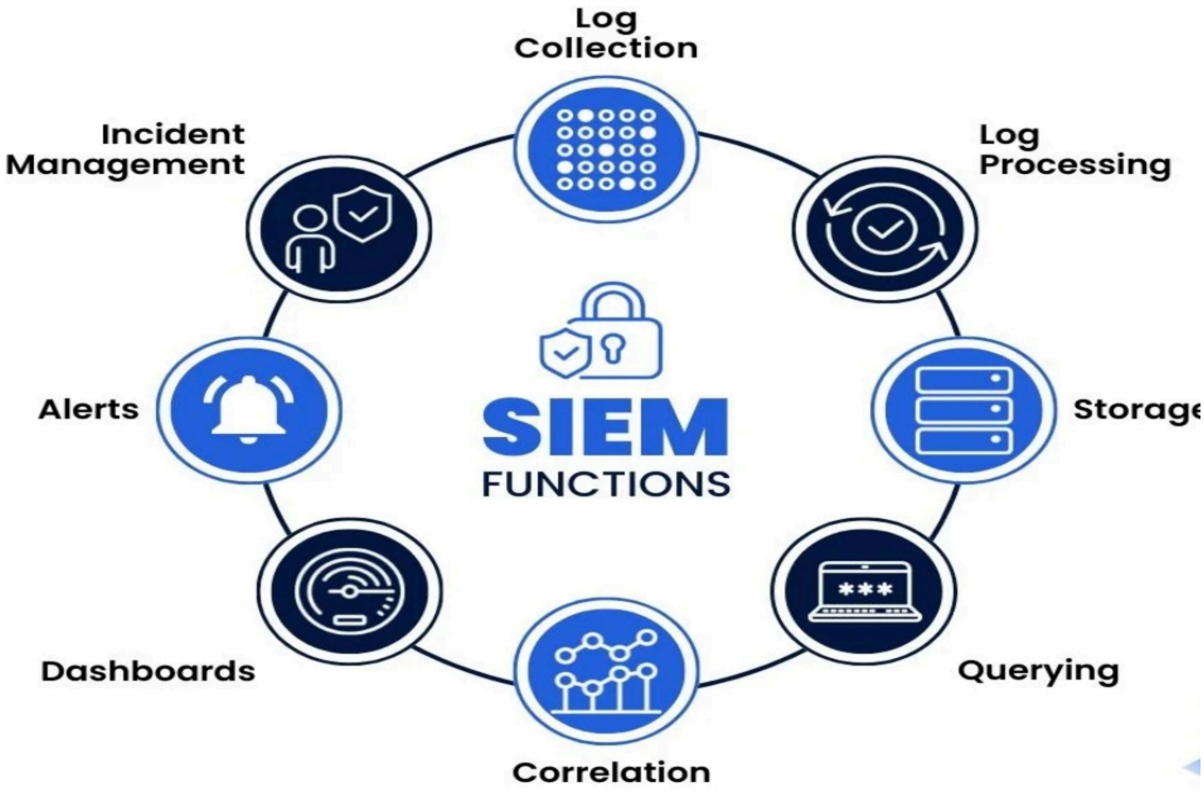
MarcViews Networks Data Sheet

Co-Managed SIEM

January, 2024

Service Overview

Our Co-Managed SIEM service offers organizations the flexibility to leverage the power of a robust SIEM platform while benefiting from the expertise and support of our experienced security engineers. With our co-managed approach, clients retain control over their security operations while gaining access to advanced threat detection, incident response capabilities, and around-the-clock monitoring and support.



Key Features

- □ **Customized Configuration**: Tailored configuration of the SIEM platform to align with the unique security requirements and environment of each client.
- □ **Real-Time Threat Detection:** Continuous monitoring and analysis of security events and logs from various sources, enabling real-time detection of potential threats and anomalies.
- □ **Incident Response Support:** Rapid incident response support from our team of security engineers, including investigation, analysis, containment, and remediation of security incidents.
- □ **Log Management and Retention:** Centralized collection, storage, and retention of security logs and event data for compliance, forensic analysis, and incident investigation purposes.
- □ **Compliance Reporting:** Generation of compliance reports and dashboards to demonstrate adherence to regulatory requirements and industry standards (e.g., GDPR, HIPAA, PCI DSS, PIPEDA).
- □ **Threat Intelligence Integration:** Integration with threat intelligence feeds to enrich security event data and enhance threat detection capabilities.
- □ **Security Analytics:** Advanced analytics and correlation capabilities to identify patterns, trends, and potential indicators of compromise (IOCs) across diverse datasets.
- □ **User and Entity Behavior Analytics (UEBA):** Detection of anomalous user and entity behavior indicative of insider threats, compromised accounts, and advanced persistent threats (APTs).
- □ **Custom Alerting and Notification:** Customization of alerting rules and thresholds based on client-specific security policies and requirements, with timely notifications of critical security events.
- □ **Dashboards and Reporting:** Customizable dashboards and reports providing visibility into security posture, incident trends, and operational performance metrics.

Ben[1]efits

- □ **Enhanced Security Posture:** Strengthened security posture through proactive threat detection, incident response, and continuous monitoring.
- □ **Expert Support:** Access to a team of experienced security engineers for guidance, support, and expertise in managing and optimizing the SIEM environment.
- □ **Cost-Efficiency:** Cost-effective alternative to building and maintaining an in-house SIEM capability, with predictable pricing and flexible service options.
- □ **Scalability:** Scalable solution that can accommodate the evolving needs and growth of the organization, without the burden of managing infrastructure and resources.

Technical Specifications:

- □ **SIEM Platform:** Industry-leading SIEM platform with advanced features for log management, event correlation, and threat detection.
- □ **Deployment Options:** Flexible deployment options including on-premises, cloud-based, or hybrid configurations based on client preferences and requirements.
- □ **Integration Capabilities:** Integration with a wide range of security devices, applications, and platforms for seamless data collection and analysis.
- □ **Data Encryption:** Encryption of sensitive data both in transit and at rest to ensure confidentiality and integrity of security event data.

+1-289-374-6454 **www.marcviews.com**

[1] Copyright © 2024 MarcViews Networks, Inc. All rights reserved. Co-Managed SIEM service is provided in collaboration with MarcViews Networks' team of certified security engineers and analysts. While clients retain control over their security operations, MarcViews Networks offers expertise, support, and guidance to optimize the SIEM environment, enhance threat detection capabilities, and improve overall security posture. Service availability and features may vary depending on the specific service level agreement (SLA) and client requirements. For more information, please contact MarcViews Networks' sales.