Datasheet

VIETTEL SECURITY INFORMATION & EVENT MANAGEMENT (VCS - CyM)

CHALLENGES

- Overwhelming Volume of Data makes it difficult to identify and prioritize critical vulnerabilities that require immediate attention.
- Limited Time & Resources lead to delayed responses and increased risk of breaches.
- Complex and Inefficient Log Collection and Analysis.

Viettel Security Information & Event Management (VCS-CyM), a self-developed product by Viettel Cyber Security company, empowers businesses to overcome security challenges by providing a comprehensive suite of tools enabling security operation teams to proactively manage complex IT security infrastructures.

VCS-CyM centralizes log management by collecting, standardizing, storing, and correlating all logs and cybersecurity events across an organization's IT systems. This comprehensive data allows for real-time search, monitoring, analysis, and visualization of operational data generated by all devices within the network.



BENEFITS

Prioritize Vulnerability Handling - Real-time Comprehensive Monitoring

- Effortless Deployment Flexible Scalability
- Efficient Investment Centralized Management
- Continuously Updated Threat Intelligence
- Experienced Team of Experts

KEY FEATURES

Search and Investigate

VCS-CyM's user-friendly search interface allows defining search criteria in natural language. You can effortlessly expand or narrow results during security monitoring and investigations, while also viewing raw event and warning data for comprehensive analysis, even when encountering standardization issues.

Customizable Correlation Analysis

VCS-CyM comes equipped with over 1000 pre-built correlation rules for real-time anomaly detection & system analysis. These rules can be customized, added, modified, or deleted to suit specific customer requirements and use cases. Additionally, customers can easily enable or disable rules based on their preferences. Moreover, seamless import & export functionalities facilitate convenient storage & updates of organization-specific rule sets.

Data Storage Optimization

VCS-CyM delivers a real-time alerting dashboard that prioritizes notifications based on attack severity and target impact. Leveraging rapid log collection, processing, and analysis, the system generates alerts in under a minute, even for large-scale environments handling up to 60,000 events per second (EPS).

Real-Time Alerting

VCS-CyM employs a robust data storage system that is indexed, backed up, and designed for efficient retrieval in case of incidents. To optimize performance and cost, the system supports flexible storage policies across various storage types.

Data Collection & Standardization

VCS-CyM collects security logs from various sources (servers, devices, applications, etc.) via syslog, API, JDBC, or agents. The system analyzes and removes redundant data, standardizes & classifies it according to a common format optimized for analysis. The system also allows for storing original raw logs for future investigation & tracing.

Intuitive and User-Friendly Dashboard

VCS-CyM collects security logs from various sources (servers, devices, applications, etc.) via syslog, API, JDBC, or agents. The system analyzes and removes redundant data, standardizes & classifies it according to a common format optimized for analysis. The system also allows for storing original raw logs for future investigation & tracing.

Datasheet

VIETTEL SECURITY INFORMATION & EVENT MANAGEMENT (VCS - CyM)

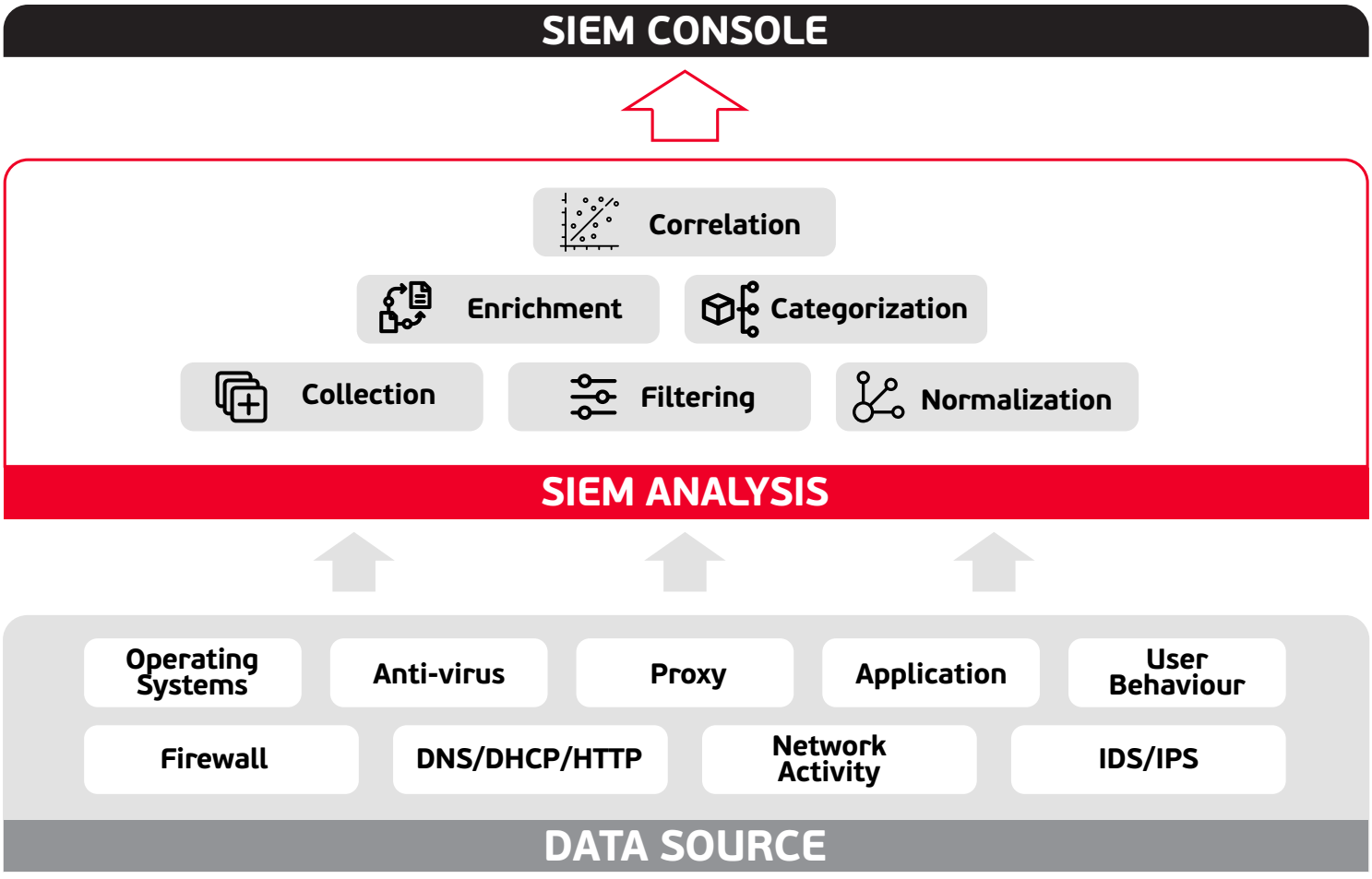
Log Source Management

VCS-CyM provides a comprehensive log source management interface that enables proactive onboarding of new applications and devices, ensuring comprehensive system monitoring. The system also supports real-time status and EPS monitoring for each log source, facilitating early detection of log ingestion issues that could lead to log loss or gaps.

Continuous Updates

VCS-CyM is committed to continuous improvement and innovation, ensuring that customers always benefit from the latest features, rule sets, and security knowledge. Updates are delivered regularly through product releases, keeping the system at the forefront of cybersecurity defense.

DEPLOYMENT MODEL



Three layers of data processing in the architectural model of VCS-CyM

Data Source layer

Acting as the raw data source, this layer gathers comprehensive data from various IT infrastructure systems, including operating systems, applications, antivirus solutions, network devices, security devices (firewalls, proxies, IPS/IDS) & user access logs maintained by the organization's IT system administrators.

SIEM Analysis layer

Data analysis system layer ingests data from Data Sources, data is normalized, classified, and undergoes correlation analysis across multiple dimensions to detect signs and unusual behavior within the system.

SIEM Console layer

This layer functions as a front-end system, providing users with an interface to operate, monitor, and handle alerts, violations, and conduct searches and investigations within the system.