Datasheet

Viettel Security Information & Event Management

VCS-CyM

Security Information and Event Management (SIEM)

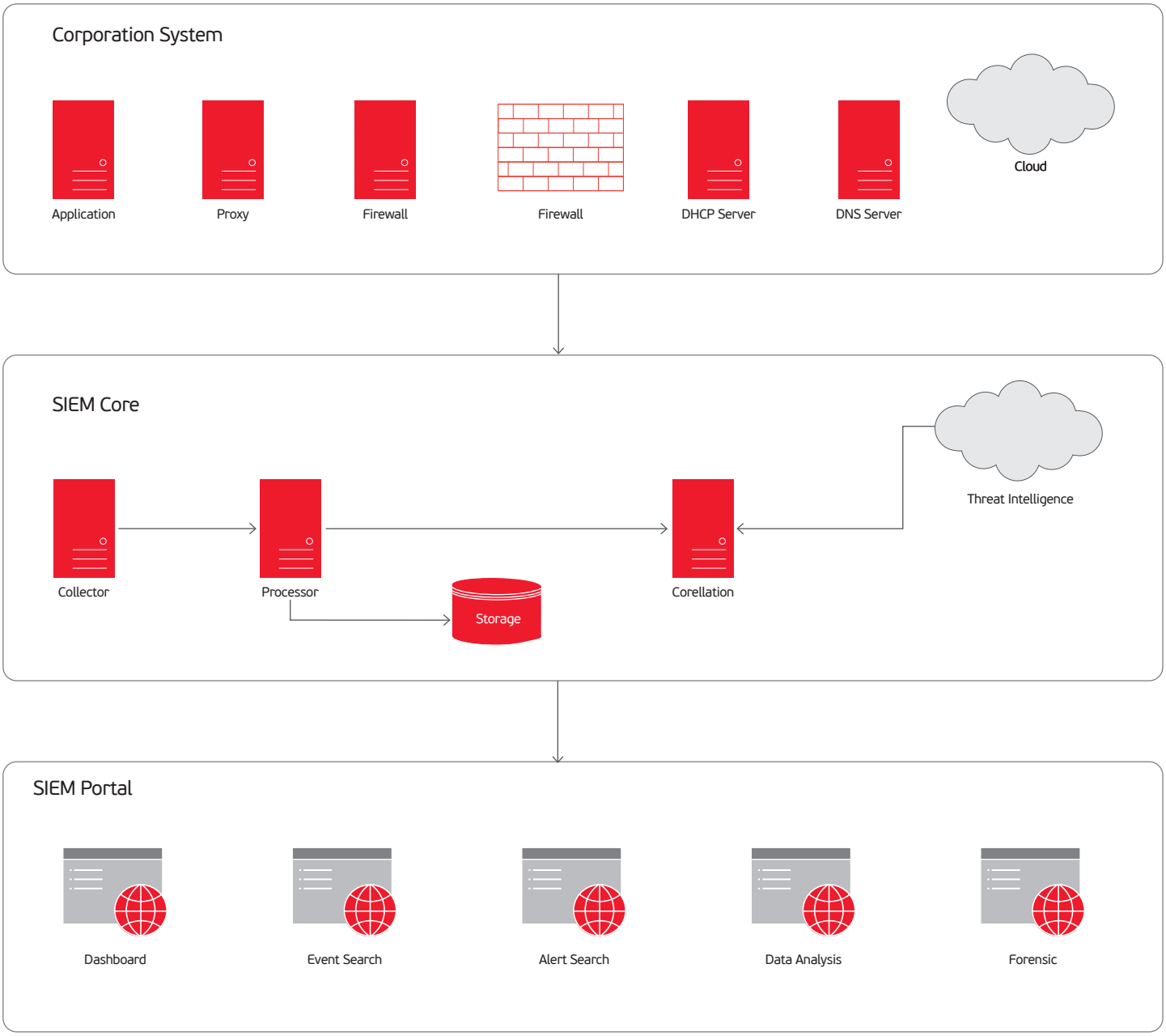
Security Information and Event Management (SIEM) is a solution for centrally collecting, storing and processing security data.

This solution can collect and comprehensively monitor the security data in the system, analyze the correlation in real time to detect anomalies and cybersecurity threat, so that the organization can handle these problem promptly.

Benefits

- Monitor all components in the system: server, applications, devices
- Monitor in real-time
- Operate as centralized management
- Use familiar search language
- Highly customizable suitable for many types of organizations
- Security knowledge is constantly updated
- Supported by a team of experienced professionals
- Flexible deployment architecture, easy to scale according to the system's scale

Operational Structure of SIEM System



Datasheet

Viettel Security Information & Event Management

VCS-CyM

Search and Investigate

VCS-CyM delivers a friendly search interface and user-defined search terms, similar to human language. With the actions right on the interface, users can easily expand or narrow the search terms, making it convenient and fast to search events and alerts during monitoring and investigation.

Log Source Management

VCS-CyM provides a log source management interface that allows users to easily add new applications or devices to the system, ensuring continuous monitoring of the organization's system.

Correlation

VCS-CyM provides nearly 1000 rules to detect anomalies in the system. Users can also customize and add new laws depending on the demand of their business.

Auto Update

VCS-CyM can automatically update users with new versions, new laws, and new knowledge, helping users to comprehensively monitor their systems.

Deployment

VCS-CyM can be deployed centrally or distributed depending on the size of the customer system. It can also be expanded and upgraded easily.

Real-time Alerts

VCS-CyM provides a real-time alert monitoring interface, the alerts are prioritized depending on the severity of the attack type as well as the target being attacked. This helps monitor to prioritize the problems to handle for the best results.

Optimize Data Storage

VCS-CyM provides a data storage system that is indexed and backed up to carefully preserve all data, serving the investigation and tracing process in case of problems. The storage system can be customized according to the size of the customer system.

Device Support

VCS-CyM provides standardizers available for more than 100 types of popular applications and devices. As for new types of applications and devices, the system has a ready-made interface to add their standardizers easily, and then automatically updates for users.

Visual Monitoring Dashboard

VCS-CyM visualizes data into the dashboard for users to easily get an overview of the problems in the system.

Based on dashboards, according to each business, the monitor can immediately identify system problems or attacks right from their system access stage. In addition to the default dashboards, users can also create their own dashboards and easily customize with the demand of their organizations.