Datasheet

Viettel Security Operation Center Platform
(VCS-SOCP)

viettel security

The necessity of Viettel SOC Platform

In the context of increasingly developed information technology, digital transformation takes place in all types of organizations, building a solution which is highly customizable, flexible and suitable for both large as well as medium and small-sized businesses becomes challenging. The use of many cyber security tools and a shortage of human resources are leading to ineffective optimization and troubleshooting. To solve this problem, the solution of Security Operation Center Platform - Viettel SOC Platform is developed based on the integration of various solutions, supporting quick deployment and easy expansion on one single platform. The solution is designed to be highly modular, supporting clients to focus on monitoring, analyzing and comprehensively controlling information security incidents.

Viettel SOC Platform

Viettel SOC Platform is a comprehensive centralized solution, which allows integrating various solutions including the existing cyber security solutions of the organization, with following comprehensive monitoring and managing abilities:

- Provide comprehensive security on Endpoint, Network layers and other systems.
- Collect logs, apply centralized management and send fast and on time alerts from different databases.
- Automatically analyze, investigate, trace based on available playbook, save time and utilize cyber security intelligence of VCS.
- Allow organization to customize playbook and workflows.
- Allow integrating solutions on a single platform, save deployment time and optimize investment cost for organization.
- Use Machine Learning to analyze and handle attacking data.
- Provide cyber security intelligence fast and opportunely.

VIETTEL SECURITY OPERATION CENTER PLATFORM



Endpoint Security | Network Security | Security Information & Event Management | Security Orchestration, Automation & Response

Viettel Threat Intelligence

Key points

Easy onboarding

Sign-in

- 2-factor authentication sign-in
- Support SSO, SLO standard
- Allow centralized sign-in.

Tenant management

- Guarantee the multi-tenancy architecture
- Support authentication, limit the connection and data transmission speed

User management

- Add/Edit/Remove/Reset passwords of users

Centralized and comprehensive monitoring

Manage and monitor the entire system: log tracking and analysis, infrastructure management and customer service

- Provide an enclosed incident monitoring display.
- Provide agents' status monitoring.

Investigation and Response

Provide feature to aid customers investigate and respond to abnormal activities

- Look for events to investigate when incidents occur
- Provide computer isolating & process blocking features
- Provide data visualized tools to support trace tracking

Dashboard

Provide the management tools on dashboard for comprehensive and complete system monitoring

Report

- Provide and create reports of KPI and Service Level Agreement (SLA) for ticket
- Automatically send periodical reports to clients
- Allow customizing the report

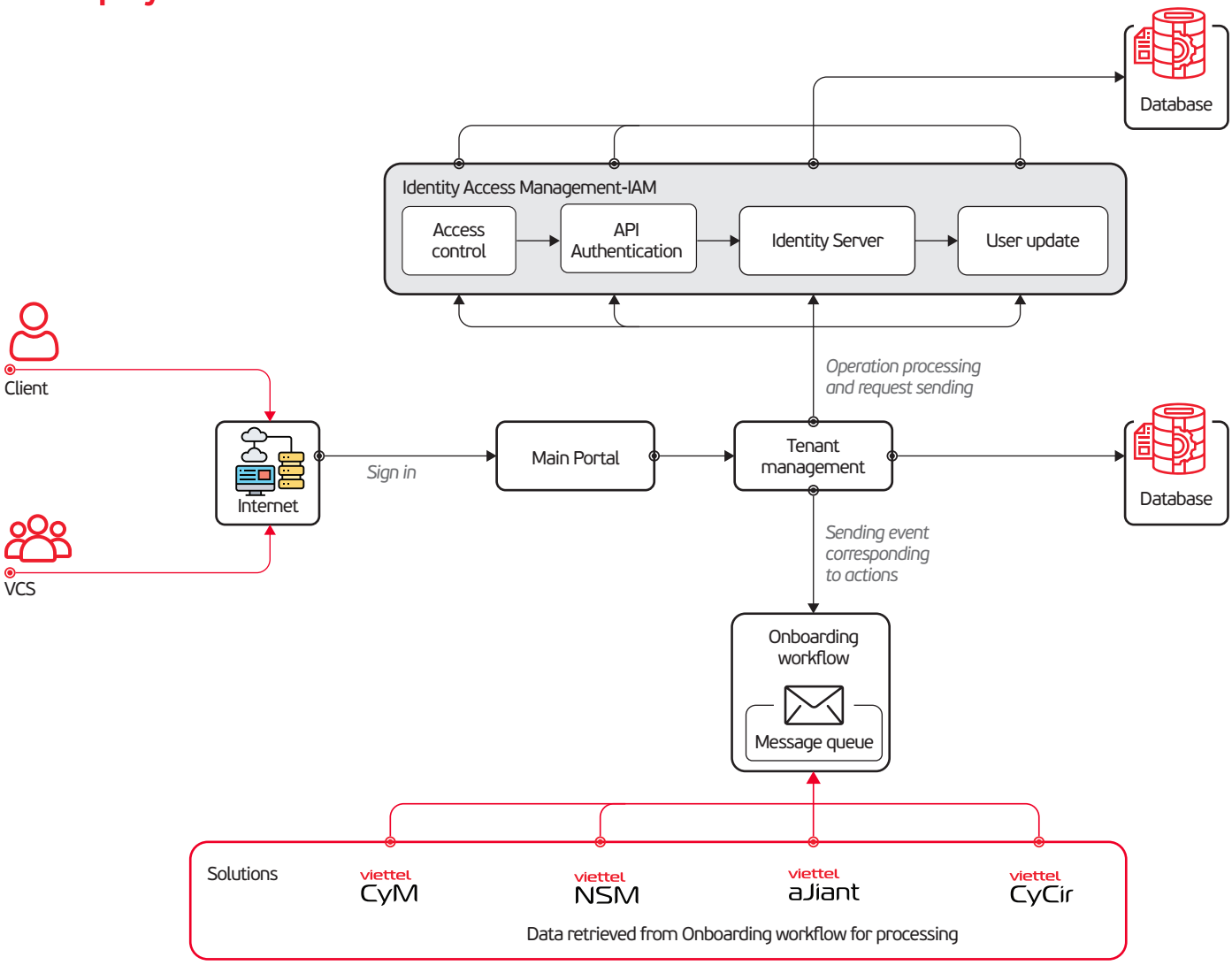
Flexible deployment model

Provide the solution based on the requirements & administration model of each organization including:

- On-premise
- Cloud
- Hybrid

Viettel Security Operation Center Platform (VCS-SOCP)

Model deployment



Elements of the system:

- IAM: Identity Access Management
- Main Portal: Links to solutions in the system, users and tenants management
- Element solutions support the multi-tenant system such as: Viettel Endpoint Detection & Response (VCS –aJiant), Viettel Network Security Monitoring (VCS – NSM), Viettel Security Information & Event Management (VCS-CyM), Viettel Security Orchestration, Automation & Response (VCS-CyCir).

HIGHLIGHTS

1. Allow centralized and comprehensive monitoring, analysis, investigation and processing on a single platform.
2. Apply centralized management, decentralization and user identifying synchronization on tools.
3. Provide the Integrated platform to expand Viettel Network Security tools and available tools which are compatible for the organization to optimize investment and operating costs.
4. Deploy flexibly on On-premise, cloud and hybrid.
5. Utilize machine learning, automatize attack scenario and procedure, reduce troubleshooting time.
6. Allow customizing workflows based on the organization's requirements.