Viettel Security Orchestration, Automation and Response

viettel security

Necessity of the Solution

In the context of information technology (IT) development, cyberattacks are becoming more diverse both in scale and purpose, resulting in a continuous increase of damages caused by cybersecurity incidents according to consecutive annual reports. The increase in the number of cyberattacks leads to a proportional increase in the workload of the cybersecurity team for each organization. Consequently, resource overloads occur and decreases productivity.

Additionally, using separate tools and solutions to monitor and respond to cybersecurity also causes other challenges for theorganization such as:

• Too many duplicate alerts for the same object due to independent and heterogeneous operating solutions.
• Lack of insight in the investigation and response process.
• Too many manual processing steps, affecting the quality of work.
• Lack of skilled personnel to operate and master information security tools.

The above challenges lead to the inevitable need of organizations to find a platform to help improve the efficiency of the operation process and respond to cybersecurity incidents.

Viettel Security Orchestration Automation and Response Solution (VCS-CyCir)

VCS-CyCir, a security orchestration, automation and response solution, is responsible for defining, prioritizing and standardizing incident response functions. Built on automation technology with the integration of security and information technologies according to dynamical playbooks, VCS-CyCir helps organizations optimize efficiency in the process of managing and operating cybersecurity systems.

Benefits of the Solution

1. Maximize the efficiency of incident operation, monitoring and response.
2. Automate and standardize response processes.
3. Reduce operating load and improve working efficiency.

Highlight Features of the Solution

Coordinate all Cybersecurity Solutions

VCS-CyCir allows separate security tools to work smoothly together to improve productivity in complex security processes. In addition to supporting many popular tools and playbooks, VCS-CyCir also provides customization capabilities to integrate security technologies and develop playbooks according to the organization's needs.

Automate the Operation of Cybersecurity

The workflow engine integrated in VCS-CyCir provides the ability to automate sequence of actions already defined in playbooks in seconds, instead of hours when done manually. This reduces the effort spent on repetitive tasks to improve incident response performance. This engine also allows users to monitor and intervene in the automatic processing flow if necessary. Besides, VCS-CyCir provides an intuitive interface for users to build playbooks by using the existing support interface or creating new playbooks in Python language.

Manage Incident and Coordinate Operation

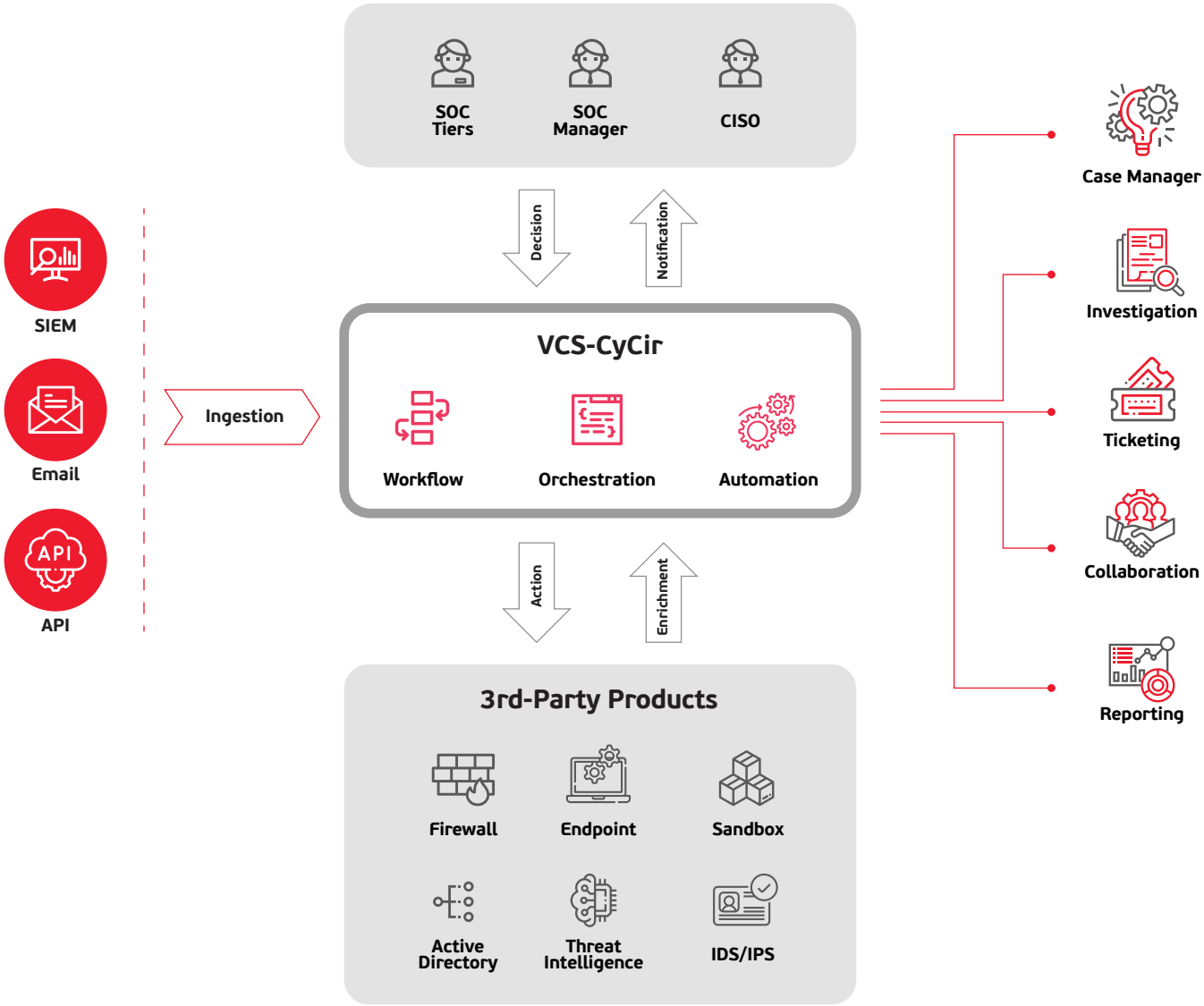
VCS-CyCir keeps track of all information during investigation, response and synthesis, in order to provide analysts with a single centralized administration interface. They can gain a comprehensive view about incidents, shorten analysis time, and make effective decisions for incident response. The management information includes:

• **Operational coordination**: Team members can easily interact on specific issues in each case to quickly make decisions or assign work to the right person.
• **Cybersecurity threat intelligence management**: With integration with cybersecurity intelligence platforms, VCS-CyCir manages and delivers incident-related threats intelligence proactively and intuitively for analysts, helping to optimize analysis and incident.
• **Support for investigation and tracing**: VCS-CyCir provides users with the most convenient and optimal toolkit for investigation and tracing of cyber attacks.

Provide Dashboard and Cybersecurity Report

VCS-CyCir supports tools to extract specialized reports and dashboards for all 3 user groups of the organization: Analyst, SOC Manager and Chief Information Security Officer (CISO). All events and actions are stored to help the organization measure the effectiveness of the SOC operation team from many different perspectives.

MODEL OF DEPLOYMENT AND OPERATION OF VCS CYCIR



- **Data Source layer:** Include solutions and APIs that serve as input alerts for the VCS-CyCir system.
- **3rd Party Products:** Include cybersecurity technologies and solutions integrated with VCS-CyCir. These products support data enrichment in the process of investigation and analysis; and recommend specific actions for other cybersecurity solutions in the system to respond to cybersecurity incidents.
- **VCS-CyCir Core Engine:**
  - Workflow: Define and automate cybersecurity operating procedures.
  - Orchestration: Integrate and coordinate security technologies to work together.
  - Automation: Automate manual tasks during cybersecurity operation.