Datasheet

Viettel Vulnerability Space

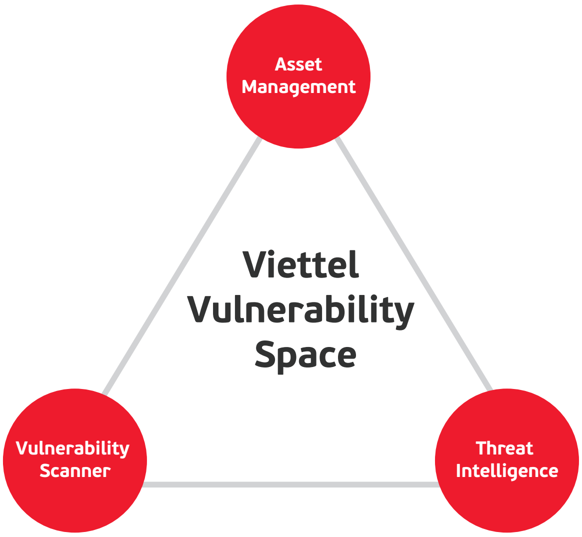
VCS-V2S

viettel security

Overview

Viettel Vulnerability Space is a solution that allows periodically identifying, classifying, prioritizing and minimizing security vulnerabilities of software versions on PC, Server, etc. to support security management and monitoring process on the client network.

Necessity of VCS-V2S



1. Provide a way to support the integration of information from popular Vulnerability Scanner systems, thus improving the ability to identify vulnerabilities and taking advantage of client's available resources.

2. Provide integration with many popular Threat Intelligence with the aim to quickly identify and react to new threats appearing on the Internet.

3. Periodically review and identify vulnerabilities and threats on the network. Provide an overview of them in the client's network.

4. Push alerts of high-level risks and vulnerabilities on computers to 3rd party ticket operation flows.

5. Provide customized process to verify vulnerability information and improve alert accuracy for operation and handling.

Main features

Data integration

- Support integration with popular scanner systems in the world such as Nessus, Acunetix, Nmap, Rapid, etc.
- Ability to integrate and receive alerts from many Threat Intelligence products around the world.
- Easily integrate organizational assets including: Computing Device, Service, Software, Person, Group through Rest API, File, etc. for the purpose of managing and giving accurate alerts.

Control

- Configure and periodically perform automatic network vulnerability scanning through scanner controlling.
- Automatically identify computers at risk of losing security on the network based on Threat Intelligence alerts.
- Periodically review high-risk vulnerabilities which already existed on the network and push alerts.

Report

- Give an overview of vulnerability on the network across multiple perspective, support vulnerability information reports in many forms and uses.
- Reporting and statistics of important data on the impact of security vulnerabilities in the organization, supporting the analysis and operation of information security.

Alert and operation

- Integrate and push alerts of subjects at risk of losing information security on the network to 3rd party Ticketing systems.
- Push alerts through multiple channels such as REST API, Redis, Kafka, etc.

Verify security vulnerability information

- Develop a process to verify information, determine the actual number of exploitable vulnerabilities on the network based on expert knowledge.
- Support automatically vulnerability information verification based on operating history and analysis process.

Advantages

01 Compatible with many different Threat Intelligence and Scanner systems.

02 Periodically review threats, not just prevent new ones.

03 Centralized control portal for the whole process.

04 Professional vulnerability management process from identification > verification > management and handling support.

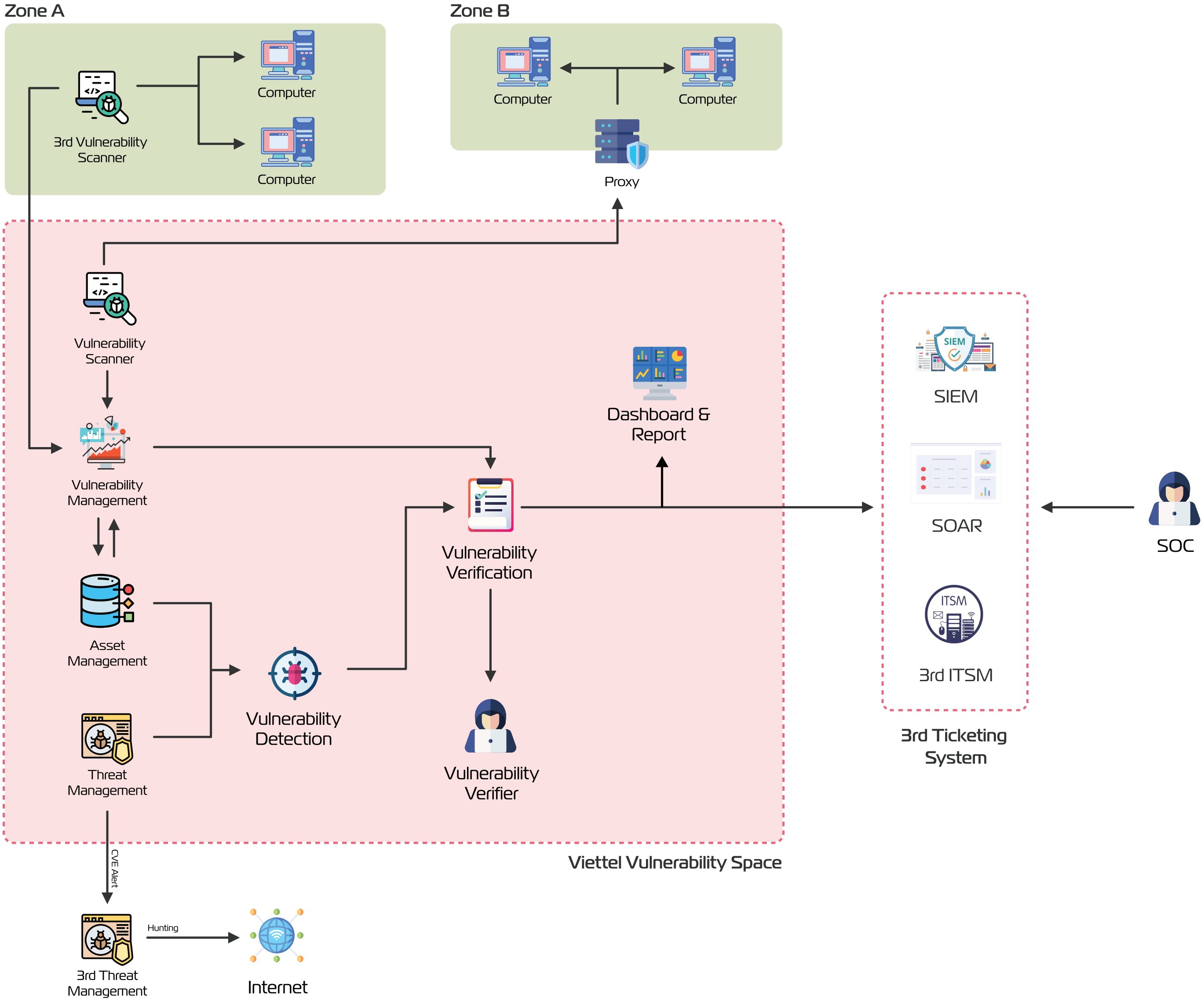
Viettel Cyber Security

For more information, go to ▸ www.viettelcybersecurity.com

FS PF BeauSans Pro

viettel security

Model and operation



1. Threat Intelligence system: Including Viettel Threat Intelligence systems (deployed at Viettel) and possibly client's available ones to push CVE alerts to Vulnerability Space system.

2. Scanners:

- Scanners located in the client zone: either Viettel's scanners located in the client zone for vulnerability scanning or client's available ones, with the aim to scan for vulnerabilities in the network and push information back to the Vulnerability Space system.
- Scanners located at Server Vulnerability Space: Support to remote scan for vulnerabilities in client's network areas, through a reverse proxy.

3. Vulnerability Space System: Centralized vulnerability management system, which collects vulnerability information from scanners, early identifies vulnerabilities in client's asset file based on early alerts from Threat Intelligence, periodically scans for vulnerabilities and threats on asset file, and provides vulnerability information on devices.

4. Vulnerability Verify: The process supports verifying vulnerability information on assets, identifying ones that are actually exploitable on the network to provide accurate information for SOC to operate.

5. Vulnerability Verifier: The operation team verifies vulnerabilities based on the information of vulnerability and client's asset file.

6. 3rd Ticketing System: 3rd ITSM systems (SIEM, SOAR, JIRA, etc.) of clients to creat tickets which deal with vulnerabilities, and measure performance KPIs.

7. SOC: Alert operation team, who generate tickets and send to handlers.