Datasheet

Viettel Network Security Monitoring

(VCS - NSM)

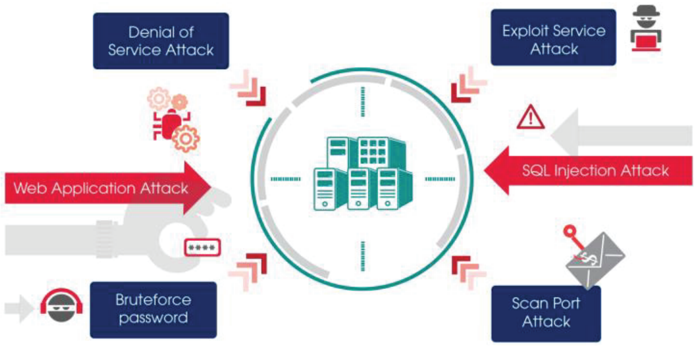
viettel security

Necessity of solution

Cyber attacks have been increasingly diverse in scale and purpose, which are not merely acts of systems intrusion, information exploitation for personal purposes but also organized attacks fueled by economic and political motivations. Advanced persistent attacks can be organized, dedicated types of malware are created to break an organization's security systems. These attack threats are briefly called as APT (Advanced Persistent Threats). These attacks often cause serious damages to organizations for a long time without being detected.

To solve the problem of APT prevention, it is necessary for organizations and businesses to have a continuous network monitoring solution to detect anomalies, attack signs against their information systems.

Viettel Network Security Monitoring (VCS - NSM)



VCS -NSM is a solution with sensors that monitor alerts of attacks on organizations' network layer.

The solution is able to monitor network traffic in real-time and analyze packets to issue alerts about attacks scanning and mining vulnerabilities of applications and services targeting IT systems of governing units. NSM is deployed simply and quickly without any influence on services and applications in network infrastructure

KEY FEATURES

PACKET EXTRACTION AND ANALYSIS

The DPI technology is applied to extract packets, analyze and detect anomalies in the network along with common protocol decoders and automated malware analysis technology on the HyperVisor platform (Sandboxing), the solution provides a new, optimal and fully automated malware detection platform.

IVERSE AND CONSTANTLY UPDATED CODE

The solution is integrated with a code detecting various abnormal behavior groups on network layers and constantly being updated to be able to detect the latest attack signs including abnormal behavior groups such as Network Scan, Trojan Activities, Shellcode Detect, Web Application Attack, Suspicious Login, etc.

Moreover, the solution is combined with a code correlating abnormal signs during the investigation of APT attacks to link the smallest events on network layers and detecting potential attack signs disguised under queries to servers.

CYBER ATTACK DETECTION

The system is able to detect various types of attacks from common types based on signatures to advanced, disguised and hidden attacks such as APT. The solution includes a number of outstanding features in terms of cyber attack detection:

- Detecting attacks scanning passwords in network.
- Detecting denial-of-service attack signs.
- Detecting attack signs scanning vulnerability.
- Detecting web application attack signs (SQL Injection, XSS, etc.).
- Detecting APTs.
- Detecting signs of scanning network information.
- Detecting signs of mining services

SUPPORT FOR IN-DEPTH INSPECTION AND

The NSM solution provides a set of tools assisting administrators and experts with in-depth investigation, review and analysis of cyber incidents, including:

- Reviewing connections related to a cyber attack sign.
- Reviewing connections related to an address and a computer within network.
- Supporting the regeneration of connections and queries within network in the form of PCAP to serve in-depth investigation and analysis

ADVANTAGES

1. CENTRALIZED ADMINISTRATION THROUGH WEB PORTAL
2. DETECTION OF CYBER ATTACKS IN REAL-TIME
3. IDENTIFICATION OF VARIOUS TYPES OF ATTACKS
4. INTEGRATION WITH OTHER IT SOLUTIONS
5. OPTIMAL SUPPORT FOR IN-DEPTH INVESTIGATION AND ANALYSIS
6. FLEXIBLE DEPLOYMENT AND SIMPLE EXTENSION WITH OUT-OF-BAND MODEL

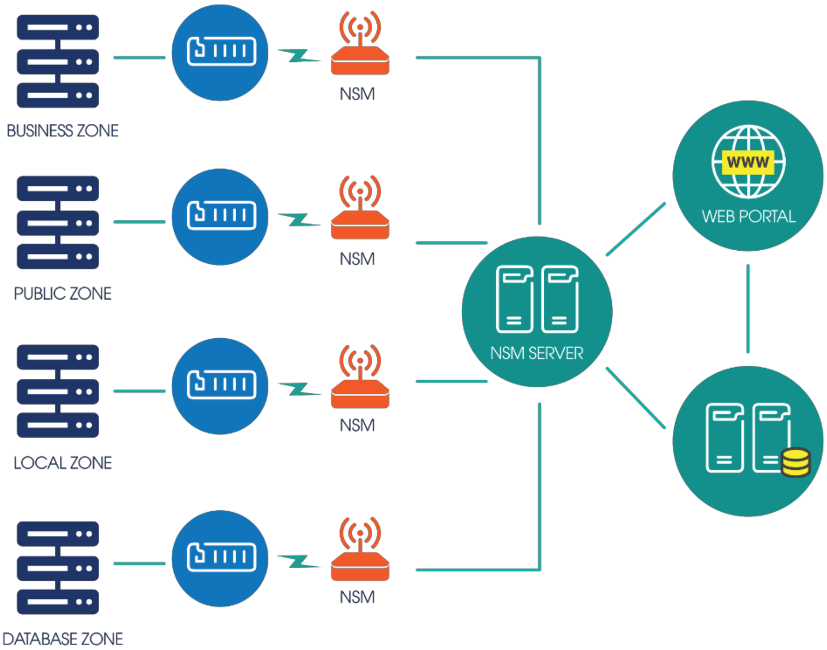
DEPLOYMENT MODEL

The NSM includes 3 main components: NSM Sensor, NSM Server and NSM Web Portal. Where:

- **NSM Sensor:** Refers to sensors collecting and analyzing network traffic, deployed in each network domain of organizations. Network traffic in relevant network domains will be configured port mirroring to NSM sensors, therefore, the organization's data is not be influenced.

- **NSM Server:** Refers to a server controlling, analyzing, and linking data of related events processed and collected by NSM Sensors, thereby giving alerts on potential cyber attacks against organization's system.

- **NSM Web Portal:** Refers to an interface managing and displaying alerts processed and collected from NSM Server.


BUSINESS ZONE
NSM
PUBLIC ZONE
NSM
LOCAL ZONE
NSM
DATABASE ZONE
NSM
NSM SERVER
WWW
WEB PORTAL