Datasheet

Cybersecurity Threat Hunting Service

viettel security

NECESSITY OF THREAT HUNTING

In recent years, cybersecurity attacks have increased in both number and sophistication level. Security threats and malware can cause significant damage to the reputation and finances of the business.

Businesses and organizations are making efforts to build a cybersecurity system with tight security and the ability to detect attacks early. However, according to a recent research, a large number of cyber threats still go undetected.

Therefore, the Threat Hunting Services help to detect and prevent malware, uncover advanced threats hiding within the organization.

VIETTEL THREAT HUNTING SERVICE

The Information Security Threat Hunting service (Threat Hunting) of Viettel Cybersecurity Company uses proactive threat hunting techniques carried out by highly qualified and experienced security experts.

Service benefits:

- Proactive detection of malware and potential cybersecurity threats in the network, even when the threats are beyond the control of security software and solutions, in order to limit the risk of incidents.
- Increase in response speed to security threats; decrease in cost and time of digital investigation.
- Regular updates, supplement and improvement for security systems. Increase in knowledge about the organization's network system for IT
- and information security personnel.
  Improvement in knowledge and professional skills for the in-house
- cybersecurity team.

SERVICE HIGHLIGHTS

Global Threat Collection and Analysis

The Viettel Threat Intelligence system continuously collects information about global cybersecurity threats from a number of sources such as the Internet, underground fraudster communities, as well as internal Viettel monitoring systems. This information is used to conduct a vulnerability assessment of the system. The threats include:

- Cyberattack groups and campaigns
- Types of malware
- Security vulnerabilities
- Threats of data leak
- Other security threats

Network Data Collection

Viettel experts collect network data, directly on systems or through available SIEM solutions, in order to analyze and detect malware and security threats. The data includes:

- Log on host (Event Log, audit log, file list, etc.)
- Log network (NSM, NetFlow, etc.)
- Log security solutions (Firewall, IDS/IPS, Antivirus, etc.)
- Log applications (Web, Database, DNS, LDAP, etc.)

Scan to Detect Malware and Threats

Based on collected network data and global risk information, and combined with interactive Machine Learning – Viettel iML, Viettel experts conduct in-depth scans including:

- Review according to network attack techniques, standardize according to the framework MITER ATT&CK.
- Review according to signs of intrusion identified by Viettel Threat Intelligence system.
- Review according typical signs of APT attacks.
- Review according to machine learning results of Viettel iML solution.

In-depth Analysis and Digital Investigation

When detecting malware and threats, Viettel experts implement malware analysis, in-depth exploitation code, digital investigation on suspected computers, collected logs, and identify:

- Time, origin, cause of infection
- Types of malware, malicious behavior
- Control server, attack infrastructure
- Group, related attack campaign

Rapid Incident Response

After in-depth analysis, Viettel experts propose a solution for troubleshooting and quick response to detected malwares and threats:

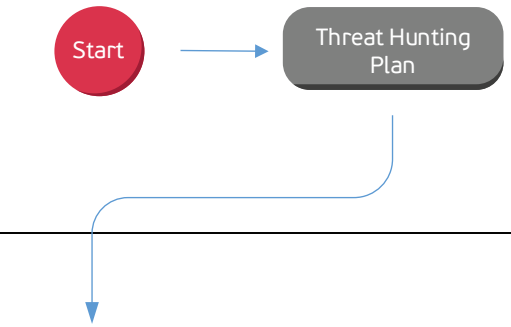
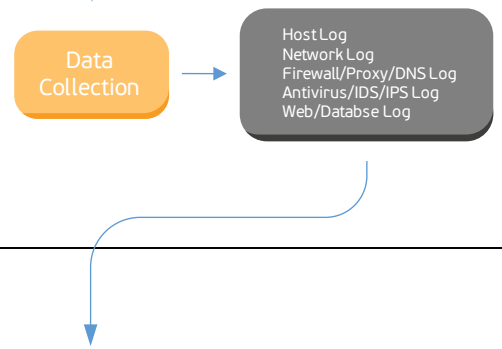
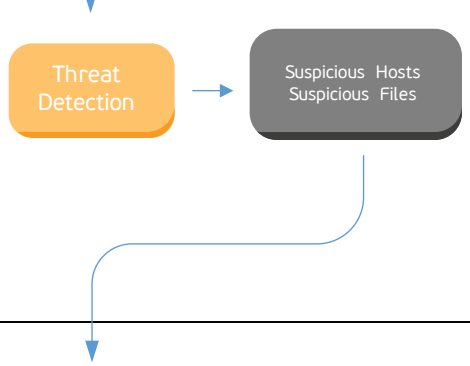
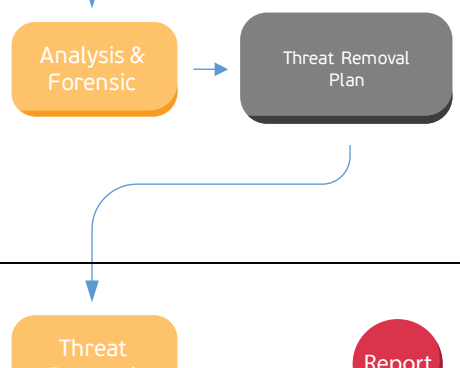
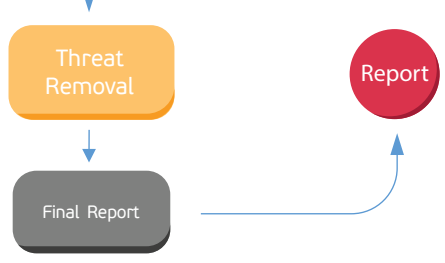
- Remove, clean malware
- Update, install critical patches
- Tighten security configuration of systems
- Implementation process

Cybersecurity Threat Hunting Service

viettel security

IMPLEMENTING PROCEDURES

The Threat Hunting Service of VCS is performed according to the following process:

Process	Details
	Viettel proposes a plan to implement Threat Hunting, Customers approve the plan in which the contents including but not limited to: • Log list (Host, FW/Proxy/DNS, AV, etc.) • Method of collecting each type of logs • Storage and review place: At Customer's computer / Via VCS iML system • Implementation method: On-site/Remote • Implementation time • Implementation personnel and coordination personnel
	Customers prepare the necessary conditions: • Compute r implementation (if Customer chooses to perform on Customer's computer) • Ready network connection to the necessary computers and systems Viettel implements, Customers supervise: • Host log (review tool): Viettel does it directly on computer or Customer pushes the tool through AD/SCCM/AV/SE/EDR/etc. • FW/Proxy/DNS/AV/Network/Web/Database/etc.: Viettel via SIEM or Customer via admin console
	Viettel implements, Customers monitor: • Host log: Via iML or directly on the server • FW/Proxy/DNS/AV/Network/Web/Database/etc.: Directly on Analyst's laptop/ Customer's PC or via Customer's SIEM/SOC system Methods of detecting threats: • According to network attack techniques (ATT&CK Framework standard) • According to the identification signs of intrusion detection determined by Viettel Threat Intelligent system • According to the typical signs of APT attack researched and built by Viettel • According to the machine learning results of the iML system (if using the hunting option on the iML system)
	Viettel implements Forensics, Customers monitor: • Forensics directly on suspected infected machines • Forensics by looking up the collected log types • Decompile and analyze samples on Analyst's laptop Viettel proposes Threat Removal Plan, Customers approve: • Removal plan for malware • Hardening plan for existing solutions Plan for additional implementation of information security solutions
	Customers/Viettel remove(s) malware and implements simple short-term measures which do not affect the system: • Malware removal • Simple hardening (installing patches, simple configuration, etc.) Viettel reports Threat Hunting: • Report on contents implemented and results • Propose the next content for Customer