viettel
security

Company
PROFILE

table of
contents

INTRO-DUCTION

Viettel Cyber Security is a branch of Viettel Group, conducting in-depth researches development of information security solutions, providing a wide range of cybersecurity services and products for domestic as well as foreign organizations.

Mission

Protecting the national security in cyberspace and leading the domestic cybersecurity market .

Vision

Leading in researching, developing Information security solutions, bringing in-depth knowledges into each Information security product and service in Vietnam, thereby constantly improving the capacity of informationsecurity for Vietnam cyberspace.
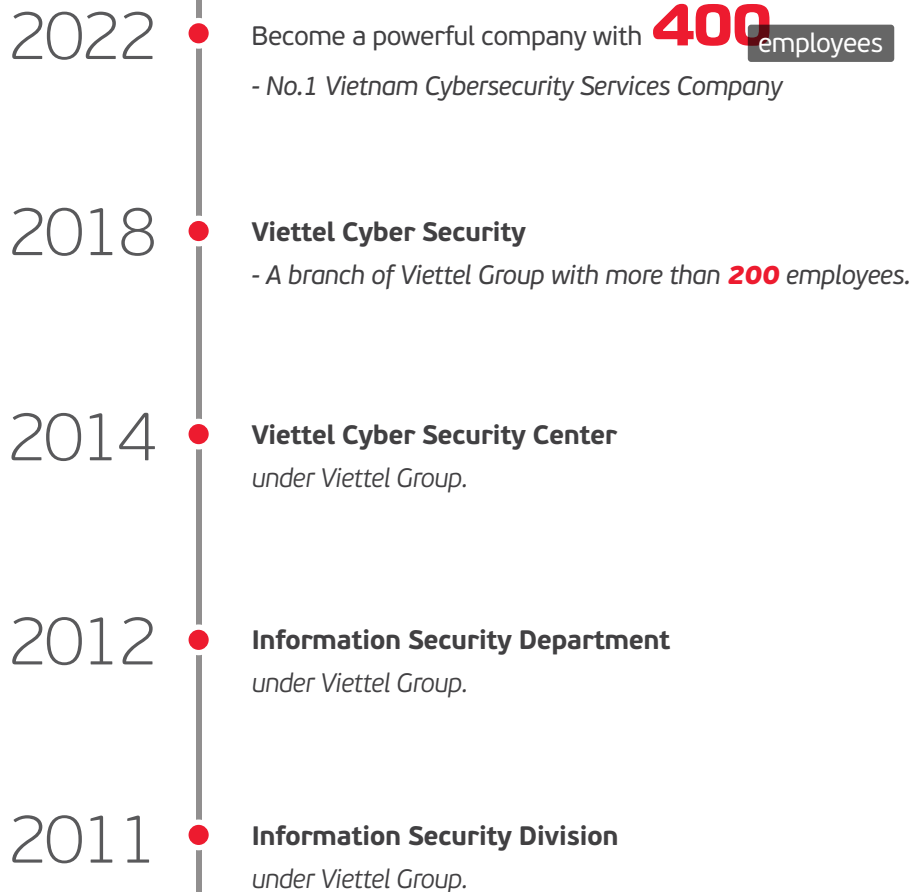
Goal

In 2025, to become the main partner providing cyber security products and services for 50% of the national critical infrastructures and organizations.
In addition, to increase the human resources to 500 employees of which 300 information security experts, 10% world-class level

Establishment HISTORY

2022 — Become a powerful company with **400** employees
- No.1 Vietnam Cybersecurity Services Company

2018 — **Viettel Cyber Security**
- A branch of Viettel Group with more than **200** employees.

2014 — **Viettel Cyber Security Center**
under Viettel Group.

2012 — **Information Security Department**
under Viettel Group.

2011 — **Information Security Division**
under Viettel Group.

HUMAN RESOURCES

Viettel Cyber Security always strives to attract and retain high qualified human resources by valued training & development programs and talent management.
Viettel Cyber Security experts have experiences in conducting critical research, detecting vulnerabilities for large and reputable organizations over the world. Those experts are appreciated and recognized by trusted global community and organizations.

ACHIEVE-MENTS
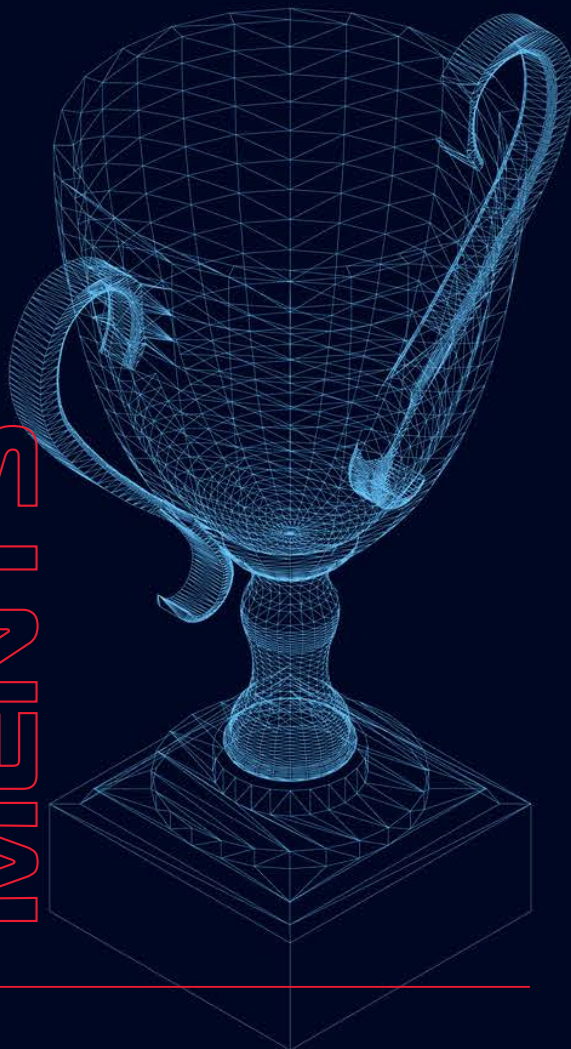
Pwn2Own

- **Top 5** of Pwn2Own 2020 in Tokyo - Japan
- **Top 5** of Pwn2Own 2021 in Vancouver - Canada
- **Top 2** of Pwn2Own 2022 in Toronto - Canada
- **Top 3** of Pwn2Own 2023 in Vancouver - Canada
- **Master of Pwn2Own** 2023 in Toronto - Canada

In-depth research

- **Top 1** in Twilio Bug Bounty Program
- **Top 3** of BugCrowd researchers
- **Top 10** in Paypal Inc. Bug Bounty Program
- **Top 20** in Microsoft Bug Bounty Program
- **Top 30** in Tesla Bug Bounty Program
- **Top 70** in Facebook Bug Bounty Program

About **400** Zero-day detected in various platforms

- Microsoft
- Google
- Zimbra
- Facebook
- BugCrowd
- Telerik
- Mattermost
- LimeSurvey
...

- Paypal
- Richfaces
- Cisco
- Chrome
- Tesla
- Okta
- Twilio
- Struts

Frost and Sullivan

- 2020 Vietnam Managed Security Service Provider of the Year
- 2022 Vietnam Cybersecurity Services Company of the Year

Cybersecurity Excellence Awards

- 13 Gold Awards Cybersecurity Excellence Awards 2022
- 11 Gold Awards Cybersecurity Excellence Awards 2023

Cybersec Asia Readers' Choice Awards

- Best in **Online Fraud Management 2022**
- Best in **Managed Security Services 2023**

Global InfoSec Awards

Best in **Next-Gen Security Penetration Testing 2023**

IT World Awards

- Bronze Award 2017, 2020, 2023
- Silver Award 2021, 2022
- Gold Award 2020, 2022, 2023
- Grand Globee Winner 2022

Stevie Awards

Silver Award 2017

PROFESSIONAL CERTIFICATIONS

ISO 27001-certified
Security Operations Center (SOC)

CREST

PEN TEST   SOC

CREST-accredited
Penetration Testing
Security Operations Center (SOC)

GLOBAL

Security Operation Center - S.O.C

11
Countries

1,000
Websites

28,000
Servers

16,000
Applications

50,000
Endpoints

100+ million
Subscribers

Vietnam · Laos · Cambodia · Myanmar · Timo-Leste · Tanzania · Mozambique · Burundi
Cameroon · Peru · Haiti

Myanmar

Laos

Vietnam

Cambodia

Timo-Leste

CUSTOMERS

GOVERNMENTS

Ministry of Finance	General Department of Taxation	Ministry of Defense
Office of the Government	Office of the National Assembly of Vietnam	42 People's Committees/ Departments and Sectors

BANKING & ENTERPRISES

SeABank · VPBank · Vietcombank · VietinBank · MB · BIDV · MSB

Vietnam Airlines · EVN · PTSC (A member of PETROVIETNAM) · SNP · DAIKIN · PVI INSURANCE · VPS SECURITIES

PRODUCT

SOLUTIONS FOR THE GOVERNMENT AND LARGE-SIZED ENTERPRISES

Network and Application
- Viettel Network Security Monitoring `VCS - NSM`
- Viettel Smart Web Protection `VCS - SWP`

Endpoint
- Viettel Endpoint Detection & Response `VCS - aJiant`
- Viettel Mobility Management `VCS M-Suite`

Security Analytics
- Viettel Threat Intelligence `VCS - Threat Intelligence`
- Viettel Security Information & Event Management `VCS - CyM`
- Viettel Security Orchestration, Automation & Response `VCS - CyCir`
- Viettel Killchain & Anomaly Detection `VCS - KIAN`

Fraud Detection
- Viettel Financial Fraud Detection & Response `VCS - F2DR`

SOLUTION FOR MEDIUM AND SMALL-SIZED ENTERPRISES
- Viettel Anti-DDoS
- Viettel Cloudrity

TELCO AND ISP SOLUTIONS
- Viettel Telecom Anomaly Detection `VCS - TAD`
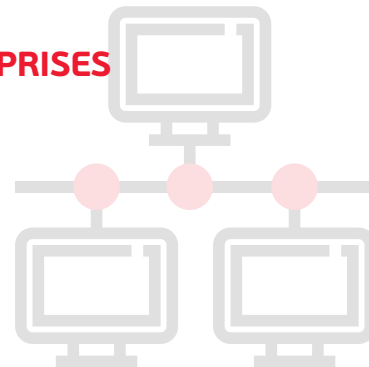- Viettel Anti Fake Phone Number `VCS - AFPN`

SOLUTIONS FOR THE GOVERNMENT AND LARGE-SIZED ENTERPRISES

Network & Application

Network Security Monitoring

Make early detection and alert of Advanced Persistent Threat (APT) on network layers. Flexibly deploy as Out-of-Band architecture.
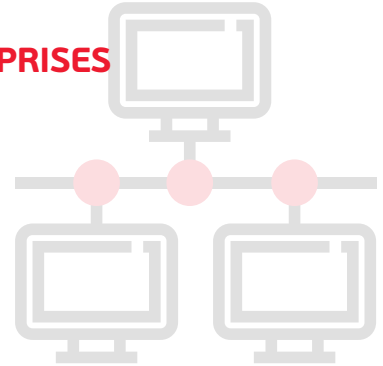
Main features:
• Real-time-detected abnormal signs and exploit attacks to network.
• Support for in-depth investigation and analysis of Information Security incidents.

VCS - NSM

SOLUTIONS FOR THE GOVERNMENT AND LARGE-SIZED ENTERPRISES

Network & Application

Web Application Firewall

The Layer 7 application firewall protects websites against web application attacks. Flexibly deploy as Out-of-Band architecture.

Main features:
• The Layer 7 application firewall protects websites against web application attacks.
• Flexibly deploy as Out-of-Band architecture.

VCS - SWP

SOLUTIONS FOR THE GOVERNMENT AND LARGE-SIZED ENTERPRISES

Endpoint

Endpoint Detection & Response

Monitoring, detection and alert of abnormal behaviors on Endpoint layer.
Support analyzing, investigating and responding to information security incidents on Endpoint layer in real time.
Deploy as Server - Client model.

Main features:
• Manage, monitor and respond to information security incidents in the Endpoint layer in real-time.
• Transparent operation to users, taking less than 1% of system resources.

VCS - aJiant

Mobility Management

Support remoted working while ensuring information security compliance policies.

Main features:
• Manage device, session accessing to internal system.
• Analyze packets, monitor users' behaviors.
• Store and manage log, protect private data.

VCS M-Suite

SOLUTIONS FOR THE GOVERNMENT AND LARGE-SIZED ENTERPRISES

Security Analytics

Threat Intelligence

A Database system of information security threats over the world, providing data, knowledges of global attacks and threats.

Main features:
• Collect threats from various sources: Dark/Deep Web, Social Network, Open Source, Community Source, Private Source.
• Provide Threat Feed (IP, domain, hash,) for other solutions to improve threat detection for organization.
• Support API and database with standard format data (STIX/TAXII).
• Alert the latest cyber threats.
• Provide detailed information and methods to handle new threats.

VCS - Threat Intelligence

Security Information & Event Management

Manage, monitor and provide 24/7 overview of information security situation.
Detect and alert real-time information security incidents in the organization.
Deploy as on-premise or cloud architecture.

Main features:
• Collect and standardize various data sources.
• Analyze, correlate with log sources to detect Information Security incidents.
• Continuously update information security knowledges.

VCS - CyM

SOLUTIONS FOR THE GOVERNMENT AND LARGE-SIZED ENTERPRISES

Security Analytics

Security Orchestration, Automation & Response

Smart security coordination platform,
automatic response.

Main features:
• Automatically integrate technologies and security processes into system operation.
• Create an integrated and comprehensive ecosystem of cyber security solutions for productivity optimization.

VCS - CyCir

User & Entity Behavior Analytics

Detection of abnormal behaviors and attack chains into the information system.
Based on Big Data and Machine Learning platforms.

Main features:
• Profile entities and supervised behavior.
• Detect the sequence of attacks based on available setting.
• Real-time detection & alerts.

VCS - KIAN

SOLUTIONS FOR THE GOVERNMENT AND LARGE-SIZED ENTERPRISES

Fraud Detection

Financial Fraud Detection & Response

Viettel Financial Fraud Detection & Response is a solution to detect and respond to money fraudulent activities and promotion abuse by combining the dynamic profiling engine and chain rules along with traditional rules to establish smart rules to detect complex fraudulent scenario without impacts on the user experience. The solution provides a comprehensive tool to detect, investigate, operate and respond; helping banks in responding and preventing fraud.

Main features:
• A streamlined and self-contained experience for detecting, investigating, and responding to fraud incidents
• Strong rule base to create scenarios for complex fraud detection
• Automatic risk assessment of objects on any smallest abnormal behaviors
• Automatic incident handling and response
• Simple integration and setup
• Blacklist and whitelist monitoring

VCS - F2DR

SOLUTION FOR SMALL AND MEDIUM-SIZED BUSINESSES

Viettel Anti-DDoS

Anti DDoS Volume-Based is the solution to minimize bandwidth denial-of-service attacks that congest uplink traffic of clients and affect services or network leading to widespread service loss, ensuring good quality for the client's transmission channel in normal condition as well as under DDoS attacks.

Main features:
• Detect, quick response and instant notification to client high-bandwidth DDOS attacks
• Support a variety of real-time warning channels via Email, SMS, Portal
• Handle all popular DDoS attacks with high-bandwidth up to hundreds of Gbps, quickly and regularly update new attack patterns.
• Apply advanced technologies to detect and block attacks such as DPI, Profiling, Machine Learning, BGP Flowspec, Remote trigger black hole,...

Viettel Cloudrity

Prevent of enterprises' web applications from exploit and DDoS attacks based on Cloud Computing Platform, apply CDN, SDN NFV and Global Balancing technologies.

Main features:
• Block attacks automatically
• Update virtual patches.
• Detect attacks based on the signature.
• Apply Machine Learning technology to correlate with network attacks.

TELCO AND ISP SOLUTIONS
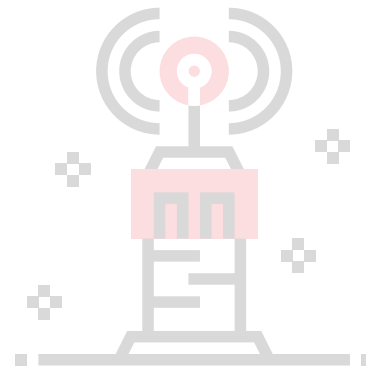
Telecom Anti Fake Phone Number

The system helps to protect the domestic telecommunication subscribers from the danger of being phished, appropriated, threaten, slanded, also helps to protect and improve the reputation of the network operator, trust of customers.

Main features:
• Detecting and blocking fake calls automatically without the need for subscribers interaction or operators interaction, with high accuracy and very low latency.
• Full control and very flexible for a telecom group to satisfy all governments' requirements for all countries it has operation.
• Simple and fast deployment, but with high efficiency.

VCS - AFPN

Telecom Anomaly Detection Security Edition

Detect and prevent dangerous signaling messages to attack subcribers such as: Location tracking, phishing calls and messages, etc.
Detect and prevent alerts such as: DDoS attacks, fraud, subcriber distribution information.

Main features:
• Detect attacks and abnormal signs in the network.
• Automatically block dangerous external alerts.

VCS - TAD

SERVICES

Managed Security Services

Threat Hunting Service

IoT Security Assessment Service

Pentest & Audit Service

MANAGED SECURITY SERVICE

Support 24/7/365 monitoring and incidents response for organizations and bussinesses
• Support to monitor and respond incidents on all system layers.
• Periodically positive prevent: Audit, Pentest, Threat Hunting.
• Operated 24/7 by a team of experienced and qualified experts for handling the most complicated incidents.
• Manage, operate and co-operate in 6 personel groups: SOC manager, Content, monitor Threat & 3 Tiers.

IOT SECURITY ASSESSMENT SERVICE

Viettel Cyber Security Company offers a set of proactive IoT Security Assessment Service (IoT Security Assessment) which can check hardware, firmware, protocols and mobile apps to assess potential security risks, thereby offering solutions timely.

Highlights:
• Assessment of Hardware devices
• Assessment of Firmware
• Assessment of Mobile and Cloud System
• Assessment of Protocols
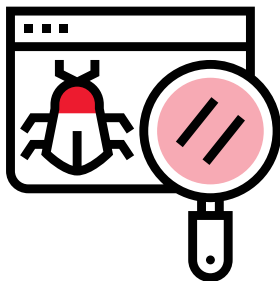
THREAT HUNTING SERVICE

• A service that combines network, end-point, application, and user behavior threat analytics to uncover a cyber threat and attack campaigns that traditional security monitoring mechanisms miss.

• Leverage deep knowledge and experience to conduct an analysis of your security data and systems, known attack patterns – especially those unique to your industry, currently popular exploits and vulnerabilities, and your high value assets to formulate a hypothesis for their hunt.

• Utilize automated and manual tools, techniques and procedures to identify suspicious behavior and advanced threats that may evade automated security solutions.

• Propose suggestions to prevent, detect malware attacks and intrusions.

PENTEST & AUDIT SERVICE

Pentest & Audit Service

Client's information security testing and audit based on Blackbox and Whitebox methods selected by clients.

• Ensure security for the entire system in each stage of design, deployment, testing and operation.

• Scan, pentest to find out the system vulnerabilites.

• Indentify, define and avaluate the impact of weak points to the system.

BugBounty Platform (SafeVuln)

The platform connects security researcher and enterprise demanding security vulnerability detection in its products and services.

• Enterprises offer applications and products that required to find out security vulnerabilities to SafeVuln.

• Security experts research for vulnerabilities in applications and products and report to SafeVuln.

• After reports are approved, security researchers will be rewarded from enterprises via SafeVuln.

X-DATA (Red Teaming Service)

On-demand Advanced Penetration Testing that is aimed at revealing real-world opportunities for malicious insiders or bad actors to be able to compromise all aspects of organization.

• Identify physical, hardware, software and human vulnerabilities to reach out X point which is confirmed before implementation.

• Obtain a more realistic understanding of risk for your organization.

• Help address and fix all identified security weaknesses.

In-time support by leading
A team of highly qualified technological experts is willing to support, respond incidents in a rapid and professional manner.

In-house developement
Research, develop and provide comprehensive and high-quality information security solutions and services.

The most optimal cost
The leading security information solutions come along with the most reasonable cost

COMPETITIVE ADVANTAGES

Service Level Agreement (SLA)
Clear, transparent and correct Service Level Agreement (SLA).

Diverse products ecosystem
Various and closely connected products ecosystem.

Big Data
The No. 1 MSSP in Vietnam possesses with a large amount of data, convenient for analysis and attacks prevention.

HEADQUARTER IN HANOI

⊙ Keangnam Landmark 72, Pham Hung St., Nam Tu Liem Dist., Hanoi, Vietnam

⊕ www.viettelcybersecurity.com

⊠ vcs.sales@viettel.com.vn

▯ (+84) 971 360 360

THE SOUTHERN OFFICE

⊙ Floor 28A2 - Viettel building, 285 Cach Mang Thang Tam Street, Ward 12, District 10, Ho Chi Minh City, Vietnam

viettel
security