viettel
IDC

Datasheet

VIETTEL THREAT INTELLIGENCE



No. 1 in Vietnam for Data center and Cloud Computing Services
Website: https://viettelidc.com.vn
Hotline: 1800 8088

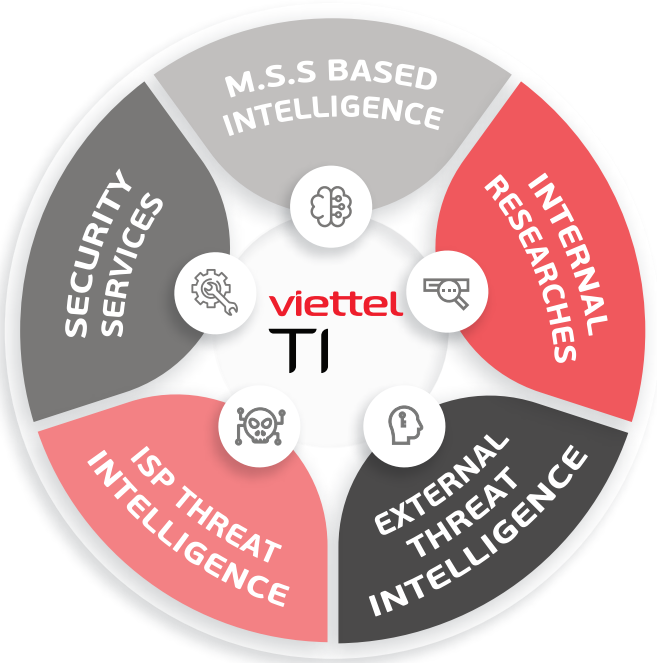
Datasheet
VIETTEL THREAT INTELLIGENCE

THE NECESSITY OF THREAT INTELLIGENCE

In the era of Industry 4.0, while benefiting from the advancements of information technology, cyberattack techniques used by hackers have also become more advanced , unpredictable, and methodical—especially targeted attacks (APT) aimed at the critical core of an organization's IT infrastructure.
Therefore, gaining early awareness and continuously updating information on emerging threats is a vital strategy for organizations and businesses in preventing attacks and ensuring information security.

VIETTEL THREAT INTELLIGENCE SERVICE

The Viettel Threat Intelligence solution provides in-depth cybersecurity information collected from various sources on threats targeting organizations. This intelligence can also be used to enrich data feeds for security solutions such as SIEM, Network IDS, EDR, etc., via internationally standardized APIs like STIX/TAXII. As a result, organizations and businesses receive timely alerts and can make strategic decisions in response to cybersecurity risks.



Viettel is a leading provider of Threat Intelligence services. The data sources of Viettel Threat Intelligence include:
- Global ISP-level data sources
- Data from international partners (e.g., FIRSTM, APWG)
- Data collected through cybersecurity services such as penetration testing (Pentest) and threat hunting
- Data gathered during the delivery of 24/7 managed security services (MSS)
- In-house research data from monitoring APT campaigns, threat actor groups, and zero-day/1-day vulnerabilities studied by Viettel

KEY FEATURES

Threat Collection

Viettel Threat Intelligence is capable of collecting cybersecurity threat information from various sources, especially from proprietary, confidential, and non-public sources for analysis and alerting.

Threat Feeds

Provides MRTI (Machine Readable Threat Intelligence) through Threat Feeds (IP, domain, hash, etc.) in STIX/TAXII format for integration with solutions such as SIEM, IPS/IDS, Antivirus, and others.
Automatic updates ensure these solutions are continuously refreshed with the latest threat indicators and malware signatures, with no latency and no need for human intervention.

Threat Scoring

Provides expert analysis and scoring of threat alerts based on severity levels—enabling customers to make informed and appropriate response decisions.

Monitoring & Analytics

Provides tools to support customers in investigating, analyzing , and searching for cybersecurity threats across cyberspace.

Keyword Monitoring

Allows organizations and businesses to define custom keywords for monitoring. Any information related to the configured keywords that appears will trigger an alert.

Threat Category

Identifies threats by specific alert categories, helping customers easily monitor and manage the types of risks affecting their organization.

Global Threat Report

Viettel Threat Intelligence also provides a global overview, enabling businesses to stay informed about the current cybersecurity landscape worldwide:
- Top trending cybersecurity events and threats gaining global attention
- Active threat actor groups
- Prevalent malware and attack techniques
- Vulnerabilities currently being exploited or closely monitored across the globe

Datasheet
VIETTEL THREAT INTELLIGENCE

VIETTEL THREAT INTELLIGENCE SERVICE PACKAGES

No.	FEATURE	DESCRIPTION	FEATURE PACKAGE			
			Basic	Advanced	Extreme	Threat Feed
1	Vulnerability Actionable Response	Provides the latest alerts and recommended remediation methods, including indicators of vulnerability exploitation to help customers identify potential threats.	✓	✓	✓	
2	APT Alert	Alerts on targeted threat actor groups that may pose a risk to customers (based on industry, geography, etc.)		✓	✓	
3	Malware Alert	Alerts on malware that could potentially impact the organization (based on industry, scope, etc.)			✓	
4	Phishing Alert	Provides domains and phishing applications that may abuse branding or impersonate interfaces to steal customer credentials.			✓	
5	Brand Abuse	Provides domains and applications related to the use of the customer's brand			✓	
6	Data Leak	Provides information on stolen or leaked data found on forums, underground markets, and dark web platforms related to the customer			✓	
7	Compromised Systems Alert	Provides alerts on customer infrastructure communicating with malware infrastructure Provides information on service vulnerabilities and unusual open ports on the organization's public domain/IP			✓	
8	Fraud Alert	Provides information on financial fraud Data on accounts and passwords used in online transactions Bank card data, including card numbers and card types			✓	
9	Machine Readable Threat Intelligence	Provides threat intelligence and indicators for integration with SIEM, EDR, etc., enhancing detection capabilities for the organization	✓ (public)*	✓ (public +private)*	✓ (public +private)*	✓ (public +private)*
10	Alert	Alerts delivered via portal and email	✓	✓	✓	
11	Report	Monthly and quarterly cybersecurity reports		✓	✓	
12	Support Service	24/7 support assistance		✓	✓	

Note (*)

Public refers to attack indicators and vulnerability information that have been publicly reported by vendors or the media.
Private refers to exclusive attack indicators and vulnerability information that only Viettel possesses, obtained through incident investigations (across a large customer base), confidential sources, or commercial threat intelligence feeds.