Datasheet

Viettel Managed Security Service

viettel security

Security Operation Center (S.O.C)

Security Operation Center (S.O.C), is a centralized unit which monitors and deals with cybersecurity-related issues to detect, analyze, respond, prevent and trace cybersecurity incidents, ensuring information safety and security for an organization.

- Human: Refer to a cybersecurity expert team that are well trained to operate (SOC) to monitor, detect and prevent incidents, trace and remedy damages caused by an attack.
- Procedure: Refers to policies, rules, regulations and recommendations on cybersecurity assurance issued by an organization.
- Technology: Refers to technical solutions, specialized tools that assist monitoring, detecting, preventing and tracing cybersecurity incidents.

Necessity of S.O.C

In the context of global trend towards a 'smart nation' era, the Fourth Industrial Revolution is being accelerated all over the world. As a matter of fact, ever-increasing interactions on the Internet lead to a greater threat of cybersecurity, for example:

- The development of IT creates an ideal environment for hackers' attacks against organizations.
- Hackers' methods of attack are becoming more sophisticated and unpredictable on a larger scale.
- Users' awareness about cybersecurity is limited.
- Inconsistent and patchy investment of organizations in the field of cybersecurity.
- Difficulties in observing cybersecurity policies.

Managed Security Service (MSS)

In recent years, businesses are aiming at reduction of personnel and other resources. Therefore, they have switched to external service providers to relieve the enterprise's financial pressure, and hence, cybersecurity issues in businesses and organizations are not an exceptional case to this trend.

Apart from that, the lack of accurate orientations for cybersecurity causes the inconsistent investment and patchy purchase, leading to the waste of huge investments on cybersecurity without meeting the expectation.

Therefore, the cybersecurity service providers provide businesses and organizations the most advanced security technologies with a team of leading experts in this field. At the same time, the significant expenses for investment, management and maintenance of a S.O.C system can be also saved.

With the rapid growth of digital space and its constant threats, the Managed Security Service (MSS) is gaining certain attraction in the market, as a matter of fact. Managed Security Service (MSS) supports clients in managing and safeguarding organization's information assets by using service of a MSS provider. The service provider will be responsible for delivering, maintaining and managing organization's IT system. Moreover, the use of Managed Security Service helps clients save time on developing a S.O.C center based on real projects (usually about 12 to 18 months), this also solves the Time-Cost-Performance problem for clients.

S.O.C System Model

SIEM agent	Endpoint Detection & Response	Network Security Monitoring	WAF
Gateway Security	Anti DDoS	Scanner & Discovery	3rd Party Security Log Firewall · Windows Event log · DNS · AD · SysLog · VPN · AntiVirus · ...

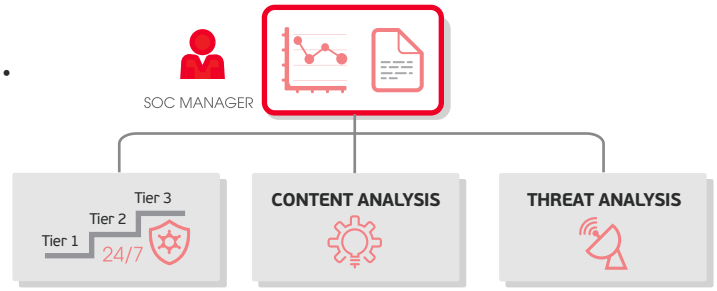
Viettel S.O.C

With the rapid growth of digital space and its constant threats, Viettel S.O.C establishes a defendable perimeter for IT systems of organizations and businesses, by these 5 following principles:

- Fully Managed Security
- Comprehensive Solutions
- Centralized Visibility
- 24/7 Availability
- Expert-team Approach

Operation of S.O.C system

Viettel Operation of S.O.C system develops for clients the model if personel components operating international-standard certified S.O.C system divides into 6 following groups:



- Tier 1 (Viettel): Monitor online 24/7 handle all warning as instructed.
- Tier 2 (Clients): Receive incidents from Tier 1 and tackle normal incidents and escalate unsolved incidents to Tier 3.
- Tier 3 (Viettel): Receive escalation incidents from Tier 2 for more in-depth processing, and rewrite the processing instruction for similar incidents to guide and train Tier 2.
- Content Analysis (Viettel): Improve and optimize the system's processing capacity.
- Threat Analysis (Viettel): Review, analyze, update knowledge of new risks to the system.
- SOC Manager (Viettel & Clients): Administer the system; test and evaluate the system's performance ratio.

Viettel Managed Security Service (MSS)

Managed Security Service (MSS) of Viettel Cyber Security provides a series of information security solutions with flexible options depending on clients' needs and status in combination with policy consultancy to ensure that information security and functions for testing and analyzing information security breaches will be the good choice for clients. Information security procedures and policies are divided into 6 procedures:

Highlights

Based on the strengths of leading telecommunications and Internet service provider in Vietnam and neighboring countries, as well as the team of world-class experts and cutting-edge technology, Viettel becomes a leading provider of managed security services for domestic and foreign organizations, with these outstanding advantages:

- Leading telecommunications service provider and ISP.
- Transparent and clear solution.
- Professional & well-qualified personnel 24/7 incident response capability.

Furthermore, Viettel is committed to providing clients with the first-class & highest efficiency service, adding to businesses massive values:

- Enhance security with ability to identify anomalies & risks of information insecurity threats throughout its network.
- Increase cost-efficiency by consolidating security technologies & team.
- Faster incident response times and detection of security events
- Reduce business impact of security incidents.