IGLOO SECURITY

One Step Ahead
National Defense Strategy for Securing Cyber Security

December, 2016

1. We are in Danger

Real World

Nuclear Bomb

Terror

Enemy Forces

Bullet

Missile

Cyber World

Virus

Malicious code

Cyber Attack

Hackers

Forgery

2. Attackers?

Real World

Hostile Countries
Terrorists
Etc.

Cyber World

Hackers

Professional hackers either **working on their own** **or** **employed by the government or the military service.**

3. Homeland Security

Homeland

1. Territory

2. Airspace

3. Territorial Sea

4. Cyber Space

Enormous Costs

Low cost, High damage

Who is in charge?

1. Army

2. Air Force

3. Navy

4. Who?

4. Border Defense

Real World (Border)

1. Border line

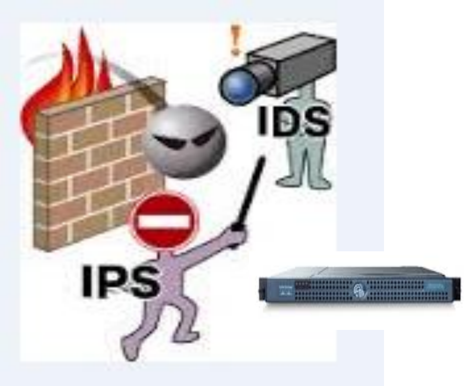
CCTV

2. Surveillance

3. Immigration Control

Cyber World (International Gateway)

1. Firewall



2. Detection

3. Contents Filtering

5. National Defense

Real World (National Defense)

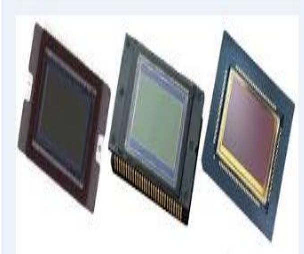
Intrusion Monitoring by Agents

CCTV

Protect main government agencies

Cyber World (National Backbone Network)

By Sensors and Radar



Check Network Bottleneck

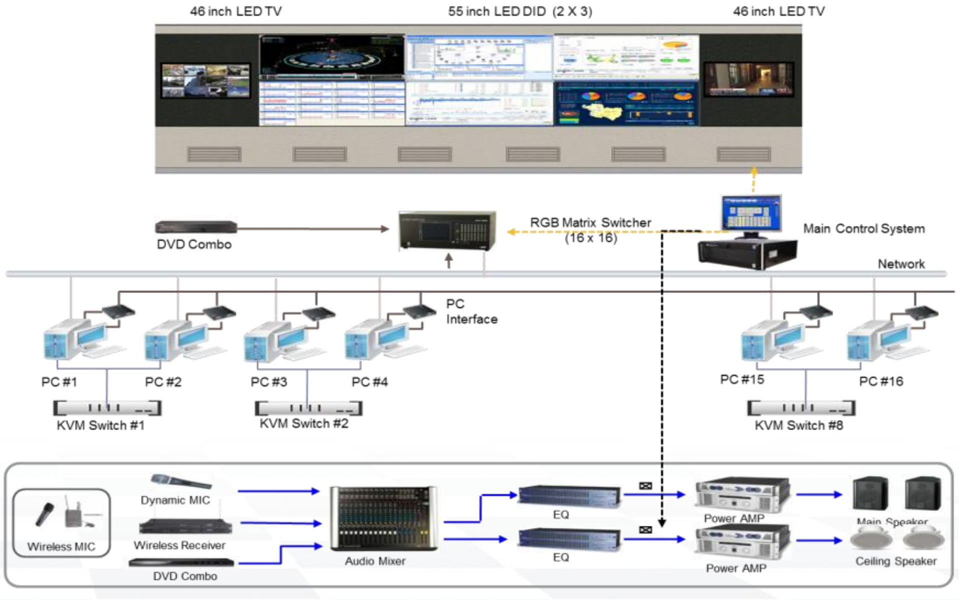
6. Control Tower

Real World (War Room)

Command control room exists for the real world.

Cyber World (SOC)

SOC (Security Operation Center) exists for the Cyber world.



7. Trained People

Real World

Policeman, etc.

Soldiers, etc.

Cyber World

Specialized Analyst, etc.

White Hackers, etc.

We need to train people to secure our life in Real and Cyber world.

National Cyber Defense Strategy

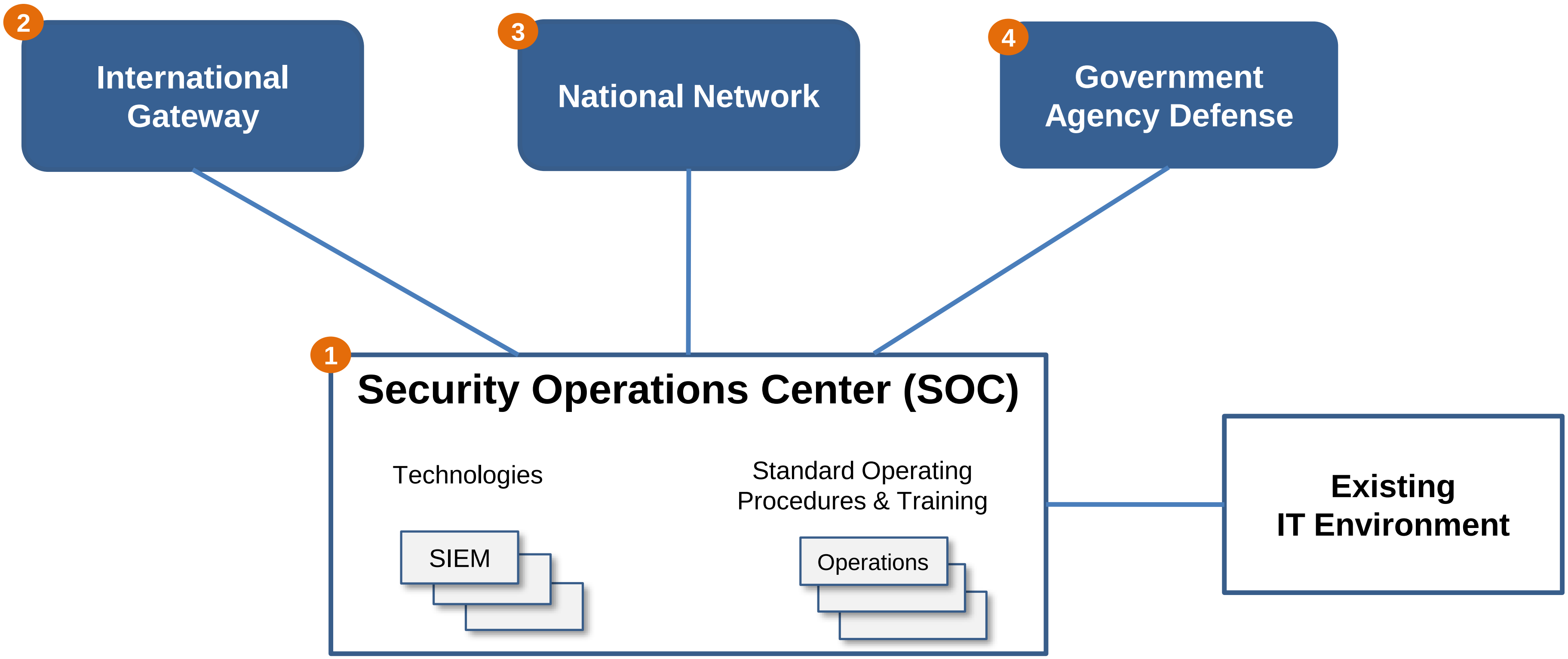
Main Roles and Prioritization for Cyber Security Center

Main Roles	Content	Priority
Precautionary measure to evaluate cyber vulnerabilities	Analyze vulnerabilities of national government network and IT system	?
Detecting cyber threats at national level	Build a security system to detect international and local cyber attacks on the national network	?
Preventing cyber attacks on major government agencies	Effectively defend major government agencies from diverse cyber attacks	?
Cyber emergency response activities	Monitor status of national cyber threats and establish procedures for processing intrusion incidents	?
Information security for important government officials	Prevent information leakage from government agencies and strengthen level of security	?
Establishing malware defense system	Detect malware and build malware analysis system	?
Preventing cyber attacks originating from foreign locations	Protect local services from cyber attacks originating from foreign locations	?
Training expert cyber manpower for the government	Provide operation training for implemented systems, customized training for operators and transfer technology needed for self operation	?
Evaluating the level of information security of government agencies	Provide support to develop the capacity to carry out and evaluate the Information Security Management System (ISMS)	?
Fostering private sector information security firms	Promote the information security industry	?

Tasks

- Protecting the International Gateway
- Protecting Government Agencies
- Protecting the National Network
- Operating the Security Operation Center

Overall Framework

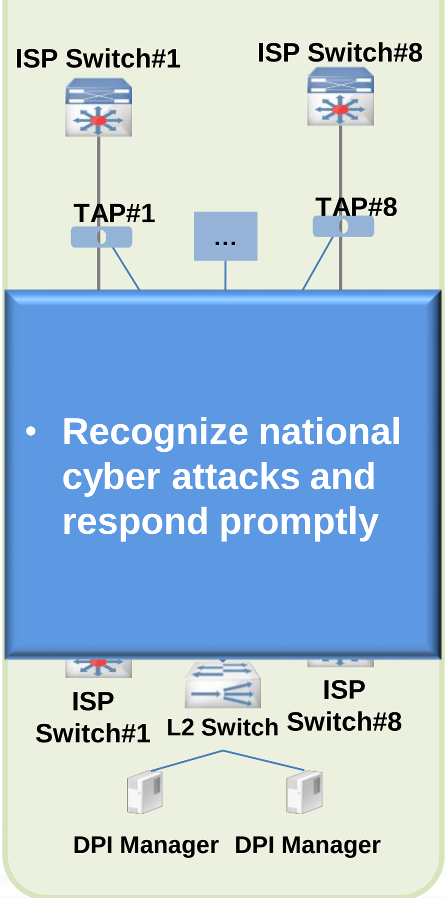

2
International Gateway
3
National Network
4
Government Agency Defense
1
Security Operations Center (SOC)
Technologies
SIEM
Standard Operating Procedures & Training
Operations
Existing IT Environment

Overview > Scope of Tasks

Category	Scope of Tasks
1 SOC Security Operation Center	**Technology** SIEM 3D Monitoring VMS Malicious Code / URL Detection and Monitoring System Homepage Monitoring System
	Infrastructure Service Network & H/W configuration Server Room SMS/NMS/ Security Monitoring & VIP Room Power/Disaster Prevention
	Training Security Training CERT Management Training Product Training Operation Training
2 International Gateway	Secure stability of domestic services by monitoring harmful foreign sites Maintain availability of Internet services by controlling applications that cause massive traffic Defend against cyber threats by detecting unknown and harmful foreign traffic
3 National Backbone Network	Protect national operation system by detecting abnormal traffic Secure the national network by monitoring for malicious activities Secure the national network from various types of DDoS attack
4 Government Agency Defense	Secure stability of government services by defending against cyber attacks Enhance reliability of government services by monitoring for malicious activities Defend against web application based attack

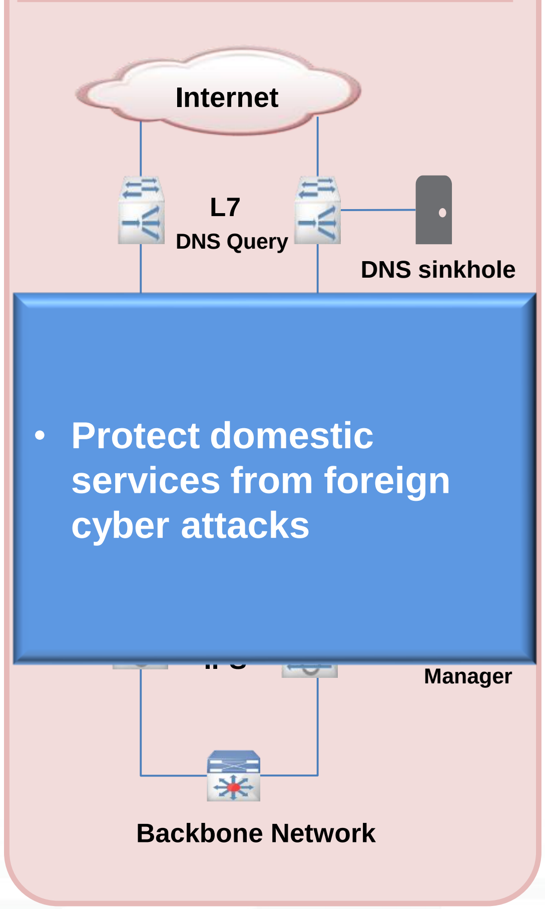
National Cyber Attack Defense

Security Operation Center



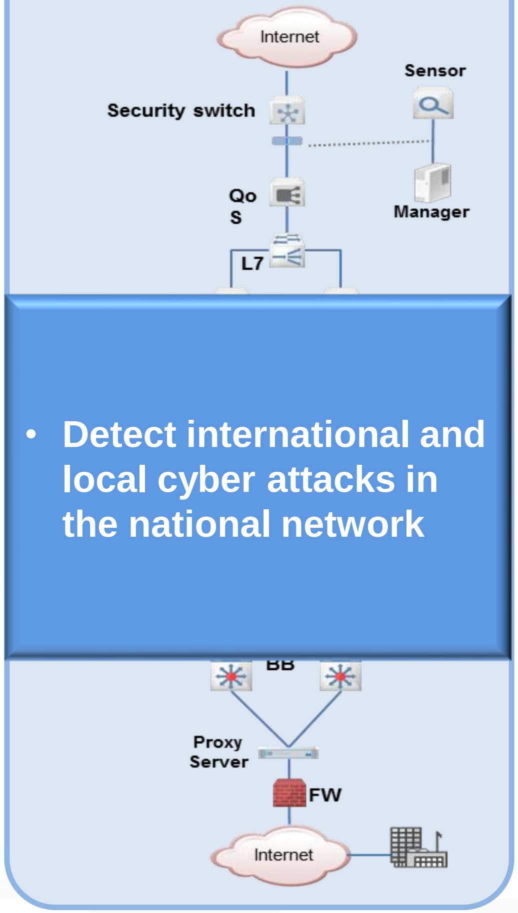
- Recognize national cyber attacks and respond promptly

International Gateway



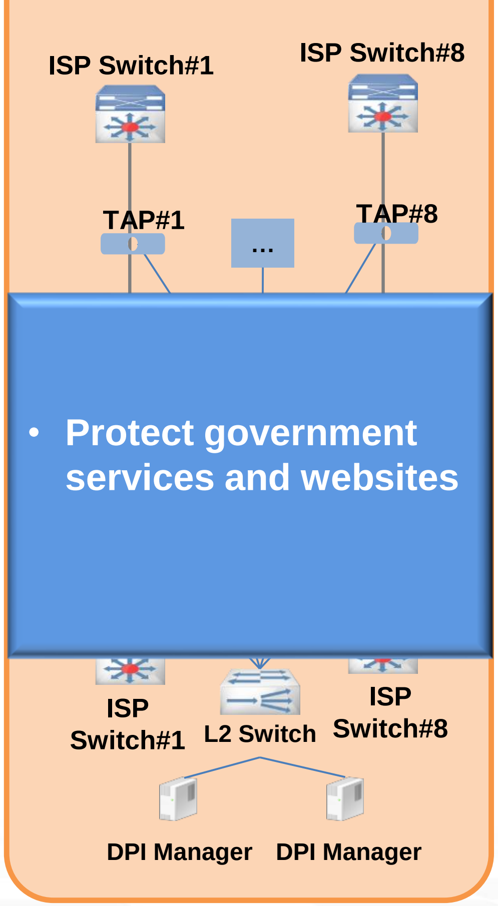
- Protect domestic services from foreign cyber attacks

National Backbone Network



- Detect international and local cyber attacks in the national network

Government Network



- Protect government services and websites

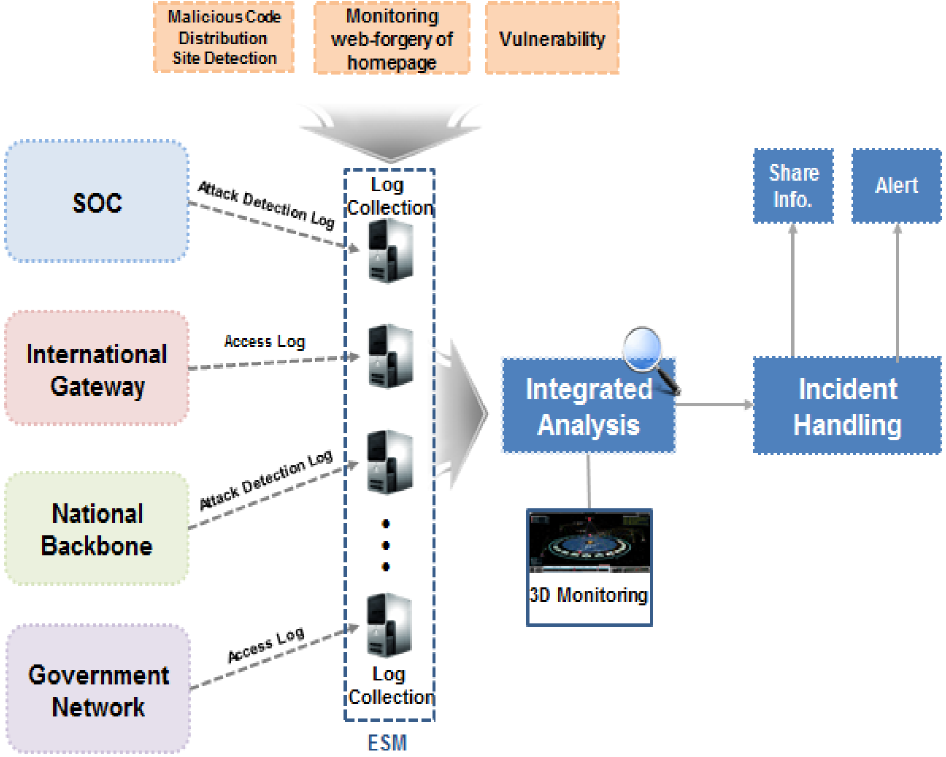
Security Operation Center

To maintain continuous monitoring and respond to cyber threats, a system and infrastructure for the security operation center, or the SOC, must be in place. The SOC helps to secure government services and websites as well as protect the national backbone network by providing status of cyber threats through non-stop surveillance. This system should take user convenience into consideration during construction for efficient non-stop monitoring.

Overview

- Collect all information on attack, access and vulnerability that can occur in the cyber space from different sectors.

- Systematic operation of infrastructure and system required for immediate recognition of and response to cyber attacks



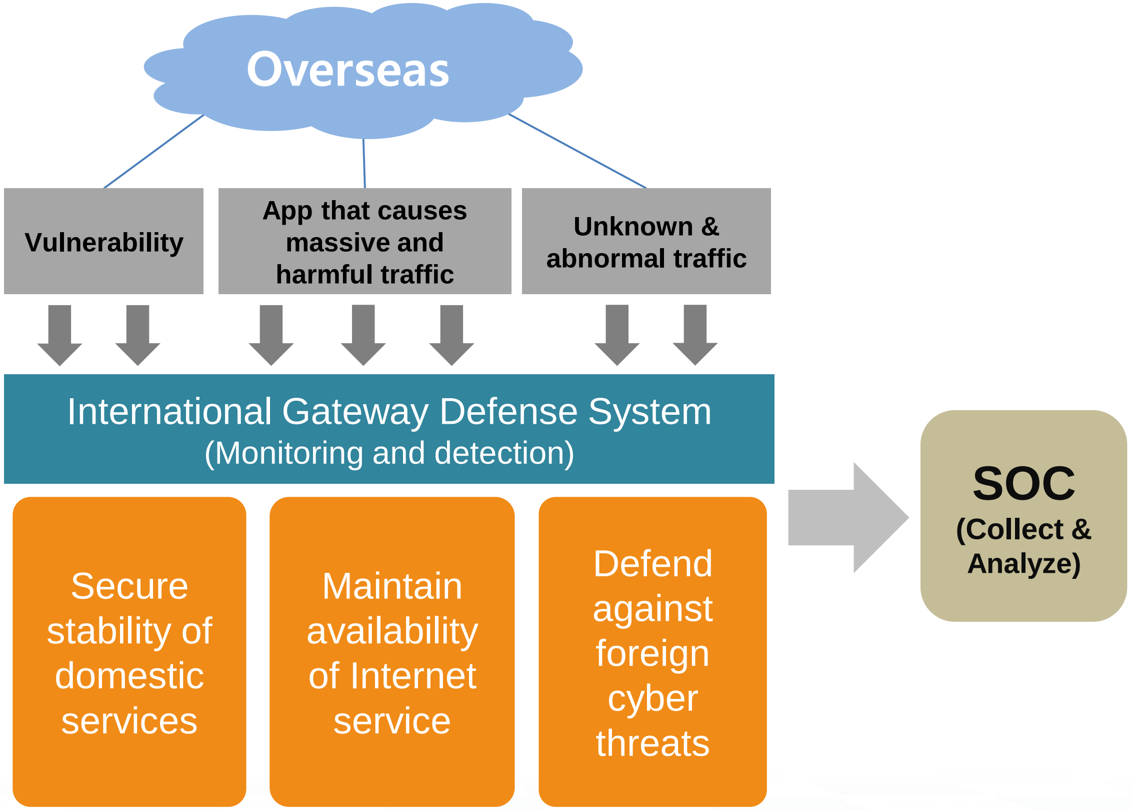
[Example of Monitoring Configuration]

International Gateway

The International Gateway needs to protect domestic services from foreign cyber threats and ensure availability and continuity of the Internet. To achieve these goals, measures for controlling the traffic passing through the International Gateway and to block harmful traffic so that it does not enter into the national network must be implemented.

Overview

- Prevent damage by blocking domestic Internet users and systems from connecting to illegal and harmful foreign sites or servers
- Control services that cause excess amount of traffic in order to ensure the availability of the Internet
- Detect and block harmful traffic including attack patterns


Overseas
Vulnerability
App that causes massive and harmful traffic
Unknown & abnormal traffic
International Gateway Defense System
(Monitoring and detection)
Secure stability of domestic services
Maintain availability of Internet service
Defend against foreign cyber threats
SOC
(Collect & Analyze)

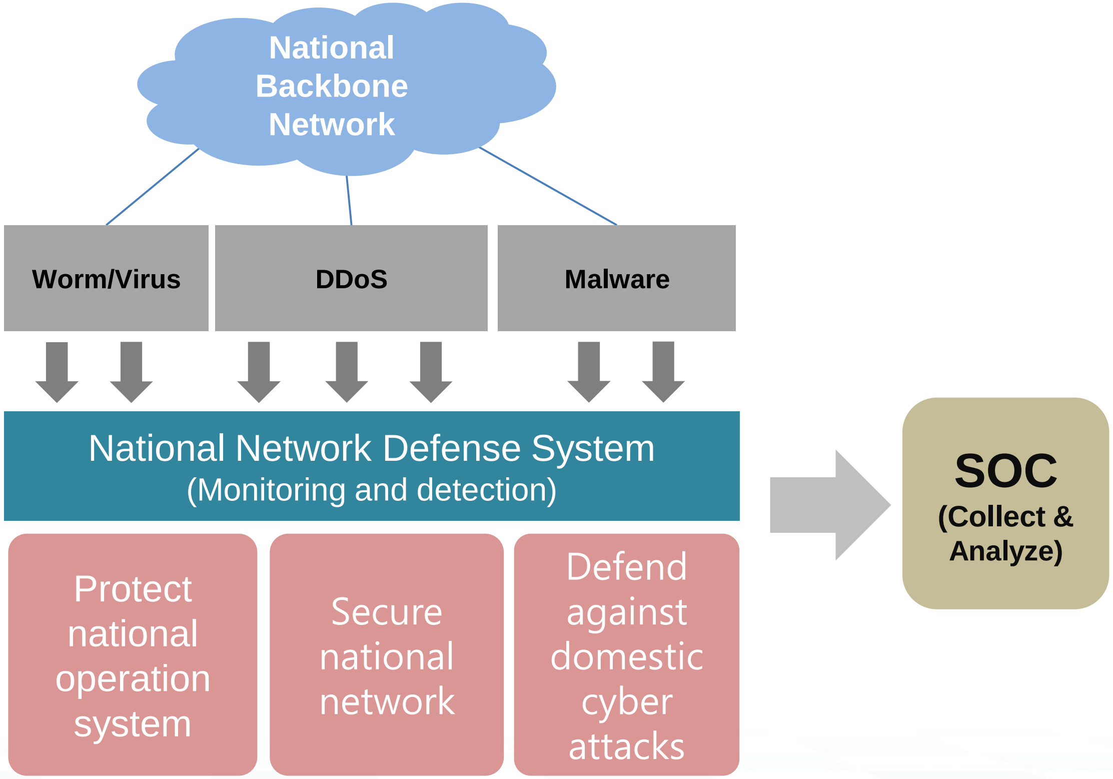
[Concept of the Protecting the International Gateway]

National Backbone Network

To effectively protect the National Backbone Network, a system of security to secure the internal system and effectively detect internal/external cyber threats occurring in the network needs to be implemented. Abnormal or unusual traffic need to be analyzed at the SOC and dealt with to keep the National Backbone Network safe from cyber threats of domestic origins.

Overview

- Detect in/out bound traffic that contain attack patterns occurring in the National Backbone Network
- Send the abnormal or unusual traffic to the SOC management system to analyze for attack information of the detected threat


National Backbone Network
Worm/Virus
DDoS
Malware
National Network Defense System
(Monitoring and detection)
Protect national operation system
Secure national network
Defend against domestic cyber attacks
SOC
(Collect & Analyze)

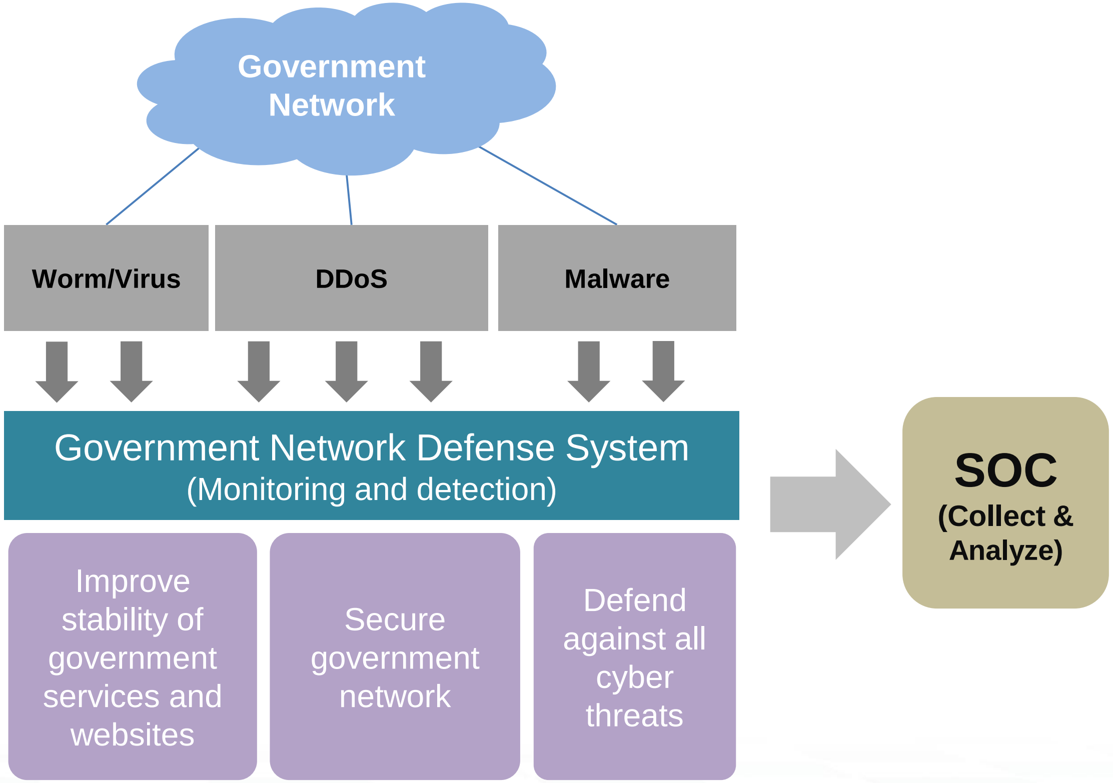
[Concept of Protecting the National Backbone Network]

Government Network

Due to the value and importance of public services that the government provides and the need for secure network to share information for government work, protecting the network and services of major government agencies is essential for any country.

Overview

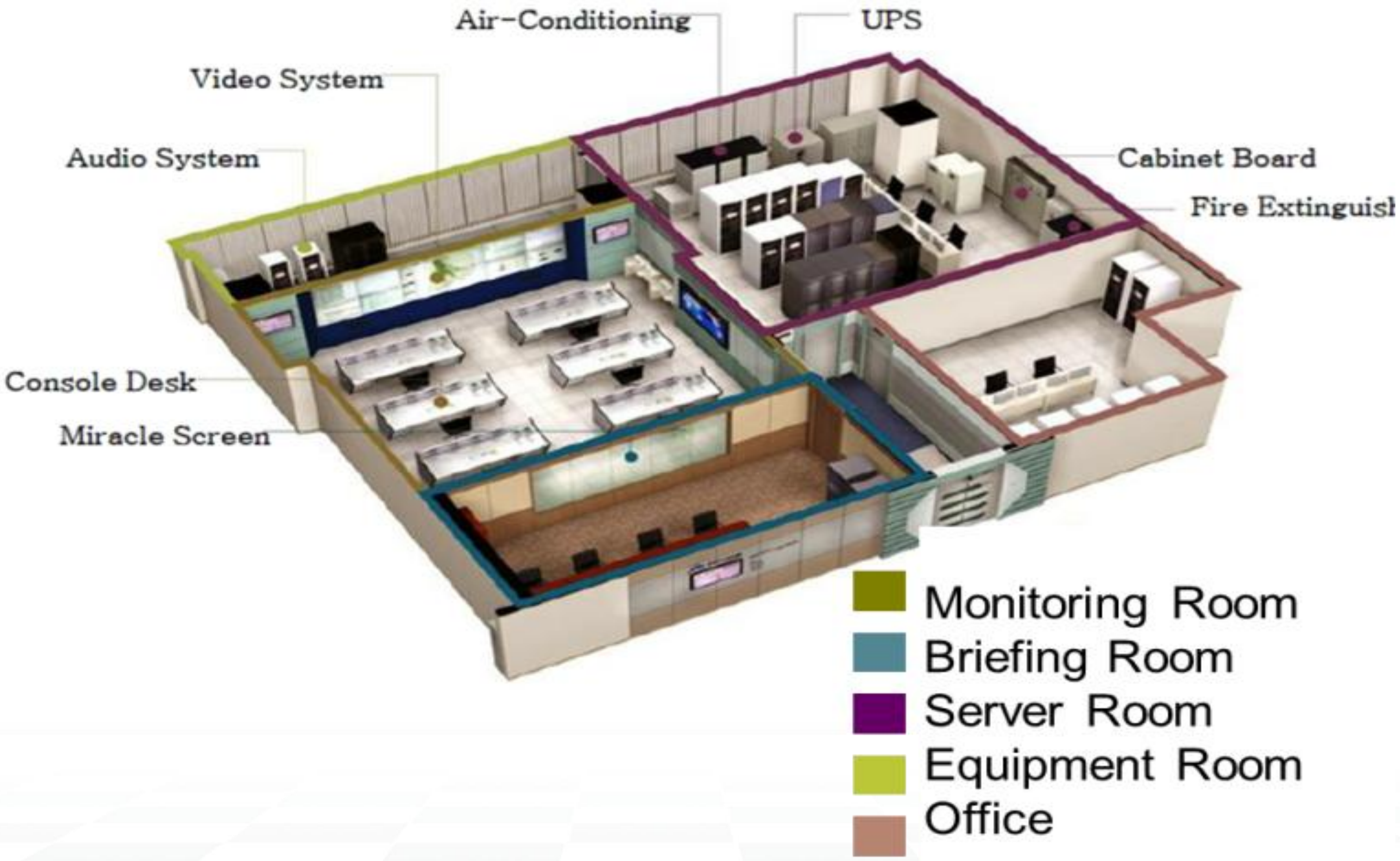
- Construct multi-layered defense system to effectively prevent attacks against major government agencies
- Detect in/out bound traffic that contain attack patterns
- Send the abnormal or unusual traffic to the SOC management system to analyze for attack information of the detected threat


Government Network
Worm/Virus
DDoS
Malware
Government Network Defense System
(Monitoring and detection)
Improve stability of government services and websites
Secure government network
Defend against all cyber threats
SOC
(Collect & Analyze)

[Concept of Protecting the Government Network]

Center Operation Management

The Security Operation Center consists of the Briefing Room, the Monitoring Room, the Server Room, the Equipment Room, and the Video/Audio System.

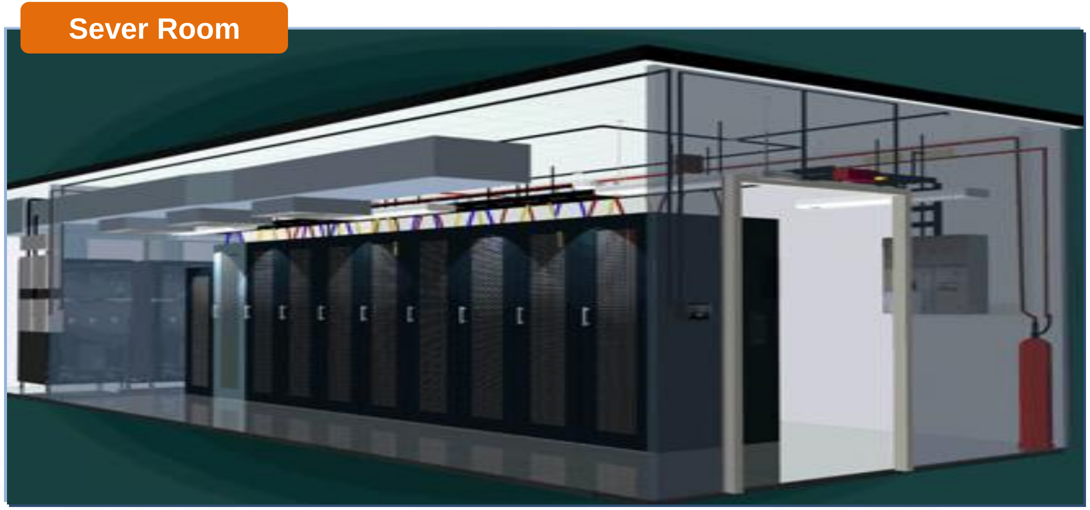


Monitoring & VIP Room

Monitoring Room

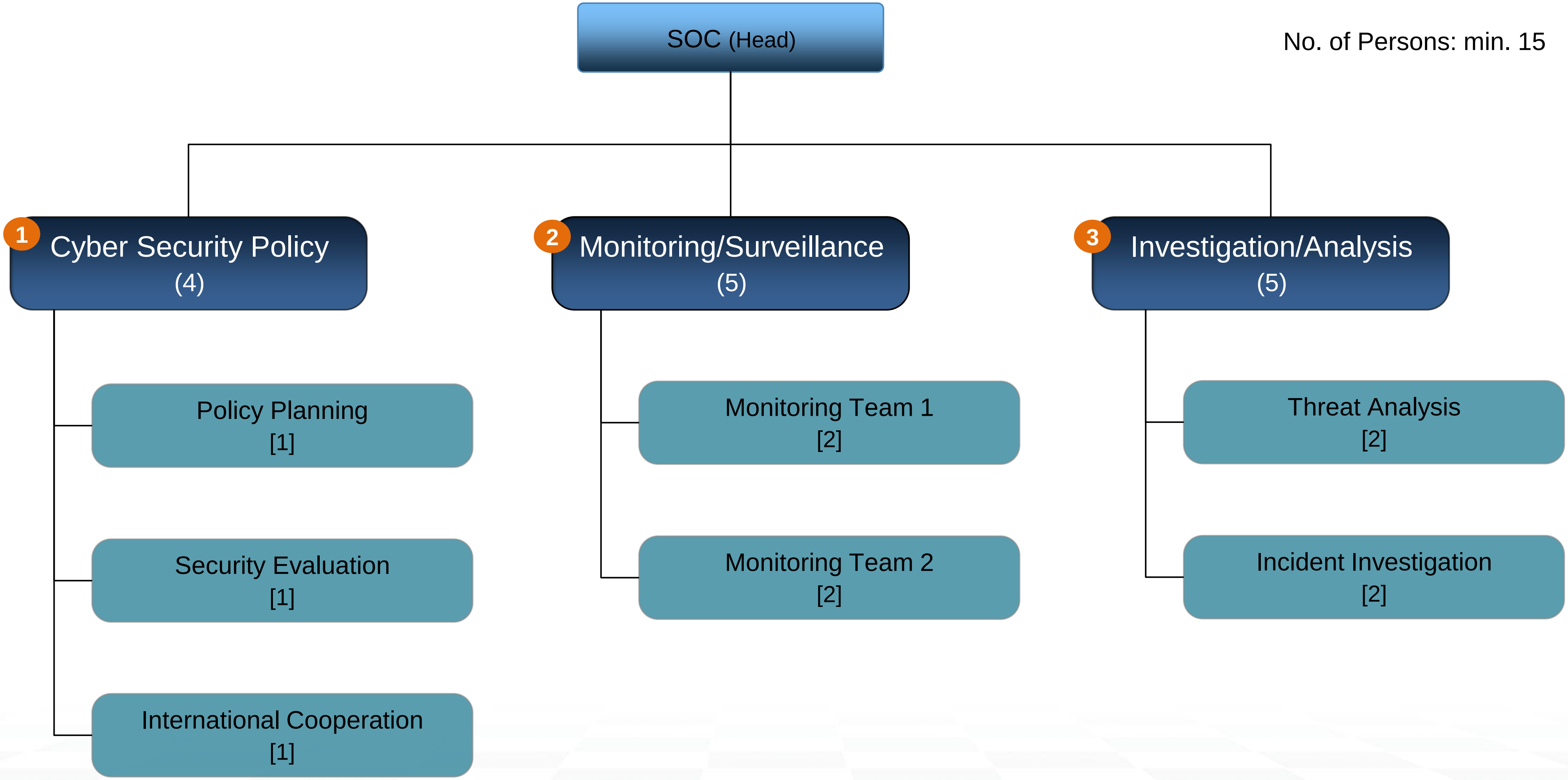
VIP Room

Sever Room



Example of Recommended Organizational Structure

No. of Persons: min. 15



SOC (Head)

1 Cyber Security Policy (4)

- Policy Planning [1]
- Security Evaluation [1]
- International Cooperation [1]

2 Monitoring/Surveillance (5)

- Monitoring Team 1 [2]
- Monitoring Team 2 [2]

3 Investigation/Analysis (5)

- Threat Analysis [2]
- Incident Investigation [2]

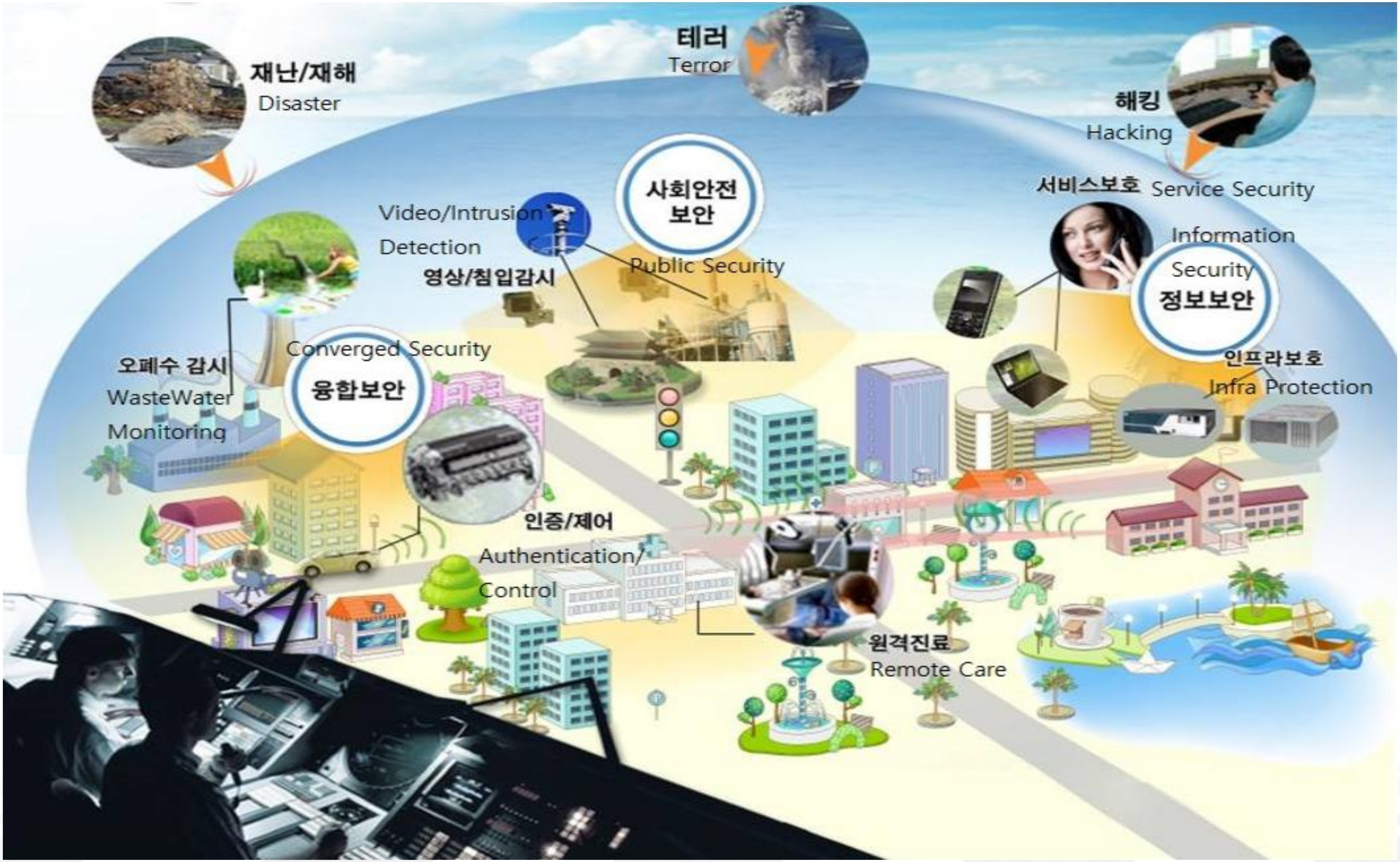
Training

Training needs of the organization in charge of cyber security must be assessed for training courses and programs to be designed to match such needs in order to maximize investment in training. These courses and programs are developed by experts in relevant fields and are designed to accelerate productivity and facilitate adoption of information security solutions quickly and efficiently.

Category	Objectives	Content	Trainees
Security Training	The main objective of security training is to understand attacker's tactics and strategies in detail to help protect assets. This session provides hands-on experience in finding vulnerabilities and discovering intrusions. It also helps to prevent attacks with detailed countermeasures.	• Basic Hacking • Web Hacking • System Hacking • Malware Analysis • Mobile Vulnerability & Forensics • Incident Response Forensics	1 2
Monitoring Training	The main objective of operation training is to provide a guideline on how to organize and operate the SOC and its procedures. Also it provides in-depth security information with comprehensive incident handling plan and procedures.	• SOC organization and operation • Security monitoring and incident response	1 2 3
CERT Management Training	The main objective of CERT management training is to provide the skills and knowledge required to manage CERT.	• Information Security Management	1 2
Product Training	Product training includes necessary information for system configuration method such as surveillance system, security system, emergency recovery methods, disability reaction method and other methods of operating systems.	• Training related with products implemented on the site - TBD	1 2 3

* These courses can be adjusted in accordance with the customer's needs.

What Is It About?



Introducing Igloo Security Inc.

Brief History

IGLOOSECURITY

ISM Solution/Service No.1, IGLOO Sec.

As of 2015 June

Employees	600
Annual Revenue	56.4M
Average Annual Growth	10%
Engineer ratio	70%
Patents	22
Certificates	14
Awards	28
R&D Investment	13%

Business Areas

SOLUTION

SIEM
(SPiDER TM)

PSIM
(LIGER-1)

Email Security
(e-Scort)

Endpoint Vulnerability Attack Prevention
(KiMO)

SERVICES

On-Site
MSS

Remote
MSS

Information Security Consulting

Attack Simulation

Security Training

Vulnerability Assessment

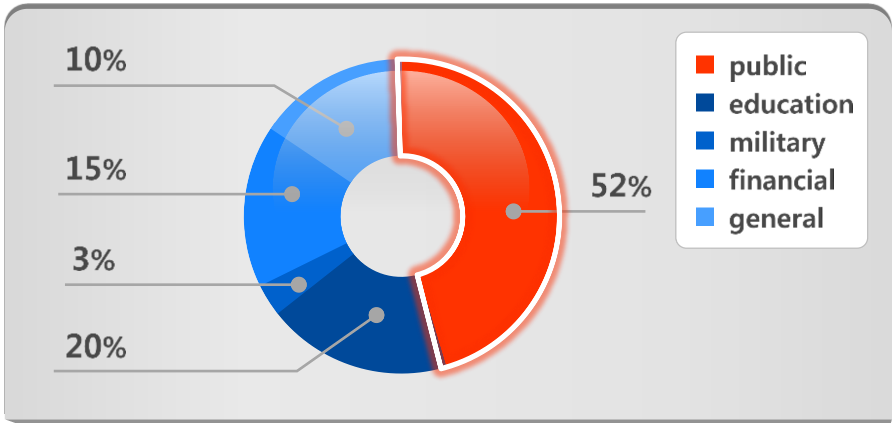
What Can We Do?

	Category	Scope of Tasks					
1	✓ SOC Security Operation Center	Technology	SIEM	3D Monitoring	VMS	Malicious Code / URL Detection and Monitoring System	Homepage Monitoring System
		Infrastructure	Service Network & H/W configuration	Server Room	SMS/NMS/ Security	Monitoring & VIP Room	Power/Disaster Prevention
		Training	Security Training	CERT Management Training	Product Training	Operation Training	
2	International Gateway		Secure stability of domestic services by monitoring harmful traffic	Maintain availability of internet services by controlling application that causes massive traffic	Defend cyber threats by detecting unknown and harmful traffic		
3	National Network		Protect national operational system by detecting in/outbound traffic	Secure the national network by monitoring malicious activity	Secure the national network from various types of DDoS attack		
4	Government Agency Defense		Secure stability of governmental services by defending attacks	Enhance reliability of governmental services by monitoring malicious activities	Defend web application based attack		

Business Reference: Korean Market

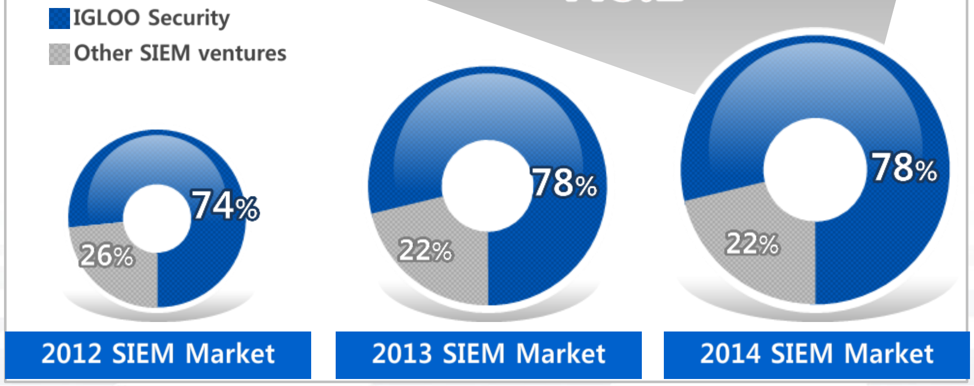
500 Reputable Clients from Various Industries

Industrial ratio in the market



13 years of SIEM Market

No.1



Main Clients

Industry/Education (200)

SAMSUNG
LG
GS칼텍스
KERIS 한국교육학술정보원
LOTTE
NEXON
CJ
HYUNDAI MOBIS

Finance/Telecom./etc./Overseas (140)

NH농협
Leading Tomorrow IBK 기업은행
금융결제원
KB국민은행
한국은행 THE BANK OF KOREA
우리은행
KEB 외환은행
Kdn 한전KDN
SK telecom
LG U+
kt
친환경 에너지기업 한수원(주) 월성원자력본부

Government/Public (160)

법무부 MINISTRY OF JUSTICE
문화체육관광부 Ministry of Culture, Sports and Tourism
금융감독원 FINANCIAL SUPERVISORY SERVICE
ncia 행/정/안/전/부 정부통합전산센터
행정안전부
MOFAT 외교통상부 Ministry of Foreign Affairs and Trade

Successful WinBack Cases

MOFAT 외교통상부 Ministry of Foreign Affairs and Trade
전라남도교육청 JEOLLANAMDO OFFICE OF EDUCATION
경기도교육정보기록원 Gyeonggi-Do Education Information Archives
• • •

Business Reference: Global Market

Country	Site	Project description	Actual solutions and services provided
Ethiopia	**Security Operation Center of National Commercial Bank**	• Establishment of Security Operating Center(SOC) to monitor and respond to cyber-threats from the interior design to the solution deployment. • Delivered training on the management and operation of SOC in order to operate the SOC themselves efficiently and accurately with competence.	• SPiDER TM (SIEM) • SPiDER 3D (3D Visualization Console) • SPiDER-∑ (Information Analysis System) • SPiDER Portal (Information Sharing System) • Vulnerability Management System • Training Service • Maintenance Service
	National Security Operation Center	• Establishment of Security Operating Center(SOC) to monitor and respond to cyber-threats from the interior design to the solution deployment. • Delivered training on the management and operation of SOC in order to operate the SOC themselves efficiently and accurately with competence.	• SPiDER TM (SIEM) • SPiDER 3D (3D Visualization Console) • SPiDER-∑ (Information Analysis System) • Vulnerability Management System • Training Service • Maintenance Service
Rwanda	**National Computer Security Incident Response Team**	• Supplied Security Information and Event Management (SIEM) and other security solutions to monitor and respond to cyber-threats. • Delivered monitoring training on the CSIRT in order to operate the solution.	• SPiDER TM (SIEM) • SPiDER 3D (3D Visualization Console) • SPiDER-∑ (Information Analysis System) • SPiDER Portal (Information Sharing System) • Vulnerability Management System • Penetration Testing Tool • Training Service • Maintenance Service
	National Security Operation Center	• Supplied Security Information and Event Management (SIEM) and other security solutions to monitor and respond to cyber-threats. • Delivered monitoring training on the SOC in order to operate the solution	• SPiDER TM (SIEM) • SPiDER 3D (3D Visualization Console) • Penetration Testing Tool • Training Service • Maintenance Service

Business Reference: Global Market

Country	Site	Project description	Actual solutions and services provided
Morocco	**National Computer Emergency Response Team**	• Delivered information security solutions and carried out on-site installation, testing, and stabilization. • Provided Lecture on the solutions for productive operation and hands-on training.	• SPiDER TM (SIEM) • SPiDER 3D (3D Visualization Console) • SPiDER-∑ (Information Analysis System) • SPiDER Portal (Information Sharing System) • Vulnerability Management System • Training Service • Maintenance Service
Japan	**MSS service company**	• Supplied Security Information and Event Management (SIEM) • Supported Security Monitoring service and initial analysis for incident cases • Delivered training on the operation of Security Monitoring service in order to operate MSS servcice efficiently and accurately with competence.	• SPiDER TM (SIEM) • SPiDER 3D (3D Visualization Console) • Managed Security Service(MSS) • Training Service • Maintenance Service
	SoftBank	• Supplied Security Information and Event Management (SIEM) and other security solutions to monitor and respond to cyber-threats. • Supplied Physical Security Information Management	• SPiDER TM (SIEM) • SPiDER 3D (3D Visualization Console) • LiGER • Maintenance Service
	Fujitsu	• Supplied Security Information and Event Management (SIEM) and other security solutions to monitor and respond to cyber-threats. • Provided stabilization support for effective operation	• SPiDER TM (SIEM) • Maintenance Service

Our Products for Ensuring Your Cyber Security

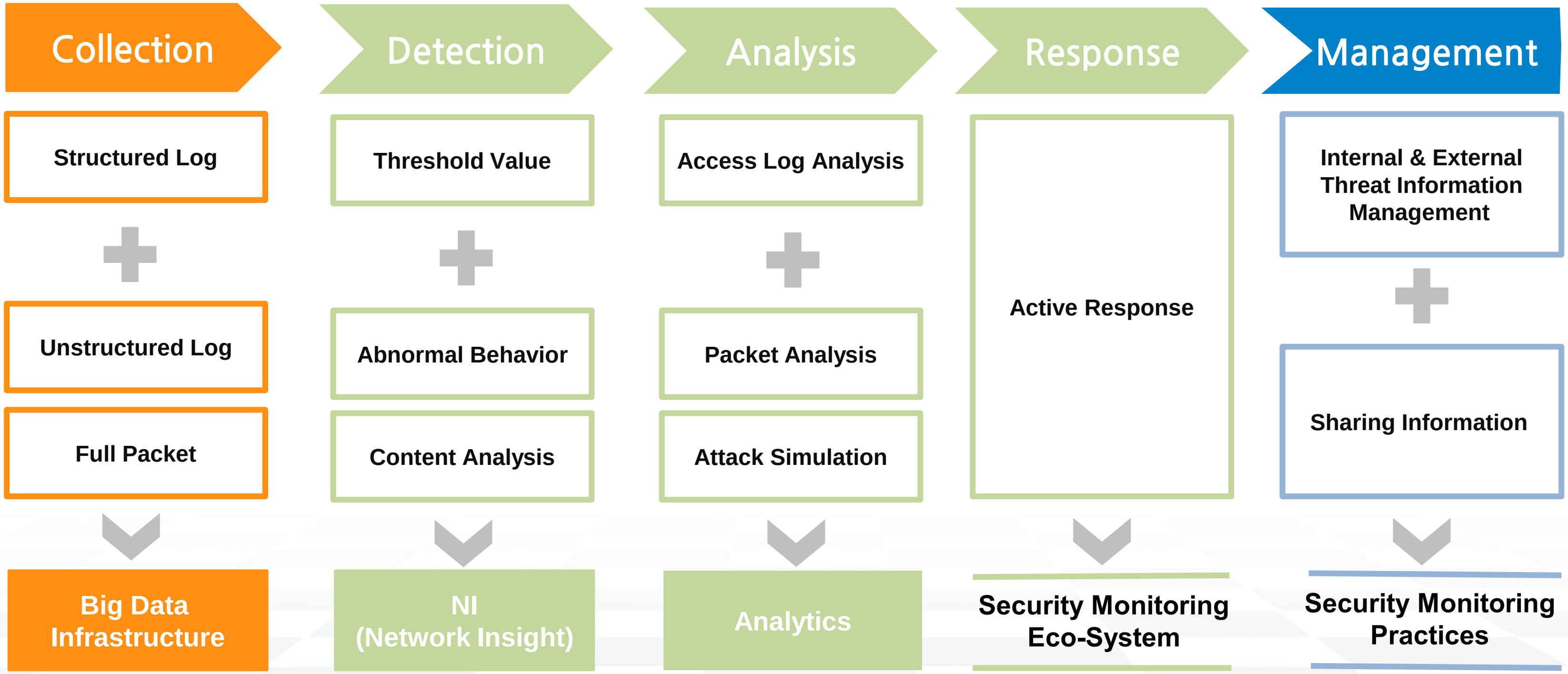
IGLOOSECURITY

SPiDER TM

SPiDER TM **Integrated Security Management Solution**
with accumulated know-how and technology of Managed Security Services and Big data capabilities.

❖ Product Introduction

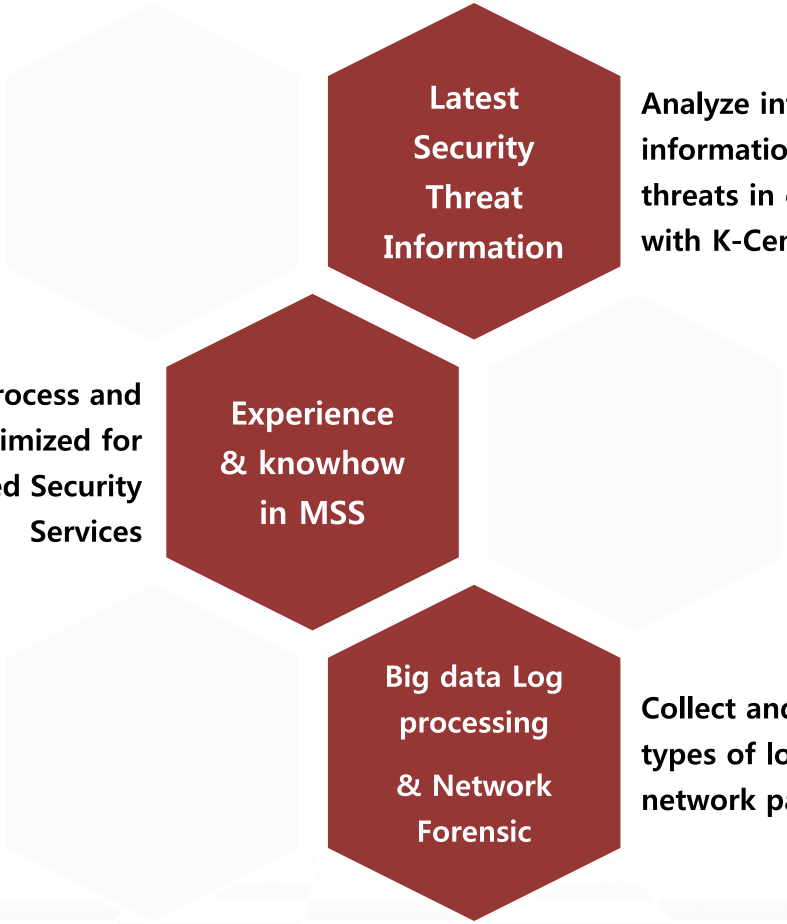
SPiDER TM is an integrated security management solution with 15 years of experience of Managed Security Services and Big data capabilities from IGLOO SECURITY. It can enhance agility and efficiency of security monitoring services through centralized monitoring environment structure from initial detection to log/network packet analysis, at the same time, assuring complete visibility on the overall infrastructure. Also, all logs and network packets are collected and saved in real time and analyze them in connection with the latest external threat information such as harmful IPs and malicious URLs, various threat elements can be quickly and effectively detected, blocked and prevented.



SPiDER TM

SPiDER TM

❖ Advantage of SPiDER TM



Latest Security Threat Information

Analyze internal information and external threats in connection with K-Center

Provide process and function optimized for Managed Security Services

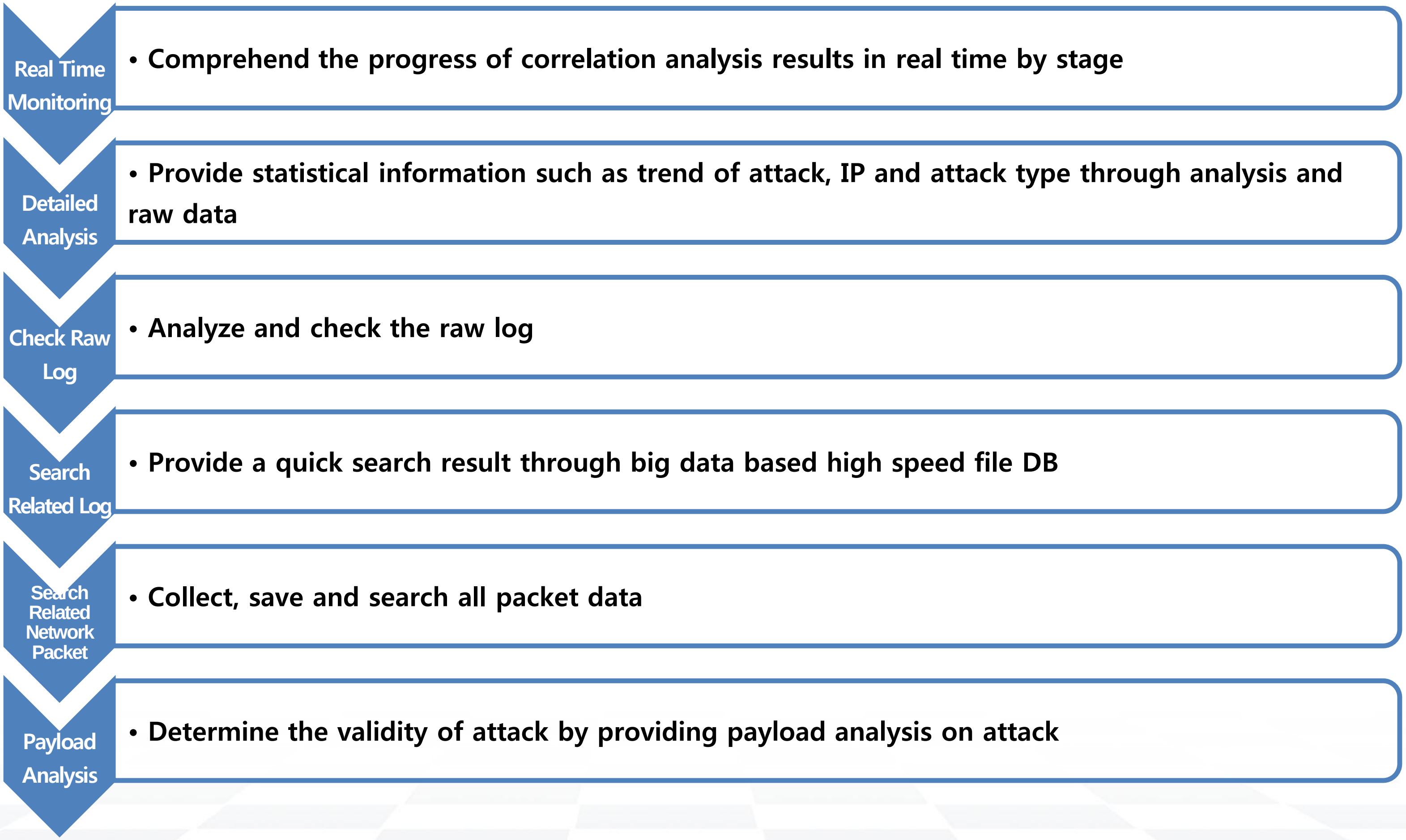
Experience & knowhow in MSS

Big data Log processing & Network Forensic

Collect and analyze all types of logs and all network packets

SPiDER TM

❖ Work Flow



Real Time Monitoring
- Comprehend the progress of correlation analysis results in real time by stage

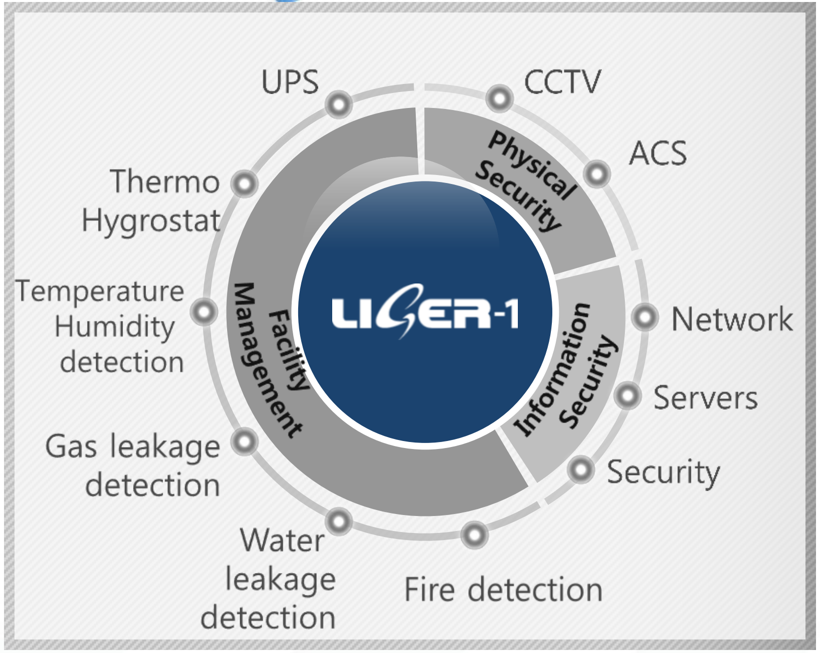
Detailed Analysis
- Provide statistical information such as trend of attack, IP and attack type through analysis and raw data

Check Raw Log
- Analyze and check the raw log

Search Related Log
- Provide a quick search result through big data based high speed file DB

Search Related Network Packet
- Collect, save and search all packet data

Payload Analysis
- Determine the validity of attack by providing payload analysis on attack



LiGER-1 Products

01. iPSIM (Physical Security Information Management)

- Integrates information of heterogeneous systems.
- Risk prevention and response by correlation analysis.

02. iDCM$^+$ (Data Center Management plus)

- Real-time failure detection of various computational facilities : Network security, Door security, Video surveillance, UPS, etc
- Monitoring of power usage

03. iDCM (Data Center Management)

- A system identifying the details of the entire resources in real-time through network topology

04. I^{2}CM (Internal Information Convergence Management)

- A system for evidentiary and prevention of internal information leakage

05. IRM (Integrated Resource Management)

- Identify the status of security devices on site
- Managing of security environment : operating history (Installation, Failure, Repair)and maintenance

IGLOO SECURITY

Thank You!