(GNA-G) GREN SECURITY ACTIVITIES

KISTI SECURITY ACTIVITIES

-INTRODUCTION OF KREONET CYBER–THREAT RESPONSE FRAMEWORK-

Cyber Security R&D Center
YoonSu Lee

Contents

- Overview
- Security Activities
- Security R&D

OVERVIEW

OVERVIEW : Why Security Operation Center?

▣ Cyber Threats

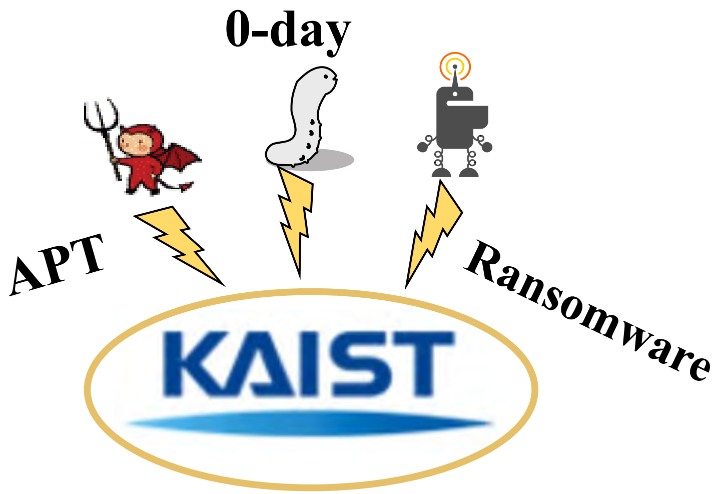
- Constantly evolving, i.e., APT attacks, Ransomware virus, etc
- Emerging unknown attacks, i.e., 0-day, 1-day, etc

▣ Individual organization

- low IT budget, especially information security
- Lack of highly experienced security operators
- Difficulty in managing security Infra. & Policy, etc

▣ Centralized Security Operation Center

- **1) Cost-effective**
  - ➢ 1 security center covers many organizations
- **2) Highly experienced security operators**
  - ➢ Collaboration with other centers, CERTs, etc.
- **3) Apply united security policy**
  - ➢ IDS/IPS, Firewall, etc
- **4) Provide total security service**
  - ➢ Monitoring, Analysis, Response, Consulting, etc.



과학기술사이버안전센터
Sience and Technology Cyber Security Center

Network based Security Service

OVERVIEW : KREONET Cyber-Threat Response Framework

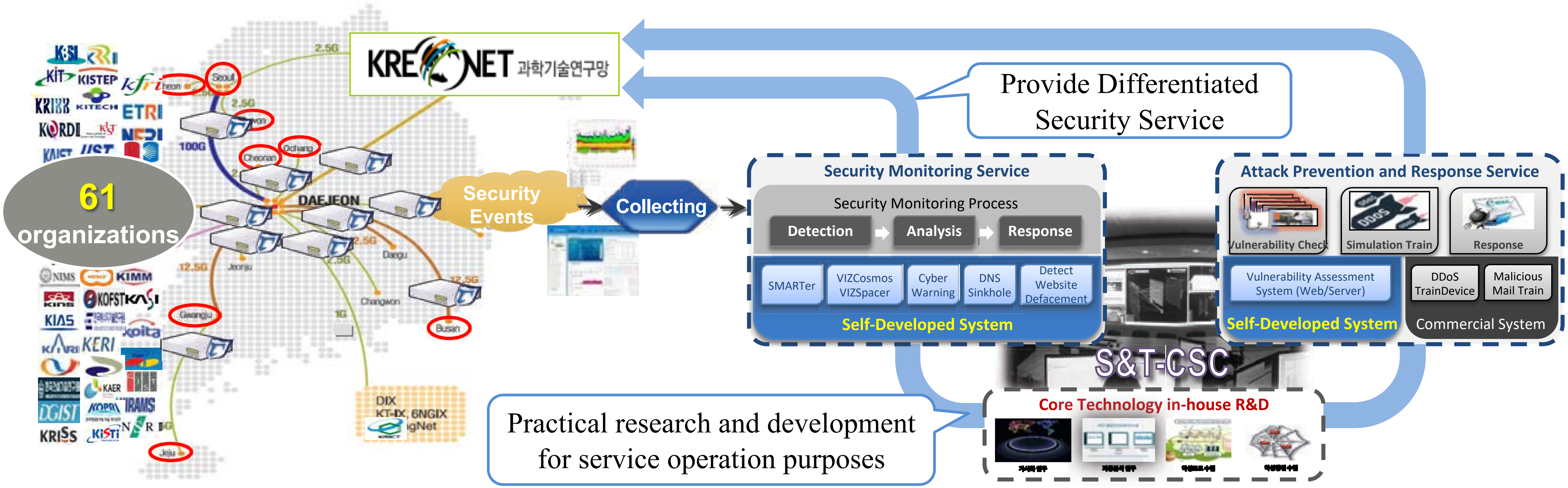
▣ Science & Technology Cyber Security Center (S&T-CSC) Since 2005

- Taking charge of cyber security service for 61 Korea government-funded organizations.

  ☞ ex.: KISTI, KAIST, GIST, ETRI, KIST, etc

- **Security Operation Center**(SOC) based on **KREONET**(Korea Research Environment Open NETworks)

  ☞ Real-time monitoring, analysis and response for cyber threats



Provide Differentiated Security Service

Security Monitoring Service

Security Monitoring Process

Detection → Analysis → Response

SMARTer | VIZCosmos VIZSpacer | Cyber Warning | DNS Sinkhole | Detect Website Defacement

Self-Developed System

Attack Prevention and Response Service

Vulnerability Check | Simulation Train | Response

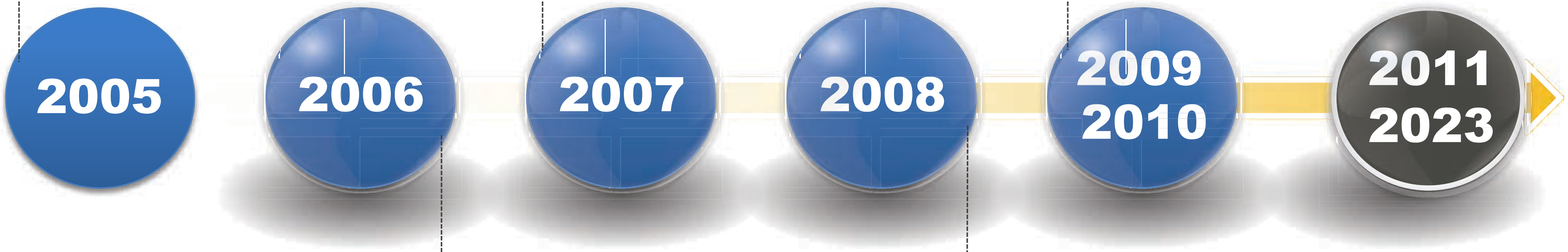
Vulnerability Assessment System (Web/Server) | DDoS TrainDevice | Malicious Mail Train

Self-Developed System | Commercial System

Core Technology in-house R&D

Practical research and development for service operation purposes

OVERVIEW : History of S&T-CSC



The year 2005

Beginning of S&T-SEC

⁎ Security Targets : 10 Institutes

⁎ System : Threat Management System (TMS)

2006

⁎ Security Targets : 20 Institutes

⁎ System : TMS

2007

⁎ Security Targets : 25 Institutes

⁎ Systems : TMS (25 Institutes), Security Monitoring Analysis and Response soluTion (SMART) (10 Institutes)

2008

⁎ Security Targets : 38 Institutes

⁎ Systems: TMS (38 Institutes), SMART (28 Institutes)

2009 ~ 2010

System stabilization

⁎ Security Targets : 39 Institutes

⁎ Systems : TMS (38 Institutes), SMART (28 Institutes)

2011 ~ 2023

Expanding S&T-CSC

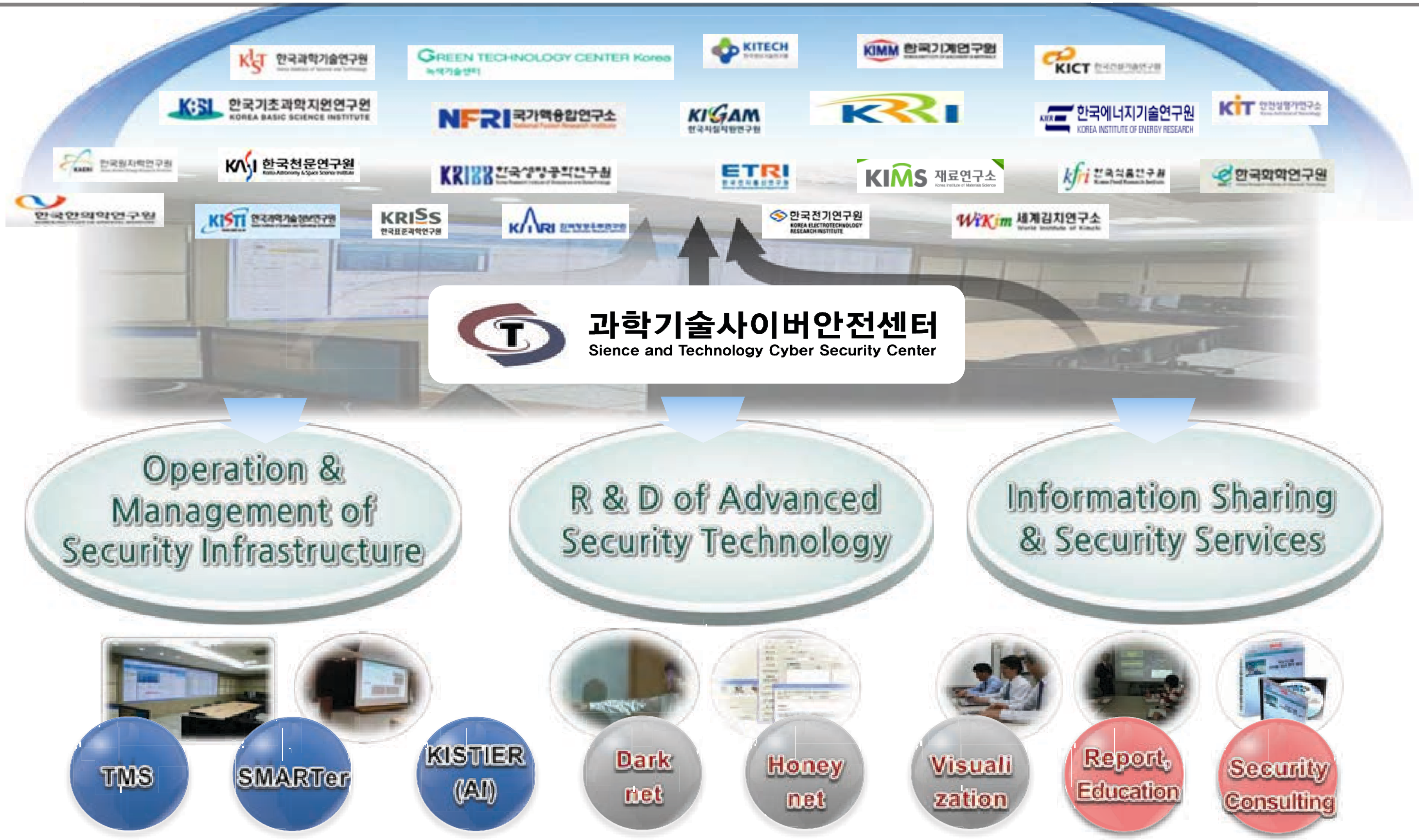
⁎ Security Targets : 190 Institutes

⁎ Systems : TMS(190 Institutes), SMART(26 Institutes)

- KREONET based Security Monitoring

OVERVIEW : Main Role

Provide security monitoring, analysis and response service for 200 organizations



과학기술사이버안전센터
Sience and Technology Cyber Security Center

Operation & Management of Security Infrastructure

R & D of Advanced Security Technology

Information Sharing & Security Services

TMS

SMARTer

KISTIER (AI)

Dark net

Honey net

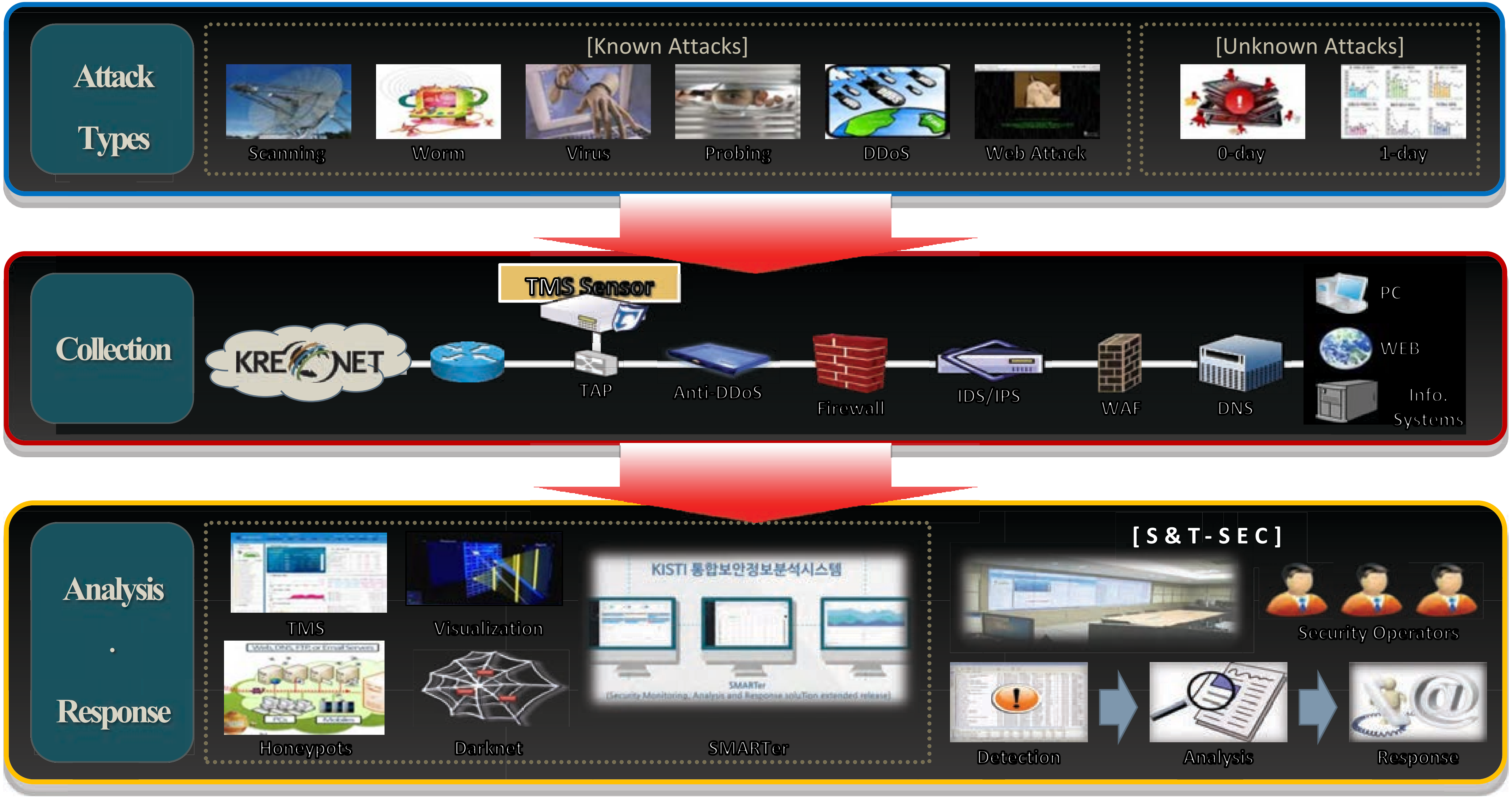
Visuali zation

Report, Education

Security Consulting

SECURITY ACTIVITIES

Security Activities : Monitoring, Analysis and Response (1/3)



Attack Types

[Known Attacks]

Scanning

Worm

Virus

Probing

DDoS

Web Attack

[Unknown Attacks]

0-day

1-day

Collection

KREONET

TMS Sensor

TAP

Anti-DDoS

Firewall

IDS/IPS

WAF

DNS

PC

WEB

Info. Systems

Analysis · Response

TMS

Visualization

Honeypots

Darknet

KISTI 통합보안정보분석시스템

SMARTer

(Security Monitoring, Analysis and Response soluTion extended release)

SMARTer

[S&T-SEC]

Security Operators

Detection

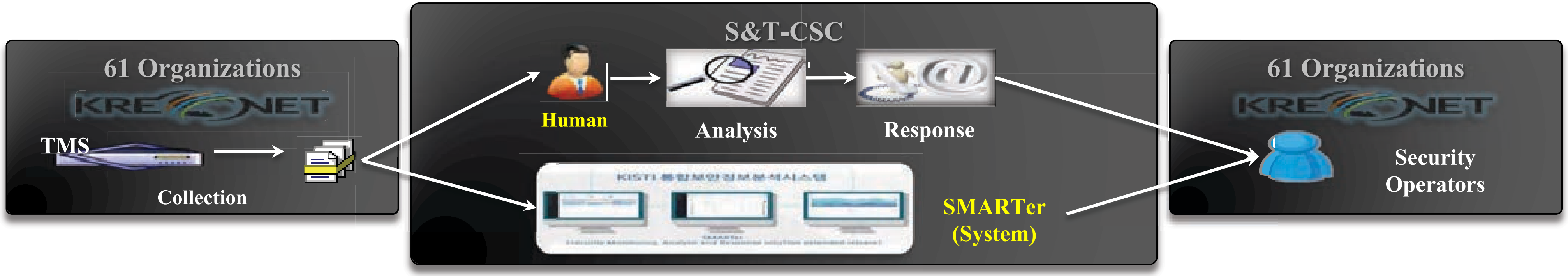
Analysis

Response

Security Activities : Monitoring, Analysis and Response (2/3)

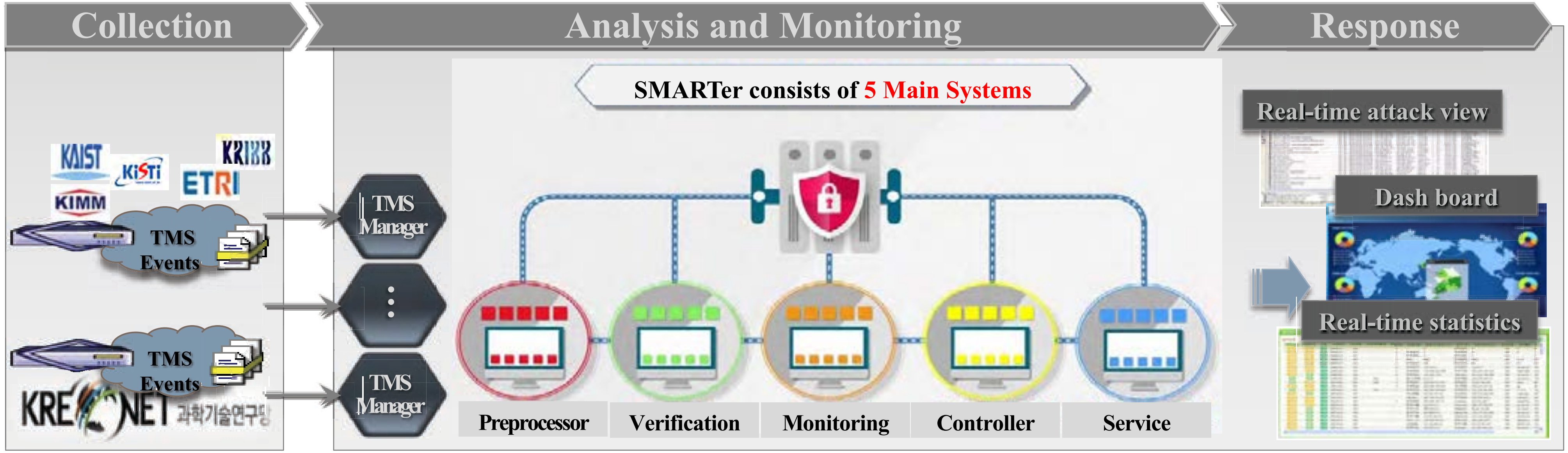
Overall Framework of S&T-SEC

Analysis Based on Human + System



SMARTer

(Capacity)1 million security events per 1 min → Semi-Auto Analysis → Quick Notification



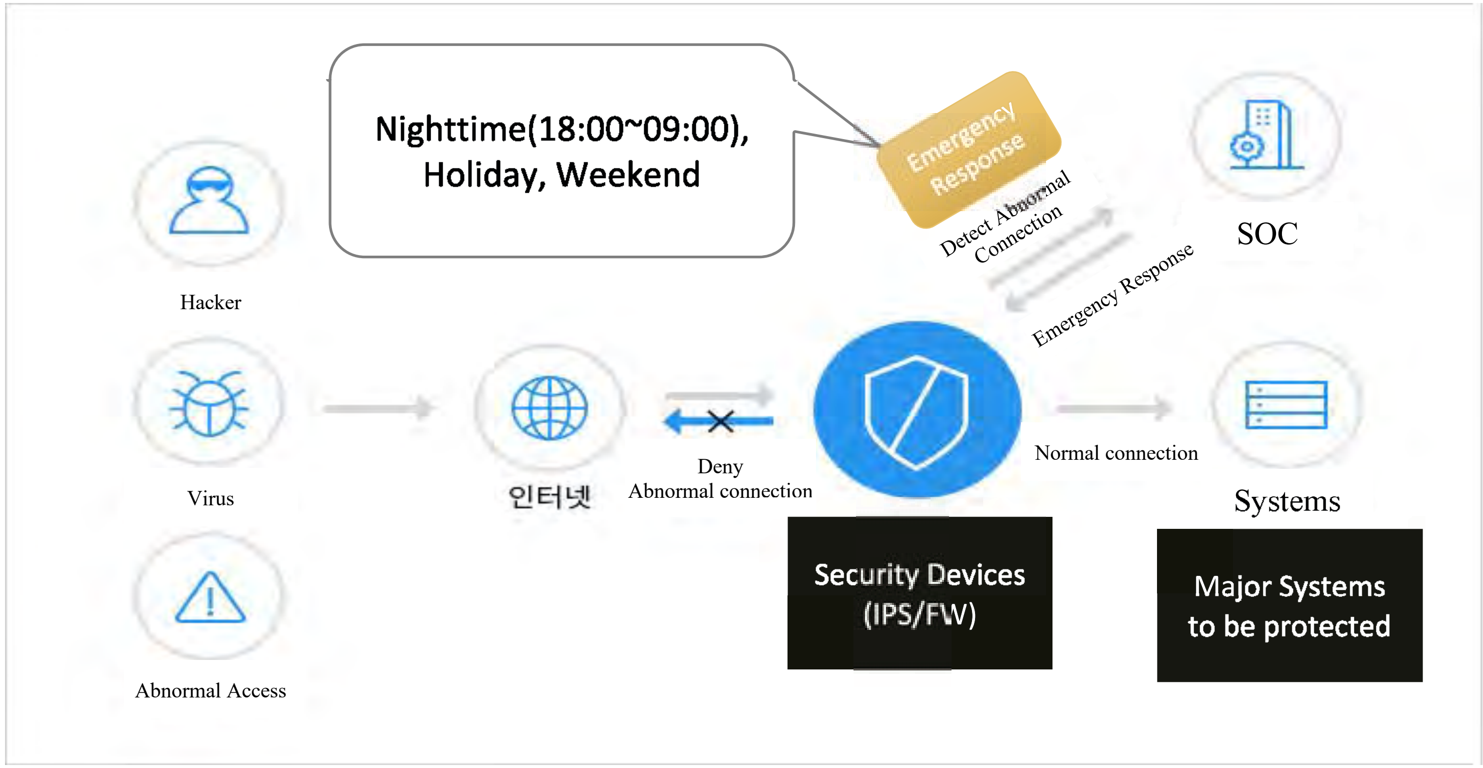
SMARTer : Security Monitoring, Analysis and Response soluTion extended release

Security Activities : Monitoring, Analysis and Response (3/3)

Emergency Response

Response support for situations in which response is impossible for the information security manager

For minimize damage by Cyber attacks, **SOC deny abnormal connection** between attacker and victim **during non-business hours**



Nighttime(18:00~09:00), Holiday, Weekend

(2022-Trial Service)

8 Organizations

↓

(2023-Official Service)

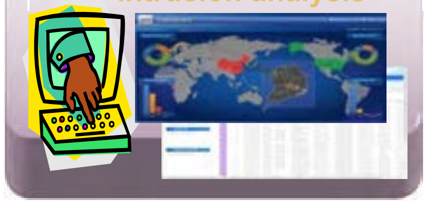
61 Organizations

Security Activities : Accident Analysis & Recovery

On-Off Site Accident Countermeasures

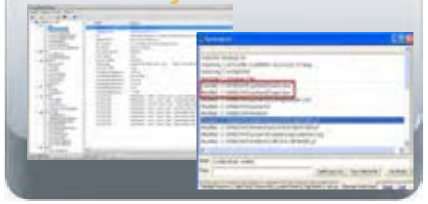
Detection

Receiving requests of intrusion analysis



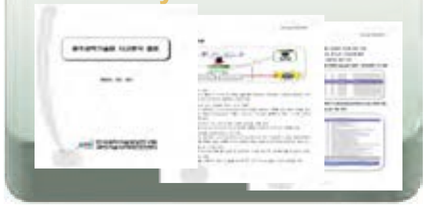
On-site Analysis

Inspecting the targeted systems



Report

Reporting analyzed results



Response

Applying the reports for the target systems

Off site Analysis : Systems

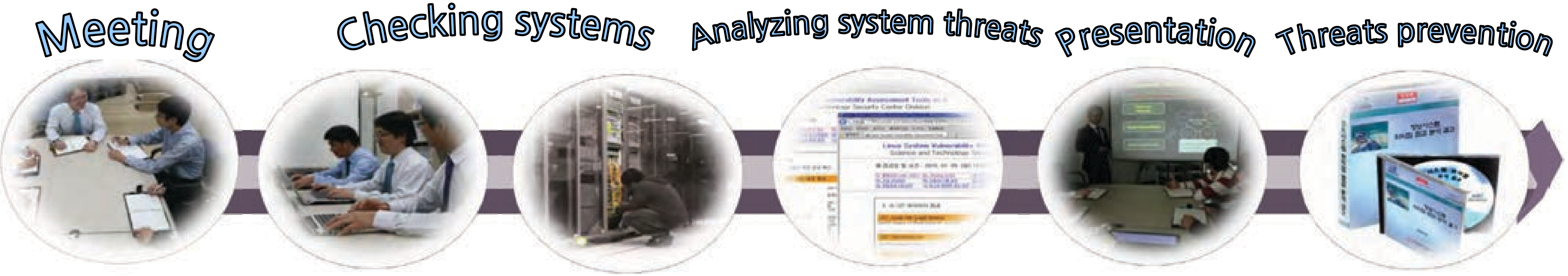
Inspecting compromised systems

Off site Analysis : Websites

Inspecting abnormal homepages

Security Activities : Security Consulting

Security Consulting for Preventing Cyber Threats and Attacks

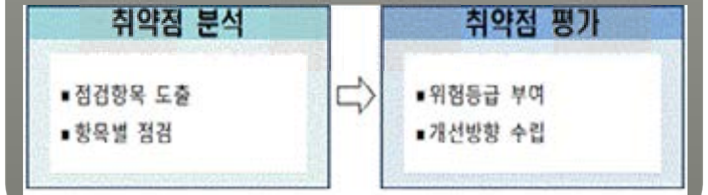


Activities for threats prevention

Vulnerability Assessment

Check Vulnerabilities and elimination

Vulnerability Check System (Website)	Vulnerability Check System (Server)	Vulnerability Check by human (Website)


취약점 분석

- 점검항목 도출
- 항목별 점검

취약점 평가

- 위험등급 부여
- 개선방향 수립

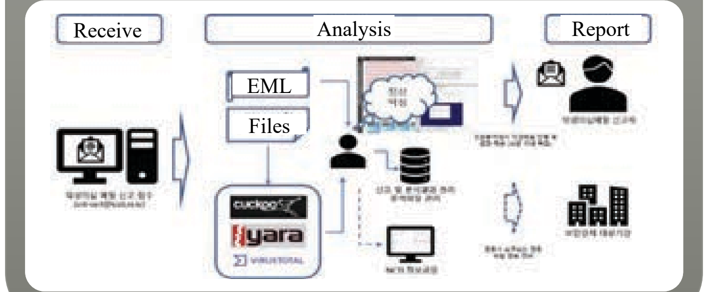
Simulation Training

Train Human and System against cyber threat

Security Policy		Security Technique		
Emergency alarm	Role play for emergence situation	Penetration	Malicious Mail Attack	DDoS Attack

Analysis Malicious Mail

Receive Suspicious mails from Orgs, Analysis and Response for malicious mail



Security Activities : Information Sharing & Education

Security Technology Trend and Security Guide for Institutes

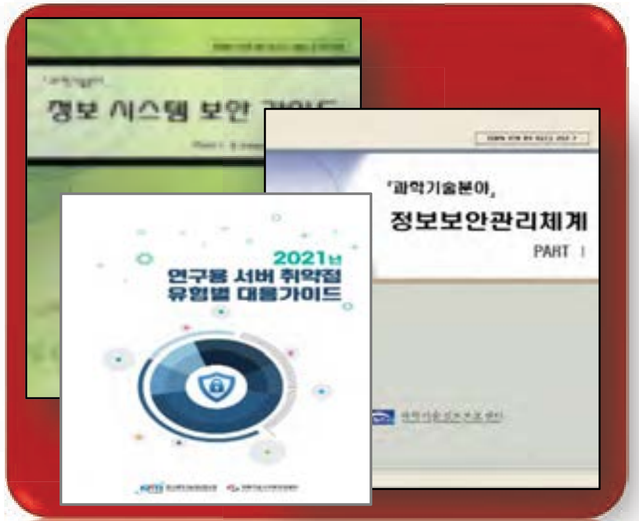
A. Security trend reports

B. Security guidebooks

C. Security Education

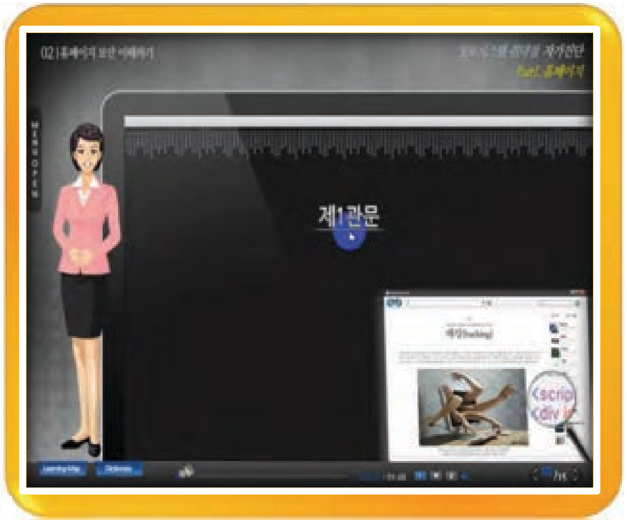
「과학기술분야」
월간 사이버위협동향 보고서
2021년 03월

「과학기술분야」
월간 관제현황 보고서
2021년 03월


정보 시스템 보안 가이드

2021년
연구용 서버 취약점
유형별 대응가이드

「과학기술분야」
정보보안관리체계
PART Ⅰ

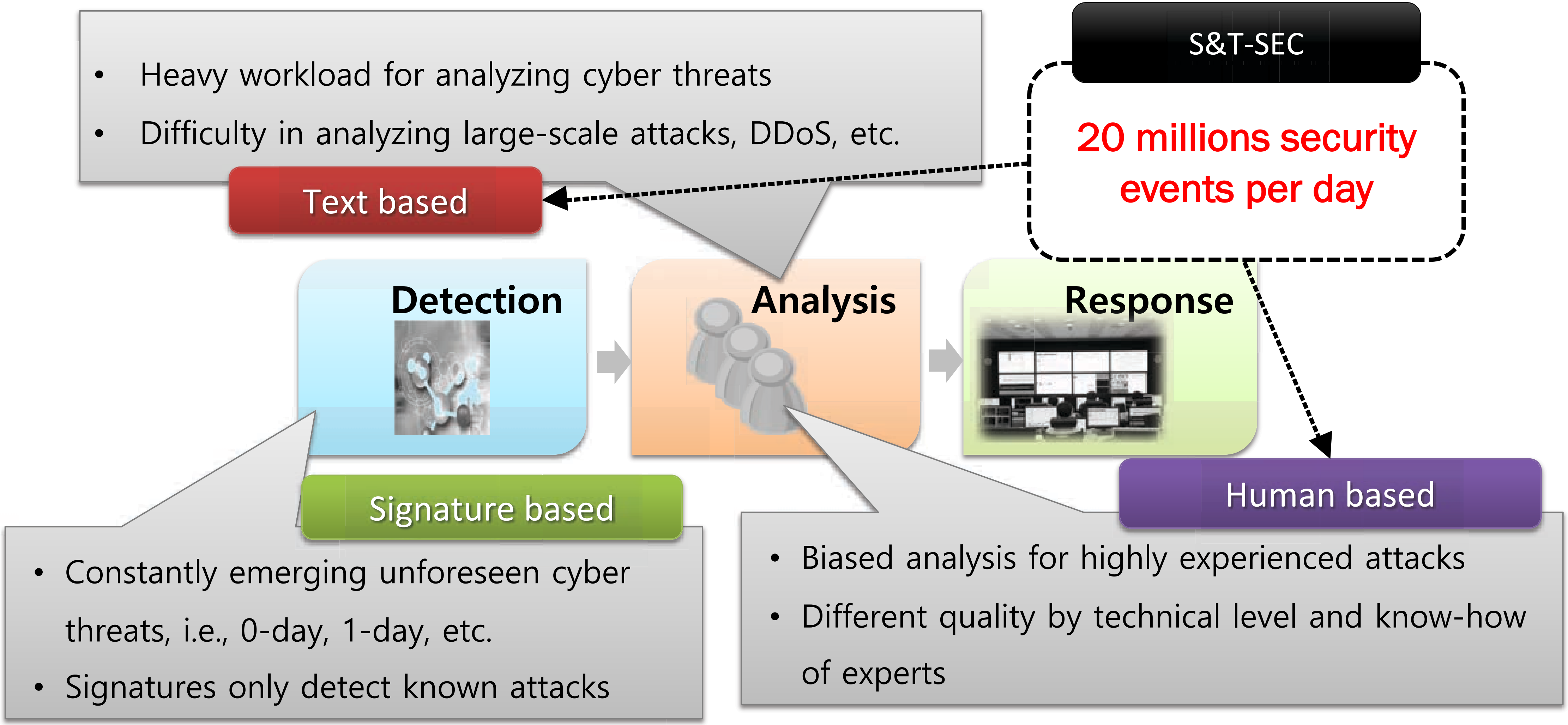


SECURITY R&D

R&D : Technical Issues

Low analysis efficiency → Text and Human

Focusing on Known Attacks → Signature



- Heavy workload for analyzing cyber threats
- Difficulty in analyzing large-scale attacks, DDoS, etc.

Text based

S&T-SEC

20 millions security events per day

Detection

Analysis

Response

Signature based

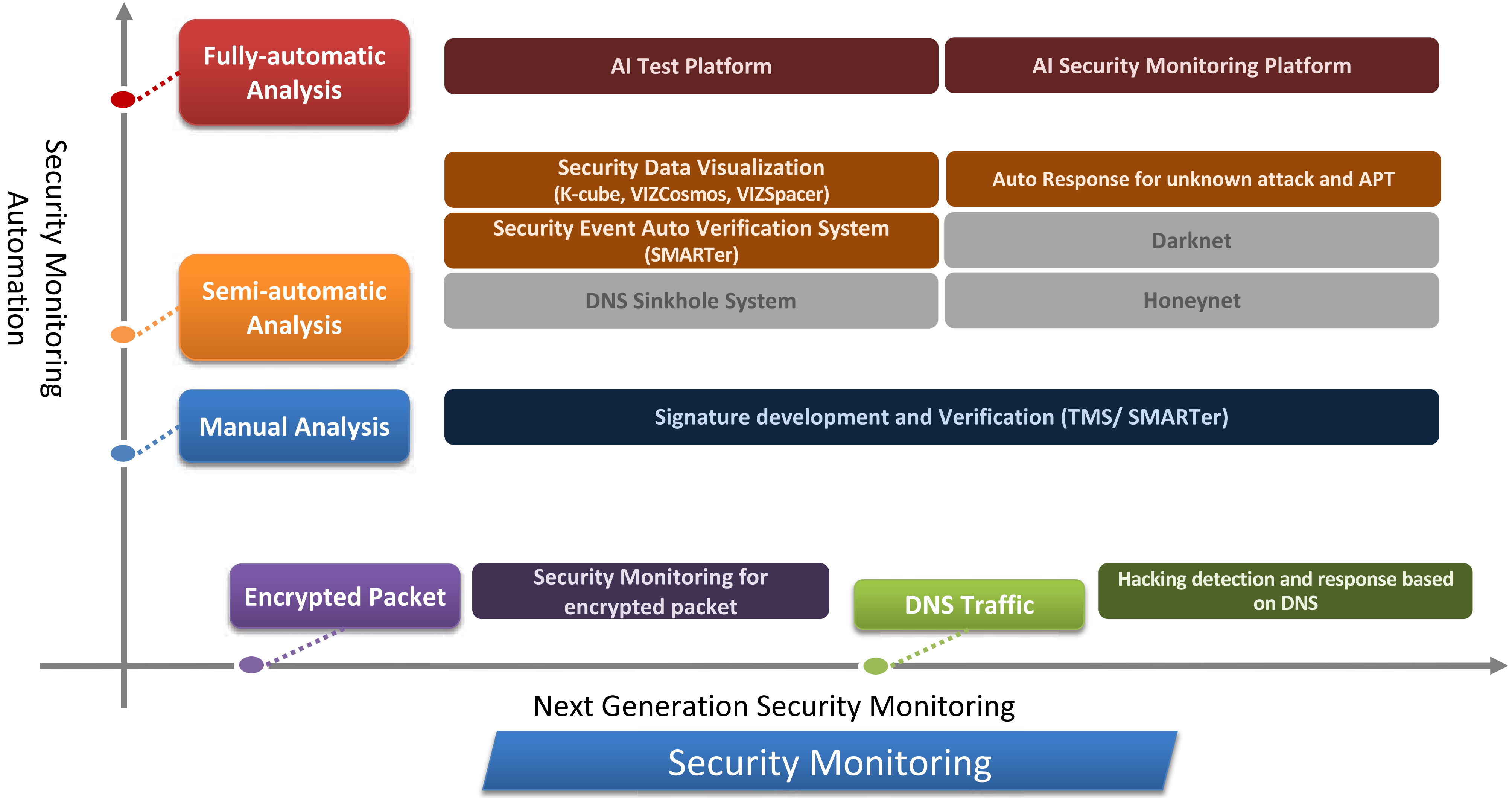
- Constantly emerging unforeseen cyber threats, i.e., 0-day, 1-day, etc.
- Signatures only detect known attacks

Human based

- Biased analysis for highly experienced attacks
- Different quality by technical level and know-how of experts

R&D : Roadmap – Human based → System based

Conduct Various R&D for Security Monitoring Automation and Next Generation Security Monitoring



Security Monitoring Automation

Fully-automatic Analysis

AI Test Platform

AI Security Monitoring Platform

Security Data Visualization (K-cube, VIZCosmos, VIZSpacer)

Auto Response for unknown attack and APT

Security Event Auto Verification System (SMARTer)

Darknet

Semi-automatic Analysis

DNS Sinkhole System

Honeynet

Manual Analysis

Signature development and Verification (TMS/ SMARTer)

Encrypted Packet

Security Monitoring for encrypted packet

DNS Traffic

Hacking detection and response based on DNS

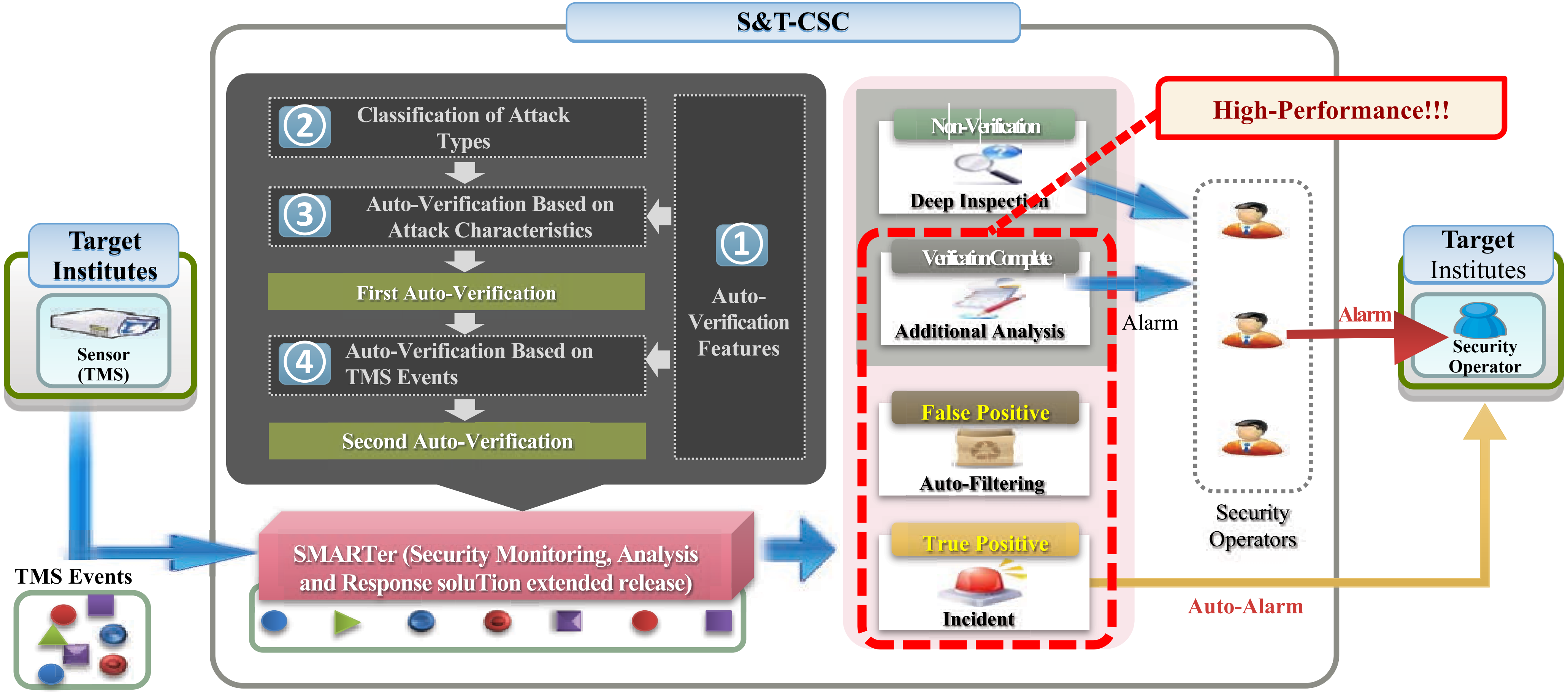
Next Generation Security Monitoring

Security Monitoring

R&D : SMARTer

Auto-Verification Algorithms for analysis techniques and know-how

Concept of SMARTer : Automated Verification of Security Events



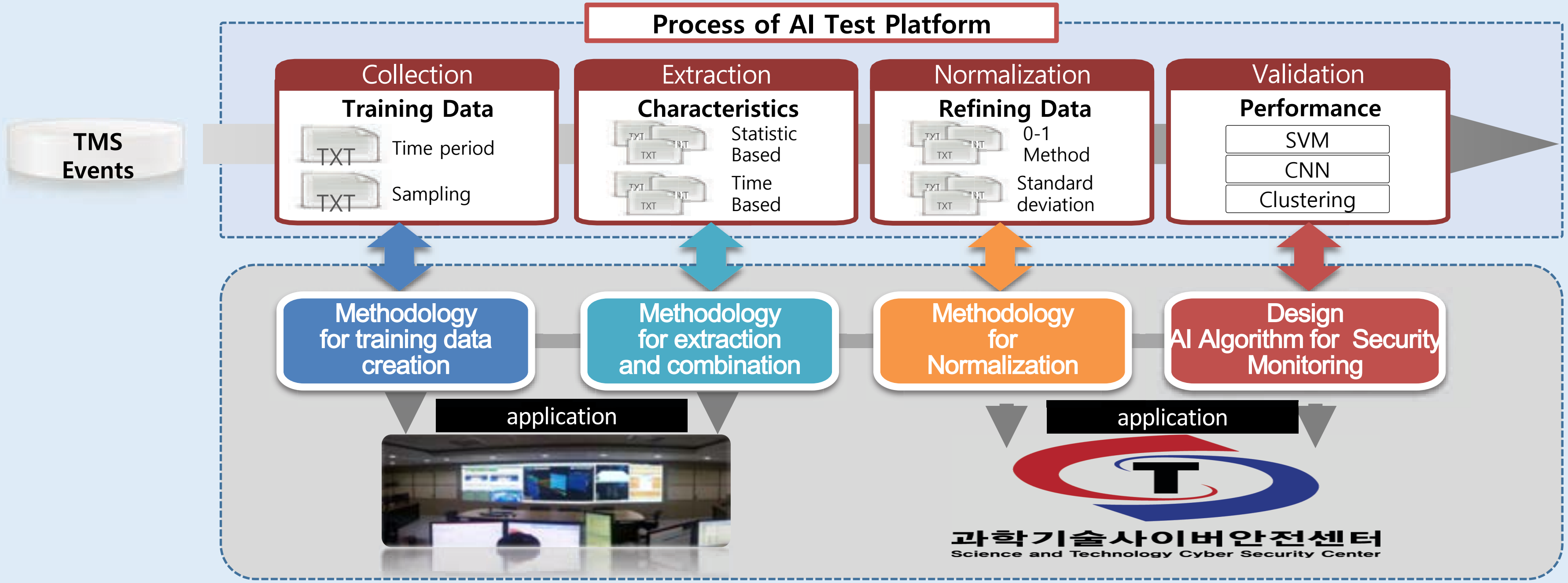
R&D : KISTler

Automation total AI creation process with one flow & AI Model Optimization for security monitoring

AI Building Platform of Building AI Models for Security Monitoring (2018 ~)

Research environment to develop AI Security Monitoring Methodology

- There are numerous information that are created by various security systems(Firewall, IDS, IPS, VPN, and others), so it is not easy to adopt Artificial Intelligence on Security Monitoring Area.
- **AI Test Platform for Security Monitoring will be established to perform various research on Collection, Extraction, Normalization, and Validation phase for develop an AI system for Security Monitoring**



Process of AI Test Platform

TMS Events

Collection
Training Data
TXT Time period
TXT Sampling

Extraction
Characteristics
Statistic Based
Time Based

Normalization
Refining Data
0-1 Method
Standard deviation

Validation
Performance
SVM
CNN
Clustering

Methodology for training data creation

Methodology for extraction and combination

Methodology for Normalization

Design AI Algorithm for Security Monitoring

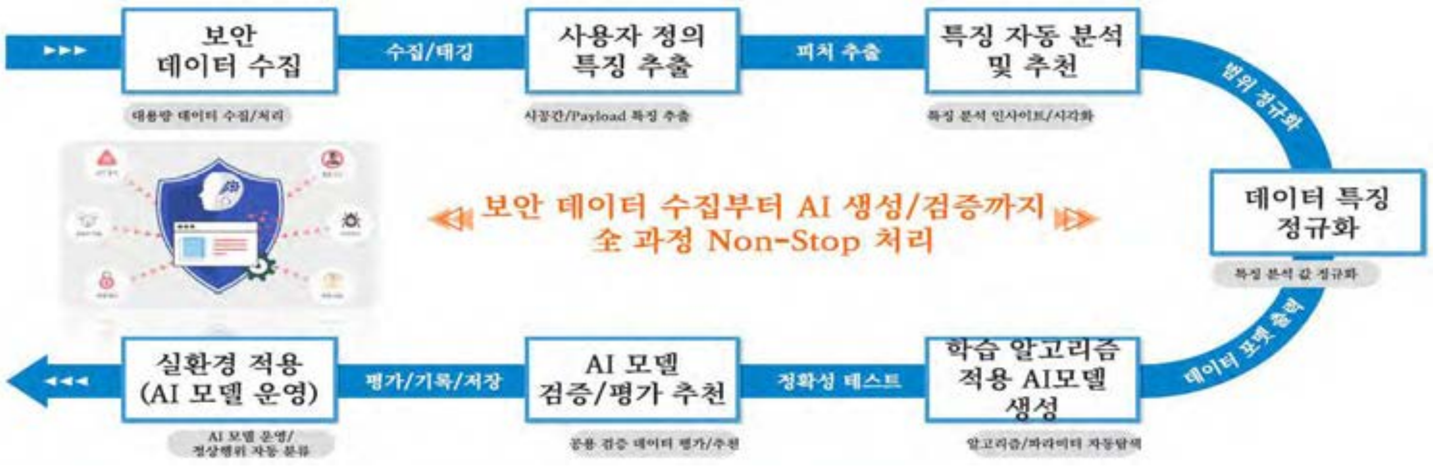
application

application

과학기술사이버안전센터
Science and Technology Cyber Security Center

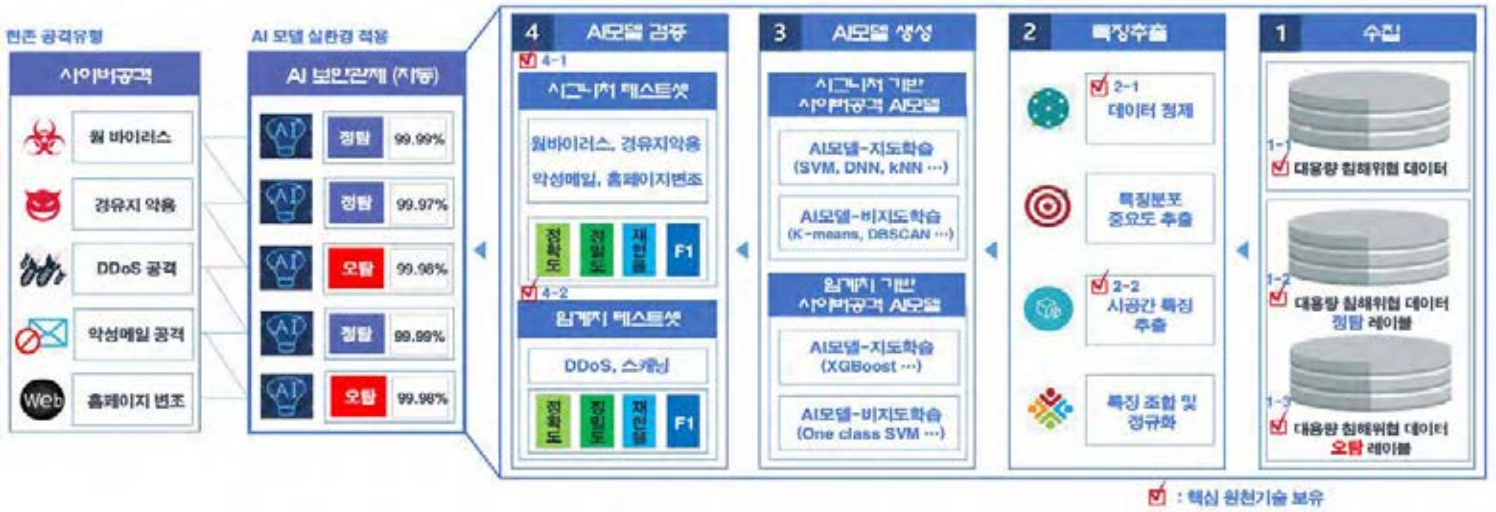
R&D : KISTler

Automation total AI creation process with one flow & AI Model Optimization for security monitoring



Automation total AI creation process with one flow

AI Model Optimization for security monitoring



R&D : Visualization of IDS Alerts

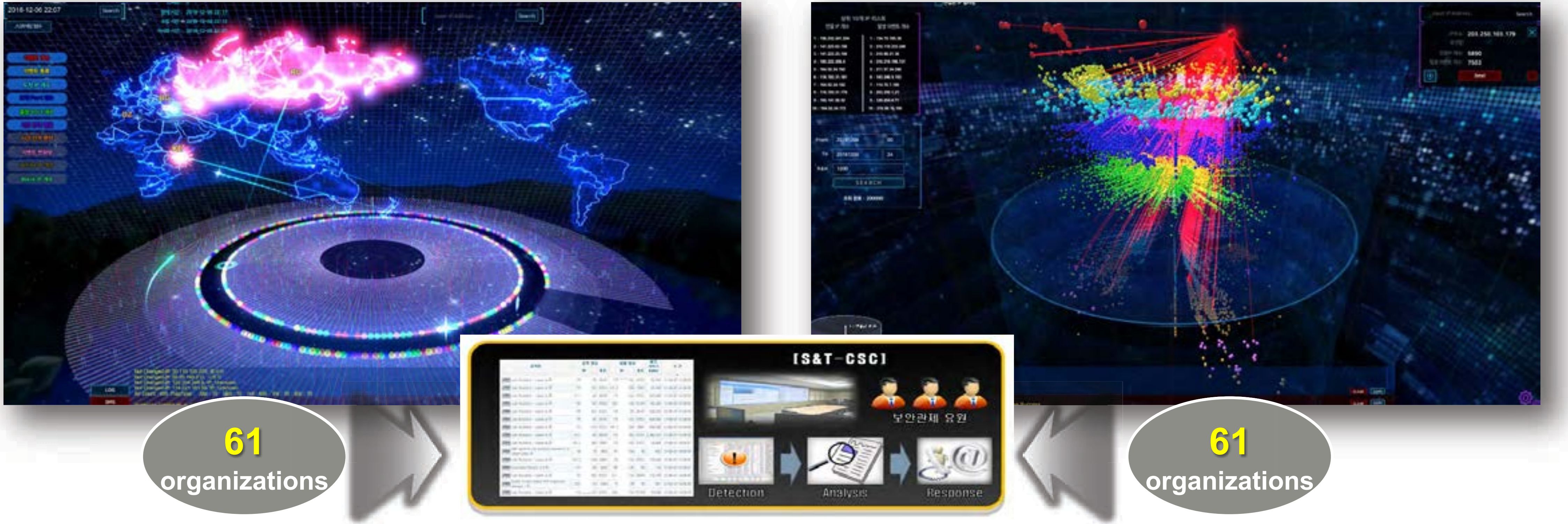
Overcome of the main limitation (Text-based analysis) in SMARTer & AI models

VizSpacer — Monitoring Behaviors of Each System

VizCosmos — Correlation Analysis for All IPs

Vizualization of Security events, potential attacks and root causes for emergence response

Vizualization of Correlation of security events and Monitoring of sophisticated attacks



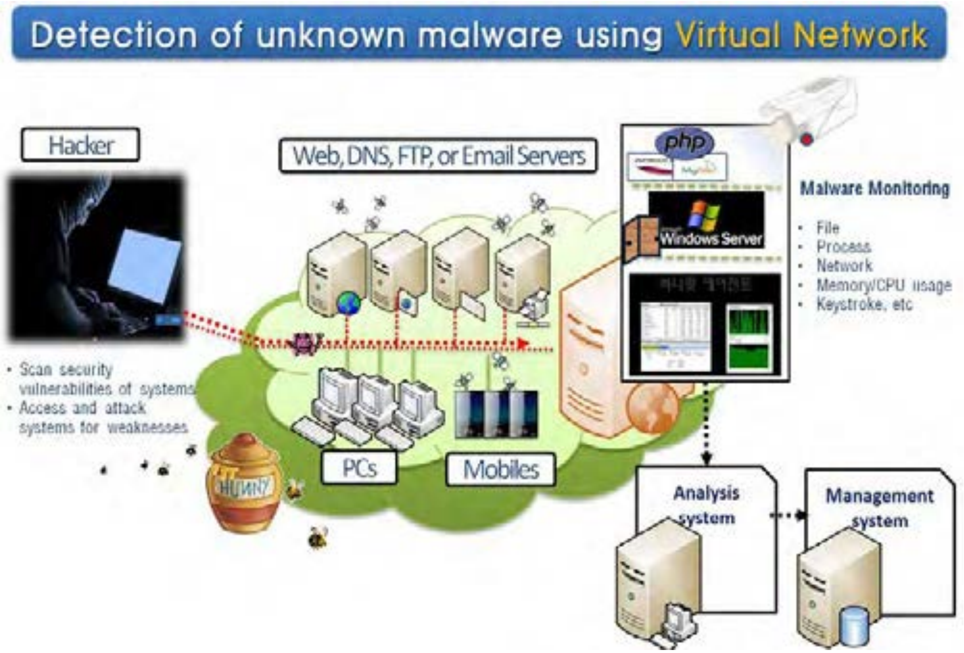
61 organizations

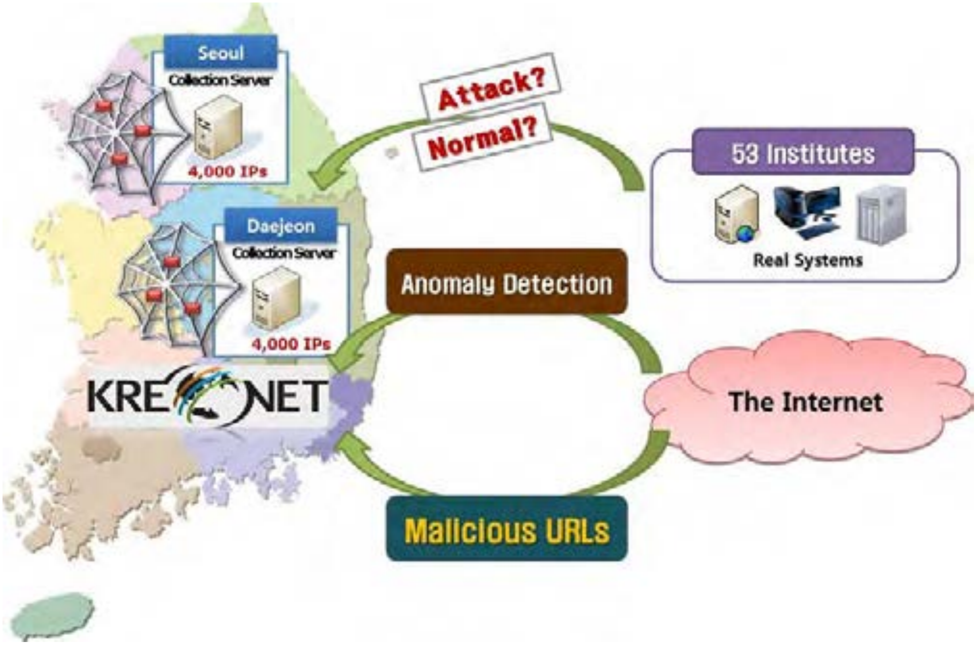
61 organizations

R&D : Honeynet and Darknet

▣ **A network consisting of virtual systems, i.e., servers, personal computers and mobile phones with intentional vulnerabilities.**

- Has been set up from 2013 to 2014, to invite hackers to the virtual systems and collect and analyze their activities and methods.
- Allows detecting unknown malicious activities and codes.


Detection of unknown malware using Virtual Network
Hacker
Web, DNS, FTP, or Email Servers
php
Windows Server
Malware Monitoring
• File
• Process
• Network
• Memory/CPU usage
• Keystroke, etc
• Scan security vulnerabilities of systems
• Access and attack systems for weaknesses
HUNNY
PCs
Mobiles
Analysis system
Management system



Detection, analysis and Response for Unknown attacks

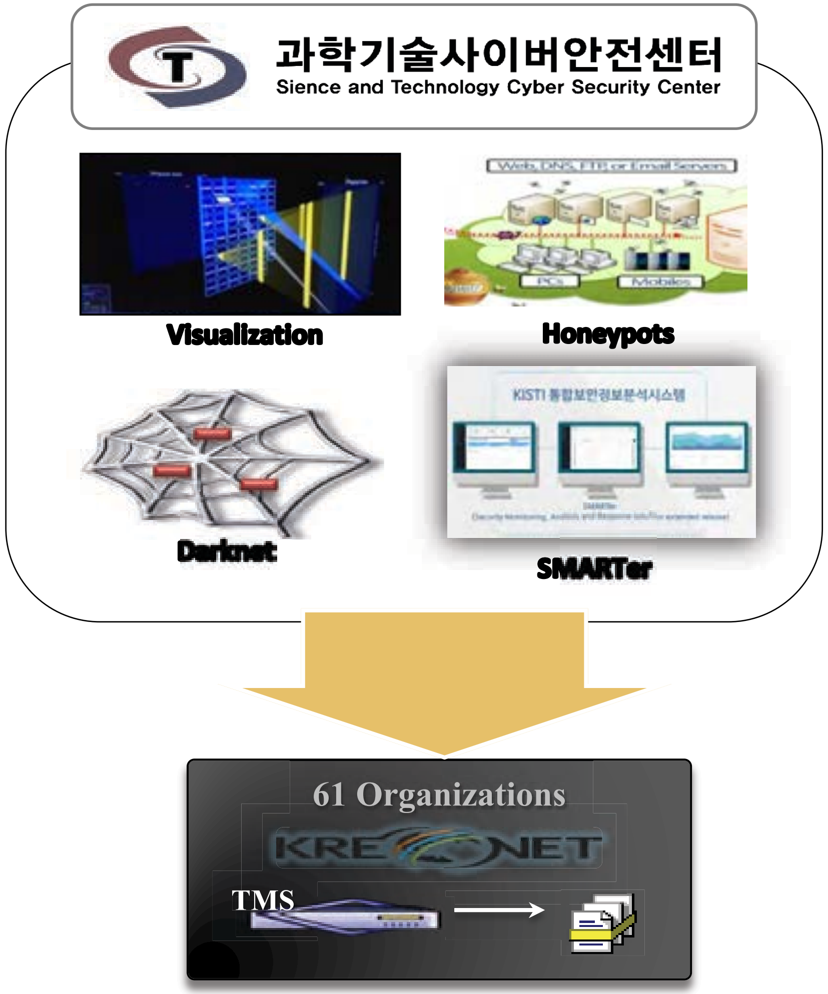
Conclusion

▣ S&T-CSC

- Has **experience, know-how and techniques more than 18 years**
- **Security Monitoring, Analysis and Response** technology
  - ➢ SMARTer : building a lightweight solution('16)
  - ➢ Visualization System : K-Cube, VizSpacer/CosMos
  - ➢ Honeypots and Darknet, AI Platform, etc.
- Various Security Services
  - ➢ On-off site accident analysis
  - ➢ Emergency Response
  - ➢ Security consulting
  - ➢ Security Education, etc

▣ Other countries, ministries, CERTs, etc

- Collaboration with S&T-CSC
  - ➢ Technology transfer, MoU, etc.
- Effectively deploy and manage security infra. & policy, etc.
- Provide high-quality security service


과학기술사이버안전센터
Sience and Technology Cyber Security Center
Visualization
Honeypots
Darknet
SMARTer
61 Organizations
KREONET
TMS