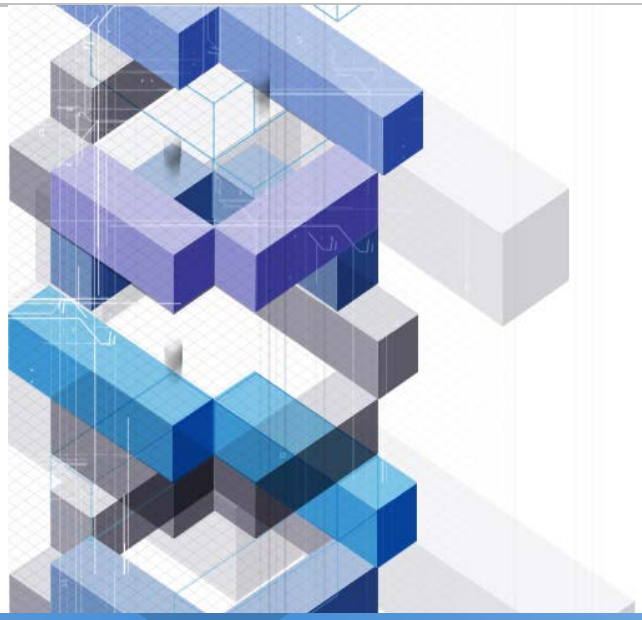


Collection, analysis and response stages

Consisting 6 core module

www.ecsc.go.kr

교육사이버안전센터
Education Cyber Security Center

Contents

1 Overview

2 Collection

3 Analysis

4 Response

Overview

❖ Technical Introduction to Korea's ECSC security monitoring method

- **How to collect security information** from different institutional heterogeneous security systems
- **How to implement correlation analysis** on the mass data collected
- **How to effectively respond** to intrusion incidents

[Security Information]

● Information detected by pattern-based security system such as IPS or IDS

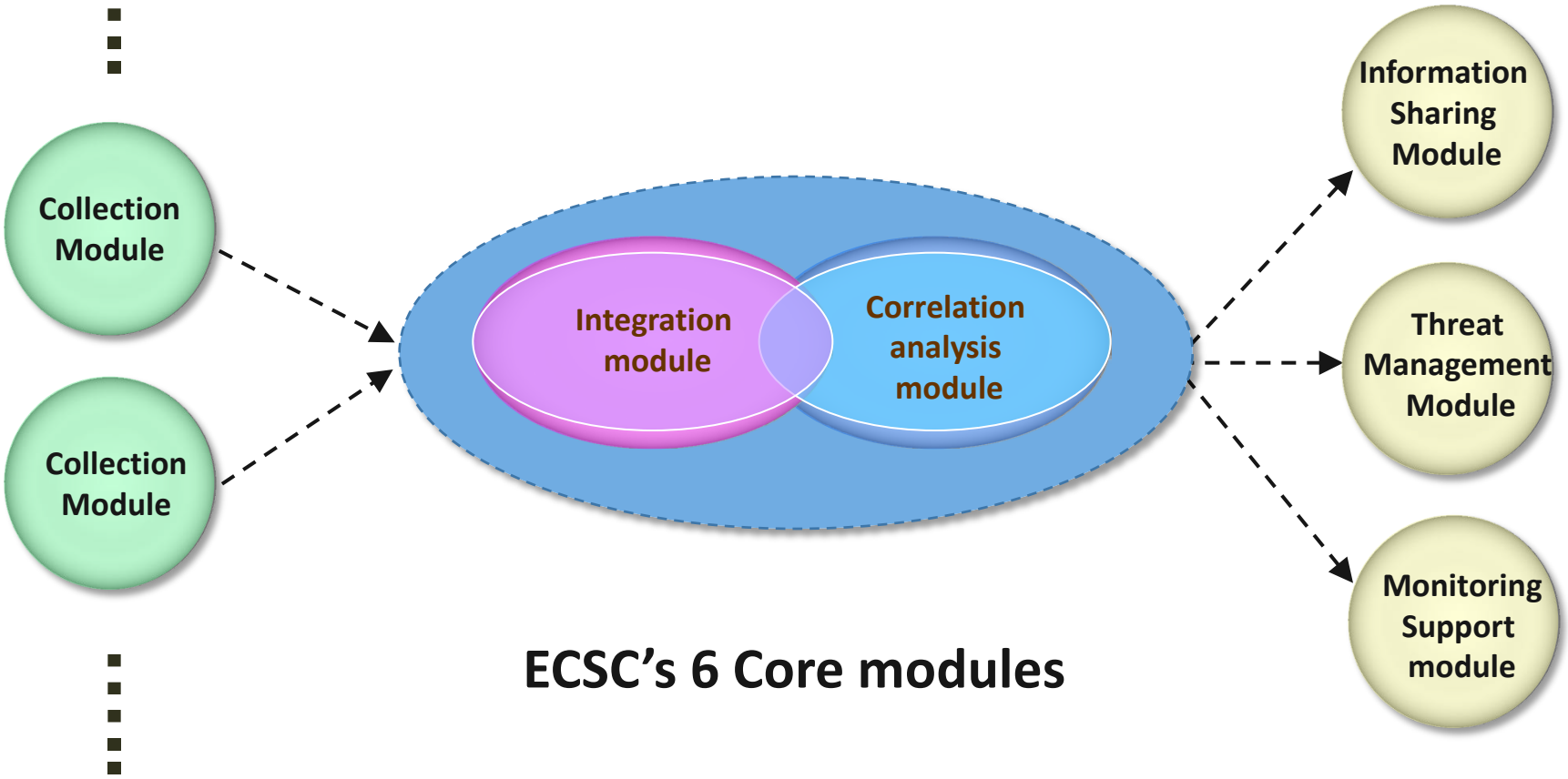
Stages of security monitoring

Collect logs in real time from pattern-based detection systems of individual institutions

Classify the patterns of attacks and apply different correlation analysis to them

Share intrusion information in real time through and information sharing system and respond quickly

6 Core Modules



ECSC's 6 Core modules

Collection Stage

Issues related to the collection stage

- **What information** to collect
- **How to collect** the logs detected from individual systems?
- **How to regularize** different logs of heterogeneous security systems?
- How to **collect massive amounts** of data?

Analysis Stage

❖ Issues of the analysis stage

- Is all the collected information related to hacking incidents?
- **How to implement correlation analysis** on collected information?
- **How to classify** hacking attack patterns ?
- **What analysis strategy** should be applied to the mass data?

Response Stage

❖ Issues of the response stage

- What are **efficient response strategies** and methods for different attack patterns?
- What is the **most efficient response system** to intrusion incidents?

Contents

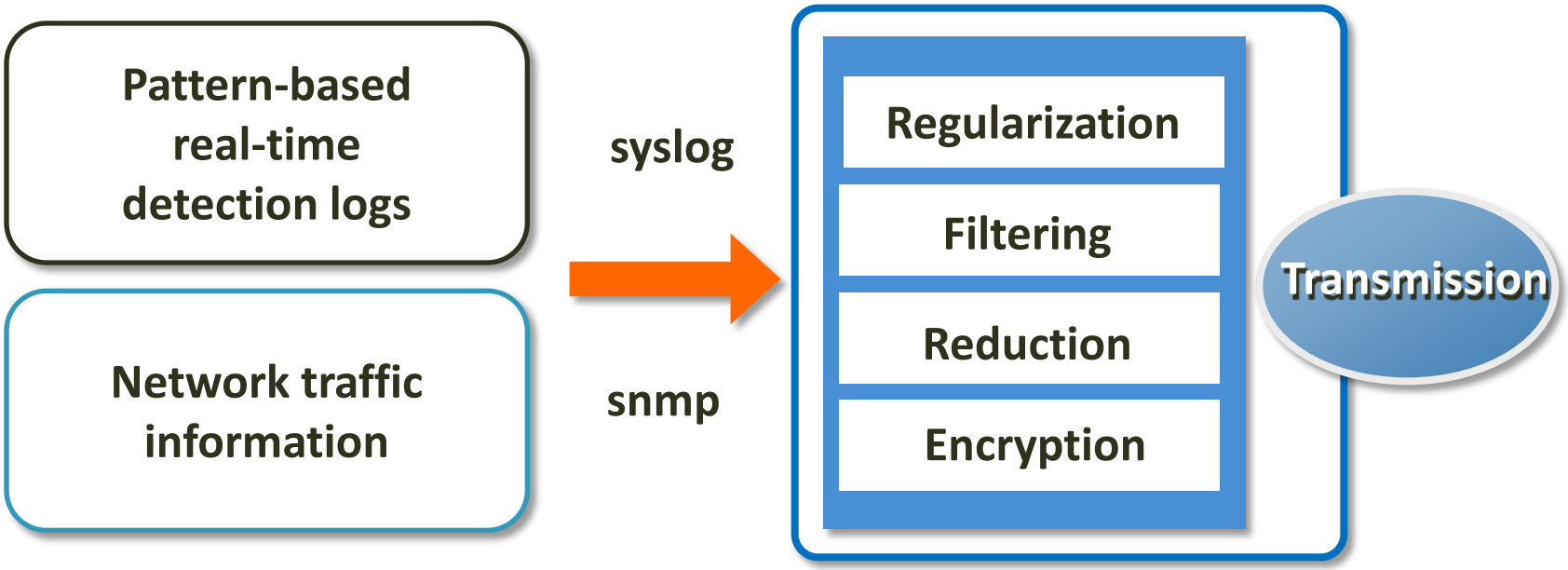
1 Overview

2 Collection

3 Analysis

4 Response

Process of collecting security information



❖ Collection module

Collecting Security Information

❖ Pattern-based security information

- Real-time logs from **pattern-based detection system** such as IPS or IDS
- **The key to precise detection** is patterns: to combine patterns of individual security systems and **ECSC's own pattern**
- Operate a consultative organization to apply a **precise detection pattern**

[ECSC detection pattern]

● Develop its own patterns by investigating and analyzing actual cases and use open source of IDS snort
● Share patterns in cooperation with related institutions

❖ Network Traffic Information

- Real-time traffic information form the backbone switch in related institutions and information on CPU usage

ECSC Detection Pattern

❖ Develop own pattern

- **Develop highly accurate** patterns by investigating actual cases

- Apply them to individual institutions through **consultative organization for detection pattern sharing**

[An example of ECSC detection pattern]

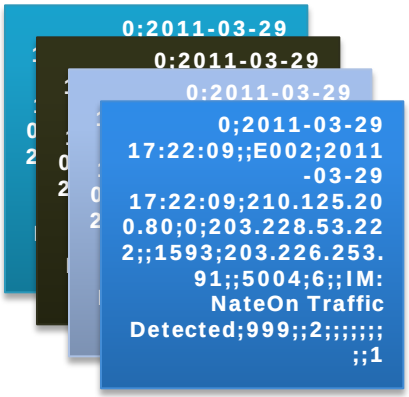
● POST method run through command "netstat ", ".exe", "dir", "ls",

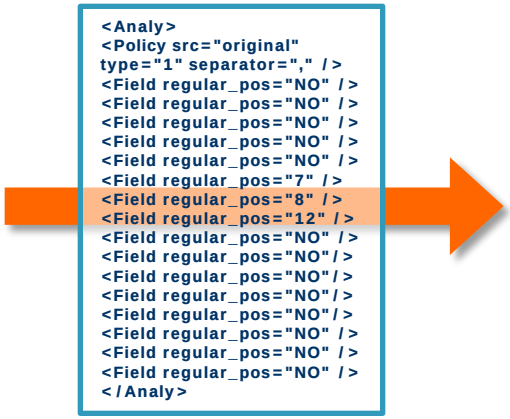
alert tcp any any <> any $HTTP_PORT (content:"POST";depth:4;pcre:"/\x0d\x0a.*(netstat(%20|\+)+\x2Da|\x2Eexe(%20|\+)+\x2Fc|cmd(%20|\+)+\x2Fc|dir(%20|\+)+c\x3A\x5C|ls(%20|\+)+152\x2E99\x2E)/i";)

Regularization of Security Information

❖ Regularize real-time logs from individual systems

- **Regularize real-time logs** from heterogeneous systems through an xml-based policy



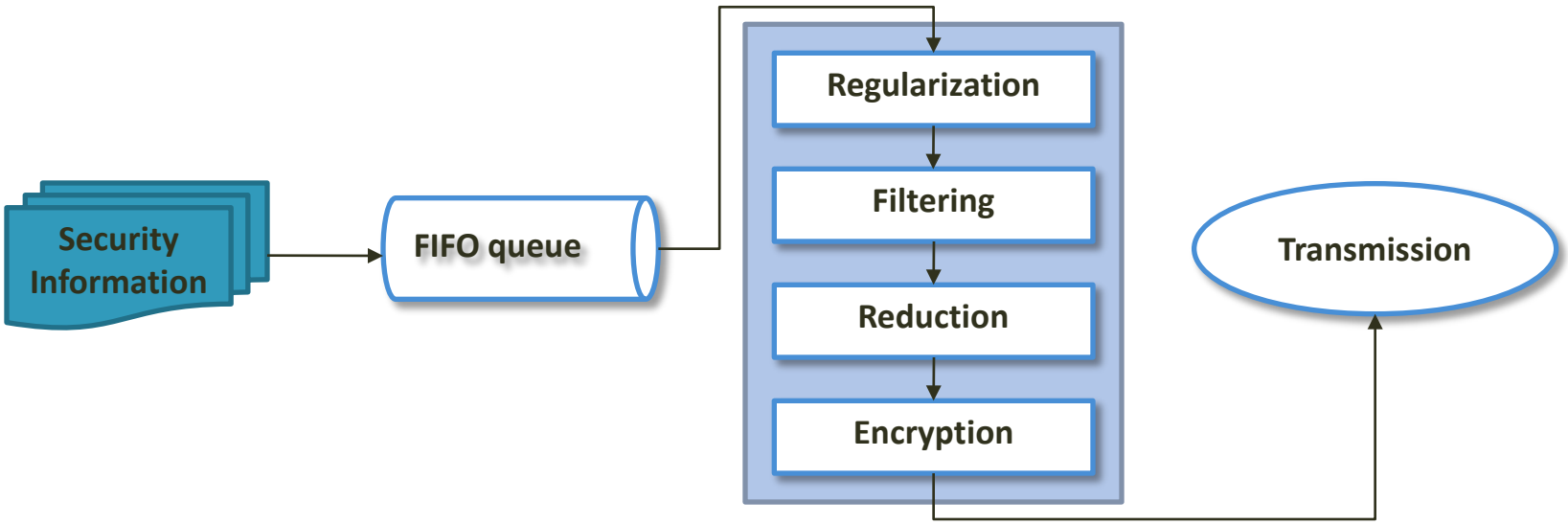


- DST_IP: '203.226.253.91'
- SRC_IP: '203.228.53.222'
- COMP_YN: 'Y'
- ATTACK_NM: 'IM: NateOn Traffic Detected'
- CNT: '1'
- EQP_IP: '210.125.200.80'
- EQP_TYPE: '05'
- DST_PORT: '5004'
- COMP_CNT: '1'
- PAYLOAD: ''
- BODY_TYPE: 'LOG_IA'
- INST_CD: '73034000'
- SRC_PORT: '1593'
- PROTOCOL: '6'
- OPTION2: ''
- OPTION1: ''
- EQP_TIME: '20110329171929'
- SIMS_TIME: '20110329171929'
- OPTION3: ''

Xml regularization policy

Filtering, Reduction, Encryption

- **Filtering, reduction, and encryption of security information**
  - Filter detection errors(**false positive**)
  - **Reduce recurring information**: reduce logs with the same starting IP, arriving IP, and attacking name
  - **Transmit encryption** to the central center (SSL)



Contents

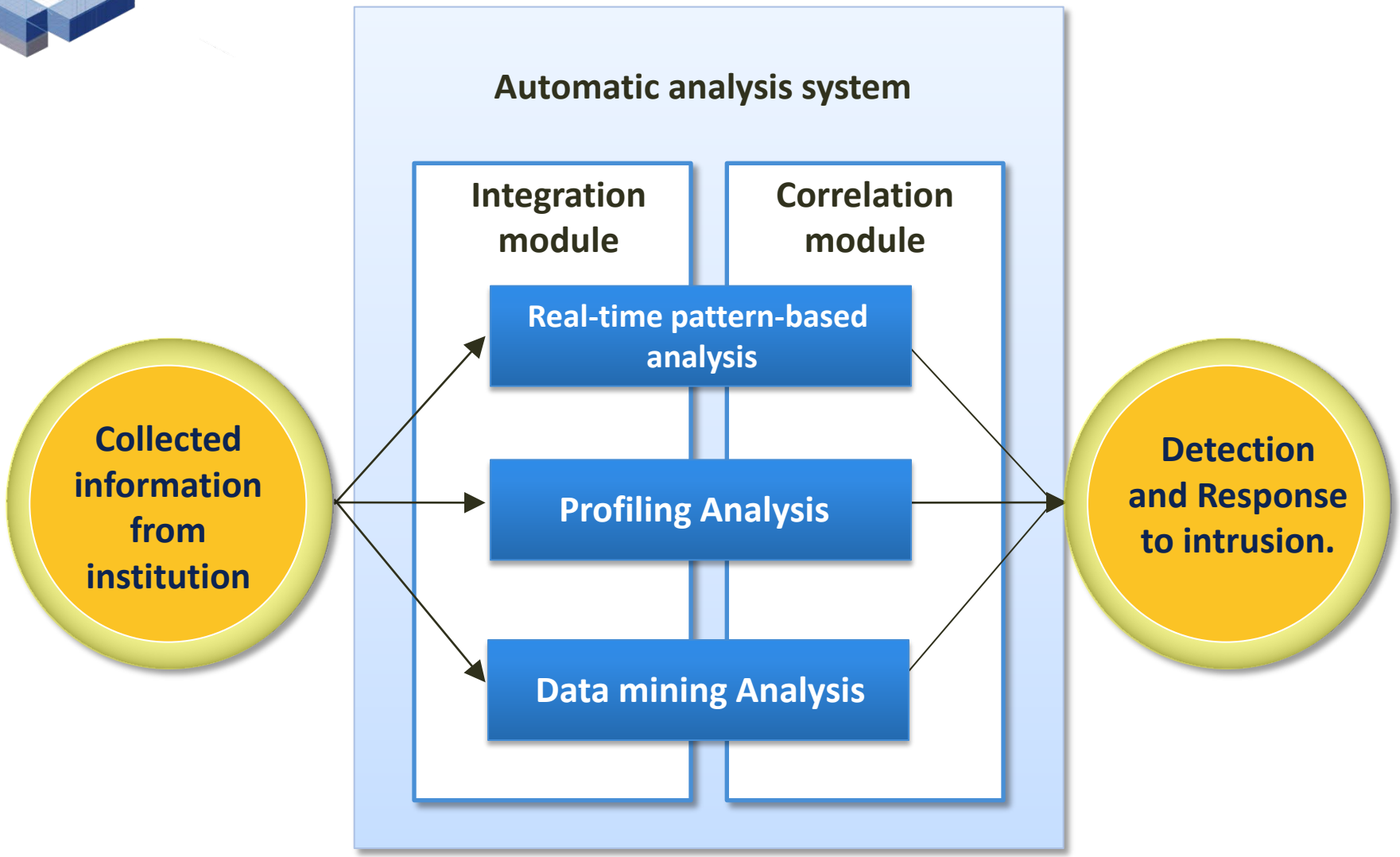
1 Overview

2 Collection

3 Analysis

4 Response

Analysis Method on Security Information



Analysis Method on Security Information

Pattern

real-time correlation analysis on information detected by patterns with **high accuracy**

Profiling

analyze critical values by profiling information detected by patterns with **low accuracy**

Mining

create statistics for 5 minute increments to **utilize for security monitoring**

Real-time Pattern-Based Analysis

❖ Real-time pattern-based analysis

- **Grade risk level by real-time correlation analysis** on information detected by accurate detection pattern (ECSC pattern)
- Correlation analysis:
  - Correlation analysis on logs with the same attack **pattern based on attack IP**
  - Correlation analysis on **black list IP** based on attack IP
  - Correlation analysis on **vulnerabilities** based on target IP

[Classification of attack patterns and correlation analysis methods]

● Cooperation between ECSC monitoring researchers and related institutions

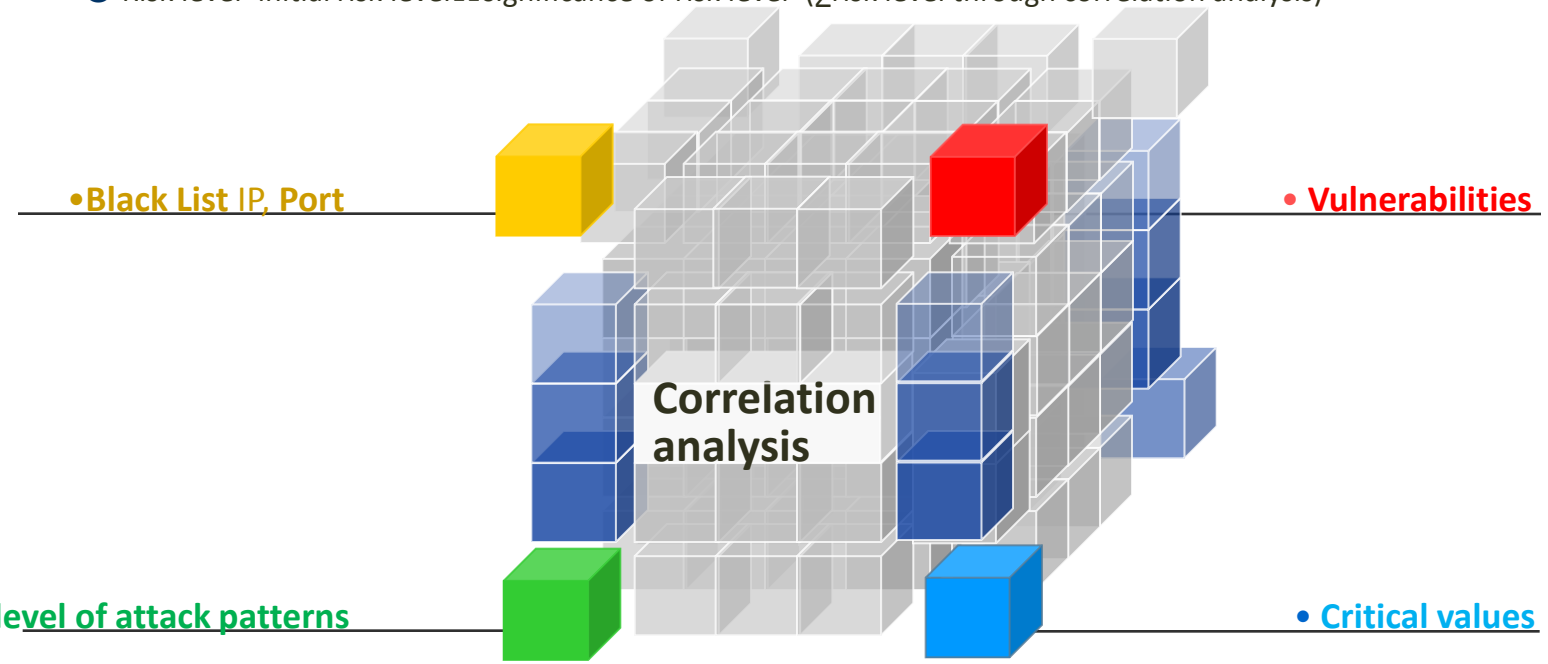
Real-time Pattern-Based Analysis

❖ Real-time correlation analysis

- Calculate risk level through correlation analysis based on attack patterns, attack information, vulnerabilities, and critical values

[Risk level]

● Risk level=initial risk level X significance of risk level+(∑risk level through correlation analysis)



Profiling-based Analysis

❖ Profiling pattern-based analysis

- Analyze information detected through patterns with **low accuracy by comparing it with profiled critical values**

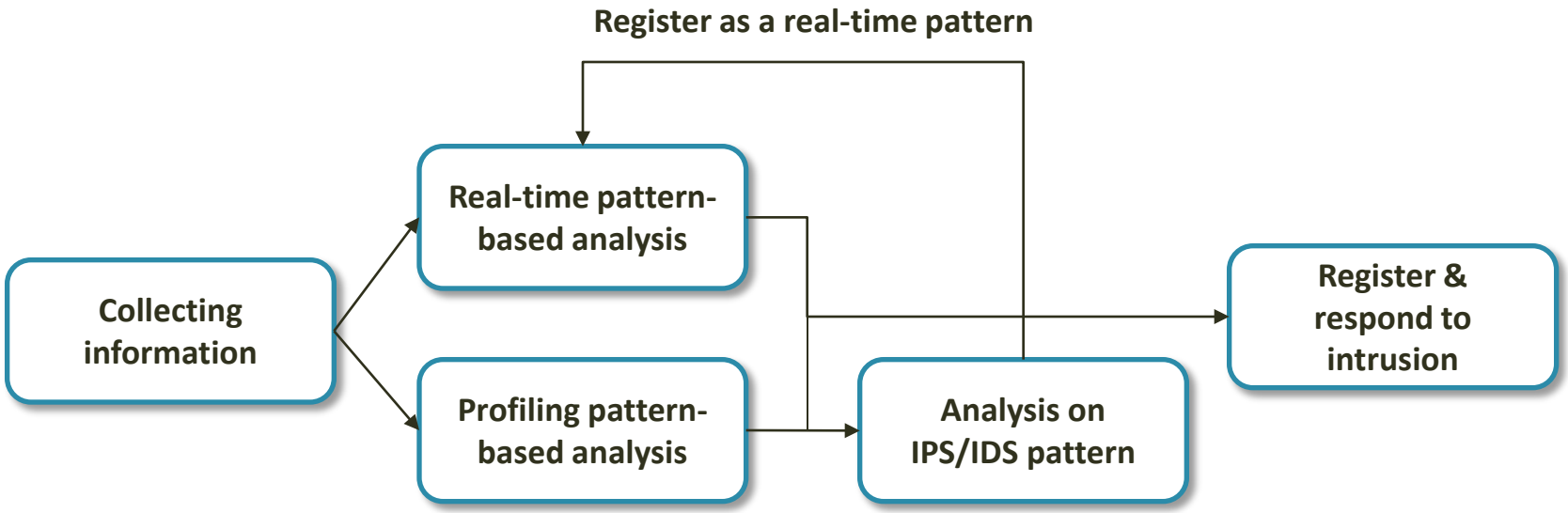
- Profile critical values in advance**: profiling critical values by different institutions and patterns**

[Standard of profiling]

Profiling pattern by different institutions : Analyze weekly averages or the average of the previous day

Profiling-based Analysis

- Through profiling-based analysis, we register patterns with high accuracy as a real-time monitoring pattern that is analyzed automatically

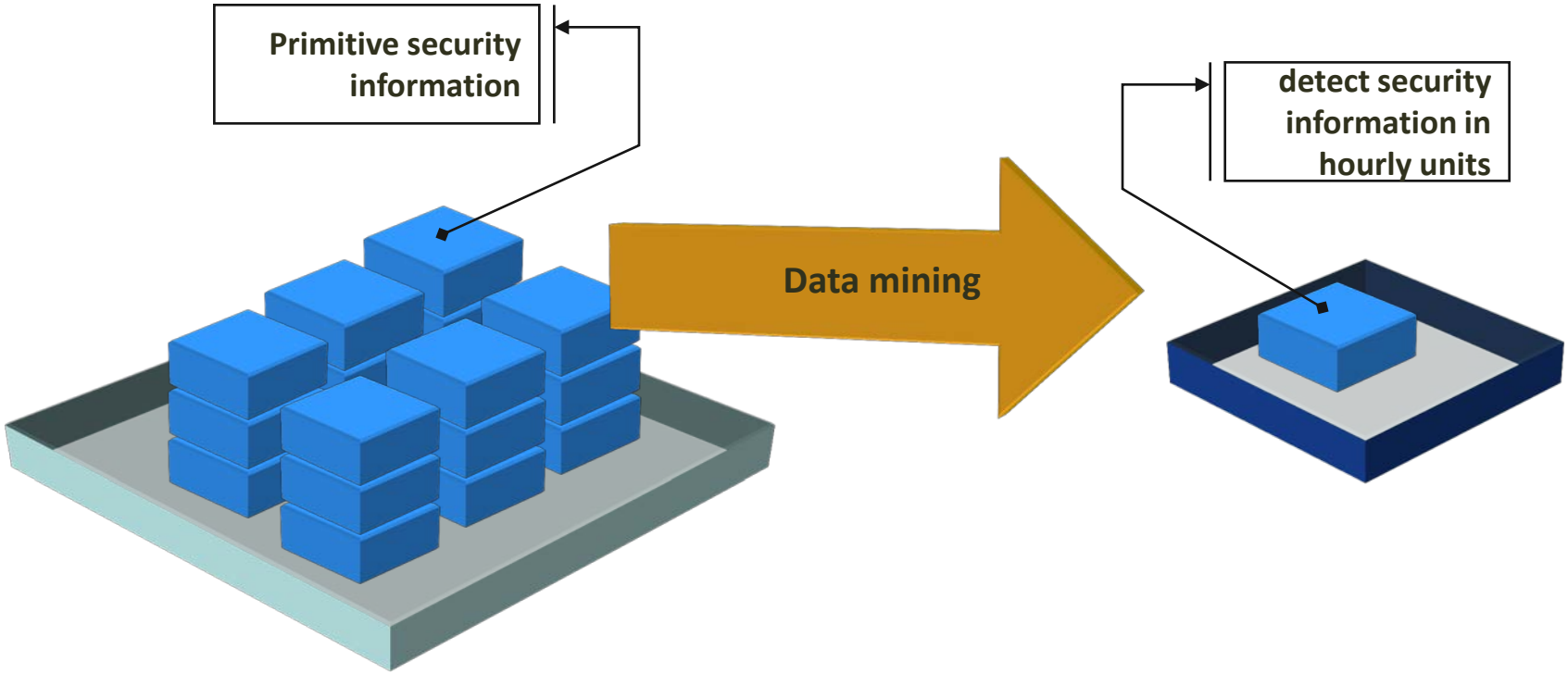


Data mining Analysis

❖ Data mining analysis

- Create a statistic **every 5 minutes** from the original data and **utilize it for monitoring**
- Data mining **based on the top attack name, top place, top target, and top traffic increase**

Data mining Analysis

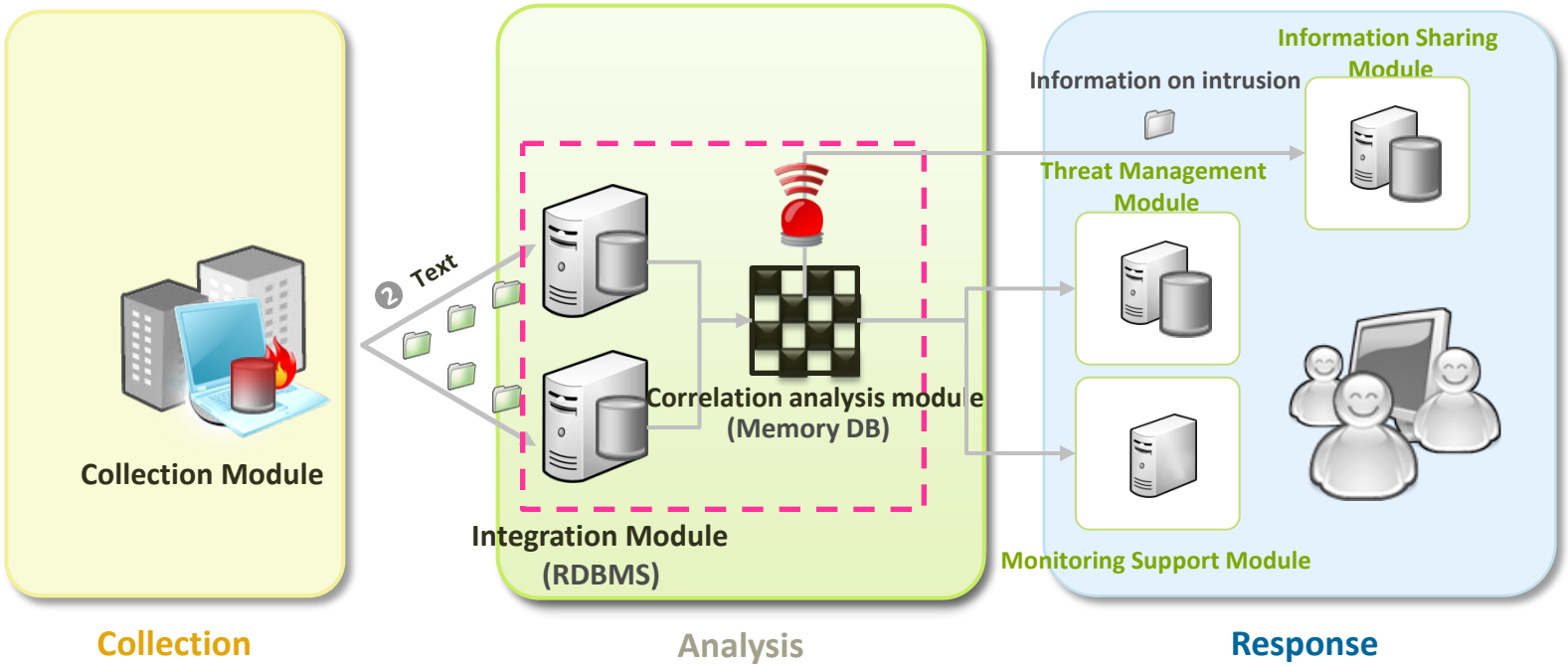


Apply **new monitoring pattern** based on mining results

Analysis on mass data

Architecture for analysis on mass data in real time

- Utilize **memory DB** for real-time correlation analysis
- Maximize capacity of resources by establishing integration structure



Contents

1 Overview

2 Collection

3 Analysis

4 **Response**

Response to Intrusion Incidents

Monitoring support module

provide efficient analysis environment to monitoring researchers through 3D visualization

Threat management module

supports future statistical management by registering and controlling analyzed data

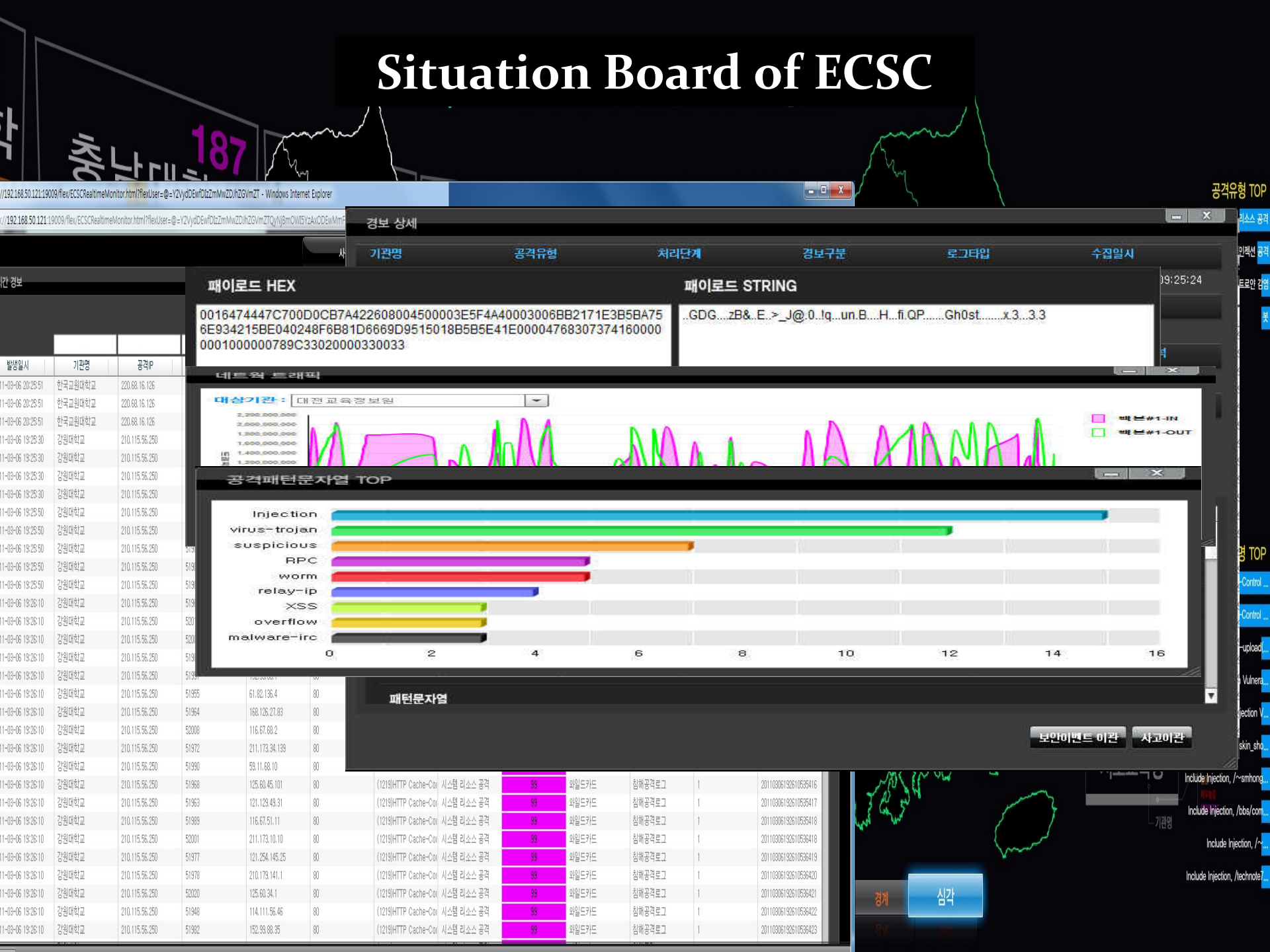
Information sharing module

provide intrusion incident and threat information to related institutions in real time

Monitoring Support Module

- **Provide an efficient monitoring environment**
  - **Enable immediate monitoring** through 3D visualization
  - **Enable an individual monitoring environment** for each researcher
  - Establish real-time monitoring based on Web2.0

Situation Board of ECSC



Threat Management Module

- **Systematic threat management**
  - **Efficient threat management** with the 6 sigma process
  - Systematization of registration-processing-completion of intrusion incident
  - Efficient management of statistics

Information Sharing Module

- **Sharing updated information on intrusion and new technology**
  - Share **updated security trends**
  - Share statistics of **intrusions and detailed information**
  - Share **vulnerabilities**
  - Share new **hacking technologies**

교육사이버안전지원시스템
EDUCATION SECURITY SUPPORT SYSTEM

홈 | 사용자정보변경 | 장비현황관리 | 사이트맵 | 로그아웃

시스템관리자 (교육사이버안전센터) / 교육사이버안전지원시스템이란?

사이트맵 | 상황판 | 로그아웃

교육사이버안전지원시스템이란?

보안정보 | 침해사고대응 | 보안취약점 | ECSC보안동향 | 보안장비보유현황 | DNS 싱크홀 | 보안게시판

보안정보

보안게시판

ECSC Security Info.
ECSC 보안정보 교육기관의 보안정보를 보실수 있습니다.

교육기관 위험도

단위시간 전체 사고 신

- 전체기관

사고처리 현황

사고번호	제조사	상태
T09-1110001 [동명대학	나우콤	연동
T09-0615001 [광운대학	나우콤	연동
T09-0328006 [부산예술	Cisco	연동

- 침해공격현황
- 예경보발령현황
- 바이러스발생현황
- 보안권고문
- 뉴스클리핑
- 유해 IP목록
- ECSC탐지룰
- 보안이벤트

침해공격현황

HOME | 보안정보 | 침해공격현황

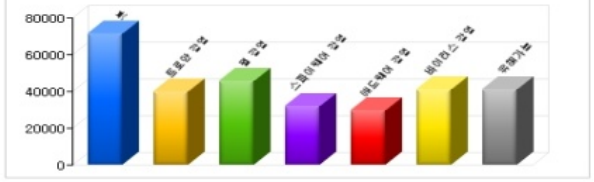
• 단위시간 : 2010-11-25 14:55 ~ 2010-11-25 19:55
단위시간설정

단위시간 전체 침해공격 현황

- 전체기관

- 악성코드 감염 [66%]
- 웹 해킹 [15%]
- 서비스거부 공격 [9%]
- 단순침입시도 [8%]

악성코드감염 | 웹해킹 | 서비스거부공격 | 단순침입시도



단위시간 기관유형 침해공격 현황

- 산하기관

- 악성코드 감염 [64%]
- 서비스거부 공격 [18%]
- 단순침입시도 [17%]

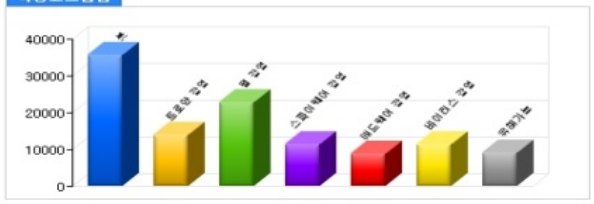
악성코드감염 | 서비스거부공격 | 단순침입시도

단위시간 침해공격 현황

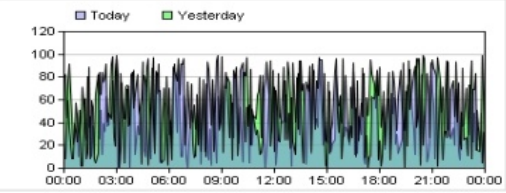
- 교육사이버안전센터

- 악성코드 감염 [100%]

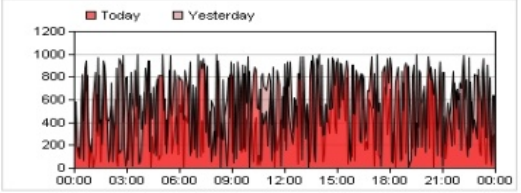
악성코드감염



리소스 현황



트래픽 현황



간 : 2009-11-25 ~ 2010-11-25
단위시간설정

종결
995

- 1. 웹해킹 [62%]
- 2. 악성코드 감염 [26%]
- 3. 경유지 악용 [5%]
- 4. 서비스거부 공격 [4%]
- 5. 단순침입시도 [0%]

교육사이버안전센터
Education Cyber Security Center

교육사이버안전센터
Education Cyber Security Center

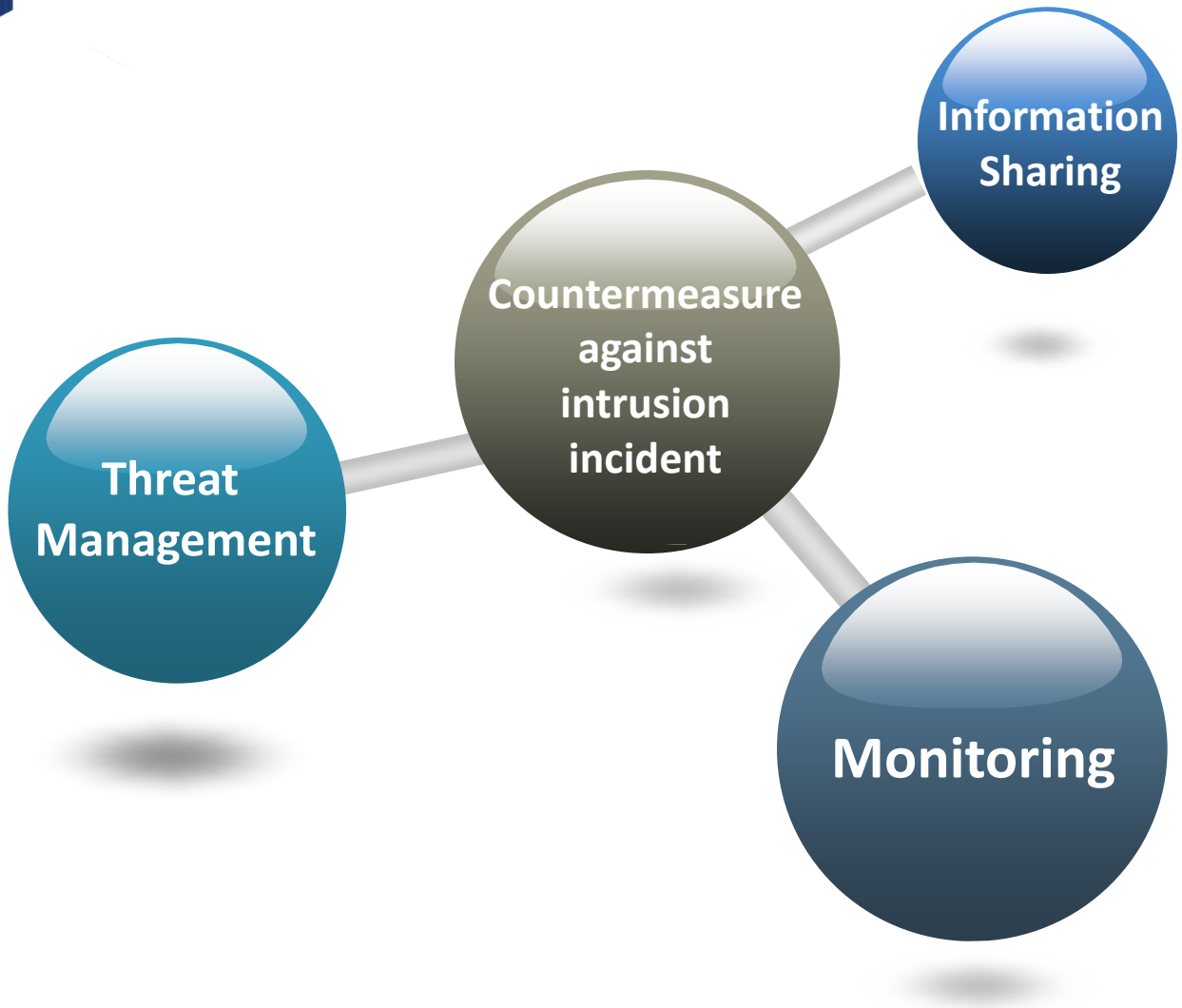
100-400 서울 종구 퇴계로 299 KERIS빌딩 교육사이버안전센터 사고신고 TEL: 02-2118-1777 / FAX: 02-2118-1714

WEBMASTER@ECSC.GO.KR

교육사이버안전지원시스템
02·2118·1777

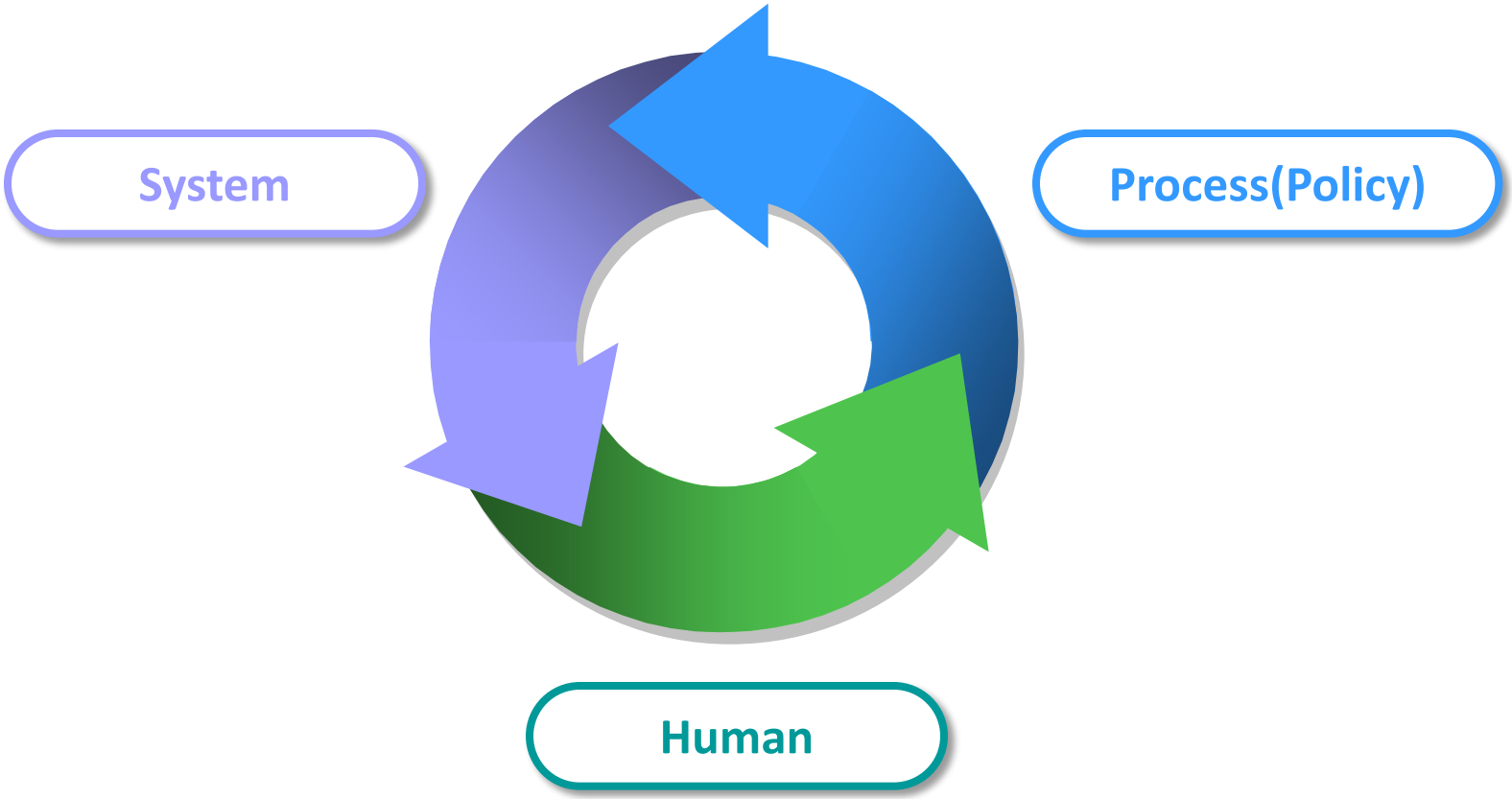
교육사이버안전지원시스템
02·2118·1777

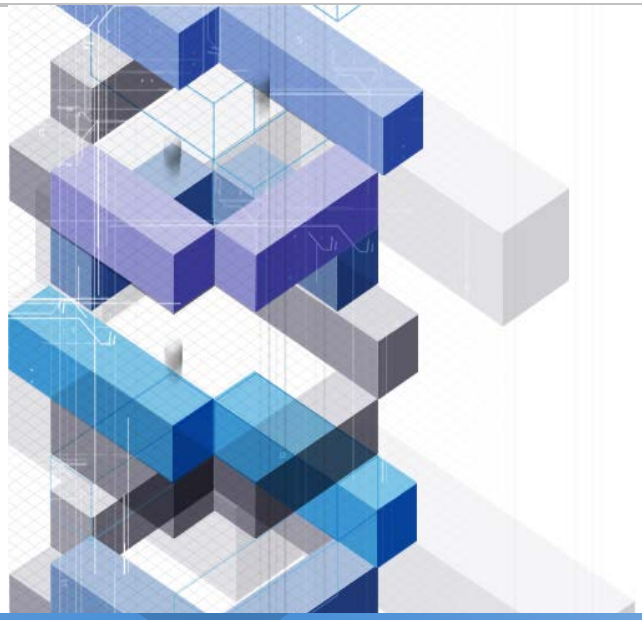
Countermeasure against Intrusion Incident



Conclusion

- What do we need for a powerful countermeasure system?





Thank You !

www.ecsc.go.kr

교육사이버안전센터
Education Cyber Security Center