KISA KOREA INTERNET & SECURITY AGENCY

C-TAS Ecosystem for Cyber Threat Analysis & Sharing in Korea

2017. 12. 7

Sang Wook Seo, KISA/KrCERT
Jung Hee Kim, KISA/KrCERT
Dong Ryun Lee, KISA/KrCERT
Prof. Huy Kang Kim, Korea Univ.

About authors

Sang Wook Seo (Speaker)

- General Researcher, National Cyber Intelligence Team, Korea Internet & Security Agency
- Ph.D Course, Graduate School of Information Security, Korea University
- Big Data System & Data Architect, Data Mining & Machine Learning in Security

Jung Hee Kim

- Director, Cyber Threat Intelligence Center, Korea Internet & Security Agency
- Director of National & Global Cyber Threat Intelligence Cooperation in Korea

Dong Ryun Lee

- Manager, National Cyber Intelligence Team, Korea Internet & Security Agency
- Coordinator of National Cyber Threat Intelligence Network in Korea

Huy Kang Kim

- Associate Professor, Graduate School of Information Security, Korea University
- Founder of A3 Security Consulting (1999), Technical Director of NCSOFT (2004-2010)
- Online Game Security, Fraud Detection System, Network & System Security

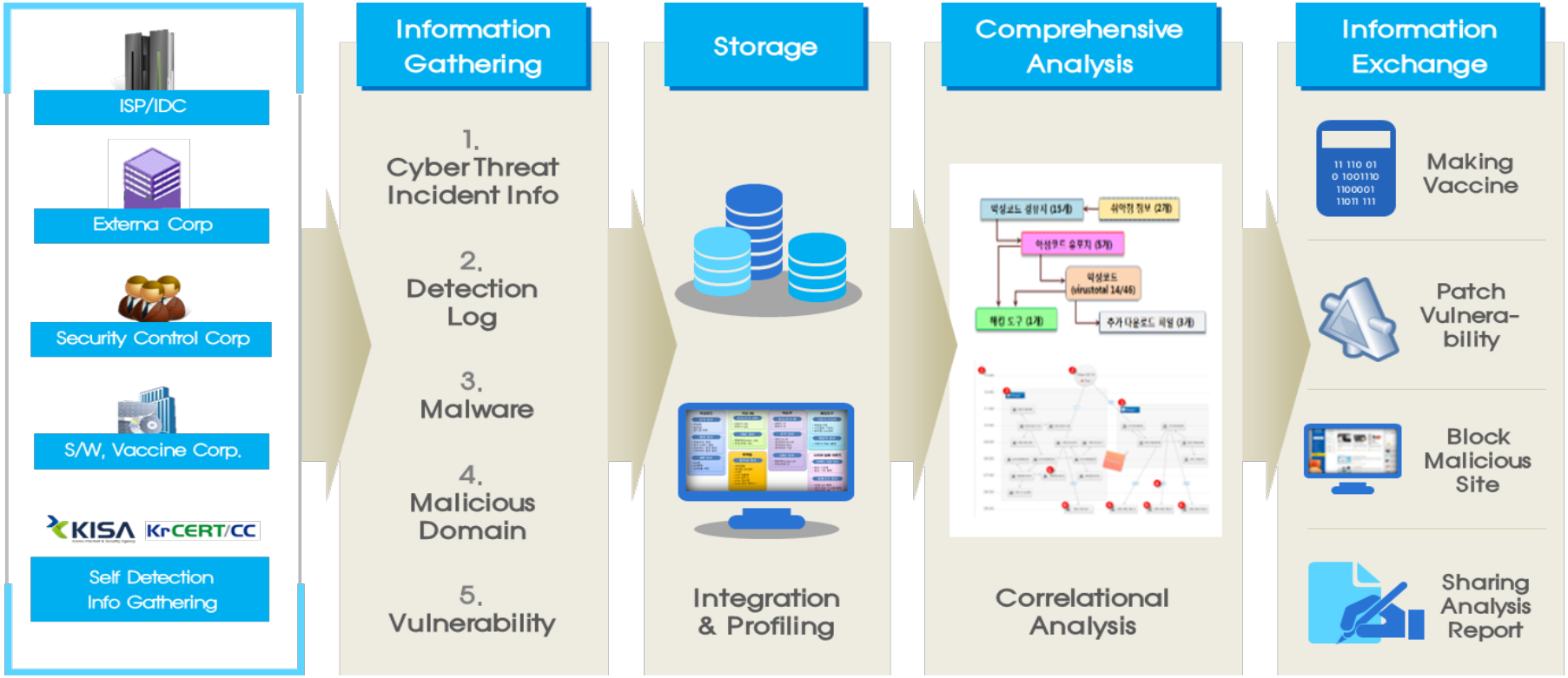
Contents

1. C-TAS System

1-1. Introduction to C-TAS System

C-TAS System Overview

- C-TAS system was developed to prevent the spread of harm from various cyber incidents by collecting, analyzing and disseminating cyber threats



1-2. Motivation & History

C-TAS(Cyber Threat Analysis & Sharing) System

❖ by KISA(Korea Internet & Security Agency), August 2014

Motivation

❖ 7.7 DDoS Attack (2009) & 3.4 DDoS Attack (2011)

❖ NH APT Attack (2011) & 3.20 APT Attack (2013, DarkSeoul)

❖ Korea Hydro & Nuclear Power Hacking (2014)

Development

❖ 12.05 ~ 12.11 : MMS 1.0 & MML 1.0

❖ 13.08 ~ 13.12 : MMS 1.1 & MML 1.1

❖ 13.09 ~ 14.07 : C-TAS 1.0 & C-TAS 1.0

❖ 15.05 ~ 15.12 : C-TAS 1.1 & C-TEX 1.1 (MMS -> TIMS)

❖ 16.05 ~ 16.12 : C-TAS 1.2 & C-TEX 1.2 (with STIX 1.2)

❖ 17.05 ~ 17.12 : C-TAS 2.0 & C-TEX 2.0 (with STIX 2.0)

❖ C-TAS : Cyber Threat Analysis & Sharing

❖ C-TEX : Cyber Threat EXpression

❖ MMS : Malware Management System

❖ MML : Malware Markup Language

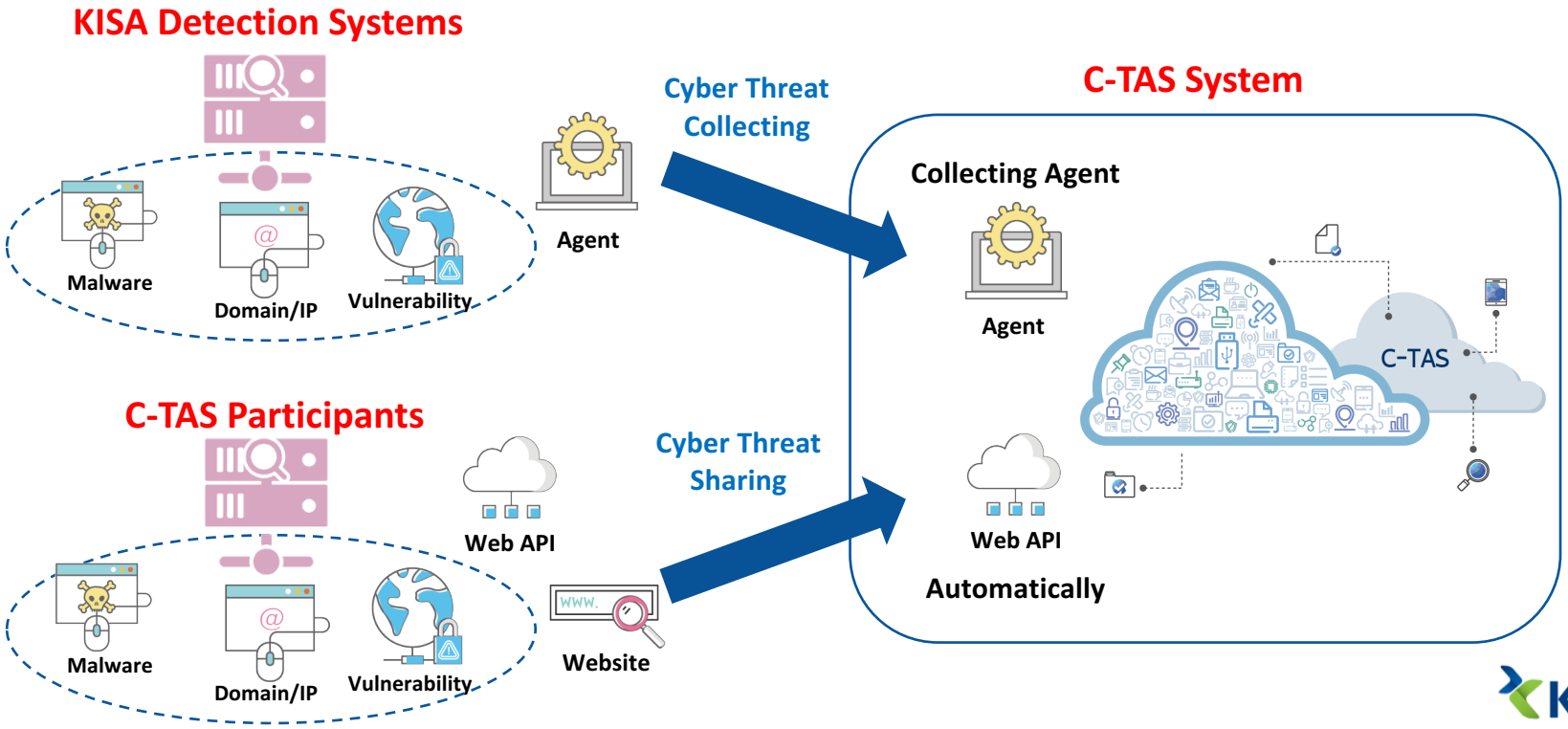
❖ TIMS : Threat Intelligence Management System

KISA

1-3. Collecting Cyber Threat

From KISA & Participants

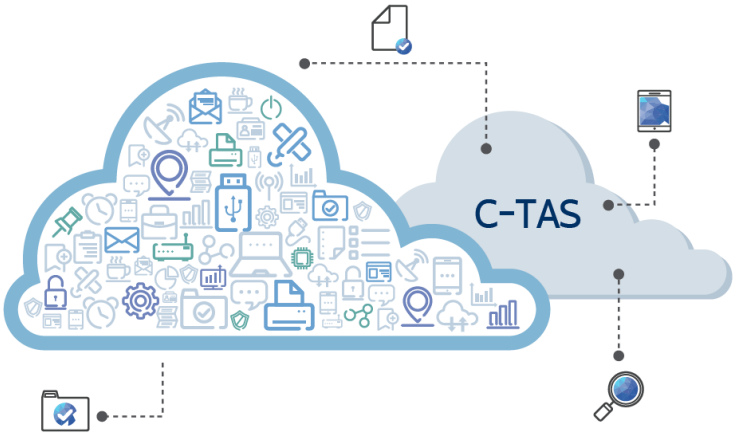
- Cyber Threat : Malware, Malicious Domain/IP, Vulnerability Info and etc
- Collecting Method : Agent, Web API, Website



1-4. Disseminating Cyber Threat

To C-TAS Participants

- **The ways to disseminate cyber threats are :**
  - Web API to respond to cyber threats in real time
  - Website to download & upload cyber threats manually
  - STIX/TAXII 2.0 will be supported in 2018



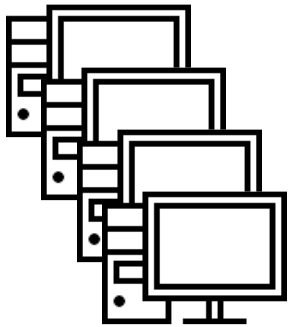
C-TEX & STIX 2.0 (2018)

The ways to disseminate are :

① Web API (export API) & TAXII (2018)

② Website (https://cshare.krcert.or.kr)

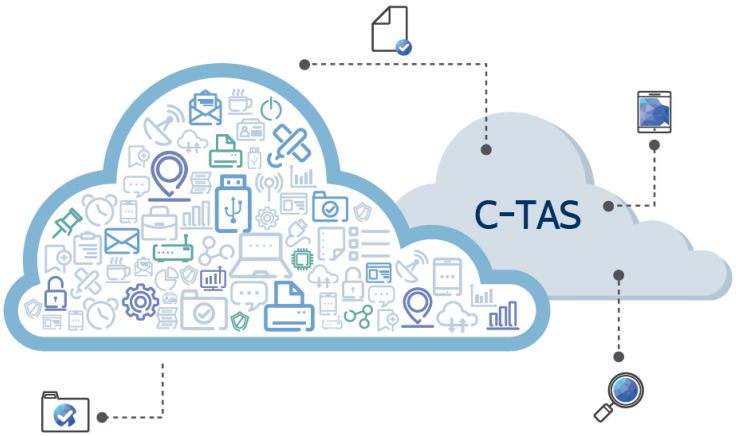
C-TAS Participants



1-5. Sharing Policy

To Participate in C-TAS

- If you want cyber threats, you must share cyber threats (no free-riding)
- You can get the same types of cyber threat you share (type symmetric)
- The amount you share decides your grade (4 grades)
- Higher grades give you additional information (quality symmetric)



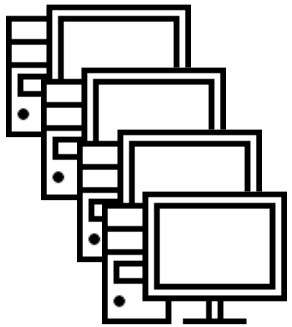
Depending on the grade

The sharing policy is :

① No free-riding

② Type & Quality Symmetric

C-TAS Participants



1-6. C-TEX Sample

Collect Markup Language

C-TEX 1.2 (XML)

```
<mcf>
    <when>
        <date>2015-07-08</date>
        <time>05:36:19</time>
    </when>
    <method>system</method>
    <channel>mcf</channel>
    <source />
    <comment />
    <address>
        <domain>www.      .com</domain>
        <ip>211.192.139.    </ip>
        <icountry>KR</icountry>
        <url>http://www.      .com/dataroom/kk/index.html</url>
        <type>distribute</type>
        <company></company>
        <completed>Y</completed>
        <hosting></hosting>
        <toolkit>CKVIP</toolkit>
    </address>
    <vulnerability>
        <cve>CVE-2013-0422</cve>
        <product>JAVA</product>
    </vulnerability>
    <sample>
        <md5>3da8ef90d78766208088d7fa72a      </md5>
        <sha256>81ab5d27b5311cc7ee1139a2d11c71e5aec1f974caee0000716cfae2c29      </sha256>
        <ssdeep>1536:Vxl7fW/zh0M3Ii7T7zV3J32gkA5FM+AfKdPFY+5NfZCqmBXkhOJF4BDu:vlDKdXl3p29c
        <name>de.exe</name>
        <type>infoleak</type>
    </sample>
</mcf>
```

C-TEX 2.0 (JSON)

```
{
    "when": {
        "date": "2015-07-08",
        "time": "05:36:19"
    },
    "method": "system",
    "channel": "mcf",
    "source": "",
    "comment": "",
    "address": [
        {
            "domain": "www.      .com",
            "ip": "211.192.139.    ",
            "icountry": "KR",
            "url": "http://www.      .com/dataroom/kk/index.html",
            "type": "distribute",
            "company": "",
            "completed": "Y",
            "hosting": "",
            "toolkit": "CKVIP",
        },
    "vulnerability": [
        {
            "cve": "CVE-2013-0422",
            "product": "JAVA",
        },
    ],
    "sample": {
        "md5": "3da8ef90d78766208088d7fa72a      ",
        "sha256": "81ab5d27b5311cc7ee1139a2d11c71e5aec1f974caee0000716cfae2c29      ",
        "ssdeep": "1536:Vxl7fW/zh0M3Ii7T7zV3J32gkA5FM+AfKdPFY+5NfZCqmBXkhOJF4BDu:vlDKdXl3
        "name": "de.exe",
        "type": "infoleak",
    }
}
```

KISA

1-7. C-TEX to STIX

C-TEX 1.2 to STIX 1.2

C-TEX 1.2 (XML)

```
<mcf>
    <when>
        <date>2015-07-08</date>
        <time>05:36:19</time>
    </when>
    <method>system</method>
    <channel>mcf</channel>
    <source />
    <comment />
    <address>
        <domain>www.      .com</domain>
        <ip>211.192.139.    </ip>
        <icountry>KR</icountry>
        <url>http://www.      .com/dataroom/kk/index.html</url>
        <type>distribute</type>
        <company></company>
        <completed>Y</completed>
        <hosting></hosting>
        <toolkit>CKVIP</toolkit>
    </address>
    <vulnerability>
        <cve>CVE-2013-0422</cve>
        <product>JAVA</product>
    </vulnerability>
    <sample>
        <md5>3da8ef90d78766208088d7fa72a      </md5>
        <sha256>81ab5d27b5311cc7ee1139a2d11c71e5aec1f974caee0000716cfae2c29      </sha256>
        <ssdeep>1536:Vxl7fW/zh0M3Ii7T7zV3J32gkA5FM+AfKdPFY+5NfZCqmBXkhOJF4BDu:vlDKdXl3p29c
        <name>de.exe</name>
        <type>infoleak</type>
    </sample>
</mcf>
```

STIX 1.2 (XML)

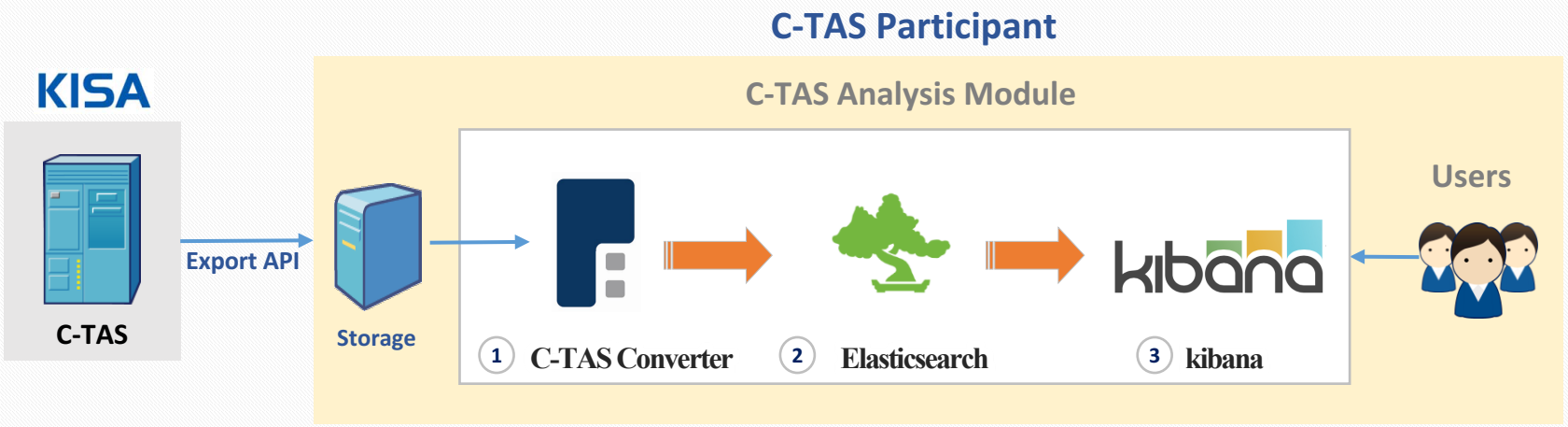
```
<stix:STIX_Package>

    <stix:STIX_Header>
        <stix:Information_Source>
            <stixCommon:Identity>
                <stixCommon:Name>KISA</stixCommon:Name>
            </stixCommon:Identity>
            <stixCommon:Role xsi:type="stixVocabs:InformationSourceRoleVocab-1.0">Initial Author</stixCommon:Role>
            <stixCommon:Time>
                <cyboxCommon:Produced_Time precision="day">2015-07-08T00:00:00Z</cyboxCommon:Produced_Time>
            </stixCommon:Time>
        </stix:Information_Source>
    </stix:STIX_Header>

    <stix:Indicators>
        <stix:Indicator timestamp="2015-07-08T00:00:00Z" xsi:type="indicator:IndicatorType">
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">IP Watchlist</indicator:Type>
            <indicator:Observable>
                <cybox:Object>
                    <cybox:Properties category="ipv4-addr" xsi:type="AddressObj:AddressObjectType">
                        <AddressObj:Address_Value condition="Equals">211.192.139.    </AddressObj:Address_Value>
                    </cybox:Properties>
                    <cybox:Related_Objects>
                        <cybox:Related_Object>
                            <cybox:Properties xsi:type="DomainNameObj:DomainNameObjectType">
                                <DomainNameObj:Value condition="Equals">www.      .com</DomainNameObj:Value>
                            </cybox:Properties>
                            <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.1">Resolved_To</cybox:Relationship>
                        </cybox:Related_Object>
                    </cybox:Related_Objects>
                    <cybox:Related_Objects>
                        <cybox:Related_Object>
                            <cybox:Properties xsi:type="FileObj:FileObjectType">
                                <FileObj:Hashes>
                                    <cyboxCommon:Hash>
                                        <cyboxCommon:Type>MD5</cyboxCommon:Type>
                                        <cyboxCommon:Simple_Hash_Value>3da8ef90d78766208088d7fa72a      </cyboxCommon:Simple_Hash_Value>
                                    </cyboxCommon:Hash>
                                </FileObj:Hashes>
                            </cybox:Properties>
                            <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.1">Downloaded_From</cybox:Relationship>
                        </cybox:Related_Object>
                    </cybox:Related_Objects>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
    </stix:Indicators>

</stix:STIX_Package>
```

1-8. Supports for C-TAS Participants

To Search & Visualize Threats

C-TAS Analysis Module : Modified ELK Stack

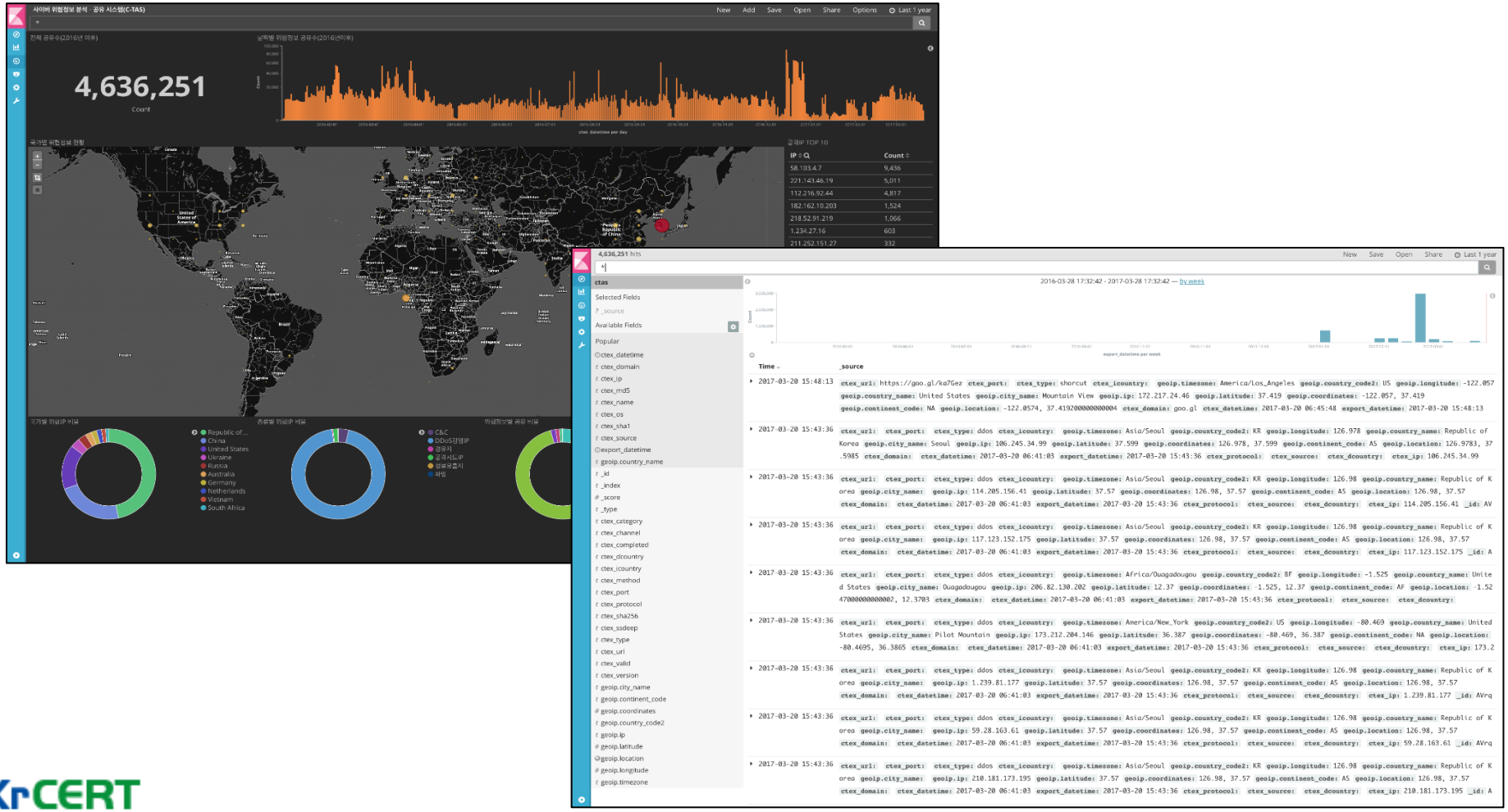
C-TAS AM : Tool for C-TAS participants to search and visualize cyber threats easily



1. Logstash is replaced by C-TAS Converter to support C-TEX
2. Elasticsearch helps C-TAS participants to search cyber threats
3. Kibana helps C-TAS participants to visualize cyber threats

1-8. Supports for C-TAS Participants

Dashboard & Search Result

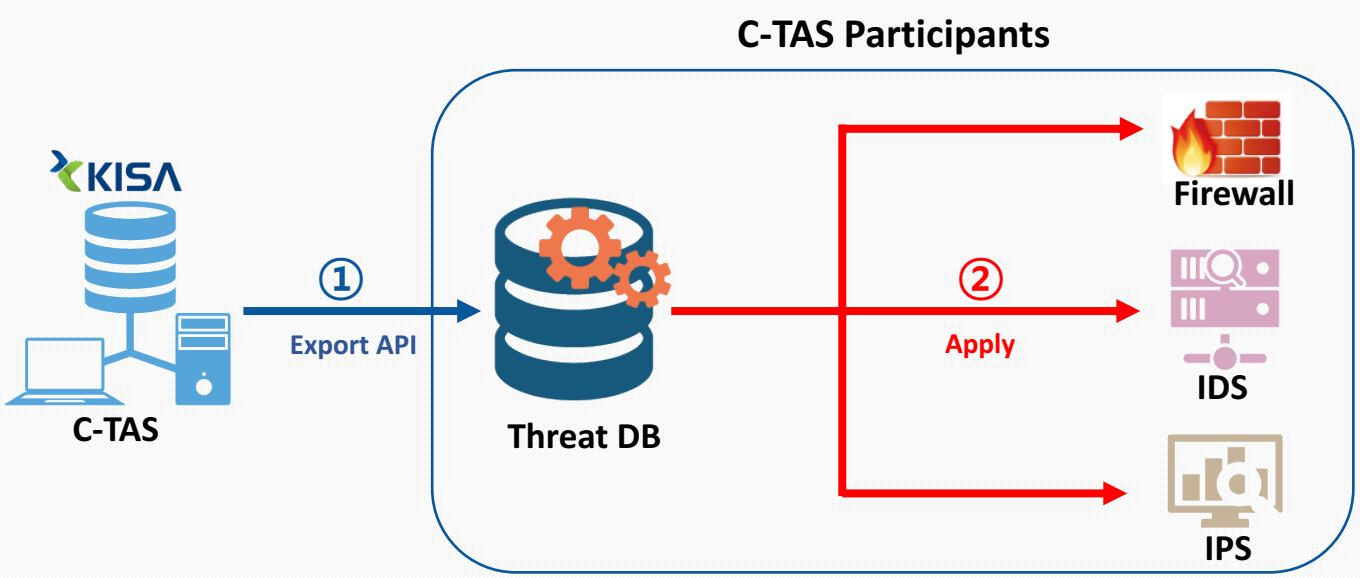


1-9. Cyber Threat Use Cases

1. Malicious Domain/IP

For All Participants

C-TAS to Security Solution



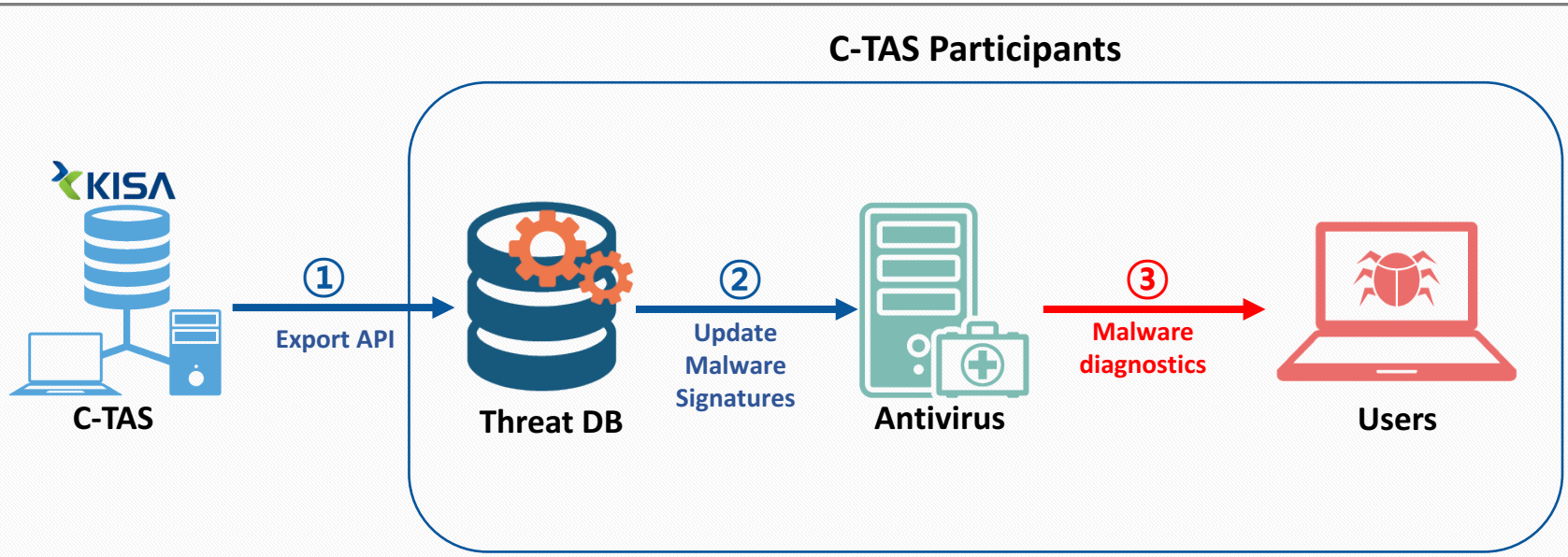
- Store the malicious Domain/IPs from C-TAS into Threat DB
- Apply cyber threat information in Threat DB to their security solutions

1-9. Cyber Threat Use Cases

2. Malware Sample

For AV & Security

C-TAS to Antivirus



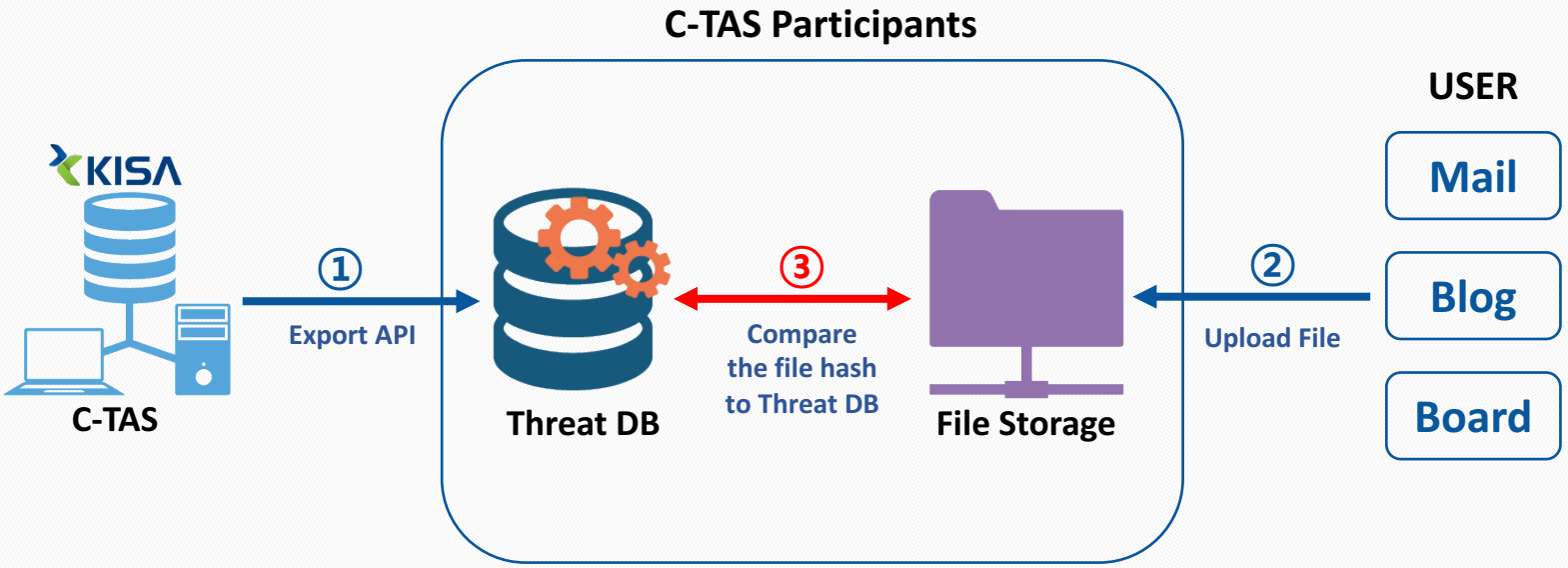
- Store the malware samples from C-TAS into Threat DB
- Update malware signatures for antivirus using Threat DB
- Detect malware in users' computer

1-9. Cyber Threat Use Cases

3. Malware Hash

For Web Service

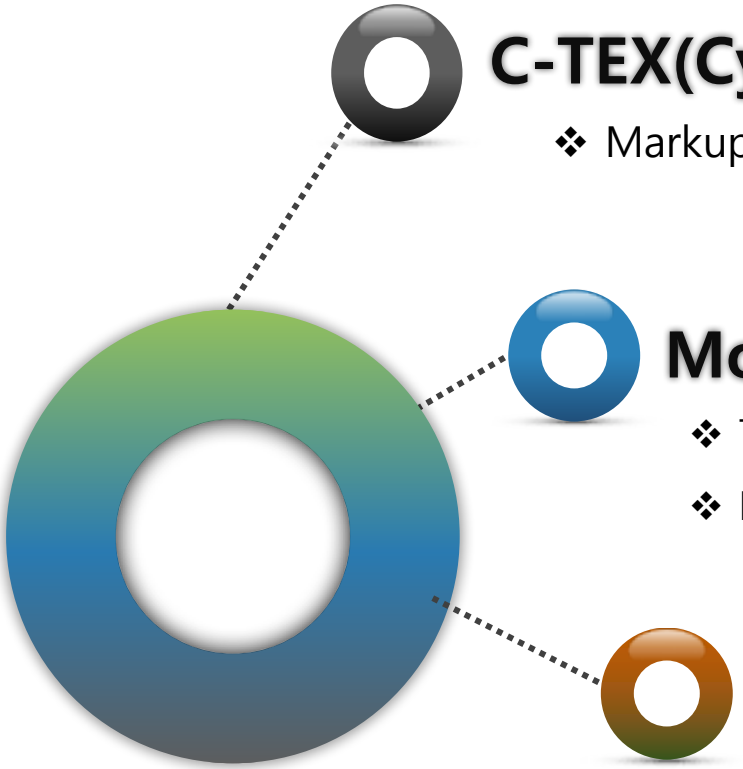
C-TAS to Web Service



- Store the malware hashes from C-TAS into Threat DB
- Web users upload files to a blog or send files over email
- Compare the file hashes to the malware hashes in Threat DB

2. C-TEX Structure

2-1. Introduction to C-TEX



C-TEX(Cyber Threat EXpression)

- ❖ Markup Language to express cyber threats

Motivation

- ❖ To make it easy for everybody to share cyber threats
- ❖ Even for kids!

Development

- ❖ 12.05 ~ 12.11 : MMS 1.0 & MML 1.0
- ❖ 13.08 ~ 13.12 : MMS 1.1 & MML 1.1
- ❖ 13.09 ~ 14.07 : C-TAS 1.0 & C-TAS 1.0
- ❖ 15.05 ~ 15.12 : C-TAS 1.1 & C-TEX 1.1 (MMS -> TIMS)
- ❖ 16.05 ~ 16.12 : C-TAS 1.2 & C-TEX 1.2 (with STIX 1.2)
- ❖ 17.05 ~ 17.12 : C-TAS 2.0 & C-TEX 2.0 (with STIX 2.0)

- ❖ C-TAS : Cyber Threat Analysis & Sharing
- ❖ C-TEX : Cyber Threat EXpression
- ❖ MMS : Malware Management System
- ❖ MML : Malware Markup Language
- ❖ TIMS : Threat Intelligence Management System

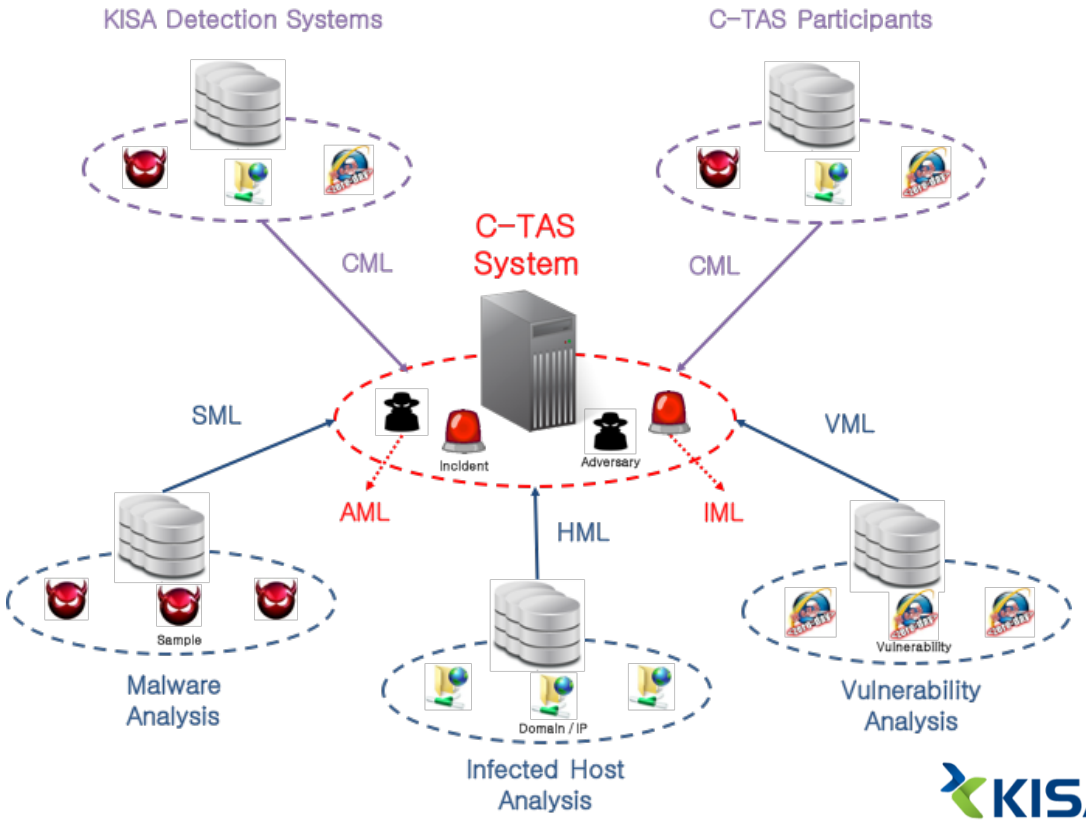
KISA

2-2. C-TEX Structure

C-TEX (Cyber Threat EXpression)

- Collect Markup Language: Address(Domain/IP), Sample(Malware), Vulnerability(Vulnerability)
- Core Markup Languages: Incident, Domain, Host, Sample, Vulnerability, Adversary

- CML (Collect Markup Language)
  - Address, Sample, Vulnerability
- IML (Incident Markup Language)
  - Details on cyber Incident
- DML (Domain Markup Language)
  - Details on registered Domain
- HML (Host Markup Language)
  - Details on hacked Host
- SML (Sample Markup Language)
  - Details on malware Sample
- VML (Vulnerability Markup Language)
  - Details on Vulnerability info
- AML (Adversary Markup Language)
  - Details on Adversary

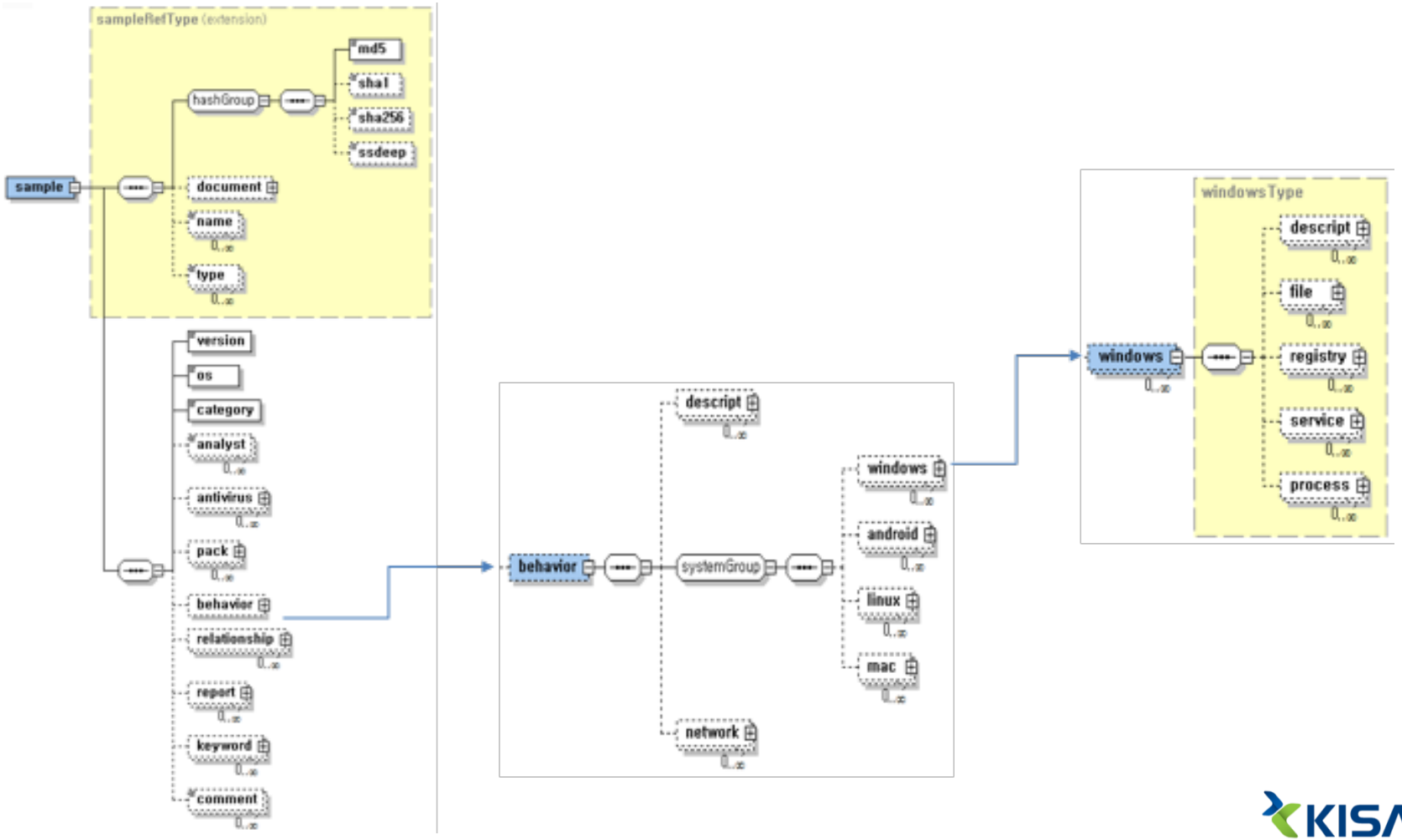


KrCERT

KISA

2-3. C-TEX Schema

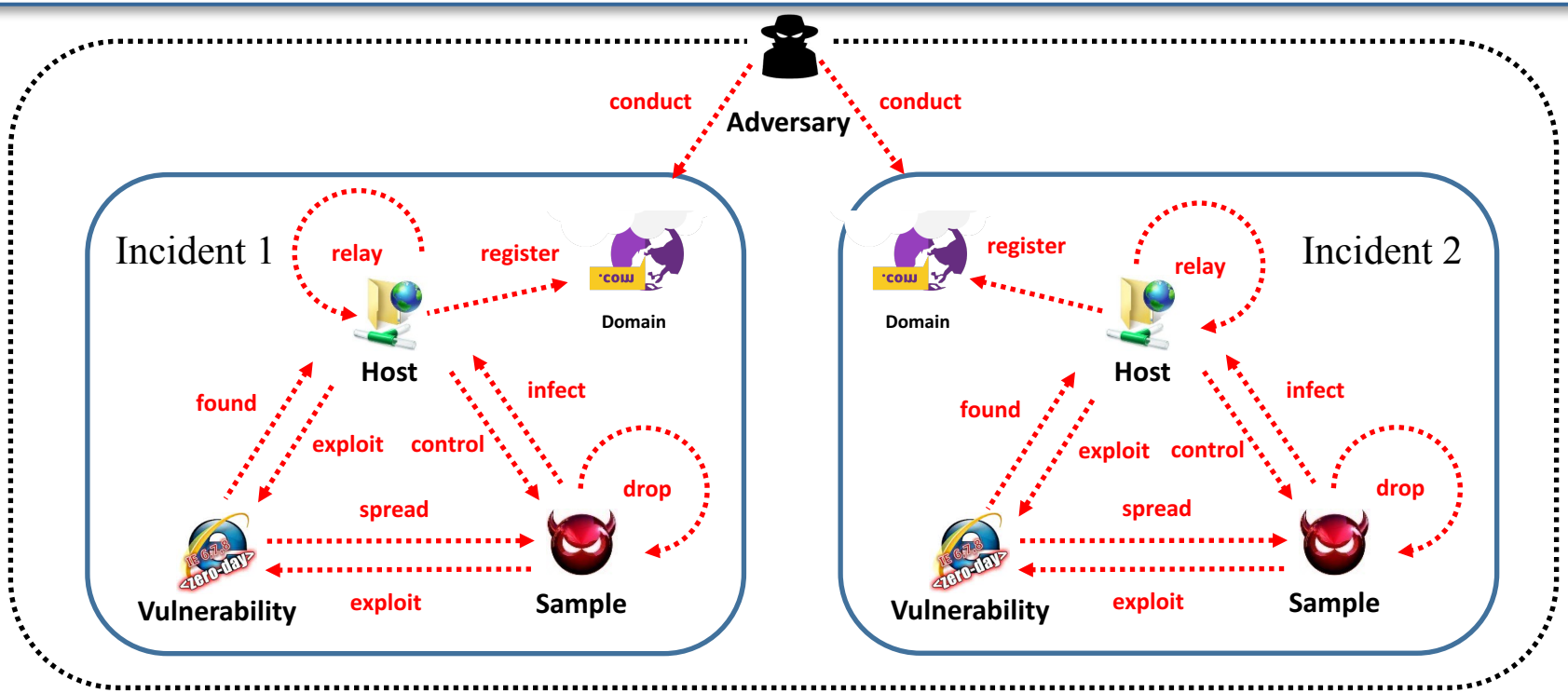
Sample Markup Language



2-4. C-TEXg Structure

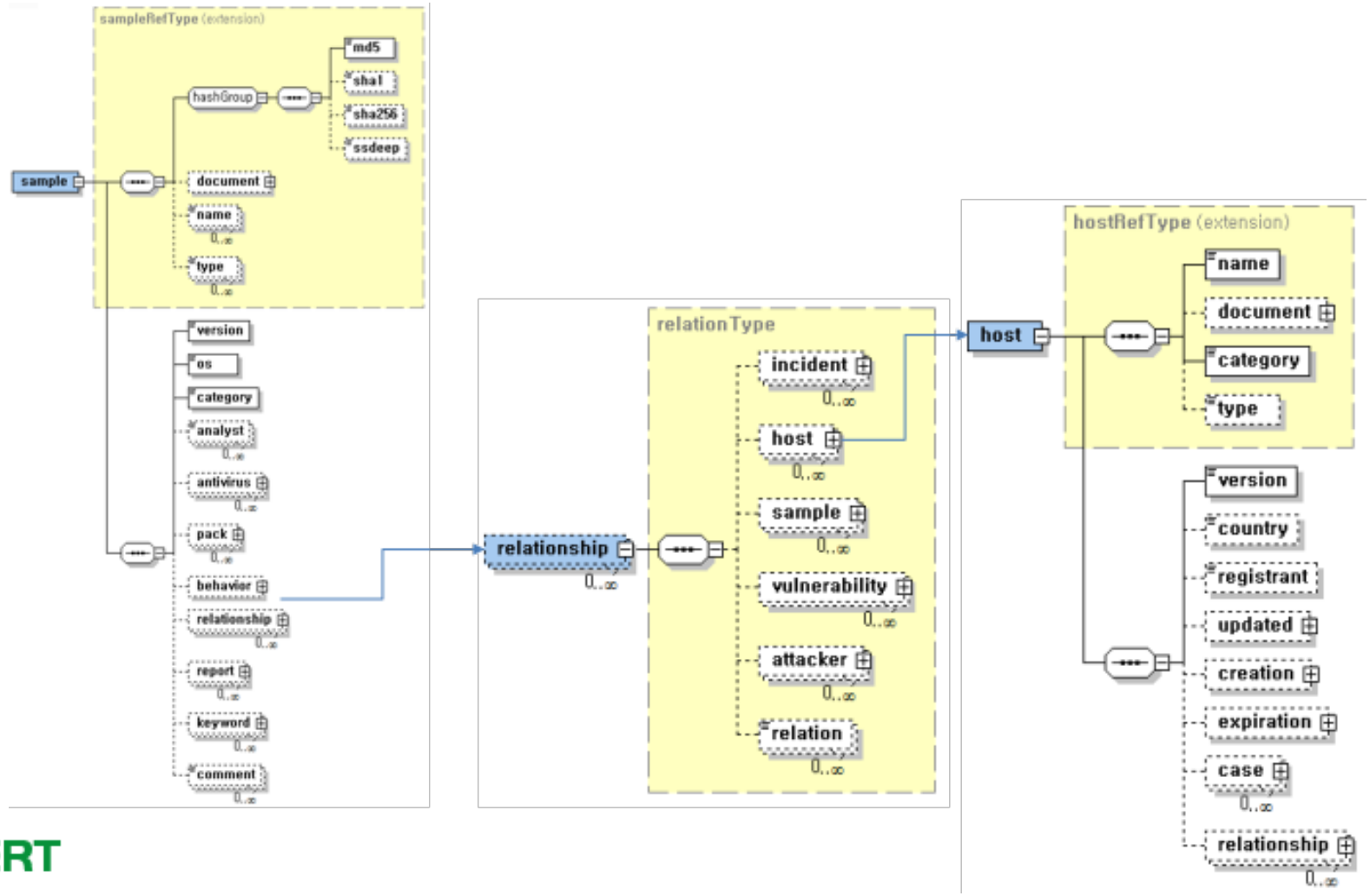
C-TEXg (C-TEX for graph)

- AML (Adversary) has relationships with IML (Incident)
- IML (Incident) has relationships with HML (Host), SML (Sample), VML (vulnerability)
- HML (Host), SML (Malware), VML (Vulnerability) has relationships with each other
- HML (Host) has relationship with DML (Domain)



2-5. C-TEXg Schema

Relationships between xMLs



KrCERT

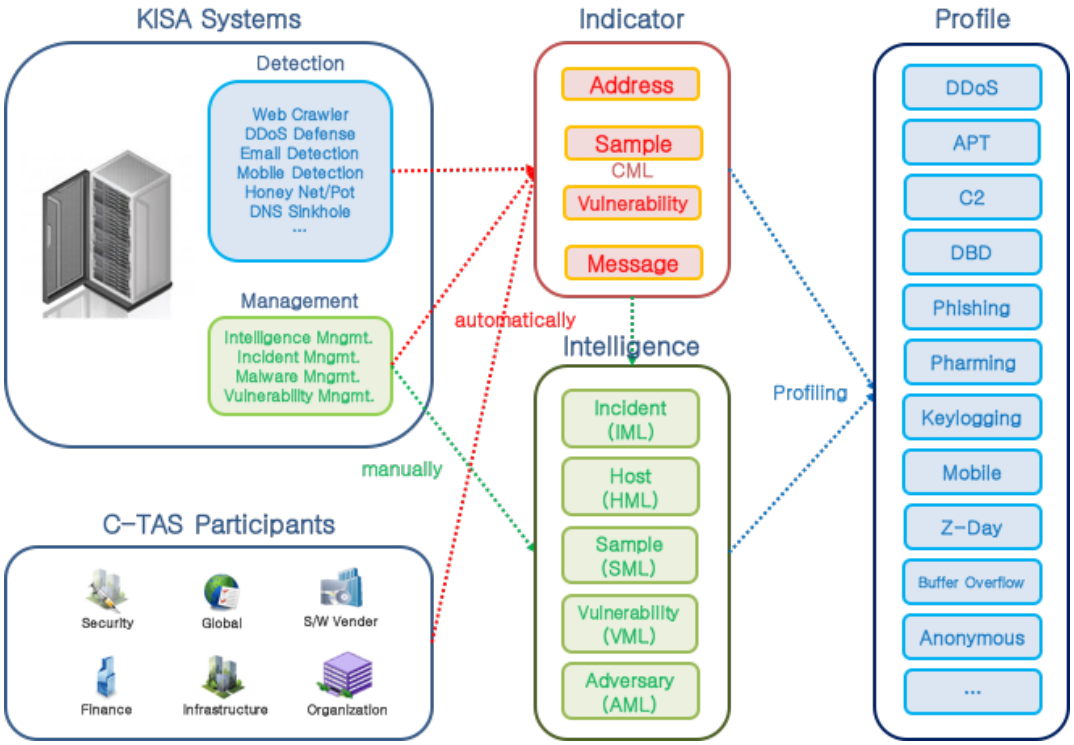
KISA

2-6. Internal Sources

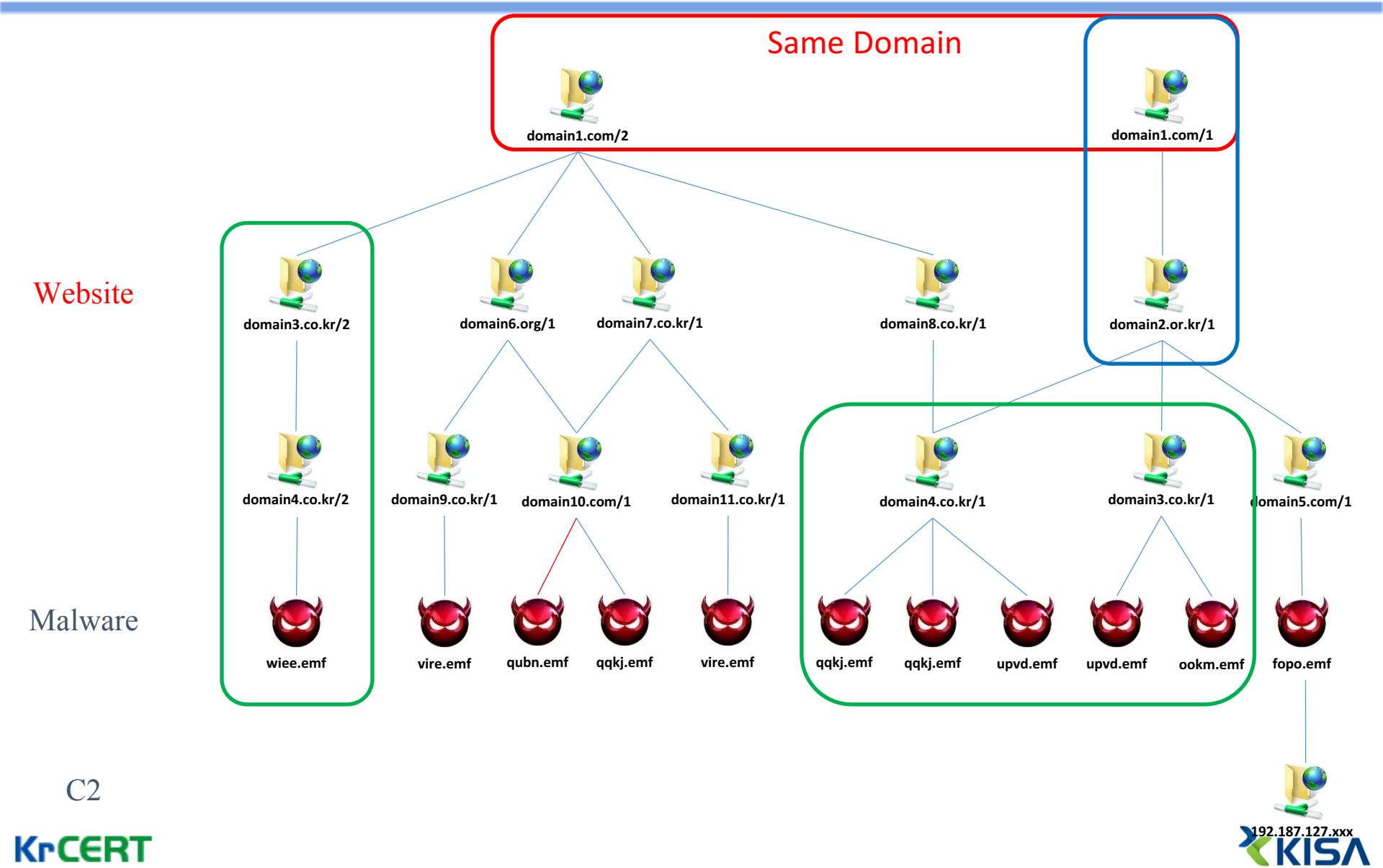
From KISA Systems

- Cyber Threat Detection Systems collect cyber threats in CML
- The analysts turn cyber threat information into intelligence in IML, HML, SML, VML, AML

- Cyber Threat Detection Systems
  - Web Crawler
  - DDoS Defense System
  - Email Detection Sysytem
  - Mobile Detection System
  - Honeypot/Honeynet
  - DNS Sinkhole
  - etc.
- Threat Intelligence Mngmt. System
  - Incident Mngmt. System
  - Malware Mngmt. System
  - Vulnerability Mngmt. System



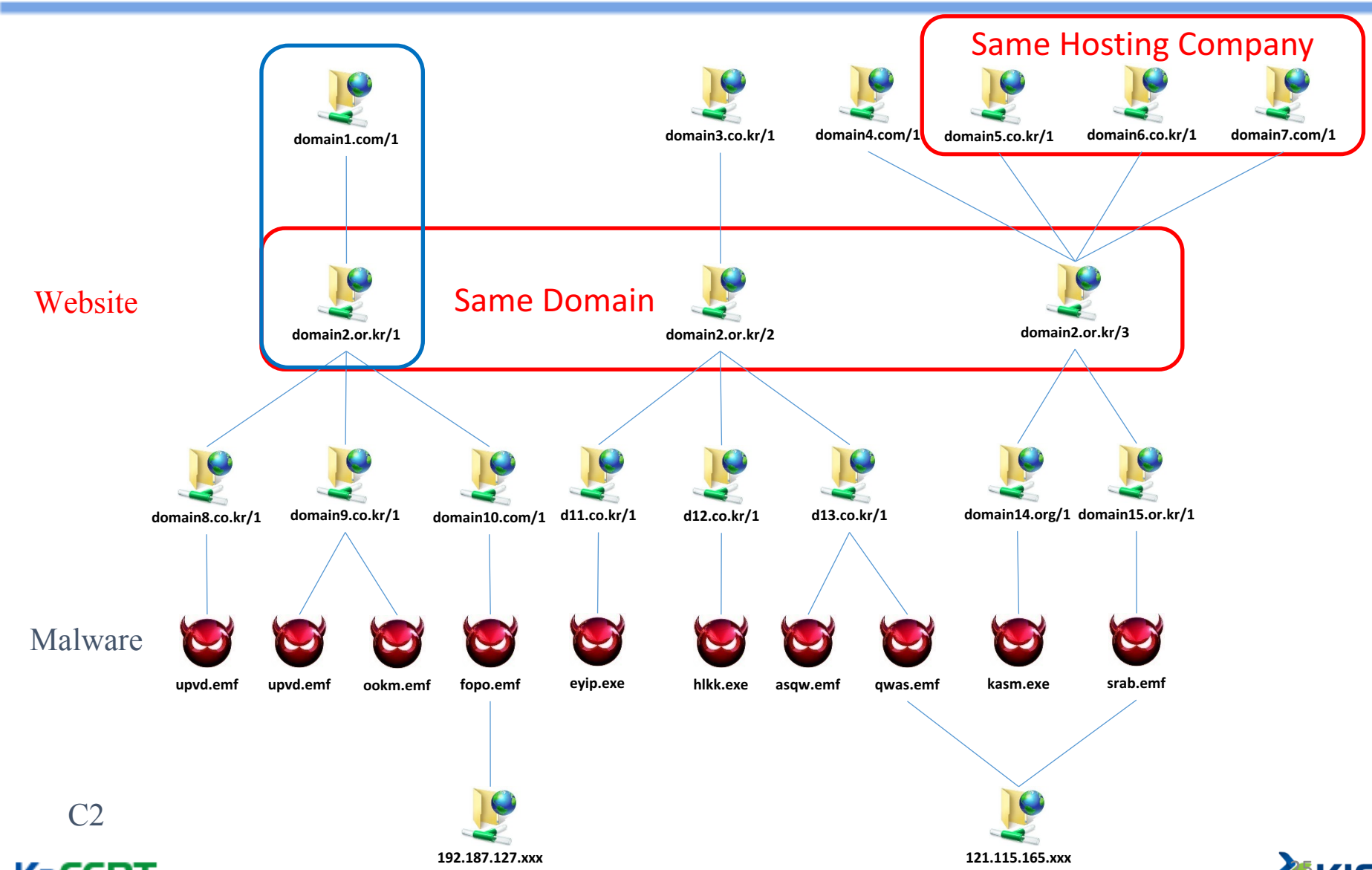
2-7. C-TEX Use Case (Drive By Download)



KrCERT

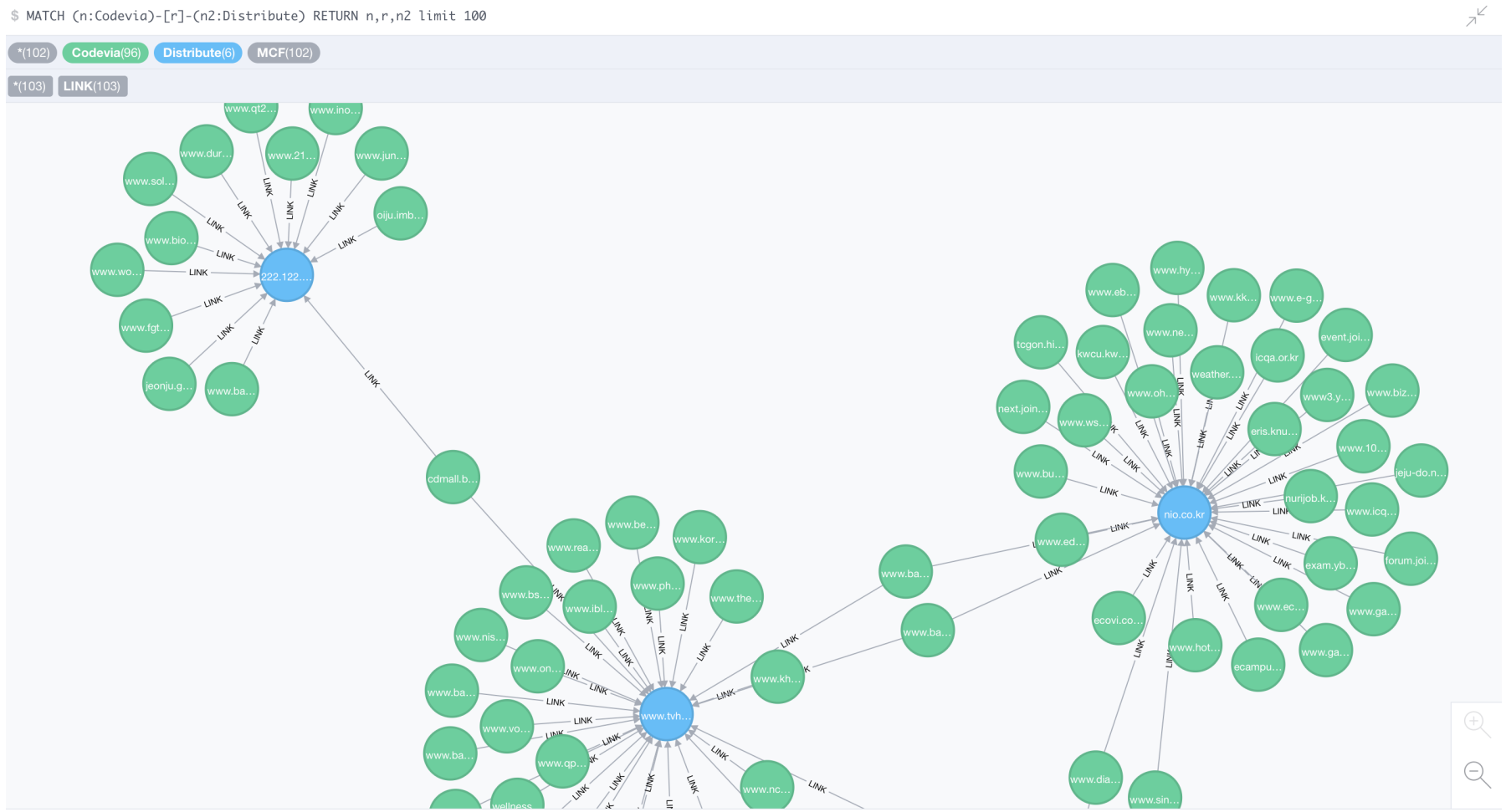
KISA

2-7. C-TEX Use Case (Drive By Download)



2-8. C-TEXg Use Case (Drive By Download)

C-TEXg in GraphDB



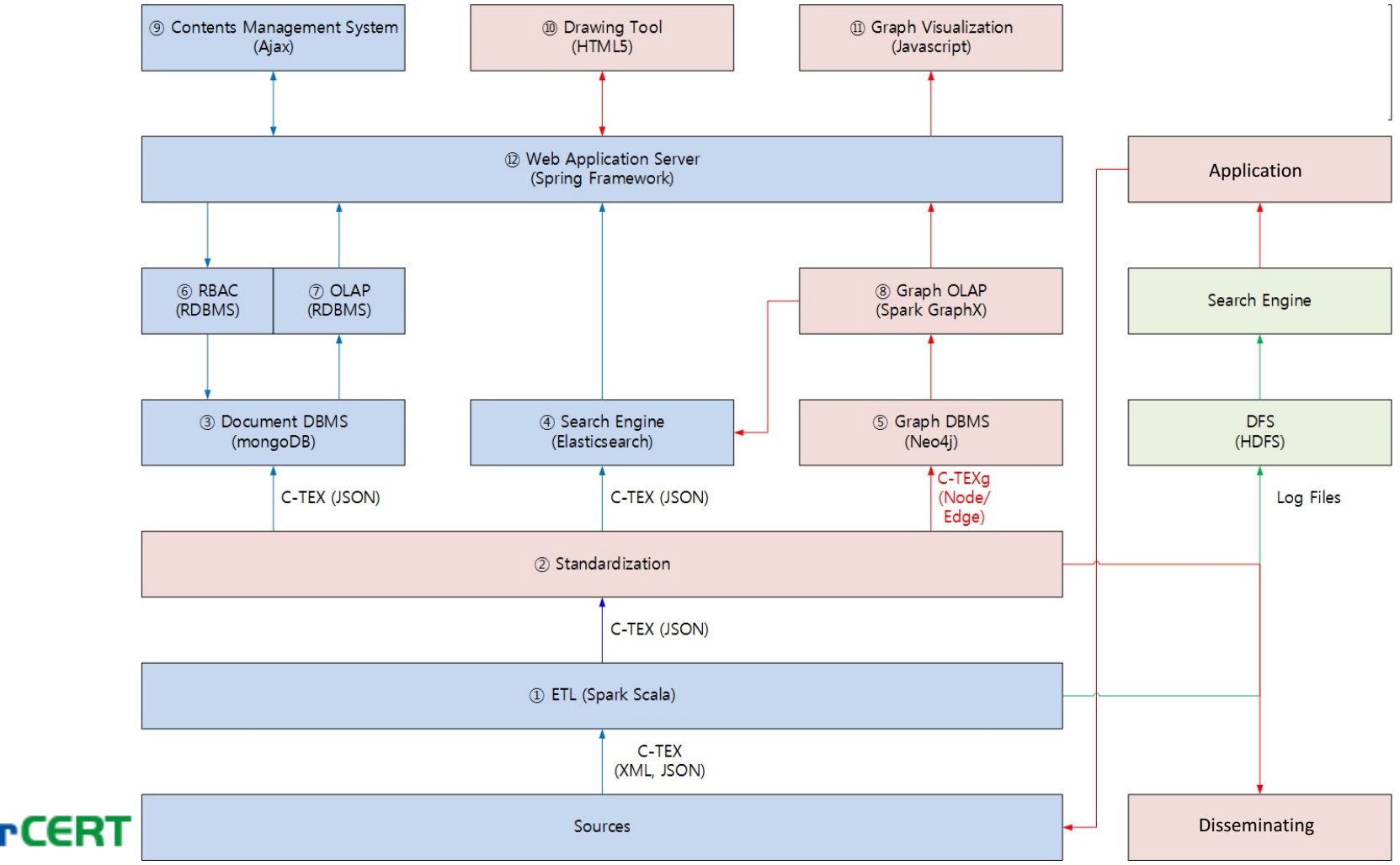
Displaying 102 nodes, 103 relationships (completed with 3 additional relationships).

AUTO-COMPLETE ON

3. Big Data in C-TAS

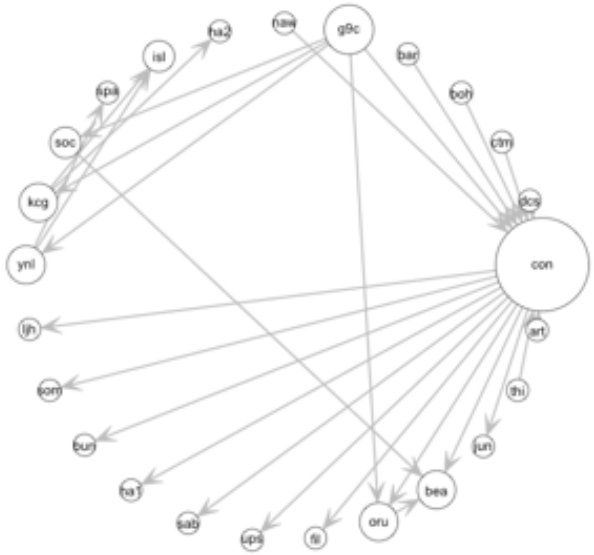
3-1. Big Data Platform in C-TAS

C-TAS System Architecture

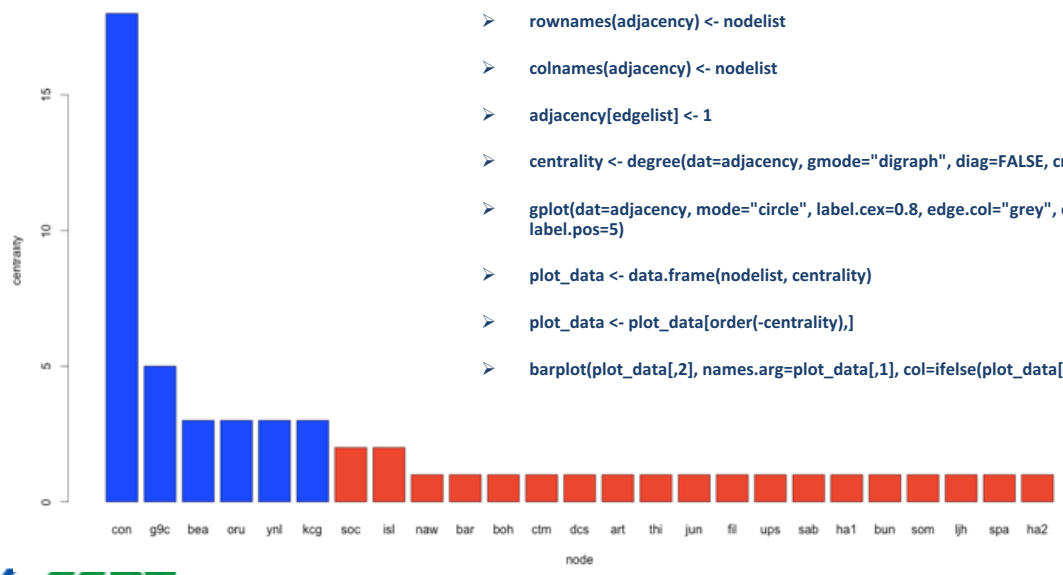


3-2. Big Data Analysis in C-TAS

Threat Network Analysis



- library(sna)
- edgelist <- read.csv(file="edgelist.csv", header=TRUE, sep=",")
- nodelist <- read.csv(file="nodelist.csv", header=TRUE, sep=",")
- edgelist <- as.matrix(edgelist)
- nodelist <- as.matrix(nodelist)
- adjacency <- matrix(data=0, nrow=25, ncol=25)
- rownames(adjacency) <- nodelist
- colnames(adjacency) <- nodelist
- adjacency[edgelist] <- 1
- centrality <- degree(dat=adjacency, gmode="digraph", diag=FALSE, cmode="freeman", rescale=FALSE)
- gplot(dat=adjacency, mode="circle", label.cex=0.8, edge.col="grey", displaylabels=TRUE, vertex.cex=sqrt(centrality), vertex.col="white", label.pos=5)
- plot_data <- data.frame(nodelist, centrality)
- plot_data <- plot_data[order(-centrality),]
- barplot(plot_data[,2], names.arg=plot_data[,1], col=ifelse(plot_data[,2]<3, "red", "blue"), xlab="node", ylab="centrality", main="TNA")



KrCERT

KISA

KISA KOREA INTERNET & SECURITY AGENCY

Thank you!